hyperledger-fabricdocs Documentation

Release master

hyperledger

Sep 02, 2020

Contents

Enterprise grade permissioned distributed ledger platform that offers modularity and versatility for a broad set of industry use cases.

CHAPTER 1

Introduction

In general terms, a blockchain is an immutable transaction ledger, maintained within a distributed network of *peer nodes*. These nodes each maintain a copy of the ledger by applying transactions that have been validated by a *consensus protocol*, grouped into blocks that include a hash that bind each block to the preceding block.

The first and most widely recognized application of blockchain is the Bitcoin cryptocurrency, though others have followed in its footsteps. Ethereum, an alternative cryptocurrency, took a different approach, integrating many of the same characteristics as Bitcoin but adding *smart contracts* to create a platform for distributed applications. Bitcoin and Ethereum fall into a class of blockchain that we would classify as *public permissionless* blockchain technology. Basically, these are public networks, open to anyone, where participants interact anonymously.

As the popularity of Bitcoin, Ethereum and a few other derivative technologies grew, interest in applying the underlying technology of the blockchain, distributed ledger and distributed application platform to more innovative *enterprise* use cases also grew. However, many enterprise use cases require performance characteristics that the permissionless blockchain technologies are unable (presently) to deliver. In addition, in many use cases, the identity of the participants is a hard requirement, such as in the case of financial transactions where Know-Your-Customer (KYC) and Anti-Money Laundering (AML) regulations must be followed.

For enterprise use, we need to consider the following requirements:

- Participants must be identified/identifiable
- Networks need to be *permissioned*
- High transaction throughput performance
- Low latency of transaction confirmation
- Privacy and confidentiality of transactions and data pertaining to business transactions

While many early blockchain platforms are currently being *adapted* for enterprise use, Hyperledger Fabric has been *designed* for enterprise use from the outset. The following sections describe how Hyperledger Fabric (Fabric) differentiates itself from other blockchain platforms and describes some of the motivation for its architectural decisions.

1.1 Hyperledger Fabric

Hyperledger Fabric is an open source enterprise-grade permissioned distributed ledger technology (DLT) platform, designed for use in enterprise contexts, that delivers some key differentiating capabilities over other popular distributed ledger or blockchain platforms.

One key point of differentiation is that Hyperledger was established under the Linux Foundation, which itself has a long and very successful history of nurturing open source projects under **open governance** that grow strong sustaining communities and thriving ecosystems. Hyperledger is governed by a diverse technical steering committee, and the Hyperledger Fabric project by a diverse set of maintainers from multiple organizations. It has a development community that has grown to over 35 organizations and nearly 200 developers since its earliest commits.

Fabric has a highly **modular** and **configurable** architecture, enabling innovation, versatility and optimization for a broad range of industry use cases including banking, finance, insurance, healthcare, human resources, supply chain and even digital music delivery.

Fabric is the first distributed ledger platform to support **smart contracts authored in general-purpose programming languages** such as Java, Go and Node.js, rather than constrained domain-specific languages (DSL). This means that most enterprises already have the skill set needed to develop smart contracts, and no additional training to learn a new language or DSL is needed.

The Fabric platform is also **permissioned**, meaning that, unlike with a public permissionless network, the participants are known to each other, rather than anonymous and therefore fully untrusted. This means that while the participants may not *fully* trust one another (they may, for example, be competitors in the same industry), a network can be operated under a governance model that is built off of what trust *does* exist between participants, such as a legal agreement or framework for handling disputes.

One of the most important of the platform's differentiators is its support for **pluggable consensus protocols** that enable the platform to be more effectively customized to fit particular use cases and trust models. For instance, when deployed within a single enterprise, or operated by a trusted authority, fully byzantine fault tolerant consensus might be considered unnecessary and an excessive drag on performance and throughput. In situations such as that, a crash fault-tolerant (CFT) consensus protocol might be more than adequate whereas, in a multi-party, decentralized use case, a more traditional byzantine fault tolerant (BFT) consensus protocol might be required.

Fabric can leverage consensus protocols that **do not require a native cryptocurrency** to incent costly mining or to fuel smart contract execution. Avoidance of a cryptocurrency reduces some significant risk/attack vectors, and absence of cryptographic mining operations means that the platform can be deployed with roughly the same operational cost as any other distributed system.

The combination of these differentiating design features makes Fabric one of the **better performing platforms** available today both in terms of transaction processing and transaction confirmation latency, and it enables **privacy and confidentiality** of transactions and the smart contracts (what Fabric calls "chaincode") that implement them.

Let's explore these differentiating features in more detail.

1.2 Modularity

Hyperledger Fabric has been specifically architected to have a modular architecture. Whether it is pluggable consensus, pluggable identity management protocols such as LDAP or OpenID Connect, key management protocols or cryptographic libraries, the platform has been designed at its core to be configured to meet the diversity of enterprise use case requirements.

At a high level, Fabric is comprised of the following modular components:

- A pluggable *ordering service* establishes consensus on the order of transactions and then broadcasts blocks to peers.

- A pluggable *membership service provider* is responsible for associating entities in the network with cryptographic identities.
- An optional *peer-to-peer gossip service* disseminates the blocks output by ordering service to other peers.
- Smart contracts ("chaincode") run within a container environment (e.g. Docker) for isolation. They can be written in standard programming languages but do not have direct access to the ledger state.
- The ledger can be configured to support a variety of DBMSs.
- A pluggable endorsement and validation policy enforcement that can be independently configured per application.

There is fair agreement in the industry that there is no "one blockchain to rule them all". Hyperledger Fabric can be configured in multiple ways to satisfy the diverse solution requirements for multiple industry use cases.

1.3 Permissioned vs Permissionless Blockchains

In a permissionless blockchain, virtually anyone can participate, and every participant is anonymous. In such a context, there can be no trust other than that the state of the blockchain, prior to a certain depth, is immutable. In order to mitigate this absence of trust, permissionless blockchains typically employ a "mined" native cryptocurrency or transaction fees to provide economic incentive to offset the extraordinary costs of participating in a form of byzantine fault tolerant consensus based on "proof of work" (PoW).

Permissioned blockchains, on the other hand, operate a blockchain amongst a set of known, identified and often vetted participants operating under a governance model that yields a certain degree of trust. A permissioned blockchain provides a way to secure the interactions among a group of entities that have a common goal but which may not fully trust each other. By relying on the identities of the participants, a permissioned blockchain can use more traditional crash fault tolerant (CFT) or byzantine fault tolerant (BFT) consensus protocols that do not require costly mining.

Additionally, in such a permissioned context, the risk of a participant intentionally introducing malicious code through a smart contract is diminished. First, the participants are known to one another and all actions, whether submitting application transactions, modifying the configuration of the network or deploying a smart contract are recorded on the blockchain following an endorsement policy that was established for the network and relevant transaction type. Rather than being completely anonymous, the guilty party can be easily identified and the incident handled in accordance with the terms of the governance model.

1.4 Smart Contracts

A smart contract, or what Fabric calls "chaincode", functions as a trusted distributed application that gains its security/trust from the blockchain and the underlying consensus among the peers. It is the business logic of a blockchain application.

There are three key points that apply to smart contracts, especially when applied to a platform:

- many smart contracts run concurrently in the network,
- they may be deployed dynamically (in many cases by anyone), and
- application code should be treated as untrusted, potentially even malicious.

Most existing smart-contract capable blockchain platforms follow an **order-execute** architecture in which the consensus protocol:

- validates and orders transactions then propagates them to all peer nodes,
- each peer then executes the transactions sequentially.

The order-execute architecture can be found in virtually all existing blockchain systems, ranging from public/permissionless platforms such as Ethereum (with PoW-based consensus) to permissioned platforms such as Tendermint, Chain, and Quorum.

Smart contracts executing in a blockchain that operates with the order-execute architecture must be deterministic; otherwise, consensus might never be reached. To address the non-determinism issue, many platforms require that the smart contracts be written in a non-standard, or domain-specific language (such as Solidity) so that non-deterministic operations can be eliminated. This hinders wide-spread adoption because it requires developers writing smart contracts to learn a new language and may lead to programming errors.

Further, since all transactions are executed sequentially by all nodes, performance and scale is limited. The fact that the smart contract code executes on every node in the system demands that complex measures be taken to protect the overall system from potentially malicious contracts in order to ensure resiliency of the overall system.

1.5 A New Approach

Fabric introduces a new architecture for transactions that we call **execute-order-validate**. It addresses the resiliency, flexibility, scalability, performance and confidentiality challenges faced by the order-execute model by separating the transaction flow into three steps:

- *execute* a transaction and check its correctness, thereby endorsing it,
- *order* transactions via a (pluggable) consensus protocol, and
- *validate* transactions against an application-specific endorsement policy before committing them to the ledger

This design departs radically from the order-execute paradigm in that Fabric executes transactions before reaching final agreement on their order.

In Fabric, an application-specific endorsement policy specifies which peer nodes, or how many of them, need to vouch for the correct execution of a given smart contract. Thus, each transaction need only be executed (endorsed) by the subset of the peer nodes necessary to satisfy the transaction's endorsement policy. This allows for parallel execution increasing overall performance and scale of the system. This first phase also **eliminates any non-determinism**, as inconsistent results can be filtered out before ordering.

Because we have eliminated non-determinism, Fabric is the first blockchain technology that **enables use of standard programming languages**. In the 1.1.0 release, smart contracts can be written in either Go or Node.js, while there are plans to support other popular languages including Java in subsequent releases.

1.6 Privacy and Confidentiality

As we have discussed, in a public, permissionless blockchain network that leverages PoW for its consensus model, transactions are executed on every node. This means that neither can there be confidentiality of the contracts themselves, nor of the transaction data that they process. Every transaction, and the code that implements it, is visible to every node in the network. In this case, we have traded confidentiality of contract and data for byzantine fault tolerant consensus delivered by PoW.

This lack of confidentiality can be problematic for many business/enterprise use cases. For example, in a network of supply-chain partners, some consumers might be given preferred rates as a means of either solidifying a relationship, or promoting additional sales. If every participant can see every contract and transaction, it becomes impossible to maintain such business relationships in a completely transparent network – everyone will want the preferred rates!

As a second example, consider the securities industry, where a trader building a position (or disposing of one) would not want her competitors to know of this, or else they will seek to get in on the game, weakening the trader's gambit.

In order to address the lack of privacy and confidentiality for purposes of delivering on enterprise use case requirements, blockchain platforms have adopted a variety of approaches. All have their trade-offs.

Encrypting data is one approach to providing confidentiality; however, in a permissionless network leveraging PoW for its consensus, the encrypted data is sitting on every node. Given enough time and computational resource, the encryption could be broken. For many enterprise use cases, the risk that their information could become compromised is unacceptable.

Zero knowledge proofs (ZKP) are another area of research being explored to address this problem, the trade-off here being that, presently, computing a ZKP requires considerable time and computational resources. Hence, the trade-off in this case is performance for confidentiality.

In a permissioned context that can leverage alternate forms of consensus, one might explore approaches that restrict the distribution of confidential information exclusively to authorized nodes.

Hyperledger Fabric, being a permissioned platform, enables confidentiality through its channel architecture. Basically, participants on a Fabric network can establish a "channel" between the subset of participants that should be granted visibility to a particular set of transactions. Think of this as a network overlay. Thus, only those nodes that participate in a channel have access to the smart contract (chaincode) and data transacted, preserving the privacy and confidentiality of both.

To improve upon its privacy and confidentiality capabilities, Fabric has added support for private data and is working on zero knowledge proofs (ZKP) available in the future. More on this as it becomes available.

1.7 Pluggable Consensus

The ordering of transactions is delegated to a modular component for consensus that is logically decoupled from the peers that execute transactions and maintain the ledger. Specifically, the ordering service. Since consensus is modular, its implementation can be tailored to the trust assumption of a particular deployment or solution. This modular architecture allows the platform to rely on well-established toolkits for CFT (crash fault-tolerant) or BFT (byzantine fault-tolerant) ordering.

In the currently available releases, Fabric offers a CFT ordering service implemented with Kafka and Zookeeper. In subsequent releases, Fabric will deliver a Raft consensus ordering service implemented with etcd/Raft and a fully decentralized BFT ordering service.

Note also that these are not mutually exclusive. A Fabric network can have multiple ordering services supporting different applications or application requirements.

1.8 Performance and Scalability

Performance of a blockchain platform can be affected by many variables such as transaction size, block size, network size, as well as limits of the hardware, etc. The Hyperledger community is currently developing a draft set of measures within the Performance and Scale working group, along with a corresponding implementation of a benchmarking framework called Hyperledger Caliper.

While that work continues to be developed and should be seen as a definitive measure of blockchain platform performance and scale characteristics, a team from IBM Research has published a peer reviewed paper that evaluated the architecture and performance of Hyperledger Fabric. The paper offers an in-depth discussion of the architecture of Fabric and then reports on the team's performance evaluation of the platform using a preliminary release of Hyperledger Fabric v1.1.

The benchmarking efforts that the research team did yielded a significant number of performance improvements for the Fabric v1.1.0 release that more than doubled the overall performance of the platform from the v1.0.0 release levels.

1.9 Conclusion

Any serious evaluation of blockchain platforms should include Hyperledger Fabric in its short list.

Combined, the differentiating capabilities of Fabric make it a highly scalable system for permissioned blockchains supporting flexible trust assumptions that enable the platform to support a wide range of industry use cases ranging from government, to finance, to supply-chain logistics, to healthcare and so much more.

More importantly, Hyperledger Fabric is the most active of the (currently) ten Hyperledger projects. The community building around the platform is growing steadily, and the innovation delivered with each successive release far outpaces any of the other enterprise blockchain platforms.

1.10 Acknowledgement

The preceding is derived from the peer reviewed "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains" - Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolic, Sharon Weed Cocco, Jason Yellick

CHAPTER 2

What's new in v1.3

A quick rundown of the new features and documentation in the v1.3 release of Hyperledger Fabric:

2.1 New features

- *MSP Implementation with Identity Mixer*: A way to keep identities anonymous and unlinkable through the use of zero-knowledge proofs. There is a tool that can generate Identity Mixer credentials in test environments known as *idexmigen*, the documentation for which can be found in *Identity Mixer MSP configuration generator (idemixgen)*.
- *Setting key-level endorsement policies*: Allows the default chaincode-level endorsement policy to be overridden by a per-key endorsement policy.
- *Query the CouchDB State Database With Pagination*: Clients can now page through result sets from chaincode queries, making it feasible to support large result sets with high performance.
- *Chaincode for Developers*: As an addition to the current Fabric support for chaincode written in Go and node.js, Java is now supported. You can find a javadoc for this here.
- *Peer channel-based event services*: The peer channel-based event service itself is not new (it first debuted in v1.1), but the v1.3 release marks the end of the old event hub. Applications using the old event hub must switch over to the new peer channel-based event service prior to upgrading to v1.3.

2.2 New tutorials

- *Upgrading to the Newest Version of Fabric*: Leverages the BYFN network to show how an upgrade flow should work. Includes both a script (which can serve as a template for upgrades), as well as the individual commands.
- *Query the CouchDB State Database With Pagination*: Expands the current CouchDB tutorial to add pagination.

2.3 Other new documentation

- *Blockchain network*: Conceptual documentation that shows how the parts of a network interact with each other. The initial version of this document was added in v1.2.

CHAPTER 3

Release notes

For more information, including *FAB* numbers for the issues and code reviews that made up these changes (in addition to other hygiene/performance/bug fixes we did not explicitly document), check out the release notes. Note that these links will not work on the release candidate, only on the GA release.

- Fabric release notes.
- Fabric CA release notes.

CHAPTER 4

Key Concepts

4.1 Introduction

Hyperledger Fabric is a platform for distributed ledger solutions underpinned by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility, and scalability. It is designed to support pluggable implementations of different components and accommodate the complexity and intricacies that exist across the economic ecosystem.

We recommend first-time users begin by going through the rest of the introduction below in order to gain familiarity with how blockchains work and with the specific features and components of Hyperledger Fabric.

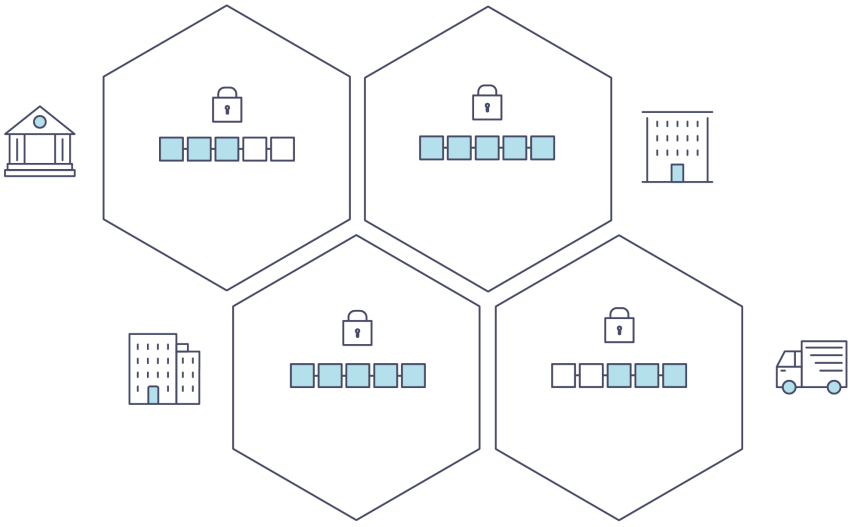
Once comfortable — or if you're already familiar with blockchain and Hyperledger Fabric — go to *Getting Started* and from there explore the demos, technical specifications, APIs, etc.

4.1.1 What is a Blockchain?

A Distributed Ledger

At the heart of a blockchain network is a distributed ledger that records all the transactions that take place on the network.

A blockchain ledger is often described as **decentralized** because it is replicated across many network participants, each of whom **collaborate** in its maintenance. We'll see that decentralization and collaboration are powerful attributes that mirror the way businesses exchange goods and services in the real world.



In addition to being decentralized and collaborative, the information recorded to a blockchain is append-only, using cryptographic techniques that guarantee that once a transaction has been added to the ledger it cannot be modified. This property of "immutability" makes it simple to determine the provenance of information because participants can be sure information has not been changed after the fact. It's why blockchains are sometimes described as **systems of proof**.

Smart Contracts

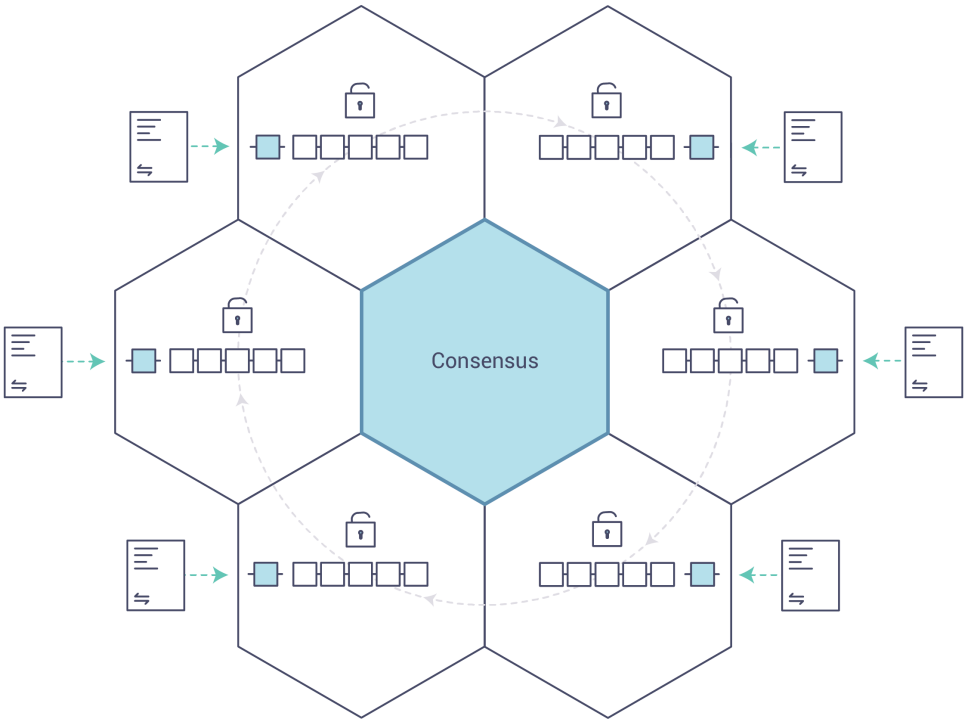
To support the consistent update of information — and to enable a whole host of ledger functions (transacting, querying, etc) — a blockchain network uses **smart contracts** to provide controlled access to the ledger.

Smart contracts are not only a key mechanism for encapsulating information and keeping it simple across the network, they can also be written to allow participants to execute certain aspects of transactions automatically.

A smart contract can, for example, be written to stipulate the cost of shipping an item where the shipping charge changes depending on how quickly the item arrives. With the terms agreed to by both parties and written to the ledger, the appropriate funds change hands automatically when the item is received.

Consensus

The process of keeping the ledger transactions synchronized across the network — to ensure that ledgers update only when transactions are approved by the appropriate participants, and that when ledgers do update, they update with the same transactions in the same order — is called **consensus**.



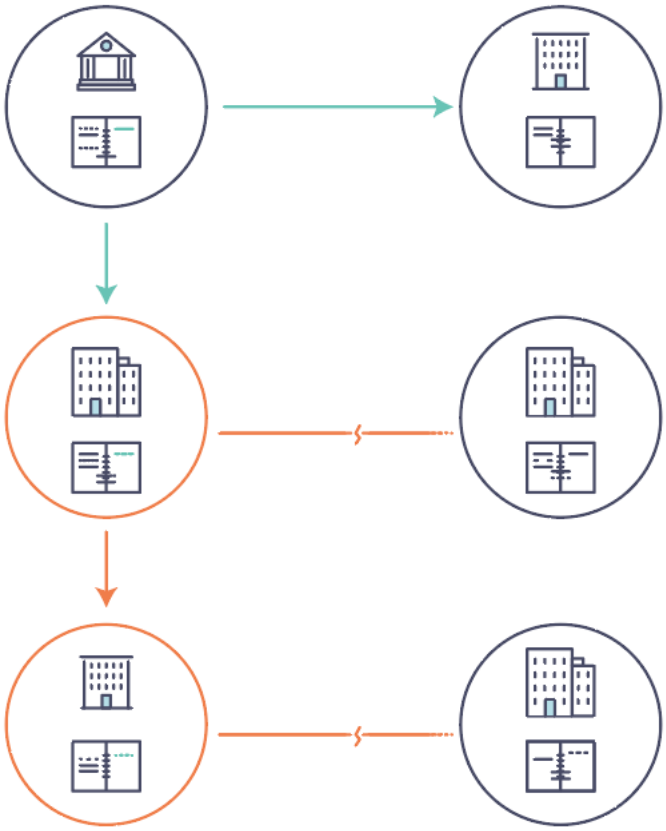
You'll learn a lot more about ledgers, smart contracts and consensus later. For now, it's enough to think of a blockchain as a shared, replicated transaction system which is updated via smart contracts and kept consistently synchronized through a collaborative process called consensus.

4.1.2 Why is a Blockchain useful?

Today's Systems of Record

The transactional networks of today are little more than slightly updated versions of networks that have existed since business records have been kept. The members of a **business network** transact with each other, but they maintain separate records of their transactions. And the things they're transacting — whether it's Flemish tapestries in the 16th century or the securities of today — must have their provenance established each time they're sold to ensure that the business selling an item possesses a chain of title verifying their ownership of it.

What you're left with is a business network that looks like this:



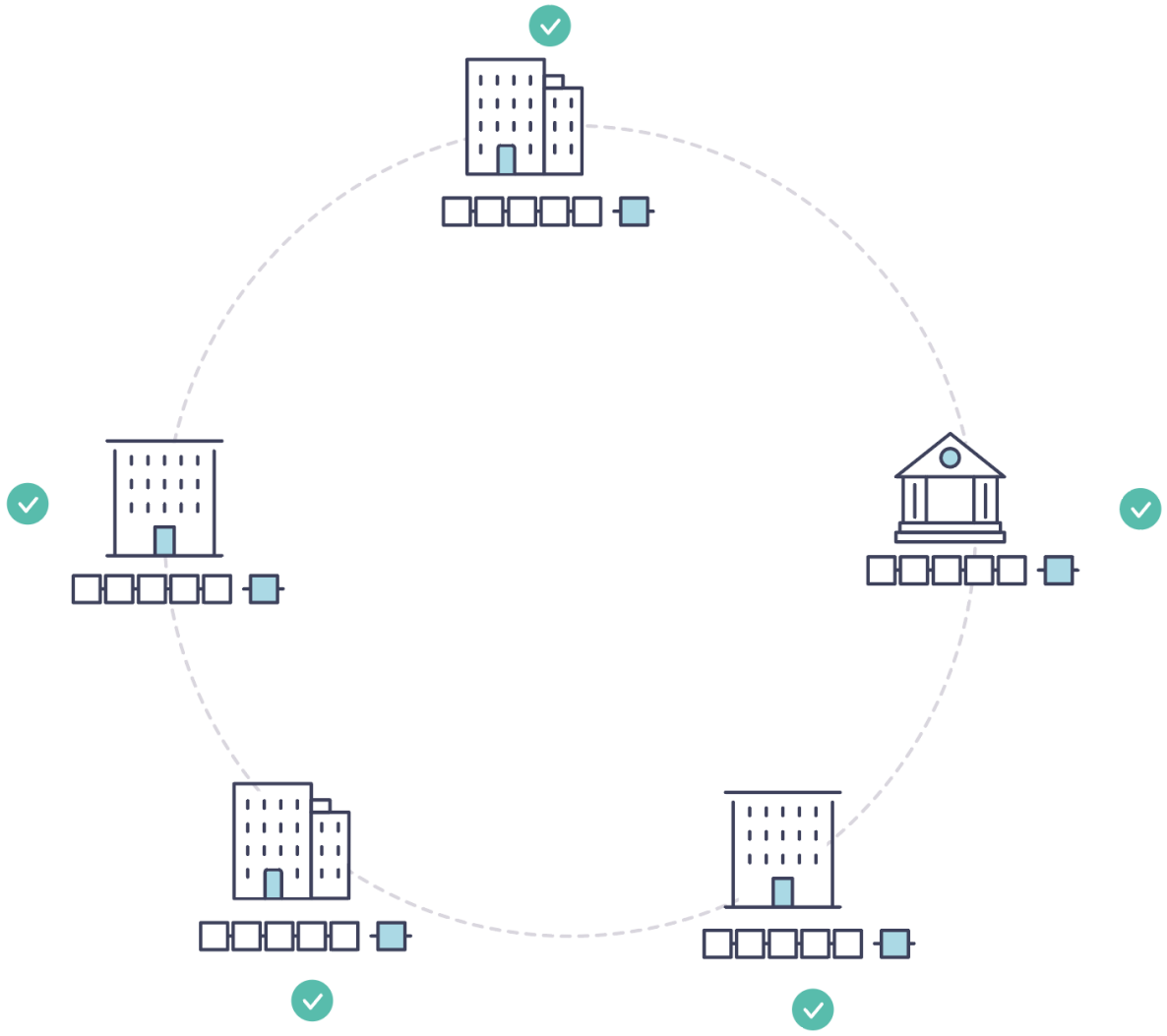
Modern technology has taken this process from stone tablets and paper folders to hard drives and cloud platforms, but the underlying structure is the same. Unified systems for managing the identity of network participants do not exist, establishing provenance is so laborious it takes days to clear securities transactions (the world volume of which is numbered in the many trillions of dollars), contracts must be signed and executed manually, and every database in the system contains unique information and therefore represents a single point of failure.

It's impossible with today's fractured approach to information and process sharing to build a system of record that spans a business network, even though the needs of visibility and trust are clear.

The Blockchain Difference

What if, instead of the rat's nest of inefficiencies represented by the "modern" system of transactions, business networks had standard methods for establishing identity on the network, executing transactions, and storing data? What if establishing the provenance of an asset could be determined by looking through a list of transactions that, once written, cannot be changed, and can therefore be trusted?

That business network would look more like this:



This is a blockchain network, wherein every participant has their own replicated copy of the ledger. In addition to ledger information being shared, the processes which update the ledger are also shared. Unlike today's systems, where a participant's **private** programs are used to update their **private** ledgers, a blockchain system has **shared** programs to update **shared** ledgers.

With the ability to coordinate their business network through a shared ledger, blockchain networks can reduce the time, cost, and risk associated with private information and processing while improving trust and visibility.

You now know what blockchain is and why it's useful. There are a lot of other details that are important, but they all relate to these fundamental ideas of the sharing of information and processes.

4.1.3 What is Hyperledger Fabric?

The Linux Foundation founded the Hyperledger project in 2015 to advance cross-industry blockchain technologies. Rather than declaring a single blockchain standard, it encourages a collaborative approach to developing blockchain technologies via a community process, with intellectual property rights that encourage open development and the adoption of key standards over time.

Hyperledger Fabric is one of the blockchain projects within Hyperledger. Like other blockchain technologies, it has a ledger, uses smart contracts, and is a system by which participants manage their transactions.

Where Hyperledger Fabric breaks from some other blockchain systems is that it is **private** and **permissioned**. Rather than an open permissionless system that allows unknown identities to participate in the network (requiring protocols like "proof of work" to validate transactions and secure the network), the members of a Hyperledger Fabric network enroll through a trusted **Membership Service Provider (MSP)**.

Hyperledger Fabric also offers several pluggable options. Ledger data can be stored in multiple formats, consensus mechanisms can be swapped in and out, and different MSPs are supported.

Hyperledger Fabric also offers the ability to create **channels**, allowing a group of participants to create a separate ledger of transactions. This is an especially important option for networks where some participants might be competitors and not want every transaction they make — a special price they're offering to some participants and not others, for example — known to every participant. If two participants form a channel, then those participants — and no others — have copies of the ledger for that channel.

Shared Ledger

Hyperledger Fabric has a ledger subsystem comprising two components: the **world state** and the **transaction log**. Each participant has a copy of the ledger to every Hyperledger Fabric network they belong to.

The world state component describes the state of the ledger at a given point in time. It's the database of the ledger. The transaction log component records all transactions which have resulted in the current value of the world state; it's the update history for the world state. The ledger, then, is a combination of the world state database and the transaction log history.

The ledger has a replaceable data store for the world state. By default, this is a LevelDB key-value store database. The transaction log does not need to be pluggable. It simply records the before and after values of the ledger database being used by the blockchain network.

Smart Contracts

Hyperledger Fabric smart contracts are written in **chaincode** and are invoked by an application external to the blockchain when that application needs to interact with the ledger. In most cases, chaincode interacts only with the database component of the ledger, the world state (querying it, for example), and not the transaction log.

Chaincode can be implemented in several programming languages. Currently, Go and Node are supported.

Privacy

Depending on the needs of a network, participants in a Business-to-Business (B2B) network might be extremely sensitive about how much information they share. For other networks, privacy will not be a top concern.

Hyperledger Fabric supports networks where privacy (using channels) is a key operational requirement as well as networks that are comparatively open.

Consensus

Transactions must be written to the ledger in the order in which they occur, even though they might be between different sets of participants within the network. For this to happen, the order of transactions must be established and a method for rejecting bad transactions that have been inserted into the ledger in error (or maliciously) must be put into place.

This is a thoroughly researched area of computer science, and there are many ways to achieve it, each with different trade-offs. For example, PBFT (Practical Byzantine Fault Tolerance) can provide a mechanism for file replicas to communicate with each other to keep each copy consistent, even in the event of corruption. Alternatively, in Bitcoin, ordering happens through a process called mining where competing computers race to solve a cryptographic puzzle which defines the order that all processes subsequently build upon.

Hyperledger Fabric has been designed to allow network starters to choose a consensus mechanism that best represents the relationships that exist between participants. As with privacy, there is a spectrum of needs; from networks that are highly structured in their relationships to those that are more peer-to-peer.

We'll learn more about the Hyperledger Fabric consensus mechanisms, which currently include SOLO and Kafka.

4.1.4 Where can I learn more?

- Identity (conceptual documentation)

A conceptual doc that will take you through the critical role identities play in a Fabric network (using an established PKI structure and x.509 certificates).

- Membership (conceptual documentation)

Talks through the role of a Membership Service Provider (MSP), which converts identities into roles in a Fabric network.

- Peers (conceptual documentation)

Peers — owned by organizations — host the ledger and smart contracts and make up the physical structure of a Fabric network.

- *Building Your First Network* (tutorial)

Learn how to download Fabric binaries and bootstrap your own sample network with a sample script. Then tear down the network and learn how it was constructed one step at a time.

- *Writing Your First Application* (tutorial)

Deploys a very simple network — even simpler than Build Your First Network — to use with a simple smart contract and application.

- *Transaction Flow*

A high level look at a sample transaction flow.

- *Hyperledger Fabric Model*

A high level look at some of components and concepts brought up in this introduction as well as a few others and describes how they work together in a sample transaction flow.

4.2 Hyperledger Fabric Functionalities

Hyperledger Fabric is an implementation of distributed ledger technology (DLT) that delivers enterprise-ready network security, scalability, confidentiality and performance, in a modular blockchain architecture. Hyperledger Fabric delivers the following blockchain network functionalities:

4.2.1 Identity management

To enable permissioned networks, Hyperledger Fabric provides a membership identity service that manages user IDs and authenticates all participants on the network. Access control lists can be used to provide additional layers of permission through authorization of specific network operations. For example, a specific user ID could be permitted to invoke a chaincode application, but be blocked from deploying new chaincode.

4.2.2 Privacy and confidentiality

Hyperledger Fabric enables competing business interests, and any groups that require private, confidential transactions, to coexist on the same permissioned network. Private **channels** are restricted messaging paths that can be used to provide transaction privacy and confidentiality for specific subsets of network members. All data, including transaction, member and channel information, on a channel are invisible and inaccessible to any network members not explicitly granted access to that channel.

4.2.3 Efficient processing

Hyperledger Fabric assigns network roles by node type. To provide concurrency and parallelism to the network, transaction execution is separated from transaction ordering and commitment. Executing transactions prior to ordering them enables each peer node to process multiple transactions simultaneously. This concurrent execution increases processing efficiency on each peer and accelerates delivery of transactions to the ordering service.

In addition to enabling parallel processing, the division of labor unburdens ordering nodes from the demands of transaction execution and ledger maintenance, while peer nodes are freed from ordering (consensus) workloads. This bifurcation of roles also limits the processing required for authorization and authentication; all peer nodes do not have to trust all ordering nodes, and vice versa, so processes on one can run independently of verification by the other.

4.2.4 Chaincode functionality

Chaincode applications encode logic that is invoked by specific types of transactions on the channel. Chaincode that defines parameters for a change of asset ownership, for example, ensures that all transactions that transfer ownership are subject to the same rules and requirements. **System chaincode** is distinguished as chaincode that defines operating parameters for the entire channel. Lifecycle and configuration system chaincode defines the rules for the channel; endorsement and validation system chaincode defines the requirements for endorsing and validating transactions.

4.2.5 Modular design

Hyperledger Fabric implements a modular architecture to provide functional choice to network designers. Specific algorithms for identity, ordering (consensus) and encryption, for example, can be plugged in to any Hyperledger Fabric network. The result is a universal blockchain architecture that any industry or public domain can adopt, with the assurance that its networks will be interoperable across market, regulatory and geographic boundaries.

4.3 Hyperledger Fabric Model

This section outlines the key design features woven into Hyperledger Fabric that fulfill its promise of a comprehensive, yet customizable, enterprise blockchain solution:

- *Assets* — Asset definitions enable the exchange of almost anything with monetary value over the network, from whole foods to antique cars to currency futures.
- *Chaincode* — Chaincode execution is partitioned from transaction ordering, limiting the required levels of trust and verification across node types, and optimizing network scalability and performance.
- *Ledger Features* — The immutable, shared ledger encodes the entire transaction history for each channel, and includes SQL-like query capability for efficient auditing and dispute resolution.
- *Privacy* — Channels and private data collections enable private and confidential multi-lateral transactions that are usually required by competing businesses and regulated industries that exchange assets on a common network.
- *Security & Membership Services* — Permissioned membership provides a trusted blockchain network, where participants know that all transactions can be detected and traced by authorized regulators and auditors.
- *Consensus* — A unique approach to consensus enables the flexibility and scalability needed for the enterprise.

4.3.1 Assets

Assets can range from the tangible (real estate and hardware) to the intangible (contracts and intellectual property). Hyperledger Fabric provides the ability to modify assets using chaincode transactions.

Assets are represented in Hyperledger Fabric as a collection of key-value pairs, with state changes recorded as transactions on a *Channel* ledger. Assets can be represented in binary and/or JSON form.

You can easily define and use assets in your Hyperledger Fabric applications using the Hyperledger Composer tool.

4.3.2 Chaincode

Chaincode is software defining an asset or assets, and the transaction instructions for modifying the asset(s); in other words, it's the business logic. Chaincode enforces the rules for reading or altering key-value pairs or other state database information. Chaincode functions execute against the ledger's current state database and are initiated through a transaction proposal. Chaincode execution results in a set of key-value writes (write set) that can be submitted to the network and applied to the ledger on all peers.

4.3.3 Ledger Features

The ledger is the sequenced, tamper-resistant record of all state transitions in the fabric. State transitions are a result of chaincode invocations ('transactions') submitted by participating parties. Each transaction results in a set of asset key-value pairs that are committed to the ledger as creates, updates, or deletes.

The ledger is comprised of a blockchain ('chain') to store the immutable, sequenced record in blocks, as well as a state database to maintain current fabric state. There is one ledger per channel. Each peer maintains a copy of the ledger for each channel of which they are a member.

Some features of a Fabric ledger:

- Query and update ledger using key-based lookups, range queries, and composite key queries
- Read-only queries using a rich query language (if using CouchDB as state database)
- Read-only history queries — Query ledger history for a key, enabling data provenance scenarios
- Transactions consist of the versions of keys/values that were read in chaincode (read set) and keys/values that were written in chaincode (write set)
- Transactions contain signatures of every endorsing peer and are submitted to ordering service
- Transactions are ordered into blocks and are "delivered" from an ordering service to peers on a channel
- Peers validate transactions against endorsement policies and enforce the policies
- Prior to appending a block, a versioning check is performed to ensure that states for assets that were read have not changed since chaincode execution time
- There is immutability once a transaction is validated and committed
- A channel's ledger contains a configuration block defining policies, access control lists, and other pertinent information
- Channels contain *Membership Service Provider* instances allowing for crypto materials to be derived from different certificate authorities

See the ledger topic for a deeper dive on the databases, storage structure, and "query-ability."

4.3.4 Privacy

Hyperledger Fabric employs an immutable ledger on a per-channel basis, as well as chaincode that can manipulate and modify the current state of assets (i.e. update key-value pairs). A ledger exists in the scope of a channel — it can be shared across the entire network (assuming every participant is operating on one common channel) — or it can be privatized to include only a specific set of participants.

In the latter scenario, these participants would create a separate channel and thereby isolate/segregate their transactions and ledger. In order to solve scenarios that want to bridge the gap between total transparency and privacy, chaincode can be installed only on peers that need to access the asset states to perform reads and writes (in other words, if a chaincode is not installed on a peer, it will not be able to properly interface with the ledger).

When a subset of organizations on that channel need to keep their transaction data confidential, a private data collection (collection) is used to segregate this data in a private database, logically separate from the channel ledger, accessible only to the authorized subset of organizations.

Thus, channels keep transactions private from the broader network whereas collections keep data private between subsets of organizations on the channel.

To further obfuscate the data, values within chaincode can be encrypted (in part or in total) using common cryptographic algorithms such as AES before sending transactions to the ordering service and appending blocks to the ledger. Once encrypted data has been written to the ledger, it can be decrypted only by a user in possession of the corresponding key that was used to generate the cipher text. For further details on chaincode encryption, see the *Chaincode for Developers* topic.

See the *Private Data* topic for more details on how to achieve privacy on your blockchain network.

4.3.5 Security & Membership Services

Hyperledger Fabric underpins a transactional network where all participants have known identities. Public Key Infrastructure is used to generate cryptographic certificates which are tied to organizations, network components, and end users or client applications. As a result, data access control can be manipulated and governed on the broader network and on channel levels. This "permissioned" notion of Hyperledger Fabric, coupled with the existence and capabilities of channels, helps address scenarios where privacy and confidentiality are paramount concerns.

See the *Membership Service Providers (MSP)* topic to better understand cryptographic implementations, and the sign, verify, authenticate approach used in Hyperledger Fabric.

4.3.6 Consensus

In distributed ledger technology, consensus has recently become synonymous with a specific algorithm, within a single function. However, consensus encompasses more than simply agreeing upon the order of transactions, and this differentiation is highlighted in Hyperledger Fabric through its fundamental role in the entire transaction flow, from proposal and endorsement, to ordering, validation and commitment. In a nutshell, consensus is defined as the full-circle verification of the correctness of a set of transactions comprising a block.

Consensus is achieved ultimately when the order and results of a block's transactions have met the explicit policy criteria checks. These checks and balances take place during the lifecycle of a transaction, and include the usage of endorsement policies to dictate which specific members must endorse a certain transaction class, as well as system chaincodes to ensure that these policies are enforced and upheld. Prior to commitment, the peers will employ these system chaincodes to make sure that enough endorsements are present, and that they were derived from the appropriate entities. Moreover, a versioning check will take place during which the current state of the ledger is agreed or consented upon, before any blocks containing transactions are appended to the ledger. This final check provides protection against double spend operations and other threats that might compromise data integrity, and allows for functions to be executed against non-static variables.

In addition to the multitude of endorsement, validity and versioning checks that take place, there are also ongoing identity verifications happening in all directions of the transaction flow. Access control lists are implemented on hierarchical layers of the network (ordering service down to channels), and payloads are repeatedly signed, verified and authenticated as a transaction proposal passes through the different architectural components. To conclude, consensus is not merely limited to the agreed upon order of a batch of transactions; rather, it is an overarching characterization that is achieved as a byproduct of the ongoing verifications that take place during a transaction's journey from proposal to commitment.

Check out the *Transaction Flow* diagram for a visual representation of consensus.

4.4 Blockchain network

This topic will describe, **at a conceptual level**, how Hyperledger Fabric allows organizations to collaborate in the formation of blockchain networks. If you're an architect, administrator or developer, you can use this topic to get a solid understanding of the major structure and process components in a Hyperledger Fabric blockchain network. This topic will use a manageable worked example that introduces all of the major components in a blockchain network. After understanding this example you can read more detailed information about these components elsewhere in the documentation, or try building a sample network.

After reading this topic and understanding the concept of policies, you will have a solid understanding of the decisions that organizations need to make to establish the policies that control a deployed Hyperledger Fabric network. You'll also understand how organizations manage network evolution using declarative policies – a key feature of Hyperledger Fabric. In a nutshell, you'll understand the major technical components of Hyperledger Fabric and the decisions organizations need to make about them.

4.4.1 What is a blockchain network?

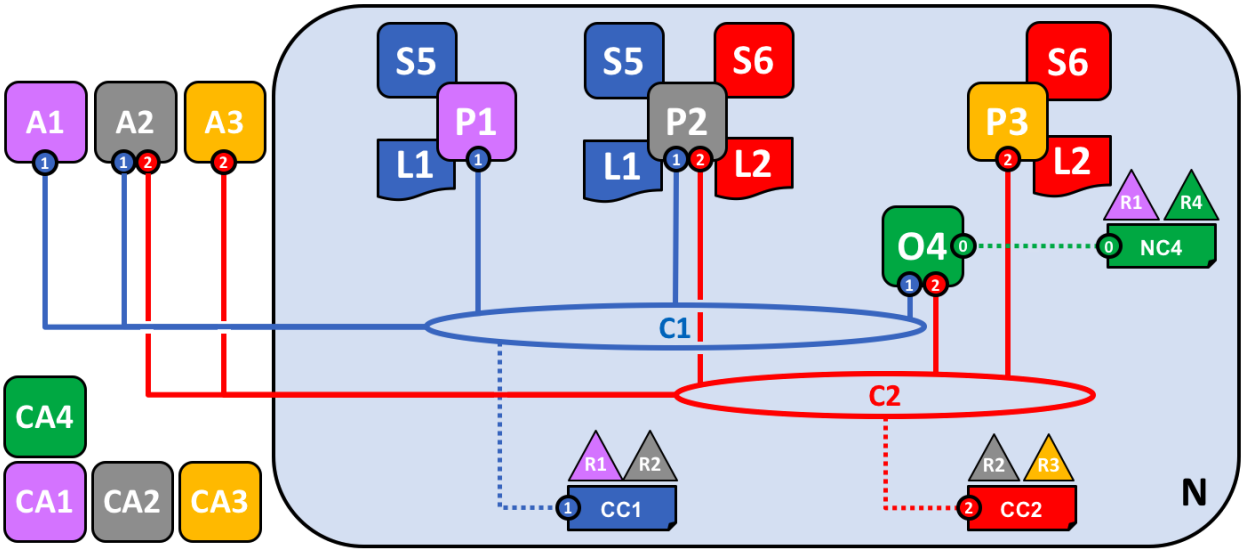
A blockchain network is a technical infrastructure that provides ledger and smart contract (chaincode) services to applications. Primarily, smart contracts are used to generate transactions which are subsequently distributed to every peer node in the network where they are immutably recorded on their copy of the ledger. The users of applications might be end users using client applications or blockchain network administrators.

In most cases, multiple organizations come together as a consortium to form the network and their permissions are determined by a set of policies that are agreed by the consortium when the network is originally configured. Moreover, network policies can change over time subject to the agreement of the organizations in the consortium, as we'll discover when we discuss the concept of *modification policy*.

4.4.2 The sample network

Before we start, let's show you what we're aiming at! Here's a diagram representing the **final state** of our sample network.

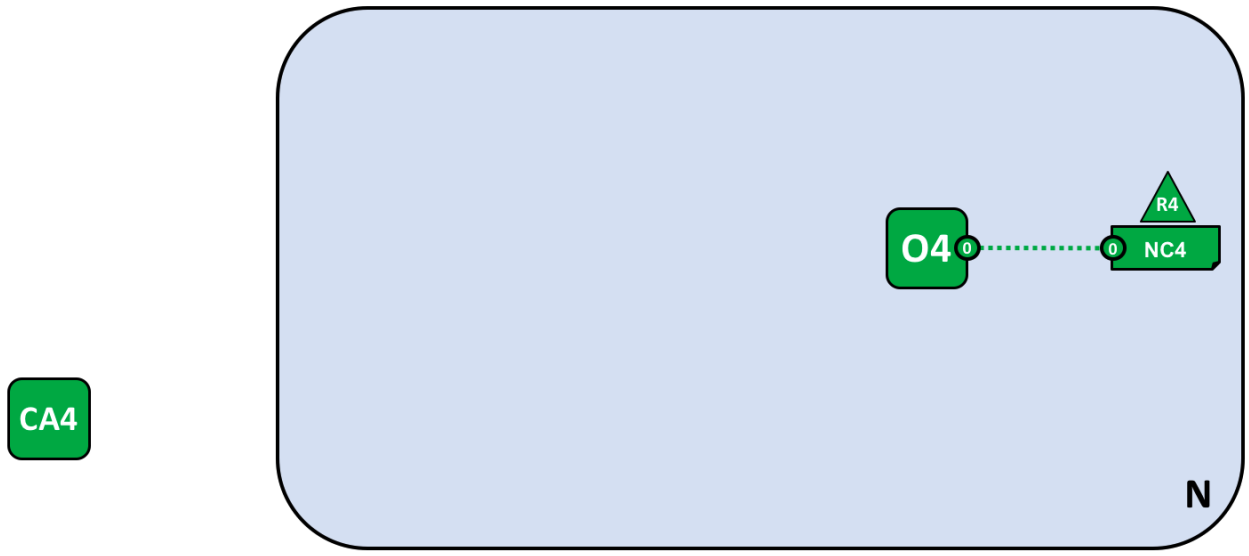
Don't worry that this might look complicated! As we go through this topic, we will build up the network piece by piece, so that you see how the organizations R1, R2, R3 and R4 contribute infrastructure to the network to help form it. This infrastructure implements the blockchain network, and it is governed by policies agreed by the organizations who form the network – for example, who can add new organizations. You'll discover how applications consume the ledger and smart contract services provided by the blockchain network.



Four organizations, R1, R2, R3 and R4 have jointly decided, and written into an agreement, that they will set up and exploit a Hyperledger Fabric network. R4 has been assigned to be the network initiator – it has been given the power to set up the initial version of the network. R4 has no intention to perform business transactions on the network. R1 and R2 have a need for a private communications within the overall network, as do R2 and R3. Organization R1 has a client application that can perform business transactions within channel C1. Organization R2 has a client application that can do similar work both in channel C1 and C2. Organization R3 has a client application that can do this on channel C2. Peer node P1 maintains a copy of the ledger L1 associated with C1. Peer node P2 maintains a copy of the ledger L1 associated with C1 and a copy of ledger L2 associated with C2. Peer node P3 maintains a copy of the ledger L2 associated with C2. The network is governed according to policy rules specified in network configuration NC4, the network is under the control of organizations R1 and R4. Channel C1 is governed according to the policy rules specified in channel configuration CC1; the channel is under the control of organizations R1 and R2. Channel C2 is governed according to the policy rules specified in channel configuration CC2; the channel is under the control of organizations R2 and R3. There is an ordering service O4 that services as a network administration point for N, and uses the system channel. The ordering service also supports application channels C1 and C2, for the purposes of transaction ordering into blocks for distribution. Each of the four organizations has a preferred Certificate Authority.

4.4.3 Creating the Network

Let's start at the beginning by creating the basis for the network:



The network is formed when an orderer is started. In our example network, N, the ordering service comprising a single node, O4, is configured according to a network configuration NC4, which gives administrative rights to organization R4. At the network level, Certificate Authority CA4 is used to dispense identities to the administrators and network nodes of the R4 organization.

We can see that the first thing that defines a **network, N,** is an **ordering service, O4**. It's helpful to think of the ordering service as the initial administration point for the network. As agreed beforehand, O4 is initially configured and started by an administrator in organization R4, and hosted in R4. The configuration NC4 contains the policies that describe the starting set of administrative capabilities for the network. Initially this is set to only give R4 rights over the network. This will change, as we'll see later, but for now R4 is the only member of the network.

Certificate Authorities

You can also see a Certificate Authority, CA4, which is used to issue certificates to administrators and network nodes. CA4 plays a key role in our network because it dispenses X.509 certificates that can be used to identify components as belonging to organization R4. Certificates issued by CAs can also be used to sign transactions to indicate that an organization endorses the transaction result – a precondition of it being accepted onto the ledger. Let's examine these two aspects of a CA in a little more detail.

Firstly, different components of the blockchain network use certificates to identify themselves to each other as being from a particular organization. That's why there is usually more than one CA supporting a blockchain network – different organizations often use different CAs. We're going to use four CAs in our network; one of for each organization. Indeed, CAs are so important that Hyperledger Fabric provides you with a built-in one (called *Fabric-CA*) to help you get going, though in practice, organizations will choose to use their own CA.

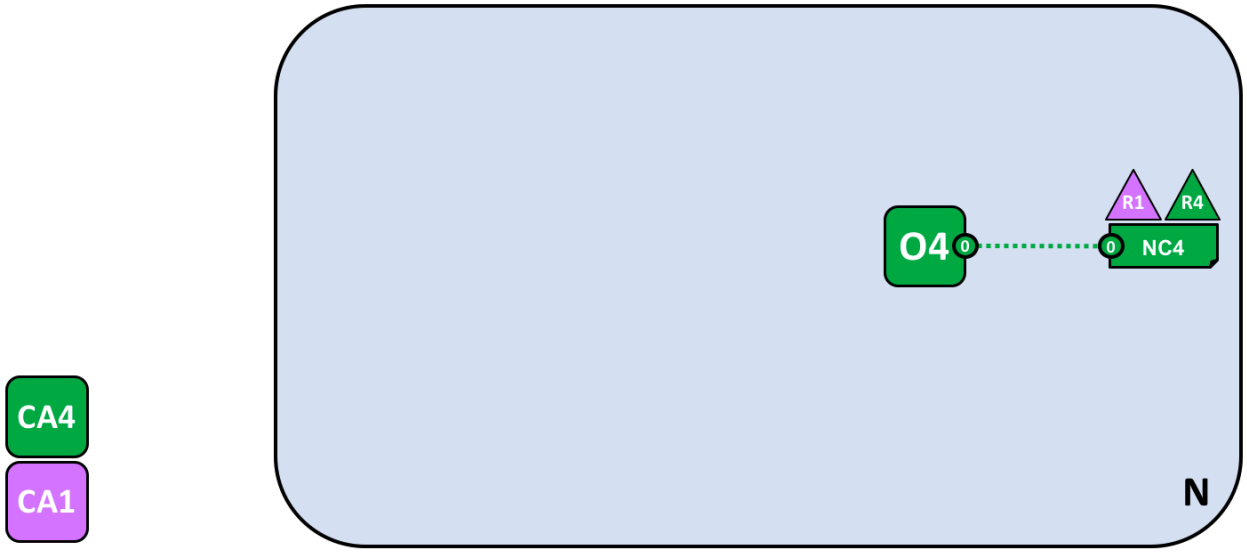
The mapping of certificates to member organizations is achieved by via a structure called a Membership Services Provider (MSP). Network configuration NC4 uses a named MSP to identify the properties of certificates dispensed by CA4 which associate certificate holders with organization R4. NC4 can then use this MSP name in policies to grant actors from R4 particular rights over network resources. An example of such a policy is to identify the administrators in R4 who can add new member organizations to the network. We don't show MSPs on these diagrams, as they would just clutter them up, but they are very important.

Secondly, we'll see later how certificates issued by CAs are at the heart of the transaction generation and validation process. Specifically, X.509 certificates are used in client application transaction proposals and smart contract transaction responses to digitally sign transactions. Subsequently the network nodes who host copies of the ledger verify that transaction signatures are valid before accepting transactions onto the ledger.

Let's recap the basic structure of our example blockchain network. There's a resource, the network N, accessed by a set of users defined by a Certificate Authority CA4, who have a set of rights over the resources in the network N as described by policies contained inside a network configuration NC4. All of this is made real when we configure and start the ordering service node O4.

4.4.4 Adding Network Administrators

NC4 was initially configured to only allow R4 users administrative rights over the network. In this next phase, we are going to allow organization R1 users to administer the network. Let's see how the network evolves:



Organization R4 updates the network configuration to make organization R1 an administrator too. After this point R1 and R4 have equal rights over the network configuration.

We see the addition of a new organization R1 as an administrator – R1 and R4 now have equal rights over the network. We can also see that certificate authority CA1 has been added – it can be used to identify users from the R1 organization. After this point, users from both R1 and R4 can administer the network.

Although the orderer node, O4, is running on R4's infrastructure, R1 has shared administrative rights over it, as long as it can gain network access. It means that R1 or R4 could update the network configuration NC4 to allow the R2 organization a subset of network operations. In this way, even though R4 is running the ordering service, and R1 has full administrative rights over it, R2 has limited rights to create new consortia.

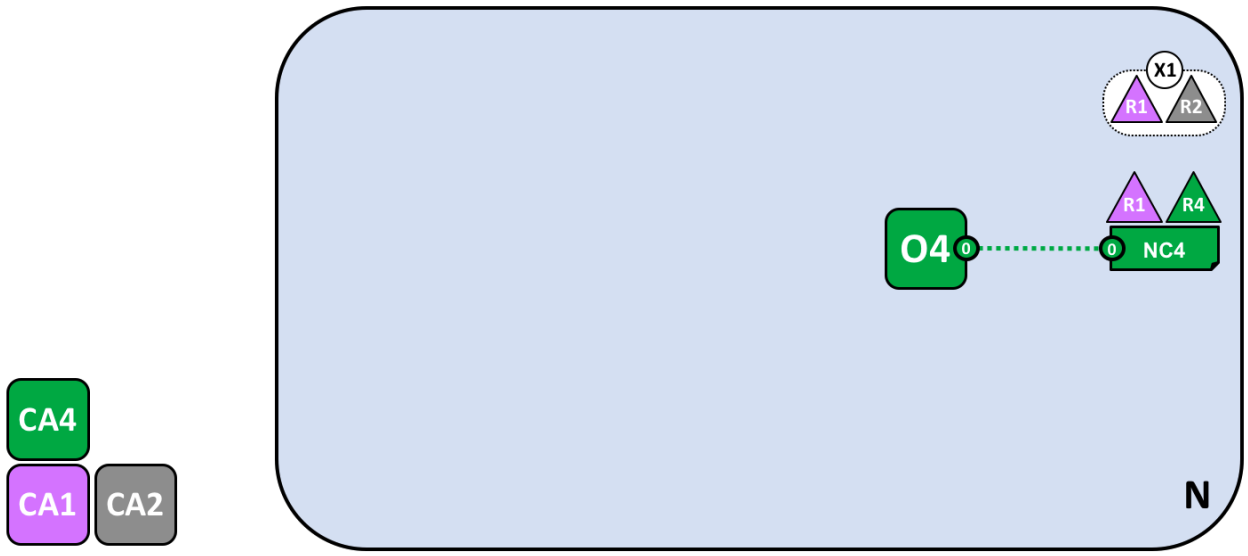
In its simplest form, the ordering service is a single node in the network, and that's what you can see in the example. Ordering services are usually multi-node, and can be configured to have different nodes in different organizations. For example, we might run O4 in R4 and connect it to O2, a separate orderer node in organization R1. In this way, we would have a multi-site, multi-organization administration structure.

We'll discuss the ordering service a little more *later in this topic*, but for now just think of the ordering service as an administration point which provides different organizations controlled access to the network.

4.4.5 Defining a Consortium

Although the network can now be administered by R1 and R4, there is very little that can be done. The first thing we need to do is define a consortium. This word literally means "a group with a shared destiny", so it's an appropriate choice for a set of organizations in a blockchain network.

Let's see how a consortium is defined:



A network administrator defines a consortium X1 that contains two members, the organizations R1 and R2. This consortium definition is stored in the network configuration NC4, and will be used at the next stage of network development. CA1 and CA2 are the respective Certificate Authorities for these organizations.

Because of the way NC4 is configured, only R1 or R4 can create new consortia. This diagram shows the addition of a new consortium, X1, which defines R1 and R2 as its constituting organizations. We can also see that CA2 has been added to identify users from R2. Note that a consortium can have any number of organizational members – we have just shown two as it is the simplest configuration.

Why are consortia important? We can see that a consortium defines the set of organizations in the network who share a need to **transact** with one another – in this case R1 and R2. It really makes sense to group organizations together if they have a common goal, and that's exactly what's happening.

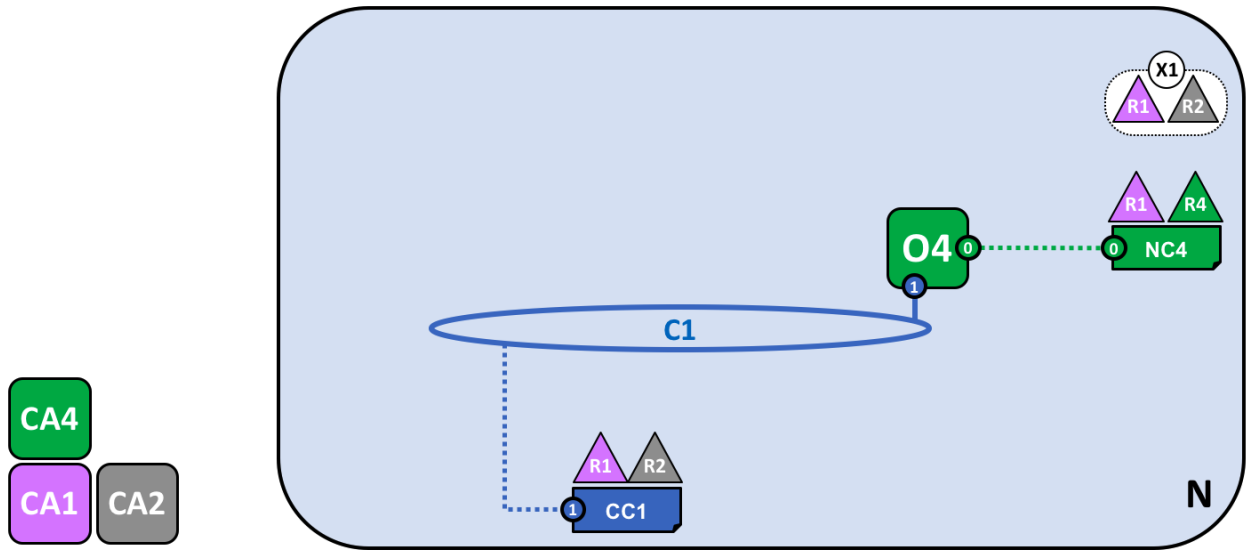
The network, although started by a single organization, is now controlled by a larger set of organizations. We could have started it this way, with R1, R2 and R4 having shared control, but this build up makes it easier to understand.

We're now going to use consortium X1 to create a really important part of a Hyperledger Fabric blockchain – **a channel**.

4.4.6 Creating a channel for a consortium

So let's create this key part of the Fabric blockchain network – **a channel**. A channel is a primary communications mechanism by which the members of a consortium can communicate with each other. There can be multiple channels in a network, but for now, we'll start with one.

Let's see how the first channel has been added to the network:



A channel C1 has been created for R1 and R2 using the consortium definition X1. The channel is governed by a channel configuration CC1, completely separate to the network configuration. CC1 is managed by R1 and R2 who have equal rights over C1. R4 has no rights in CC1 whatsoever.

The channel C1 provides a private communications mechanism for the consortium X1. We can see channel C1 has been connected to the ordering service O4 but that nothing else is attached to it. In the next stage of network development, we're going to connect components such as client applications and peer nodes. But at this point, a channel represents the **potential** for future connectivity.

Even though channel C1 is a part of the network N, it is quite distinguishable from it. Also notice that organizations R3 and R4 are not in this channel – it is for transaction processing between R1 and R2. In the previous step, we saw how R4 could grant R1 permission to create new consortia. It's helpful to mention that R4 **also** allowed R1 to create channels! In this diagram, it could have been organization R1 or R4 who created a channel C1. Again, note that a channel can have any number of organizations connected to it – we've shown two as it's the simplest configuration.

Again, notice how channel C1 has a completely separate configuration, CC1, to the network configuration NC4. CC1 contains the policies that govern the rights that R1 and R2 have over the channel C1 – and as we've seen, R3 and R4 have no permissions in this channel. R3 and R4 can only interact with C1 if they are added by R1 or R2 to the appropriate policy in the channel configuration CC1. An example is defining who can add a new organization to the channel. Specifically, note that R4 cannot add itself to the channel C1 – it must, and can only, be authorized by R1 or R2.

Why are channels so important? Channels are useful because they provide a mechanism for private communications and private data between the members of a consortium. Channels provide privacy from other channels, and from the network. Hyperledger Fabric is powerful in this regard, as it allows organizations to share infrastructure and keep it private at the same time. There's no contradiction here – different consortia within the network will have a need for different information and processes to be appropriately shared, and channels provide an efficient mechanism to do this. Channels provide an efficient sharing of infrastructure while maintaining data and communications privacy.

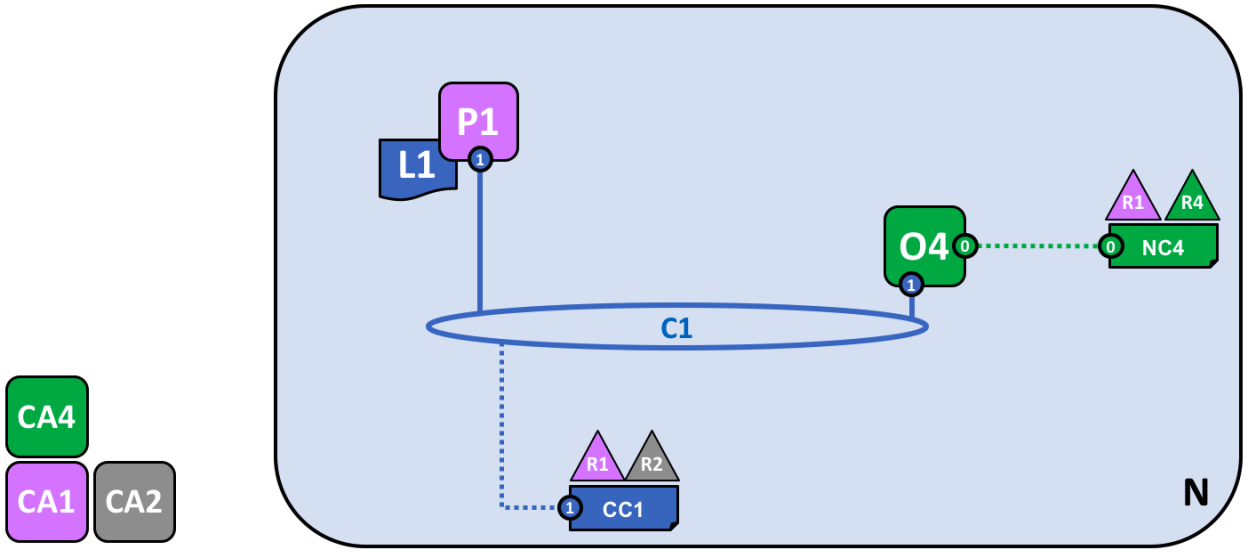
We can also see that once a channel has been created, it is in a very real sense "free from the network". It is only organizations that are explicitly specified in a channel configuration that have any control over it, from this time forward into the future. Likewise, any updates to network configuration NC4 from this time onwards will have no direct effect on channel configuration CC1; for example if consortia definition X1 is changed, it will not affect the members of channel C1. Channels are therefore useful because they allow private communications between the organizations constituting the channel. Moreover, the data in a channel is completely isolated from the rest of the network, including other channels.

As an aside, there is also a special **system channel** defined for use by the ordering service. It behaves in exactly the

same way as a regular channel, which are sometimes called **application channels** for this reason. We don't normally need to worry about this channel, but we'll discuss a little bit more about it *later in this topic*.

4.4.7 Peers and Ledgers

Let's now start to use the channel to connect the blockchain network and the organizational components together. In the next stage of network development, we can see that our network N has just acquired two new components, namely a peer node P1 and a ledger instance, L1.



A peer node P1 has joined the channel C1. P1 physically hosts a copy of the ledger L1. P1 and O4 can communicate with each other using channel C1.

Peer nodes are the network components where copies of the blockchain ledger are hosted! At last, we're starting to see some recognizable blockchain components! P1's purpose in the network is purely to host a copy of the ledger L1 for others to access. We can think of L1 as being **physically hosted** on P1, but **logically hosted** on the channel C1. We'll see this idea more clearly when we add more peers to the channel.

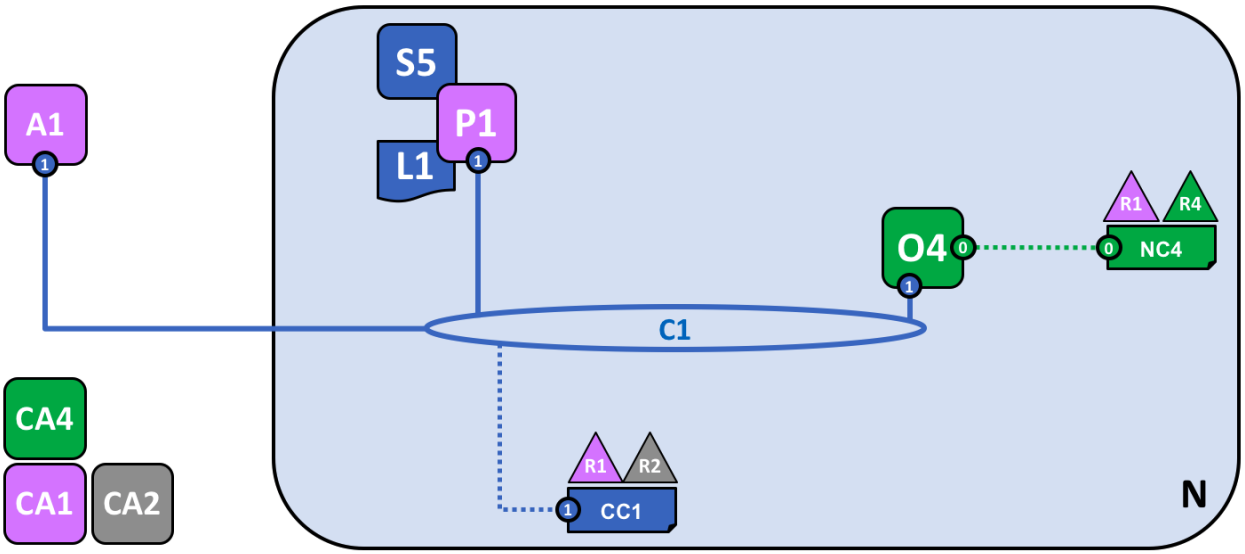
A key part of a P1's configuration is an X.509 identity issued by CA1 which associates P1 with organization R1. Once P1 is started, it can **join** channel C1 using the orderer O4. When O4 receives this join request, it uses the channel configuration CC1 to determine P1's permissions on this channel. For example, CC1 determines whether P1 can read and/or write information to the ledger L1.

Notice how peers are joined to channels by the organizations that own them, and though we've only added one peer, we'll see how there can be multiple peer nodes on multiple channels within the network. We'll see the different roles that peers can take on a little later.

4.4.8 Applications and Smart Contract chaincode

Now that the channel C1 has a ledger on it, we can start connecting client applications to consume some of the services provided by workhorse of the ledger, the peer!

Notice how the network has grown:



A smart contract S5 has been installed onto P1. Client application A1 in organization R1 can use S5 to access the ledger via peer node P1. A1, P1 and O4 are all joined to channel C1, i.e. they can all make use of the communication facilities provided by that channel.

In the next stage of network development, we can see that client application A1 can use channel C1 to connect to specific network resources – in this case A1 can connect to both peer node P1 and orderer node O4. Again, see how channels are central to the communication between network and organization components. Just like peers and orderers, a client application will have an identity that associates it with an organization. In our example, client application A1 is associated with organization R1; and although it is outside the Fabric blockchain network, it is connected to it via the channel C1.

It might now appear that A1 can access the ledger L1 directly via P1, but in fact, all access is managed via a special program called a smart contract chaincode, S5. Think of S5 as defining all the common access patterns to the ledger; S5 provides a well-defined set of ways by which the ledger L1 can be queried or updated. In short, client application A1 has to go through smart contract S5 to get to ledger L1!

Smart contract chaincodes can be created by application developers in each organization to implement a business process shared by the consortium members. Smart contracts are used to help generate transactions which can be subsequently distributed to the every node in the network. We'll discuss this idea a little later; it'll be easier to understand when the network is bigger. For now, the important thing to understand is that to get to this point two operations must have been performed on the smart contract; it must have been **installed**, and then **instantiated**.

Installing a smart contract

After a smart contract S5 has been developed, an administrator in organization R1 must install it onto peer node P1. This is a straightforward operation; after it has occurred, P1 has full knowledge of S5. Specifically, P1 can see the **implementation** logic of S5 – the program code that it uses to access the ledger L1. We contrast this to the S5 **interface** which merely describes the inputs and outputs of S5, without regard to its implementation.

When an organization has multiple peers in a channel, it can choose the peers upon which it installs smart contracts; it does not need to install a smart contract on every peer.

Instantiating a smart contract

However, just because P1 has installed S5, the other components connected to channel C1 are unaware of it; it must first be instantiated on channel C1. In our example, which only has a single peer node P1, an administrator in organization

R1 must instantiate S5 on channel C1 using P1. After instantiation, every component on channel C1 is aware of the existence of S5; and in our example it means that S5 can now be invoked by client application A1!

Note that although every component on the channel can now access S5, they are not able to see its program logic. This remains private to those nodes who have installed it; in our example that means P1. Conceptually this means that it's the smart contract **interface** that is instantiated, in contrast to the smart contract **implementation** that is installed. To reinforce this idea; installing a smart contract shows how we think of it being **physically hosted** on a peer, whereas instantiating a smart contract shows how we consider it **logically hosted** by the channel.

Endorsement policy

The most important piece of additional information supplied at instantiation is an endorsement policy. It describes which organizations must approve transactions before they will be accepted by other organizations onto their copy of the ledger. In our sample network, transactions can be only be accepted onto ledger L1 if R1 or R2 endorse them.

The act of instantiation places the endorsement policy in channel configuration CC1; it enables it to be accessed by any member of the channel. You can read more about endorsement policies in the transaction flow topic.

Invoking a smart contract

Once a smart contract has been installed on a peer node and instantiated on a channel it can be invoked by a client application. Client applications do this by sending transaction proposals to peers owned by the organizations specified by the smart contract endorsement policy. The transaction proposal serves as input to the smart contract, which uses it to generate an endorsed transaction response, which is returned by the peer node to the client application.

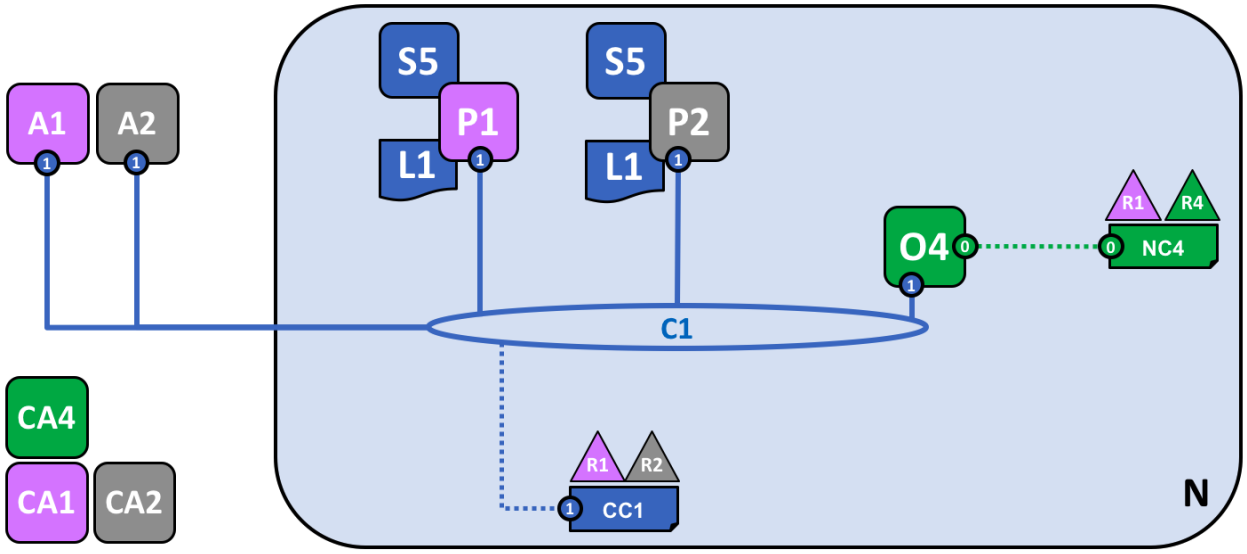
It's these transactions responses that are packaged together with the transaction proposal to form a fully endorsed transaction, which can be distributed to the entire network. We'll look at this in more detail later For now, it's enough to understand how applications invoke smart contracts to generate endorsed transactions.

By this stage in network development we can see that organization R1 is fully participating in the network. Its applications – starting with A1 – can access the ledger L1 via smart contract S5, to generate transactions that will be endorsed by R1, and therefore accepted onto the ledger because they conform to the endorsement policy.

4.4.9 Network completed

Recall that our objective was to create a channel for consortium X1 – organizations R1 and R2. This next phase of network development sees organization R2 add its infrastructure to the network.

Let's see how the network has evolved:



The network has grown through the addition of infrastructure from organization R2. Specifically, R2 has added peer node P2, which hosts a copy of ledger L1, and chaincode S5. P2 has also joined channel C1, as has application A2. A2 and P2 are identified using certificates from CA2. All of this means that both applications A1 and A2 can invoke S5 on C1 either using peer node P1 or P2.

We can see that organization R2 has added a peer node, P2, on channel C1. P2 also hosts a copy of the ledger L1 and smart contract S5. We can see that R2 has also added client application A2 which can connect to the network via channel C1. To achieve this, an administrator in organization R2 has created peer node P2 and joined it to channel C1, in the same way as an administrator in R1.

We have created our first operational network! At this stage in network development, we have a channel in which organizations R1 and R2 can fully transact with each other. Specifically, this means that applications A1 and A2 can generate transactions using smart contract S5 and ledger L1 on channel C1.

Generating and accepting transactions

In contrast to peer nodes, which always host a copy of the ledger, we see that there are two different kinds of peer nodes; those which host smart contracts and those which do not. In our network, every peer hosts a copy of the smart contract, but in larger networks, there will be many more peer nodes that do not host a copy of the smart contract. A peer can only *run* a smart contract if it is installed on it, but it can *know* about the interface of a smart contract by being connected to a channel.

You should not think of peer nodes which do not have smart contracts installed as being somehow inferior. It's more the case that peer nodes with smart contracts have a special power – to help **generate** transactions. Note that all peer nodes can **validate** and subsequently **accept** or **reject** transactions onto their copy of the ledger L1. However, only peer nodes with a smart contract installed can take part in the process of transaction **endorsement** which is central to the generation of valid transactions.

We don't need to worry about the exact details of how transactions are generated, distributed and accepted in this topic – it is sufficient to understand that we have a blockchain network where organizations R1 and R2 can share information and processes as ledger-captured transactions. We'll learn a lot more about transactions, ledgers, smart contracts in other topics.

Types of peers

In Hyperledger Fabric, while all peers are the same, they can assume multiple roles depending on how the network is configured. We now have enough understanding of a typical network topology to describe these roles.

- *Committing peer*. Every peer node in a channel is a committing peer. It receives blocks of generated transactions, which are subsequently validated before they are committed to the peer node's copy of the ledger as an append operation.
- *Endorsing peer*. Every peer with a smart contract *can* be an endorsing peer if it has a smart contract installed. However, to actually *be* an endorsing peer, the smart contract on the peer must be used by a client application to generate a digitally signed transaction response. The term *endorsing peer* is an explicit reference to this fact.

  An endorsement policy for a smart contract identifies the organizations whose peer should digitally sign a generated transaction before it can be accepted onto a committing peer's copy of the ledger.

These are the two major types of peer; there are two other roles a peer can adopt:

- *Leader peer*. When an organization has multiple peers in a channel, a leader peer is a node which takes responsibility for distributing transactions from the orderer to the other committing peers in the organization. A peer can choose to participate in static or dynamic leadership selection.

  It is helpful, therefore to think of two sets of peers from leadership perspective – those that have static leader selection, and those with dynamic leader selection. For the static set, zero or more peers can be configured as leaders. For the dynamic set, one peer will be elected leader by the set. Moreover, in the dynamic set, if a leader peer fails, then the remaining peers will re-elect a leader.

  It means that an organization's peers can have one or more leaders connected to the ordering service. This can help to improve resilience and scalability in large networks which process high volumes of transactions.
- *Anchor peer*. If a peer needs to communicate with a peer in another organization, then it can use one of the **anchor peers** defined in the channel configuration for that organization. An organization can have zero or more anchor peers defined for it, and an anchor peer can help with many different cross-organization communication scenarios.

Note that a peer can be a committing peer, endorsing peer, leader peer and anchor peer all at the same time! Only the anchor peer is optional – for all practical purposes there will always be a leader peer and at least one endorsing peer and at least one committing peer.

Install not instantiate

In a similar way to organization R1, organization R2 must install smart contract S5 onto its peer node, P2. That's obvious – if applications A1 or A2 wish to use S5 on peer node P2 to generate transactions, it must first be present; installation is the mechanism by which this happens. At this point, peer node P2 has a physical copy of the smart contract and the ledger; like P1, it can both generate and accept transactions onto its copy of ledger L1.

However, in contrast to organization R1, organization R2 does not need to instantiate smart contract S5 on channel C1. That's because S5 has already been instantiated on the channel by organization R1. Instantiation only needs to happen once; any peer which subsequently joins the channel knows that smart contract S5 is available to the channel. This fact reflects the fact that ledger L1 and smart contract really exist in a physical manner on the peer nodes, and a logical manner on the channel; R2 is merely adding another physical instance of L1 and S5 to the network.

In our network, we can see that channel C1 connects two client applications, two peer nodes and an ordering service. Since there is only one channel, there is only one **logical** ledger with which these components interact. Peer nodes P1 and P2 have identical copies of ledger L1. Copies of smart contract S5 will usually be identically implemented using the same programming language, but if not, they must be semantically equivalent.

We can see that the careful addition of peers to the network can help support increased throughput, stability, and resilience. For example, more peers in a network will allow more applications to connect to it; and multiple peers in an organization will provide extra resilience in the case of planned or unplanned outages.

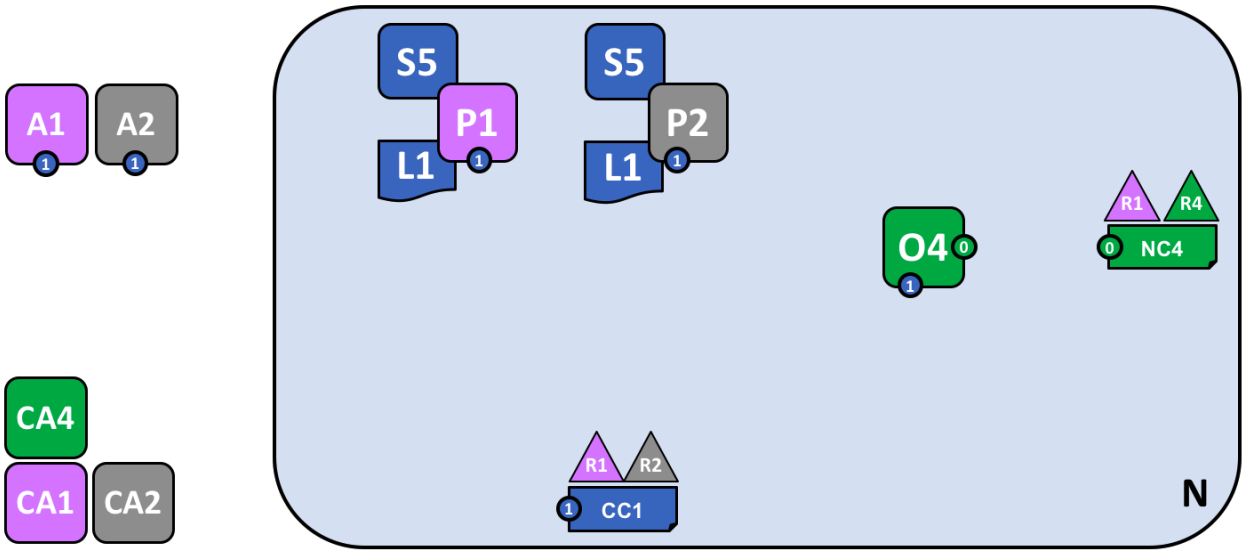
It all means that it is possible to configure sophisticated topologies which support a variety of operational goals – there is no theoretical limit to how big a network can get. Moreover, the technical mechanism by which peers within an individual organization efficiently discover and communicate with each other – the gossip protocol – will accommodate a large number of peer nodes in support of such topologies.

The careful use of network and channel policies allow even large networks to be well-governed. Organizations are free to add peer nodes to the network so long as they conform to the policies agreed by the network. Network and channel policies create the balance between autonomy and control which characterizes a de-centralized network.

4.4.10 Simplifying the visual vocabulary

We're now going to simplify the visual vocabulary used to represent our sample blockchain network. As the size of the network grows, the lines initially used to help us understand channels will become cumbersome. Imagine how complicated our diagram would be if we added another peer or client application, or another channel?

That's what we're going to do in a minute, so before we do, let's simplify the visual vocabulary. Here's a simplified representation of the network we've developed so far:



The diagram shows the facts relating to channel C1 in the network N as follows: Client applications A1 and A2 can use channel C1 for communication with peers P1 and P2, and orderer O4. Peer nodes P1 and P2 can use the communication services of channel C1. Ordering service O4 can make use of the communication services of channel C1. Channel configuration CC1 applies to channel C1.

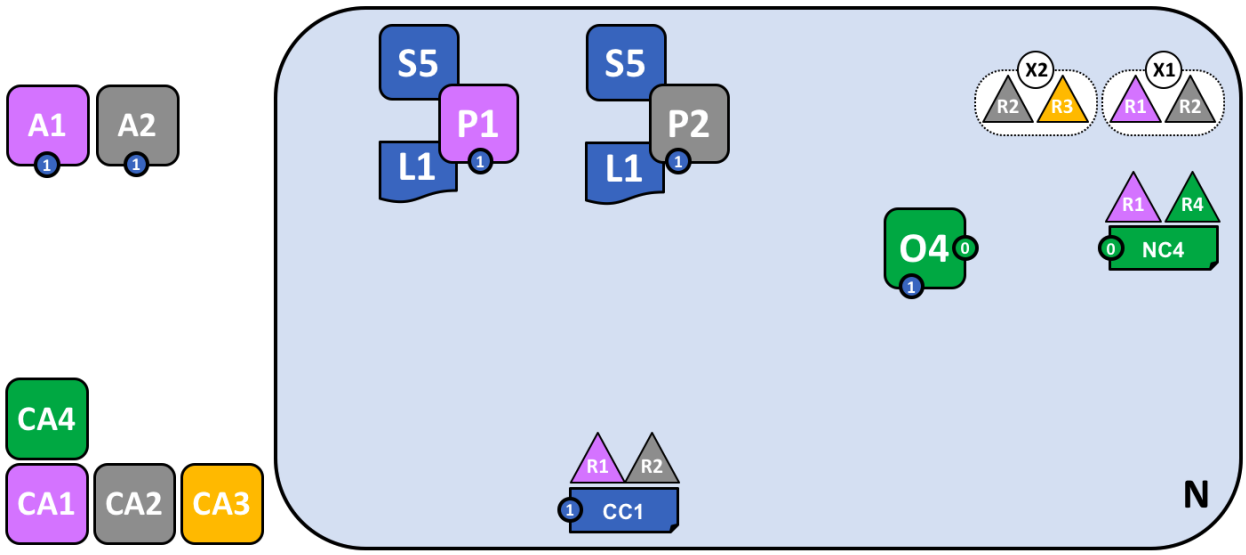
Note that the network diagram has been simplified by replacing channel lines with connection points, shown as blue circles which include the channel number. No information has been lost. This representation is more scalable because it eliminates crossing lines. This allows us to more clearly represent larger networks. We've achieved this simplification by focusing on the connection points between components and a channel, rather than the channel itself.

4.4.11 Adding another consortium definition

In this next phase of network development, we introduce organization R3. We're going to give organizations R2 and R3 a separate application channel which allows them to transact with each other. This application channel will be

completely separate to that previously defined, so that R2 and R3 transactions can be kept private to them.

Let's return to the network level and define a new consortium, X2, for R2 and R3:



A network administrator from organization R1 or R4 has added a new consortium definition, X2, which includes organizations R2 and R3. This will be used to define a new channel for X2.

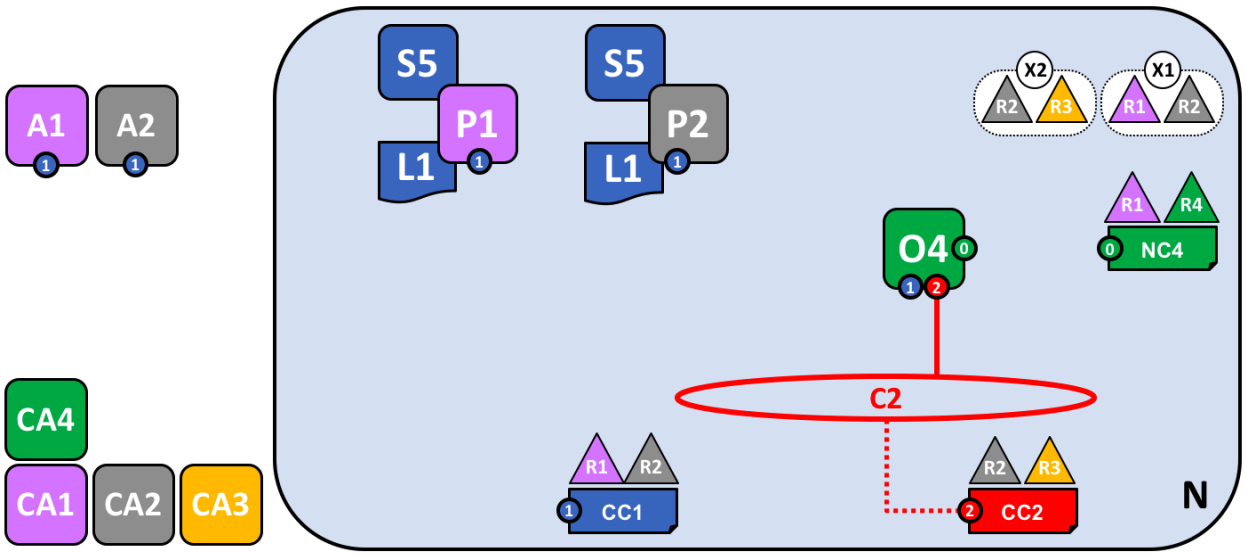
Notice that the network now has two consortia defined: X1 for organizations R1 and R2 and X2 for organizations R2 and R3. Consortium X2 has been introduced in order to be able to create a new channel for R2 and R3.

A new channel can only be created by those organizations specifically identified in the network configuration policy, NC4, as having the appropriate rights to do so, i.e. R1 or R4. This is an example of a policy which separates organizations that can manage resources at the network level versus those who can manage resources at the channel level. Seeing these policies at work helps us understand why Hyperledger Fabric has a sophisticated **tiered** policy structure.

In practice, consortium definition X2 has been added to the network configuration NC4. We discuss the exact mechanics of this operation elsewhere in the documentation.

4.4.12 Adding a new channel

Let's now use this new consortium definition, X2, to create a new channel, C2. To help reinforce your understanding of the simpler channel notation, we've used both visual styles – channel C1 is represented with blue circular end points, whereas channel C2 is represented with red connecting lines:



A new channel C2 has been created for R2 and R3 using consortium definition X2. The channel has a channel configuration CC2, completely separate to the network configuration NC4, and the channel configuration CC1. Channel C2 is managed by R2 and R3 who have equal rights over C2 as defined by a policy in CC2. R1 and R4 have no rights defined in CC2 whatsoever.

The channel C2 provides a private communications mechanism for the consortium X2. Again, notice how organizations united in a consortium are what form channels. The channel configuration CC2 now contains the policies that govern channel resources, assigning management rights to organizations R2 and R3 over channel C2. It is managed exclusively by R2 and R3; R1 and R4 have no power in channel C2. For example, channel configuration CC2 can subsequently be updated to add organizations to support network growth, but this can only be done by R2 or R3.

Note how the channel configurations CC1 and CC2 remain completely separate from each other, and completely separate from the network configuration, NC4. Again we're seeing the de-centralized nature of a Hyperledger Fabric network; once channel C2 has been created, it is managed by organizations R2 and R3 independently to other network elements. Channel policies always remain separate from each other and can only be changed by the organizations authorized to do so in the channel.

As the network and channels evolve, so will the network and channel configurations. There is a process by which this is accomplished in a controlled manner – involving configuration transactions which capture the change to these configurations. Every configuration change results in a new configuration block transaction being generated, and *later in this topic*, we'll see how these blocks are validated and accepted to create updated network and channel configurations respectively.

Network and channel configurations

Throughout our sample network, we see the importance of network and channel configurations. These configurations are important because they encapsulate the **policies** agreed by the network members, which provide a shared reference for controlling access to network resources. Network and channel configurations also contain **facts** about the network and channel composition, such as the name of consortia and its organizations.

For example, when the network is first formed using the ordering service node O4, its behaviour is governed by the network configuration NC4. The initial configuration of NC4 only contains policies that permit organization R4 to manage network resources. NC4 is subsequently updated to also allow R1 to manage network resources. Once this change is made, any administrator from organization R1 or R4 that connects to O4 will have network management rights because that is what the policy in the network configuration NC4 permits. Internally, each node in the ordering service records each channel in the network configuration, so that there is a record of each channel created, at the network level.

It means that although ordering service node O4 is the actor that created consortia X1 and X2 and channels C1 and C2, the **intelligence** of the network is contained in the network configuration NC4 that O4 is obeying. As long as O4 behaves as a good actor, and correctly implements the policies defined in NC4 whenever it is dealing with network resources, our network will behave as all organizations have agreed. In many ways NC4 can be considered more important than O4 because, ultimately, it controls network access.

The same principles apply for channel configurations with respect to peers. In our network, P1 and P2 are likewise good actors. When peer nodes P1 and P2 are interacting with client applications A1 or A2 they are each using the policies defined within channel configuration CC1 to control access to the channel C1 resources.

For example, if A1 wants to access the smart contract chaincode S5 on peer nodes P1 or P2, each peer node uses its copy of CC1 to determine the operations that A1 can perform. For example, A1 may be permitted to read or write data from the ledger L1 according to policies defined in CC1. We'll see later the same pattern for actors in channel and its channel configuration CC2. Again, we can see that while the peers and applications are critical actors in the network, their behaviour in a channel is dictated more by the channel configuration policy than any other factor.

Finally, it is helpful to understand how network and channel configurations are physically realized. We can see that network and channel configurations are logically singular – there is one for the network, and one for each channel. This is important; every component that accesses the network or the channel must have a shared understanding of the permissions granted to different organizations.

Even though there is logically a single configuration, it is actually replicated and kept consistent by every node that forms the network or channel. For example, in our network peer nodes P1 and P2 both have a copy of channel configuration CC1, and by the time the network is fully complete, peer nodes P2 and P3 will both have a copy of channel configuration CC2. Similarly ordering service node O4 has a copy of the network configuration, but in a *multi-node configuration*, every ordering service node will have its own copy of the network configuration.

Both network and channel configurations are kept consistent using the same blockchain technology that is used for user transactions – but for **configuration** transactions. To change a network or client configuration, an administrator must submit a configuration transaction to change the network or channel configuration. It must be signed by the organizations identified in the appropriate policy as being responsible for configuration change. This policy is called the **mod_policy** and we'll *discuss it later*.

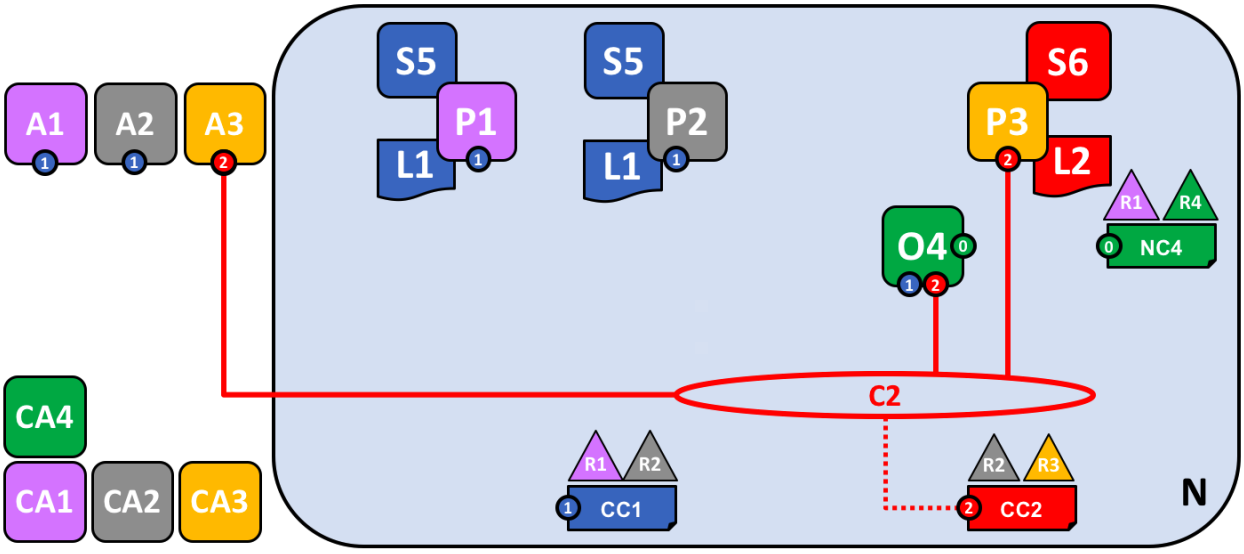
Indeed, the ordering service nodes operate a mini-blockchain, connected via the **system channel** we mentioned earlier. Using the system channel ordering service nodes distribute network configuration transactions. These transactions are used to co-operatively maintain a consistent copy of the network configuration at each ordering service node. In a similar way, peer nodes in an **application channel** can distribute channel configuration transactions. Likewise, these transactions are used to maintain a consistent copy of the channel configuration at each peer node.

This balance between objects that are logically singular, by being physically distributed is a common pattern in Hyperledger Fabric. Objects like network configurations, that are logically single, turn out to be physically replicated among a set of ordering services nodes for example. We also see it with channel configurations, ledgers, and to some extent smart contracts which are installed in multiple places but whose interfaces exist logically at the channel level. It's a pattern you see repeated time and again in Hyperledger Fabric, and enables Hyperledger Fabric to be both de-centralized and yet manageable at the same time.

4.4.13 Adding another peer

Now that organization R3 is able to fully participate in channel C2, let's add its infrastructure components to the channel. Rather than do this one component at a time, we're going to add a peer, its local copy of a ledger, a smart contract and a client application all at once!

Let's see the network with organization R3's components added:



The diagram shows the facts relating to channels C1 and C2 in the network N as follows: Client applications A1 and A2 can use channel C1 for communication with peers P1 and P2, and ordering service O4; client applications A3 can use channel C2 for communication with peer P3 and ordering service O4. Ordering service O4 can make use of the communication services of channels C1 and C2. Channel configuration CC1 applies to channel C1, CC2 applies to channel C2.

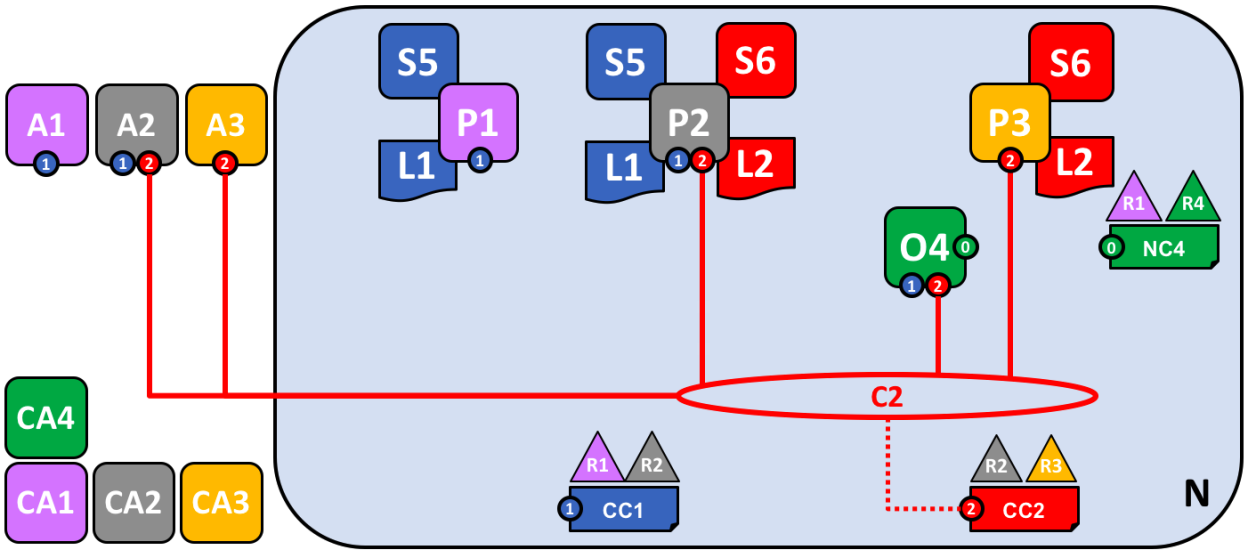
First of all, notice that because peer node P3 is connected to channel C2, it has a **different** ledger – L2 – to those peer nodes using channel C1. The ledger L2 is effectively scoped to channel C2. The ledger L1 is completely separate; it is scoped to channel C1. This makes sense – the purpose of the channel C2 is to provide private communications between the members of the consortium X2, and the ledger L2 is the private store for their transactions.

In a similar way, the smart contract S6, installed on peer node P3, and instantiated on channel C2, is used to provide controlled access to ledger L2. Application A3 can now use channel C2 to invoke the services provided by smart contract S6 to generate transactions that can be accepted onto every copy of the ledger L2 in the network.

At this point in time, we have a single network that has two completely separate channels defined within it. These channels provide independently managed facilities for organizations to transact with each other. Again, this is decentralization at work; we have a balance between control and autonomy. This is achieved through policies which are applied to channels which are controlled by, and affect, different organizations.

4.4.14 Joining a peer to multiple channels

In this final stage of network development, let's return our focus to organization R2. We can exploit the fact that R2 is a member of both consortia X1 and X2 by joining it to multiple channels:



The diagram shows the facts relating to channels C1 and C2 in the network N as follows: Client applications A1 can use channel C1 for communication with peers P1 and P2, and ordering service O4; client application A2 can use channel C1 for communication with peers P1 and P2 and channel C2 for communication with peers P2 and P3 and ordering service O4; client application A3 can use channel C2 for communication with peer P3 and ordering service O4. Ordering service O4 can make use of the communication services of channels C1 and C2. Channel configuration CC1 applies to channel C1, CC2 applies to channel C2.

We can see that R2 is a special organization in the network, because it is the only organization that is a member of two application channels! It is able to transact with organization R1 on channel C1, while at the same time it can also transact with organization R3 on a different channel, C2.

Notice how peer node P2 has smart contract S5 installed for channel C1 and smart contract S6 installed for channel C2. Peer node P2 is a full member of both channels at the same time via different smart contracts for different ledgers.

This is a very powerful concept – channels provide both a mechanism for the separation of organizations, and a mechanism for collaboration between organizations. All the while, this infrastructure is provided by, and shared between, a set of independent organizations.

It is also important to note that peer node P2's behaviour is controlled very differently depending upon the channel in which it is transacting. Specifically, the policies contained in channel configuration CC1 dictate the operations available to P2 when it is transacting in channel C1, whereas it is the policies in channel configuration CC2 that control P2's behaviour in channel C2.

Again, this is desirable – R2 and R1 agreed the rules for channel C1, whereas R2 and R3 agreed the rules for channel C2. These rules were captured in the respective channel policies – they can and must be used by every component in a channel to enforce correct behaviour, as agreed.

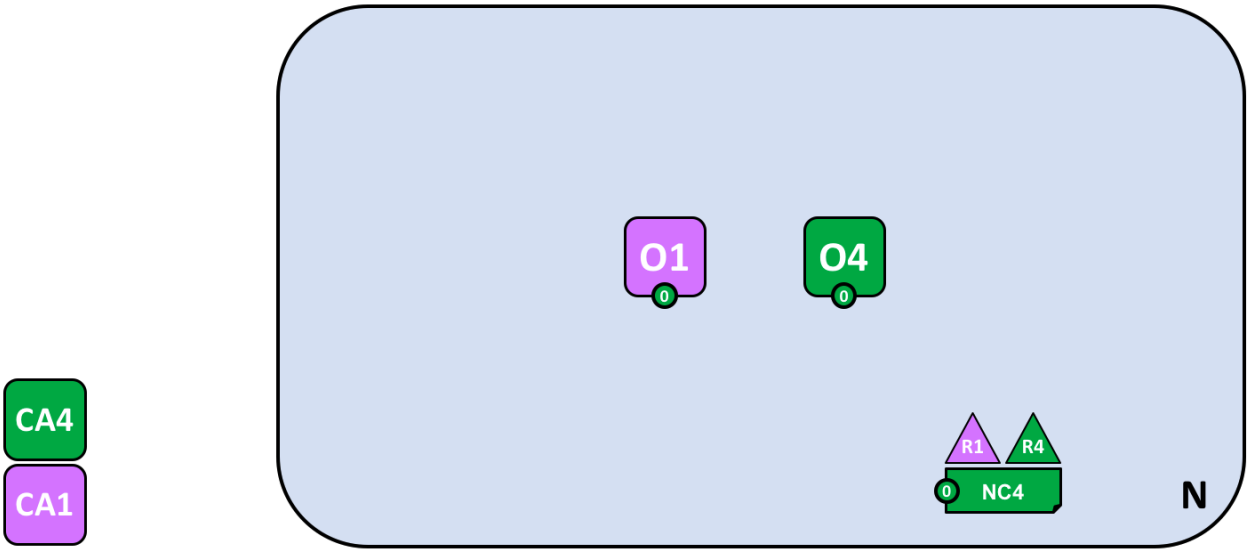
Similarly, we can see that client application A2 is now able to transact on channels C1 and C2. And likewise, it too will be governed by the policies in the appropriate channel configurations. As an aside, note that client application A2 and peer node P2 are using a mixed visual vocabulary – both lines and connections. You can see that they are equivalent; they are visual synonyms.

The ordering service

The observant reader may notice that the ordering service node appears to be a centralized component; it was used to create the network initially, and connects to every channel in the network. Even though we added R1 and R4 to the network configuration policy NC4 which controls the orderer, the node was running on R4's infrastructure. In a world of de-centralization, this looks wrong!

Don't worry! Our example network showed the simplest ordering service configuration to help you understand the idea of a network administration point. In fact, the ordering service can itself too be completely de-centralized! We mentioned earlier that an ordering service could be comprised of many individual nodes owned by different organizations, so let's see how that would be done in our sample network.

Let's have a look at a more realistic ordering service node configuration:



A multi-organization ordering service. The ordering service comprises ordering service nodes O1 and O4. O1 is provided by organization R1 and node O4 is provided by organization R4. The network configuration NC4 defines network resource permissions for actors from both organizations R1 and R4.

We can see that this ordering service completely de-centralized – it runs in organization R1 and it runs in organization R4. The network configuration policy, NC4, permits R1 and R4 equal rights over network resources. Client applications and peer nodes from organizations R1 and R4 can manage network resources by connecting to either node O1 or node O4, because both nodes behave the same way, as defined by the policies in network configuration NC4. In practice, actors from a particular organization *tend* to use infrastructure provided by their home organization, but that's certainly not always the case.

De-centralized transaction distribution

As well as being the management point for the network, the ordering service also provides another key facility – it is the distribution point for transactions. The ordering service is the component which gathers endorsed transactions from applications and orders them into transaction blocks, which are subsequently distributed to every peer node in the channel. At each of these committing peers, transactions are recorded, whether valid or invalid, and their local copy of the ledger updated appropriately.

Notice how the ordering service node O4 performs a very different role for the channel C1 than it does for the network N. When acting at the channel level, O4's role is to gather transactions and distribute blocks inside channel C1. It does this according to the policies defined in channel configuration CC1. In contrast, when acting at the network level, O4's role is to provide a management point for network resources according to the policies defined in network configuration NC4. Notice again how these roles are defined by different policies within the channel and network configurations respectively. This should reinforce to you the importance of declarative policy based configuration in Hyperledger Fabric. Policies both define, and are used to control, the agreed behaviours by each and every member of a consortium.

We can see that the ordering service, like the other components in Hyperledger Fabric, is a fully de-centralized component. Whether acting as a network management point, or as a distributor of blocks in a channel, its nodes can be

distributed as required throughout the multiple organizations in a network.

Changing policy

Throughout our exploration of the sample network, we've seen the importance of the policies to control the behaviour of the actors in the system. We've only discussed a few of the available policies, but there are many that can be declaratively defined to control every aspect of behaviour. These individual policies are discussed elsewhere in the documentation.

Most importantly of all, Hyperledger Fabric provides a uniquely powerful policy that allows network and channel administrators to manage policy change itself! The underlying philosophy is that policy change is a constant, whether it occurs within or between organizations, or whether it is imposed by external regulators. For example, new organizations may join a channel, or existing organizations may have their permissions increased or decreased. Let's investigate a little more how change policy is implemented in Hyperledger Fabric.

They key point of understanding is that policy change is managed by a policy within the policy itself. The **modification policy**, or **mod_policy** for short, is a first class policy within a network or channel configuration that manages change. Let's give two brief examples of how we've **already** used mod_policy can be used to manage change in our network!

The first example was when the network was initially set up. At this time, only organization R4 was allowed to manage the network. In practice, this was achieved by making R4 the only organization defined in the network configuration NC4 with permissions to network resources. Moreover, the mod_policy for NC4 only mentioned organization R4 – only R4 was allowed to change this configuration.

We then evolved the network N to also allow organization R1 to administer the network. R4 did this by adding R1 to the policies for channel creation and consortium creation. Because of this change, R1 was able to define the consortia X1 and X2, and create the channels C1 and C2. R1 had equal administrative rights over the channel and consortium policies in the network configuration.

R4 however, could grant even more power over the network configuration to R1! R4 could add R1 to the mod_policy such that R1 would be able to manage change of the network policy too.

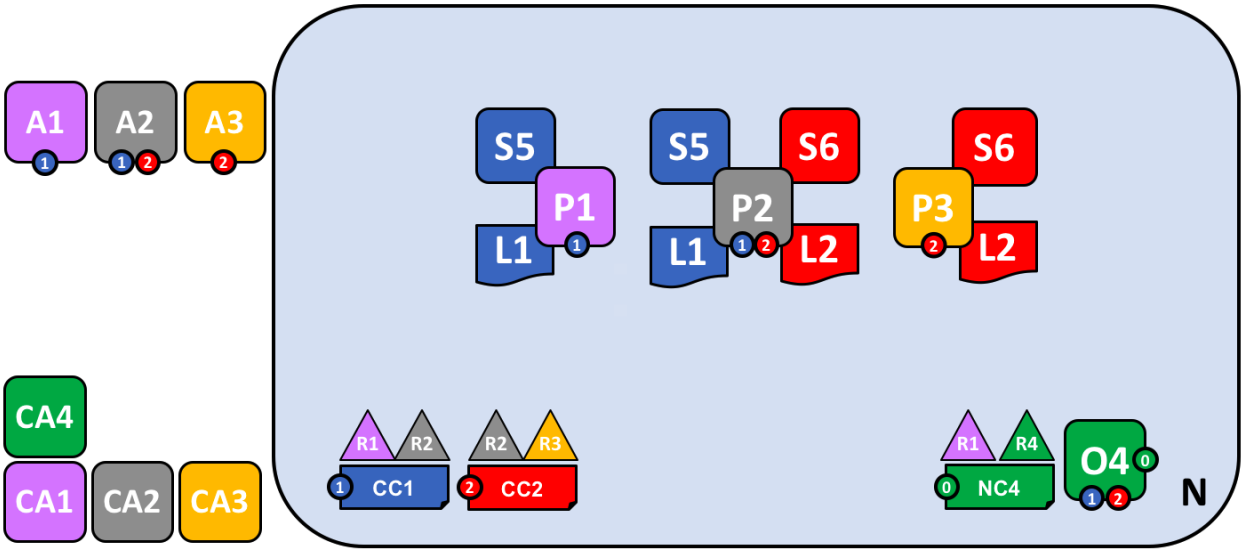
This second power is much more powerful than the first, because now R1 now has **full control** over the network configuration NC4! This means that R1 can, in principle remove R4's management rights from the network. In practice, R4 would configure the mod_policy such that R4 would need to also approve the change, or that all organizations in the mod_policy would have to approve the change. There's lots of flexibility to make the mod_policy as sophisticated as it needs to be to support whatever change process is required.

This is mod_policy at work – it has allowed the graceful evolution of a basic configuration into a sophisticated one. All the time this has occurred with the agreement of all organization involved. The mod_policy behaves like every other policy inside a network or channel configuration; it defines a set of organizations that are allowed to change the mod_policy itself.

We've only scratched the surface of the power of policies and mod_policy in particular in this subsection. It is discussed at much more length in the policy topic, but for now let's return to our finished network!

4.4.15 Network fully formed

Let's recap what our network looks like using a consistent visual vocabulary. We've re-organized it slightly using our more compact visual syntax, because it better accommodates larger topologies:



In this diagram we see that the Fabric blockchain network consists of two application channels and one ordering channel. The organizations R1 and R4 are responsible for the ordering channel, R1 and R2 are responsible for the blue application channel while R2 and R3 are responsible for the red application channel. Client applications A1 is an element of organization R1, and CA1 is its certificate authority. Note that peer P2 of organization R2 can use the communication facilities of the blue and the red application channel. Each application channel has its own channel configuration, in this case CC1 and CC2. The channel configuration of the system channel is part of the network configuration, NC4.

We're at the end of our conceptual journey to build a sample Hyperledger Fabric blockchain network. We've created a four organization network with two channels and three peer nodes, with two smart contracts and an ordering service. It is supported by four certificate authorities. It provides ledger and smart contract services to three client applications, who can interact with it via the two channels. Take a moment to look through the details of the network in the diagram, and feel free to read back through the topic to reinforce your knowledge, or go to a more detailed topic.

Summary of network components

Here's a quick summary of the network components we've discussed:

- Ledger. One per channel. Comprised of the Blockchain and the World state
- Smart contract (aka chaincode)
- Peer nodes
- Ordering service
- Channel
- Certificate Authority

4.4.16 Network summary

In this topic, we've seen how different organizations share their infrastructure to provide an integrated Hyperledger Fabric blockchain network. We've seen how the collective infrastructure can be organized into channels that provide private communications mechanisms that are independently managed. We've seen how actors such as client applications, administrators, peers and orderers are identified as being from different organizations by their use of certificates

from their respective certificate authorities. And in turn, we've seen the importance of policy to define the agreed permissions that these organizational actors have over network and channel resources.

4.5 Identity

4.5.1 What is an Identity?

The different actors in a blockchain network include peers, orderers, client applications, administrators and more. Each of these actors — active elements inside or outside a network able to consume services — has a digital identity encapsulated in an X.509 digital certificate. These identities really matter because they **determine the exact permissions over resources and access to information that actors have in a blockchain network.**

A digital identity furthermore has some additional attributes that Fabric uses to determine permissions, and it gives the union of an identity and the associated attributes a special name — **principal**. Principals are just like userIDs or groupIDs, but a little more flexible because they can include a wide range of properties of an actor's identity, such as the actor's organization, organizational unit, role or even the actor's specific identity. When we talk about principals, they are the properties which determine their permissions.

For an identity to be **verifiable**, it must come from a **trusted** authority. A membership service provider (MSP) is how this is achieved in Fabric. More specifically, an MSP is a component that defines the rules that govern the valid identities for this organization. The default MSP implementation in Fabric uses X.509 certificates as identities, adopting a traditional Public Key Infrastructure (PKI) hierarchical model (more on PKI later).

4.5.2 A Simple Scenario to Explain the Use of an Identity

Imagine that you visit a supermarket to buy some groceries. At the checkout you see a sign that says that only Visa, Mastercard and AMEX cards are accepted. If you try to pay with a different card — let's call it an "ImagineCard" — it doesn't matter whether the card is authentic and you have sufficient funds in your account. It will be not be accepted.

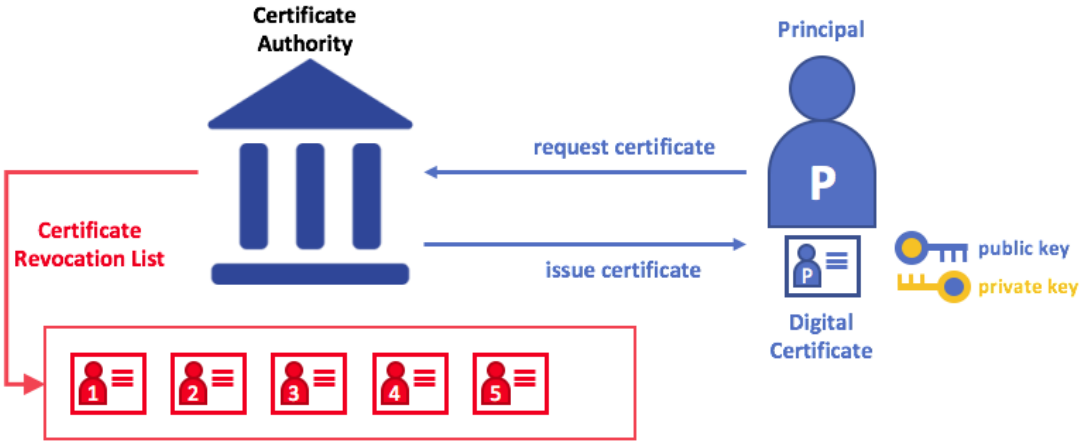
Having a valid credit card is not enough — it must also be accepted by the store! PKIs and MSPs work together in the same way — a PKI provides a list of identities, and an MSP says which of these are members of a given organization that participates in the network.

PKI certificate authorities and MSPs provide a similar combination of functionalities. A PKI is like a card provider — it dispenses many different types of verifiable identities. An MSP, on the other hand, is like the list of card providers accepted by the store, determining which identities are the trusted members (actors) of the store payment network. **MSPs turn verifiable identities into the members of a blockchain network**.

Let's drill into these concepts in a little more detail.

4.5.3 What are PKIs?

A public key infrastructure (PKI) is a collection of internet technologies that provides secure communications in a network. It's PKI that puts the **S** in **HTTPS** — and if you're reading this documentation on a web browser, you're probably using a PKI to make sure it comes from a verified source.



The elements of Public Key Infrastructure (PKI). A PKI is comprised of Certificate Authorities who issue digital certificates to parties (e.g., users of a service, service provider), who then use them to authenticate themselves in the messages they exchange with their environment. A CA's Certificate Revocation List (CRL) constitutes a reference for the certificates that are no longer valid. Revocation of a certificate can happen for a number of reasons. For example, a certificate may be revoked because the cryptographic private material associated to the certificate has been exposed.

Although a blockchain network is more than a communications network, it relies on the PKI standard to ensure secure communication between various network participants, and to ensure that messages posted on the blockchain are properly authenticated. It's therefore important to understand the basics of PKI and then why MSPs are so important.

There are four key elements to PKI:

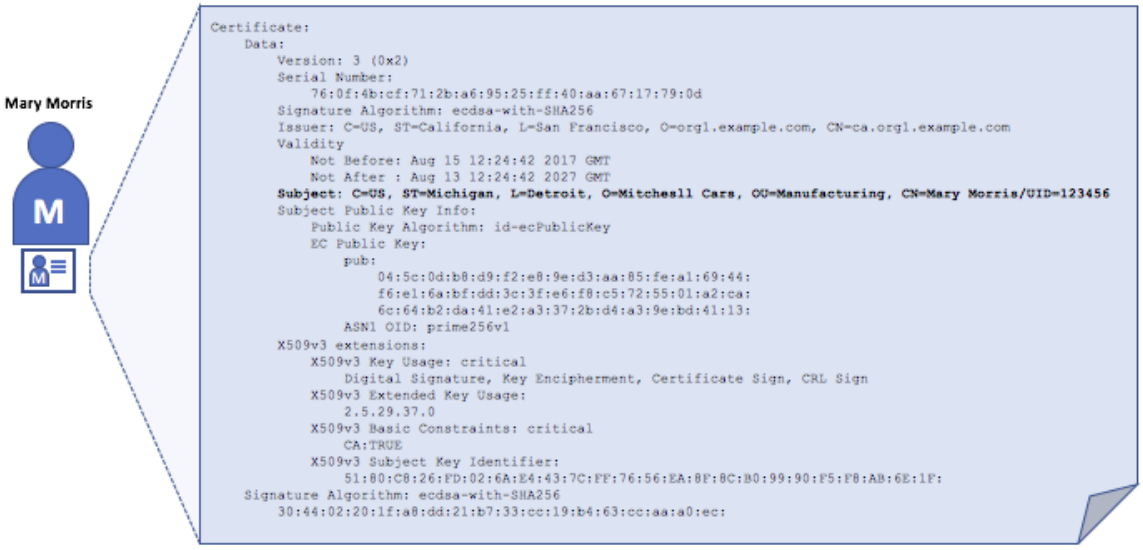
- **Digital Certificates**
- **Public and Private Keys**
- **Certificate Authorities**
- **Certificate Revocation Lists**

Let's quickly describe these PKI basics, and if you want to know more details, Wikipedia is a good place to start.

4.5.4 Digital Certificates

A digital certificate is a document which holds a set of attributes relating to the holder of the certificate. The most common type of certificate is the one compliant with the X.509 standard, which allows the encoding of a party's identifying details in its structure.

For example, Mary Morris in the Manufacturing Division of Mitchell Cars in Detroit, Michigan might have a digital certificate with a `SUBJECT` attribute of `C=US`, `ST=Michigan`, `L=Detroit`, `O=Mitchell Cars`, `OU=Manufacturing`, `CN=Mary Morris /UID=123456`. Mary's certificate is similar to her government identity card — it provides information about Mary which she can use to prove key facts about her. There are many other attributes in an X.509 certificate, but let's concentrate on just these for now.



A digital certificate describing a party called Mary Morris. Mary is the `SUBJECT` *of the certificate, and the highlighted* `SUBJECT` *text shows key facts about Mary. The certificate also holds many more pieces of information, as you can see. Most importantly, Mary's public key is distributed within her certificate, whereas her private signing key is not. This signing key must be kept private.*

What is important is that all of Mary's attributes can be recorded using a mathematical technique called cryptography (literally, "*secret writing*") so that tampering will invalidate the certificate. Cryptography allows Mary to present her certificate to others to prove her identity so long as the other party trusts the certificate issuer, known as a **Certificate Authority** (CA). As long as the CA keeps certain cryptographic information securely (meaning, its own **private signing key**), anyone reading the certificate can be sure that the information about Mary has not been tampered with — it will always have those particular attributes for Mary Morris. Think of Mary's X.509 certificate as a digital identity card that is impossible to change.

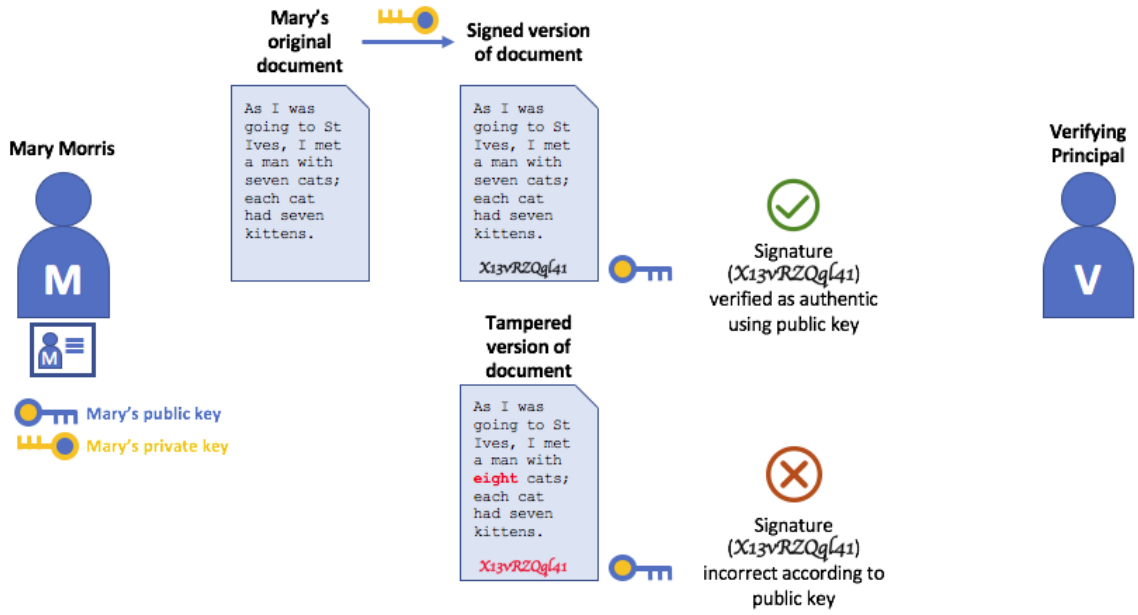
4.5.5 Authentication, Public keys, and Private Keys

Authentication and message integrity are important concepts in secure communications. Authentication requires that parties who exchange messages are assured of the identity that created a specific message. For a message to have "integrity" means that cannot have been modified during its transmission. For example, you might want to be sure you're communicating with the real Mary Morris rather than an impersonator. Or if Mary has sent you a message, you might want to be sure that it hasn't been tampered with by anyone else during transmission.

Traditional authentication mechanisms rely on **digital signatures** that, as the name suggests, allow a party to digitally **sign** its messages. Digital signatures also provide guarantees on the integrity of the signed message.

Technically speaking, digital signature mechanisms require each party to hold two cryptographically connected keys: a public key that is made widely available and acts as authentication anchor, and a private key that is used to produce **digital signatures** on messages. Recipients of digitally signed messages can verify the origin and integrity of a received message by checking that the attached signature is valid under the public key of the expected sender.

The unique relationship between a private key and the respective public key is the cryptographic magic that makes secure communications possible. The unique mathematical relationship between the keys is such that the private key can be used to produce a signature on a message that only the corresponding public key can match, and only on the same message.

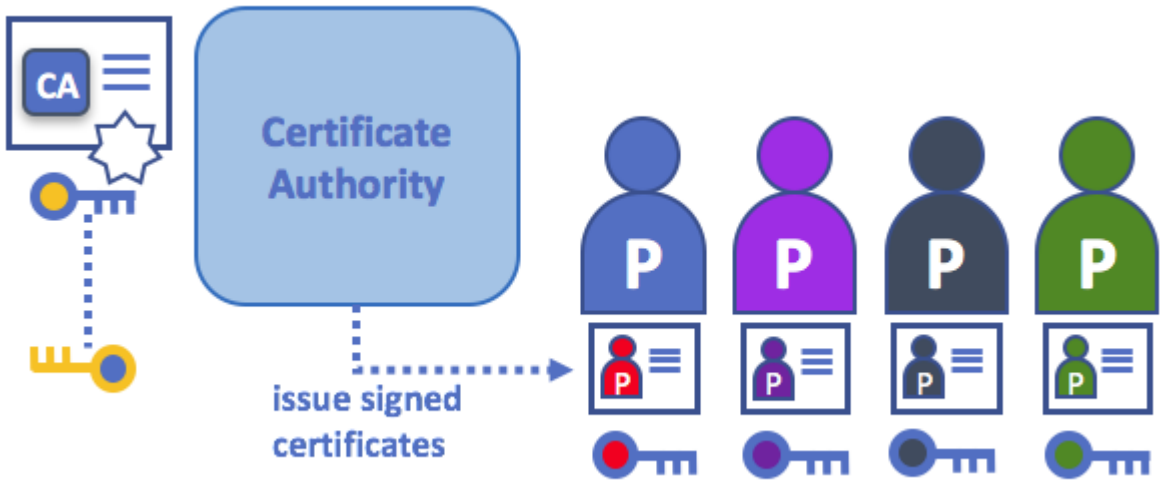


In the example above, Mary uses her private key to sign the message. The signature can be verified by anyone who sees the signed message using her public key.

4.5.6 Certificate Authorities

As you've seen, an actor or a node is able to participate in the blockchain network, via the means of a **digital identity** issued for it by an authority trusted by the system. In the most common case, digital identities (or simply **identities**) have the form of cryptographically validated digital certificates that comply with X.509 standard and are issued by a Certificate Authority (CA).

CAs are a common part of internet security protocols, and you've probably heard of some of the more popular ones: Symantec (originally Verisign), GeoTrust, DigiCert, GoDaddy, and Comodo, among others.



A Certificate Authority dispenses certificates to different actors. These certificates are digitally signed by the CA and

bind together the actor with the actor's public key (and optionally with a comprehensive list of properties). As a result, if one trusts the CA (and knows its public key), it can trust that the specific actor is bound to the public key included in the certificate, and owns the included attributes, by validating the CA's signature on the actor's certificate.

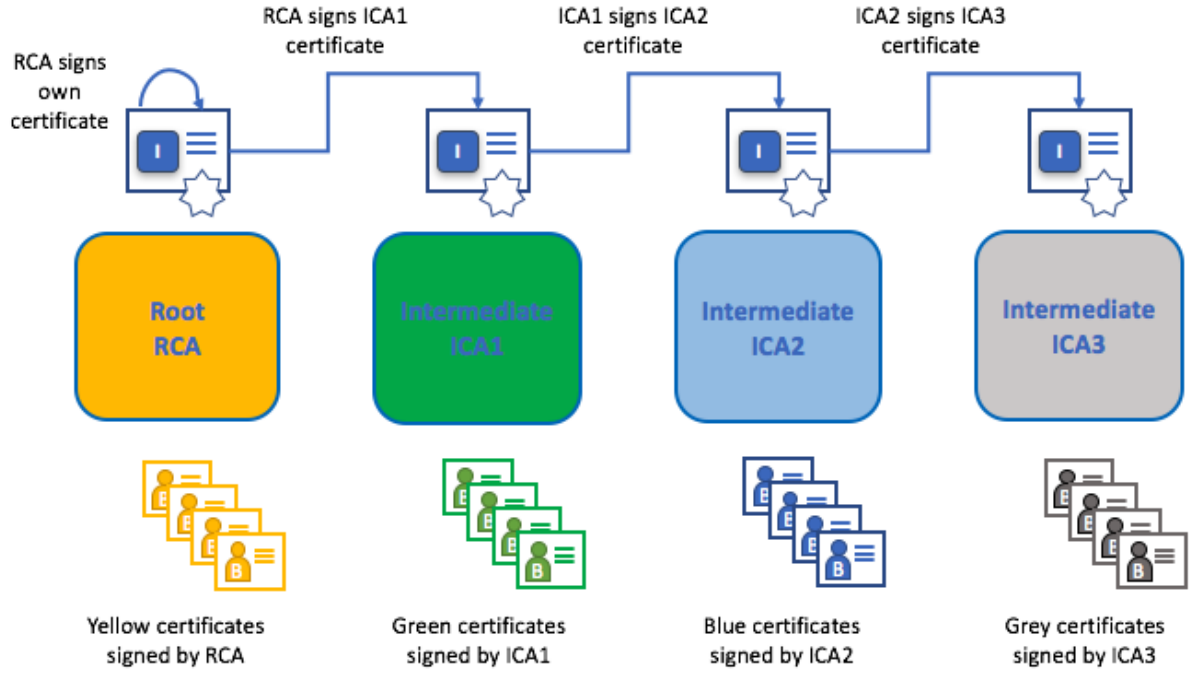
Certificates can be widely disseminated, as they do not include either the actors' nor the CA's private keys. As such they can be used as anchor of trusts for authenticating messages coming from different actors.

CAs also have a certificate, which they make widely available. This allows the consumers of identities issued by a given CA to verify them by checking that the certificate could only have been generated by the holder of the corresponding private key (the CA).

In a blockchain setting, every actor who wishes to interact with the network needs an identity. In this setting, you might say that **one or more CAs** can be used to **define the members of an organization's from a digital perspective**. It's the CA that provides the basis for an organization's actors to have a verifiable digital identity.

Root CAs, Intermediate CAs and Chains of Trust

CAs come in two flavors: **Root CAs** and **Intermediate CAs**. Because Root CAs (Symantec, Geotrust, etc) have to **securely distribute** hundreds of millions of certificates to internet users, it makes sense to spread this process out across what are called *Intermediate CAs*. These Intermediate CAs have their certificates issued by the root CA or another intermediate authority, allowing the establishment of a "chain of trust" for any certificate that is issued by any CA in the chain. This ability to track back to the Root CA not only allows the function of CAs to scale while still providing security — allowing organizations that consume certificates to use Intermediate CAs with confidence — it limits the exposure of the Root CA, which, if compromised, would endanger the entire chain of trust. If an Intermediate CA is compromised, on the other hand, there will be a much smaller exposure.



A chain of trust is established between a Root CA and a set of Intermediate CAs as long as the issuing CA for the certificate of each of these Intermediate CAs is either the Root CA itself or has a chain of trust to the Root CA.

Intermediate CAs provide a huge amount of flexibility when it comes to the issuance of certificates across multiple organizations, and that's very helpful in a permissioned blockchain system (like Fabric). For example, you'll see that different organizations may use different Root CAs, or the same Root CA with different Intermediate CAs — it really does depend on the needs of the network.

Fabric CA

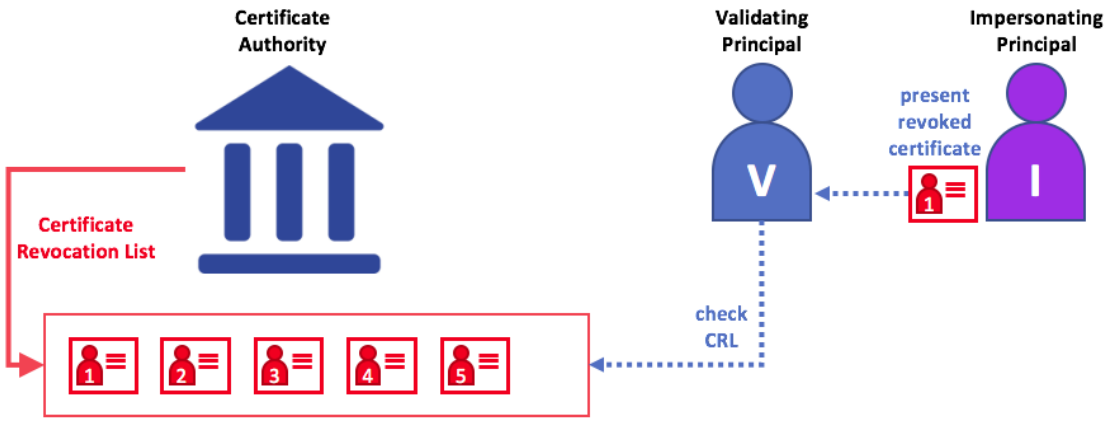
It's because CAs are so important that Fabric provides a built-in CA component to allow you to create CAs in the blockchain networks you form. This component — known as **Fabric CA** is a private root CA provider capable of managing digital identities of Fabric participants that have the form of X.509 certificates. Because Fabric CA is a custom CA targeting the Root CA needs of Fabric, it is inherently not capable of providing SSL certificates for general/automatic use in browsers. However, because **some** CA must be used to manage identity (even in a test environment), Fabric CA can be used to provide and manage certificates. It is also possible — and fully appropriate — to use a public/commerical root or intermediate CA to provide identification.

If you're interested, you can read a lot more about Fabric CA in the CA documentation section.

4.5.7 Certificate Revocation Lists

A Certificate Revocation List (CRL) is easy to understand — it's just a list of references to certificates that a CA knows to be revoked for one reason or another. If you recall the store scenario, a CRL would be like a list of stolen credit cards.

When a third party wants to verify another party's identity, it first checks the issuing CA's CRL to make sure that the certificate has not been revoked. A verifier doesn't have to check the CRL, but if they don't they run the risk of accepting a compromised identity.



Using a CRL to check that a certificate is still valid. If an impersonator tries to pass a compromised digital certificate to a validating party, it can be first checked against the issuing CA's CRL to make sure it's not listed as no longer valid.

Note that a certificate being revoked is very different from a certificate expiring. Revoked certificates have not expired — they are, by every other measure, a fully valid certificate. For more in-depth information about CRLs, click here.

Now that you've seen how a PKI can provide verifiable identities through a chain of trust, the next step is to see how these identities can be used to represent the trusted members of a blockchain network. That's where a Membership Service Provider (MSP) comes into play — **it identifies the parties who are the members of a given organization in the blockchain network**.

To learn more about membership, check out the conceptual documentation on MSPs.

an# Membership

If you've read through the documentation on identity you've seen how a PKI can provide verifiable identities through a chain of trust. Now let's see how these identities can be used to represent the trusted members of a blockchain network.

This is where a **Membership Service** Provider (MSP) comes into play — **it identifies which Root CAs and Intermediate CAs are trusted to define the members of a trust domain, e.g., an organization**, either by listing the identities of their members, or by identifying which CAs are authorized to issue valid identities for their members, or — as will usually be the case — through a combination of both.

The power of an MSP goes beyond simply listing who is a network participant or member of a channel. An MSP can identify specific **roles** an actor might play either within the scope of the organization the MSP represents (e.g., admins, or as members of a sub-organization group), and sets the basis for defining **access privileges** in the context of a network and channel (e.g., channel admins, readers, writers).

The configuration of an MSP is advertised to all the channels where members of the corresponding organization participate (in the form of a **channel MSP**). In addition to the channel MSP, peers, orderers, and clients also maintain a **local MSP** to authenticate member messages outside the context of a channel and to define the permissions over a particular component (who has the ability to install chaincode on a peer, for example).

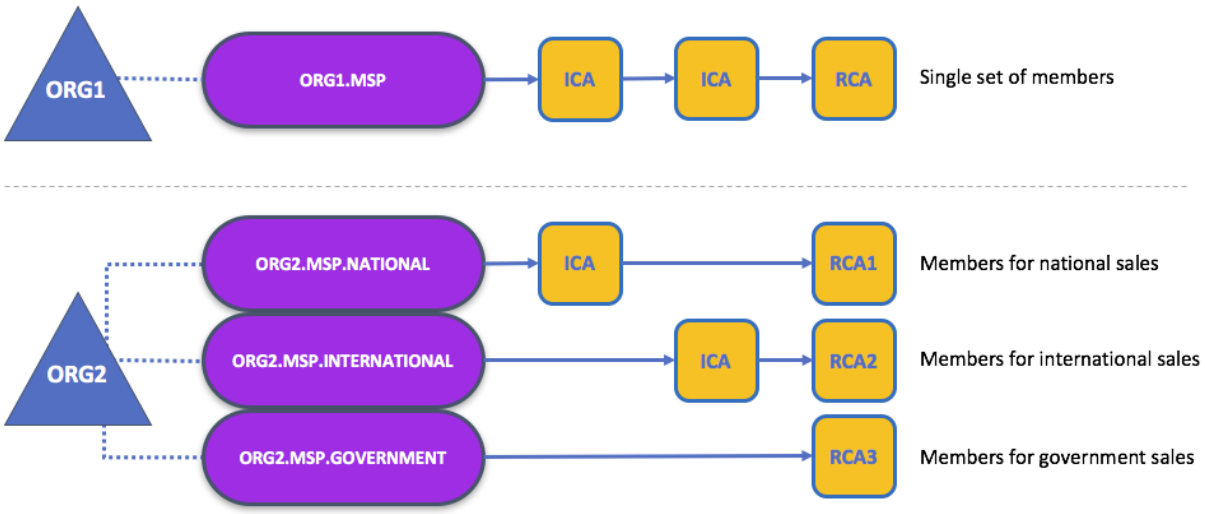
In addition, an MSP can allow for the identification of a list of identities that have been revoked — as discussed in the Identity documentation — but we will talk about how that process also extends to an MSP.

We'll talk more about local and channel MSPs in a moment. For now let's see what MSPs do in general.

4.6 Mapping MSPs to Organizations

An **organization** is a managed group of members. This can be something as big as a multinational corporation or a small as a flower shop. What's most important about organizations (or **orgs**) is that they manage their members under a single MSP. Note that this is different from the organization concept defined in an X.509 certificate, which we'll talk about later.

The exclusive relationship between an organization and its MSP makes it sensible to name the MSP after the organization, a convention you'll find adopted in most policy configurations. For example, organization `ORG1` would likely have an MSP called something like `ORG1-MSP`. In some cases an organization may require multiple membership groups — for example, where channels are used to perform very different business functions between organizations. In these cases it makes sense to have multiple MSPs and name them accordingly, e.g., `ORG2-MSP-NATIONAL` and `ORG2-MSP-GOVERNMENT`, reflecting the different membership roots of trust within `ORG2` in the `NATIONAL` sales channel compared to the `GOVERNMENT` regulatory channel.



Two different MSP configurations for an organization. The first configuration shows the typical relationship between an MSP and an organization — a single MSP defines the list of members of an organization. In the second

configuration, different MSPs are used to represent different organizational groups with national, international, and governmental affiliation.

4.6.1 Organizational Units and MSPs

An organization is often divided up into multiple **organizational units** (OUs), each of which has a certain set of responsibilities. For example, the `ORG1` organization might have both `ORG1-MANUFACTURING` and `ORG1-DISTRIBUTION` OUs to reflect these separate lines of business. When a CA issues X.509 certificates, the `OU` field in the certificate specifies the line of business to which the identity belongs.

We'll see later how OUs can be helpful to control the parts of an organization who are considered to be the members of a blockchain network. For example, only identities from the `ORG1-MANUFACTURING` OU might be able to access a channel, whereas `ORG1-DISTRIBUTION` cannot.

Finally, though this is a slight misuse of OUs, they can sometimes be used by different organizations in a consortium to distinguish each other. In such cases, the different organizations use the same Root CAs and Intermediate CAs for their chain of trust, but assign the `OU` field to identify members of each organization. We'll also see how to configure MSPs to achieve this later.

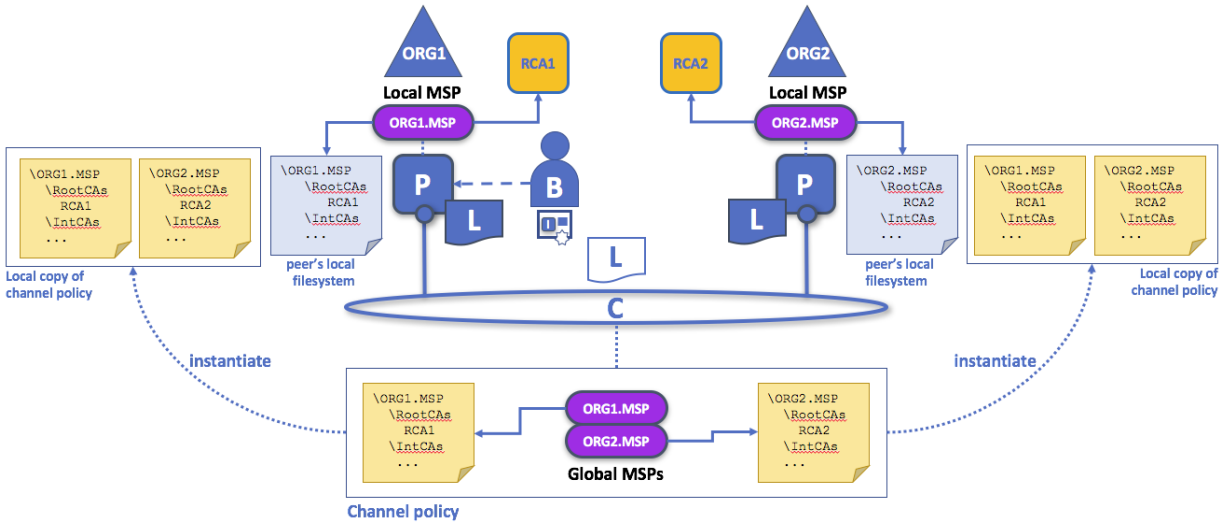
4.7 Local and Channel MSPs

MSPs appear in two places in a blockchain network: channel configuration (**channel MSPs**), and locally on an actor's premise (**local MSP**). **Local MSPs are defined for clients (users) and for nodes (peers and orderers)**. Node local MSPs define the permissions for that node (who the peer admins are, for example). The local MSPs of the users allow the user side to authenticate itself in its transactions as a member of a channel (e.g. in chaincode transactions), or as the owner of a specific role into the system (an org admin, for example, in configuration transactions).

Every node and user must have a local MSP defined, as it defines who has administrative or participatory rights at that level (peer admins will not necessarily be channel admins, and vice versa).

In contrast, **channel MSPs define administrative and participatory rights at the channel level**. Every organization participating in a channel must have an MSP defined for it. Peers and orderers on a channel will all share the same view of channel MSPs, and will therefore be able to correctly authenticate the channel participants. This means that if an organization wishes to join the channel, an MSP incorporating the chain of trust for the organization's members would need to be included in the channel configuration. Otherwise transactions originating from this organization's identities will be rejected.

The key difference here between local and channel MSPs is not how they function — both turn identities into roles — but their **scope**.



Local and channel MSPs. The trust domain (e.g., the organization) of each peer is defined by the peer's local MSP, e.g., ORG1 or ORG2. Representation of an organization on a channel is achieved by adding the organization's MSP to the channel configuration. For example, the channel of this figure is managed by both ORG1 and ORG2. Similar principles apply for the network, orderers, and users, but these are not shown here for simplicity.

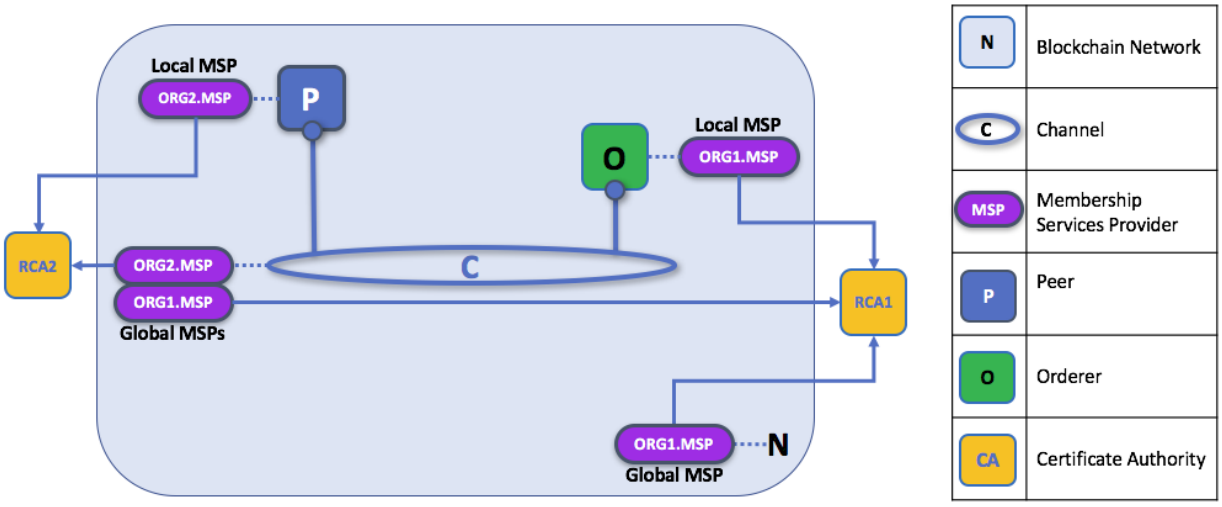
You may find it helpful to see how local and channel MSPs are used by seeing what happens when a blockchain administrator installs and instantiates a smart contract, as shown in the *diagram above*.

An administrator `B` connects to the peer with an identity issued by `RCA1` and stored in their local MSP. When `B` tries to install a smart contract on the peer, the peer checks its local MSP, `ORG1-MSP`, to verify that the identity of `B` is indeed a member of `ORG1`. A successful verification will allow the install command to complete successfully. Subsequently, `B` wishes to instantiate the smart contract on the channel. Because this is a channel operation, all organizations on the channel must agree to it. Therefore, the peer must check the MSPs of the channel before it can successfully commit this command. (Other things must happen too, but concentrate on the above for now.)

Local MSPs are only defined on the file system of the node or user to which they apply. Therefore, physically and logically there is only one local MSP per node or user. However, as channel MSPs are available to all nodes in the channel, they are logically defined once in the channel configuration. However, **a channel MSP is also instantiated on the file system of every node in the channel and kept synchronized via consensus**. So while there is a copy of each channel MSP on the local file system of every node, logically a channel MSP resides on and is maintained by the channel or the network.

4.8 MSP Levels

The split between channel and local MSPs reflects the needs of organizations to administer their local resources, such as a peer or orderer nodes, and their channel resources, such as ledgers, smart contracts, and consortia, which operate at the channel or network level. It's helpful to think of these MSPs as being at different **levels**, with **MSPs at a higher level relating to network administration concerns** while **MSPs at a lower level handle identity for the administration of private resources**. MSPs are mandatory at every level of administration — they must be defined for the network, channel, peer, orderer, and users.

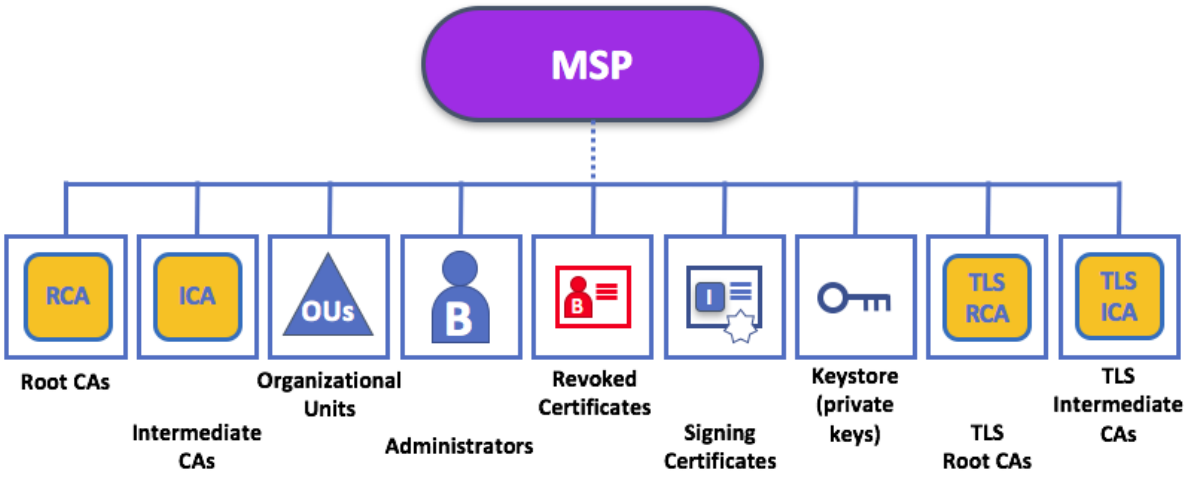


MSP Levels. The MSPs for the peer and orderer are local, whereas the MSPs for a channel (including the network configuration channel) are shared across all participants of that channel. In this figure, the network configuration channel is administered by ORG1, but another application channel can be managed by ORG1 and ORG2. The peer is a member of and managed by ORG2, whereas ORG1 manages the orderer of the figure. ORG1 trusts identities from RCA1, whereas ORG2 trusts identities from RCA2. Note that these are administration identities, reflecting who can administer these components. So while ORG1 administers the network, ORG2.MSP does exist in the network definition.

- **Network MSP:** The configuration of a network defines who are the members in the network — by defining the MSPs of the participant organizations — as well as which of these members are authorized to perform administrative tasks (e.g., creating a channel).
- **Channel MSP:** It is important for a channel to maintain the MSPs of its members separately. A channel provides private communications between a particular set of organizations which in turn have administrative control over it. Channel policies interpreted in the context of that channel's MSPs define who has ability to participate in certain action on the channel, e.g., adding organizations, or instantiating chaincodes. Note that there is no necessary relationship between the permission to administrate a channel and the ability to administrate the network configuration channel (or any other channel). Administrative rights exist within the scope of what is being administrated (unless the rules have been written otherwise — see the discussion of the `ROLE` attribute below).
- **Peer MSP:** This local MSP is defined on the file system of each peer and there is a single MSP instance for each peer. Conceptually, it performs exactly the same function as channel MSPs with the restriction that it only applies to the peer where it is defined. An example of an action whose authorization is evaluated using the peer's local MSP is the installation of a chaincode on the peer.
- **Orderer MSP:** Like a peer MSP, an orderer local MSP is also defined on the file system of the node and only applies to that node. Like peer nodes, orderers are also owned by a single organization and therefore have a single MSP to list the actors or nodes it trusts.

4.9 MSP Structure

So far, you've seen that the most important element of an MSP are the specification of the root or intermediate CAs that are used to establish an actor's or node's membership in the respective organization. There are, however, more elements that are used in conjunction with these two to assist with membership functions.



The figure above shows how a local MSP is stored on a local filesystem. Even though channel MSPs are not physically structured in exactly this way, it's still a helpful way to think about them.

As you can see, there are nine elements to an MSP. It's easiest to think of these elements in a directory structure, where the MSP name is the root folder name with each subfolder representing different elements of an MSP configuration.

Let's describe these folders in a little more detail and see why they are important.

- **Root CAs:** This folder contains a list of self-signed X.509 certificates of the Root CAs trusted by the organization represented by this MSP. There must be at least one Root CA X.509 certificate in this MSP folder.

  This is the most important folder because it identifies the CAs from which all other certificates must be derived to be considered members of the corresponding organization.

- **Intermediate CAs:** This folder contains a list of X.509 certificates of the Intermediate CAs trusted by this organization. Each certificate must be signed by one of the Root CAs in the MSP or by an Intermediate CA whose issuing CA chain ultimately leads back to a trusted Root CA.

  An intermediate CA may represent a different subdivision of the organization (like `ORG1-MANUFACTURING` and `ORG1-DISTRIBUTION` do for `ORG1`), or the organization itself (as may be the case if a commercial CA is leveraged for the organization's identity management). In the latter case intermediate CAs can be used to represent organization subdivisions. Here you may find more information on best practices for MSP configuration. Notice, that it is possible to have a functioning network that does not have an Intermediate CA, in which case this folder would be empty.

  Like the Root CA folder, this folder defines the CAs from which certificates must be issued to be considered members of the organization.

- **Organizational Units (OUs):** These are listed in the `$FABRIC_CFG_PATH/msp/config.yaml` file and contain a list of organizational units, whose members are considered to be part of the organization represented by this MSP. This is particularly useful when you want to restrict the members of an organization to the ones holding an identity (signed by one of MSP designated CAs) with a specific OU in it.

  Specifying OUs is optional. If no OUs are listed, all the identities that are part of an MSP — as identified by the Root CA and Intermediate CA folders — will be considered members of the organization.

- **Administrators:** This folder contains a list of identities that define the actors who have the role of administrators for this organization. For the standard MSP type, there should be one or more X.509 certificates in this list.

  It's worth noting that just because an actor has the role of an administrator it doesn't mean that they can administer particular resources! The actual power a given identity has with respect to administering the system is determined by the policies that manage system resources. For example, a channel policy might specify that

`ORG1-MANUFACTURING` administrators have the rights to add new organizations to the channel, whereas the `ORG1-DISTRIBUTION` administrators have no such rights.

Even though an X.509 certificate has a `ROLE` attribute (specifying, for example, that an actor is an `admin`), this refers to an actor's role within its organization rather than on the blockchain network. This is similar to the purpose of the `OU` attribute, which — if it has been defined — refers to an actor's place in the organization.

The `ROLE` attribute **can** be used to confer administrative rights at the channel level if the policy for that channel has been written to allow any administrator from an organization (or certain organizations) permission to perform certain channel functions (such as instantiating chaincode). In this way, an organizational role can confer a network role.

- **Revoked Certificates:** If the identity of an actor has been revoked, identifying information about the identity — not the identity itself — is held in this folder. For X.509-based identities, these identifiers are pairs of strings known as Subject Key Identifier (SKI) and Authority Access Identifier (AKI), and are checked whenever the X.509 certificate is being used to make sure the certificate has not been revoked.

  This list is conceptually the same as a CA's Certificate Revocation List (CRL), but it also relates to revocation of membership from the organization. As a result, the administrator of an MSP, local or channel, can quickly revoke an actor or node from an organization by advertising the updated CRL of the CA the revoked certificate as issued by. This "list of lists" is optional. It will only become populated as certificates are revoked.

- **Node Identity:** This folder contains the identity of the node, i.e., cryptographic material that — in combination to the content of `KeyStore` — would allow the node to authenticate itself in the messages that is sends to other participants of its channels and network. For X.509 based identities, this folder contains an **X.509 certificate**. This is the certificate a peer places in a transaction proposal response, for example, to indicate that the peer has endorsed it — which can subsequently be checked against the resulting transaction's endorsement policy at validation time.

  This folder is mandatory for local MSPs, and there must be exactly one X.509 certificate for the node. It is not used for channel MSPs.

- **`KeyStore` for Private Key:** This folder is defined for the local MSP of a peer or orderer node (or in an client's local MSP), and contains the node's **signing key**. This key matches cryptographically the node's identity included in **Node Identity** folder and is used to sign data — for example to sign a transaction proposal response, as part of the endorsement phase.

  This folder is mandatory for local MSPs, and must contain exactly one private key. Obviously, access to this folder must be limited only to the identities of users who have administrative responsibility on the peer.

  Configuration of a **channel MSPs** does not include this folder, as channel MSPs solely aim to offer identity validation functionalities and not signing abilities.

- **TLS Root CA:** This folder contains a list of self-signed X.509 certificates of the Root CAs trusted by this organization **for TLS communications**. An example of a TLS communication would be when a peer needs to connect to an orderer so that it can receive ledger updates.

  MSP TLS information relates to the nodes inside the network — the peers and the orderers, in other words, rather than the applications and administrations that consume the network.

  There must be at least one TLS Root CA X.509 certificate in this folder.

- **TLS Intermediate CA:** This folder contains a list intermediate CA certificates CAs trusted by the organization represented by this MSP **for TLS communications**. This folder is specifically useful when commercial CAs are used for TLS certificates of an organization. Similar to membership intermediate CAs, specifying intermediate TLS CAs is optional.

  For more information about TLS, click here.

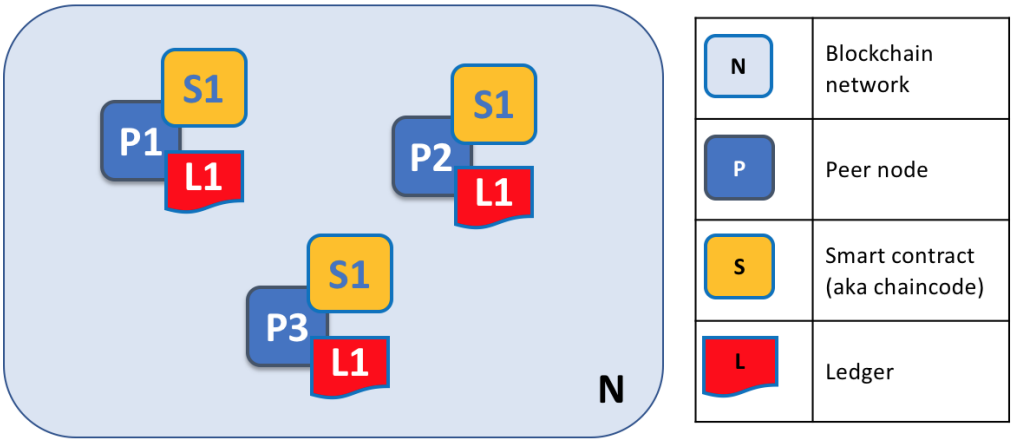
If you've read this doc as well as our doc on Identity), you should have a pretty good grasp of how identities and membership work in Hyperledger Fabric. You've seen how a PKI and MSPs are used to identify the actors collaborating in

a blockchain network. You've learned how certificates, public/private keys, and roots of trust work, in addition to how MSPs are physically and logically structured.

4.10 Peers

A blockchain network is comprised primarily of a set of *peer nodes* (or, simply, *peers*). Peers are a fundamental element of the network because they host ledgers and smart contracts. Recall that a ledger immutably records all the transactions generated by smart contracts (or *chaincode*). Smart contracts and ledgers are used to encapsulate the shared *processes* and shared *information* in a network, respectively. These aspects of a peer make them a good starting point to understand a Hyperledger Fabric network.

Other elements of the blockchain network are of course important: ledgers and smart contracts, orderers, policies, channels, applications, organizations, identities, and membership, and you can read more about them in their own dedicated sections. This section focusses on peers, and their relationship to those other elements in a Hyperledger Fabric network.



A blockchain network is comprised of peer nodes, each of which can hold copies of ledgers and copies of smart contracts. In this example, the network N consists of peers P1, P2 and P3, each of which maintain their own instance of the distributed ledger L1. P1, P2 and P3 use the same chaincode, S1, to access their copy of that distributed ledger.

Peers can be created, started, stopped, reconfigured, and even deleted. They expose a set of APIs that enable administrators and applications to interact with the services that they provide. We'll learn more about these services in this section.

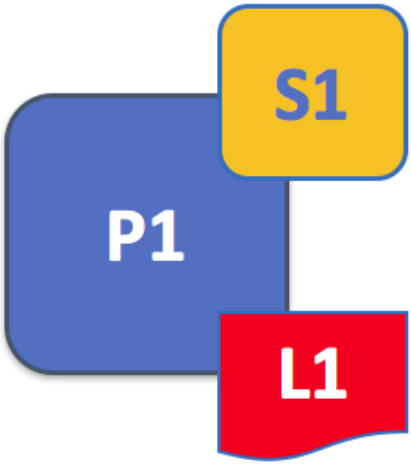
4.10.1 A word on terminology

Hyperledger Fabric implements smart contracts with a technology concept it calls **chaincode** — simply a piece of code that accesses the ledger, written in one of the supported programming languages. In this topic, we'll usually use the term **chaincode**, but feel free to read it as **smart contract** if you're more used to that term. It's the same thing!

4.10.2 Ledgers and Chaincode

Let's look at a peer in a little more detail. We can see that it's the peer that hosts both the ledger and chaincode. More accurately, the peer actually hosts *instances* of the ledger, and *instances* of chaincode. Note that this provides a

deliberate redundancy in a Fabric network — it avoids single points of failure. We'll learn more about the distributed and decentralized nature of a blockchain network later in this section.

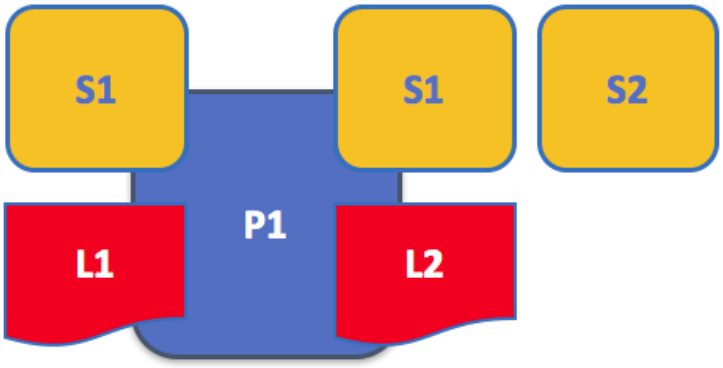


A peer hosts instances of ledgers and instances of chaincodes. In this example, P1 hosts an instance of ledger L1 and an instance of chaincode S1. There can be many ledgers and chaincodes hosted on an individual peer.

Because a peer is a *host* for ledgers and chaincodes, applications and administrators must interact with a peer if they want to access these resources. That's why peers are considered the most fundamental building blocks of a Hyperledger Fabric network. When a peer is first created, it has neither ledgers nor chaincodes. We'll see later how ledgers get created, and how chaincodes get installed, on peers.

Multiple Ledgers

A peer is able to host more than one ledger, which is helpful because it allows for a flexible system design. The simplest configuration is for a peer to manage a single ledger, but it's absolutely appropriate for a peer to host two or more ledgers when required.



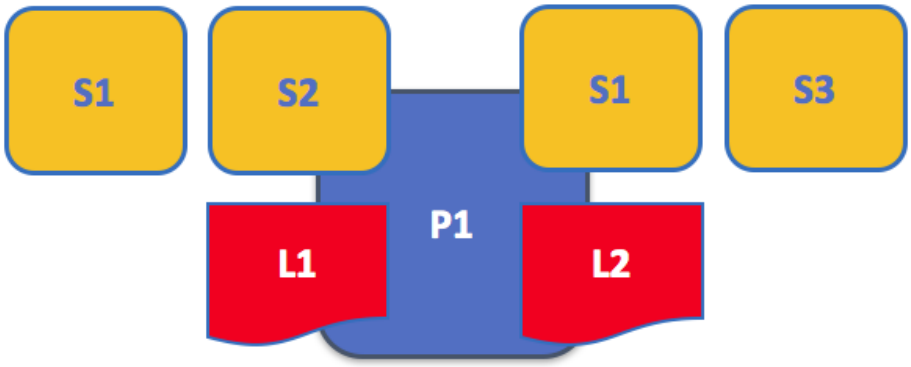
A peer hosting multiple ledgers. Peers host one or more ledgers, and each ledger has zero or more chaincodes that

apply to them. In this example, we can see that the peer P1 hosts ledgers L1 and L2. Ledger L1 is accessed using chaincode S1. Ledger L2 on the other hand can be accessed using chaincodes S1 and S2.

Although it is perfectly possible for a peer to host a ledger instance without hosting any chaincodes which access that ledger, it's rare that peers are configured this way. The vast majority of peers will have at least one chaincode installed on it which can query or update the peer's ledger instances. It's worth mentioning in passing that, whether or not users have installed chaincodes for use by external applications, peers also have special **system chaincodes** that are always present. These are not discussed in detail in this topic.

Multiple Chaincodes

There isn't a fixed relationship between the number of ledgers a peer has and the number of chaincodes that can access that ledger. A peer might have many chaincodes and many ledgers available to it.



An example of a peer hosting multiple chaincodes. Each ledger can have many chaincodes which access it. In this example, we can see that peer P1 hosts ledgers L1 and L2, where L1 is accessed by chaincodes S1 and S2, and L2 is accessed by S1 and S3. We can see that S1 can access both L1 and L2.

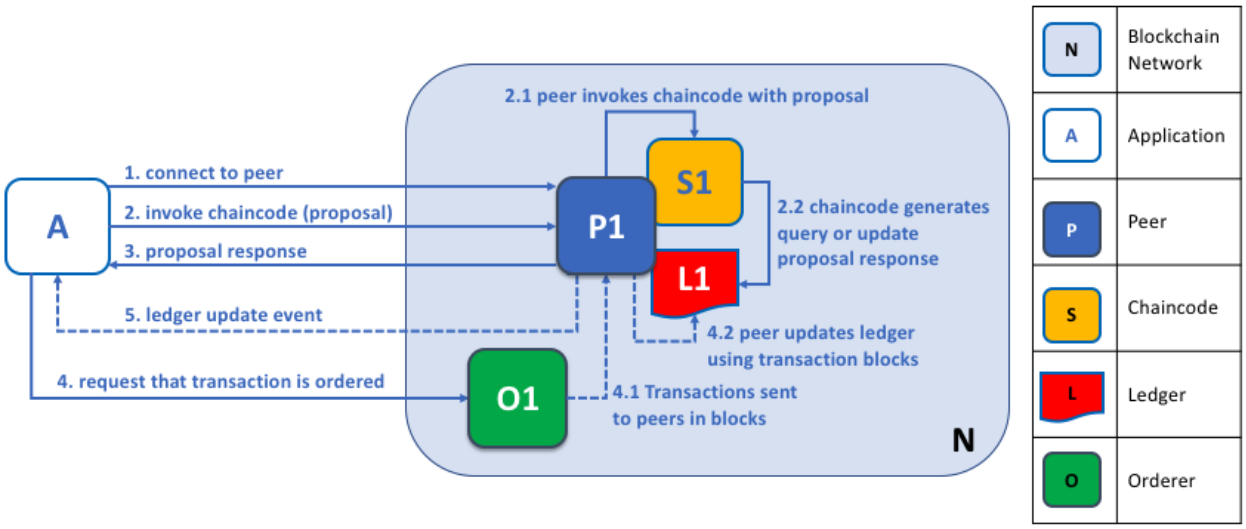
We'll see a little later why the concept of **channels** in Hyperledger Fabric is important when hosting multiple ledgers or multiple chaincodes on a peer.

4.10.3 Applications and Peers

We're now going to show how applications interact with peers to access the ledger. Ledger-query interactions involve a simple three-step dialogue between an application and a peer; ledger-update interactions are a little more involved, and require two extra steps. We've simplified these steps a little to help you get started with Hyperledger Fabric, but don't worry — what's most important to understand is the difference in application-peer interactions for ledger-query compared to ledger-update transaction styles.

Applications always connect to peers when they need to access ledgers and chaincodes. The Hyperledger Fabric Software Development Kit (SDK) makes this easy for programmers — its APIs enable applications to connect to peers, invoke chaincodes to generate transactions, submit transactions to the network that will get ordered and committed to the distributed ledger, and receive events when this process is complete.

Through a peer connection, applications can execute chaincodes to query or update a ledger. The result of a ledger query transaction is returned immediately, whereas ledger updates involve a more complex interaction between applications, peers and orderers. Let's investigate this in a little more detail.



Peers, in conjunction with orderers, ensure that the ledger is kept up-to-date on every peer. In this example, application A connects to P1 and invokes chaincode S1 to query or update the ledger L1. P1 invokes S1 to generate a proposal response that contains a query result or a proposed ledger update. Application A receives the proposal response and, for queries, the process is now complete. For updates, A builds a transaction from all of the responses, which it sends it to O1 for ordering. O1 collects transactions from across the network into blocks, and distributes these to all peers, including P1. P1 validates the transaction before applying to L1. Once L1 is updated, P1 generates an event, received by A, to signify completion.

A peer can return the results of a query to an application immediately since all of the information required to satisfy the query is in the peer's local copy of the ledger. Peers never consult with other peers in order to respond to a query from an application. Applications can, however, connect to one or more peers to issue a query; for example, to corroborate a result between multiple peers, or retrieve a more up-to-date result from a different peer if there's a suspicion that information might be out of date. In the diagram, you can see that ledger query is a simple three-step process.

An update transaction starts in the same way as a query transaction, but has two extra steps. Although ledger-updating applications also connect to peers to invoke a chaincode, unlike with ledger-querying applications, an individual peer cannot perform a ledger update at this time, because other peers must first agree to the change — a process called **consensus**. Therefore, peers return to the application a **proposed** update — one that this peer would apply subject to other peers' prior agreement. The first extra step — step four — requires that applications send an appropriate set of matching proposed updates to the entire network of peers as a transaction for commitment to their respective ledgers. This is achieved by the application using an **orderer** to package transactions into blocks, and distribute them to the entire network of peers, where they can be verified before being applied to each peer's local copy of the ledger. As this whole ordering processing takes some time to complete (seconds), the application is notified asynchronously, as shown in step five.

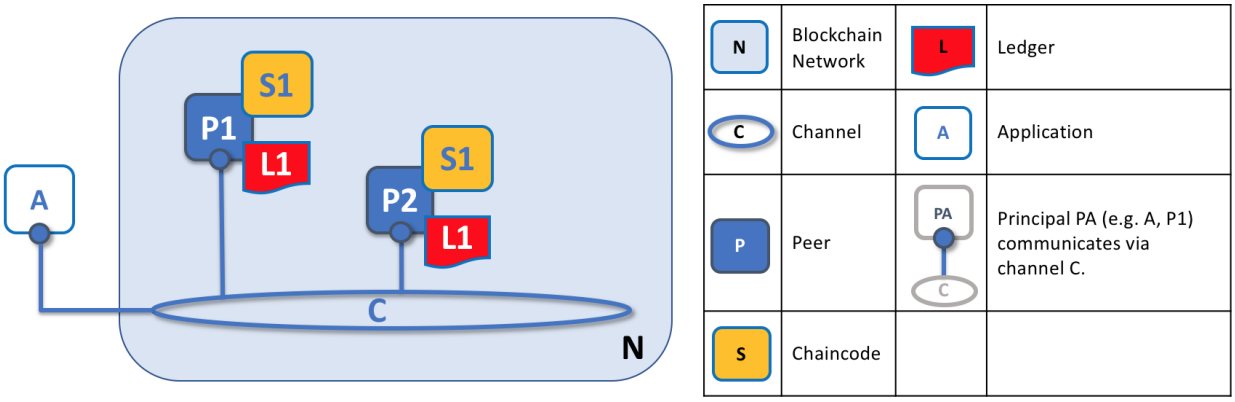
Later in this section, you'll learn more about the detailed nature of this ordering process — and for a really detailed look at this process see the Transaction Flow topic.

4.10.4 Peers and Channels

Although this section is about peers rather than channels, it's worth spending a little time understanding how peers interact with each other, and with applications, via *channels* — a mechanism by which a set of components within a blockchain network can communicate and transact *privately*.

These components are typically peer nodes, orderer nodes and applications and, by joining a channel, they agree to collaborate to collectively share and manage identical copies of the ledger associated with that channel. Conceptually, you can think of channels as being similar to groups of friends (though the members of a channel certainly don't need

to be friends!). A person might have several groups of friends, with each group having activities they do together. These groups might be totally separate (a group of work friends as compared to a group of hobby friends), or there can be some crossover between them. Nevertheless, each group is its own entity, with "rules" of a kind.



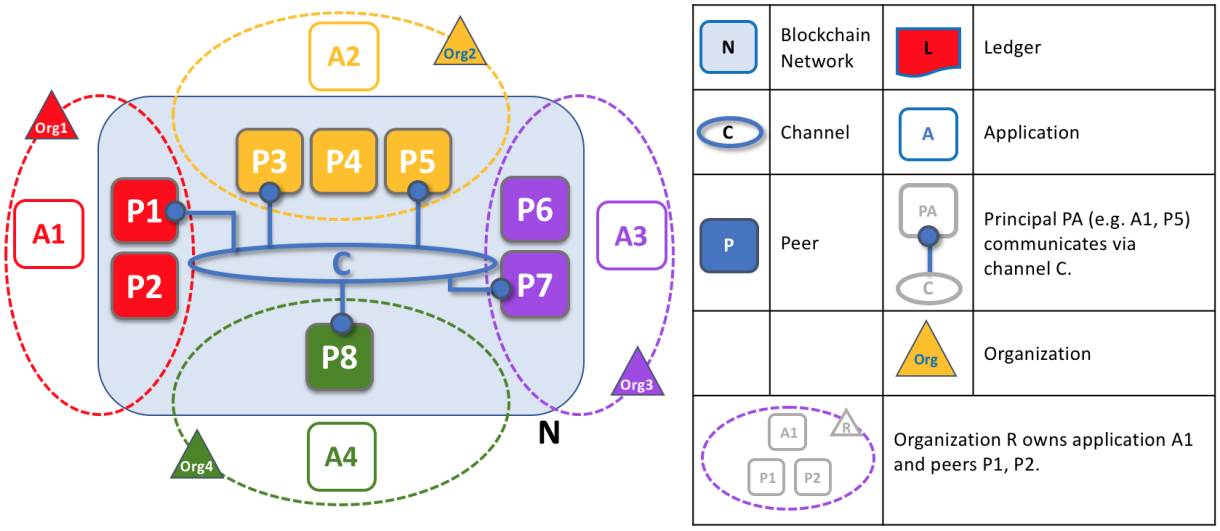
Channels allow a specific set of peers and applications to communicate with each other within a blockchain network. In this example, application A can communicate directly with peers P1 and P2 using channel C. You can think of the channel as a pathway for communications between particular applications and peers. (For simplicity, orderers are not shown in this diagram, but must be present in a functioning network.)

We see that channels don't exist in the same way that peers do — it's more appropriate to think of a channel as a logical structure that is formed by a collection of physical peers. *It is vital to understand this point — peers provide the control point for access to, and management of, channels.*

4.10.5 Peers and Organizations

Now that you understand peers and their relationship to ledgers, chaincodes and channels, you'll be able to see how multiple organizations come together to form a blockchain network.

Blockchain networks are administered by a collection of organizations rather than a single organization. Peers are central to how this kind of distributed network is built because they are owned by — and are the connection points to the network for — these organizations.



Peers in a blockchain network with multiple organizations. The blockchain network is built up from the peers owned and contributed by the different organizations. In this example, we see four organizations contributing eight peers to form a network. The channel C connects five of these peers in the network N — P1, P3, P5, P7 and P8. The other peers owned by these organizations have not been joined to this channel, but are typically joined to at least one other channel. Applications that have been developed by a particular organization will connect to their own organization's peers as well as those of different organizations. Again, for simplicity, an orderer node is not shown in this diagram.

It's really important that you can see what's happening in the formation of a blockchain network. *The network is both formed and managed by the multiple organizations who contribute resources to it.* Peers are the resources that we're discussing in this topic, but the resources an organization provides are more than just peers. There's a principle at work here — the network literally does not exist without organizations contributing their individual resources to the collective network. Moreover, the network grows and shrinks with the resources that are provided by these collaborating organizations.

You can see that (other than the ordering service) there are no centralized resources — in the *example above*, the network, **N**, would not exist if the organizations did not contribute their peers. This reflects the fact that the network does not exist in any meaningful sense unless and until organizations contribute the resources that form it. Moreover, the network does not depend on any individual organization — it will continue to exist as long as one organization remains, no matter which other organizations may come and go. This is at the heart of what it means for a network to be decentralized.

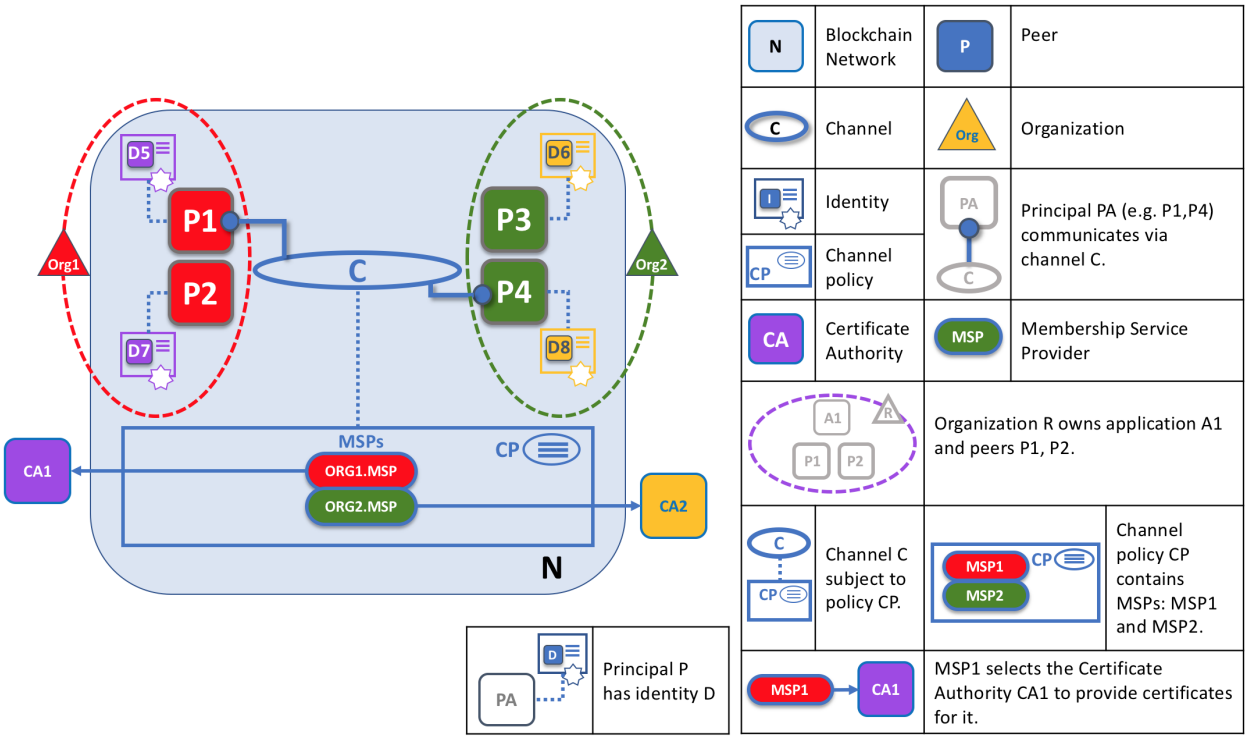
Applications in different organizations, as in the *example above*, may or may not be the same. That's because it's entirely up to an organization as to how its applications process their peers' copies of the ledger. This means that both application and presentation logic may vary from organization to organization even though their respective peers host exactly the same ledger data.

Applications connect either to peers in their organization, or peers in another organization, depending on the nature of the ledger interaction that's required. For ledger-query interactions, applications typically connect to their own organization's peers. For ledger-update interactions, we'll see later why applications need to connect to peers representing *every* organization that is required to endorse the ledger update.

4.10.6 Peers and Identity

Now that you've seen how peers from different organizations come together to form a blockchain network, it's worth spending a few moments understanding how peers get assigned to organizations by their administrators.

Peers have an identity assigned to them via a digital certificate from a particular certificate authority. You can read lots more about how X.509 digital certificates work elsewhere in this guide but, for now, think of a digital certificate as being like an ID card that provides lots of verifiable information about a peer. *Each and every peer in the network is assigned a digital certificate by an administrator from its owning organization*.



When a peer connects to a channel, its digital certificate identifies its owning organization via a channel MSP. In this example, P1 and P2 have identities issued by CA1. Channel C determines from a policy in its channel configuration that identities from CA1 should be associated with Org1 using ORG1.MSP. Similarly, P3 and P4 are identified by ORG2.MSP as being part of Org2.

Whenever a peer connects using a channel to a blockchain network, *a policy in the channel configuration uses the peer's identity to determine its rights.* The mapping of identity to organization is provided by a component called a *Membership Service Provider* (MSP) — it determines how a peer gets assigned to a specific role in a particular organization and accordingly gains appropriate access to blockchain resources. Moreover, a peer can be owned only by a single organization, and is therefore associated with a single MSP. We'll learn more about peer access control later in this section, and there's an entire section on MSPs and access control policies elsewhere in this guide. But for now, think of an MSP as providing linkage between an individual identity and a particular organizational role in a blockchain network.

To digress for a moment, peers as well as *everything that interacts with a blockchain network acquire their organizational identity from their digital certificate and an MSP*. Peers, applications, end users, administrators and orderers must have an identity and an associated MSP if they want to interact with a blockchain network. *We give a name to every entity that interacts with a blockchain network using an identity — a principal.* You can learn lots more about principals and organizations elsewhere in this guide, but for now you know more than enough to continue your understanding of peers!

Finally, note that it's not really important where the peer is physically located — it could reside in the cloud, or in a data centre owned by one of the organizations, or on a local machine — it's the identity associated with it that identifies it as being owned by a particular organization. In our example above, P3 could be hosted in Org1's data center, but as long as the digital certificate associated with it is issued by CA2, then it's owned by Org2.

4.10.7 Peers and Orderers

We've seen that peers form the basis for a blockchain network, hosting ledgers and chaincode which can be queried and updated by peer-connected applications. However, the mechanism by which applications and peers interact with

each other to ensure that every peer's ledger is kept consistent is mediated by special nodes called *orderers*, and it's to these nodes we now turn our attention.

An update transaction is quite different from a query transaction because a single peer cannot, on its own, update the ledger — updating requires the consent of other peers in the network. A peer requires other peers in the network to approve a ledger update before it can be applied to a peer's local ledger. This process is called *consensus*, which takes much longer to complete than a simple query. But when all the peers required to approve the transaction do so, and the transaction is committed to the ledger, peers will notify their connected applications that the ledger has been updated. You're about to be shown a lot more detail about how peers and orderers manage the consensus process in this section.

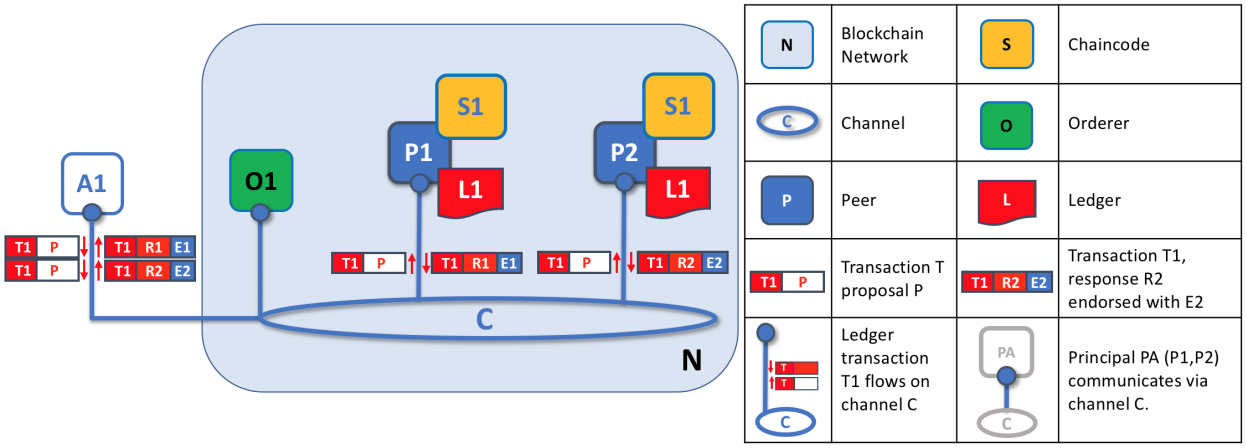
Specifically, applications that want to update the ledger are involved in a 3-phase process, which ensures that all the peers in a blockchain network keep their ledgers consistent with each other. In the first phase, applications work with a subset of *endorsing peers*, each of which provide an endorsement of the proposed ledger update to the application, but do not apply the proposed update to their copy of the ledger. In the second phase, these separate endorsements are collected together as transactions and packaged into blocks. In the final phase, these blocks are distributed back to every peer where each transaction is validated before being applied to that peer's copy of the ledger.

As you will see, orderer nodes are central to this process, so let's investigate in a little more detail how applications and peers use orderers to generate ledger updates that can be consistently applied to a distributed, replicated ledger.

Phase 1: Proposal

Phase 1 of the transaction workflow involves an interaction between an application and a set of peers — it does not involve orderers. Phase 1 is only concerned with an application asking different organizations' endorsing peers to agree to the results of the proposed chaincode invocation.

To start phase 1, applications generate a transaction proposal which they send to each of the required set of peers for endorsement. Each of these *endorsing peers* then independently executes a chaincode using the transaction proposal to generate a transaction proposal response. It does not apply this update to the ledger, but rather simply signs it and returns it to the application. Once the application has received a sufficient number of signed proposal responses, the first phase of the transaction flow is complete. Let's examine this phase in a little more detail.



Transaction proposals are independently executed by peers who return endorsed proposal responses. In this example, application A1 generates transaction T1 proposal P which it sends to both peer P1 and peer P2 on channel C. P1 executes S1 using transaction T1 proposal P generating transaction T1 response R1 which it endorses with E1. Independently, P2 executes S1 using transaction T1 proposal P generating transaction T1 response R2 which it endorses with E2. Application A1 receives two endorsed responses for transaction T1, namely E1 and E2.

Initially, a set of peers are chosen by the application to generate a set of proposed ledger updates. Which peers are chosen by the application? Well, that depends on the *endorsement policy* (defined for a chaincode), which defines the set of organizations that need to endorse a proposed ledger change before it can be accepted by the network. This

is literally what it means to achieve consensus — every organization who matters must have endorsed the proposed ledger change *before* it will be accepted onto any peer's ledger.

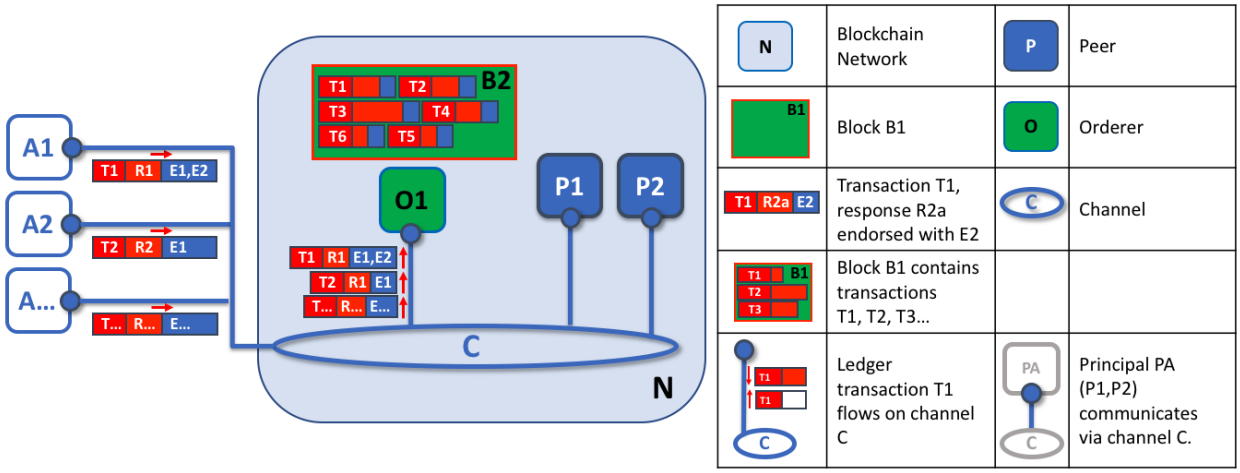
A peer endorses a proposal response by adding its digital signature, and signing the entire payload using its private key. This endorsement can be subsequently used to prove that this organization's peer generated a particular response. In our example, if peer P1 is owned by organization Org1, endorsement E1 corresponds to a digital proof that "Transaction T1 response R1 on ledger L1 has been provided by Org1's peer P1!".

Phase 1 ends when the application receives signed proposal responses from sufficient peers. We note that different peers can return different and therefore inconsistent transaction responses to the application *for the same transaction proposal*. It might simply be that the result was generated at different times on different peers with ledgers at different states, in which case an application can simply request a more up-to-date proposal response. Less likely, but much more seriously, results might be different because the chaincode is *non-deterministic*. Non-determinism is the enemy of chaincodes and ledgers and if it occurs it indicates a serious problem with the proposed transaction, as inconsistent results cannot, obviously, be applied to ledgers. An individual peer cannot know that their transaction result is non-deterministic — transaction responses must be gathered together for comparison before non-determinism can be detected. (Strictly speaking, even this is not enough, but we defer this discussion to the transaction section, where non-determinism is discussed in detail.)

At the end of phase 1, the application is free to discard inconsistent transaction responses if it wishes to do so, effectively terminating the transaction workflow early. We'll see later that if an application tries to use an inconsistent set of transaction responses to update the ledger, it will be rejected.

Phase 2: Packaging

The second phase of the transaction workflow is the packaging phase. The orderer is pivotal to this process — it receives transactions containing endorsed transaction proposal responses from many applications. It orders each transaction relative to other transactions, and packages batches of transactions into blocks ready for distribution back to all peers connected to the orderer, including the original endorsing peers.



The first role of an orderer node is to package proposed ledger updates. In this example, application A1 sends a transaction T1 endorsed by E1 and E2 to the orderer O1. In parallel, Application A2 sends transaction T2 endorsed by E1 to the orderer O1. O1 packages transaction T1 from application A1 and transaction T2 from application A2 together with other transactions from other applications in the network into block B2. We can see that in B2, the transaction order is T1,T2,T3,T4,T6,T5 – which may not be the order in which these transactions arrived at the orderer node! (This example shows a very simplified orderer configuration.)

An orderer receives proposed ledger updates concurrently from many different applications in the network on a particular channel. Its job is to arrange these proposed updates into a well-defined sequence, and package them into *blocks*

for subsequent distribution. These blocks will become the *blocks* of the blockchain! Once an orderer has generated a block of the desired size, or after a maximum elapsed time, it will be sent to all peers connected to it on a particular channel. We'll see how this block is processed in phase 3.

It's worth noting that the sequencing of transactions in a block is not necessarily the same as the order of arrival of transactions at the orderer! Transactions can be packaged in any order into a block, and it's this sequence that becomes the order of execution. What's important is that there **is** a strict order, rather than **what** that order is.

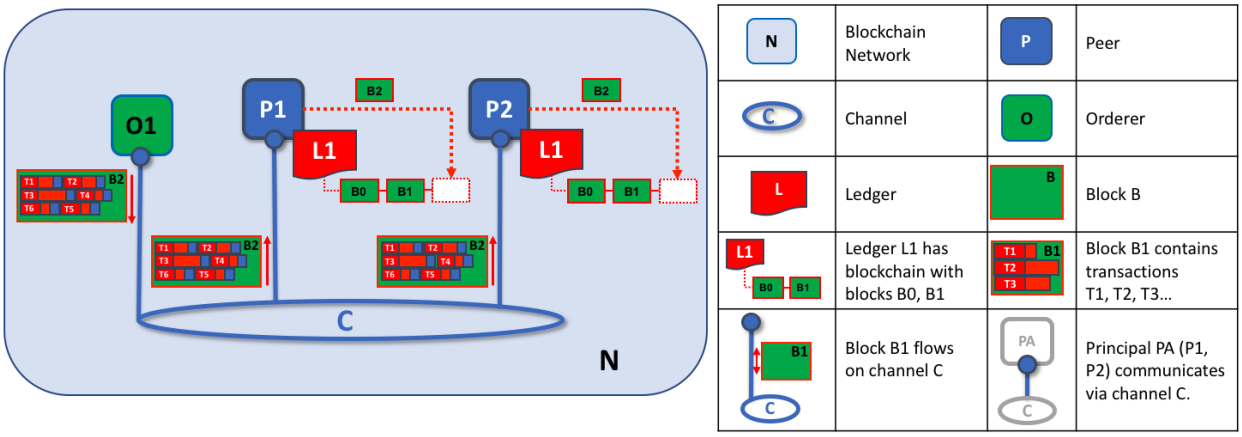
This strict ordering of transactions within blocks makes Hyperledger Fabric a little different from other blockchains where the same transaction can be packaged into multiple different blocks. In Hyperledger Fabric, this cannot happen — the blocks generated by a collection of orderers are said to be **final** because once a transaction has been written to a block, its position in the ledger is immutably assured. Hyperledger Fabric's finality means that a disastrous occurrence known as a **ledger fork** cannot occur. Once transactions are captured in a block, history cannot be rewritten for that transaction at a future point in time.

We can see also see that, whereas peers host the ledger and chaincodes, orderers most definitely do not. Every transaction that arrives at an orderer is mechanically packaged in a block — the orderer makes no judgement as to the value of a transaction, it simply packages it. That's an important property of Hyperledger Fabric — all transactions are marshalled into a strict order — transactions are never dropped or de-prioritized.

At the end of phase 2, we see that orderers have been responsible for the simple but vital processes of collecting proposed transaction updates, ordering them, packaging them into blocks, ready for distribution.

Phase 3: Validation

The final phase of the transaction workflow involves the distribution and subsequent validation of blocks from the orderer to the peers, where they can be applied to the ledger. Specifically, at each peer, every transaction within a block is validated to ensure that it has been consistently endorsed by all relevant organizations before it is applied to the ledger. Failed transactions are retained for audit, but are not applied to the ledger.



The second role of an orderer node is to distribute blocks to peers. In this example, orderer O1 distributes block B2 to peer P1 and peer P2. Peer P1 processes block B2, resulting in a new block being added to ledger L1 on P1. In parallel, peer P2 processes block B2, resulting in a new block being added to ledger L1 on P2. Once this process is complete, the ledger L1 has been consistently updated on peers P1 and P2, and each may inform connected applications that the transaction has been processed.

Phase 3 begins with the orderer distributing blocks to all peers connected to it. Peers are connected to orderers on channels such that when a new block is generated, all of the peers connected to the orderer will be sent a copy of the new block. Each peer will process this block independently, but in exactly the same way as every other peer on the channel. In this way, we'll see that the ledger can be kept consistent. It's also worth noting that not every peer needs to

be connected to an orderer — peers can cascade blocks to other peers using the **gossip** protocol, who also can process them independently. But let's leave that discussion to another time!

Upon receipt of a block, a peer will process each transaction in the sequence in which it appears in the block. For every transaction, each peer will verify that the transaction has been endorsed by the required organizations according to the *endorsement policy* of the chaincode which generated the transaction. For example, some transactions may only need to be endorsed by a single organization, whereas others may require multiple endorsements before they are considered valid. This process of validation verifies that all relevant organizations have generated the same outcome or result. Also note that this validation is different than the endorsement check in phase 1, where it is the application that receives the response from endorsing peers and makes the decision to send the proposal transactions. In case the application violates the endorsement policy by sending wrong transactions, the peer is still able to reject the transaction in the validation process of phase 3.

If a transaction has been endorsed correctly, the peer will attempt to apply it to the ledger. To do this, a peer must perform a ledger consistency check to verify that the current state of the ledger is compatible with the state of the ledger when the proposed update was generated. This may not always be possible, even when the transaction has been fully endorsed. For example, another transaction may have updated the same asset in the ledger such that the transaction update is no longer valid and therefore can no longer be applied. In this way each peer's copy of the ledger is kept consistent across the network because they each follow the same rules for validation.

After a peer has successfully validated each individual transaction, it updates the ledger. Failed transactions are not applied to the ledger, but they are retained for audit purposes, as are successful transactions. This means that peer blocks are almost exactly the same as the blocks received from the orderer, except for a valid or invalid indicator on each transaction in the block.

We also note that phase 3 does not require the running of chaincodes — this is done only during phase 1, and that's important. It means that chaincodes only have to be available on endorsing nodes, rather than throughout the blockchain network. This is often helpful as it keeps the logic of the chaincode confidential to endorsing organizations. This is in contrast to the output of the chaincodes (the transaction proposal responses) which are shared with every peer in the channel, whether or not they endorsed the transaction. This specialization of endorsing peers is designed to help scalability.

Finally, every time a block is committed to a peer's ledger, that peer generates an appropriate *event*. *Block events* include the full block content, while *block transaction events* include summary information only, such as whether each transaction in the block has been validated or invalidated. *Chaincode* events that the chaincode execution has produced can also be published at this time. Applications can register for these event types so that they can be notified when they occur. These notifications conclude the third and final phase of the transaction workflow.

In summary, phase 3 sees the blocks which are generated by the orderer consistently applied to the ledger. The strict ordering of transactions into blocks allows each peer to validate that transaction updates are consistently applied across the blockchain network.

Orderers and Consensus

This entire transaction workflow process is called *consensus* because all peers have reached agreement on the order and content of transactions, in a process that is mediated by orderers. Consensus is a multi-step process and applications are only notified of ledger updates when the process is complete — which may happen at slightly different times on different peers.

We will discuss orderers in a lot more detail in a future orderer topic, but for now, think of orderers as nodes which collect and distribute proposed ledger updates from applications for peers to validate and include on the ledger.

That's it! We've now finished our tour of peers and the other components that they relate to in Hyperledger Fabric. We've seen that peers are in many ways the most fundamental element — they form the network, host chaincodes and the ledger, handle transaction proposals and responses, and keep the ledger up-to-date by consistently applying transaction updates to it.

4.11 Private data

4.11.1 What is private data?

In cases where a group of organizations on a channel need to keep data private from other organizations on that channel, they have the option to create a new channel comprising just the organizations who need access to the data. However, creating separate channels in each of these cases creates additional administrative overhead (maintaining chaincode versions, policies, MSPs, etc), and doesn't allow for use cases in which you want all channel participants to see a transaction while keeping a portion of the data private.

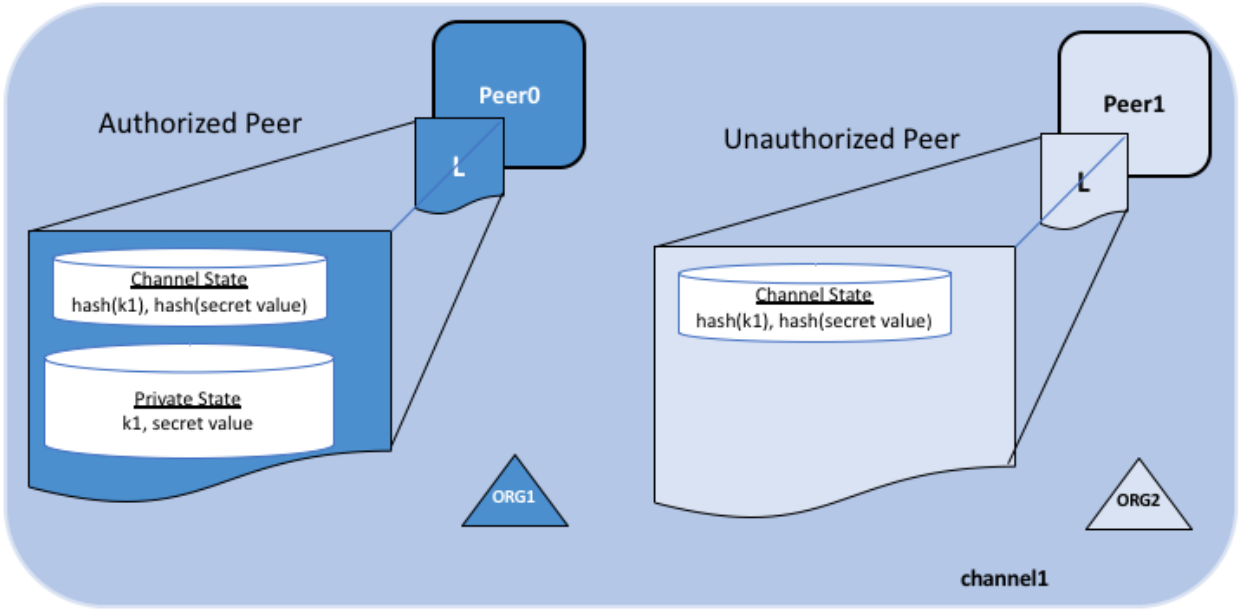
That's why, starting in v1.2, Fabric offers the ability to create **private data collections**, which allow a defined subset of organizations on a channel the ability to endorse, commit, or query private data without having to create a separate channel.

4.11.2 What is a private data collection?

A collection is the combination of two elements:

1. **The actual private data**, sent peer-to-peer via gossip protocol to only the organization(s) authorized to see it. This data is stored in a private database on the peer (sometimes called a "side" database, or "SideDB"). The ordering service is not involved here and does not see the private data. Note that setting up gossip requires setting up anchor peers in order to bootstrap cross-organization communication.
2. **A hash of that data**, which is endorsed, ordered, and written to the ledgers of every peer on the channel. The hash serves as evidence of the transaction and is used for state validation and can be used for audit purposes.

The following diagram illustrates the ledger contents of a peer authorized to have private data and one which is not.



Collection members may decide to share the private data with other parties if they get into a dispute or if they want to transfer the asset to a third party. The third party can then compute the hash of the private data and see if it matches the state on the channel ledger, proving that the state existed between the collection members at a certain point in time.

When to use a collection within a channel vs. a separate channel

- Use **channels** when entire transactions (and ledgers) must be kept confidential within a set of organizations that are members of the channel.
- Use **collections** when transactions (and ledgers) must be shared among a set of organizations, but when only a subset of those organizations should have access to some (or all) of the data within a transaction. Additionally, since private data is disseminated peer-to-peer rather than via blocks, use private data collections when transaction data must be kept confidential from ordering service nodes.

4.11.3 Transaction flow with private data

When private data collections are referenced in chaincode, the transaction flow is slightly different in order to protect the confidentiality of the private data as transactions are proposed, endorsed, and committed to the ledger.

For details on transaction flows that don't use private data refer to our documentation on transaction flow.

1. The client application submits a proposal request to invoke a chaincode function (reading or writing private data) to endorsing peers which are part of authorized organizations of the collection. The private data, or data used to generate private data in chaincode, is sent in a `transient` field of the proposal.
2. The endorsing peers simulate the transaction and store the private data in a `transient data store` (a temporary storage local to the peer). They distribute the private data, based on the collection policy, to authorized peers via gossip.
3. The endorsing peer sends the proposal response back to the client with public data, including a hash of the private data key and value. *No private data is sent back to the client*. For more information on how endorsement works with private data, click here.
4. The client application submits the transaction to the ordering service (with hashes of the private data) which gets distributed into blocks as normal. The block with the hashed values is distributed to all the peers. In this way, all peers on the channel can validate transactions with the hashes of the private data in a consistent way, without knowing the actual private data.
5. At block-committal time, authorized peers use the collection policy to determine if they are authorized to have access to the private data. If they do, they will first check their local `transient data store` to determine if they have already received the private data at chaincode endorsement time. If not, they will attempt to pull the private data from another peer. Then they will validate the private data against the hashes in the public block and commit the transaction and the block. Upon validation/commit, the private data is moved to their copy of the private state database and private writeset storage. The private data is then deleted from the `transient data store`.

A use case to explain collections

Consider a group of five organizations on a channel who trade produce:

- **A Farmer** selling his goods abroad
- **A Distributor** moving goods abroad
- **A Shipper** moving goods between parties
- **A Wholesaler** purchasing goods from distributors
- **A Retailer** purchasing goods from shippers and wholesalers

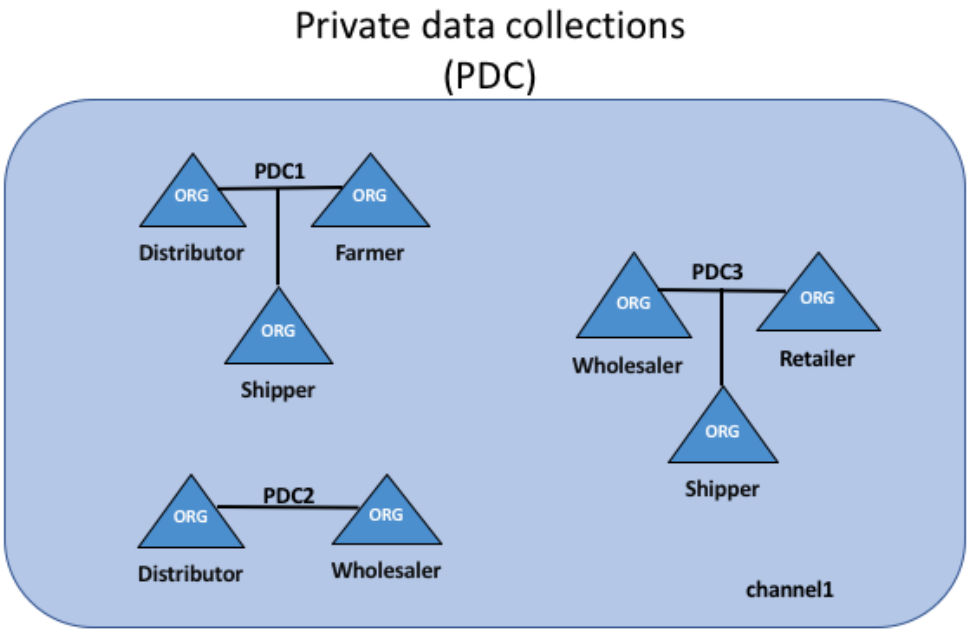
The **Distributor** might want to make private transactions with the **Farmer** and **Shipper** to keep the terms of the trades confidential from the **Wholesaler** and the **Retailer** (so as not to expose the markup they're charging).

The **Distributor** may also want to have a separate private data relationship with the **Wholesaler** because it charges them a lower price than it does the **Retailer**.

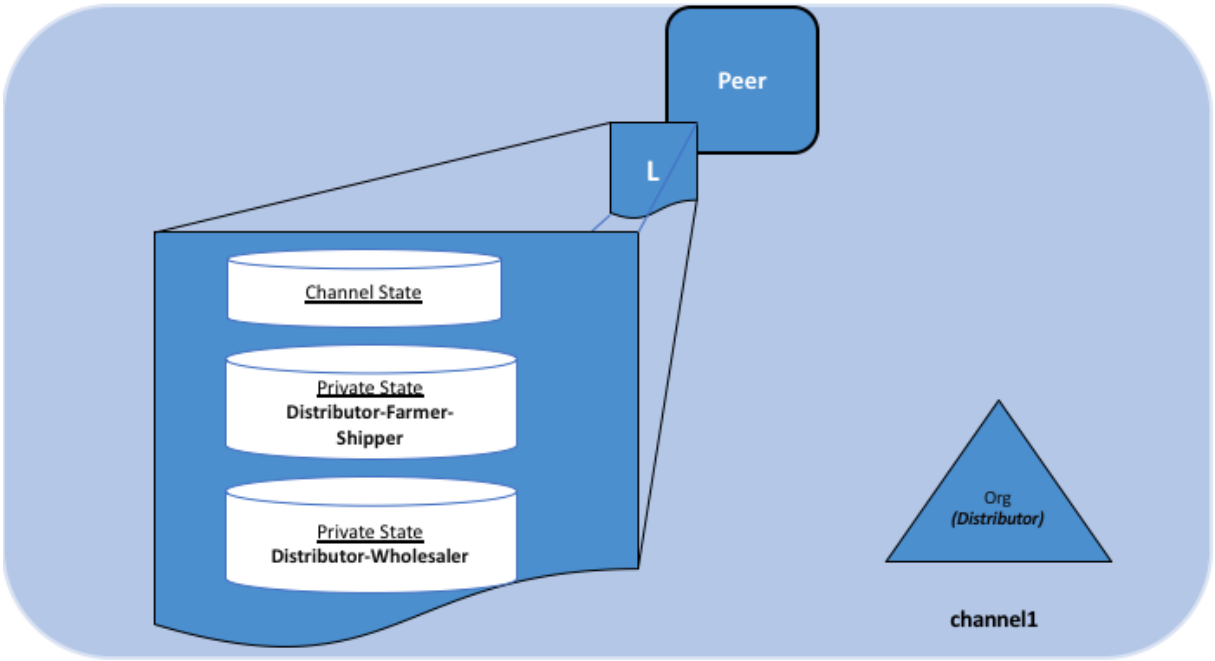
The **Wholesaler** may also want to have a private data relationship with the **Retailer** and the **Shipper**.

Rather than defining many small channels for each of these relationships, multiple private data collections **(PDC)** can be defined to share private data between:

1. PDC1: **Distributor**, **Farmer** and **Shipper**
2. PDC2: **Distributor** and **Wholesaler**
3. PDC3: **Wholesaler**, **Retailer** and **Shipper**



Using this example, peers owned by the **Distributor** will have multiple private databases inside their ledger which includes the private data from the **Distributor**, **Farmer** and **Shipper** relationship and the **Distributor** and **Wholesaler** relationship. Because these databases are kept separate from the database that holds the channel ledger, private data is sometimes referred to as "SideDB".



4.11.4 How a private data collection is defined

For more details on collection definitions, and other low level information about private data and collections, refer to the private data reference topic.

4.11.5 Purging data

For very sensitive data, even the parties sharing the private data might want — or might be required by government regulations — to "purge" the data stored on their peers after a set amount of time, leaving behind only a hash of the data to serve as immutable evidence of the transaction.

In some of these cases, the private data only needs to exist on the peer's private database until it can be replicated into a database external to the blockchain network. The data might also only need to exist on the peers until a chaincode business process is done with it (trade settled, contract fulfilled, etc). To support the later use case, it is possible to purge private data if it has not been modified once a set number of subsequent blocks have been added to the private database.

4.12 Ledger

4.12.1 What is a Ledger?

A ledger contains the current state of a business as a journal of transactions. The earliest European and Chinese ledgers date from almost 1000 years ago, and the Sumerians had stone ledgers 4000 years ago – but let's start with a more up-to-date example!

You're probably used to looking at your bank account every month. What's most important to you is the available balance – it's what you're able to spend at the current moment in time. If you want to see how your balance was derived, then you can look through the transaction credits and debits that determined it. This is a real life example

of a ledger – a state (your bank balance), and a set of ordered transactions (credits and debits) that determine it. Hyperledger Fabric is motivated by these same two concerns – to present the current value of a set of ledger states, and to capture the history of the transactions that determined these states.

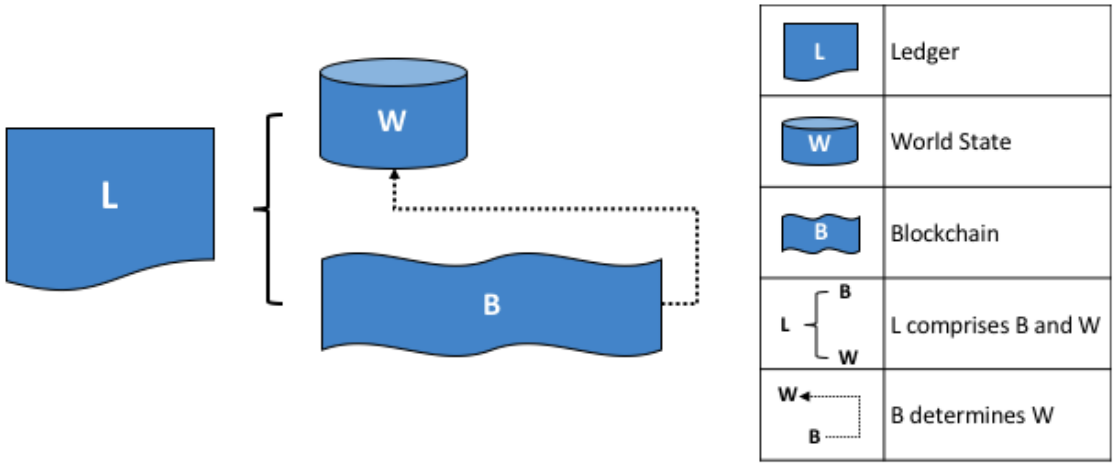
Let's take a closer look at the Hyperledger Fabric ledger structure!

4.12.2 A Blockchain Ledger

A blockchain ledger consists of two distinct, though related, parts – a world state and a blockchain.

Firstly, there's a **world state** – a database that holds the **current values** of a set of ledger states. The world state makes it easy for a program to get the current value of these states, rather than having to calculate them by traversing the entire transaction log. Ledger states are, by default, expressed as **key-value** pairs, though we'll see later that Hyperledger Fabric provides flexibility in this regard. The world state can change frequently, as states can be created, updated and deleted.

Secondly, there's a **blockchain** – a transaction log that records all the changes that determine the world state. Transactions are collected inside blocks that are appended to the blockchain – enabling you to understand the history of changes that have resulted in the current world state. The blockchain data structure is very different to the world state because once written, it cannot be modified. It is an **immutable** sequence of blocks, each of which contains a set of ordered transactions.



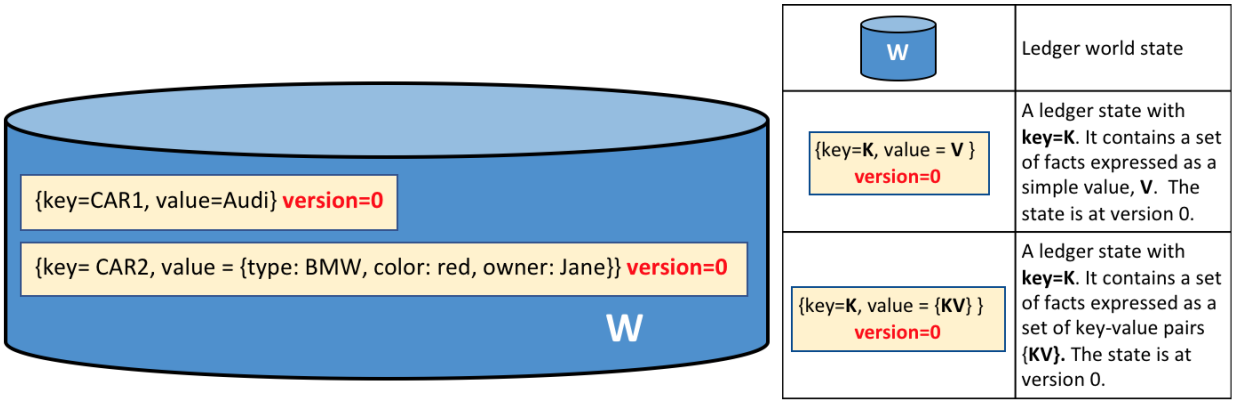
The visual vocabulary expressed in facts is as follows: Ledger L comprises blockchain B and World State W. Blockchain B determines World State W. Also expressed as: World state W is derived from blockchain B.

It's helpful to think of there being one **logical** ledger in a Hyperledger Fabric network. In reality, the network maintains multiple copies of a ledger – which are kept consistent with every other copy through a process called **consensus**. The term **Distributed Ledger Technology** (**DLT**) is often associated with this kind of ledger – one that is logically singular, but has many consistent copies distributed throughout a network.

Let's now examine the world state and blockchain data structures in more detail.

4.12.3 World State

The world state represents the current values of all ledger states. It's extremely useful because programs usually need the current value of a ledger state and that's always easily available. You do not need to traverse the entire blockchain to calculate the current value of any ledger state – you just get it directly from the world state.



The visual vocabulary expressed in facts is as follows: There is a ledger state with key=CAR1 and value=Audi. There is a ledger state with key=CAR2 and a more complex value {model:BMW, color=red, owner=Jane}. Both states are at version 0.

Ledger state is used to record application information to be shared via the blockchain. The example above shows ledger states for two cars, CAR1 and CAR2. You can see that states have a key and a value. Your application programs invoke chaincode which access states via simple APIs – they **get**, **put** and **delete** states using a state key. Notice how a state value can be simple (Audi. . .) or complex (type:BMW. . .).

Physically, the world state is implemented as a database. This makes a lot of sense because a database provides a rich set of operators for the efficient storage and retrieval of states. We'll see later that Hyperledger Fabric can be configured to use different world state databases to address the needs of different types of state values and the access patterns required by applications, for example in complex queries.

Transactions capture changes to the world state, and as you'd expect, transactions have a lifecycle. They are created by applications, and finally end up being committed to the ledger blockchain. The whole lifecycle is described in detail here; but the key design point for Hyperledger Fabric is that only transactions that are **signed** by a set of **endorsing organizations** will result in an update to the world state. If a transaction is not signed by sufficient endorsers, then it will fail this validity check, and will not result in an update to the world state.

You'll also notice that a state has a version number, and in the diagram above, states CAR1 and CAR2 are at their starting versions, 0. The version number of a state is incremented every time the state changes. It is also checked whenever the state is updated – to make sure it matches the version when the transaction was created. This check ensures that the world state changing **from the same expected value to the same expected value** as when the transaction was created.

Finally, when a ledger is first created, the world state is empty. Because any transaction which represents a valid change to world state is recorded on the blockchain, it means that the world state can be re-generated from the blockchain at any time. This can be very convenient – for example, the world state is automatically generated when a peer is created. Moreover, if a peer fails abnormally, the world state can be regenerated on peer restart, before transactions are accepted.

4.12.4 Blockchain

Let's now turn our attention from the ledger world state to the ledger blockchain.

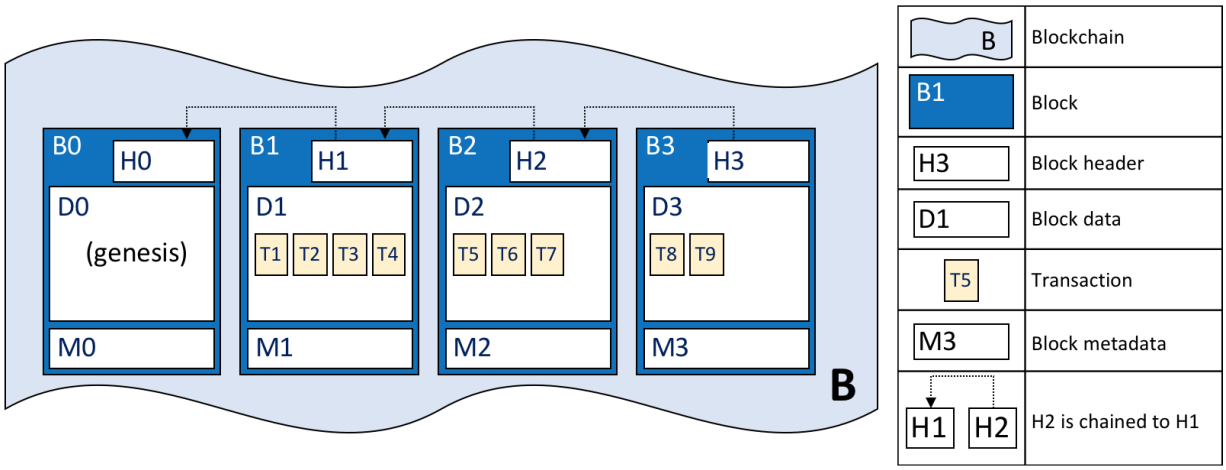
The blockchain is a transaction log, structured as interlinked blocks, where each block contains a sequence of transactions, each of which represents a query or update to the world state. The exact mechanism by which transactions are

ordered is discussed elsewhere – what's important is that block sequencing, as well as transaction sequencing within blocks, is established when blocks are first created.

Each block's header includes a hash of the block's transactions, as well a copy of the hash of the prior block's header. In this way, all transactions on the ledger are sequenced and cryptographically linked together. This hashing and linking makes the ledger data very secure. Even if one node hosting the ledger was tampered with, it would not be able to convince all the other nodes that it has the 'correct' blockchain because the ledger is distributed throughout a network of independent nodes.

Physically, the blockchain is always implemented as a file, in contrast to the world state, which uses a database. This is a sensible design choice as the blockchain data structure is heavily biased towards a very small set of simple operations. Appending to the end of the blockchain is the primary operation, and query is currently a relatively infrequent operation.

Let's have a look at the structure of a blockchain in a little more detail.



The visual vocabulary expressed in facts is as follows: Blockchain B contains blocks B0, B1, B2, B3. B0 is the first block in the blockchain, the genesis block

In the above diagram, we can see that **block** B2 has a **block data** D2 which contains all its transactions: T5, T6, T7.

Most importantly, B2 has a **block header** H2, which contains a cryptographic **hash** of all the transactions in D2 as well as with the equivalent hash from the previous block B1. In this way, blocks are inextricably and immutably linked to each other, which the term **blockchain** so neatly captures!

Finally, as you can see in the diagram, the first block in the blockchain is called the **genesis block**. It's the starting point for the ledger, though it does not contain any user transactions. Instead, it contains a configuration transaction containing the initial state of the network channel (not shown). We discuss the genesis block in more detail when we discuss the blockchain network and channels in the documentation.

4.12.5 Blocks

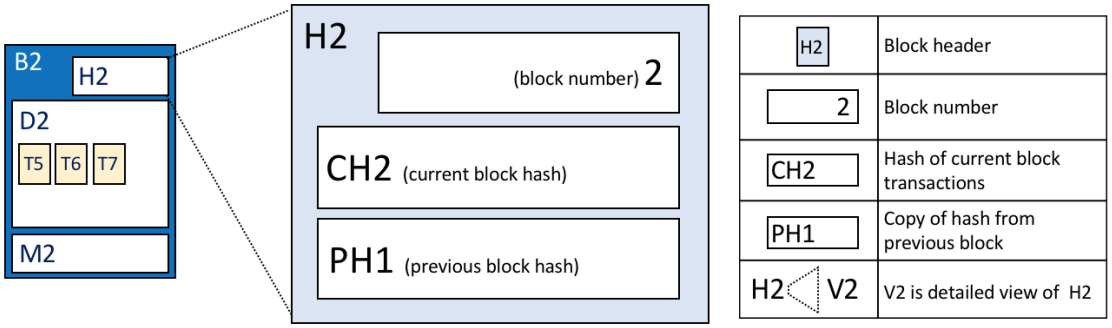
Let's have a closer look at the structure of a block. It consists of three sections

- **Block Header**

  This section comprises three fields, written when a block is created.

  – **Block number**: An integer starting at 0 (the genesis block), and increased by 1 for every new block appended to the blockchain.

- **Current Block Hash**: The hash of all the transactions contained in the current block.
- **Previous Block Hash**: A copy of the hash from the previous block in the blockchain.



The visual vocabulary expressed in facts is as follows: Block header H2 of block B2 consists of block number 2, the hash CH2 of the current block data D2, and a copy of a hash PH1 from the previous block, block number 1.

- **Block Data**

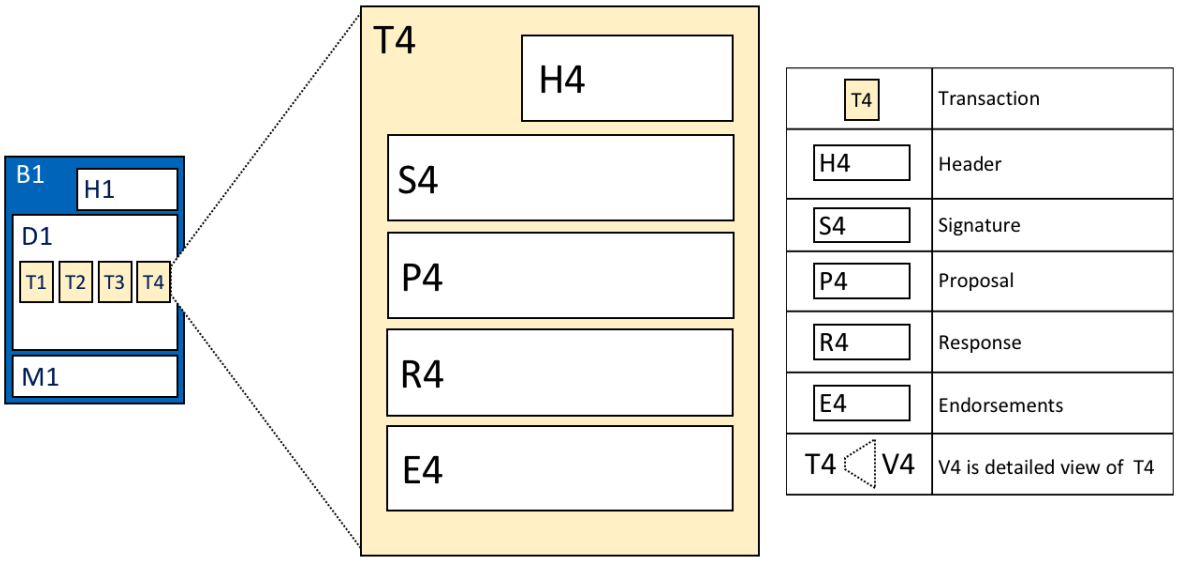
  This section contains a list of transactions arranged in order. It is written when the block is created. These transactions have a rich but straightforward structure, which we describe *later* in this topic.

- **Block Metadata**

  This section contains the time when the block was written, as well as the certificate, public key and signature of the block writer. Subsequently, the block committer also adds a valid/invalid indicator for every transaction, though this information is not included in the hash, as that is created when the block is created.

4.12.6 Transactions

As we've seen, a transaction captures changes to the world state. Let's have a look at the detailed **blockdata** structure which contains the transactions in a block.



The visual vocabulary expressed in facts is as follows: Transaction T4 in blockdata D1 of block B1 consists of transaction header, H4, a transaction signature, S4, a transaction proposal P4, a transaction response, R4, and a list of endorsements, E4.

In the above example, we can see the following fields:

- **Header**

  This section, illustrated by H4, captures some essential metadata about the transaction – for example, the name of the relevant chaincode, and its version.

- **Signature**

  This section, illustrated by S4, contains a cryptographic signature, created by the client application. This field is used to check that the transaction details have not been tampered with, as it requires the application's private key to generate it.

- **Proposal**

  This field, illustrated by P4, encodes the input parameters supplied by an application to the chaincode which creates the proposed ledger update. When the chaincode runs, this proposal provides a set of input parameters, which, in combination with the current world state, determines the new world state.

- **Response**

  This section, illustrated by R4, captures the before and after values of the world state, as a **Read Write set** (RW-set). It's the output of a chaincode, and if the transaction is successfully validated, it will be applied to the ledger to update the world state.

- **Endorsements**

  As shown in E4, this is a list of signed transaction responses from each required organization sufficient to satisfy the endorsement policy. You'll notice that, whereas only one transaction response is included in the transaction, there are multiple endorsements. That's because each endorsement effectively encodes its organization's particular transaction response – meaning that there's no need to include any transaction response that doesn't match sufficient endorsements as it will be rejected as invalid, and not update the world state.

That concludes the major fields of the transaction – there are others, but these are the essential ones that you need to understand to have a solid understanding of the ledger data structure.

4.12.7 World State database options

The world state is physically implemented as a database, to provide simple and efficient storage and retrieval of ledger states. As we've seen, ledger states can have simple or complex values, and to accommodate this, the world state database implementation can vary, allowing these values to be efficiently implemented. Options for the world state database currently include LevelDB and CouchDB.

LevelDB is the default and is particularly appropriate when ledger states are simple key-value pairs. A LevelDB database is closely co-located with a network node – it is embedded within the same operating system process.

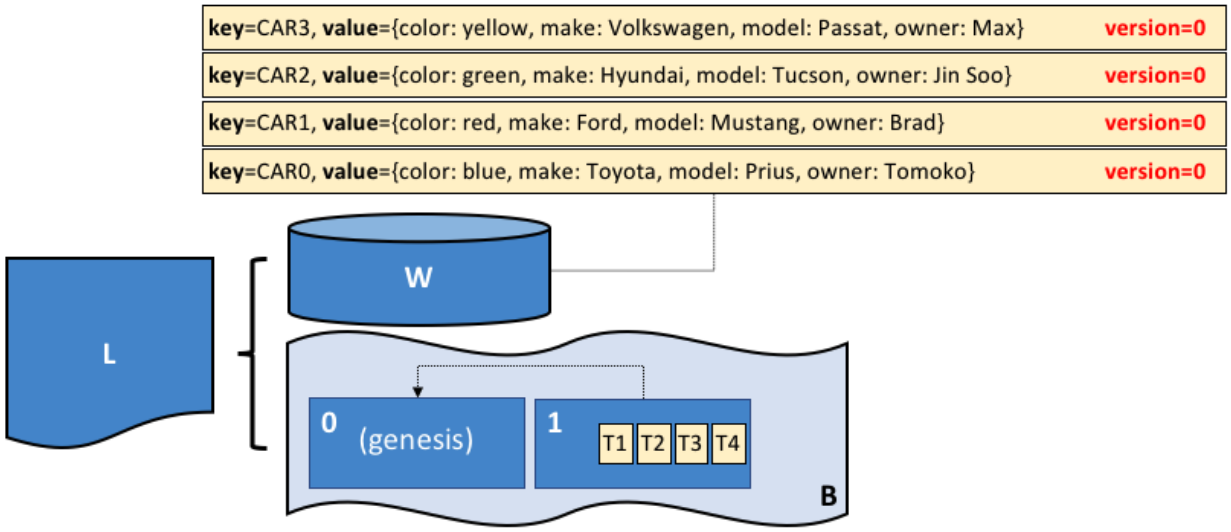
CouchDB is a particularly appropriate choice when ledger states are structured as JSON documents because CouchDB supports the rich queries and update of richer data types often found in business transactions. Implementation-wise, CouchDB runs in a separate operating system process, but there is still a 1:1 relation between a network node and a CouchDB instance. All of this is invisible to chaincode. See CouchDB as the StateDatabase for more information on CouchDB.

In LevelDB and CouchDB, we see an important aspect of Hyperledger Fabric – it is *pluggable*. The world state database could be a relational data store, or a graph store, or a temporal database. This provides great flexibility in the types of ledger states that can be efficiently accessed, allowing Hyperledger Fabric to address many different types of problems.

4.12.8 Example Ledger: fabcar

As we end this topic on the ledger, let's have a look at a sample ledger. If you've run the fabcar sample application, then you've created this ledger.

The fabcar sample app creates a set of 10 cars, of different color, make, model and owner. Here's what the ledger looks like after the first four cars have been created.



The visual vocabulary expressed in facts is as follows: The ledger L, comprises a world state, W and a blockchain, B. W contains four states with keys: CAR1, CAR2, CAR3 and CAR4. B contains two blocks, 0 and 1. Block 1 contains four transactions: T1, T2, T3, T4.

We can see that the ledger world state contains states that correspond to CAR0, CAR1, CAR2 and CAR3. CAR0 has a value which indicates that it is a blue Toyota Prius, owned by Tomoko, and we can see similar states and values for the other cars. Moreover, we can see that all car states are at version number 0, indicating that this is their starting version number – they have not been updated since they were created.

We can also see that the ledger blockchain contains two blocks. Block 0 is the genesis block, though it does not contain any transactions that relate to cars. Block 1 however, contains transactions T1, T2, T3, T4 and these correspond to transactions that created the initial states for CAR0 to CAR3 in the world state. We can see that block 1 is linked to block 0.

We have not shown the other fields in the blocks or transactions, specifically headers and hashes. If you're interested in the precise details of these, you will find a dedicated reference topic elsewhere in the documentation. It gives you a fully worked example of an entire block with its transactions in glorious detail – but for now, you have achieved a solid conceptual understanding of a Hyperledger Fabric ledger. Well done!

4.12.9 More information

See the Transaction Flow, Read-Write set semantics and CouchDB as the StateDatabase topics for a deeper dive on transaction flow, concurrency control, and the world state database.

4.13 Use Cases

The Hyperledger Requirements WG is documenting a number of blockchain use cases and maintaining an inventory here.

CHAPTER 5

Getting Started

5.1 Prerequisites

Before we begin, if you haven't already done so, you may wish to check that you have all the prerequisites below installed on the platform(s) on which you'll be developing blockchain applications and/or operating Hyperledger Fabric.

5.1.1 Install cURL

Download the latest version of the cURL tool if it is not already installed or if you get errors running the curl commands from the documentation.

Note: If you're on Windows please see the specific note on *Windows extras* below.

5.1.2 Docker and Docker Compose

You will need the following installed on the platform on which you will be operating, or developing on (or for), Hyperledger Fabric:

- MacOSX, *nix, or Windows 10: Docker Docker version 17.06.2-ce or greater is required.
- Older versions of Windows: Docker Toolbox - again, Docker version Docker 17.06.2-ce or greater is required.

You can check the version of Docker you have installed with the following command from a terminal prompt:

```
docker --version
```

Note: Installing Docker for Mac or Windows, or Docker Toolbox will also install Docker Compose. If you already had Docker installed, you should check that you have Docker Compose version 1.14.0 or greater installed. If not, we

recommend that you install a more recent version of Docker.

You can check the version of Docker Compose you have installed with the following command from a terminal prompt:

```
docker-compose --version
```

5.1.3 Go Programming Language

Hyperledger Fabric uses the Go Programming Language for many of its components.

- Go version 1.10.x is required.

Given that we will be writing chaincode programs in Go, there are two environment variables you will need to set properly; you can make these settings permanent by placing them in the appropriate startup file, such as your personal `~/.bashrc` file if you are using the `bash` shell under Linux.

First, you must set the environment variable `GOPATH` to point at the Go workspace containing the downloaded Fabric code base, with something like:

```
export GOPATH=$HOME/go
```

Note: You **must** set the GOPATH variable

Even though, in Linux, Go's `GOPATH` variable can be a colon-separated list of directories, and will use a default value of `$HOME/go` if it is unset, the current Fabric build framework still requires you to set and export that variable, and it must contain **only** the single directory name for your Go workspace. (This restriction might be removed in a future release.)

Second, you should (again, in the appropriate startup file) extend your command search path to include the Go `bin` directory, such as the following example for `bash` under Linux:

```
export PATH=$PATH:$GOPATH/bin
```

While this directory may not exist in a new Go workspace installation, it is populated later by the Fabric build system with a small number of Go executables used by other parts of the build system. So even if you currently have no such directory yet, extend your shell search path as above.

5.1.4 Node.js Runtime and NPM

If you will be developing applications for Hyperledger Fabric leveraging the Hyperledger Fabric SDK for Node.js, you will need to have version 8.9.x of Node.js installed.

Note: Node.js version 9.x is not supported at this time.

- Node.js - version 8.9.x or greater

Note: Installing Node.js will also install NPM, however it is recommended that you confirm the version of NPM installed. You can upgrade the `npm` tool with the following command:

```
npm install npm@5.6.0 -g
```

Python

Note: The following applies to Ubuntu 16.04 users only.

By default Ubuntu 16.04 comes with Python 3.5.1 installed as the `python3` binary. The Fabric Node.js SDK requires an iteration of Python 2.7 in order for `npm install` operations to complete successfully. Retrieve the 2.7 version with the following command:

```
sudo apt-get install python
```

Check your version(s):

```
python --version
```

5.1.5 Windows extras

If you are developing on Windows 7, you will want to work within the Docker Quickstart Terminal which uses Git Bash and provides a better alternative to the built-in Windows shell.

However experience has shown this to be a poor development environment with limited functionality. It is suitable to run Docker based scenarios, such as *Getting Started*, but you may have difficulties with operations involving the `make` and `docker` commands.

On Windows 10 you should use the native Docker distribution and you may use the Windows PowerShell. However, for the `binaries` command to succeed you will still need to have the `uname` command available. You can get it as part of Git but beware that only the 64bit version is supported.

Before running any `git clone` commands, run the following commands:

```
git config --global core.autocrlf false
git config --global core.longpaths true
```

You can check the setting of these parameters with the following commands:

```
git config --get core.autocrlf
git config --get core.longpaths
```

These need to be `false` and `true` respectively.

The `curl` command that comes with Git and Docker Toolbox is old and does not handle properly the redirect used in *Getting Started*. Make sure you install and use a newer version from the cURL downloads page

For Node.js you also need the necessary Visual Studio C++ Build Tools which are freely available and can be installed with the following command:

```
npm install --global windows-build-tools
```

See the NPM windows-build-tools page for more details.

Once this is done, you should also install the NPM GRPC module with the following command:

```
npm install --global grpc
```

Your environment should now be ready to go through the *Getting Started* samples and tutorials.

Note: If you have questions not addressed by this documentation, or run into issues with any of the tutorials, please visit the *Still Have Questions?* page for some tips on where to find additional help.

5.2 Install Samples, Binaries and Docker Images

While we work on developing real installers for the Hyperledger Fabric binaries, we provide a script that will download and install samples and binaries to your system. We think that you'll find the sample applications installed useful to learn more about the capabilities and operations of Hyperledger Fabric.

Note: If you are running on **Windows** you will want to make use of the Docker Quickstart Terminal for the upcoming terminal commands. Please visit the *Prerequisites* if you haven't previously installed it.

If you are using Docker Toolbox on Windows 7 or macOS, you will need to use a location under `C:\Users` (Windows 7) or `/Users` (macOS) when installing and running the samples.

If you are using Docker for Mac, you will need to use a location under `/Users`, `/Volumes`, `/private`, or `/tmp`. To use a different location, please consult the Docker documentation for file sharing.

If you are using Docker for Windows, please consult the Docker documentation for shared drives and use a location under one of the shared drives.

Determine a location on your machine where you want to place the *fabric-samples* repository and enter that directory in a terminal window. The command that follows will perform the following steps:

1. If needed, clone the *hyperledger/fabric-samples* repository
2. Checkout the appropriate version tag
3. Install the Hyperledger Fabric platform-specific binaries and config files for the version specified into the /bin and /config directories of fabric-samples
4. Download the Hyperledger Fabric docker images for the version specified

Once you are ready, and in the directory into which you will install the Fabric Samples and binaries, go ahead and execute the following command:

```
curl -sSL http://bit.ly/2ysbOFE | bash -s 1.3.0
```

Note: If you want to download different versions for Fabric, Fabric-ca and thirdparty Docker images, you must pass the version identifier for each.

```
curl -sSL http://bit.ly/2ysbOFE | bash -s <fabric> <fabric-ca> <thirdparty>
curl -sSL http://bit.ly/2ysbOFE | bash -s 1.3.0 1.3.0 0.4.13
```

Note: If you get an error running the above curl command, you may have too old a version of curl that does not handle redirects or an unsupported environment.

Please visit the *Prerequisites* page for additional information on where to find the latest version of curl and get the right environment. Alternately, you can substitute the un-shortened URL: https://raw.githubusercontent.com/hyperledger/fabric/master/scripts/bootstrap.sh

Note: You can use the command above for any published version of Hyperledger Fabric. Simply replace *1.3.0* with the version identifier of the version you wish to install.

The command above downloads and executes a bash script that will download and extract all of the platform-specific binaries you will need to set up your network and place them into the cloned repo you created above. It retrieves the following platform-specific binaries:

- `configtxgen`,
- `configtxlator`,
- `cryptogen`,
- `discover`,
- `idemixgen`
- `orderer`,
- `peer`, and
- `fabric-ca-client`

and places them in the `bin` sub-directory of the current working directory.

You may want to add that to your PATH environment variable so that these can be picked up without fully qualifying the path to each binary. e.g.:

```
export PATH=<path to download location>/bin:$PATH
```

Finally, the script will download the Hyperledger Fabric docker images from Docker Hub into your local Docker registry and tag them as 'latest'.

The script lists out the Docker images installed upon conclusion.

Look at the names for each image; these are the components that will ultimately comprise our Hyperledger Fabric network. You will also notice that you have two instances of the same image ID - one tagged as "amd64-1.x.x" and one tagged as "latest". Prior to 1.2.0, the image being downloaded was determined by `uname -m` and showed as "x86_64-1.x.x".

Note: On different architectures, the x86_64/amd64 would be replaced with the string identifying your architecture.

Note: If you have questions not addressed by this documentation, or run into issues with any of the tutorials, please visit the *Still Have Questions?* page for some tips on where to find additional help.

Before we begin, if you haven't already done so, you may wish to check that you have all the *Prerequisites* installed on the platform(s) on which you'll be developing blockchain applications and/or operating Hyperledger Fabric.

Once you have the prerequisites installed, you are ready to download and install HyperLedger Fabric. While we work on developing real installers for the Fabric binaries, we provide a script that will *Install Samples, Binaries and Docker Images* to your system. The script also will download the Docker images to your local registry.

5.3 Hyperledger Fabric SDKs

Hyperledger Fabric offers a number of SDKs to support various programming languages. There are two officially released SDKs for Node.js and Java:

- Hyperledger Fabric Node SDK and Node SDK documentation.
- Hyperledger Fabric Java SDK.

In addition, there are three more SDKs that have not yet been officially released (for Python, Go and REST), but they are still available for downloading and testing:

- Hyperledger Fabric Python SDK.
- Hyperledger Fabric Go SDK.
- Hyperledger Fabric REST SDK.

5.4 Hyperledger Fabric CA

Hyperledger Fabric provides an optional certificate authority service that you may choose to use to generate the certificates and key material to configure and manage identity in your blockchain network. However, any CA that can generate ECDSA certificates may be used.

CHAPTER 6

Tutorials

We offer tutorials to get you started with Hyperledger Fabric. The first is oriented to the Hyperledger Fabric **application developer**, *Writing Your First Application*. It takes you through the process of writing your first blockchain application for Hyperledger Fabric using the Hyperledger Fabric Node SDK.

The second tutorial is oriented towards the Hyperledger Fabric network operators, *Building Your First Network*. This one walks you through the process of establishing a blockchain network using Hyperledger Fabric and provides a basic sample application to test it out.

There are also tutorials for updating your channel, *Adding an Org to a Channel*, and upgrading your network to a later version of Hyperledger Fabric, *Upgrading Your Network Components*.

Finally, we offer two chaincode tutorials. One oriented to developers, *Chaincode for Developers*, and the other oriented to operators, *Chaincode for Operators*.

Note: If you have questions not addressed by this documentation, or run into issues with any of the tutorials, please visit the *Still Have Questions?* page for some tips on where to find additional help.

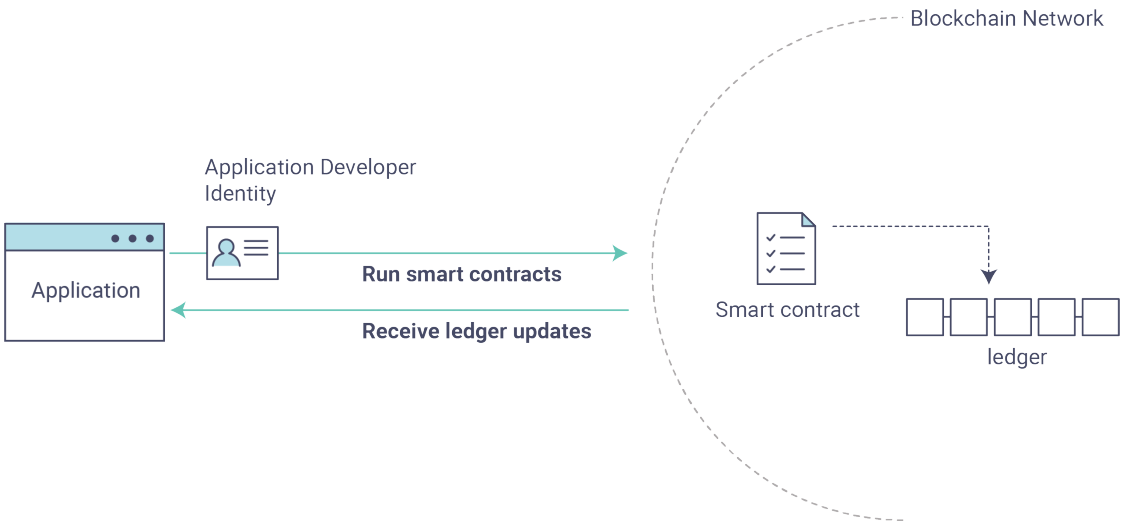
6.1 Writing Your First Application

Note: If you're not yet familiar with the fundamental architecture of a Fabric network, you may want to visit the *Introduction* and *Building Your First Network* documentation prior to continuing.

In this section we'll be looking at a handful of sample programs to see how Fabric apps work. These apps (and the smart contract they use) – collectively known as `fabcar` – provide a broad demonstration of Fabric functionality. Notably, we will show the process for interacting with a Certificate Authority and generating enrollment certificates, after which we will leverage these identities to query and update a ledger.

We'll go through three principle steps:

1. Setting up a development environment. Our application needs a network to interact with, so we'll download one stripped down to just the components we need for registration/enrollment, queries and updates:



2. Learning the parameters of the sample smart contract our app will use. Our smart contract contains various functions that allow us to interact with the ledger in different ways. We'll go in and inspect that smart contract to learn about the functions our applications will be using.

3. Developing the applications to be able to query and update assets on the ledger. We'll get into the app code itself (our apps have been written in Javascript) and manually manipulate the variables to run different kinds of queries and updates.

After completing this tutorial you should have a basic understanding of how an application is programmed in conjunction with a smart contract to interact with the ledger (i.e. the peer) on a Fabric network.

6.1.1 Setting up your Dev Environment

If you've already run through *Building Your First Network*, you should have your dev environment setup and will have downloaded *fabric-samples* as well as the accompanying artifacts. To run this tutorial, what you need to do now is tear down any existing networks you have, which you can do by issuing the following:

```
./byfn.sh down
```

If you don't have a development environment and the accompanying artifacts for the network and applications, visit the *Prerequisites* page and ensure you have the necessary dependencies installed on your machine.

Next, if you haven't done so already, visit the *Install Samples, Binaries and Docker Images* page and follow the provided instructions. Return to this tutorial once you have cloned the `fabric-samples` repository, and downloaded the latest stable Fabric images and available utilities.

At this point everything should be installed. Navigate to the `fabcar` subdirectory within your `fabric-samples` repository and take a look at what's inside:

```
cd fabric-samples/fabcar && ls
```

You should see the following:

```
enrollAdmin.js     invoke.js       package.json    query.js        registerUser.js␣
↪startFabric.sh
```

Before starting we also need to do a little housekeeping. Run the following command to kill any stale or active containers:

```
docker rm -f $(docker ps -aq)
```

Clear any cached networks:

```
# Press 'y' when prompted by the command

docker network prune
```

And lastly if you've already run through this tutorial, you'll also want to delete the underlying chaincode image for the `fabcar` smart contract. If you're a user going through this content for the first time, then you won't have this chaincode image on your system:

```
docker rmi dev-peer0.org1.example.com-fabcar-1.0-
↪5c906e402ed29f20260ae42283216aa75549c571e2e380f3615826365d8269ba
```

Install the clients & launch the network

Note: The following instructions require you to be in the `fabcar` subdirectory within your local clone of the `fabric-samples` repo. Remain at the root of this subdirectory for the remainder of this tutorial.

Run the following command to install the Fabric dependencies for the applications. We are concerned with `fabric-ca-client` which will allow our app(s) to communicate with the CA server and retrieve identity material, and with `fabric-client` which allows us to load the identity material and talk to the peers and ordering service.

```
npm install
```

Launch your network using the `startFabric.sh` shell script. This command will spin up our various Fabric entities and launch a smart contract container for chaincode written in Golang:

```
./startFabric.sh
```

You also have the option of running this tutorial against chaincode written in Node.js. If you'd like to pursue this route, issue the following command instead:

```
./startFabric.sh node
```

Note: Be aware that the Node.js chaincode scenario will take roughly 90 seconds to complete; perhaps longer. The script is not hanging, rather the increased time is a result of the fabric-shim being installed as the chaincode image is being built.

Alright, now that you've got a sample network and some code, let's take a look at how the different pieces fit together.

6.1.2 How Applications Interact with the Network

For a more in-depth look at the components in our `fabcar` network (and how they're deployed) as well as how applications interact with those components on more of a granular level, see understand_fabcar_network.

Developers more interested in seeing what applications **do** – as well as looking at the code itself to see how an application is constructed – should continue. For now, the most important thing to know is that applications use a software development kit (SDK) to access the **APIs** that permit queries and updates to the ledger.

6.1.3 Enrolling the Admin User

Note: The following two sections involve communication with the Certificate Authority. You may find it useful to stream the CA logs when running the upcoming programs.

To stream your CA logs, split your terminal or open a new shell and issue the following:

```
docker logs -f ca.example.com
```

Now hop back to your terminal with the `fabcar` content...

When we launched our network, an admin user – `admin` – was registered with our Certificate Authority. Now we need to send an enroll call to the CA server and retrieve the enrollment certificate (eCert) for this user. We won't delve into enrollment details here, but suffice it to say that the SDK and by extension our applications need this cert in order to form a user object for the admin. We will then use this admin object to subsequently register and enroll a new user. Send the admin enroll call to the CA server:

```
node enrollAdmin.js
```

This program will invoke a certificate signing request (CSR) and ultimately output an eCert and key material into a newly created folder – `hfc-key-store` – at the root of this project. Our apps will then look to this location when they need to create or load the identity objects for our various users.

6.1.4 Register and Enroll `user1`

With our newly generated admin eCert, we will now communicate with the CA server once more to register and enroll a new user. This user – `user1` – will be the identity we use when querying and updating the ledger. It's important to note here that it is the `admin` identity that is issuing the registration and enrollment calls for our new user (i.e. this user is acting in the role of a registrar). Send the register and enroll calls for `user1`:

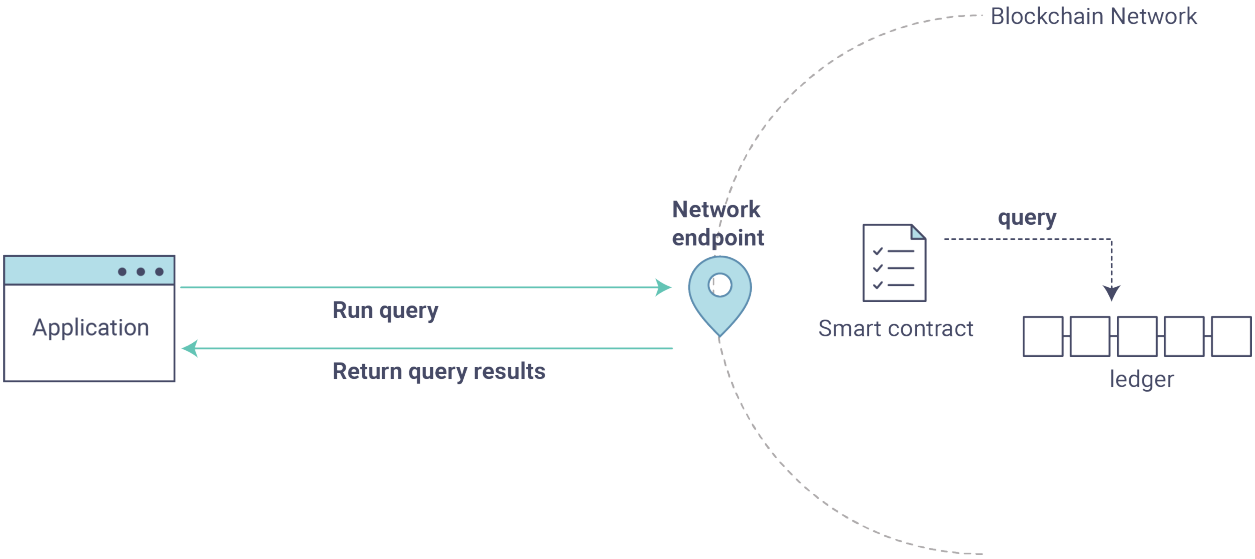
```
node registerUser.js
```

Similar to the admin enrollment, this program invokes a CSR and outputs the keys and eCert into the `hfc-key-store` subdirectory. So now we have identity material for two separate users – `admin` & `user1`. Time to interact with the ledger...

6.1.5 Querying the Ledger

Queries are how you read data from the ledger. This data is stored as a series of key-value pairs, and you can query for the value of a single key, multiple keys, or – if the ledger is written in a rich data storage format like JSON – perform complex searches against it (looking for all assets that contain certain keywords, for example).

This is a representation of how a query works:



First, let's run our `query.js` program to return a listing of all the cars on the ledger. We will use our second identity – `user1` – as the signing entity for this application. The following line in our program specifies `user1` as the signer:

```
fabric_client.getUserContext('user1', true);
```

Recall that the `user1` enrollment material has already been placed into our `hfc-key-store` subdirectory, so we simply need to tell our application to grab that identity. With the user object defined, we can now proceed with reading from the ledger. A function that will query all the cars, `queryAllCars`, is pre-loaded in the app, so we can simply run the program as is:

```
node query.js
```

It should return something like this:

```
Successfully loaded user1 from persistence
Query has completed, checking results
Response is  [{"Key":"CAR0", "Record":{"colour":"blue","make":"Toyota","model":"Prius
↪","owner":"Tomoko"}},
{"Key":"CAR1",   "Record":{"colour":"red","make":"Ford","model":"Mustang","owner":
↪"Brad"}},
{"Key":"CAR2", "Record":{"colour":"green","make":"Hyundai","model":"Tucson","owner":
↪"Jin Soo"}},
{"Key":"CAR3", "Record":{"colour":"yellow","make":"Volkswagen","model":"Passat","owner
↪":"Max"}},
{"Key":"CAR4", "Record":{"colour":"black","make":"Tesla","model":"S","owner":"Adriana
↪"}},
{"Key":"CAR5", "Record":{"colour":"purple","make":"Peugeot","model":"205","owner":
↪"Michel"}},
{"Key":"CAR6", "Record":{"colour":"white","make":"Chery","model":"S22L","owner":"Aarav
↪"}},
{"Key":"CAR7", "Record":{"colour":"violet","make":"Fiat","model":"Punto","owner":"Pari
↪"}},
{"Key":"CAR8", "Record":{"colour":"indigo","make":"Tata","model":"Nano","owner":
↪"Valeria"}},
{"Key":"CAR9", "Record":{"colour":"brown","make":"Holden","model":"Barina","owner":
↪"Shotaro"}}]
```

These are the 10 cars. A black Tesla Model S owned by Adriana, a red Ford Mustang owned by Brad, a violet Fiat Punto owned by Pari, and so on. The ledger is key-value based and, in our implementation, the key is `CAR0` through

CAR9. This will become particularly important in a moment.

Let's take a closer look at this program. Use an editor (e.g. atom or visual studio) and open `query.js`.

The initial section of the application defines certain variables such as channel name, cert store location and network endpoints. In our sample app, these variables have been baked-in, but in a real app these variables would have to be specified by the app dev.

```
var channel = fabric_client.newChannel('mychannel');
var peer = fabric_client.newPeer('grpc://localhost:7051');
channel.addPeer(peer);

var member_user = null;
var store_path = path.join(__dirname, 'hfc-key-store');
console.log('Store path:'+store_path);
var tx_id = null;
```

This is the chunk where we construct our query:

```
// queryCar chaincode function - requires 1 argument, ex: args: ['CAR4'],
// queryAllCars chaincode function - requires no arguments , ex: args: [''],
const request = {
  //targets : --- letting this default to the peers assigned to the channel
  chaincodeId: 'fabcar',
  fcn: 'queryAllCars',
  args: ['']
};
```

When the application ran, it invoked the `fabcar` chaincode on the peer, ran the `queryAllCars` function within it, and passed no arguments to it.

To take a look at the available functions within our smart contract, navigate to the `chaincode/fabcar/go` subdirectory at the root of `fabric-samples` and open `fabcar.go` in your editor.

Note: These same functions are defined within the Node.js version of the `fabcar` chaincode.

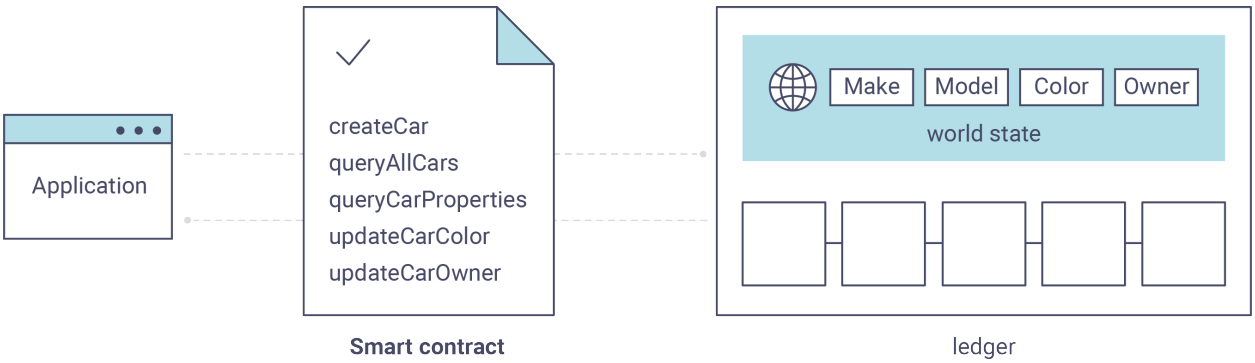
You'll see that we have the following functions available to call: `initLedger`, `queryCar`, `queryAllCars`, `createCar`, and `changeCarOwner`.

Let's take a closer look at the `queryAllCars` function to see how it interacts with the ledger.

```
func (s *SmartContract) queryAllCars(APIstub shim.ChaincodeStubInterface) sc.Response
↪{

      startKey := "CAR0"
      endKey := "CAR999"

      resultsIterator, err := APIstub.GetStateByRange(startKey, endKey)
```

This defines the range of `queryAllCars`. Every car between `CAR0` and `CAR999` – 1,000 cars in all, assuming every key has been tagged properly – will be returned by the query.

Below is a representation of how an app would call different functions in chaincode. Each function must be coded against an available API in the chaincode shim interface, which in turn allows the smart contract container to properly interface with the peer ledger.



We can see our `queryAllCars` function, as well as one called `createCar`, that will allow us to update the ledger and ultimately append a new block to the chain in a moment.

But first, go back to the `query.js` program and edit the constructor request to query `CAR4`. We do this by changing the function in `query.js` from `queryAllCars` to `queryCar` and passing `CAR4` as the specific key.

The `query.js` program should now look like this:

```
const request = {
  //targets : --- letting this default to the peers assigned to the channel
  chaincodeId: 'fabcar',
  fcn: 'queryCar',
  args: ['CAR4']
};
```

Save the program and navigate back to your `fabcar` directory. Now run the program again:

```
node query.js
```

You should see the following:

```
{"colour":"black","make":"Tesla","model":"S","owner":"Adriana"}
```

If you go back and look at the result from when we queried every car before, you can see that `CAR4` was Adriana's black Tesla model S, which is the result that was returned here.

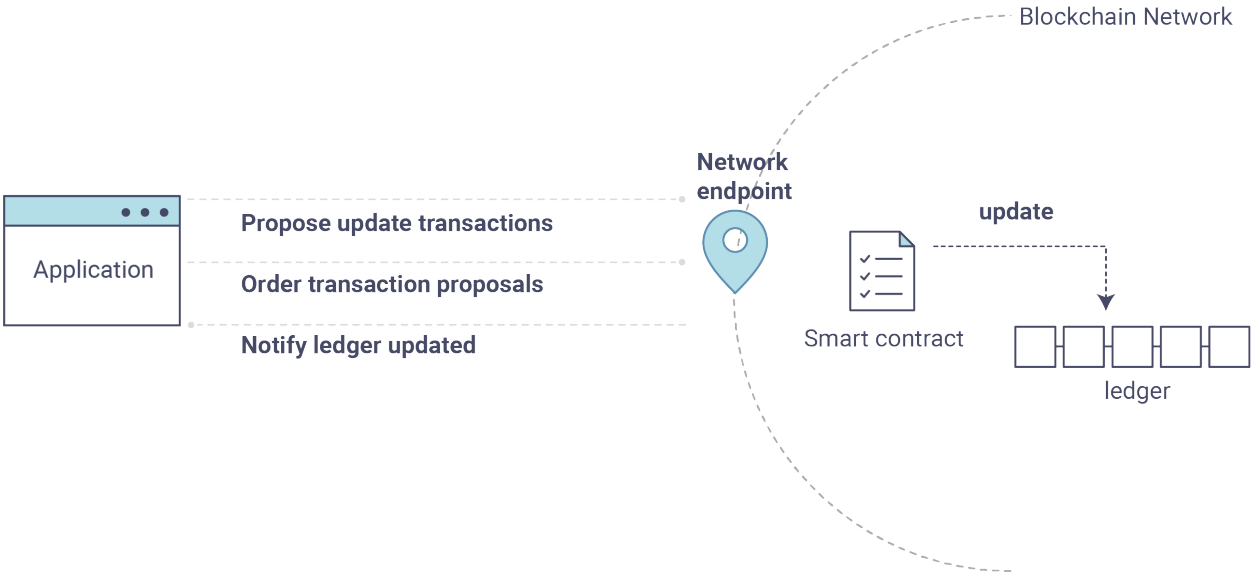
Using the `queryCar` function, we can query against any key (e.g. `CAR0`) and get whatever make, model, color, and owner correspond to that car.

Great. At this point you should be comfortable with the basic query functions in the smart contract and the handful of parameters in the query program. Time to update the ledger...

6.1.6 Updating the Ledger

Now that we've done a few ledger queries and added a bit of code, we're ready to update the ledger. There are a lot of potential updates we could make, but let's start by creating a car.

Below we can see how this process works. An update is proposed, endorsed, then returned to the application, which in turn sends it to be ordered and written to every peer's ledger:



Our first update to the ledger will be to create a new car. We have a separate Javascript program – `invoke.js` – that we will use to make updates. Just as with queries, use an editor to open the program and navigate to the code block where we construct our invocation:

```
// createCar chaincode function - requires 5 args, ex: args: ['CAR12', 'Honda',
↪'Accord', 'Black', 'Tom'],
// changeCarOwner chaincode function - requires 2 args , ex: args: ['CAR10', 'Barry'],
// must send the proposal to endorsing peers
var request = {
  //targets: let default to the peer assigned to the client
  chaincodeId: 'fabcar',
  fcn: '',
  args: [''],
  chainId: 'mychannel',
  txId: tx_id
};
```

You'll see that we can call one of two functions – `createCar` or `changeCarOwner`. First, let's create a red Chevy Volt and give it to an owner named Nick. We're up to `CAR9` on our ledger, so we'll use `CAR10` as the identifying key here. Edit this code block to look like this:

```
var request = {
  //targets: let default to the peer assigned to the client
  chaincodeId: 'fabcar',
  fcn: 'createCar',
  args: ['CAR10', 'Chevy', 'Volt', 'Red', 'Nick'],
  chainId: 'mychannel',
  txId: tx_id
};
```

Save it and run the program:

```
node invoke.js
```

There will be some output in the terminal about `ProposalResponse` and promises. However, all we're concerned with is this message:

```
The transaction has been committed on peer localhost:7053
```

To see that this transaction has been written, go back to `query.js` and change the argument from `CAR4` to `CAR10`.

In other words, change this:

```
const request = {
  //targets : --- letting this default to the peers assigned to the channel
  chaincodeId: 'fabcar',
  fcn: 'queryCar',
  args: ['CAR4']
};
```

To this:

```
const request = {
  //targets : --- letting this default to the peers assigned to the channel
  chaincodeId: 'fabcar',
  fcn: 'queryCar',
  args: ['CAR10']
};
```

Save once again, then query:

```
node query.js
```

Which should return this:

```
Response is  {"colour":"Red","make":"Chevy","model":"Volt","owner":"Nick"}
```

Congratulations. You've created a car!

So now that we've done that, let's say that Nick is feeling generous and he wants to give his Chevy Volt to someone named Dave.

To do this go back to `invoke.js` and change the function from `createCar` to `changeCarOwner` and input the arguments like this:

```
var request = {
  //targets: let default to the peer assigned to the client
  chaincodeId: 'fabcar',
  fcn: 'changeCarOwner',
  args: ['CAR10', 'Dave'],
  chainId: 'mychannel',
  txId: tx_id
};
```

The first argument – `CAR10` – reflects the car that will be changing owners. The second argument – `Dave` – defines the new owner of the car.

Save and execute the program again:

```
node invoke.js
```

Now let's query the ledger again and ensure that Dave is now associated with the `CAR10` key:

```
node query.js
```

It should return this result:

```
Response is  {"colour":"Red","make":"Chevy","model":"Volt","owner":"Dave"}
```

The ownership of `CAR10` has been changed from Nick to Dave.

Note: In a real world application the chaincode would likely have some access control logic. For example, only certain authorized users may create new cars, and only the car owner may transfer the car to somebody else.

6.1.7 Summary

Now that we've done a few queries and a few updates, you should have a pretty good sense of how applications interact with the network. You've seen the basics of the roles smart contracts, APIs, and the SDK play in queries and updates and you should have a feel for how different kinds of applications could be used to perform other business tasks and operations.

In subsequent documents we'll learn how to actually **write** a smart contract and how some of these more low level application functions can be leveraged (especially relating to identity and membership services).

6.1.8 Additional Resources

The Hyperledger Fabric Node SDK repo is an excellent resource for deeper documentation and sample code. You can also consult the Fabric community and component experts on Hyperledger Rocket Chat.

6.2 Building Your First Network

Note: These instructions have been verified to work against the latest stable Docker images and the pre-compiled setup utilities within the supplied tar file. If you run these commands with images or tools from the current master branch, it is possible that you will see configuration and panic errors.

The build your first network (BYFN) scenario provisions a sample Hyperledger Fabric network consisting of two organizations, each maintaining two peer nodes, and a "solo" ordering service.

6.2.1 Install prerequisites

Before we begin, if you haven't already done so, you may wish to check that you have all the *Prerequisites* installed on the platform(s) on which you'll be developing blockchain applications and/or operating Hyperledger Fabric.

You will also need to *Install Samples, Binaries and Docker Images*. You will notice that there are a number of samples included in the `fabric-samples` repository. We will be using the `first-network` sample. Let's open that sub-directory now.

```
cd fabric-samples/first-network
```

Note: The supplied commands in this documentation **MUST** be run from your `first-network` sub-directory of the `fabric-samples` repository clone. If you elect to run the commands from a different location, the various provided scripts will be unable to find the binaries.

6.2.2 Want to run it now?

We provide a fully annotated script - `byfn.sh` - that leverages these Docker images to quickly bootstrap a Hyperledger Fabric network comprised of 4 peers representing two different organizations, and an orderer node. It will also launch a container to run a scripted execution that will join peers to a channel, deploy and instantiate chaincode and drive execution of transactions against the deployed chaincode.

Here's the help text for the `byfn.sh` script:

```
Usage:
  byfn.sh <mode> [-c <channel name>] [-t <timeout>] [-d <delay>] [-f <docker-compose-
↪file>] [-s <dbtype>] [-l <language>] [-i <imagetag>] [-v]
    <mode> - one of 'up', 'down', 'restart', 'generate' or 'upgrade'
      - 'up' - bring up the network with docker-compose up
      - 'down' - clear the network with docker-compose down
      - 'restart' - restart the network
      - 'generate' - generate required certificates and genesis block
      - 'upgrade'  - upgrade the network from v1.0.x to v1.1
    -c <channel name> - channel name to use (defaults to "mychannel")
    -t <timeout> - CLI timeout duration in seconds (defaults to 10)
    -d <delay> - delay duration in seconds (defaults to 3)
    -f <docker-compose-file> - specify which docker-compose file use (defaults to␣
↪docker-compose-cli.yaml)
    -s <dbtype> - the database backend to use: goleveldb (default) or couchdb
    -l <language> - the chaincode language: golang (default), node or java
    -i <imagetag> - the tag to be used to launch the network (defaults to "latest")
    -v - verbose mode
  byfn.sh -h (print this message)

Typically, one would first generate the required certificates and
genesis block, then bring up the network. e.g.:

        byfn.sh generate -c mychannel
        byfn.sh up -c mychannel -s couchdb
        byfn.sh up -c mychannel -s couchdb -i 1.1.0-alpha
        byfn.sh up -l node
        byfn.sh down -c mychannel
        byfn.sh upgrade -c mychannel

Taking all defaults:
        byfn.sh generate
        byfn.sh up
        byfn.sh down
```

If you choose not to supply a channel name, then the script will use a default name of `mychannel`. The CLI timeout parameter (specified with the -t flag) is an optional value; if you choose not to set it, then the CLI will give up on query requests made after the default setting of 10 seconds.

Generate Network Artifacts

Ready to give it a go? Okay then! Execute the following command:

```
./byfn.sh generate
```

You will see a brief description as to what will occur, along with a yes/no command line prompt. Respond with a `y` or hit the return key to execute the described action.

```
Generating certs and genesis block for channel 'mychannel' with CLI timeout of '10'␣
↪seconds and CLI delay of '3' seconds
Continue? [Y/n] y
proceeding ...
/Users/xxx/dev/fabric-samples/bin/cryptogen

############################################################
##### Generate certificates using cryptogen tool #########
############################################################
org1.example.com
2017-06-12 21:01:37.334 EDT [bccsp] GetDefault -> WARN 001 Before using BCCSP, please␣
↪call InitFactories(). Falling back to bootBCCSP.
...

/Users/xxx/dev/fabric-samples/bin/configtxgen
############################################################
#########  Generating Orderer Genesis block ##############
############################################################
2017-06-12 21:01:37.558 EDT [common/configtx/tool] main -> INFO 001 Loading␣
↪configuration
2017-06-12 21:01:37.562 EDT [msp] getMspConfig -> INFO 002 intermediate certs folder␣
↪not found at [/Users/xxx/dev/byfn/crypto-config/ordererOrganizations/example.com/
↪msp/intermediatecerts]. Skipping.: [stat /Users/xxx/dev/byfn/crypto-config/
↪ordererOrganizations/example.com/msp/intermediatecerts: no such file or directory]
...
2017-06-12 21:01:37.588 EDT [common/configtx/tool] doOutputBlock -> INFO 00b␣
↪Generating genesis block
2017-06-12 21:01:37.590 EDT [common/configtx/tool] doOutputBlock -> INFO 00c Writing␣
↪genesis block

#################################################################
### Generating channel configuration transaction 'channel.tx' ###
#################################################################
2017-06-12 21:01:37.634 EDT [common/configtx/tool] main -> INFO 001 Loading␣
↪configuration
2017-06-12 21:01:37.644 EDT [common/configtx/tool] doOutputChannelCreateTx -> INFO␣
↪002 Generating new channel configtx
2017-06-12 21:01:37.645 EDT [common/configtx/tool] doOutputChannelCreateTx -> INFO␣
↪003 Writing new channel tx

#################################################################
#######    Generating anchor peer update for Org1MSP   ##########
#################################################################
2017-06-12 21:01:37.674 EDT [common/configtx/tool] main -> INFO 001 Loading␣
↪configuration
2017-06-12 21:01:37.678 EDT [common/configtx/tool] doOutputAnchorPeersUpdate -> INFO␣
↪002 Generating anchor peer update
2017-06-12 21:01:37.679 EDT [common/configtx/tool] doOutputAnchorPeersUpdate -> INFO␣
↪003 Writing anchor peer update

#################################################################
#######    Generating anchor peer update for Org2MSP   ##########
#################################################################
2017-06-12 21:01:37.700 EDT [common/configtx/tool] main -> INFO 001 Loading␣
↪configuration
2017-06-12 21:01:37.704 EDT [common/configtx/tool] doOutputAnchorPeersUpdate -> INFO␣
↪002 Generating anchor peer update
```

(continues on next page)

(continued from previous page)

```
2017-06-12 21:01:37.704 EDT [common/configtx/tool] doOutputAnchorPeersUpdate -> INFO␣
↪003 Writing anchor peer update
```

This first step generates all of the certificates and keys for our various network entities, the `genesis block` used to bootstrap the ordering service, and a collection of configuration transactions required to configure a *Channel*.

Bring Up the Network

Next, you can bring the network up with one of the following commands:

```
./byfn.sh up
```

The above command will compile Golang chaincode images and spin up the corresponding containers. Go is the default chaincode language, however there is also support for Node.js and Java chaincode. If you'd like to run through this tutorial with node chaincode, pass the following command instead:

```
# we use the -l flag to specify the chaincode language
# forgoing the -l flag will default to Golang

./byfn.sh up -l node
```

Note: For more information on the Node.js shim, please refer to its documentation.

Note: For more information on the Java shim, please refer to its documentation.

o make the sample run with Java chaincode, you have to specify `-l java` as follows:

```
./byfn.sh up -l java
```

Note: Do not run both of these commands. Only one language can be tried unless you bring down and recreate the network between.

Once again, you will be prompted as to whether you wish to continue or abort. Respond with a `y` or hit the return key:

```
Starting for channel 'mychannel' with CLI timeout of '10' seconds and CLI delay of '3
↪' seconds
Continue? [Y/n]
proceeding ...
Creating network "net_byfn" with the default driver
Creating peer0.org1.example.com
Creating peer1.org1.example.com
Creating peer0.org2.example.com
Creating orderer.example.com
Creating peer1.org2.example.com
Creating cli


 ____    _____      _      ____    _____
/ ___|  |_   _|    / \    |  _ \  |_   _|
```

(continues on next page)

(continued from previous page)

```
\___ \    | |     / _ \   | |_) |   | |
 ___) |   | |    / ___ \  |  _ <    | |
|____/    |_|   /_/   \_\ |_| \_\   |_|

Channel name : mychannel
Creating channel...
```

The logs will continue from there. This will launch all of the containers, and then drive a complete end-to-end application scenario. Upon successful completion, it should report the following in your terminal window:

```
Query Result: 90
2017-05-16 17:08:15.158 UTC [main] main -> INFO 008 Exiting.....
===================== Query successful on peer1.org2 on channel 'mychannel'␣
↪=====================

===================== All GOOD, BYFN execution completed =====================



 _____   _   _   ____
| ____| | \ | | |  _ \
|  _|   |  \| | | | | |
| |___  | |\  | | |_| |
|_____| |_| \_| |____/
```

You can scroll through these logs to see the various transactions. If you don't get this result, then jump down to the *Troubleshooting* section and let's see whether we can help you discover what went wrong.

Bring Down the Network

Finally, let's bring it all down so we can explore the network setup one step at a time. The following will kill your containers, remove the crypto material and four artifacts, and delete the chaincode images from your Docker Registry:

```
./byfn.sh down
```

Once again, you will be prompted to continue, respond with a `y` or hit the return key:

```
Stopping with channel 'mychannel' and CLI timeout of '10'
Continue? [Y/n] y
proceeding ...
WARNING: The CHANNEL_NAME variable is not set. Defaulting to a blank string.
WARNING: The TIMEOUT variable is not set. Defaulting to a blank string.
Removing network net_byfn
468aaa6201ed
...
Untagged: dev-peer1.org2.example.com-mycc-1.0:latest
Deleted: sha256:ed3230614e64e1c83e510c0c282e982d2b06d148b1c498bbdcc429e2b2531e91
...
```

If you'd like to learn more about the underlying tooling and bootstrap mechanics, continue reading. In these next sections we'll walk through the various steps and requirements to build a fully-functional Hyperledger Fabric network.

Note: The manual steps outlined below assume that the `CORE_LOGGING_LEVEL` in the `cli` container is set to `DEBUG`. You can set this by modifying the `docker-compose-cli.yaml` file in the `first-network` directory. e.g.

```
cli:
  container_name: cli
  image: hyperledger/fabric-tools:$IMAGE_TAG
  tty: true
  stdin_open: true
  environment:
    - GOPATH=/opt/gopath
    - CORE_VM_ENDPOINT=unix:///host/var/run/docker.sock
    - CORE_LOGGING_LEVEL=DEBUG
    #- CORE_LOGGING_LEVEL=INFO
```

6.2.3 Crypto Generator

We will use the `cryptogen` tool to generate the cryptographic material (x509 certs and signing keys) for our various network entities. These certificates are representative of identities, and they allow for sign/verify authentication to take place as our entities communicate and transact.

How does it work?

Cryptogen consumes a file - `crypto-config.yaml` - that contains the network topology and allows us to generate a set of certificates and keys for both the Organizations and the components that belong to those Organizations. Each Organization is provisioned a unique root certificate (`ca-cert`) that binds specific components (peers and orderers) to that Org. By assigning each Organization a unique CA certificate, we are mimicking a typical network where a participating *Member* would use its own Certificate Authority. Transactions and communications within Hyperledger Fabric are signed by an entity's private key (`keystore`), and then verified by means of a public key (`signcerts`).

You will notice a `count` variable within this file. We use this to specify the number of peers per Organization; in our case there are two peers per Org. We won't delve into the minutiae of x.509 certificates and public key infrastructure right now. If you're interested, you can peruse these topics on your own time.

Before running the tool, let's take a quick look at a snippet from the `crypto-config.yaml`. Pay specific attention to the "Name", "Domain" and "Specs" parameters under the `OrdererOrgs` header:

```
OrdererOrgs:
#---------------------------------------------------------
# Orderer
# ---------------------------------------------------------
- Name: Orderer
  Domain: example.com
  CA:
      Country: US
      Province: California
      Locality: San Francisco
  #   OrganizationalUnit: Hyperledger Fabric
  #   StreetAddress: address for org # default nil
  #   PostalCode: postalCode for org # default nil
  # ---------------------------------------------------------
  # "Specs" - See PeerOrgs below for complete description
# ---------------------------------------------------------
  Specs:
    - Hostname: orderer
# ---------------------------------------------------------
# "PeerOrgs" - Definition of organizations managing peer nodes
```

(continues on next page)

(continued from previous page)

```
 # ---------------------------------------------------------
PeerOrgs:
# ---------------------------------------------------------
# Org1
# ---------------------------------------------------------
- Name: Org1
  Domain: org1.example.com
  EnableNodeOUs: true
```

The naming convention for a network entity is as follows - "{{.Hostname}}.{{.Domain}}". So using our ordering node as a reference point, we are left with an ordering node named - `orderer.example.com` that is tied to an MSP ID of `Orderer`. This file contains extensive documentation on the definitions and syntax. You can also refer to the *Membership Service Providers (MSP)* documentation for a deeper dive on MSP.

After we run the `cryptogen` tool, the generated certificates and keys will be saved to a folder titled `crypto-config`.

6.2.4 Configuration Transaction Generator

The `configtxgen` tool is used to create four configuration artifacts:

- orderer `genesis block`,
- channel `configuration transaction`,
- and two `anchor peer transactions` - one for each Peer Org.

Please see *configtxgen* for a complete description of this tool's functionality.

The orderer block is the *Genesis Block* for the ordering service, and the channel configuration transaction file is broadcast to the orderer at *Channel* creation time. The anchor peer transactions, as the name might suggest, specify each Org's *Anchor Peer* on this channel.

How does it work?

Configtxgen consumes a file - `configtx.yaml` - that contains the definitions for the sample network. There are three members - one Orderer Org (`OrdererOrg`) and two Peer Orgs (`Org1` & `Org2`) each managing and maintaining two peer nodes. This file also specifies a consortium - `SampleConsortium` - consisting of our two Peer Orgs. Pay specific attention to the "Profiles" section at the top of this file. You will notice that we have two unique headers. One for the orderer genesis block - `TwoOrgsOrdererGenesis` - and one for our channel - `TwoOrgsChannel`.

These headers are important, as we will pass them in as arguments when we create our artifacts.

Note: Notice that our `SampleConsortium` is defined in the system-level profile and then referenced by our channel-level profile. Channels exist within the purview of a consortium, and all consortia must be defined in the scope of the network at large.

This file also contains two additional specifications that are worth noting. Firstly, we specify the anchor peers for each Peer Org (`peer0.org1.example.com` & `peer0.org2.example.com`). Secondly, we point to the location of the MSP directory for each member, in turn allowing us to store the root certificates for each Org in the orderer genesis block. This is a critical concept. Now any network entity communicating with the ordering service can have its digital signature verified.

6.2.5 Run the tools

You can manually generate the certificates/keys and the various configuration artifacts using the `configtxgen` and `cryptogen` commands. Alternately, you could try to adapt the byfn.sh script to accomplish your objectives.

Manually generate the artifacts

You can refer to the `generateCerts` function in the byfn.sh script for the commands necessary to generate the certificates that will be used for your network configuration as defined in the `crypto-config.yaml` file. However, for the sake of convenience, we will also provide a reference here.

First let's run the `cryptogen` tool. Our binary is in the `bin` directory, so we need to provide the relative path to where the tool resides.

```
../bin/cryptogen generate --config=./crypto-config.yaml
```

You should see the following in your terminal:

```
org1.example.com
org2.example.com
```

The certs and keys (i.e. the MSP material) will be output into a directory - `crypto-config` - at the root of the `first-network` directory.

Next, we need to tell the `configtxgen` tool where to look for the `configtx.yaml` file that it needs to ingest. We will tell it look in our present working directory:

```
export FABRIC_CFG_PATH=$PWD
```

Then, we'll invoke the `configtxgen` tool to create the orderer genesis block:

```
../bin/configtxgen -profile TwoOrgsOrdererGenesis -outputBlock ./channel-artifacts/
↪genesis.block
```

You should see an output similar to the following in your terminal:

```
2017-10-26 19:21:56.301 EDT [common/tools/configtxgen] main -> INFO 001 Loading␣
↪configuration
2017-10-26 19:21:56.309 EDT [common/tools/configtxgen] doOutputBlock -> INFO 002␣
↪Generating genesis block
2017-10-26 19:21:56.309 EDT [common/tools/configtxgen] doOutputBlock -> INFO 003␣
↪Writing genesis block
```

Note: The orderer genesis block and the subsequent artifacts we are about to create will be output into the `channel-artifacts` directory at the root of this project.

Create a Channel Configuration Transaction

Next, we need to create the channel transaction artifact. Be sure to replace `$CHANNEL_NAME` or set `CHANNEL_NAME` as an environment variable that can be used throughout these instructions:

```
# The channel.tx artifact contains the definitions for our sample channel

export CHANNEL_NAME=mychannel  && ../bin/configtxgen -profile TwoOrgsChannel -
↪outputCreateChannelTx ./channel-artifacts/channel.tx -channelID $CHANNEL_NAME
```

You should see an output similar to the following in your terminal:

```
2017-10-26 19:24:05.324 EDT [common/tools/configtxgen] main -> INFO 001 Loading␣
↪configuration
2017-10-26 19:24:05.329 EDT [common/tools/configtxgen] doOutputChannelCreateTx ->␣
↪INFO 002 Generating new channel configtx
2017-10-26 19:24:05.329 EDT [common/tools/configtxgen] doOutputChannelCreateTx ->␣
↪INFO 003 Writing new channel tx
```

Next, we will define the anchor peer for Org1 on the channel that we are constructing. Again, be sure to replace `$CHANNEL_NAME` or set the environment variable for the following commands. The terminal output will mimic that of the channel transaction artifact:

```
../bin/configtxgen -profile TwoOrgsChannel -outputAnchorPeersUpdate ./channel-
↪artifacts/Org1MSPanchors.tx -channelID $CHANNEL_NAME -asOrg Org1MSP
```

Now, we will define the anchor peer for Org2 on the same channel:

```
../bin/configtxgen -profile TwoOrgsChannel -outputAnchorPeersUpdate ./channel-
↪artifacts/Org2MSPanchors.tx -channelID $CHANNEL_NAME -asOrg Org2MSP
```

6.2.6 Start the network

Note: If you ran the `byfn.sh` example above previously, be sure that you have brought down the test network before you proceed (see *Bring Down the Network*).

We will leverage a script to spin up our network. The docker-compose file references the images that we have previously downloaded, and bootstraps the orderer with our previously generated `genesis.block`.

We want to go through the commands manually in order to expose the syntax and functionality of each call.

First let's start our network:

```
docker-compose -f docker-compose-cli.yaml up -d
```

If you want to see the realtime logs for your network, then do not supply the `-d` flag. If you let the logs stream, then you will need to open a second terminal to execute the CLI calls.

Environment variables

For the following CLI commands against `peer0.org1.example.com` to work, we need to preface our commands with the four environment variables given below. These variables for `peer0.org1.example.com` are baked into the CLI container, therefore we can operate without passing them. **HOWEVER**, if you want to send calls to other peers or the orderer, then you can provide these values accordingly by editing the `docker-compose-base.yaml` before starting the container. Modify the following four environment variables to use a different peer and org.

```
# Environment variables for PEER0

CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp
CORE_PEER_ADDRESS=peer0.org1.example.com:7051
CORE_PEER_LOCALMSPID="Org1MSP"
CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt
```

Create & Join Channel

Recall that we created the channel configuration transaction using the `configtxgen` tool in the *Create a Channel Configuration Transaction* section, above. You can repeat that process to create additional channel configuration transactions, using the same or different profiles in the `configtx.yaml` that you pass to the `configtxgen` tool. Then you can repeat the process defined in this section to establish those other channels in your network.

We will enter the CLI container using the `docker exec` command:

```
docker exec -it cli bash
```

If successful you should see the following:

```
root@0d78bb69300d:/opt/gopath/src/github.com/hyperledger/fabric/peer#
```

If you do not want to run the CLI commands against the default peer `peer0.org1.example.com`, replace the values of `peer0` or `org1` in the four environment variables and run the commands:

```
# Environment variables for PEER0

export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp
export CORE_PEER_ADDRESS=peer0.org1.example.com:7051
export CORE_PEER_LOCALMSPID="Org1MSP"
export CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt
```

Next, we are going to pass in the generated channel configuration transaction artifact that we created in the *Create a Channel Configuration Transaction* section (we called it `channel.tx`) to the orderer as part of the create channel request.

We specify our channel name with the `-c` flag and our channel configuration transaction with the `-f` flag. In this case it is `channel.tx`, however you can mount your own configuration transaction with a different name. Once again we will set the `CHANNEL_NAME` environment variable within our CLI container so that we don't have to explicitly pass this argument. Channel names must be all lower case, less than 250 characters long and match the regular expression `[a-z][a-z0-9.-]*`.

```
export CHANNEL_NAME=mychannel

# the channel.tx file is mounted in the channel-artifacts directory within your CLI␣
↪container
# as a result, we pass the full path for the file
# we also pass the path for the orderer ca-cert in order to verify the TLS handshake
# be sure to export or replace the $CHANNEL_NAME variable appropriately

peer channel create -o orderer.example.com:7050 -c $CHANNEL_NAME -f ./channel-
↪artifacts/channel.tx --tls --cafile /opt/gopath/src/github.com/hyperledger/fabric/
↪peer/crypto/ordererOrganizations/example.com/orderers/orderer.example.com/msp/
↪tlscacerts/tlsca.example.com-cert.pem
```

(continues on next page)

(continued from previous page)

Note: Notice the `--cafile` that we pass as part of this command. It is the local path to the orderer's root cert, allowing us to verify the TLS handshake.

This command returns a genesis block - `<CHANNEL-NAME.block>` - which we will use to join the channel. It contains the configuration information specified in `channel.tx` If you have not made any modifications to the default channel name, then the command will return you a proto titled `mychannel.block`.

Note: You will remain in the CLI container for the remainder of these manual commands. You must also remember to preface all commands with the corresponding environment variables when targeting a peer other than `peer0.org1.example.com`.

Now let's join `peer0.org1.example.com` to the channel.

```
# By default, this joins ``peer0.org1.example.com`` only
# the <CHANNEL-NAME.block> was returned by the previous command
# if you have not modified the channel name, you will join with mychannel.block
# if you have created a different channel name, then pass in the appropriately named␣
↪block

 peer channel join -b mychannel.block
```

You can make other peers join the channel as necessary by making appropriate changes in the four environment variables we used in the *Environment variables* section, above.

Rather than join every peer, we will simply join `peer0.org2.example.com` so that we can properly update the anchor peer definitions in our channel. Since we are overriding the default environment variables baked into the CLI container, this full command will be the following:

```
CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp CORE_PEER_
↪ADDRESS=peer0.org2.example.com:7051 CORE_PEER_LOCALMSPID="Org2MSP" CORE_PEER_TLS_
↪ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt peer␣
↪channel join -b mychannel.block
```

Alternatively, you could choose to set these environment variables individually rather than passing in the entire string. Once they've been set, you simply need to issue the `peer channel join` command again and the CLI container will act on behalf of `peer0.org2.example.com`.

Update the anchor peers

The following commands are channel updates and they will propagate to the definition of the channel. In essence, we adding additional configuration information on top of the channel's genesis block. Note that we are not modifying the genesis block, but simply adding deltas into the chain that will define the anchor peers.

Update the channel definition to define the anchor peer for Org1 as `peer0.org1.example.com`:

```
peer channel update -o orderer.example.com:7050 -c $CHANNEL_NAME -f ./channel-
↪artifacts/Org1MSPanchors.tx --tls --cafile /opt/gopath/src/github.com/hyperledger/
↪fabric/peer/crypto/ordererOrganizations/example.com/orderers/orderer.example.com/
↪msp/tlscacerts/tlsca.example.com-cert.pem
```

Now update the channel definition to define the anchor peer for Org2 as `peer0.org2.example.com`. Identically to the `peer channel join` command for the Org2 peer, we will need to preface this call with the appropriate environment variables.

```
CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp CORE_PEER_
↪ADDRESS=peer0.org2.example.com:7051 CORE_PEER_LOCALMSPID="Org2MSP" CORE_PEER_TLS_
↪ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt peer␣
↪channel update -o orderer.example.com:7050 -c $CHANNEL_NAME -f ./channel-artifacts/
↪Org2MSPanchors.tx --tls --cafile /opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/
↪tlsca.example.com-cert.pem
```

Install & Instantiate Chaincode

Note: We will utilize a simple existing chaincode. To learn how to write your own chaincode, see the *Chaincode for Developers* tutorial.

Applications interact with the blockchain ledger through `chaincode`. As such we need to install the chaincode on every peer that will execute and endorse our transactions, and then instantiate the chaincode on the channel.

First, install the sample Go, Node.js or Java chaincode onto one of the four peer nodes. These commands place the specified source code flavor onto our peer's filesystem.

Note: You can only install one version of the source code per chaincode name and version. The source code exists on the peer's file system in the context of chaincode name and version; it is language agnostic. Similarly the instantiated chaincode container will be reflective of whichever language has been installed on the peer.

Golang

```
# this installs the Go chaincode
peer chaincode install -n mycc -v 1.0 -p github.com/chaincode/chaincode_example02/go/
```

Node.js

```
# this installs the Node.js chaincode
# make note of the -l flag; we use this to specify the language
peer chaincode install -n mycc -v 1.0 -l node -p /opt/gopath/src/github.com/chaincode/
↪chaincode_example02/node/
```

Java

```
peer chaincode install -n mycc -v 1.0 -l java -p /opt/gopath/src/github.com/chaincode/
↪chaincode_example02/java/
```

Next, instantiate the chaincode on the channel. This will initialize the chaincode on the channel, set the endorsement policy for the chaincode, and launch a chaincode container for the targeted peer. Take note of the `-P` argument. This is our policy where we specify the required level of endorsement for a transaction against this chaincode to be validated.

In the command below you'll notice that we specify our policy as `-P "AND ('Org1MSP.peer','Org2MSP.peer')"`. This means that we need "endorsement" from a peer belonging to Org1 **AND** Org2 (i.e. two endorsement). If we changed the syntax to `OR` then we would need only one endorsement.

Golang

```
# be sure to replace the $CHANNEL_NAME environment variable if you have not exported␣
↪it
# if you did not install your chaincode with a name of mycc, then modify that␣
↪argument as well

peer chaincode instantiate -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪mycc -v 1.0 -c '{"Args":["init","a", "100", "b","200"]}' -P "AND ('Org1MSP.peer',
↪'Org2MSP.peer')"
```

Node.js

Note: The instantiation of the Node.js chaincode will take roughly a minute. The command is not hanging; rather it is installing the fabric-shim layer as the image is being compiled.

```
# be sure to replace the $CHANNEL_NAME environment variable if you have not exported␣
↪it
# if you did not install your chaincode with a name of mycc, then modify that␣
↪argument as well
# notice that we must pass the -l flag after the chaincode name to identify the␣
↪language

peer chaincode instantiate -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪mycc -l node -v 1.0 -c '{"Args":["init","a", "100", "b","200"]}' -P "AND ('Org1MSP.
↪peer','Org2MSP.peer')"
```

Java

Note: Please note, Java chaincode instantiation might take time as it compiles chaincode and downloads docker container with java environment.

```
peer chaincode instantiate -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪mycc -l java -v 1.0 -c '{"Args":["init","a", "100", "b","200"]}' -P "AND ('Org1MSP.
↪peer','Org2MSP.peer')"
```

See the endorsement policies documentation for more details on policy implementation.

If you want additional peers to interact with ledger, then you will need to join them to the channel, and install the same name, version and language of the chaincode source onto the appropriate peer's filesystem. A chaincode container will be launched for each peer as soon as they try to interact with that specific chaincode. Again, be cognizant of the fact that the Node.js images will be slower to compile.

Once the chaincode has been instantiated on the channel, we can forgo the `-l` flag. We need only pass in the channel identifier and name of the chaincode.

Query

Let's query for the value of `a` to make sure the chaincode was properly instantiated and the state DB was populated. The syntax for query is as follows:

```
# be sure to set the -C and -n flags appropriately

peer chaincode query -C $CHANNEL_NAME -n mycc -c '{"Args":["query","a"]}'
```

Invoke

Now let's move `10` from `a` to `b`. This transaction will cut a new block and update the state DB. The syntax for invoke is as follows:

```
# be sure to set the -C and -n flags appropriately

peer chaincode invoke -o orderer.example.com:7050 --tls true --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪mycc --peerAddresses peer0.org1.example.com:7051 --tlsRootCertFiles /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.example.com/peers/
↪peer0.org1.example.com/tls/ca.crt --peerAddresses peer0.org2.example.com:7051 --
↪tlsRootCertFiles /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt -c '{
↪"Args":["invoke","a","b","10"]}'
```

Query

Let's confirm that our previous invocation executed properly. We initialized the key `a` with a value of `100` and just removed `10` with our previous invocation. Therefore, a query against `a` should reveal `90`. The syntax for query is as follows.

```
# be sure to set the -C and -n flags appropriately

peer chaincode query -C $CHANNEL_NAME -n mycc -c '{"Args":["query","a"]}'
```

We should see the following:

```
Query Result: 90
```

Feel free to start over and manipulate the key value pairs and subsequent invocations.

What's happening behind the scenes?

Note: These steps describe the scenario in which `script.sh` is run by './byfn.sh up'. Clean your network with `./byfn.sh down` and ensure this command is active. Then use the same docker-compose prompt to launch your network again

---

- A script - `script.sh` - is baked inside the CLI container. The script drives the `createChannel` command against the supplied channel name and uses the channel.tx file for channel configuration.

- The output of `createChannel` is a genesis block - `<your_channel_name>.block` - which gets stored on the peers' file systems and contains the channel configuration specified from channel.tx.
- The `joinChannel` command is exercised for all four peers, which takes as input the previously generated genesis block. This command instructs the peers to join `<your_channel_name>` and create a chain starting with `<your_channel_name>.block`.
- Now we have a channel consisting of four peers, and two organizations. This is our `TwoOrgsChannel` profile.
- `peer0.org1.example.com` and `peer1.org1.example.com` belong to Org1; `peer0.org2.example.com` and `peer1.org2.example.com` belong to Org2
- These relationships are defined through the `crypto-config.yaml` and the MSP path is specified in our docker compose.
- The anchor peers for Org1MSP (`peer0.org1.example.com`) and Org2MSP (`peer0.org2.example.com`) are then updated. We do this by passing the `Org1MSPanchors.tx` and `Org2MSPanchors.tx` artifacts to the ordering service along with the name of our channel.
- A chaincode - **chaincode_example02** - is installed on `peer0.org1.example.com` and `peer0.org2.example.com`
- The chaincode is then "instantiated" on `peer0.org2.example.com`. Instantiation adds the chaincode to the channel, starts the container for the target peer, and initializes the key value pairs associated with the chaincode. The initial values for this example are ["a","100" "b","200"]. This "instantiation" results in a container by the name of `dev-peer0.org2.example.com-mycc-1.0` starting.
- The instantiation also passes in an argument for the endorsement policy. The policy is defined as `-P "AND ('Org1MSP.peer','Org2MSP.peer')"`, meaning that any transaction must be endorsed by a peer tied to Org1 and Org2.
- A query against the value of "a" is issued to `peer0.org1.example.com`. The chaincode was previously installed on `peer0.org1.example.com`, so this will start a container for Org1 peer0 by the name of `dev-peer0.org1.example.com-mycc-1.0`. The result of the query is also returned. No write operations have occurred, so a query against "a" will still return a value of "100".
- An invoke is sent to `peer0.org1.example.com` to move "10" from "a" to "b"
- The chaincode is then installed on `peer1.org2.example.com`
- A query is sent to `peer1.org2.example.com` for the value of "a". This starts a third chaincode container by the name of `dev-peer1.org2.example.com-mycc-1.0`. A value of 90 is returned, correctly reflecting the previous transaction during which the value for key "a" was modified by 10.

What does this demonstrate?

Chaincode **MUST** be installed on a peer in order for it to successfully perform read/write operations against the ledger. Furthermore, a chaincode container is not started for a peer until an `init` or traditional transaction - read/write - is performed against that chaincode (e.g. query for the value of "a"). The transaction causes the container to start. Also, all peers in a channel maintain an exact copy of the ledger which comprises the blockchain to store the immutable, sequenced record in blocks, as well as a state database to maintain a snapshot of the current state. This includes those peers that do not have chaincode installed on them (like `peer1.org1.example.com` in the above example) . Finally, the chaincode is accessible after it is installed (like `peer1.org2.example.com` in the above example) because it has already been instantiated.

How do I see these transactions?

Check the logs for the CLI Docker container.

```
docker logs -f cli
```

You should see the following output:

```
2017-05-16 17:08:01.366 UTC [msp] GetLocalMSP -> DEBU 004 Returning existing local MSP
2017-05-16 17:08:01.366 UTC [msp] GetDefaultSigningIdentity -> DEBU 005 Obtaining␣
↪default signing identity
2017-05-16 17:08:01.366 UTC [msp/identity] Sign -> DEBU 006 Sign: plaintext:␣
↪0AB1070A6708031A0C08F1E3ECC80510...6D7963631A0A0A0571756572790A0161
2017-05-16 17:08:01.367 UTC [msp/identity] Sign -> DEBU 007 Sign: digest:␣
↪E61DB37F4E8B0D32C9FE10E3936BA9B8CD278FAA1F3320B08712164248285C54
Query Result: 90
2017-05-16 17:08:15.158 UTC [main] main -> INFO 008 Exiting.....
===================== Query successful on peer1.org2 on channel 'mychannel'␣
↪=====================

===================== All GOOD, BYFN execution completed =====================


 _____   _   _   ____
| ____| | \ | | |  _ \
|  _|   |  \| | | | | |
| |___  | |\  | | |_| |
|_____| |_| \_| |____/
```

You can scroll through these logs to see the various transactions.

How can I see the chaincode logs?

Inspect the individual chaincode containers to see the separate transactions executed against each container. Here is the combined output from each container:

```
$ docker logs dev-peer0.org2.example.com-mycc-1.0
04:30:45.947 [BCCSP_FACTORY] DEBU : Initialize BCCSP [SW]
ex02 Init
Aval = 100, Bval = 200

$ docker logs dev-peer0.org1.example.com-mycc-1.0
04:31:10.569 [BCCSP_FACTORY] DEBU : Initialize BCCSP [SW]
ex02 Invoke
Query Response:{"Name":"a","Amount":"100"}
ex02 Invoke
Aval = 90, Bval = 210

$ docker logs dev-peer1.org2.example.com-mycc-1.0
04:31:30.420 [BCCSP_FACTORY] DEBU : Initialize BCCSP [SW]
ex02 Invoke
Query Response:{"Name":"a","Amount":"90"}
```

6.2.7 Understanding the Docker Compose topology

The BYFN sample offers us two flavors of Docker Compose files, both of which are extended from the `docker-compose-base.yaml` (located in the `base` folder). Our first flavor, `docker-compose-cli.yaml`, provides us with a CLI container, along with an orderer, four peers. We use this file for the entirety of the instructions on this page.

Note: the remainder of this section covers a docker-compose file designed for the SDK. Refer to the Node SDK repo for details on running these tests.

The second flavor, `docker-compose-e2e.yaml`, is constructed to run end-to-end tests using the Node.js SDK. Aside from functioning with the SDK, its primary differentiation is that there are containers for the fabric-ca servers. As a result, we are able to send REST calls to the organizational CAs for user registration and enrollment.

If you want to use the `docker-compose-e2e.yaml` without first running the byfn.sh script, then we will need to make four slight modifications. We need to point to the private keys for our Organization's CA's. You can locate these values in your crypto-config folder. For example, to locate the private key for Org1 we would follow this path - `crypto-config/peerOrganizations/org1.example.com/ca/`. The private key is a long hash value followed by `_sk`. The path for Org2 would be - `crypto-config/peerOrganizations/org2.example.com/ca/`.

In the `docker-compose-e2e.yaml` update the FABRIC_CA_SERVER_TLS_KEYFILE variable for ca0 and ca1. You also need to edit the path that is provided in the command to start the ca server. You are providing the same private key twice for each CA container.

6.2.8 Using CouchDB

The state database can be switched from the default (goleveldb) to CouchDB. The same chaincode functions are available with CouchDB, however, there is the added ability to perform rich and complex queries against the state database data content contingent upon the chaincode data being modeled as JSON.

To use CouchDB instead of the default database (goleveldb), follow the same procedures outlined earlier for generating the artifacts, except when starting the network pass `docker-compose-couch.yaml` as well:

```
docker-compose -f docker-compose-cli.yaml -f docker-compose-couch.yaml up -d
```

chaincode_example02 should now work using CouchDB underneath.

Note: If you choose to implement mapping of the fabric-couchdb container port to a host port, please make sure you are aware of the security implications. Mapping of the port in a development environment makes the CouchDB REST API available, and allows the visualization of the database via the CouchDB web interface (Fauxton). Production environments would likely refrain from implementing port mapping in order to restrict outside access to the CouchDB containers.

You can use **chaincode_example02** chaincode against the CouchDB state database using the steps outlined above, however in order to exercise the CouchDB query capabilities you will need to use a chaincode that has data modeled as JSON, (e.g. **marbles02**). You can locate the **marbles02** chaincode in the `fabric/examples/chaincode/go` directory.

We will follow the same process to create and join the channel as outlined in the *Create & Join Channel* section above. Once you have joined your peer(s) to the channel, use the following steps to interact with the **marbles02** chaincode:

- Install and instantiate the chaincode on `peer0.org1.example.com`:

```
# be sure to modify the $CHANNEL_NAME variable accordingly for the instantiate command

peer chaincode install -n marbles -v 1.0 -p github.com/chaincode/marbles02/go
peer chaincode instantiate -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -v 1.0 -c '{"Args":["init"]}' -P "OR ('Org0MSP.peer','Org1MSP.peer')"
```

- Create some marbles and move them around:

```
# be sure to modify the $CHANNEL_NAME variable accordingly

peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -c '{"Args":["initMarble","marble1","blue","35","tom"]}'
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -c '{"Args":["initMarble","marble2","red","50","tom"]}'
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -c '{"Args":["initMarble","marble3","blue","70","tom"]}'
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -c '{"Args":["transferMarble","marble2","jerry"]}'
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -c '{"Args":["transferMarblesBasedOnColor","blue","jerry"]}'
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -c '{"Args":["delete","marble1"]}'
```

- If you chose to map the CouchDB ports in docker-compose, you can now view the state database through the CouchDB web interface (Fauxton) by opening a browser and navigating to the following URL:

  `http://localhost:5984/_utils`

You should see a database named `mychannel` (or your unique channel name) and the documents inside it.

Note: For the below commands, be sure to update the $CHANNEL_NAME variable appropriately.

You can run regular queries from the CLI (e.g. reading `marble2`):

```
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":["readMarble","marble2"]}
↪'
```

The output should display the details of `marble2`:

```
Query Result: {"color":"red","docType":"marble","name":"marble2","owner":"jerry","size
↪":50}
```

You can retrieve the history of a specific marble - e.g. `marble1`:

```
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":["getHistoryForMarble",
↪"marble1"]}'
```

The output should display the transactions on `marble1`:

```
Query Result: [{"TxId":
↪"1c3d3caf124c89f91a4c0f353723ac736c58155325f02890adebaa15e16e6464", "Value":{
↪"docType":"marble","name":"marble1","color":"blue","size":35,"owner":"tom"}},{"TxId
↪":"755d55c281889eaeebf405586f9e25d71d36eb3d35420af833a20a2f53a3eefd", "Value":{
↪"docType":"marble","name":"marble1","color":"blue","size":35,"owner":"jerry"}},{
↪"TxId":"81945102d813dde6147f85e56a89262555e04f14788ee33e28b232eef36d98f", "Value":{}
↪]
```

(continues on next page)

(continued from previous page)

You can also perform rich queries on the data content, such as querying marble fields by owner `jerry`:

```
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":["queryMarblesByOwner",
↪"jerry"]}'
```

The output should display the two marbles owned by `jerry`:

```
Query Result: [{"Key":"marble2", "Record":{"color":"red","docType":"marble","name":
↪"marble2","owner":"jerry","size":50}},{"Key":"marble3", "Record":{"color":"blue",
↪"docType":"marble","name":"marble3","owner":"jerry","size":70}}]
```

6.2.9 Why CouchDB

CouchDB is a kind of NoSQL solution. It is a document-oriented database where document fields are stored as key-value maps. Fields can be either a simple key-value pair, list, or map. In addition to keyed/composite-key/key-range queries which are supported by LevelDB, CouchDB also supports full data rich queries capability, such as non-key queries against the whole blockchain data, since its data content is stored in JSON format and fully queryable. Therefore, CouchDB can meet chaincode, auditing, reporting requirements for many use cases that not supported by LevelDB.

CouchDB can also enhance the security for compliance and data protection in the blockchain. As it is able to implement field-level security through the filtering and masking of individual attributes within a transaction, and only authorizing the read-only permission if needed.

In addition, CouchDB falls into the AP-type (Availability and Partition Tolerance) of the CAP theorem. It uses a master-master replication model with `Eventual Consistency`. More information can be found on the Eventual Consistency page of the CouchDB documentation. However, under each fabric peer, there is no database replicas, writes to database are guaranteed consistent and durable (not `Eventual Consistency`).

CouchDB is the first external pluggable state database for Fabric, and there could and should be other external database options. For example, IBM enables the relational database for its blockchain. And the CP-type (Consistency and Partition Tolerance) databases may also in need, so as to enable data consistency without application level guarantee.

6.2.10 A Note on Data Persistence

If data persistence is desired on the peer container or the CouchDB container, one option is to mount a directory in the docker-host into a relevant directory in the container. For example, you may add the following two lines in the peer container specification in the `docker-compose-base.yaml` file:

```
volumes:
 - /var/hyperledger/peer0:/var/hyperledger/production
```

For the CouchDB container, you may add the following two lines in the CouchDB container specification:

```
volumes:
 - /var/hyperledger/couchdb0:/opt/couchdb/data
```

6.2.11 Troubleshooting

- Always start your network fresh. Use the following command to remove artifacts, crypto, containers and chaincode images:

```
./byfn.sh down
```

Note: You **will** see errors if you do not remove old containers and images.

- If you see Docker errors, first check your docker version (*Prerequisites*), and then try restarting your Docker process. Problems with Docker are oftentimes not immediately recognizable. For example, you may see errors resulting from an inability to access crypto material mounted within a container.

  If they persist remove your images and start from scratch:

```
docker rm -f $(docker ps -aq)
docker rmi -f $(docker images -q)
```

- If you see errors on your create, instantiate, invoke or query commands, make sure you have properly updated the channel name and chaincode name. There are placeholder values in the supplied sample commands.
- If you see the below error:

```
Error: Error endorsing chaincode: rpc error: code = 2 desc = Error installing␣
↪chaincode code mycc:1.0(chaincode /var/hyperledger/production/chaincodes/mycc.1.
↪0 exits)
```

  You likely have chaincode images (e.g. `dev-peer1.org2.example.com-mycc-1.0` or `dev-peer0.org1.example.com-mycc-1.0`) from prior runs. Remove them and try again.

```
docker rmi -f $(docker images | grep peer[0-9]-peer[0-9] | awk '{print $3}')
```

- If you see something similar to the following:

```
Error connecting: rpc error: code = 14 desc = grpc: RPC failed fast due to␣
↪transport failure
Error: rpc error: code = 14 desc = grpc: RPC failed fast due to transport failure
```

  Make sure you are running your network against the "1.0.0" images that have been retagged as "latest".

- If you see the below error:

```
[configtx/tool/localconfig] Load -> CRIT 002 Error reading configuration:␣
↪Unsupported Config Type ""
panic: Error reading configuration: Unsupported Config Type ""
```

  Then you did not set the `FABRIC_CFG_PATH` environment variable properly. The configtxgen tool needs this variable in order to locate the configtx.yaml. Go back and execute an `export FABRIC_CFG_PATH=$PWD`, then recreate your channel artifacts.

- To cleanup the network, use the `down` option:

```
./byfn.sh down
```

- If you see an error stating that you still have "active endpoints", then prune your Docker networks. This will wipe your previous networks and start you with a fresh environment:

```
docker network prune
```

  You will see the following message:

```
WARNING! This will remove all networks not used by at least one container.
Are you sure you want to continue? [y/N]
```

Select `y`.

- If you see an error similar to the following:

```
/bin/bash: ./scripts/script.sh: /bin/bash^M: bad interpreter: No such file or␣
↪directory
```

Ensure that the file in question (**script.sh** in this example) is encoded in the Unix format. This was most likely caused by not setting `core.autocrlf` to `false` in your Git configuration (see *Windows extras*). There are several ways of fixing this. If you have access to the vim editor for instance, open the file:

```
vim ./fabric-samples/first-network/scripts/script.sh
```

Then change its format by executing the following vim command:

```
:set ff=unix
```

Note: If you continue to see errors, share your logs on the **fabric-questions** channel on Hyperledger Rocket Chat or on StackOverflow.

6.3 Adding an Org to a Channel

Note: Ensure that you have downloaded the appropriate images and binaries as outlined in *Install Samples, Binaries and Docker Images* and *Prerequisites* that conform to the version of this documentation (which can be found at the bottom of the table of contents to the left). In particular, your version of the `fabric-samples` folder must include the `eyfn.sh` ("Extending Your First Network") script and its related scripts.

This tutorial serves as an extension to the *Building Your First Network* (BYFN) tutorial, and will demonstrate the addition of a new organization – `Org3` – to the application channel (`mychannel`) autogenerated by BYFN. It assumes a strong understanding of BYFN, including the usage and functionality of the aforementioned utilities.

While we will focus solely on the integration of a new organization here, the same approach can be adopted when performing other channel configuration updates (updating modification policies or altering batch size, for example). To learn more about the process and possibilities of channel config updates in general, check out *Updating a Channel Configuration*). It's also worth noting that channel configuration updates like the one demonstrated here will usually be the responsibility of an organization admin (rather than a chaincode or application developer).

Note: Make sure the automated `byfn.sh` script runs without error on your machine before continuing. If you have exported your binaries and the related tools (`cryptogen`, `configtxgen`, etc) into your PATH variable, you'll be able to modify the commands accordingly without passing the fully qualified path.

6.3.1 Setup the Environment

We will be operating from the root of the `first-network` subdirectory within your local clone of `fabric-samples`. Change into that directory now. You will also want to open a few extra terminals for ease

of use.

First, use the `byfn.sh` script to tidy up. This command will kill any active or stale docker containers and remove previously generated artifacts. It is by no means **necessary** to bring down a Fabric network in order to perform channel configuration update tasks. However, for the sake of this tutorial, we want to operate from a known initial state. Therefore let's run the following command to clean up any previous environments:

```
./byfn.sh down
```

Now generate the default BYFN artifacts:

```
./byfn.sh generate
```

And launch the network making use of the scripted execution within the CLI container:

```
./byfn.sh up
```

Now that you have a clean version of BYFN running on your machine, you have two different paths you can pursue. First, we offer a fully commented script that will carry out a config transaction update to bring Org3 into the network.

Also, we will show a "manual" version of the same process, showing each step and explaining what it accomplishes (since we show you how to bring down your network before this manual process, you could also run the script and then look at each step).

6.3.2 Bring Org3 into the Channel with the Script

You should be in `first-network`. To use the script, simply issue the following:

```
./eyfn.sh up
```

The output here is well worth reading. You'll see the Org3 crypto material being added, the config update being created and signed, and then chaincode being installed to allow Org3 to execute ledger queries.

If everything goes well, you'll get this message:

```
========= All GOOD, EYFN test execution completed ===========
```

`eyfn.sh` can be used with the same Node.js chaincode and database options as `byfn.sh` by issuing the following (instead of `./byfn.sh up`):

```
./byfn.sh up -c testchannel -s couchdb -l node
```

And then:

```
./eyfn.sh up -c testchannel -s couchdb -l node
```

For those who want to take a closer look at this process, the rest of the doc will show you each command for making a channel update and what it does.

6.3.3 Bring Org3 into the Channel Manually

Note: The manual steps outlined below assume that the `CORE_LOGGING_LEVEL` in the `cli` and *Org3cli'* containers is set to `DEBUG`.

For the `cli` container, you can set this by modifying the `docker-compose-cli.yaml` file in the `first-network` directory. e.g.

```
cli:
  container_name: cli
  image: hyperledger/fabric-tools:$IMAGE_TAG
  tty: true
  stdin_open: true
  environment:
    - GOPATH=/opt/gopath
    - CORE_VM_ENDPOINT=unix:///host/var/run/docker.sock
    #- CORE_LOGGING_LEVEL=INFO
    - CORE_LOGGING_LEVEL=DEBUG
```

For the `Org3cli` container, you can set this by modifying the `docker-compose-org3.yaml` file in the `first-network` directory. e.g.

```
Org3cli:
  container_name: Org3cli
  image: hyperledger/fabric-tools:$IMAGE_TAG
  tty: true
  stdin_open: true
  environment:
    - GOPATH=/opt/gopath
    - CORE_VM_ENDPOINT=unix:///host/var/run/docker.sock
    #- CORE_LOGGING_LEVEL=INFO
    - CORE_LOGGING_LEVEL=DEBUG
```

If you've used the `eyfn.sh` script, you'll need to bring your network down. This can be done by issuing:

```
./eyfn.sh down
```

This will bring down the network, delete all the containers and undo what we've done to add Org3.

When the network is down, bring it back up again.

```
./byfn.sh generate
```

Then:

```
./byfn.sh up
```

This will bring your network back to the same state it was in before you executed the `eyfn.sh` script.

Now we're ready to add Org3 manually. As a first step, we'll need to generate Org3's crypto material.

6.3.4 Generate the Org3 Crypto Material

In another terminal, change into the `org3-artifacts` subdirectory from `first-network`.

```
cd org3-artifacts
```

There are two `yaml` files of interest here: `org3-crypto.yaml` and `configtx.yaml`. First, generate the crypto material for Org3:

```
../../bin/cryptogen generate --config=./org3-crypto.yaml
```

This command reads in our new crypto `yaml` file – `org3-crypto.yaml` – and leverages `cryptogen` to generate the keys and certificates for an Org3 CA as well as two peers bound to this new Org. As with the BYFN implementation, this crypto material is put into a newly generated `crypto-config` folder within the present working directory (in our case, `org3-artifacts`).

Now use the `configtxgen` utility to print out the Org3-specific configuration material in JSON. We will preface the command by telling the tool to look in the current directory for the `configtx.yaml` file that it needs to ingest.

```
export FABRIC_CFG_PATH=$PWD && ../../bin/configtxgen -printOrg Org3MSP > ../channel-
↪artifacts/org3.json
```

The above command creates a JSON file – `org3.json` – and outputs it into the `channel-artifacts` subdirectory at the root of `first-network`. This file contains the policy definitions for Org3, as well as three important certificates presented in base 64 format: the admin user certificate (which will be needed to act as the admin of Org3 later on), a CA root cert, and a TLS root cert. In an upcoming step we will append this JSON file to the channel configuration.

Our final piece of housekeeping is to port the Orderer Org's MSP material into the Org3 `crypto-config` directory. In particular, we are concerned with the Orderer's TLS root cert, which will allow for secure communication between Org3 entities and the network's ordering node.

```
cd ../ && cp -r crypto-config/ordererOrganizations org3-artifacts/crypto-config/
```

Now we're ready to update the channel configuration...

6.3.5 Prepare the CLI Environment

The update process makes use of the configuration translator tool – `configtxlator`. This tool provides a stateless REST API independent of the SDK. Additionally it provides a CLI, to simplify configuration tasks in Fabric networks. The tool allows for the easy conversion between different equivalent data representations/formats (in this case, between protobufs and JSON). Additionally, the tool can compute a configuration update transaction based on the differences between two channel configurations.

First, exec into the CLI container. Recall that this container has been mounted with the BYFN `crypto-config` library, giving us access to the MSP material for the two original peer organizations and the Orderer Org. The bootstrapped identity is the Org1 admin user, meaning that any steps where we want to act as Org2 will require the export of MSP-specific environment variables.

```
docker exec -it cli bash
```

Export the `ORDERER_CA` and `CHANNEL_NAME` variables:

```
export ORDERER_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.
↪example.com-cert.pem  && export CHANNEL_NAME=mychannel
```

Check to make sure the variables have been properly set:

```
echo $ORDERER_CA && echo $CHANNEL_NAME
```

Note: If for any reason you need to restart the CLI container, you will also need to re-export the two environment variables – `ORDERER_CA` and `CHANNEL_NAME`.

6.3.6 Fetch the Configuration

Now we have a CLI container with our two key environment variables – `ORDERER_CA` and `CHANNEL_NAME` exported. Let's go fetch the most recent config block for the channel – `mychannel`.

The reason why we have to pull the latest version of the config is because channel config elements are versioned.. Versioning is important for several reasons. It prevents config changes from being repeated or replayed (for instance, reverting to a channel config with old CRLs would represent a security risk). Also it helps ensure concurrency (if you want to remove an Org from your channel, for example, after a new Org has been added, versioning will help prevent you from removing both Orgs, instead of just the Org you want to remove).

```
peer channel fetch config config_block.pb -o orderer.example.com:7050 -c $CHANNEL_
↪NAME --tls --cafile $ORDERER_CA
```

This command saves the binary protobuf channel configuration block to `config_block.pb`. Note that the choice of name and file extension is arbitrary. However, following a convention which identifies both the type of object being represented and its encoding (protobuf or JSON) is recommended.

When you issued the `peer channel fetch` command, there was a decent amount of output in the terminal. The last line in the logs is of interest:

```
2017-11-07 17:17:57.383 UTC [channelCmd] readBlock -> DEBU 011 Received block: 2
```

This is telling us that the most recent configuration block for `mychannel` is actually block 2, **NOT** the genesis block. By default, the `peer channel fetch config` command returns the most **recent** configuration block for the targeted channel, which in this case is the third block. This is because the BYFN script defined anchor peers for our two organizations – `Org1` and `Org2` – in two separate channel update transactions.

As a result, we have the following configuration sequence:

- block 0: genesis block
- block 1: Org1 anchor peer update
- block 2: Org2 anchor peer update

6.3.7 Convert the Configuration to JSON and Trim It Down

Now we will make use of the `configtxlator` tool to decode this channel configuration block into JSON format (which can be read and modified by humans). We also must strip away all of the headers, metadata, creator signatures, and so on that are irrelevant to the change we want to make. We accomplish this by means of the `jq` tool:

```
configtxlator proto_decode --input config_block.pb --type common.Block | jq .data.
↪data[0].payload.data.config > config.json
```

This leaves us with a trimmed down JSON object – `config.json`, located in the `fabric-samples` folder inside `first-network` – which will serve as the baseline for our config update.

Take a moment to open this file inside your text editor of choice (or in your browser). Even after you're done with this tutorial, it will be worth studying it as it reveals the underlying configuration structure and the other kind of channel updates that can be made. We discuss them in more detail in *Updating a Channel Configuration*.

6.3.8 Add the Org3 Crypto Material

Note: The steps you've taken up to this point will be nearly identical no matter what kind of config update you're trying to make. We've chosen to add an org with this tutorial because it's one of the most complex channel configuration updates you can attempt.

We'll use the `jq` tool once more to append the Org3 configuration definition – `org3.json` – to the channel's application groups field, and name the output – `modified_config.json`.

```
jq -s '.[0] * {"channel_group":{"groups":{"Application":{"groups": {"Org3MSP":.[1]}}}}
↪}' config.json ./channel-artifacts/org3.json > modified_config.json
```

Now, within the CLI container we have two JSON files of interest – `config.json` and `modified_config.json`. The initial file contains only Org1 and Org2 material, whereas "modified" file contains all three Orgs. At this point it's simply a matter of re-encoding these two JSON files and calculating the delta.

First, translate `config.json` back into a protobuf called `config.pb`:

```
configtxlator proto_encode --input config.json --type common.Config --output config.pb
```

Next, encode `modified_config.json` to `modified_config.pb`:

```
configtxlator proto_encode --input modified_config.json --type common.Config --output␣
↪modified_config.pb
```

Now use `configtxlator` to calculate the delta between these two config protobufs. This command will output a new protobuf binary named `org3_update.pb`:

```
configtxlator compute_update --channel_id $CHANNEL_NAME --original config.pb --
↪updated modified_config.pb --output org3_update.pb
```

This new proto – `org3_update.pb` – contains the Org3 definitions and high level pointers to the Org1 and Org2 material. We are able to forgo the extensive MSP material and modification policy information for Org1 and Org2 because this data is already present within the channel's genesis block. As such, we only need the delta between the two configurations.

Before submitting the channel update, we need to perform a few final steps. First, let's decode this object into editable JSON format and call it `org3_update.json`:

```
configtxlator proto_decode --input org3_update.pb --type common.ConfigUpdate | jq . >␣
↪org3_update.json
```

Now, we have a decoded update file – `org3_update.json` – that we need to wrap in an envelope message. This step will give us back the header field that we stripped away earlier. We'll name this file `org3_update_in_envelope.json`:

```
echo '{"payload":{"header":{"channel_header":{"channel_id":"mychannel", "type":2}},
↪"data":{"config_update":'$(cat org3_update.json)'}}}' | jq . > org3_update_in_
↪envelope.json
```

Using our properly formed JSON – `org3_update_in_envelope.json` – we will leverage the `configtxlator` tool one last time and convert it into the fully fledged protobuf format that Fabric requires. We'll name our final update object `org3_update_in_envelope.pb`:

```
configtxlator proto_encode --input org3_update_in_envelope.json --type common.
↪Envelope --output org3_update_in_envelope.pb
```

6.3.9 Sign and Submit the Config Update

Almost done!

We now have a protobuf binary – `org3_update_in_envelope.pb` – within our CLI container. However, we need signatures from the requisite Admin users before the config can be written to the ledger. The modification policy (mod_policy) for our channel Application group is set to the default of "MAJORITY", which means that we need a majority of existing org admins to sign it. Because we have only two orgs – Org1 and Org2 – and the majority of two is two, we need both of them to sign. Without both signatures, the ordering service will reject the transaction for failing to fulfill the policy.

First, let's sign this update proto as the Org1 Admin. Remember that the CLI container is bootstrapped with the Org1 MSP material, so we simply need to issue the `peer channel signconfigtx` command:

```
peer channel signconfigtx -f org3_update_in_envelope.pb
```

The final step is to switch the CLI container's identity to reflect the Org2 Admin user. We do this by exporting four environment variables specific to the Org2 MSP.

Note: Switching between organizations to sign a config transaction (or to do anything else) is not reflective of a real-world Fabric operation. A single container would never be mounted with an entire network's crypto material. Rather, the config update would need to be securely passed out-of-band to an Org2 Admin for inspection and approval.

Export the Org2 environment variables:

```
# you can issue all of these commands at once

export CORE_PEER_LOCALMSPID="Org2MSP"

export CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt

export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp

export CORE_PEER_ADDRESS=peer0.org2.example.com:7051
```

Lastly, we will issue the `peer channel update` command. The Org2 Admin signature will be attached to this call so there is no need to manually sign the protobuf a second time:

Note: The upcoming update call to the ordering service will undergo a series of systematic signature and policy checks. As such you may find it useful to stream and inspect the ordering node's logs. From another shell, issue a `docker logs -f orderer.example.com` command to display them.

Send the update call:

```
peer channel update -f org3_update_in_envelope.pb -c $CHANNEL_NAME -o orderer.example.
↪com:7050 --tls --cafile $ORDERER_CA
```

You should see a message digest indication similar to the following if your update has been submitted successfully:

```
2018-02-24 18:56:33.499 UTC [msp/identity] Sign -> DEBU 00f Sign: digest:␣
↪3207B24E40DE2FAB87A2E42BC004FEAA1E6FDCA42977CB78C64F05A88E556ABA
```

You will also see the submission of our configuration transaction:

```
2018-02-24 18:56:33.499 UTC [channelCmd] update -> INFO 010 Successfully submitted␣
↪channel update
```

The successful channel update call returns a new block – block 5 – to all of the peers on the channel. If you remember, blocks 0-2 are the initial channel configurations while blocks 3 and 4 are the instantiation and invocation of the `mycc` chaincode. As such, block 5 serves as the most recent channel configuration with Org3 now defined on the channel.

Inspect the logs for `peer0.org1.example.com`:

```
docker logs -f peer0.org1.example.com
```

Follow the demonstrated process to fetch and decode the new config block if you wish to inspect its contents.

6.3.10 Configuring Leader Election

Note: This section is included as a general reference for understanding the leader election settings when adding organizations to a network after the initial channel configuration has completed. This sample defaults to dynamic leader election, which is set for all peers in the network in *peer-base.yaml*.

Newly joining peers are bootstrapped with the genesis block, which does not contain information about the organization that is being added in the channel configuration update. Therefore new peers are not able to utilize gossip as they cannot verify blocks forwarded by other peers from their own organization until they get the configuration transaction which added the organization to the channel. Newly added peers must therefore have one of the following configurations so that they receive blocks from the ordering service:

1. To utilize static leader mode, configure the peer to be an organization leader:

```
CORE_PEER_GOSSIP_USELEADERELECTION=false
CORE_PEER_GOSSIP_ORGLEADER=true
```

Note: This configuration must be the same for all new peers added to the channel.

---

2. To utilize dynamic leader election, configure the peer to use leader election:

```
CORE_PEER_GOSSIP_USELEADERELECTION=true
CORE_PEER_GOSSIP_ORGLEADER=false
```

Note: Because peers of the newly added organization won't be able to form membership view, this option will be similar to the static configuration, as each peer will start proclaiming itself to be a leader. However, once they get updated with the configuration transaction that adds the organization to the channel, there will be only one active leader for the organization. Therefore, it is recommended to leverage this option if you eventually want the organization's peers to utilize leader election.

6.3.11 Join Org3 to the Channel

At this point, the channel configuration has been updated to include our new organization – `Org3` – meaning that peers attached to it can now join `mychannel`.

First, let's launch the containers for the Org3 peers and an Org3-specific CLI.

Open a new terminal and from `first-network` kick off the Org3 docker compose:

```
docker-compose -f docker-compose-org3.yaml up -d
```

This new compose file has been configured to bridge across our initial network, so the two peers and the CLI container will be able to resolve with the existing peers and ordering node. With the three new containers now running, exec into the Org3-specific CLI container:

```
docker exec -it Org3cli bash
```

Just as we did with the initial CLI container, export the two key environment variables: `ORDERER_CA` and `CHANNEL_NAME`:

```
export ORDERER_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.
↪example.com-cert.pem && export CHANNEL_NAME=mychannel
```

Check to make sure the variables have been properly set:

```
echo $ORDERER_CA && echo $CHANNEL_NAME
```

Now let's send a call to the ordering service asking for the genesis block of `mychannel`. The ordering service is able to verify the Org3 signature attached to this call as a result of our successful channel update. If Org3 has not been successfully appended to the channel config, the ordering service should reject this request.

Note: Again, you may find it useful to stream the ordering node's logs to reveal the sign/verify logic and policy checks.

Use the `peer channel fetch` command to retrieve this block:

```
peer channel fetch 0 mychannel.block -o orderer.example.com:7050 -c $CHANNEL_NAME --
↪tls --cafile $ORDERER_CA
```

Notice, that we are passing a `0` to indicate that we want the first block on the channel's ledger (i.e. the genesis block). If we simply passed the `peer channel fetch config` command, then we would have received block 5 – the updated config with Org3 defined. However, we can't begin our ledger with a downstream block – we must start with block 0.

Issue the `peer channel join` command and pass in the genesis block – `mychannel.block`:

```
peer channel join -b mychannel.block
```

If you want to join the second peer for Org3, export the `TLS` and `ADDRESS` variables and reissue the `peer channel join command`:

```
export CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org3.example.com/peers/peer1.org3.example.com/tls/ca.crt &&
↪ export CORE_PEER_ADDRESS=peer1.org3.example.com:7051

peer channel join -b mychannel.block
```

6.3.12 Upgrade and Invoke Chaincode

The final piece of the puzzle is to increment the chaincode version and update the endorsement policy to include Org3. Since we know that an upgrade is coming, we can forgo the futile exercise of installing version 1 of the chaincode.

We are solely concerned with the new version where Org3 will be part of the endorsement policy, therefore we'll jump directly to version 2 of the chaincode.

From the Org3 CLI:

```
peer chaincode install -n mycc -v 2.0 -p github.com/chaincode/chaincode_example02/go/
```

Modify the environment variables accordingly and reissue the command if you want to install the chaincode on the second peer of Org3. Note that a second installation is not mandated, as you only need to install chaincode on peers that are going to serve as endorsers or otherwise interface with the ledger (i.e. query only). Peers will still run the validation logic and serve as committers without a running chaincode container.

Now jump back to the **original** CLI container and install the new version on the Org1 and Org2 peers. We submitted the channel update call with the Org2 admin identity, so the container is still acting on behalf of `peer0.org2`:

```
peer chaincode install -n mycc -v 2.0 -p github.com/chaincode/chaincode_example02/go/
```

Flip to the `peer0.org1` identity:

```
export CORE_PEER_LOCALMSPID="Org1MSP"

export CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt

export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp

export CORE_PEER_ADDRESS=peer0.org1.example.com:7051
```

And install again:

```
peer chaincode install -n mycc -v 2.0 -p github.com/chaincode/chaincode_example02/go/
```

Now we're ready to upgrade the chaincode. There have been no modifications to the underlying source code, we are simply adding Org3 to the endorsement policy for a chaincode – `mycc` – on `mychannel`.

Note: Any identity satisfying the chaincode's instantiation policy can issue the upgrade call. By default, these identities are the channel Admins.

Send the call:

```
peer chaincode upgrade -o orderer.example.com:7050 --tls $CORE_PEER_TLS_ENABLED --
↪cafile $ORDERER_CA -C $CHANNEL_NAME -n mycc -v 2.0 -c '{"Args":["init","a","90","b",
↪"210"]}' -P "OR ('Org1MSP.peer','Org2MSP.peer','Org3MSP.peer')"
```

You can see in the above command that we are specifying our new version by means of the `v` flag. You can also see that the endorsement policy has been modified to `-P "OR ('Org1MSP.peer','Org2MSP.peer','Org3MSP.peer')"`, reflecting the addition of Org3 to the policy. The final area of interest is our constructor request (specified with the `c` flag).

As with an instantiate call, a chaincode upgrade requires usage of the `init` method. **If** your chaincode requires arguments be passed to the `init` method, then you will need to do so here.

The upgrade call adds a new block – block 6 – to the channel's ledger and allows for the Org3 peers to execute transactions during the endorsement phase. Hop back to the Org3 CLI container and issue a query for the value of `a`. This will take a bit of time because a chaincode image needs to be built for the targeted peer, and the container needs to start:

```
peer chaincode query -C $CHANNEL_NAME -n mycc -c '{"Args":["query","a"]}'
```

We should see a response of `Query Result: 90`.

Now issue an invocation to move `10` from `a` to `b`:

```
peer chaincode invoke -o orderer.example.com:7050  --tls $CORE_PEER_TLS_ENABLED --
↪cafile $ORDERER_CA -C $CHANNEL_NAME -n mycc -c '{"Args":["invoke","a","b","10"]}'
```

Query one final time:

```
peer chaincode query -C $CHANNEL_NAME -n mycc -c '{"Args":["query","a"]}'
```

We should see a response of `Query Result: 80`, accurately reflecting the update of this chaincode's world state.

6.3.13 Conclusion

The channel configuration update process is indeed quite involved, but there is a logical method to the various steps. The endgame is to form a delta transaction object represented in protobuf binary format and then acquire the requisite number of admin signatures such that the channel configuration update transaction fulfills the channel's modification policy.

The `configtxlator` and `jq` tools, along with the ever-growing `peer channel` commands, provide us with the functionality to accomplish this task.

6.4 Upgrading Your Network Components

Note: When we use the term "upgrade" in this documentation, we're primarily referring to changing the version of a component (for example, going from a v1.2 binary to a v1.3 binary). The term "update," on the other hand, refers not to versions but to configuration changes, such as updating a channel configuration or a deployment script. As there is no data migration, technically speaking, in Fabric, we will not use the term "migration" or "migrate" here.

Note: Also, if your network is not yet at Fabric v1.2, follow the instructions for Upgrading Your Network to v1.2. The instructions in this documentation only cover moving from v1.2 to v1.3, not from any other version to v1.3.

6.4.1 Overview

Because the *Building Your First Network* (BYFN) tutorial defaults to the "latest" binaries, if you have run it since the release of v1.3, your machine will have v1.3 binaries and tools installed on it and you will not be able to upgrade them.

As a result, this tutorial will provide a network based on Hyperledger Fabric v1.2 binaries as well as the v1.3 binaries you will be upgrading to. In addition, we will show how to add the new v1.3 capabilities. For more information about capabilities, check out our *Capability Requirements* documentation.

There are two new capabilities for v1.3:

1. A top-level `channel` capability that allows Identity Mixer to work.
2. A `channel\application` capability that enables state-based endorsement. For more information about state-based endorsement check out our documentation on *Endorsement policies*.

The first may be set on all channels, including the orderer system channel. The second may only be set in the application group (which is only defined in application channels and affects **peer network** behavior, such as how transactions are handled by the peer).

Note: Setting capabilities as part of an upgrade (or at any other time) is optional. However, unless a capability is set, it cannot be leveraged (to use state-based endorsement or Identity Mixer, in this case).

Because the BYFN deployment script creates a channel called `mychannel`, we will also update the configuration of `mychannel`. Any subsequently created channels will copy the configuration of the orderer system channel and will therefore have the `channel` capability enabled.

At a high level, our upgrade tutorial will perform the following steps:

1. Back up the ledger and MSPs.
2. Upgrade the orderer binaries to Fabric v1.3.
3. Upgrade the peer binaries to Fabric v1.3.
4. Enable the v1.3 capabilities.

This tutorial will demonstrate how to perform each of these steps individually with CLI commands. We will also describe how the CLI `tools` image can be updated.

Note: Because BYFN uses a "SOLO" ordering service (one orderer), our script brings down the entire network. However, in production environments, the orderers and peers can be upgraded simultaneously and on a rolling basis. In other words, you can upgrade the binaries in any order without bringing down the network.

Because BYFN does not support the following components, our script for upgrading BYFN will not cover them:

- **Fabric CA**
- **Kafka**
- **CouchDB**
- **SDK**

The process for upgrading these components — if necessary — will be covered in a section following the tutorial. We will also show how to upgrade the Node chaincode shim.

Prerequisites

If you haven't already done so, ensure you have all of the dependencies on your machine as described in *Prerequisites*.

6.4.2 Launch a v1.2 network

Before we can upgrade to v1.3, we must first provision a network running Fabric v1.2 images.

Just as in the BYFN tutorial, we will be operating from the `first-network` subdirectory within your local clone of `fabric-samples`. Change into that directory now. You will also want to open a few extra terminals for ease of use.

Clean up

We want to operate from a known state, so we will use the `byfn.sh` script to kill any active or stale docker containers and remove any previously generated artifacts. Run:

```
./byfn.sh down
```

Generate the crypto and bring up the network

With a clean environment, launch our v1.2 BYFN network using these four commands:

```
git fetch origin

git checkout v1.2.0

./byfn.sh generate

./byfn.sh up -t 3000 -i 1.2.0
```

Note: If you have locally built v1.2 images, they will be used by the example. If you get errors, please consider cleaning up your locally built v1.2 images and running the example again. This will download v1.2 images from docker hub.

If BYFN has launched properly, you will see:

```
==================== All GOOD, BYFN execution completed ====================
```

We are now ready to upgrade our network to Hyperledger Fabric v1.3.

Get the newest samples

Note: The instructions below pertain to whatever is the most recently published version of v1.3.x. Please substitute 1.3.x with the version identifier of the published release that you are testing. In other words, replace '1.3.x' with '1.3.0' if you are testing the first release.

Before completing the rest of the tutorial, it's important to get the v1.3.x version of the samples, you can do this by issuing:

```
git fetch origin

git checkout v1.3.x
```

Want to upgrade now?

We have a script that will upgrade all of the components in BYFN as well as enable capabilities. If you are running a production network, or are an administrator of some part of a network, this script can serve as a template for performing your own upgrades.

Afterwards, we will walk you through the steps in the script and describe what each piece of code is doing in the upgrade process.

To run the script, issue these commands:

```
# Note, replace '1.3.x' with a specific version, for example '1.2.0'.
# Don't pass the image flag '-i 1.3.x' if you prefer to default to 'latest' images.

./byfn.sh upgrade -i 1.3.x
```

If the upgrade is successful, you should see the following:

```
==================== All GOOD, End-2-End UPGRADE Scenario execution completed␣
↪====================
```

if you want to upgrade the network manually, simply run `./byfn.sh down` again and perform the steps up to — but not including — `./byfn.sh upgrade -i 1.3.x`. Then proceed to the next section.

Note: Many of the commands you'll run in this section will not result in any output. In general, assume no output is good output.

6.4.3 Upgrade the orderer containers

Orderer containers should be upgraded in a rolling fashion (one at a time). At a high level, the orderer upgrade process goes as follows:

1. Stop the orderer.
2. Back up the orderer's ledger and MSP.
3. Restart the orderer with the latest images.
4. Verify upgrade completion.

As a consequence of leveraging BYFN, we have a solo orderer setup, therefore, we will only perform this process once. In a Kafka setup, however, this process will have to be performed for each orderer.

Note: This tutorial uses a docker deployment. For native deployments, replace the file `orderer` with the one from the release artifacts. Backup the `orderer.yaml` and replace it with the `orderer.yaml` file from the release artifacts. Then port any modified variables from the backed up `orderer.yaml` to the new one. Utilizing a utility like `diff` may be helpful.

Let's begin the upgrade process by **bringing down the orderer**:

```
docker stop orderer.example.com

export LEDGERS_BACKUP=./ledgers-backup

# Note, replace '1.3.x' with a specific version, for example '1.3.0'.
# Set IMAGE_TAG to 'latest' if you prefer to default to the images tagged 'latest' on␣
↪your system.

export IMAGE_TAG=$(go env GOARCH)-1.3.x-stable
```

We have created a variable for a directory to put file backups into, and exported the `IMAGE_TAG` we'd like to move to.

Once the orderer is down, you'll want to **backup its ledger and MSP**:

```
mkdir -p $LEDGERS_BACKUP

docker cp orderer.example.com:/var/hyperledger/production/orderer/ ./$LEDGERS_BACKUP/
↪orderer.example.com
```

In a production network this process would be repeated for each of the Kafka-based orderers in a rolling fashion.

Now **download and restart the orderer** with our new fabric image:

```
docker-compose -f docker-compose-cli.yaml up -d --no-deps orderer.example.com
```

Because our sample uses a "solo" ordering service, there are no other orderers in the network that the restarted orderer must sync up to. However, in a production network leveraging Kafka, it will be a best practice to issue `peer channel fetch <blocknumber>` after restarting the orderer to verify that it has caught up to the other orderers.

6.4.4 Upgrade the peer containers

Next, let's look at how to upgrade peer containers to Fabric v1.3. Peer containers should, like the orderers, be upgraded in a rolling fashion (one at a time). As mentioned during the orderer upgrade, orderers and peers may be upgraded in parallel, but for the purposes of this tutorial we've separated the processes out. At a high level, we will perform the following steps:

1. Stop the peer.
2. Back up the peer's ledger and MSP.
3. Remove chaincode containers and images.
4. Restart the peer with latest image.
5. Verify upgrade completion.

We have four peers running in our network. We will perform this process once for each peer, totaling four upgrades.

Note: Again, this tutorial utilizes a docker deployment. For **native** deployments, replace the file `peer` with the one from the release artifacts. Backup your `core.yaml` and replace it with the one from the release artifacts. Port any modified variables from the backed up `core.yaml` to the new one. Utilizing a utility like `diff` may be helpful.

Let's **bring down the first peer** with the following command:

```
export PEER=peer0.org1.example.com

docker stop $PEER
```

We can then **backup the peer's ledger and MSP**:

```
mkdir -p $LEDGERS_BACKUP

docker cp $PEER:/var/hyperledger/production ./$LEDGERS_BACKUP/$PEER
```

With the peer stopped and the ledger backed up, **remove the peer chaincode containers**:

```
CC_CONTAINERS=$(docker ps | grep dev-$PEER | awk '{print $1}')
if [ -n "$CC_CONTAINERS" ] ; then docker rm -f $CC_CONTAINERS ; fi
```

And the peer chaincode images:

```
CC_IMAGES=$(docker images | grep dev-$PEER | awk '{print $1}')
if [ -n "$CC_IMAGES" ] ; then docker rmi -f $CC_IMAGES ; fi
```

Now we'll re-launch the peer using the v1.3 image tag:

```
docker-compose -f docker-compose-cli.yaml up -d --no-deps $PEER
```

Note: Although, BYFN supports using CouchDB, we opted for a simpler implementation in this tutorial. If you are using CouchDB, however, issue this command instead of the one above:

```
docker-compose -f docker-compose-cli.yaml -f docker-compose-couch.yaml up -d --no-
↪deps $PEER
```

Note: You do not need to relaunch the chaincode container. When the peer gets a request for a chaincode, (invoke or query), it first checks if it has a copy of that chaincode running. If so, it uses it. Otherwise, as in this case, the peer launches the chaincode (rebuilding the image if required).

Verify peer upgrade completion

We've completed the upgrade for our first peer, but before we move on let's check to ensure the upgrade has been completed properly with a chaincode invoke.

Note: Before you attempt this, you may want to upgrade peers from enough organizations to satisfy your endorsement policy. Although, this is only mandatory if you are updating your chaincode as part of the upgrade process. If you are not updating your chaincode as part of the upgrade process, it is possible to get endorsements from peers running at different Fabric versions.

Before we get into the CLI container and issue the invoke, make sure the CLI is updated to the most current version by issuing:

```
docker-compose -f docker-compose-cli.yaml stop cli

docker-compose -f docker-compose-cli.yaml up -d --no-deps cli
```

If you specifically want the v1.3 version of the CLI, issue:

```
IMAGE_TAG=$(go env GOARCH)-1.3.x-stable docker-compose -f docker-compose-cli.yaml up -
↪d --no-deps cli
```

Once you have the version of the CLI you want, get into the CLI container:

```
docker exec -it cli bash
```

Now you'll need to set two environment variables — the name of the channel and the name of the `ORDERER_CA`:

```
CH_NAME=mychannel

ORDERER_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.
↪example.com-cert.pem
```

Now you can issue the invoke:

```
peer chaincode invoke -o orderer.example.com:7050 --peerAddresses peer0.org1.example.
↪com:7051 --tlsRootCertFiles /opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt --
↪peerAddresses peer0.org2.example.com:7051 --tlsRootCertFiles /opt/gopath/src/github.
↪com/hyperledger/fabric/peer/crypto/peerOrganizations/org2.example.com/peers/peer0.
↪org2.example.com/tls/ca.crt --tls --cafile $ORDERER_CA  -C $CH_NAME -n mycc -c '{
↪"Args":["invoke","a","b","10"]}'
```

Our query earlier revealed `a` to have a value of `90` and we have just removed `10` with our invoke. Therefore, a query against `a` should reveal `80`. Let's see:

```
peer chaincode query -C mychannel -n mycc -c '{"Args":["query","a"]}'
```

We should see the following:

```
Query Result: 80
```

After verifying the peer was upgraded correctly, make sure to issue an `exit` to leave the container before continuing to upgrade your peers. You can do this by repeating the process above with a different peer name exported.

```
export PEER=peer1.org1.example.com
export PEER=peer0.org2.example.com
export PEER=peer1.org2.example.com
```

Note: All peers must be upgraded BEFORE enabling the v1.3 capability.

6.4.5 Enable the v1.3 capabilities

Note: A reminder that while we show how to enable capabilities as part of this tutorial, this is an optional step UNLESS you are leveraging the capability or capabilities.

Although Fabric binaries can and should be upgraded in a rolling fashion, it is important to finish upgrading binaries before enabling capabilities. Any binaries which are not upgraded to v1.3 before enabling the new capabilities may intentionally crash to indicate a misconfiguration which could otherwise result in a state fork.

Once a capability has been enabled, it becomes part of the permanent record for that channel. This means that even after disabling the capability, old binaries will not be able to participate in the channel because they cannot process beyond the block which enabled the capability to get to the block which disables it. As a result, once a capability has been enabled, disabling it is neither recommended nor supported.

For this reason, think of enabling channel capabilities as a point of no return. Please experiment with the new capabilities in a test setting and be confident before proceeding to enable them in production.

Capabilities are enabled through a channel configuration transaction. For more information on updating channel configs, check out *Adding an Org to a Channel* or the doc on *Updating a Channel Configuration*.

To learn about what the new capabilities are in v1.3 and what they enable, refer back to the *Overview*.

As with any channel config update, we will have to follow this process:

1. Get the latest channel config.
2. Create a modified channel config.

3. Create a config update transaction.

Orderer system channel

You should still be in the CLI container. If not, reissue:

```
docker exec -it cli bash
```

Let's set our environment variables for the OrdererOrg so that we can update the orderer system channel. Issue these commands:

```
CORE_PEER_LOCALMSPID="OrdererMSP"

CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.
↪example.com-cert.pem

CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/users/Admin@example.com/msp

ORDERER_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.
↪example.com-cert.pem

And let's set our channel name to ``testchainid`` (this is the name of the
orderer system channel):
```

```
CH_NAME=testchainid
```

Channel group

The orderer system channel has both an `orderer` group and a `channel` group. We're only enabling a capability for the `channel` group in this release.

The first step is to get the latest channel configuration.

```
peer channel fetch config config_block.pb -o orderer.example.com:7050 -c $CH_NAME --
↪tls --cafile $ORDERER_CA

configtxlator proto_decode --input config_block.pb --type common.Block --output␣
↪config_block.json

jq .data.data[0].payload.data.config config_block.json > config.json
```

Next, create a modified channel config:

```
jq -s '.[0] * {"channel_group":{"values": {"Capabilities": .[1]}}}' config.json ./
↪scripts/capabilities.json > modified_config.json
```

Note what we're changing here: `Capabilities` are being added as a `value` of the top level `channel_group` (in the `testchainid` channel, as before).

```
configtxlator proto_encode --input config.json --type common.Config --output config.pb

configtxlator proto_encode --input modified_config.json --type common.Config --output␣
↪modified_config.pb
```

(continues on next page)

(continued from previous page)

```
configtxlator compute_update --channel_id $CH_NAME --original config.pb --updated␣
↪modified_config.pb --output config_update.pb
```

Package the config update into a transaction:

```
configtxlator proto_decode --input config_update.pb --type common.ConfigUpdate --
↪output config_update.json

echo '{"payload":{"header":{"channel_header":{"channel_id":"'$CH_NAME'", "type":2}},
↪"data":{"config_update":'$(cat config_update.json)'}}}' | jq . > config_update_in_
↪envelope.json

configtxlator proto_encode --input config_update_in_envelope.json --type common.
↪Envelope --output config_update_in_envelope.pb
```

Submit the config update transaction:

```
peer channel update -f config_update_in_envelope.pb -c $CH_NAME -o orderer.example.
↪com:7050 --tls true --cafile $ORDERER_CA
```

Congratulations! You have now enabled the orderer/channel group v1.3 capability.

Application channel

As we said earlier, within the `application` channel, both the `application` group and the `channel` group must be updated.

These can occur in any order, but we'll start with the `channel` group.

Channel group

Because we're updating the config of the channel group, the relevant orgs — Org1, Org2, and the OrdererOrg — need to sign it. This task would usually be performed by the individual org admins, but in BYFN this task falls to us.

Start by setting the environment variables as Org1:

```
export CORE_PEER_LOCALMSPID="Org1MSP"

export CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt

export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp

export CORE_PEER_ADDRESS=peer0.org1.example.com:7051

export ORDERER_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.
↪example.com-cert.pem

export CH_NAME="mychannel"
```

Note that we're now on `mychannel` (where we'll remain when we update the `application` group in the next section).

Fetch, decode, and scope the config:

```
peer channel fetch config config_block.pb -o orderer.example.com:7050 -c $CH_NAME --
↪tls --cafile $ORDERER_CA

configtxlator proto_decode --input config_block.pb --type common.Block --output␣
↪config_block.json

jq .data.data[0].payload.data.config config_block.json > config.json
```

Create a modified config:

```
jq -s '.[0] * {"channel_group":{"values": {"Capabilities": .[1]}}}' config.json ./
↪scripts/capabilities.json > modified_config.json
```

Create the config update:

```
configtxlator proto_encode --input config.json --type common.Config --output config.pb

configtxlator proto_encode --input modified_config.json --type common.Config --output␣
↪modified_config.pb

configtxlator compute_update --channel_id $CH_NAME --original config.pb --updated␣
↪modified_config.pb --output config_update.pb
```

Package the config update into a transaction:

```
configtxlator proto_decode --input config_update.pb --type common.ConfigUpdate --
↪output config_update.json

echo '{"payload":{"header":{"channel_header":{"channel_id":"'$CH_NAME'", "type":2}},
↪"data":{"config_update":'$(cat config_update.json)'}}}' | jq . > config_update_in_
↪envelope.json

configtxlator proto_encode --input config_update_in_envelope.json --type common.
↪Envelope --output config_update_in_envelope.pb
```

We've already switched into Org1, so we can sign the update:

```
peer channel signconfigtx -f config_update_in_envelope.pb
```

Now we need to switch to Org2 and sign:

```
export CORE_PEER_LOCALMSPID="Org2MSP"

export CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt

export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp

export CORE_PEER_ADDRESS=peer0.org2.example.com:7051
```

Org2 signs the update transaction:

```
peer channel signconfigtx -f config_update_in_envelope.pb
```

Now, we switch to the OrdererOrg. Then sign and submit:

```
CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.
↪example.com-cert.pem

CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/users/Admin@example.com/msp

ORDERER_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.
↪example.com-cert.pem

peer channel update -f config_update_in_envelope.pb -c $CH_NAME -o orderer.example.
↪com:7050 --tls true --cafile $ORDERER_CA
```

Congratulations! You have now enabled the application/channel group v1.3 capability.

Application group

To change the configuration of the application group, you'll only need the signature of a peer from both Org1 and Org2. Begin by setting your environment variables as Org1:

```
export CORE_PEER_LOCALMSPID="Org1MSP"

export CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt

export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp

export CORE_PEER_ADDRESS=peer0.org1.example.com:7051

export ORDERER_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.
↪example.com-cert.pem
```

Next, get the latest channel config:

```
peer channel fetch config config_block.pb -o orderer.example.com:7050 -c $CH_NAME --
↪tls --cafile $ORDERER_CA

configtxlator proto_decode --input config_block.pb --type common.Block --output␣
↪config_block.json

jq .data.data[0].payload.data.config config_block.json > config.json
```

Create a modified channel config:

```
jq -s '.[0] * {"channel_group":{"values": {"Capabilities": .[1]}}}' config.json ./
↪scripts/capabilities.json > modified_config.json
```

Note what we're changing here: `Capabilities` are being added as a `value` of the `Application` group under `channel_group` (in `mychannel`).

Create a config update transaction:

```
configtxlator proto_encode --input config.json --type common.Config --output config.pb

configtxlator proto_encode --input modified_config.json --type common.Config --output␣
↪modified_config.pb

configtxlator compute_update --channel_id $CH_NAME --original config.pb --updated␣
↪modified_config.pb --output config_update.pb
```

Package the config update into a transaction:

```
configtxlator proto_decode --input config_update.pb --type common.ConfigUpdate --
↪output config_update.json

echo '{"payload":{"header":{"channel_header":{"channel_id":"'$CH_NAME'", "type":2}},
↪"data":{"config_update":'$(cat config_update.json)'}}}' | jq . > config_update_in_
↪envelope.json

configtxlator proto_encode --input config_update_in_envelope.json --type common.
↪Envelope --output config_update_in_envelope.pb
```

Org1 signs the transaction:

```
peer channel signconfigtx -f config_update_in_envelope.pb
```

Set the environment variables as Org2:

```
export CORE_PEER_LOCALMSPID="Org2MSP"

export CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt

export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp

export CORE_PEER_ADDRESS=peer0.org2.example.com:7051
```

Org2 submits the config update transaction with its signature:

```
peer channel update -f config_update_in_envelope.pb -c $CH_NAME -o orderer.example.
↪com:7050 --tls true --cafile $ORDERER_CA
```

Congratulations! You have now enabled the application/application group v1.3 capability.

Re-verify upgrade completion

Let's make sure the network is still running by moving another `10` from `a` to `b`:

```
peer chaincode invoke -o orderer.example.com:7050 --peerAddresses peer0.org1.example.
↪com:7051 --tlsRootCertFiles /opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt --
↪peerAddresses peer0.org2.example.com:7051 --tlsRootCertFiles /opt/gopath/src/github.
↪com/hyperledger/fabric/peer/crypto/peerOrganizations/org2.example.com/peers/peer0.
↪org2.example.com/tls/ca.crt --tls --cafile $ORDERER_CA  -C $CH_NAME -n mycc -c '{
↪"Args":["invoke","a","b","10"]}'
```

And then querying the value of `a`, which should reveal a value of `70`. Let's see:

```
peer chaincode query -C $CH_NAME -n mycc -c '{"Args":["query","a"]}'
```

We should see the following:

```
Query Result: 70
```

6.4.6 Upgrading components BYFN does not support

Although this is the end of our update tutorial, there are other components that exist in production networks that are not supported by the BYFN sample. In this section, we'll talk through the process of updating them.

Fabric CA container

To learn how to upgrade your Fabric CA server, click over to the CA documentation.

Upgrade Node SDK clients

Note: Upgrade Fabric CA before upgrading Node SDK clients.

Use NPM to upgrade any `Node.js` client by executing these commands in the root directory of your application:

```
npm install fabric-client@1.3

npm install fabric-ca-client@1.3
```

These commands install the new version of both the Fabric client and Fabric-CA client and write the new versions `package.json`.

Upgrading the Kafka cluster

It is not required, but it is recommended that the Kafka cluster be upgraded and kept up to date along with the rest of Fabric. Newer versions of Kafka support older protocol versions, so you may upgrade Kafka before or after the rest of Fabric.

If you followed the Upgrading Your Network to v1.2 tutorial, your Kafka cluster should be at v1.0.0. If it isn't, refer to the official Apache Kafka documentation on upgrading Kafka from previous versions to upgrade the Kafka cluster brokers.

Upgrading Zookeeper

An Apache Kafka cluster requires an Apache Zookeeper cluster. The Zookeeper API has been stable for a long time and, as such, almost any version of Zookeeper is tolerated by Kafka. Refer to the Apache Kafka upgrade documentation in case there is a specific requirement to upgrade to a specific version of Zookeeper. If you would like to upgrade your Zookeeper cluster, some information on upgrading Zookeeper cluster can be found in the Zookeeper FAQ.

Upgrading CouchDB

If you are using CouchDB as state database, you should upgrade the peer's CouchDB at the same time the peer is being upgraded. Because both v1.2 and v1.3 ship with CouchDB v2.1.1, if you have followed the steps for Upgrading to v1.2, your CouchDB should be up to date.

Upgrade Node chaincode shim

To move to the new version of the Node chaincode shim a developer would need to:

1. Change the level of `fabric-shim` in their chaincode `package.json` from 1.2 to 1.3.
2. Repackage this new chaincode package and install it on all the endorsing peers in the channel.
3. Perform an upgrade to this new chaincode.

Note: This flow isn't specific to moving from 1.2 to 1.3. It is also how one would upgrade from 1.2.0 to 1.2.1 of the node fabric-shim.

Upgrade Chaincodes with vendored shim

Note: The v1.2.0 shim is compatible with the v1.3 peer, but, it is still best practice to upgrade the chaincode shim to match the current level of the peer.

A number of third party tools exist that will allow you to vendor a chaincode shim. If you used one of these tools, use the same one to update your vendoring and re-package your chaincode.

If your chaincode vendors the shim, after updating the shim version, you must install it to all peers which already have the chaincode. Install it with the same name, but a newer version. Then you should execute a chaincode upgrade on each channel where this chaincode has been deployed to move to the new version.

If you did not vendor your chaincode, you can skip this step entirely.

6.5 Using Private Data in Fabric

This tutorial will demonstrate the use of collections to provide storage and retrieval of private data on the blockchain network for authorized peers of organizations.

The information in this tutorial assumes knowledge of private data stores and their use cases. For more information, check out *Private data*.

The tutorial will take you through the following steps to practice defining, configuring and using private data with Fabric:

1. *Build a collection definition JSON file*
2. *Read and Write private data using chaincode APIs*
3. *Install and instantiate chaincode with a collection*
4. *Store private data*
5. *Query the private data as an authorized peer*

6. *Query the private data as an unauthorized peer*
7. *Purge Private Data*
8. *Using indexes with private data*
9. *Additional resources*

This tutorial will use the marbles private data sample — running on the Building Your First Network (BYFN) tutorial network — to demonstrate how to create, deploy, and use a collection of private data. The marbles private data sample will be deployed to the *Building Your First Network* (BYFN) tutorial network. You should have completed the task *Install Samples, Binaries and Docker Images*; however, running the BYFN tutorial is not a prerequisite for this tutorial. Instead the necessary commands are provided throughout this tutorial to use the network. We will describe what is happening at each step, making it possible to understand the tutorial without actually running the sample.

6.5.1 Build a collection definition JSON file

The first step in privatizing data on a channel is to build a collection definition which defines access to the private data.

The collection definition describes who can persist data, how many peers the data is distributed to, how many peers are required to disseminate the private data, and how long the private data is persisted in the private database. Later, we will demonstrate how chaincode APIs `PutPrivateData` and `GetPrivateData` are used to map the collection to the private data being secured.

A collection definition is composed of five properties:

- `name`: Name of the collection.
- `policy`: Defines the organization peers allowed to persist the collection data.
- `requiredPeerCount`: Number of peers required to disseminate the private data as a condition of the endorsement of the chaincode
- `maxPeerCount`: For data redundancy purposes, the number of other peers that the current endorsing peer will attempt to distribute the data to. If an endorsing peer goes down, these other peers are available at commit time if there are requests to pull the private data.
- `blockToLive`: For very sensitive information such as pricing or personal information, this value represents how long the data should live on the private database in terms of blocks. The data will live for this specified number of blocks on the private database and after that it will get purged, making this data obsolete from the network. To keep private data indefinitely, that is, to never purge private data, set the `blockToLive` property to `0`.

To illustrate usage of private data, the marbles private data example contains two private data collection definitions: `collectionMarbles` and `collectionMarblePrivateDetails`. The `policy` property in the `collectionMarbles` definition allows all members of the channel (Org1 and Org2) to have the private data in a private database. The `collectionMarblesPrivateDetails` collection allows only members of Org1 to have the private data in their private database.

For more information on building a policy definition refer to the *Endorsement policies* topic.

```
// collections_config.json

[
  {
       "name": "collectionMarbles",
       "policy": "OR('Org1MSP.member', 'Org2MSP.member')",
       "requiredPeerCount": 0,
       "maxPeerCount": 3,
       "blockToLive":1000000
```

(continues on next page)

(continued from previous page)

```
  },

  {
        "name": "collectionMarblePrivateDetails",
        "policy": "OR('Org1MSP.member')",
        "requiredPeerCount": 0,
        "maxPeerCount": 3,
        "blockToLive":3
  }
]
```

The data to be secured by these policies is mapped in chaincode and will be shown later in the tutorial.

This collection definition file is deployed on the channel when its associated chaincode is instantiated on the channel using the peer chaincode instantiate command. More details on this process are provided in Section 3 below.

6.5.2 Read and Write private data using chaincode APIs

The next step in understanding how to privatize data on a channel is to build the data definition in the chaincode. The marbles private data sample divides the private data into two separate data definitions according to how the data will be accessed.

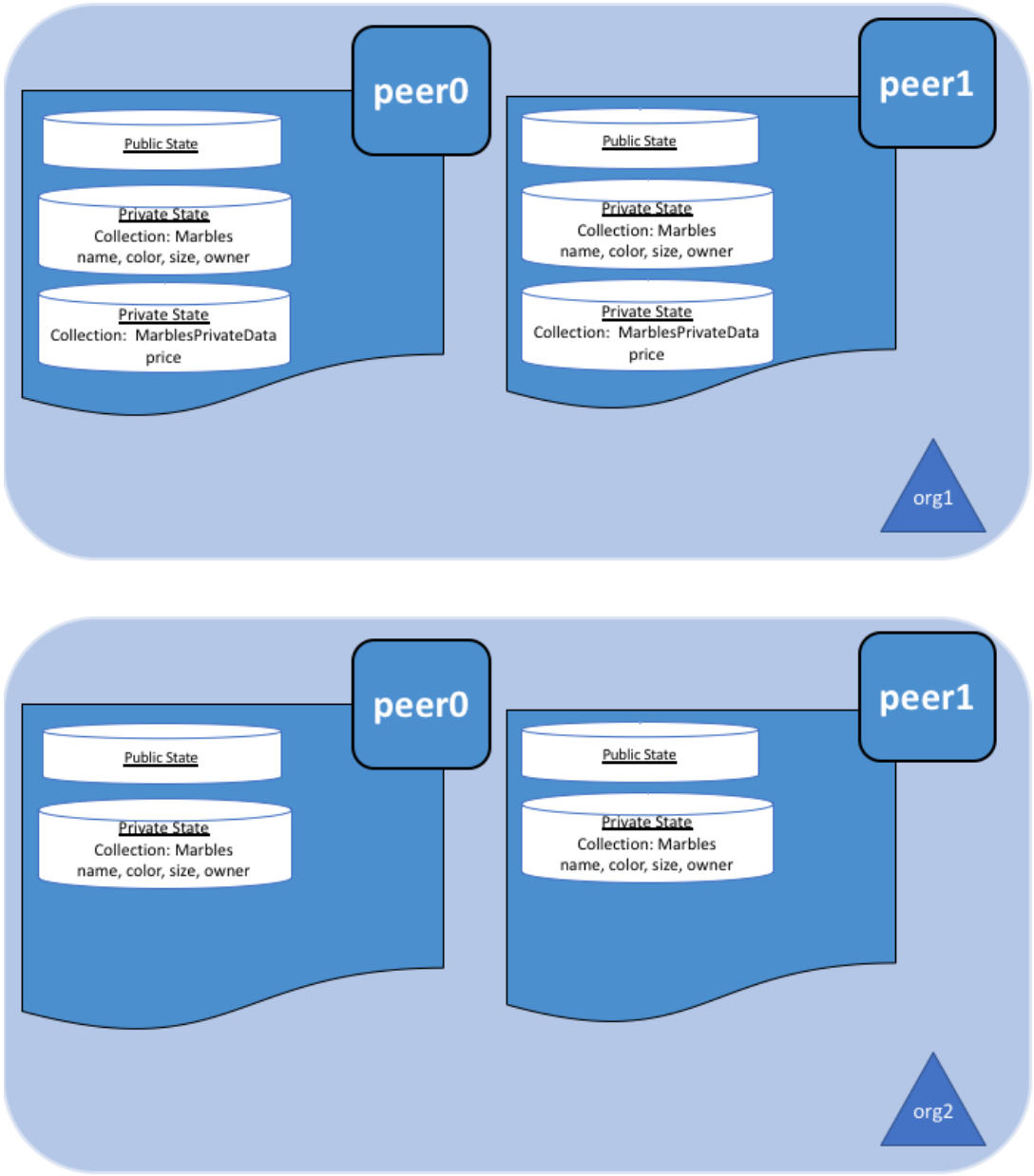
```
// Peers in Org1 and Org2 will have this private data in a side database
type marble struct {
  ObjectType string `json:"docType"`
  Name       string `json:"name"`
  Color      string `json:"color"`
  Size       int    `json:"size"`
  Owner      string `json:"owner"`
}

// Only peers in Org1 will have this private data in a side database
type marblePrivateDetails struct {
  ObjectType string `json:"docType"`
  Name       string `json:"name"`
  Price      int    `json:"price"`
}
```

Specifically access to the private data will be restricted as follows:

- `name, color, size, and owner` will be visible to all members of the channel (Org1 and Org2)
- `price` only visible to members of Org1

Thus two different sets of private data are defined in the marbles private data sample. The mapping of this data to the collection policy which restricts its access is controlled by chaincode APIs. Specifically, reading and writing private data using a collection definition is performed by calling `GetPrivateData()` and `PutPrivateData()`, which can be found here.

The following diagrams illustrate the private data model used by the marbles private data sample.



Reading collection data

Use the chaincode API `GetPrivateData()` to query private data in the database. `GetPrivateData()` takes two arguments, the **collection name** and the data key. Recall the collection `collectionMarbles` allows members of Org1 and Org2 to have the private data in a side database, and the collection `collectionMarblePrivateDetails` allows only members of Org1 to have the private data in a side database. For implementation details refer to the following two marbles private data functions:

- **readMarble** for querying the values of the `name, color, size and owner` attributes
- **readMarblePrivateDetails** for querying the values of the `price` attribute

When we issue the database queries using the peer commands later in this tutorial, we will call these two functions.

Writing private data

Use the chaincode API `PutPrivateData()` to store the private data into the private database. The API also requires the name of the collection. Since the marbles private data sample includes two different collections, it is called twice in the chaincode:

1. Write the private data `name, color, size and owner` using the collection named `collectionMarbles`.
2. Write the private data `price` using the collection named `collectionMarblePrivateDetails`.

For example, in the following snippet of the `initMarble` function, `PutPrivateData()` is called twice, once for each set of private data.

```
// ==== Create marble object and marshal to JSON ====
      objectType := "marble"
      marble := &marble{objectType, marbleName, color, size, owner}
      marbleJSONasBytes, err := json.Marshal(marble)
      if err != nil {
              return shim.Error(err.Error())
      }
      //Alternatively, build the marble json string manually if you don't want to use␣
↪struct marshalling
      //marbleJSONasString := `{"docType":"Marble",  "name": "` + marbleName + `",
↪"color": "` + color + `", "size": ` + strconv.Itoa(size) + `, "owner": "` + owner +␣
↪`"}`
      //marbleJSONasBytes := []byte(str)

      // === Save marble to state ===
      err = stub.PutPrivateData("collectionMarbles", marbleName, marbleJSONasBytes)
      if err != nil {
              return shim.Error(err.Error())
      }

      // ==== Save marble private details ====
      objectType = "marblePrivateDetails"
      marblePrivateDetails := &marblePrivateDetails{objectType, marbleName, price}
      marblePrivateDetailsBytes, err := json.Marshal(marblePrivateDetails)
      if err != nil {
              return shim.Error(err.Error())
      }
      err = stub.PutPrivateData("collectionMarblePrivateDetails", marbleName,␣
↪marblePrivateDetailsBytes)
      if err != nil {
              return shim.Error(err.Error())
      }
```

To summarize, the policy definition above for our `collection.json` allows all peers in Org1 and Org2 can store and transact (endorse, commit, query) with the marbles private data `name, color, size, owner` in their private database. But only peers in Org1 can store and transact with the `price` private data in an additional private database.

As an additional data privacy benefit, since a collection is being used, only the private data hashes go through orderer, not the private data itself, keeping private data confidential from orderer.

6.5.3 Start the network

Now we are ready to step through some commands which demonstrate using private data.

Try it yourself

Before installing and instantiating the marbles private data chaincode below, we need to start the BYFN network. For the sake of this tutorial, we want to operate from a known initial state. The following command will kill any active or stale docker containers and remove previously generated artifacts. Therefore let's run the following command to clean up any previous environments:

```
cd fabric-samples/first-network
./byfn.sh down
```

Start up the BYFN network with CouchDB by running the following command:

```
./byfn.sh up -c mychannel -s couchdb
```

This will create a simple Fabric network consisting of a single channel named `mychannel` with two organizations (each maintaining two peer nodes) and an ordering service while using CouchDB as the state database. Either LevelDB or CouchDB may be used with collections. CouchDB was chosen to demonstrate how to use indexes with private data.

Note: For collections to work, it is important to have cross organizational gossip configured correctly. Refer to our documentation on *Gossip data dissemination protocol*, paying particular attention to the section on "anchor peers". Our tutorial does not focus on gossip given it is already configured in the BYFN sample, but when configuring a channel, the gossip anchors peers are critical to configure for collections to work properly.

6.5.4 Install and instantiate chaincode with a collection

Client applications interact with the blockchain ledger through chaincode. As such we need to install and instantiate the chaincode on every peer that will execute and endorse our transactions. Chaincode is installed onto a peer and then instantiated onto the channel using peer-commands.

Install chaincode on all peers

As discussed above, the BYFN network includes two organizations, Org1 and Org2, with two peers each. Therefore the chaincode has to be installed on four peers:

- peer0.org1.example.com
- peer1.org1.example.com
- peer0.org2.example.com
- peer1.org2.example.com

Use the peer chaincode install command to install the Marbles chaincode on each peer.

Try it yourself

Assuming you have started the BYFN network, enter the CLI container.

```
docker exec -it cli bash
```

Your command prompt will change to something similar to:

```
root@81eac8493633:/opt/gopath/src/github.com/hyperledger/fabric/peer#
```

1. Use the following command to install the Marbles chaincode from the git repository onto the peer `peer0.org1.example.com` in your BYFN network. (By default, after starting the BYFN network, the active peer is set to: `CORE_PEER_ADDRESS=peer0.org1.example.com:7051`):

```
peer chaincode install -n marblesp -v 1.0 -p github.com/chaincode/
↪marbles02_private/go/
```

   When it is complete you should see something similar to:

```
install -> INFO 003 Installed remotely response:<status:200 payload:"OK"␣
↪>
```

2. Use the CLI to switch the active peer to the second peer in Org1 and install the chaincode. Copy and paste the following entire block of commands into the CLI container and run them.

```
export CORE_PEER_ADDRESS=peer1.org1.example.com:7051
peer chaincode install -n marblesp -v 1.0 -p github.com/chaincode/
↪marbles02_private/go/
```

3. Use the CLI to switch to Org2. Copy and paste the following block of commands as a group into the peer container and run them all at once.

```
export CORE_PEER_LOCALMSPID=Org2MSP
export PEER0_ORG2_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/
↪tls/ca.crt
export CORE_PEER_TLS_ROOTCERT_FILE=$PEER0_ORG2_CA
export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/
↪fabric/peer/crypto/peerOrganizations/org2.example.com/users/Admin@org2.
↪example.com/msp
```

4. Switch the active peer to the first peer in Org2 and install the chaincode:

```
export CORE_PEER_ADDRESS=peer0.org2.example.com:7051
peer chaincode install -n marblesp -v 1.0 -p github.com/chaincode/
↪marbles02_private/go/
```

5. Switch the active peer to the second peer in org2 and install the chaincode:

```
export CORE_PEER_ADDRESS=peer1.org2.example.com:7051
peer chaincode install -n marblesp -v 1.0 -p github.com/chaincode/
↪marbles02_private/go/
```

Instantiate the chaincode on the channel

Use the peer chaincode instantiate command to instantiate the marbles chaincode on a channel. To configure the chaincode collections on the channel, specify the flag `--collections-config` along with the name of the collections JSON file, `collections_config.json` in our example.

Try it yourself

Run the following commands to instantiate the marbles private data chaincode on the BYFN channel `mychannel`.

```
export ORDERER_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/
↪tlscacerts/tlsca.example.com-cert.pem
peer chaincode instantiate -o orderer.example.com:7050 --tls --cafile
↪$ORDERER_CA -C mychannel -n marblesp -v 1.0 -c '{"Args":["init"]}' -P "OR(
↪'Org1MSP.member','Org2MSP.member')" --collections-config  $GOPATH/src/
↪github.com/chaincode/marbles02_private/collections_config.json
```

Note: When specifying the value of the `--collections-config` flag, you will need to specify the fully qualified path to the collections_config.json file. For example: `--collections-config $GOPATH/src/github.com/chaincode/marbles02_private/collections_config.json`

When the instantiation completes successfully you should see something similar to:

```
[chaincodeCmd] checkChaincodeCmdParams -> INFO 001 Using default escc
[chaincodeCmd] checkChaincodeCmdParams -> INFO 002 Using default vscc
```

6.5.5 Store private data

Acting as a member of Org1, who is authorized to transact with all of the private data in the marbles private data sample, switch back to an Org1 peer and submit a request to add a marble:

Try it yourself

Copy and paste the following set of commands to the CLI command line.

```
export CORE_PEER_ADDRESS=peer0.org1.example.com:7051
export CORE_PEER_LOCALMSPID=Org1MSP
export CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/
↪fabric/peer/crypto/peerOrganizations/org1.example.com/peers/peer0.org1.
↪example.com/tls/ca.crt
export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/
↪peer/crypto/peerOrganizations/org1.example.com/users/Admin@org1.example.
↪com/msp
export PEER0_ORG1_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/
↪ca.crt
```

Invoke the marbles `initMarble` function which creates a marble with private data — name `marble1` owned by `tom` with a color `blue`, size `35` and price of `99`. Recall that private data **price** will be stored separately from the public data **name, owner, color, size**. For this reason, the `initMarble` function calls the `PutPrivateData()` API twice to persist the private data, once using each collection.

```
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/
↪src/github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.
↪com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem␣
↪-C mychannel -n marblesp -c '{"Args":["initMarble","marble1","blue","35",
↪"tom","99"]}'
```

You should see results similar to:

```
[chaincodeCmd] chaincodeInvokeOrQuery->INFO 001 Chaincode invoke
successful. result:  status:200
```

6.5.6 Query the private data as an authorized peer

Our collection definition allows all members of Org1 and Org2 to have the `name, color, size, owner` private data in their side database, but only peers in Org1 can have the `price` private data in their side database. As an authorized peer in Org1, we will query both sets of private data.

The first `query` command calls the `readMarble` function which passes `collectionMarbles` as an argument.

```
// ============================================
// readMarble - read a marble from chaincode state
// ============================================

func (t *SimpleChaincode) readMarble(stub shim.ChaincodeStubInterface, args []string)␣
↪pb.Response {
     var name, jsonResp string
     var err error
     if len(args) != 1 {
             return shim.Error("Incorrect number of arguments. Expecting name of the␣
↪marble to query")
     }

     name = args[0]
     valAsbytes, err := stub.GetPrivateData("collectionMarbles", name) //get the␣
↪marble from chaincode state

     if err != nil {
             jsonResp = "{\"Error\":\"Failed to get state for " + name + "\"}"
             return shim.Error(jsonResp)
     } else if valAsbytes == nil {
             jsonResp = "{\"Error\":\"Marble does not exist: " + name + "\"}"
             return shim.Error(jsonResp)
     }

     return shim.Success(valAsbytes)
}
```

The second `query` command calls the `readMarblePrivateDetails` function which passes `collectionMarblePrivateDetails` as an argument.

```
// ============================================
// readMarblePrivateDetails - read a marble private details from chaincode state
// ============================================

func (t *SimpleChaincode) readMarblePrivateDetails(stub shim.ChaincodeStubInterface,␣
↪args []string) pb.Response {
     var name, jsonResp string
     var err error

     if len(args) != 1 {
             return shim.Error("Incorrect number of arguments. Expecting name of the␣
↪marble to query")
     }

     name = args[0]
     valAsbytes, err := stub.GetPrivateData("collectionMarblePrivateDetails", name) //
↪get the marble private details from chaincode state

     if err != nil {
```

(continues on next page)

(continued from previous page)

```
            jsonResp = "{\"Error\":\"Failed to get private details for " + name + ":
↪" + err.Error() + "\"}"
            return shim.Error(jsonResp)
    } else if valAsbytes == nil {
            jsonResp = "{\"Error\":\"Marble private details does not exist: " + name␣
↪+ "\"}"
            return shim.Error(jsonResp)
    }
    return shim.Success(valAsbytes)
}
```

Now *Try it yourself*

Query for the `name, color, size and owner` private data of `marble1` as a member of Org1.

```
peer chaincode query -C mychannel -n marblesp -c '{"Args":["readMarble",
↪"marble1"]}'
```

You should see the following result:

```
{"color":"blue","docType":"marble","name":"marble1","owner":"tom","size":35}
```

Query for the `price` private data of `marble1` as a member of Org1.

```
peer chaincode query -C mychannel -n marblesp -c '{"Args":[
↪"readMarblePrivateDetails","marble1"]}'
```

You should see the following result:

```
{"docType":"marblePrivateDetails","name":"marble1","price":99}
```

6.5.7 Query the private data as an unauthorized peer

Now we will switch to a member of Org2 which has the marbles private data `name, color, size, owner` in its side database, but does not have the marbles `price` private data in its side database. We will query for both sets of private data.

Switch to a peer in Org2

From inside the docker container, run the following commands to switch to the peer which is unauthorized to access the marbles `price` private data.

Try it yourself

```
export CORE_PEER_ADDRESS=peer0.org2.example.com:7051
export CORE_PEER_LOCALMSPID=Org2MSP
export PEER0_ORG2_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/
↪ca.crt
export CORE_PEER_TLS_ROOTCERT_FILE=$PEER0_ORG2_CA
export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/
↪peer/crypto/peerOrganizations/org2.example.com/users/Admin@org2.example.
↪com/msp
```

Query private data Org2 is authorized to

Peers in Org2 should have the first set of marbles private data (`name, color, size and owner`) in their side database and can access it using the `readMarble()` function which is called with the `collectionMarbles` argument.

Try it yourself

```
peer chaincode query -C mychannel -n marblesp -c '{"Args":["readMarble",
↪"marble1"]}'
```

You should see something similar to the following result:

```
{"docType":"marble","name":"marble1","color":"blue","size":35,"owner":"tom"}
```

Query private data Org2 is not authorized to

Peers in Org2 do not have the marbles `price` private data in their side database. When they try to query for this data, they get back a hash of the key matching the public state but will not have the private state.

Try it yourself

```
peer chaincode query -C mychannel -n marblesp -c '{"Args":[
↪"readMarblePrivateDetails","marble1"]}'
```

You should see a result similar to:

```
{"Error":"Failed to get private details for marble1: GET_STATE failed:
transaction ID:␣
↪b04adebbf165ddc90b4ab897171e1daa7d360079ac18e65fa15d84ddfebfae90:
Private data matching public hash version is not available. Public hash
version = &version.Height{BlockNum:0x6, TxNum:0x0}, Private data version =
(*version.Height)(nil)"}
```

Members of Org2 will only be able to see the public hash of the private data.

6.5.8 Purge Private Data

For use cases where private data only needs to be on the ledger until it can be replicated into an off-chain database, it is possible to "purge" the data after a certain set number of blocks, leaving behind only hash of the data that serves as immutable evidence of the transaction.

There may be private data including personal or confidential information, such as the pricing data in our example, that the transacting parties don't want disclosed to other organizations on the channel. Thus, it has a limited lifespan, and can be purged after existing unchanged on the blockchain for a designated number of blocks using the `blockToLive` property in the collection definition.

Our `collectionMarblePrivateDetails` definition has a `blockToLive` property value of three meaning this data will live on the side database for three blocks and then after that it will get purged. Tying all of the pieces together, recall this collection definition `collectionMarblePrivateDetails` is associated with the `price` private data in the `initMarble()` function when it calls the `PutPrivateData()` API and passes the `collectionMarblePrivateDetails` as an argument.

We will step through adding blocks to the chain, and then watch the price information get purged by issuing four new transactions (Create a new marble, followed by three marble transfers) which adds four new blocks to the chain. After the fourth transaction (third marble transfer), we will verify that the price private data is purged.

Try it yourself

Switch back to peer0 in Org1 using the following commands. Copy and paste the following code block and run it inside your peer container:

```
export CORE_PEER_ADDRESS=peer0.org1.example.com:7051
export CORE_PEER_LOCALMSPID=Org1MSP
export CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/
↪fabric/peer/crypto/peerOrganizations/org1.example.com/peers/peer0.org1.
↪example.com/tls/ca.crt
export CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/
↪peer/crypto/peerOrganizations/org1.example.com/users/Admin@org1.example.
↪com/msp
export PEER0_ORG1_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/
↪crypto/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/
↪ca.crt
```

Open a new terminal window and view the private data logs for this peer by running the following command:

```
docker logs peer0.org1.example.com 2>&1 | grep -i -a -E 'private|pvt|privdata
↪'
```

You should see results similar to the following. Note the highest block number in the list. In the example below, the highest block height is `4`.

```
[pvtdatastorage] func1 -> INFO 023 Purger started: Purging expired private␣
↪data till block number [0]
[pvtdatastorage] func1 -> INFO 024 Purger finished
[kvledger] CommitWithPvtData -> INFO 022 Channel [mychannel]: Committed␣
↪block [0] with 1 transaction(s)
[kvledger] CommitWithPvtData -> INFO 02e Channel [mychannel]: Committed␣
↪block [1] with 1 transaction(s)
[kvledger] CommitWithPvtData -> INFO 030 Channel [mychannel]: Committed␣
↪block [2] with 1 transaction(s)
[kvledger] CommitWithPvtData -> INFO 036 Channel [mychannel]: Committed␣
↪block [3] with 1 transaction(s)
[kvledger] CommitWithPvtData -> INFO 03e Channel [mychannel]: Committed␣
↪block [4] with 1 transaction(s)
```

Back in the peer container, query for the **marble1** price data by running the following command. (A Query does not create a new transaction on the ledger since no data is transacted).

```
peer chaincode query -C mychannel -n marblesp -c '{"Args":[
↪"readMarblePrivateDetails","marble1"]}'
```

You should see results similar to:

```
{"docType":"marblePrivateDetails","name":"marble1","price":99}
```

The `price` data is still in the private data ledger.

Create a new **marble2** by issuing the following command. This transaction creates a new block on the chain.

```
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/
↪src/github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.
↪com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem␣
↪-C mychannel -n marblesp -c '{"Args":["initMarble","marble2","blue","35",
↪"tom","99"]}'
```

(continues on next page)

(continued from previous page)

Switch back to the Terminal window and view the private data logs for this peer again. You should see the block height increase by 1.

```
docker logs peer0.org1.example.com 2>&1 | grep -i -a -E 'private|pvt|privdata
↪'
```

Back in the peer container, query for the **marble1** price data again by running the following command:

```
peer chaincode query -C mychannel -n marblesp -c '{"Args":[
↪"readMarblePrivateDetails","marble1"]}'
```

The private data has not been purged, therefore the results are unchanged from previous query:

```
{"docType":"marblePrivateDetails","name":"marble1","price":99}
```

Transfer marble2 to "joe" by running the following command. This transaction will add a second new block on the chain.

```
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/
↪src/github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.
↪com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem␣
↪-C mychannel -n marblesp -c '{"Args":["transferMarble","marble2","joe"]}'
```

Switch back to the Terminal window and view the private data logs for this peer again. You should see the block height increase by 1.

```
docker logs peer0.org1.example.com 2>&1 | grep -i -a -E 'private|pvt|privdata
↪'
```

Back in the peer container, query for the marble1 price data by running the following command:

```
peer chaincode query -C mychannel -n marblesp -c '{"Args":[
↪"readMarblePrivateDetails","marble1"]}'
```

You should still be able to see the price private data.

```
{"docType":"marblePrivateDetails","name":"marble1","price":99}
```

Transfer marble2 to "tom" by running the following command. This transaction will create a third new block on the chain.

```
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/
↪src/github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.
↪com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem␣
↪-C mychannel -n marblesp -c '{"Args":["transferMarble","marble2","tom"]}'
```

Switch back to the Terminal window and view the private data logs for this peer again. You should see the block height increase by 1.

```
docker logs peer0.org1.example.com 2>&1 | grep -i -a -E 'private|pvt|privdata
↪'
```

Back in the peer container, query for the marble1 price data by running the following command:

```
peer chaincode query -C mychannel -n marblesp -c '{"Args":[
↪"readMarblePrivateDetails","marble1"]}'
```

You should still be able to see the price data.

```
{"docType":"marblePrivateDetails","name":"marble1","price":99}
```

Finally, transfer marble2 to "jerry" by running the following command. This transaction will create a fourth new block on the chain. The `price` private data should be purged after this transaction.

```
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/
↪src/github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.
↪com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem␣
↪-C mychannel -n marblesp -c '{"Args":["transferMarble","marble2","jerry"]}'
```

Switch back to the Terminal window and view the private data logs for this peer again. You should see the block height increase by 1.

```
docker logs peer0.org1.example.com 2>&1 | grep -i -a -E 'private|pvt|privdata
↪'
```

Back in the peer container, query for the marble1 price data by running the following command:

```
peer chaincode query -C mychannel -n marblesp -c '{"Args":[
↪"readMarblePrivateDetails","marble1"]}'
```

Because the price data has been purged, you should no longer be able to see it. You should see something similar to:

```
Error: endorsement failure during query. response: status:500
message:"{\"Error\":\"Marble private details does not exist: marble1\"}"
```

6.5.9 Using indexes with private data

Indexes can also be applied to private data collections, by packaging indexes in the `META-INF/statedb/couchdb/collections/<collection_name>/indexes` directory alongside the chaincode. An example index is available here .

For deployment of chaincode to production environments, it is recommended to define any indexes alongside chaincode so that the chaincode and supporting indexes are deployed automatically as a unit, once the chaincode has been installed on a peer and instantiated on a channel. The associated indexes are automatically deployed upon chaincode instantiation on the channel when the `--collections-config` flag is specified pointing to the location of the collection JSON file.

6.5.10 Additional resources

For additional private data education, a video tutorial has been created.

6.6 Chaincode Tutorials

6.6.1 What is Chaincode?

Chaincode is a program, written in Go, node.js, or Java that implements a prescribed interface. Chaincode runs in a secured Docker container isolated from the endorsing peer process. Chaincode initializes and manages ledger state through transactions submitted by applications.

A chaincode typically handles business logic agreed to by members of the network, so it may be considered as a "smart contract". State created by a chaincode is scoped exclusively to that chaincode and can't be accessed directly by another chaincode. However, within the same network, given the appropriate permission a chaincode may invoke another chaincode to access its state.

6.6.2 Two Personas

We offer two different perspectives on chaincode. One, from the perspective of an application developer developing a blockchain application/solution entitled *Chaincode for Developers*, and the other, *Chaincode for Operators* oriented to the blockchain network operator who is responsible for managing a blockchain network, and who would leverage the Hyperledger Fabric API to install, instantiate, and upgrade chaincode, but would likely not be involved in the development of a chaincode application.

6.7 Chaincode for Developers

6.7.1 What is Chaincode?

Chaincode is a program, written in Go, node.js, or Java that implements a prescribed interface. Chaincode runs in a secured Docker container isolated from the endorsing peer process. Chaincode initializes and manages the ledger state through transactions submitted by applications.

A chaincode typically handles business logic agreed to by members of the network, so it similar to a "smart contract". A chaincode can be invoked to update or query the ledger in a proposal transaction. Given the appropriate permission, a chaincode may invoke another chaincode, either in the same channel or in different channels, to access its state. Note that, if the called chaincode is on a different channel from the calling chaincode, only read query is allowed. That is, the called chaincode on a different channel is only a `Query`, which does not participate in state validation checks in subsequent commit phase.

In the following sections, we will explore chaincode through the eyes of an application developer. We'll present a simple chaincode sample application and walk through the purpose of each method in the Chaincode Shim API.

6.7.2 Chaincode API

Note: There is another set of chaincode APIs that allow the client (submitter) identity to be used for access control decisions, whether that is based on client identity itself, or the org identity, or on a client identity attribute. For example an asset that is represented as a key/value may include the client's identity, and only this client may be authorized to make updates to the key/value. The client identity library has APIs that chaincode can use to retrieve this submitter information to make such access control decisions.

We won't cover that in this tutorial, however it is documented here.

Every chaincode program must implement the `Chaincode` interface:

- Go
- node.js
- Java

whose methods are called in response to received transactions. In particular the `Init` method is called when a chaincode receives an `instantiate` or `upgrade` transaction so that the chaincode may perform any necessary initialization, including initialization of application state. The `Invoke` method is called in response to receiving an `invoke` transaction to process transaction proposals.

The other interface in the chaincode "shim" APIs is the `ChaincodeStubInterface`:

- Go
- node.js
- Java

which is used to access and modify the ledger, and to make invocations between chaincodes.

In this tutorial using Go chaincode, we will demonstrate the use of these APIs by implementing a simple chaincode application that manages simple "assets".

6.7.3 Simple Asset Chaincode

Our application is a basic sample chaincode to create assets (key-value pairs) on the ledger.

Choosing a Location for the Code

If you haven't been doing programming in Go, you may want to make sure that you have *Go Programming Language* installed and your system properly configured.

Now, you will want to create a directory for your chaincode application as a child directory of `$GOPATH/src/`.

To keep things simple, let's use the following command:

```
mkdir -p $GOPATH/src/sacc && cd $GOPATH/src/sacc
```

Now, let's create the source file that we'll fill in with code:

```
touch sacc.go
```

Housekeeping

First, let's start with some housekeeping. As with every chaincode, it implements the Chaincode interface in particular, `Init` and `Invoke` functions. So, let's add the Go import statements for the necessary dependencies for our chaincode. We'll import the chaincode shim package and the peer protobuf package. Next, let's add a struct `SimpleAsset` as a receiver for Chaincode shim functions.

```
package main

import (
    "fmt"

    "github.com/hyperledger/fabric/core/chaincode/shim"
    "github.com/hyperledger/fabric/protos/peer"
```

(continues on next page)

(continued from previous page)

```
)

// SimpleAsset implements a simple chaincode to manage an asset
type SimpleAsset struct {
}
```

Initializing the Chaincode

Next, we'll implement the `Init` function.

```
// Init is called during chaincode instantiation to initialize any data.
func (t *SimpleAsset) Init(stub shim.ChaincodeStubInterface) peer.Response {

}
```

Note: Note that chaincode upgrade also calls this function. When writing a chaincode that will upgrade an existing one, make sure to modify the `Init` function appropriately. In particular, provide an empty "Init" method if there's no "migration" or nothing to be initialized as part of the upgrade.

Next, we'll retrieve the arguments to the `Init` call using the ChaincodeStubInterface.GetStringArgs function and check for validity. In our case, we are expecting a key-value pair.

```
// Init is called during chaincode instantiation to initialize any
// data. Note that chaincode upgrade also calls this function to reset
// or to migrate data, so be careful to avoid a scenario where you
// inadvertently clobber your ledger's data!
func (t *SimpleAsset) Init(stub shim.ChaincodeStubInterface) peer.Response {
  // Get the args from the transaction proposal
  args := stub.GetStringArgs()
  if len(args) != 2 {
    return shim.Error("Incorrect arguments. Expecting a key and a value")
  }
}
```

Next, now that we have established that the call is valid, we'll store the initial state in the ledger. To do this, we will call ChaincodeStubInterface.PutState with the key and value passed in as the arguments. Assuming all went well, return a peer.Response object that indicates the initialization was a success.

```
// Init is called during chaincode instantiation to initialize any
// data. Note that chaincode upgrade also calls this function to reset
// or to migrate data, so be careful to avoid a scenario where you
// inadvertently clobber your ledger's data!
func (t *SimpleAsset) Init(stub shim.ChaincodeStubInterface) peer.Response {
  // Get the args from the transaction proposal
  args := stub.GetStringArgs()
  if len(args) != 2 {
    return shim.Error("Incorrect arguments. Expecting a key and a value")
  }

  // Set up any variables or assets here by calling stub.PutState()

  // We store the key and the value on the ledger
  err := stub.PutState(args[0], []byte(args[1]))
```

(continues on next page)

(continued from previous page)

```
  if err != nil {
    return shim.Error(fmt.Sprintf("Failed to create asset: %s", args[0]))
  }
  return shim.Success(nil)
}
```

Invoking the Chaincode

First, let's add the `Invoke` function's signature.

```
// Invoke is called per transaction on the chaincode. Each transaction is
// either a 'get' or a 'set' on the asset created by Init function. The 'set'
// method may create a new asset by specifying a new key-value pair.
func (t *SimpleAsset) Invoke(stub shim.ChaincodeStubInterface) peer.Response {

}
```

As with the `Init` function above, we need to extract the arguments from the `ChaincodeStubInterface`. The `Invoke` function's arguments will be the name of the chaincode application function to invoke. In our case, our application will simply have two functions: `set` and `get`, that allow the value of an asset to be set or its current state to be retrieved. We first call ChaincodeStubInterface.GetFunctionAndParameters to extract the function name and the parameters to that chaincode application function.

```
// Invoke is called per transaction on the chaincode. Each transaction is
// either a 'get' or a 'set' on the asset created by Init function. The Set
// method may create a new asset by specifying a new key-value pair.
func (t *SimpleAsset) Invoke(stub shim.ChaincodeStubInterface) peer.Response {
    // Extract the function and args from the transaction proposal
    fn, args := stub.GetFunctionAndParameters()

}
```

Next, we'll validate the function name as being either `set` or `get`, and invoke those chaincode application functions, returning an appropriate response via the `shim.Success` or `shim.Error` functions that will serialize the response into a gRPC protobuf message.

```
// Invoke is called per transaction on the chaincode. Each transaction is
// either a 'get' or a 'set' on the asset created by Init function. The Set
// method may create a new asset by specifying a new key-value pair.
func (t *SimpleAsset) Invoke(stub shim.ChaincodeStubInterface) peer.Response {
    // Extract the function and args from the transaction proposal
    fn, args := stub.GetFunctionAndParameters()

    var result string
    var err error
    if fn == "set" {
            result, err = set(stub, args)
    } else {
            result, err = get(stub, args)
    }
    if err != nil {
            return shim.Error(err.Error())
    }
```

(continues on next page)

(continued from previous page)

```
    // Return the result as success payload
    return shim.Success([]byte(result))
}
```

Implementing the Chaincode Application

As noted, our chaincode application implements two functions that can be invoked via the `Invoke` function. Let's implement those functions now. Note that as we mentioned above, to access the ledger's state, we will leverage the ChaincodeStubInterface.PutState and ChaincodeStubInterface.GetState functions of the chaincode shim API.

```
// Set stores the asset (both key and value) on the ledger. If the key exists,
// it will override the value with the new one
func set(stub shim.ChaincodeStubInterface, args []string) (string, error) {
    if len(args) != 2 {
            return "", fmt.Errorf("Incorrect arguments. Expecting a key and a value")
    }

    err := stub.PutState(args[0], []byte(args[1]))
    if err != nil {
            return "", fmt.Errorf("Failed to set asset: %s", args[0])
    }
    return args[1], nil
}

// Get returns the value of the specified asset key
func get(stub shim.ChaincodeStubInterface, args []string) (string, error) {
    if len(args) != 1 {
            return "", fmt.Errorf("Incorrect arguments. Expecting a key")
    }

    value, err := stub.GetState(args[0])
    if err != nil {
            return "", fmt.Errorf("Failed to get asset: %s with error: %s", args[0],␣
↪err)
    }
    if value == nil {
            return "", fmt.Errorf("Asset not found: %s", args[0])
    }
    return string(value), nil
}
```

Pulling it All Together

Finally, we need to add the `main` function, which will call the shim.Start function. Here's the whole chaincode program source.

```
package main

import (
    "fmt"

    "github.com/hyperledger/fabric/core/chaincode/shim"
    "github.com/hyperledger/fabric/protos/peer"
```

(continues on next page)

(continued from previous page)

```
)

// SimpleAsset implements a simple chaincode to manage an asset
type SimpleAsset struct {
}

// Init is called during chaincode instantiation to initialize any
// data. Note that chaincode upgrade also calls this function to reset
// or to migrate data.
func (t *SimpleAsset) Init(stub shim.ChaincodeStubInterface) peer.Response {
    // Get the args from the transaction proposal
    args := stub.GetStringArgs()
    if len(args) != 2 {
            return shim.Error("Incorrect arguments. Expecting a key and a value")
    }

    // Set up any variables or assets here by calling stub.PutState()

    // We store the key and the value on the ledger
    err := stub.PutState(args[0], []byte(args[1]))
    if err != nil {
            return shim.Error(fmt.Sprintf("Failed to create asset: %s", args[0]))
    }
    return shim.Success(nil)
}

// Invoke is called per transaction on the chaincode. Each transaction is
// either a 'get' or a 'set' on the asset created by Init function. The Set
// method may create a new asset by specifying a new key-value pair.
func (t *SimpleAsset) Invoke(stub shim.ChaincodeStubInterface) peer.Response {
    // Extract the function and args from the transaction proposal
    fn, args := stub.GetFunctionAndParameters()

    var result string
    var err error
    if fn == "set" {
            result, err = set(stub, args)
    } else { // assume 'get' even if fn is nil
            result, err = get(stub, args)
    }
    if err != nil {
            return shim.Error(err.Error())
    }

    // Return the result as success payload
    return shim.Success([]byte(result))
}

// Set stores the asset (both key and value) on the ledger. If the key exists,
// it will override the value with the new one
func set(stub shim.ChaincodeStubInterface, args []string) (string, error) {
    if len(args) != 2 {
            return "", fmt.Errorf("Incorrect arguments. Expecting a key and a value")
    }

    err := stub.PutState(args[0], []byte(args[1]))
    if err != nil {
```

(continues on next page)

(continued from previous page)

```
            return "", fmt.Errorf("Failed to set asset: %s", args[0])
    }
    return args[1], nil
}

// Get returns the value of the specified asset key
func get(stub shim.ChaincodeStubInterface, args []string) (string, error) {
    if len(args) != 1 {
            return "", fmt.Errorf("Incorrect arguments. Expecting a key")
    }

    value, err := stub.GetState(args[0])
    if err != nil {
            return "", fmt.Errorf("Failed to get asset: %s with error: %s", args[0],␣
↪err)
    }
    if value == nil {
            return "", fmt.Errorf("Asset not found: %s", args[0])
    }
    return string(value), nil
}

// main function starts up the chaincode in the container during instantiate
func main() {
    if err := shim.Start(new(SimpleAsset)); err != nil {
            fmt.Printf("Error starting SimpleAsset chaincode: %s", err)
    }
}
```

Building Chaincode

Now let's compile your chaincode.

```
go get -u github.com/hyperledger/fabric/core/chaincode/shim
go build
```

Assuming there are no errors, now we can proceed to the next step, testing your chaincode.

Testing Using dev mode

Normally chaincodes are started and maintained by peer. However in "dev mode", chaincode is built and started by the user. This mode is useful during chaincode development phase for rapid code/build/run/debug cycle turnaround.

We start "dev mode" by leveraging pre-generated orderer and channel artifacts for a sample dev network. As such, the user can immediately jump into the process of compiling chaincode and driving calls.

6.7.4 Install Hyperledger Fabric Samples

If you haven't already done so, please *Install Samples, Binaries and Docker Images*.

Navigate to the `chaincode-docker-devmode` directory of the `fabric-samples` clone:

```
cd chaincode-docker-devmode
```

Now open three terminals and navigate to your `chaincode-docker-devmode` directory in each.

6.7.5 Terminal 1 - Start the network

```
docker-compose -f docker-compose-simple.yaml up
```

The above starts the network with the `SingleSampleMSPSolo` orderer profile and launches the peer in "dev mode". It also launches two additional containers - one for the chaincode environment and a CLI to interact with the chaincode. The commands for create and join channel are embedded in the CLI container, so we can jump immediately to the chaincode calls.

6.7.6 Terminal 2 - Build & start the chaincode

```
docker exec -it chaincode bash
```

You should see the following:

```
root@d2629980e76b:/opt/gopath/src/chaincode#
```

Now, compile your chaincode:

```
cd sacc
go build
```

Now run the chaincode:

```
CORE_PEER_ADDRESS=peer:7052 CORE_CHAINCODE_ID_NAME=mycc:0 ./sacc
```

The chaincode is started with peer and chaincode logs indicating successful registration with the peer. Note that at this stage the chaincode is not associated with any channel. This is done in subsequent steps using the `instantiate` command.

6.7.7 Terminal 3 - Use the chaincode

Even though you are in `--peer-chaincodedev` mode, you still have to install the chaincode so the life-cycle system chaincode can go through its checks normally. This requirement may be removed in future when in `--peer-chaincodedev` mode.

We'll leverage the CLI container to drive these calls.

```
docker exec -it cli bash
```

```
peer chaincode install -p chaincodedev/chaincode/sacc -n mycc -v 0
peer chaincode instantiate -n mycc -v 0 -c '{"Args":["a","10"]}' -C myc
```

Now issue an invoke to change the value of "a" to "20".

```
peer chaincode invoke -n mycc -c '{"Args":["set", "a", "20"]}' -C myc
```

Finally, query `a`. We should see a value of `20`.

```
peer chaincode query -n mycc -c '{"Args":["query","a"]}' -C myc
```

6.7.8 Testing new chaincode

By default, we mount only `sacc`. However, you can easily test different chaincodes by adding them to the `chaincode` subdirectory and relaunching your network. At this point they will be accessible in your `chaincode` container.

6.7.9 Chaincode encryption

In certain scenarios, it may be useful to encrypt values associated with a key in their entirety or simply in part. For example, if a person's social security number or address was being written to the ledger, then you likely would not want this data to appear in plaintext. Chaincode encryption is achieved by leveraging the entities extension which is a BCCSP wrapper with commodity factories and functions to perform cryptographic operations such as encryption and elliptic curve digital signatures. For example, to encrypt, the invoker of a chaincode passes in a cryptographic key via the transient field. The same key may then be used for subsequent query operations, allowing for proper decryption of the encrypted state values.

For more information and samples, see the Encc Example within the `fabric/examples` directory. Pay specific attention to the `utils.go` helper program. This utility loads the chaincode shim APIs and Entities extension and builds a new class of functions (e.g. `encryptAndPutState` & `getStateAndDecrypt`) that the sample encryption chaincode then leverages. As such, the chaincode can now marry the basic shim APIs of `Get` and `Put` with the added functionality of `Encrypt` and `Decrypt`.

6.7.10 Managing external dependencies for chaincode written in Go

If your chaincode requires packages not provided by the Go standard library, you will need to include those packages with your chaincode. There are many tools available for managing (or "vendoring") these dependencies. The following demonstrates how to use `govendor`:

```
govendor init
govendor add +external  // Add all external package, or
govendor add github.com/external/pkg // Add specific external package
```

This imports the external dependencies into a local `vendor` directory. `peer chaincode package` and `peer chaincode install` operations will then include code associated with the dependencies into the chaincode package.

6.8 Chaincode for Operators

6.8.1 What is Chaincode?

Chaincode is a program, written in Go, node.js, or Java that implements a prescribed interface. Chaincode runs in a secured Docker container isolated from the endorsing peer process. Chaincode initializes and manages ledger state through transactions submitted by applications.

A chaincode typically handles business logic agreed to by members of the network, so it may be considered as a "smart contract". State created by a chaincode is scoped exclusively to that chaincode and can't be accessed directly by another chaincode. However, within the same network, given the appropriate permission a chaincode may invoke another chaincode to access its state.

In the following sections, we will explore chaincode through the eyes of a blockchain network operator, Noah. For Noah's interests, we will focus on chaincode lifecycle operations; the process of packaging, installing, instantiating and upgrading the chaincode as a function of the chaincode's operational lifecycle within a blockchain network.

6.8.2 Chaincode lifecycle

The Hyperledger Fabric API enables interaction with the various nodes in a blockchain network - the peers, orderers and MSPs - and it also allows one to package, install, instantiate and upgrade chaincode on the endorsing peer nodes. The Hyperledger Fabric language-specific SDKs abstract the specifics of the Hyperledger Fabric API to facilitate application development, though it can be used to manage a chaincode's lifecycle. Additionally, the Hyperledger Fabric API can be accessed directly via the CLI, which we will use in this document.

We provide four commands to manage a chaincode's lifecycle: `package`, `install`, `instantiate`, and `upgrade`. In a future release, we are considering adding `stop` and `start` transactions to disable and re-enable a chaincode without having to actually uninstall it. After a chaincode has been successfully installed and instantiated, the chaincode is active (running) and can process transactions via the `invoke` transaction. A chaincode may be upgraded any time after it has been installed.

6.8.3 Packaging

The chaincode package consists of 3 parts:

- the chaincode, as defined by `ChaincodeDeploymentSpec` or CDS. The CDS defines the chaincode package in terms of the code and other properties such as name and version,
- an optional instantiation policy which can be syntactically described by the same policy used for endorsement and described in *Endorsement policies*, and
- a set of signatures by the entities that "own" the chaincode.

The signatures serve the following purposes:

- to establish an ownership of the chaincode,
- to allow verification of the contents of the package, and
- to allow detection of package tampering.

The creator of the instantiation transaction of the chaincode on a channel is validated against the instantiation policy of the chaincode.

Creating the package

There are two approaches to packaging chaincode. One for when you want to have multiple owners of a chaincode, and hence need to have the chaincode package signed by multiple identities. This workflow requires that we initially create a signed chaincode package (a `SignedCDS`) which is subsequently passed serially to each of the other owners for signing.

The simpler workflow is for when you are deploying a SignedCDS that has only the signature of the identity of the node that is issuing the `install` transaction.

We will address the more complex case first. However, you may skip ahead to the *Installing chaincode* section below if you do not need to worry about multiple owners just yet.

To create a signed chaincode package, use the following command:

```
peer chaincode package -n mycc -p github.com/hyperledger/fabric/examples/chaincode/go/
↪example02/cmd -v 0 -s -S -i "AND('OrgA.admin')" ccpack.out
```

The `-s` option creates a package that can be signed by multiple owners as opposed to simply creating a raw CDS. When `-s` is specified, the `-S` option must also be specified if other owners are going to need to sign. Otherwise, the process will create a SignedCDS that includes only the instantiation policy in addition to the CDS.

The `-S` option directs the process to sign the package using the MSP identified by the value of the `localMspid` property in `core.yaml`.

The `-S` option is optional. However if a package is created without a signature, it cannot be signed by any other owner using the `signpackage` command.

The optional `-i` option allows one to specify an instantiation policy for the chaincode. The instantiation policy has the same format as an endorsement policy and specifies which identities can instantiate the chaincode. In the example above, only the admin of OrgA is allowed to instantiate the chaincode. If no policy is provided, the default policy is used, which only allows the admin identity of the peer's MSP to instantiate chaincode.

Package signing

A chaincode package that was signed at creation can be handed over to other owners for inspection and signing. The workflow supports out-of-band signing of chaincode package.

The ChaincodeDeploymentSpec may be optionally be signed by the collective owners to create a SignedChaincodeDeploymentSpec (or SignedCDS). The SignedCDS contains 3 elements:

1. The CDS contains the source code, the name, and version of the chaincode.
2. An instantiation policy of the chaincode, expressed as endorsement policies.
3. The list of chaincode owners, defined by means of Endorsement.

Note: Note that this endorsement policy is determined out-of-band to provide proper MSP principals when the chaincode is instantiated on some channels. If the instantiation policy is not specified, the default policy is any MSP administrator of the channel.

Each owner endorses the ChaincodeDeploymentSpec by combining it with that owner's identity (e.g. certificate) and signing the combined result.

A chaincode owner can sign a previously created signed package using the following command:

```
peer chaincode signpackage ccpack.out signedccpack.out
```

Where `ccpack.out` and `signedccpack.out` are the input and output packages, respectively. `signedccpack.out` contains an additional signature over the package signed using the Local MSP.

Installing chaincode

The `install` transaction packages a chaincode's source code into a prescribed format called a `ChaincodeDeploymentSpec` (or CDS) and installs it on a peer node that will run that chaincode.

Note: You must install the chaincode on **each** endorsing peer node of a channel that will run your chaincode.

When the `install` API is given simply a `ChaincodeDeploymentSpec`, it will default the instantiation policy and include an empty owner list.

Note: Chaincode should only be installed on endorsing peer nodes of the owning members of the chaincode to protect the confidentiality of the chaincode logic from other members on the network. Those members without the chaincode, can't be the endorsers of the chaincode's transactions; that is, they can't execute the chaincode. However, they can still validate and commit the transactions to the ledger.

To install a chaincode, send a SignedProposal to the `lifecycle system chaincode` (LSCC) described in the *System Chaincode* section. For example, to install the **sacc** sample chaincode described in section *Simple Asset Chaincode* using the CLI, the command would look like the following:

```
peer chaincode install -n asset_mgmt -v 1.0 -p sacc
```

The CLI internally creates the SignedChaincodeDeploymentSpec for **sacc** and sends it to the local peer, which calls the `Install` method on the LSCC. The argument to the `-p` option specifies the path to the chaincode, which must be located within the source tree of the user's `GOPATH`, e.g. `$GOPATH/src/sacc`. See the *CLI* section for a complete description of the command options.

Note that in order to install on a peer, the signature of the SignedProposal must be from 1 of the peer's local MSP administrators.

Instantiate

The `instantiate` transaction invokes the `lifecycle System Chaincode` (LSCC) to create and initialize a chaincode on a channel. This is a chaincode-channel binding process: a chaincode may be bound to any number of channels and operate on each channel individually and independently. In other words, regardless of how many other channels on which a chaincode might be installed and instantiated, state is kept isolated to the channel to which a transaction is submitted.

The creator of an `instantiate` transaction must satisfy the instantiation policy of the chaincode included in SignedCDS and must also be a writer on the channel, which is configured as part of the channel creation. This is important for the security of the channel to prevent rogue entities from deploying chaincodes or tricking members to execute chaincodes on an unbound channel.

For example, recall that the default instantiation policy is any channel MSP administrator, so the creator of a chaincode instantiate transaction must be a member of the channel administrators. When the transaction proposal arrives at the endorser, it verifies the creator's signature against the instantiation policy. This is done again during the transaction validation before committing it to the ledger.

The instantiate transaction also sets up the endorsement policy for that chaincode on the channel. The endorsement policy describes the attestation requirements for the transaction result to be accepted by members of the channel.

For example, using the CLI to instantiate the **sacc** chaincode and initialize the state with `john` and `0`, the command would look like the following:

```
peer chaincode instantiate -n sacc -v 1.0 -c '{"Args":["john","0"]}' -P "AND ('Org1.
↪member','Org2.member')"
```

Note: Note the endorsement policy (CLI uses polish notation), which requires an endorsement from both a member of Org1 and Org2 for all transactions to **sacc**. That is, both Org1 and Org2 must sign the result of executing the *Invoke* on **sacc** for the transactions to be valid.

After being successfully instantiated, the chaincode enters the active state on the channel and is ready to process any transaction proposals of type ENDORSER_TRANSACTION. The transactions are processed concurrently as they arrive at the endorsing peer.

Upgrade

A chaincode may be upgraded any time by changing its version, which is part of the SignedCDS. Other parts, such as owners and instantiation policy are optional. However, the chaincode name must be the same; otherwise it would be considered as a totally different chaincode.

Prior to upgrade, the new version of the chaincode must be installed on the required endorsers. Upgrade is a transaction similar to the instantiate transaction, which binds the new version of the chaincode to the channel. Other channels bound to the old version of the chaincode still run with the old version. In other words, the `upgrade` transaction only affects one channel at a time, the channel to which the transaction is submitted.

Note: Note that since multiple versions of a chaincode may be active simultaneously, the upgrade process doesn't automatically remove the old versions, so user must manage this for the time being.

There's one subtle difference with the `instantiate` transaction: the `upgrade` transaction is checked against the current chaincode instantiation policy, not the new policy (if specified). This is to ensure that only existing members specified in the current instantiation policy may upgrade the chaincode.

Note: Note that during upgrade, the chaincode `Init` function is called to perform any data related updates or re-initialize it, so care must be taken to avoid resetting states when upgrading chaincode.

Stop and Start

Note that `stop` and `start` lifecycle transactions have not yet been implemented. However, you may stop a chaincode manually by removing the chaincode container and the SignedCDS package from each of the endorsers. This is done by deleting the chaincode's container on each of the hosts or virtual machines on which the endorsing peer nodes are running, and then deleting the SignedCDS from each of the endorsing peer nodes:

Note: TODO - in order to delete the CDS from the peer node, you would need to enter the peer node's container, first. We really need to provide a utility script that can do this.

```
docker rm -f <container id>
rm /var/hyperledger/production/chaincodes/<ccname>:<ccversion>
```

Stop would be useful in the workflow for doing upgrade in controlled manner, where a chaincode can be stopped on a channel on all peers before issuing an upgrade.

CLI

Note: We are assessing the need to distribute platform-specific binaries for the Hyperledger Fabric `peer` binary. For the time being, you can simply invoke the commands from within a running docker container.

To view the currently available CLI commands, execute the following command from within a running `fabric-peer` Docker container:

```
docker run -it hyperledger/fabric-peer bash
# peer chaincode --help
```

Which shows output similar to the example below:

```
Usage:
  peer chaincode [command]

```

(continues on next page)

(continued from previous page)

```
Available Commands:
  install     Package the specified chaincode into a deployment spec and save it on␣
↪the peer's path.
  instantiate Deploy the specified chaincode to the network.
  invoke      Invoke the specified chaincode.
  list        Get the instantiated chaincodes on a channel or installed chaincodes on␣
↪a peer.
  package     Package the specified chaincode into a deployment spec.
  query       Query using the specified chaincode.
  signpackage Sign the specified chaincode package
  upgrade     Upgrade chaincode.

Flags:
      --cafile string      Path to file containing PEM-encoded trusted certificate(s)␣
↪for the ordering endpoint
  -h, --help               help for chaincode
  -o, --orderer string     Ordering service endpoint
      --tls                Use TLS when communicating with the orderer endpoint
      --transient string   Transient map of arguments in JSON encoding

Global Flags:
      --logging-level string       Default logging level and overrides, see core.yaml␣
↪for full syntax
      --test.coverprofile string   Done (default "coverage.cov")
  -v, --version

Use "peer chaincode [command] --help" for more information about a command.
```

To facilitate its use in scripted applications, the `peer` command always produces a non-zero return code in the event of command failure.

Example of chaincode commands:

```
peer chaincode install -n mycc -v 0 -p path/to/my/chaincode/v0
peer chaincode instantiate -n mycc -v 0 -c '{"Args":["a", "b", "c"]}' -C mychannel
peer chaincode install -n mycc -v 1 -p path/to/my/chaincode/v1
peer chaincode upgrade -n mycc -v 1 -c '{"Args":["d", "e", "f"]}' -C mychannel
peer chaincode query -C mychannel -n mycc -c '{"Args":["query","e"]}'
peer chaincode invoke -o orderer.example.com:7050  --tls --cafile $ORDERER_CA -C␣
↪mychannel -n mycc -c '{"Args":["invoke","a","b","10"]}'
```

6.8.4 System chaincode

System chaincode has the same programming model except that it runs within the peer process rather than in an isolated container like normal chaincode. Therefore, system chaincode is built into the peer executable and doesn't follow the same lifecycle described above. In particular, **install**, **instantiate** and **upgrade** do not apply to system chaincodes.

The purpose of system chaincode is to shortcut gRPC communication cost between peer and chaincode, and tradeoff the flexibility in management. For example, a system chaincode can only be upgraded with the peer binary. It must also register with a fixed set of parameters compiled in and doesn't have endorsement policies or endorsement policy functionality.

System chaincode is used in Hyperledger Fabric to implement a number of system behaviors so that they can be replaced or modified as appropriate by a system integrator.

The current list of system chaincodes:

1. LSCC Lifecycle system chaincode handles lifecycle requests described above.
2. CSCC Configuration system chaincode handles channel configuration on the peer side.
3. QSCC Query system chaincode provides ledger query APIs such as getting blocks and transactions.

The former system chaincodes for endorsement and validation have been replaced by the pluggable endorsement and validation function as described by the *Pluggable transaction endorsement and validation* documentation.

Extreme care must be taken when modifying or replacing these system chaincodes, especially LSCC.

6.9 System Chaincode Plugins

System chaincodes are specialized chaincodes that run as part of the peer process as opposed to user chaincodes that run in separate docker containers. As such they have more access to resources in the peer and can be used for implementing features that are difficult or impossible to be implemented through user chaincodes. Examples of System Chaincodes include QSCC (Query System Chaincode) for ledger and other Fabric-related queries, CSCC (Configuration System Chaincode) which helps regulate access control, and LSCC (Lifecycle System Chaincode).

Unlike a user chaincode, a system chaincode is not installed and instantiated using proposals from SDKs or CLI. It is registered and deployed by the peer at start-up.

System chaincodes can be linked to a peer in two ways: statically, and dynamically using Go plugins. This tutorial will outline how to develop and load system chaincodes as plugins.

6.9.1 Developing Plugins

A system chaincode is a program written in Go and loaded using the Go plugin package.

A plugin includes a main package with exported symbols and is built with the command `go build -buildmode=plugin`.

Every system chaincode must implement the Chaincode Interface and export a constructor method that matches the signature `func New() shim.Chaincode` in the main package. An example can be found in the repository at `examples/plugin/scc`.

Existing chaincodes such as the QSCC can also serve as templates for certain features, such as access control, that are typically implemented through system chaincodes. The existing system chaincodes also serve as a reference for best-practices on things like logging and testing.

Note: On imported packages: the Go standard library requires that a plugin must include the same version of imported packages as the host application (Fabric, in this case).

6.9.2 Configuring Plugins

Plugins are configured in the `chaincode.systemPlugin` section in `core.yaml`:

```
chaincode:
  systemPlugins:
    - enabled: true
      name: mysyscc
      path: /opt/lib/syscc.so
```

(continues on next page)

(continued from previous page)

```
      invokableExternal: true
      invokableCC2CC: true
```

A system chaincode must also be whitelisted in the `chaincode.system` section in `core.yaml`:

```
chaincode:
  system:
    mysyscc: enable
```

6.10 Using CouchDB

This tutorial will describe the steps required to use the CouchDB as the state database with Hyperledger Fabric. By now, you should be familiar with Fabric concepts and have explored some of the samples and tutorials.

The tutorial will take you through the following steps:

1. *Enable CouchDB in Hyperledger Fabric*
2. *Create an index*
3. *Add the index to your chaincode folder*
4. *Install and instantiate the Chaincode*
5. *Query the CouchDB State Database*
6. *Use best practices for queries and indexes*
7. *Query the CouchDB State Database With Pagination*
8. *Update an Index*
9. *Delete an Index*

For a deeper dive into CouchDB refer to *CouchDB as the State Database* and for more information on the Fabric ledger refer to the Ledger topic. Follow the tutorial below for details on how to leverage CouchDB in your blockchain network.

Throughout this tutorial we will use the Marbles sample as our use case to demonstrate how to use CouchDB with Fabric and will deploy Marbles to the *Building Your First Network* (BYFN) tutorial network. You should have completed the task *Install Samples, Binaries and Docker Images*. However, running the BYFN tutorial is not a prerequisite for this tutorial, instead the necessary commands are provided throughout this tutorial to use the network.

6.10.1 Why CouchDB?

Fabric supports two types of peer databases. LevelDB is the default state database embedded in the peer node and stores chaincode data as simple key-value pairs and supports key, key range, and composite key queries only. CouchDB is an optional alternate state database that supports rich queries when chaincode data values are modeled as JSON. Rich queries are more flexible and efficient against large indexed data stores, when you want to query the actual data value content rather than the keys. CouchDB is a JSON document datastore rather than a pure key-value store therefore enabling indexing of the contents of the documents in the database.

In order to leverage the benefits of CouchDB, namely content-based JSON queries,your data must be modeled in JSON format. You must decide whether to use LevelDB or CouchDB before setting up your network. Switching a peer from using LevelDB to CouchDB is not supported due to data compatibility issues. All peers on the network must use the same database type. If you have a mix of JSON and binary data values, you can still use CouchDB, however the binary values can only be queried based on key, key range, and composite key queries.

6.10.2 Enable CouchDB in Hyperledger Fabric

CouchDB runs as a separate database process alongside the peer, therefore there are additional considerations in terms of setup, management, and operations. A docker image of CouchDB is available and we recommend that it be run on the same server as the peer. You will need to setup one CouchDB container per peer and update each peer container by changing the configuration found in `core.yaml` to point to the CouchDB container. The `core.yaml` file must be located in the directory specified by the environment variable FABRIC_CFG_PATH:

- For docker deployments, `core.yaml` is pre-configured and located in the peer container `FABRIC_CFG_PATH` folder. However when using docker environments, you typically pass environment variables by editing the `docker-compose-couch.yaml` to override the core.yaml
- For native binary deployments, `core.yaml` is included with the release artifact distribution.

Edit the `stateDatabase` section of `core.yaml`. Specify `CouchDB` as the `stateDatabase` and fill in the associated `couchDBConfig` properties. For more details on configuring CouchDB to work with fabric, refer here. To view an example of a core.yaml file configured for CouchDB, examine the BYFN `docker-compose-couch.yaml` in the `HyperLedger/fabric-samples/first-network` directory.

6.10.3 Create an index

Why are indexes important?

Indexes allow a database to be queried without having to examine every row with every query, making them run faster and more efficiently. Normally, indexes are built for frequently occurring query criteria allowing the data to be queried more efficiently. To leverage the major benefit of CouchDB – the ability to perform rich queries against JSON data – indexes are not required, but they are strongly recommended for performance. Also, if sorting is required in a query, CouchDB requires an index of the sorted fields.

Note: Rich queries that do not have an index will work but may throw a warning in the CouchDB log that the index was not found. However, if a rich query includes a sort specification, then an index on that field is required; otherwise, the query will fail and an error will be thrown.

To demonstrate building an index, we will use the data from the Marbles sample. In this example, the Marbles data structure is defined as:

```
type marble struct {
        ObjectType string `json:"docType"` //docType is used to distinguish the␣
↪various types of objects in state database
        Name       string `json:"name"`    //the field tags are needed to keep case␣
↪from bouncing around
        Color      string `json:"color"`
        Size       int    `json:"size"`
        Owner      string `json:"owner"`
}
```

In this structure, the attributes (`docType`, `name`, `color`, `size`, `owner`) define the ledger data associated with the asset. The attribute `docType` is a pattern used in the chaincode to differentiate different data types that may need to be queried separately. When using CouchDB, it recommended to include this `docType` attribute to distinguish each type of document in the chaincode namespace. (Each chaincode is represented as its own CouchDB database, that is, each chaincode has its own namespace for keys.)

With respect to the Marbles data structure, `docType` is used to identify that this document/asset is a marble asset. Potentially there could be other documents/assets in the chaincode database. The documents in the database are searchable against all of these attribute values.

When defining an index for use in chaincode queries, each one must be defined in its own text file with the extension **.json* and the index definition must be formatted in the CouchDB index JSON format.

To define an index, three pieces of information are required:

- *fields*: these are the frequently queried fields
- *name*: name of the index
- *type*: always json in this context

For example, a simple index named `foo-index` for a field named `foo`.

```
{
    "index": {
        "fields": ["foo"]
    },
    "name" : "foo-index",
    "type" : "json"
}
```

Optionally the design document attribute `ddoc` can be specified on the index definition. A design document is CouchDB construct designed to contain indexes. Indexes can be grouped into design documents for efficiency but CouchDB recommends one index per design document.

Tip: When defining an index it is a good practice to include the `ddoc` attribute and value along with the index name. It is important to include this attribute to ensure that you can update the index later if needed. Also it gives you the ability to explicitly specify which index to use on a query.

Here is another example of an index definition from the Marbles sample with the index name `indexOwner` using multiple fields `docType` and `owner` and includes the `ddoc` attribute:

```
{
  "index":{
      "fields":["docType","owner"] // Names of the fields to be queried
  },
  "ddoc":"indexOwnerDoc", // (optional) Name of the design document in which the␣
↪index will be created.
  "name":"indexOwner",
  "type":"json"
}
```

In the example above, if the design document `indexOwnerDoc` does not already exist, it is automatically created when the index is deployed. An index can be constructed with one or more attributes specified in the list of fields and any combination of attributes can be specified. An attribute can exist in multiple indexes for the same docType. In the following example, `index1` only includes the attribute `owner`, `index2` includes the attributes `owner and color` and `index3` includes the attributes `owner, color and size`. Also, notice each index definition has its own `ddoc` value, following the CouchDB recommended practice.

```
{
  "index":{
      "fields":["owner"] // Names of the fields to be queried
  },
  "ddoc":"index1Doc", // (optional) Name of the design document in which the index␣
↪will be created.
  "name":"index1",
  "type":"json"
```

(continues on next page)

(continued from previous page)

```
}

{
  "index":{
      "fields":["owner", "color"] // Names of the fields to be queried
  },
  "ddoc":"index2Doc", // (optional) Name of the design document in which the index␣
↪will be created.
  "name":"index2",
  "type":"json"
}

{
  "index":{
      "fields":["owner", "color", "size"] // Names of the fields to be queried
  },
  "ddoc":"index3Doc", // (optional) Name of the design document in which the index␣
↪will be created.
  "name":"index3",
  "type":"json"
}
```

In general, you should model index fields to match the fields that will be used in query filters and sorts. For more details on building an index in JSON format refer to the CouchDB documentation.

A final word on indexing, Fabric takes care of indexing the documents in the database using a pattern called `index warming`. CouchDB does not typically index new or updated documents until the next query. Fabric ensures that indexes stay 'warm' by requesting an index update after every block of data is committed. This ensures queries are fast because they do not have to index documents before running the query. This process keeps the index current and refreshed every time new records are added to the state database.

6.10.4 Add the index to your chaincode folder

Once you finalize an index, it is ready to be packaged with your chaincode for deployment by being placed alongside it in the appropriate metadata folder.

If your chaincode installation and instantiation uses the Hyperledger Fabric Node SDK, the JSON index files can be located in any folder as long as it conforms to this directory structure. During the chaincode installation using the client.installChaincode() API, include the attribute (`metadataPath`) in the installation request. The value of the metadataPath is a string representing the absolute path to the directory structure containing the JSON index file(s).

Alternatively, if you are using the peer-commands to install and instantiate the chaincode, then the JSON index files must be located under the path `META-INF/statedb/couchdb/indexes` which is located inside the directory where the chaincode resides.

The Marbles sample below illustrates how the index is packaged with the chaincode which will be installed using the peer commands.

This sample includes one index named indexOwnerDoc:

```
{"index":{"fields":["docType","owner"]},"ddoc":"indexOwnerDoc", "name":"indexOwner",
↪"type":"json"}
```

Start the network

Try it yourself

Before installing and instantiating the marbles chaincode, we need to start up the BYFN network. For the sake of this tutorial, we want to operate from a known initial state. The following command will kill any active or stale docker containers and remove previously generated artifacts. Therefore let's run the following command to clean up any previous environments:

```
cd fabric-samples/first-network
./byfn.sh down
```

Now start up the BYFN network with CouchDB by running the following command:

```
./byfn.sh up -c mychannel -s couchdb
```

This will create a simple Fabric network consisting of a single channel named *mychannel* with two organizations (each maintaining two peer nodes) and an ordering service while using CouchDB as the state database.

6.10.5 Install and instantiate the Chaincode

Client applications interact with the blockchain ledger through chaincode. As such we need to install the chaincode on every peer that will execute and endorse our transactions and instantiate the chaincode on the channel. In the previous section, we demonstrated how to package the chaincode so they should be ready for deployment.

Chaincode is installed onto a peer and then instantiated onto the channel using peer-commands.

1. Use the peer chaincode install command to install the Marbles chaincode on a peer.

Try it yourself

Assuming you have started the BYFN network, navigate into the CLI container using the command:

```
docker exec -it cli bash
```

Use the following command to install the Marbles chaincode from the git repository onto a peer in your BYFN network. The CLI container defaults to using peer0 of org1:

```
peer chaincode install -n marbles -v 1.0 -p github.com/chaincode/marbles02/go
```

2. Issue the peer chaincode instantiate command to instantiate the chaincode on a channel.

Try it yourself

To instantiate the Marbles sample on the BYFN channel `mychannel` run the following command:

```
export CHANNEL_NAME=mychannel
peer chaincode instantiate -o orderer.example.com:7050 --tls --cafile /opt/
↪gopath/src/github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/
↪example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-
↪cert.pem -C $CHANNEL_NAME -n marbles -v 1.0 -c '{"Args":["init"]}' -P "OR (
↪'Org0MSP.peer','Org1MSP.peer')"
```

Verify index was deployed

Indexes will be deployed to each peer's CouchDB state database once the chaincode is both installed on the peer and instantiated on the channel. You can verify that the CouchDB index was created successfully by examining the peer log in the Docker container.

Try it yourself

To view the logs in the peer docker container, open a new Terminal window and run the following command to grep for message confirmation that the index was created.

```
docker logs peer0.org1.example.com  2>&1 | grep "CouchDB index"
```

You should see a result that looks like the following:

```
[couchdb] CreateIndex -> INFO 0be Created CouchDB index [indexOwner] in␣
↪state database [mychannel_marbles] using design document [_design/
↪indexOwnerDoc]
```

Note: If Marbles was not installed on the BYFN peer `peer0.org1.example.com`, you may need to replace it with the name of a different peer where Marbles was installed.

6.10.6 Query the CouchDB State Database

Now that the index has been defined in the JSON file and deployed alongside the chaincode, chaincode functions can execute JSON queries against the CouchDB state database, and thereby peer commands can invoke the chaincode functions.

Specifying an index name on a query is optional. If not specified, and an index already exists for the fields being queried, the existing index will be automatically used.

Tip: It is a good practice to explicitly include an index name on a query using the `use_index` keyword. Without it, CouchDB may pick a less optimal index. Also CouchDB may not use an index at all and you may not realize it, at the low volumes during testing. Only upon higher volumes you may realize slow performance because CouchDB is not using an index and you assumed it was.

Build the query in chaincode

You can perform complex rich queries against the chaincode data values using the CouchDB JSON query language within chaincode. As we explored above, the marbles02 sample chaincode includes an index and rich queries are defined in the functions - `queryMarbles` and `queryMarblesByOwner`:

- **queryMarbles** –

  Example of an **ad hoc rich query**. This is a query where a (selector) string can be passed into the function. This query would be useful to client applications that need to dynamically build their own selectors at runtime. For more information on selectors refer to CouchDB selector syntax.

- **queryMarblesByOwner** –

  Example of a parameterized query where the query logic is baked into the chaincode. In this case the function accepts a single argument, the marble owner. It then queries the state database for JSON documents matching the docType of "marble" and the owner id using the JSON query syntax.

Run the query using the peer command

In absence of a client application to test rich queries defined in chaincode, peer commands can be used. Peer commands run from the command line inside the docker container. We will customize the peer chaincode query command to use the Marbles index `indexOwner` and query for all marbles owned by "tom" using the `queryMarbles` function.

Try it yourself

Before querying the database, we should add some data. Run the following command in the peer container to create a marble owned by "tom":

```
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/
↪src/github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.
↪com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem␣
↪-C $CHANNEL_NAME -n marbles -c '{"Args":["initMarble","marble1","blue","35
↪","tom"]}'
```

After an index has been deployed during chaincode instantiation, it will automatically be utilized by chaincode queries. CouchDB can determine which index to use based on the fields being queried. If an index exists for the query criteria it will be used. However the recommended approach is to specify the `use_index` keyword on the query. The peer command below is an example of how to specify the index explicitly in the selector syntax by including the `use_index` keyword:

```
// Rich Query with index name explicitly specified:
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":["queryMarbles",
↪ "{\"selector\":{\"docType\":\"marble\",\"owner\":\"tom\"}, \"use_index\
↪":[\"_design/indexOwnerDoc\", \"indexOwner\"]}"]}'
```

Delving into the query command above, there are three arguments of interest:

- `queryMarbles`

Name of the function in the Marbles chaincode. Notice a shim `shim.ChaincodeStubInterface` is used to access and modify the ledger. The `getQueryResultForQueryString()` passes the queryString to the shim API `getQueryResult()`.

```
func (t *SimpleChaincode) queryMarbles(stub shim.ChaincodeStubInterface, args
↪[]string) pb.Response {

        //   0
        // "queryString"
         if len(args) < 1 {
                 return shim.Error("Incorrect number of arguments. Expecting 1")
         }

         queryString := args[0]

         queryResults, err := getQueryResultForQueryString(stub, queryString)
         if err != nil {
               return shim.Error(err.Error())
         }
         return shim.Success(queryResults)
}
```

- `{"selector":{"docType":"marble","owner":"tom"}`

  This is an example of an **ad hoc selector** string which finds all documents of type `marble` where the `owner` attribute has a value of `tom`.

- `"use_index":["_design/indexOwnerDoc", "indexOwner"]`

  Specifies both the design doc name `indexOwnerDoc` and index name `indexOwner`. In this example the selector query explicitly includes the index name, specified by using the `use_index` keyword. Recalling the index definition above *Create an index*, it contains a design doc, `"ddoc":"indexOwnerDoc"`. With CouchDB, if you plan to explicitly include the index name on the query, then the index definition must include the `ddoc` value, so it can be referenced with the `use_index` keyword.

The query runs successfully and the index is leveraged with the following results:

```
Query Result: [{"Key":"marble1", "Record":{"color":"blue","docType":"marble","name":
↪"marble1","owner":"tom","size":35}}]
```

6.10.7 Use best practices for queries and indexes

Queries that use indexes will complete faster, without having to scan the full database in couchDB. Understanding indexes will allow you to write your queries for better performance and help your application handle larger amounts of data or blocks on your network.

It is also important to plan the indexes you install with your chaincode. You should install only a few indexes per chaincode that support most of your queries. Adding too many indexes, or using an excessive number of fields in an index, will degrade the performance of your network. This is because the indexes are updated after each block is committed. The more indexes need to be updated through "index warming", the longer it will take for transactions to complete.

The examples in this section will help demonstrate how queries use indexes and what type of queries will have the best performance. Remember the following when writing your queries:

- All fields in the index must also be in the selector or sort sections of your query for the index to be used.
- More complex queries will have a lower performance and will be less likely to use an index.

- You should try to avoid operators that will result in a full table scan or a full index scan such as `$or`, `$in` and `$regex`.

In the previous section of this tutorial, you issued the following query against the marbles chaincode:

```
// Example one: query fully supported by the index
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":["queryMarbles", "{\
↪"selector\":{\"docType\":\"marble\",\"owner\":\"tom\"}, \"use_index\":[\
↪"indexOwnerDoc\", \"indexOwner\"]}"]}'
```

The marbles chaincode was installed with the `indexOwnerDoc` index:

```
{"index":{"fields":["docType","owner"]},"ddoc":"indexOwnerDoc", "name":"indexOwner",
↪"type":"json"}
```

Notice that both the fields in the query, `docType` and `owner`, are included in the index, making it a fully supported query. As a result this query will be able to use the data in the index, without having to search the full database. Fully supported queries such as this one will return faster than other queries from your chaincode.

If you add extra fields to the query above, it will still use the index. However, the query will additionally have to scan the indexed data for the extra fields, resulting in a longer response time. As an example, the query below will still use the index, but will take a longer time to return than the previous example.

```
// Example two: query fully supported by the index with additional data
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":["queryMarbles", "{\
↪"selector\":{\"docType\":\"marble\",\"owner\":\"tom\",\"color\":\"red\"}, \"use_
↪index\":[\"/indexOwnerDoc\", \"indexOwner\"]}"]}'
```

A query that does not include all fields in the index will have to scan the full database instead. For example, the query below searches for the owner, without specifying the the type of item owned. Since the ownerIndexDoc contains both the `owner` and `docType` fields, this query will not be able to use the index.

```
// Example three: query not supported by the index
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":["queryMarbles", "{\
↪"selector\":{\"owner\":\"tom\"}, \"use_index\":[\"indexOwnerDoc\", \"indexOwner\"]}
↪"]}'
```

In general, more complex queries will have a longer response time, and have a lower chance of being supported by an index. Operators such as `$or`, `$in`, and `$regex` will often cause the query to scan the full index or not use the index at all.

As an example, the query below contains an `$or` term that will search for every marble and every item owned by tom.

```
// Example four: query with $or supported by the index
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":["queryMarbles", "{\
↪"selector\":{"\$or\":[{\"docType\:\"marble\"},{\"owner\":\"tom\"}]}, \"use_index\
↪":[\"indexOwnerDoc\", \"indexOwner\"]}"]}'
```

This query will still use the index because it searches for fields that are included in `indexOwnerDoc`. However, the `$or` condition in the query requires a scan of all the items in the index, resulting in a longer response time.

Below is an example of a complex query that is not supported by the index.

```
// Example five: Query with $or not supported by the index
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":["queryMarbles", "{\
↪"selector\":{"\$or\":[{\"docType\":\"marble\",\"owner\":\"tom\"},{"\color\":
↪"\yellow\"}]}, \"use_index\":[\"indexOwnerDoc\", \"indexOwner\"]}"]}'
```

The query searches for all marbles owned by tom or any other items that are yellow. This query will not use the index because it will need to search the entire table to meet the `$or` condition. Depending the amount of data on your ledger, this query will take a long time to respond or may timeout.

While it is important to follow best practices with your queries, using indexes is not a solution for collecting large amounts of data. The blockchain data structure is optimized to validate and confirm transactions, and is not suited for data analytics or reporting. If you want to build a dashboard as part of your application or analyze the data from your network, the best practice is to query an off chain database that replicates the data from your peers. This will allow you to understand the data on the blockchain without degrading the performance of your network or disrupting transactions.

You can use block or chaincode events from your application to write transaction data to an off-chain database or analytics engine. For each block received, the block listener application would iterate through the block transactions and build a data store using the key/value writes from each valid transaction's `rwset`. The *Peer channel-based event services* provide replayable events to ensure the integrity of downstream data stores.

6.10.8 Query the CouchDB State Database With Pagination

When large result sets are returned by CouchDB queries, a set of APIs is available which can be called by chaincode to paginate the list of results. Pagination provides a mechanism to partition the result set by specifying a `pagesize` and a start point – a `bookmark` which indicates where to begin the result set. The client application iteratively invokes the chaincode that executes the query until no more results are returned. For more information refer to this topic on pagination with CouchDB.

We will use the Marbles sample function `queryMarblesWithPagination` to demonstrate how pagination can be implemented in chaincode and the client application.

- **queryMarblesWithPagination** –

  Example of an **ad hoc rich query with pagination**. This is a query where a (selector) string can be passed into the function similar to the above example. In this case, a `pageSize` is also included with the query as well as a `bookmark`.

In order to demonstrate pagination, more data is required. This example assumes that you have already added marble1 from above. Run the following commands in the peer container to create four more marbles owned by "tom", to create a total of five marbles owned by "tom":

Try it yourself

```
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -c '{"Args":["initMarble","marble2","yellow","35","tom"]}'
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -c '{"Args":["initMarble","marble3","green","20","tom"]}'
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -c '{"Args":["initMarble","marble4","purple","20","tom"]}'
peer chaincode invoke -o orderer.example.com:7050 --tls --cafile /opt/gopath/src/
↪github.com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/
↪orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C $CHANNEL_NAME -n␣
↪marbles -c '{"Args":["initMarble","marble5","blue","40","tom"]}'
```

In addition to the arguments for the query in the previous example, queryMarblesWithPagination adds `pagesize` and `bookmark`. `PageSize` specifies the number of records to return per query. The `bookmark` is an "anchor"

telling couchDB where to begin the page. (Each page of results returns a unique bookmark.)

- `queryMarblesWithPagination`

  Name of the function in the Marbles chaincode. Notice a shim `shim.ChaincodeStubInterface` is used to access and modify the ledger. The `getQueryResultForQueryStringWithPagination()` passes the queryString along

  with the pagesize and bookmark to the shim API `GetQueryResultWithPagination()`.

```
func (t *SimpleChaincode) queryMarblesWithPagination(stub shim.ChaincodeStubInterface,
↪ args []string) pb.Response {

      //   0
      // "queryString"
      if len(args) < 3 {
              return shim.Error("Incorrect number of arguments. Expecting 3")
      }

      queryString := args[0]
      //return type of ParseInt is int64
      pageSize, err := strconv.ParseInt(args[1], 10, 32)
      if err != nil {
              return shim.Error(err.Error())
      }
      bookmark := args[2]

      queryResults, err := getQueryResultForQueryStringWithPagination(stub,␣
↪queryString, int32(pageSize), bookmark)
      if err != nil {
              return shim.Error(err.Error())
      }
      return shim.Success(queryResults)
}
```

The following example is a peer command which calls queryMarblesWithPagination with a pageSize of `3` and no bookmark specified.

Tip: When no bookmark is specified, the query starts with the "first" page of records.

Try it yourself

```
// Rich Query with index name explicitly specified and a page size of 3:
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":[
↪"queryMarblesWithPagination", "{\"selector\":{\"docType\":\"marble\",\"owner\":\
↪"tom\"}, \"use_index\":[\"_design/indexOwnerDoc\", \"indexOwner\"]}","3",""]}'
```

The following response is received (carriage returns added for clarity), three of the five marbles are returned because the `pagsize` was set to `3`:

```
[{"Key":"marble1", "Record":{"color":"blue","docType":"marble","name":"marble1","owner
↪":"tom","size":35}},
 {"Key":"marble2", "Record":{"color":"yellow","docType":"marble","name":"marble2",
↪"owner":"tom","size":35}},
 {"Key":"marble3", "Record":{"color":"green","docType":"marble","name":"marble3",
↪"owner":"tom","size":20}}]
[{"ResponseMetadata":{"RecordsCount":"3",
```

(continues on next page)

(continued from previous page)

```
"Bookmark":
↪"g1AAAABLeJzLYWBgYMpgSmHgKy5JLCrJTq2MT8lPzkzJBYqz5yYWJeWkGoOkOWDSOSANIFk2iCyIyVySn5uVBQAGEhRz
↪"}}]
```

Note: Bookmarks are uniquely generated by CouchDB for each query and represent a placeholder in the result set. Pass the returned bookmark on the subsequent iteration of the query to retrieve the next set of results.

The following is a peer command to call queryMarblesWithPagination with a pageSize of `3`. Notice this time, the query includes the bookmark returned from the previous query.

Try it yourself

```
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":[
↪"queryMarblesWithPagination", "{\"selector\":{\"docType\":\"marble\",\"owner\":\
↪"tom\"}, \"use_index\":[\"_design/indexOwnerDoc\", \"indexOwner\"]}","3",
↪"g1AAAABLeJzLYWBgYMpgSmHgKy5JLCrJTq2MT8lPzkzJBYqz5yYWJeWkGoOkOWDSOSANIFk2iCyIyVySn5uVBQAGEhRz
↪"]}'
```

The following response is received (carriage returns added for clarity). The last two records are retrieved:

```
[{"Key":"marble4", "Record":{"color":"purple","docType":"marble","name":"marble4",
↪"owner":"tom","size":20}},
 {"Key":"marble5", "Record":{"color":"blue","docType":"marble","name":"marble5","owner
↪":"tom","size":40}}]
[{"ResponseMetadata":{"RecordsCount":"2",
"Bookmark":
↪"g1AAAABLeJzLYWBgYMpgSmHgKy5JLCrJTq2MT8lPzkzJBYqz5yYWJeWkmoKkOWDSOSANIFk2iCyIyVySn5uVBQAGYhR1
↪"}}]
```

The final command is a peer command to call queryMarblesWithPagination with a pageSize of `3` and with the bookmark from the previous query.

Try it yourself

```
peer chaincode query -C $CHANNEL_NAME -n marbles -c '{"Args":[
↪"queryMarblesWithPagination", "{\"selector\":{\"docType\":\"marble\",\"owner\":\
↪"tom\"}, \"use_index\":[\"_design/indexOwnerDoc\", \"indexOwner\"]}","3",
↪"g1AAAABLeJzLYWBgYMpgSmHgKy5JLCrJTq2MT8lPzkzJBYqz5yYWJeWkmoKkOWDSOSANIFk2iCyIyVySn5uVBQAGYhR1
↪"]}'
```

The following response is received (carriage returns added for clarity). No records are returned, indicating that all pages have been retrieved:

```
[]
[{"ResponseMetadata":{"RecordsCount":"0",
"Bookmark":
↪"g1AAAABLeJzLYWBgYMpgSmHgKy5JLCrJTq2MT8lPzkzJBYqz5yYWJeWkmoKkOWDSOSANIFk2iCyIyVySn5uVBQAGYhR1
↪"}}]
```

For an example of how a client application can iterate over the result sets using pagination, search for the `getQueryResultForQueryStringWithPagination` function in the Marbles sample.

6.10.9 Update an Index

It may be necessary to update an index over time. The same index may exist in subsequent versions of the chaincode that gets installed. In order for an index to be updated, the original index definition must have included the design document `ddoc` attribute and an index name. To update an index definition, use the same index name but alter the index definition. Simply edit the index JSON file and add or remove fields from the index. Fabric only supports the index type JSON, changing the index type is not supported. The updated index definition gets redeployed to the peer's state database when the chaincode is installed and instantiated. Changes to the index name or `ddoc` attributes will result in a new index being created and the original index remains unchanged in CouchDB until it is removed.

Note: If the state database has a significant volume of data, it will take some time for the index to be re-built, during which time chaincode invokes that issue queries may fail or timeout.

Iterating on your index definition

If you have access to your peer's CouchDB state database in a development environment, you can iteratively test various indexes in support of your chaincode queries. Any changes to chaincode though would require redeployment. Use the CouchDB Fauxton interface or a command line curl utility to create and update indexes.

Note: The Fauxton interface is a web UI for the creation, update, and deployment of indexes to CouchDB. If you want to try out this interface, there is an example of the format of the Fauxton version of the index in Marbles sample. If you have deployed the BYFN network with CouchDB, the Fauxton interface can be loaded by opening a browser and navigating to `http://localhost:5984/_utils`.

Alternatively, if you prefer not use the Fauxton UI, the following is an example of a curl command which can be used to create the index on the database `mychannel_marbles`:

> // Index for docType, owner. // Example curl command line to define index in the CouchDB channel_chaincode database

```
curl -i -X POST -H "Content-Type: application/json" -d
       "{\"index\":{\"fields\":[\"docType\",\"owner\"]},
         \"name\":\"indexOwner\",
         \"ddoc\":\"indexOwnerDoc\",
         \"type\":\"json\"}" http://hostname:port/mychannel_marbles/_index
```

Note: If you are using BYFN configured with CouchDB, replace hostname:port with `localhost:5984`.

6.10.10 Delete an Index

Index deletion is not managed by Fabric tooling. If you need to delete an index, manually issue a curl command against the database or delete it using the Fauxton interface.

The format of the curl command to delete an index would be:

```
curl -X DELETE http://localhost:5984/{database_name}/_index/{design_doc}/json/{index_
↪name} -H  "accept: */*" -H  "Host: localhost:5984"
```

To delete the index used in this tutorial, the curl command would be:

```
curl -X DELETE http://localhost:5984/mychannel_marbles/_index/indexOwnerDoc/json/
↪indexOwner -H  "accept: */*" -H  "Host: localhost:5984"
```

6.11 Videos

Refer to the Hyperledger Fabric channel on YouTube

This collection contains developers demonstrating various v1 features and components such as: ledger, channels, gossip, SDK, chaincode, MSP, and more...

CHAPTER 7

Operations Guides

7.1 Upgrading to the Newest Version of Fabric

At a high level, upgrading a Fabric network to v1.3 can be performed by following these steps:

- Upgrade the binaries for the ordering service, the Fabric CA, and the peers. These upgrades may be done in parallel.
- Upgrade client SDKs.
- Enable the two v1.3 capabilities.
- (Optional) Upgrade the Kafka cluster.

To help understand this process, we've created the *Upgrading Your Network Components* tutorial that will take you through most of the major upgrade steps, including upgrading peers, orderers, as well as the capabilities. We've included both a script as well as the individual steps to achieve these upgrades.

Because our tutorial leverages the *Building Your First Network* (BYFN) sample, it has certain limitations (it does not use Fabric CA, for example). Therefore we have included a section at the end of the tutorial that will show how to upgrade your CA, Kafka clusters, CouchDB, Zookeeper, vendored chaincode shims, and Node SDK clients.

If you want to learn more about capability requirements, check out the *Capability Requirements* documentation.

Note: With the removal of the old Event Hub in v1.3, please make sure to update your applications to be compatible with the *Peer channel-based event services*, otherwise your applications may break after upgrade.

7.2 Updating a Channel Configuration

7.2.1 What is a Channel Configuration?

Channel configurations contain all of the information relevant to the administration of a channel. Most importantly, the channel configuration specifies which organizations are members of channel, but it also includes other channel-wide configuration information such as channel access policies and block batch sizes.

This configuration is stored on the ledger in a **block**, and is therefore known as a configuration (config) block. Configuration blocks contain a single configuration. The first of these blocks is known as the "genesis block" and contains the initial configuration required to bootstrap a channel. Each time the configuration of a channel changes it is done through a new configuration block, with the latest configuration block representing the current channel configuration. Orderers and peers keep the current channel configuration in memory to facilitate all channel operations such as cutting a new block and validating block transactions.

Because configurations are stored in blocks, updating a config happens through a process called a "configuration transaction" (even though the process is a little different from a normal transaction). Updating a config is a process of pulling the config, translating into a format that humans can read, modifying it and then submitting it for approval.

For a more in-depth look at the process for pulling a config and translating it into JSON, check out Adding an Org to a Channel. In this doc, we'll be focusing on the different ways you can edit a config and the process for getting it signed.

7.2.2 Editing a Config

Channels are highly configurable, but not infinitely so. Different configuration elements have different modification policies (which specify the group of identities required to sign the config update).

To see the scope of what's possible to change it's important to look at a config in JSON format. The Adding an Org to a Channel tutorial generates one, so if you've gone through that doc you can simply refer to it. For those who have not, we'll provide one here (for ease of readability, it might be helpful to put this config into a viewer that supports JSON folding, like atom or Visual Studio).

Click here to see the config

```
{
"channel_group": {
  "groups": {
    "Application": {
      "groups": {
        "Org1MSP": {
          "mod_policy": "Admins",
          "policies": {
            "Admins": {
              "mod_policy": "Admins",
              "policy": {
                "type": 1,
                "value": {
                  "identities": [
                    {
                      "principal": {
                        "msp_identifier": "Org1MSP",
                        "role": "ADMIN"
                      },
                      "principal_classification": "ROLE"
                    }
```

(continues on next page)

(continued from previous page)

```
                ],
                "rule": {
                  "n_out_of": {
                    "n": 1,
                    "rules": [
                      {
                        "signed_by": 0
                      }
                    ]
                  }
                },
                "version": 0
              }
            },
            "version": "0"
          },
          "Readers": {
            "mod_policy": "Admins",
            "policy": {
              "type": 1,
              "value": {
                "identities": [
                  {
                    "principal": {
                      "msp_identifier": "Org1MSP",
                      "role": "MEMBER"
                    },
                    "principal_classification": "ROLE"
                  }
                ],
                "rule": {
                  "n_out_of": {
                    "n": 1,
                    "rules": [
                      {
                        "signed_by": 0
                      }
                    ]
                  }
                },
                "version": 0
              }
            },
            "version": "0"
          },
          "Writers": {
            "mod_policy": "Admins",
            "policy": {
              "type": 1,
              "value": {
                "identities": [
                  {
                    "principal": {
                      "msp_identifier": "Org1MSP",
                      "role": "MEMBER"
                    },
                    "principal_classification": "ROLE"
```

(continues on next page)

(continued from previous page)


```
                    }
                  ],
                  "rule": {
                    "n_out_of": {
                      "n": 1,
                      "rules": [
                        {
                          "signed_by": 0
                        }
                      ]
                    }
                  },
                  "version": 0
                }
              },
              "version": "0"
            }
          },
          "values": {
            "AnchorPeers": {
              "mod_policy": "Admins",
              "value": {
                "anchor_peers": [
                  {
                    "host": "peer0.org1.example.com",
                    "port": 7051
                  }
                ]
              },
              "version": "0"
            },
            "MSP": {
              "mod_policy": "Admins",
              "value": {
                "config": {
                  "admins": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNHRENDQWIrZ0F3SUJBZ0lRSWlyVmg3NVcwWmh0UjEzdmltdmliakFLQn
↪"
                  ],
                  "crypto_config": {
                    "identity_identifier_hash_function": "SHA256",
                    "signature_hash_family": "SHA2"
                  },
                  "name": "Org1MSP",
                  "root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNRekNDQWVxZ0F3SUJBZ0lSQU03ZVdTaVM4V3VVM2haMU9tR255eXd3Q2
↪"
                  ],
                  "tls_root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNTVENDQWZDZ0F3SUJBZ0lSQUtsNEFQWmV6dWt0Nk8wYjRyYjY5Y0F3Q2
↪"
                  ]
                },
                "type": 0
```


(continues on next page)

(continued from previous page)

```
            },
            "version": "0"
          }
        },
        "version": "1"
      },
      "Org2MSP": {
        "mod_policy": "Admins",
        "policies": {
          "Admins": {
            "mod_policy": "Admins",
            "policy": {
              "type": 1,
              "value": {
                "identities": [
                  {
                    "principal": {
                      "msp_identifier": "Org2MSP",
                      "role": "ADMIN"
                    },
                    "principal_classification": "ROLE"
                  }
                ],
                "rule": {
                  "n_out_of": {
                    "n": 1,
                    "rules": [
                      {
                        "signed_by": 0
                      }
                    ]
                  }
                },
                "version": 0
              }
            },
            "version": "0"
          },
          "Readers": {
            "mod_policy": "Admins",
            "policy": {
              "type": 1,
              "value": {
                "identities": [
                  {
                    "principal": {
                      "msp_identifier": "Org2MSP",
                      "role": "MEMBER"
                    },
                    "principal_classification": "ROLE"
                  }
                ],
                "rule": {
                  "n_out_of": {
                    "n": 1,
                    "rules": [
                      {
```

(continues on next page)

(continued from previous page)

```
                        "signed_by": 0
                      }
                    ]
                  }
                },
                "version": 0
              }
            },
            "version": "0"
          },
          "Writers": {
            "mod_policy": "Admins",
            "policy": {
              "type": 1,
              "value": {
                "identities": [
                  {
                    "principal": {
                      "msp_identifier": "Org2MSP",
                      "role": "MEMBER"
                    },
                    "principal_classification": "ROLE"
                  }
                ],
                "rule": {
                  "n_out_of": {
                    "n": 1,
                    "rules": [
                      {
                        "signed_by": 0
                      }
                    ]
                  }
                },
                "version": 0
              }
            },
            "version": "0"
          }
        },
        "values": {
          "AnchorPeers": {
            "mod_policy": "Admins",
            "value": {
              "anchor_peers": [
                {
                  "host": "peer0.org2.example.com",
                  "port": 7051
                }
              ]
            },
            "version": "0"
          },
          "MSP": {
            "mod_policy": "Admins",
            "value": {
              "config": {
```

(continues on next page)

(continued from previous page)


```
                    "admins": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNHVENDQWNDZ0F3SUJBZ0lSQU5Pb1lIbk9seU94dTJxZFBteStyV293Q2
↪"
                    ],
                    "crypto_config": {
                      "identity_identifier_hash_function": "SHA256",
                      "signature_hash_family": "SHA2"
                    },
                    "name": "Org2MSP",
                    "root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWVxZ0F3SUJBZ0lSQU1pVXk5SGRSbXB5MDdsSjhRMlZNWXN3Q2
↪"
                    ],
                    "tls_root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNTakNDQWZDZ0F3SUJBZ0lSQU9JNmRWUWMraHBZdkdMSlFQM1YwQU13Q2
↪"
                    ]
                  },
                  "type": 0
                },
                "version": "0"
              }
            },
            "version": "1"
          },
          "Org3MSP": {
            "groups": {},
            "mod_policy": "Admins",
            "policies": {
              "Admins": {
                "mod_policy": "Admins",
                "policy": {
                  "type": 1,
                  "value": {
                    "identities": [
                      {
                        "principal": {
                          "msp_identifier": "Org3MSP",
                          "role": "ADMIN"
                        },
                        "principal_classification": "ROLE"
                      }
                    ],
                    "rule": {
                      "n_out_of": {
                        "n": 1,
                        "rules": [
                          {
                            "signed_by": 0
                          }
                        ]
                      }
                    },
                    "version": 0
```


(continues on next page)

(continued from previous page)

```
            }
          },
          "version": "0"
        },
        "Readers": {
          "mod_policy": "Admins",
          "policy": {
            "type": 1,
            "value": {
              "identities": [
                {
                  "principal": {
                    "msp_identifier": "Org3MSP",
                    "role": "MEMBER"
                  },
                  "principal_classification": "ROLE"
                }
              ],
              "rule": {
                "n_out_of": {
                  "n": 1,
                  "rules": [
                    {
                      "signed_by": 0
                    }
                  ]
                }
              },
              "version": 0
            }
          },
          "version": "0"
        },
        "Writers": {
          "mod_policy": "Admins",
          "policy": {
            "type": 1,
            "value": {
              "identities": [
                {
                  "principal": {
                    "msp_identifier": "Org3MSP",
                    "role": "MEMBER"
                  },
                  "principal_classification": "ROLE"
                }
              ],
              "rule": {
                "n_out_of": {
                  "n": 1,
                  "rules": [
                    {
                      "signed_by": 0
                    }
                  ]
                }
              },
```

(continues on next page)

(continued from previous page)


```
                    "version": 0
                  }
                },
                "version": "0"
              }
            },
            "values": {
              "MSP": {
                "mod_policy": "Admins",
                "value": {
                  "config": {
                    "admins": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNHRENDQWIrZ0F3SUJBZ0lRQUlSNWN4U0hpVm1kSm9uY3FJVUxXekFLQn
↪"
                    ],
                    "crypto_config": {
                      "identity_identifier_hash_function": "SHA256",
                      "signature_hash_family": "SHA2"
                    },
                    "name": "Org3MSP",
                    "root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNRakNDQWVtZ0F3SUJBZ0lRUkN1U2Y0RVJNaDdHQW1ydTFIQ2FZREFLQn
↪"
                    ],
                    "tls_root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNTVENDQWZEZ0F3SUJBZ0lSQU9xc2JQQzFOVHJzclEvUUNpalh6K0F3Q2
↪"
                    ]
                  },
                  "type": 0
                },
                "version": "0"
              }
            },
            "version": "0"
          }
        },
        "mod_policy": "Admins",
        "policies": {
          "Admins": {
            "mod_policy": "Admins",
            "policy": {
              "type": 3,
              "value": {
                "rule": "MAJORITY",
                "sub_policy": "Admins"
              }
            },
            "version": "0"
          },
          "Readers": {
            "mod_policy": "Admins",
            "policy": {
              "type": 3,
```


(continues on next page)

(continued from previous page)

```
            "value": {
              "rule": "ANY",
              "sub_policy": "Readers"
            }
          },
          "version": "0"
        },
        "Writers": {
          "mod_policy": "Admins",
          "policy": {
            "type": 3,
            "value": {
              "rule": "ANY",
              "sub_policy": "Writers"
            }
          },
          "version": "0"
        }
      },
      "version": "1"
    },
    "Orderer": {
      "groups": {
        "OrdererOrg": {
          "mod_policy": "Admins",
          "policies": {
            "Admins": {
              "mod_policy": "Admins",
              "policy": {
                "type": 1,
                "value": {
                  "identities": [
                    {
                      "principal": {
                        "msp_identifier": "OrdererMSP",
                        "role": "ADMIN"
                      },
                      "principal_classification": "ROLE"
                    }
                  ],
                  "rule": {
                    "n_out_of": {
                      "n": 1,
                      "rules": [
                        {
                          "signed_by": 0
                        }
                      ]
                    }
                  },
                  "version": 0
                }
              },
              "version": "0"
            },
            "Readers": {
              "mod_policy": "Admins",
```

(continues on next page)

(continued from previous page)

```
            "policy": {
              "type": 1,
              "value": {
                "identities": [
                  {
                    "principal": {
                      "msp_identifier": "OrdererMSP",
                      "role": "MEMBER"
                    },
                    "principal_classification": "ROLE"
                  }
                ],
                "rule": {
                  "n_out_of": {
                    "n": 1,
                    "rules": [
                      {
                        "signed_by": 0
                      }
                    ]
                  }
                },
                "version": 0
              }
            },
            "version": "0"
          },
          "Writers": {
            "mod_policy": "Admins",
            "policy": {
              "type": 1,
              "value": {
                "identities": [
                  {
                    "principal": {
                      "msp_identifier": "OrdererMSP",
                      "role": "MEMBER"
                    },
                    "principal_classification": "ROLE"
                  }
                ],
                "rule": {
                  "n_out_of": {
                    "n": 1,
                    "rules": [
                      {
                        "signed_by": 0
                      }
                    ]
                  }
                },
                "version": 0
              }
            },
            "version": "0"
          }
        },
```

(continues on next page)

(continued from previous page)


```
          "values": {
            "MSP": {
              "mod_policy": "Admins",
              "value": {
                "config": {
                  "admins": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNDakNDQWJDZ0F3SUJBZ0lRSFNTTnIyMWRLTTB6THZ0dEdoQnpMVEFLQn
↪"
                  ],
                  "crypto_config": {
                    "identity_identifier_hash_function": "SHA256",
                    "signature_hash_family": "SHA2"
                  },
                  "name": "OrdererMSP",
                  "root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNMakNDQWRXZ0F3SUJBZ0lRY2cxUVZkVmU2Skd6YVU1cmxjcW4vakFLQn
↪"
                  ],
                  "tls_root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNORENDQWR1Z0F3SUJBZ0lRYWJ5SUl6cldtUFNzSjJacisvRVpXVEFLQn
↪"
                  ]
                },
                "type": 0
              },
              "version": "0"
            }
          },
          "version": "0"
        }
      },
      "mod_policy": "Admins",
      "policies": {
        "Admins": {
          "mod_policy": "Admins",
          "policy": {
            "type": 3,
            "value": {
              "rule": "MAJORITY",
              "sub_policy": "Admins"
            }
          },
          "version": "0"
        },
        "BlockValidation": {
          "mod_policy": "Admins",
          "policy": {
            "type": 3,
            "value": {
              "rule": "ANY",
              "sub_policy": "Writers"
            }
          },
          "version": "0"
```


(continues on next page)

(continued from previous page)

```
        },
        "Readers": {
          "mod_policy": "Admins",
          "policy": {
            "type": 3,
            "value": {
              "rule": "ANY",
              "sub_policy": "Readers"
            }
          },
          "version": "0"
        },
        "Writers": {
          "mod_policy": "Admins",
          "policy": {
            "type": 3,
            "value": {
              "rule": "ANY",
              "sub_policy": "Writers"
            }
          },
          "version": "0"
        }
      },
      "values": {
        "BatchSize": {
          "mod_policy": "Admins",
          "value": {
            "absolute_max_bytes": 103809024,
            "max_message_count": 10,
            "preferred_max_bytes": 524288
          },
          "version": "0"
        },
        "BatchTimeout": {
          "mod_policy": "Admins",
          "value": {
            "timeout": "2s"
          },
          "version": "0"
        },
        "ChannelRestrictions": {
          "mod_policy": "Admins",
          "version": "0"
        },
        "ConsensusType": {
          "mod_policy": "Admins",
          "value": {
            "type": "solo"
          },
          "version": "0"
        }
      },
      "version": "0"
    }
  },
  "mod_policy": "",
```

(continues on next page)

(continued from previous page)

```
  "policies": {
    "Admins": {
      "mod_policy": "Admins",
      "policy": {
        "type": 3,
        "value": {
          "rule": "MAJORITY",
          "sub_policy": "Admins"
        }
      },
      "version": "0"
    },
    "Readers": {
      "mod_policy": "Admins",
      "policy": {
        "type": 3,
        "value": {
          "rule": "ANY",
          "sub_policy": "Readers"
        }
      },
      "version": "0"
    },
    "Writers": {
      "mod_policy": "Admins",
      "policy": {
        "type": 3,
        "value": {
          "rule": "ANY",
          "sub_policy": "Writers"
        }
      },
      "version": "0"
    }
  },
  "values": {
    "BlockDataHashingStructure": {
      "mod_policy": "Admins",
      "value": {
        "width": 4294967295
      },
      "version": "0"
    },
    "Consortium": {
      "mod_policy": "Admins",
      "value": {
        "name": "SampleConsortium"
      },
      "version": "0"
    },
    "HashingAlgorithm": {
      "mod_policy": "Admins",
      "value": {
        "name": "SHA256"
      },
      "version": "0"
    },
```

(continues on next page)

(continued from previous page)

```
    "OrdererAddresses": {
      "mod_policy": "/Channel/Orderer/Admins",
      "value": {
        "addresses": [
          "orderer.example.com:7050"
        ]
      },
      "version": "0"
    }
  },
  "version": "0"
},
"sequence": "3",
"type": 0
}
```

A config might look intimidating in this form, but once you study it you'll see that it has a logical structure.

Beyond the definitions of the policies – defining who can do certain things at the channel level, and who has the permission to change who can change the config – channels also have other kinds of features that can be modified using a config update. Adding an Org to a Channel takes you through one of the most important – adding an org to a channel. Some other things that are possible to change with a config update include:

- **Batch Size.** These parameters dictate the number and size of transactions in a block. No block will appear larger than `absolute_max_bytes` large or with more than `max_message_count` transactions inside the block. If it is possible to construct a block under `preferred_max_bytes`, then a block will be cut prematurely, and transactions larger than this size will appear in their own block.

```
{
  "absolute_max_bytes": 102760448,
  "max_message_count": 10,
  "preferred_max_bytes": 524288
}
```

- **Batch Timeout.** The amount of time to wait after the first transaction arrives for additional transactions before cutting a block. Decreasing this value will improve latency, but decreasing it too much may decrease throughput by not allowing the block to fill to its maximum capacity.

```
{ "timeout": "2s" }
```

- **Channel Restrictions.** The total number of channels the orderer is willing to allocate may be specified as max_count. This is primarily useful in pre-production environments with weak consortium `ChannelCreation` policies.

```
{
 "max_count":1000
}
```

- **Channel Creation Policy.** Defines the policy value which will be set as the mod_policy for the Application group of new channels for the consortium it is defined in. The signature set attached to the channel creation request will be checked against the instantiation of this policy in the new channel to ensure that the channel creation is authorized. Note that this config value is only set in the orderer system channel.

```
{
"type": 3,
"value": {
```

(continues on next page)

(continued from previous page)

```
  "rule": "ANY",
  "sub_policy": "Admins"
  }
}
```

- **Kafka brokers.** When `ConsensusType` is set to `kafka`, the `brokers` list enumerates some subset (or preferably all) of the Kafka brokers for the orderer to initially connect to at startup. *Note that it is not possible to change your consensus type after it has been established (during the bootstrapping of the genesis block).*

```
{
  "brokers": [
    "kafka0:9092",
    "kafka1:9092",
    "kafka2:9092",
    "kafka3:9092"
  ]
}
```

- **Anchor Peers Definition.** Defines the location of the anchor peers for each Org.

```
{
  "host": "peer0.org2.example.com",
    "port": 7051
}
```

- **Hashing Structure.** The block data is an array of byte arrays. The hash of the block data is computed as a Merkle tree. This value specifies the width of that Merkle tree. For the time being, this value is fixed to `4294967295` which corresponds to a simple flat hash of the concatenation of the block data bytes.

```
{ "width": 4294967295 }
```

- **Hashing Algorithm.** The algorithm used for computing the hash values encoded into the blocks of the blockchain. In particular, this affects the data hash, and the previous block hash fields of the block. Note, this field currently only has one valid value (`SHA256`) and should not be changed.

```
{ "name": "SHA256" }
```

- **Block Validation.** This policy specifies the signature requirements for a block to be considered valid. By default, it requires a signature from some member of the ordering org.

```
{
  "type": 3,
  "value": {
    "rule": "ANY",
    "sub_policy": "Writers"
  }
}
```

- **Orderer Address.** A list of addresses where clients may invoke the orderer `Broadcast` and `Deliver` functions. The peer randomly chooses among these addresses and fails over between them for retrieving blocks.

```
{
  "addresses": [
    "orderer.example.com:7050"
  ]
}
```

Just as we add an Org by adding their artifacts and MSP information, you can remove them by reversing the process.

Note that once the consensus type has been defined and the network has been bootstrapped, it is not possible to change it through a configuration update.

There is another important channel configuration (especially for v1.1) known as **Capability Requirements**. It has its own doc that can be found here.

Let's say you want to edit the block batch size for the channel (because this is a single numeric field, it's one of the easiest changes to make). First to make referencing the JSON path easy, we define it as an environment variable.

To establish this, take a look at your config, find what you're looking for, and back track the path.

If you find batch size, for example, you'll see that it's a `value` of the `Orderer`. `Orderer` can be found under `groups`, which is under `channel_group`. The batch size value has a parameter under `value` of `max_message_count`.

Which would make the path this:

```
export MAXBATCHSIZEPATH=".channel_group.groups.Orderer.values.BatchSize.value.max_
↪message_count"
```

Next, display the value of that property:

```
jq "$MAXBATCHSIZEPATH" config.json
```

Which should return a value of `10` (in our sample network at least).

Now, let's set the new batch size and display the new value:

```
jq "$MAXBATCHSIZEPATH = 20" config.json > modified_config.json
jq "$MAXBATCHSIZEPATH" modified_config.json
```

Once you've modified the JSON, it's ready to be converted and submitted. The scripts and steps in Adding an Org to a Channel will take you through the process for converting the JSON, so let's look at the process of submitting it.

7.2.3 Get the Necessary Signatures

Once you've successfully generated the protobuf file, it's time to get it signed. To do this, you need to know the relevant policy for whatever it is you're trying to change.

By default, editing the configuration of:

- **A particular org** (for example, changing anchor peers) requires only the admin signature of that org.
- **The application** (like who the member orgs are) requires a majority of the application organizations' admins to sign.
- **The orderer** requires a majority of the ordering organizations' admins (of which there are by default only 1).
- **The top level `channel` group** requires both the agreement of a majority of application organization admins and orderer organization admins.

If you have made changes to the default policies in the channel, you'll need to compute your signature requirements accordingly.

Note: you may be able to script the signature collection, dependent on your application. In general, you may always collect more signatures than are required.

The actual process of getting these signatures will depend on how you've set up your system, but there are two main implementations. Currently, the Fabric command line defaults to a "pass it along" system. That is, the Admin of the Org proposing a config update sends the update to someone else (another Admin, typically) who needs to sign it. This

Admin signs it (or doesn't) and passes it along to the next Admin, and so on, until there are enough signatures for the config to be submitted.

This has the virtue of simplicity – when there are enough signatures, the last Admin can simply submit the config transaction (in Fabric, the `peer channel update` command includes a signature by default). However, this process will only be practical in smaller channels, since the "pass it along" method can be time consuming.

The other option is to submit the update to every Admin on a channel and wait for enough signatures to come back. These signatures can then be stitched together and submitted. This makes life a bit more difficult for the Admin who created the config update (forcing them to deal with a file per signer) but is the recommended workflow for users which are developing Fabric management applications.

Once the config has been added to the ledger, it will be a best practice to pull it and convert it to JSON to check to make sure everything was added correctly. This will also serve as a useful copy of the latest config.

7.3 Membership Service Providers (MSP)

The document serves to provide details on the setup and best practices for MSPs.

Membership Service Provider (MSP) is a component that aims to offer an abstraction of a membership operation architecture.

In particular, MSP abstracts away all cryptographic mechanisms and protocols behind issuing and validating certificates, and user authentication. An MSP may define their own notion of identity, and the rules by which those identities are governed (identity validation) and authenticated (signature generation and verification).

A Hyperledger Fabric blockchain network can be governed by one or more MSPs. This provides modularity of membership operations, and interoperability across different membership standards and architectures.

In the rest of this document we elaborate on the setup of the MSP implementation supported by Hyperledger Fabric, and discuss best practices concerning its use.

7.3.1 MSP Configuration

To setup an instance of the MSP, its configuration needs to be specified locally at each peer and orderer (to enable peer, and orderer signing), and on the channels to enable peer, orderer, client identity validation, and respective signature verification (authentication) by and for all channel members.

Firstly, for each MSP a name needs to be specified in order to reference that MSP in the network (e.g. `msp1`, `org2`, and `org3.divA`). This is the name under which membership rules of an MSP representing a consortium, organization or organization division is to be referenced in a channel. This is also referred to as the *MSP Identifier* or *MSP ID*. MSP Identifiers are required to be unique per MSP instance. For example, shall two MSP instances with the same identifier be detected at the system channel genesis, orderer setup will fail.

In the case of default implementation of MSP, a set of parameters need to be specified to allow for identity (certificate) validation and signature verification. These parameters are deduced by RFC5280, and include:

- A list of self-signed (X.509) certificates to constitute the *root of trust*
- A list of X.509 certificates to represent intermediate CAs this provider considers for certificate validation; these certificates ought to be certified by exactly one of the certificates in the root of trust; intermediate CAs are optional parameters
- A list of X.509 certificates with a verifiable certificate path to exactly one of the certificates of the root of trust to represent the administrators of this MSP; owners of these certificates are authorized to request changes to this MSP configuration (e.g. root CAs, intermediate CAs)

- A list of Organizational Units that valid members of this MSP should include in their X.509 certificate; this is an optional configuration parameter, used when, e.g., multiple organizations leverage the same root of trust, and intermediate CAs, and have reserved an OU field for their members
- A list of certificate revocation lists (CRLs) each corresponding to exactly one of the listed (intermediate or root) MSP Certificate Authorities; this is an optional parameter
- A list of self-signed (X.509) certificates to constitute the *TLS root of trust* for TLS certificate.
- A list of X.509 certificates to represent intermediate TLS CAs this provider considers; these certificates ought to be certified by exactly one of the certificates in the TLS root of trust; intermediate CAs are optional parameters.

Valid identities for this MSP instance are required to satisfy the following conditions:

- They are in the form of X.509 certificates with a verifiable certificate path to exactly one of the root of trust certificates;
- They are not included in any CRL;
- And they *list* one or more of the Organizational Units of the MSP configuration in the `OU` field of their X.509 certificate structure.

For more information on the validity of identities in the current MSP implementation, we refer the reader to msp-identity-validity-rules.

In addition to verification related parameters, for the MSP to enable the node on which it is instantiated to sign or authenticate, one needs to specify:

- The signing key used for signing by the node (currently only ECDSA keys are supported), and
- The node's X.509 certificate, that is a valid identity under the verification parameters of this MSP.

It is important to note that MSP identities never expire; they can only be revoked by adding them to the appropriate CRLs. Additionally, there is currently no support for enforcing revocation of TLS certificates.

7.3.2 How to generate MSP certificates and their signing keys?

To generate X.509 certificates to feed its MSP configuration, the application can use Openssl. We emphasize that in Hyperledger Fabric there is no support for certificates including RSA keys.

Alternatively one can use `cryptogen` tool, whose operation is explained in *Getting Started*.

Hyperledger Fabric CA can also be used to generate the keys and certificates needed to configure an MSP.

7.3.3 MSP setup on the peer & orderer side

To set up a local MSP (for either a peer or an orderer), the administrator should create a folder (e.g. `$MY_PATH/mspconfig`) that contains six subfolders and a file:

1. a folder `admincerts` to include PEM files each corresponding to an administrator certificate
2. a folder `cacerts` to include PEM files each corresponding to a root CA's certificate
3. (optional) a folder `intermediatecerts` to include PEM files each corresponding to an intermediate CA's certificate
4. (optional) a file `config.yaml` to configure the supported Organizational Units and identity classifications (see respective sections below).
5. (optional) a folder `crls` to include the considered CRLs

6. a folder `keystore` to include a PEM file with the node's signing key; we emphasise that currently RSA keys are not supported
7. a folder `signcerts` to include a PEM file with the node's X.509 certificate
8. (optional) a folder `tlscacerts` to include PEM files each corresponding to a TLS root CA's certificate
9. (optional) a folder `tlsintermediatecerts` to include PEM files each corresponding to an intermediate TLS CA's certificate

In the configuration file of the node (core.yaml file for the peer, and orderer.yaml for the orderer), one needs to specify the path to the mspconfig folder, and the MSP Identifier of the node's MSP. The path to the mspconfig folder is expected to be relative to FABRIC_CFG_PATH and is provided as the value of parameter `mspConfigPath` for the peer, and `LocalMSPDir` for the orderer. The identifier of the node's MSP is provided as a value of parameter `localMspId` for the peer and `LocalMSPID` for the orderer. These variables can be overridden via the environment using the CORE prefix for peer (e.g. CORE_PEER_LOCALMSPID) and the ORDERER prefix for the orderer (e.g. ORDERER_GENERAL_LOCALMSPID). Notice that for the orderer setup, one needs to generate, and provide to the orderer the genesis block of the system channel. The MSP configuration needs of this block are detailed in the next section.

Reconfiguration of a "local" MSP is only possible manually, and requires that the peer or orderer process is restarted. In subsequent releases we aim to offer online/dynamic reconfiguration (i.e. without requiring to stop the node by using a node managed system chaincode).

7.3.4 Organizational Units

In order to configure the list of Organizational Units that valid members of this MSP should include in their X.509 certificate, the `config.yaml` file needs to specify the organizational unit identifiers. Here is an example:

```
OrganizationalUnitIdentifiers:
  - Certificate: "cacerts/cacert1.pem"
    OrganizationalUnitIdentifier: "commercial"
  - Certificate: "cacerts/cacert2.pem"
    OrganizationalUnitIdentifier: "administrators"
```

The above example declares two organizational unit identifiers: **commercial** and **administrators**. An MSP identity is valid if it carries at least one of these organizational unit identifiers. The `Certificate` field refers to the CA or intermediate CA certificate path under which identities, having that specific OU, should be validated. The path is relative to the MSP root folder and cannot be empty.

7.3.5 Identity Classification

The default MSP implementation allows to further classify identities into clients and peers, based on the OUs of their x509 certificates. An identity should be classified as a **client** if it submits transactions, queries peers, etc. An identity should be classified as a **peer** if it endorses or commits transactions. In order to define clients and peers of a given MSP, the `config.yaml` file needs to be set appropriately. Here is an example:

```
NodeOUs:
  Enable: true
  ClientOUIdentifier:
    Certificate: "cacerts/cacert.pem"
    OrganizationalUnitIdentifier: "client"
  PeerOUIdentifier:
    Certificate: "cacerts/cacert.pem"
    OrganizationalUnitIdentifier: "peer"
```

As shown above, the `NodeOUs.Enable` is set to `true`, this enables the identify classification. Then, client (peer) identifiers are defined by setting the following properties for the `NodeOUs.ClientOUIdentifier` (`NodeOUs.PeerOUIdentifier`) key:

1. `OrganizationalUnitIdentifier`: Set this to the value that matches the OU that the x509 certificate of a client (peer) should contain.
2. `Certificate`: Set this to the CA or intermediate CA under which client (peer) identities should be validated. The field is relative to the MSP root folder. It can be empty, meaning that the identity's x509 certificate can be validated under any CA defined in the MSP configuration.

When the classification is enabled, MSP administrators need to be clients of that MSP, meaning that their x509 certificates need to carry the OU that identifies the clients. Notice also that, an identity can be either a client or a peer. The two classifications are mutually exclusive. If an identity is neither a client nor a peer, the validation will fail.

Finally, notice that for upgraded environments the 1.1 channel capability needs to be enabled before identify classification can be used.

7.3.6 Channel MSP setup

At the genesis of the system, verification parameters of all the MSPs that appear in the network need to be specified, and included in the system channel's genesis block. Recall that MSP verification parameters consist of the MSP identifier, the root of trust certificates, intermediate CA and admin certificates, as well as OU specifications and CRLs. The system genesis block is provided to the orderers at their setup phase, and allows them to authenticate channel creation requests. Orderers would reject the system genesis block, if the latter includes two MSPs with the same identifier, and consequently the bootstrapping of the network would fail.

For application channels, the verification components of only the MSPs that govern a channel need to reside in the channel's genesis block. We emphasize that it is **the responsibility of the application** to ensure that correct MSP configuration information is included in the genesis blocks (or the most recent configuration block) of a channel prior to instructing one or more of their peers to join the channel.

When bootstrapping a channel with the help of the configtxgen tool, one can configure the channel MSPs by including the verification parameters of MSP in the mspconfig folder, and setting that path in the relevant section in `configtx.yaml`.

Reconfiguration of an MSP on the channel, including announcements of the certificate revocation lists associated to the CAs of that MSP is achieved through the creation of a `config_update` object by the owner of one of the administrator certificates of the MSP. The client application managed by the admin would then announce this update to the channels in which this MSP appears.

7.3.7 Best Practices

In this section we elaborate on best practices for MSP configuration in commonly met scenarios.

1) Mapping between organizations/corporations and MSPs

We recommend that there is a one-to-one mapping between organizations and MSPs. If a different type of mapping is chosen, the following needs to be to considered:

- **One organization employing various MSPs.** This corresponds to the case of an organization including a variety of divisions each represented by its MSP, either for management independence reasons, or for privacy reasons. In this case a peer can only be owned by a single MSP, and will not recognize peers with identities from other MSPs as peers of the same organization. The implication of this is that peers may share through gossip organization-scoped data with a set of peers that are members of the same subdivision, and NOT with the full set of providers constituting the actual organization.

- **Multiple organizations using a single MSP.** This corresponds to a case of a consortium of organizations that are governed by similar membership architecture. One needs to know here that peers would propagate organization-scoped messages to the peers that have an identity under the same MSP regardless of whether they belong to the same actual organization. This is a limitation of the granularity of MSP definition, and/or of the peer's configuration.

2) One organization has different divisions (say organizational units), to which it wants to grant access to different channels.

Two ways to handle this:

- **Define one MSP to accommodate membership for all organization's members**. Configuration of that MSP would consist of a list of root CAs, intermediate CAs and admin certificates; and membership identities would include the organizational unit (`OU`) a member belongs to. Policies can then be defined to capture members of a specific `OU`, and these policies may constitute the read/write policies of a channel or endorsement policies of a chaincode. A limitation of this approach is that gossip peers would consider peers with membership identities under their local MSP as members of the same organization, and would consequently gossip with them organization-scoped data (e.g. their status).
- **Defining one MSP to represent each division**. This would involve specifying for each division, a set of certificates for root CAs, intermediate CAs, and admin Certs, such that there is no overlapping certification path across MSPs. This would mean that, for example, a different intermediate CA per subdivision is employed. Here the disadvantage is the management of more than one MSPs instead of one, but this circumvents the issue present in the previous approach. One could also define one MSP for each division by leveraging an OU extension of the MSP configuration.

3) Separating clients from peers of the same organization.

In many cases it is required that the "type" of an identity is retrievable from the identity itself (e.g. it may be needed that endorsements are guaranteed to have derived by peers, and not clients or nodes acting solely as orderers).

There is limited support for such requirements.

One way to allow for this separation is to create a separate intermediate CA for each node type - one for clients and one for peers/orderers; and configure two different MSPs - one for clients and one for peers/orderers. Channels this organization should be accessing would need to include both MSPs, while endorsement policies will leverage only the MSP that refers to the peers. This would ultimately result in the organization being mapped to two MSP instances, and would have certain consequences on the way peers and clients interact.

Gossip would not be drastically impacted as all peers of the same organization would still belong to one MSP. Peers can restrict the execution of certain system chaincodes to local MSP based policies. For example, peers would only execute "joinChannel" request if the request is signed by the admin of their local MSP who can only be a client (end-user should be sitting at the origin of that request). We can go around this inconsistency if we accept that the only clients to be members of a peer/orderer MSP would be the administrators of that MSP.

Another point to be considered with this approach is that peers authorize event registration requests based on membership of request originator within their local MSP. Clearly, since the originator of the request is a client, the request originator is always deemed to belong to a different MSP than the requested peer and the peer would reject the request.

4) Admin and CA certificates.

It is important to set MSP admin certificates to be different than any of the certificates considered by the MSP for `root of trust`, or intermediate CAs. This is a common (security) practice to separate the duties of management of membership components from the issuing of new certificates, and/or validation of existing ones.

5) Blacklisting an intermediate CA.

As mentioned in previous sections, reconfiguration of an MSP is achieved by reconfiguration mechanisms (manual reconfiguration for the local MSP instances, and via properly constructed `config_update` messages for MSP instances of a channel). Clearly, there are two ways to ensure an intermediate CA considered in an MSP is no longer considered for that MSP's identity validation:

1. Reconfigure the MSP to no longer include the certificate of that intermediate CA in the list of trusted intermediate CA certs. For the locally configured MSP, this would mean that the certificate of this CA is removed from the `intermediatecerts` folder.
2. Reconfigure the MSP to include a CRL produced by the root of trust which denounces the mentioned intermediate CA's certificate.

In the current MSP implementation we only support method (1) as it is simpler and does not require blacklisting the no longer considered intermediate CA.

6) CAs and TLS CAs

MSP identities' root CAs and MSP TLS certificates' root CAs (and relative intermediate CAs) need to be declared in different folders. This is to avoid confusion between different classes of certificates. It is not forbidden to reuse the same CAs for both MSP identities and TLS certificates but best practices suggest to avoid this in production.

7.4 Channel Configuration (configtx)

Shared configuration for a Hyperledger Fabric blockchain network is stored in a collection configuration transactions, one per channel. Each configuration transaction is usually referred to by the shorter name *configtx*.

Channel configuration has the following important properties:

1. **Versioned**: All elements of the configuration have an associated version which is advanced with every modification. Further, every committed configuration receives a sequence number.
2. **Permissioned**: Each element of the configuration has an associated policy which governs whether or not modification to that element is permitted. Anyone with a copy of the previous configtx (and no additional info) may verify the validity of a new config based on these policies.
3. **Hierarchical**: A root configuration group contains sub-groups, and each group of the hierarchy has associated values and policies. These policies can take advantage of the hierarchy to derive policies at one level from policies of lower levels.

7.4.1 Anatomy of a configuration

Configuration is stored as a transaction of type `HeaderType_CONFIG` in a block with no other transactions. These blocks are referred to as *Configuration Blocks*, the first of which is referred to as the *Genesis Block*.

The proto structures for configuration are stored in `fabric/protos/common/configtx.proto`. The Envelope of type `HeaderType_CONFIG` encodes a `ConfigEnvelope` message as the `Payload data` field. The proto for `ConfigEnvelope` is defined as follows:

```
message ConfigEnvelope {
    Config config = 1;
    Envelope last_update = 2;
}
```

The `last_update` field is defined below in the **Updates to configuration** section, but is only necessary when validating the configuration, not reading it. Instead, the currently committed configuration is stored in the `config` field, containing a `Config` message.

```
message Config {
    uint64 sequence = 1;
    ConfigGroup channel_group = 2;
}
```

The sequence number is incremented by one for each committed configuration. The channel_group field is the root group which contains the configuration. The ConfigGroup structure is recursively defined, and builds a tree of groups, each of which contains values and policies. It is defined as follows:

```
message ConfigGroup {
    uint64 version = 1;
    map<string,ConfigGroup> groups = 2;
    map<string,ConfigValue> values = 3;
    map<string,ConfigPolicy> policies = 4;
    string mod_policy = 5;
}
```

Because ConfigGroup is a recursive structure, it has hierarchical arrangement. The following example is expressed for clarity in golang notation.

```
// Assume the following groups are defined
var root, child1, child2, grandChild1, grandChild2, grandChild3 *ConfigGroup

// Set the following values
root.Groups["child1"] = child1
root.Groups["child2"] = child2
child1.Groups["grandChild1"] = grandChild1
child2.Groups["grandChild2"] = grandChild2
child2.Groups["grandChild3"] = grandChild3

// The resulting config structure of groups looks like:
// root:
//     child1:
//         grandChild1
//     child2:
//         grandChild2
//         grandChild3
```

Each group defines a level in the config hierarchy, and each group has an associated set of values (indexed by string key) and policies (also indexed by string key).

Values are defined by:

```
message ConfigValue {
    uint64 version = 1;
    bytes value = 2;
    string mod_policy = 3;
}
```

Policies are defined by:

```
message ConfigPolicy {
    uint64 version = 1;
    Policy policy = 2;
    string mod_policy = 3;
}
```

Note that Values, Policies, and Groups all have a version and a mod_policy. The version of an element is incremented each time that element is modified. The mod_policy is used to govern the required signatures to modify that element. For Groups, modification is adding or removing elements to the Values, Policies, or Groups maps (or changing the mod_policy). For Values and Policies, modification is changing the Value and Policy fields respectively (or changing the mod_policy). Each element's mod_policy is evaluated in the context of the current level of the config. Consider the following example mod policies defined

at `Channel.Groups["Application"]` (Here, we use the golang map reference syntax, so `Channel.Groups["Application"].Policies["policy1"]` refers to the base `Channel` group's `Application` group's `Policies` map's `policy1` policy.)

- `policy1` maps to `Channel.Groups["Application"].Policies["policy1"]`
- `Org1/policy2` maps to `Channel.Groups["Application"].Groups["Org1"].Policies["policy2"]`
- `/Channel/policy3` maps to `Channel.Policies["policy3"]`

Note that if a `mod_policy` references a policy which does not exist, the item cannot be modified.

7.4.2 Configuration updates

Configuration updates are submitted as an `Envelope` message of type `HeaderType_CONFIG_UPDATE`. The `Payload` `data` of the transaction is a marshaled `ConfigUpdateEnvelope`. The `ConfigUpdateEnvelope` is defined as follows:

```
message ConfigUpdateEnvelope {
    bytes config_update = 1;
    repeated ConfigSignature signatures = 2;
}
```

The `signatures` field contains the set of signatures which authorizes the config update. Its message definition is:

```
message ConfigSignature {
    bytes signature_header = 1;
    bytes signature = 2;
}
```

The `signature_header` is as defined for standard transactions, while the signature is over the concatenation of the `signature_header` bytes and the `config_update` bytes from the `ConfigUpdateEnvelope` message.

The `ConfigUpdateEnvelope` `config_update` bytes are a marshaled `ConfigUpdate` message which is defined as follows:

```
message ConfigUpdate {
    string channel_id = 1;
    ConfigGroup read_set = 2;
    ConfigGroup write_set = 3;
}
```

The `channel_id` is the channel ID the update is bound for, this is necessary to scope the signatures which support this reconfiguration.

The `read_set` specifies a subset of the existing configuration, specified sparsely where only the `version` field is set and no other fields must be populated. The particular `ConfigValue` `value` or `ConfigPolicy` `policy` fields should never be set in the `read_set`. The `ConfigGroup` may have a subset of its map fields populated, so as to reference an element deeper in the config tree. For instance, to include the `Application` group in the `read_set`, its parent (the `Channel` group) must also be included in the read set, but, the `Channel` group does not need to populate all of the keys, such as the `Orderer` `group` key, or any of the `values` or `policies` keys.

The `write_set` specifies the pieces of configuration which are modified. Because of the hierarchical nature of the configuration, a write to an element deep in the hierarchy must contain the higher level elements in its `write_set` as well. However, for any element in the `write_set` which is also specified in the `read_set` at the same version, the element should be specified sparsely, just as in the `read_set`.

For example, given the configuration:

```
Channel: (version 0)
    Orderer (version 0)
    Application (version 3)
       Org1 (version 2)
```

To submit a configuration update which modifies `Org1`, the `read_set` would be:

```
Channel: (version 0)
    Application: (version 3)
```

and the `write_set` would be

```
Channel: (version 0)
    Application: (version 3)
        Org1 (version 3)
```

When the `CONFIG_UPDATE` is received, the orderer computes the resulting `CONFIG` by doing the following:

1. Verifies the `channel_id` and `read_set`. All elements in the `read_set` must exist at the given versions.
2. Computes the update set by collecting all elements in the `write_set` which do not appear at the same version in the `read_set`.
3. Verifies that each element in the update set increments the version number of the element update by exactly 1.
4. Verifies that the signature set attached to the `ConfigUpdateEnvelope` satisfies the `mod_policy` for each element in the update set.
5. Computes a new complete version of the config by applying the update set to the current config.
6. Writes the new config into a `ConfigEnvelope` which includes the `CONFIG_UPDATE` as the `last_update` field and the new config encoded in the `config` field, along with the incremented `sequence` value.
7. Writes the new `ConfigEnvelope` into a `Envelope` of type `CONFIG`, and ultimately writes this as the sole transaction in a new configuration block.

When the peer (or any other receiver for `Deliver`) receives this configuration block, it should verify that the config was appropriately validated by applying the `last_update` message to the current config and verifying that the orderer-computed `config` field contains the correct new configuration.

7.4.3 Permitted configuration groups and values

Any valid configuration is a subset of the following configuration. Here we use the notation `peer.<MSG>` to define a `ConfigValue` whose `value` field is a marshaled proto message of name `<MSG>` defined in `fabric/protos/peer/configuration.proto`. The notations `common.<MSG>`, `msp.<MSG>`, and `orderer.<MSG>` correspond similarly, but with their messages defined in `fabric/protos/common/configuration.proto`, `fabric/protos/msp/mspconfig.proto`, and `fabric/protos/orderer/configuration.proto` respectively.

Note, that the keys `{{org_name}}` and `{{consortium_name}}` represent arbitrary names, and indicate an element which may be repeated with different names.

```
&ConfigGroup{
    Groups: map<string, *ConfigGroup> {
        "Application":&ConfigGroup{
            Groups:map<String, *ConfigGroup> {
                {{org_name}}:&ConfigGroup{
                    Values:map<string, *ConfigValue>{
```

(continues on next page)

(continued from previous page)

```
                        "MSP":msp.MSPConfig,
                        "AnchorPeers":peer.AnchorPeers,
                    },
                },
            },
        },
        "Orderer":&ConfigGroup{
            Groups:map<String, *ConfigGroup> {
                {{org_name}}:&ConfigGroup{
                    Values:map<string, *ConfigValue>{
                        "MSP":msp.MSPConfig,
                    },
                },
            },

            Values:map<string, *ConfigValue> {
                "ConsensusType":orderer.ConsensusType,
                "BatchSize":orderer.BatchSize,
                "BatchTimeout":orderer.BatchTimeout,
                "KafkaBrokers":orderer.KafkaBrokers,
            },
        },
        "Consortiums":&ConfigGroup{
            Groups:map<String, *ConfigGroup> {
                {{consortium_name}}:&ConfigGroup{
                    Groups:map<string, *ConfigGroup> {
                        {{org_name}}:&ConfigGroup{
                            Values:map<string, *ConfigValue>{
                                "MSP":msp.MSPConfig,
                            },
                        },
                    },
                    Values:map<string, *ConfigValue> {
                        "ChannelCreationPolicy":common.Policy,
                    }
                },
            },
        },
    },

    Values: map<string, *ConfigValue> {
        "HashingAlgorithm":common.HashingAlgorithm,
        "BlockHashingDataStructure":common.BlockDataHashingStructure,
        "Consortium":common.Consortium,
        "OrdererAddresses":common.OrdererAddresses,
    },
}
```

7.4.4 Orderer system channel configuration

The ordering system channel needs to define ordering parameters, and consortiums for creating channels. There must be exactly one ordering system channel for an ordering service, and it is the first channel to be created (or more accurately bootstrapped). It is recommended never to define an Application section inside of the ordering system channel genesis configuration, but may be done for testing. Note that any member with read access to the ordering system channel may see all channel creations, so this channel's access should be restricted.

The ordering parameters are defined as the following subset of config:

```
&ConfigGroup{
    Groups: map<string, *ConfigGroup> {
        "Orderer":&ConfigGroup{
            Groups:map<String, *ConfigGroup> {
                {{org_name}}:&ConfigGroup{
                    Values:map<string, *ConfigValue>{
                        "MSP":msp.MSPConfig,
                    },
                },
            },

            Values:map<string, *ConfigValue> {
                "ConsensusType":orderer.ConsensusType,
                "BatchSize":orderer.BatchSize,
                "BatchTimeout":orderer.BatchTimeout,
                "KafkaBrokers":orderer.KafkaBrokers,
            },
        },
    },
```

Each organization participating in ordering has a group element under the `Orderer` group. This group defines a single parameter `MSP` which contains the cryptographic identity information for that organization. The `Values` of the `Orderer` group determine how the ordering nodes function. They exist per channel, so `orderer.BatchTimeout` for instance may be specified differently on one channel than another.

At startup, the orderer is faced with a filesystem which contains information for many channels. The orderer identifies the system channel by identifying the channel with the consortiums group defined. The consortiums group has the following structure.

```
&ConfigGroup{
    Groups: map<string, *ConfigGroup> {
        "Consortiums":&ConfigGroup{
            Groups:map<String, *ConfigGroup> {
                {{consortium_name}}:&ConfigGroup{
                    Groups:map<string, *ConfigGroup> {
                        {{org_name}}:&ConfigGroup{
                            Values:map<string, *ConfigValue>{
                                "MSP":msp.MSPConfig,
                            },
                        },
                    },
                    Values:map<string, *ConfigValue> {
                        "ChannelCreationPolicy":common.Policy,
                    }
                },
            },
        },
    },
},
```

Note that each consortium defines a set of members, just like the organizational members for the ordering orgs. Each consortium also defines a `ChannelCreationPolicy`. This is a policy which is applied to authorize channel creation requests. Typically, this value will be set to an `ImplicitMetaPolicy` requiring that the new members of the channel sign to authorize the channel creation. More details about channel creation follow later in this document.

7.4.5 Application channel configuration

Application configuration is for channels which are designed for application type transactions. It is defined as follows:

```
&ConfigGroup{
    Groups: map<string, *ConfigGroup> {
        "Application":&ConfigGroup{
            Groups:map<String, *ConfigGroup> {
                {{org_name}}:&ConfigGroup{
                    Values:map<string, *ConfigValue>{
                        "MSP":msp.MSPConfig,
                        "AnchorPeers":peer.AnchorPeers,
                    },
                },
            },
        },
    },
}
```

Just like with the `Orderer` section, each organization is encoded as a group. However, instead of only encoding the `MSP` identity information, each org additionally encodes a list of `AnchorPeers`. This list allows the peers of different organizations to contact each other for peer gossip networking.

The application channel encodes a copy of the orderer orgs and consensus options to allow for deterministic updating of these parameters, so the same `Orderer` section from the orderer system channel configuration is included. However from an application perspective this may be largely ignored.

7.4.6 Channel creation

When the orderer receives a `CONFIG_UPDATE` for a channel which does not exist, the orderer assumes that this must be a channel creation request and performs the following.

1. The orderer identifies the consortium which the channel creation request is to be performed for. It does this by looking at the `Consortium` value of the top level group.
2. The orderer verifies that the organizations included in the `Application` group are a subset of the organizations included in the corresponding consortium and that the `ApplicationGroup` is set to `version 1`.
3. The orderer verifies that if the consortium has members, that the new channel also has application members (creation consortiums and channels with no members is useful for testing only).
4. The orderer creates a template configuration by taking the `Orderer` group from the ordering system channel, and creating an `Application` group with the newly specified members and specifying its `mod_policy` to be the `ChannelCreationPolicy` as specified in the consortium config. Note that the policy is evaluated in the context of the new configuration, so a policy requiring `ALL` members, would require signatures from all the new channel members, not all the members of the consortium.
5. The orderer then applies the `CONFIG_UPDATE` as an update to this template configuration. Because the `CONFIG_UPDATE` applies modifications to the `Application` group (its `version` is `1`), the config code validates these updates against the `ChannelCreationPolicy`. If the channel creation contains any other modifications, such as to an individual org's anchor peers, the corresponding mod policy for the element will be invoked.
6. The new `CONFIG` transaction with the new channel config is wrapped and sent for ordering on the ordering system channel. After ordering, the channel is created.

7.5 Endorsement policies

Every chaincode has an endorsement policy which specifies the set of peers on a channel that must execute chaincode and endorse the execution results in order for the transaction to be considered valid. These endorsement policies define the organizations (through their peers) who must "endorse" (i.e., approve of) the execution of a proposal.

Note: Recall that **state**, represented by key-value pairs, is separate from blockchain data. For more on this, check out our *Ledger* documentation.

As part of the transaction validation step performed by the peers, each validating peer checks to make sure that the transaction contains the appropriate **number** of endorsements and that they are from the expected sources (both of these are specified in the endorsement policy). The endorsements are also checked to make sure they're valid (i.e., that they are valid signatures from valid certificates).

7.5.1 Two ways to require endorsement

By default, endorsement policies are specified for a channel's chaincode at instantiation or upgrade time (that is, one endorsement policy covers all of the state associated with a chaincode).

However, there are cases where it may be necessary for a particular state (a particular key-value pair, in other words) to have a different endorsement policy. This **state-based endorsement** allows the default chaincode-level endorsement policies to be overridden by a different policy for the specified keys.

To illustrate the circumstances in which these two types of endorsement policies might be used, consider a channel on which cars are being exchanged. The "creation" — also known as "issuance" – of a car as an asset that can be traded (putting the key-value pair that represents it into the world state, in other words) would have to satisfy the chaincode-level endorsement policy. To see how to set a chaincode-level endorsement policy, check out the section below.

If the car requires a specific endorsement policy, it can be defined either when the car is created or afterwards. There are a number of reasons why it might be necessary or preferable to set a state-specific endorsement policy. The car might have historical importance or value that makes it necessary to have the endorsement of a licensed appraiser. Also, the owner of the car (if they're a member of the channel) might also want to ensure that their peer signs off on a transaction. In both cases, **an endorsement policy is required for a particular asset that is different from the default endorsement policies for the other assets associated with that chaincode.**

We'll show you how to define a state-based endorsement policy in a subsequent section. But first, let's see how we set a chaincode-level endorsement policy.

7.5.2 Setting chaincode-level endorsement policies

Chaincode-level endorsement policies can be specified at instantiate time using either the SDK (for some sample code on how to do this, click here) or in the peer CLI using the `-P` switch followed by the policy.

Note: Don't worry about the policy syntax (`'Org1.member'`, et all) right now. We'll talk more about the syntax in the next section.

For example:

```
peer chaincode instantiate -C <channelid> -n mycc -P "AND('Org1.member', 'Org2.member
↪')"
```

This command deploys chaincode `mycc` ("my chaincode") with the policy `AND('Org1.member', 'Org2.member')` which would require that a member of both Org1 and Org2 sign the transaction.

Notice that, if the identity classification is enabled (see *Membership Service Providers (MSP)*), one can use the `PEER` role to restrict endorsement to only peers.

For example:

```
peer chaincode instantiate -C <channelid> -n mycc -P "AND('Org1.peer', 'Org2.peer')"
```

A new organization added to the channel after instantiation can query a chaincode (provided the query has appropriate authorization as defined by channel policies and any application level checks enforced by the chaincode) but will not be able to execute or endorse the chaincode. The endorsement policy needs to be modified to allow transactions to be committed with endorsements from the new organization.

Note: if not specified at instantiation time, the endorsement policy defaults to "any member of the organizations in the channel". For example, a channel with "Org1" and "Org2" would have a default endorsement policy of "OR('Org1.member', 'Org2.member')".

Endorsement policy syntax

As you can see above, policies are expressed in terms of principals ("principals" are identities matched to a role). Principals are described as `'MSP.ROLE'`, where `MSP` represents the required MSP ID and `ROLE` represents one of the four accepted roles: `member`, `admin`, `client`, and `peer`.

Here are a few examples of valid principals:

- `'Org0.admin'`: any administrator of the `Org0` MSP
- `'Org1.member'`: any member of the `Org1` MSP
- `'Org1.client'`: any client of the `Org1` MSP
- `'Org1.peer'`: any peer of the `Org1` MSP

The syntax of the language is:

```
EXPR(E[, E...])
```

Where `EXPR` is either `AND`, `OR`, or `OutOf`, and `E` is either a principal (with the syntax described above) or another nested call to `EXPR`.

For example:

- `AND('Org1.member', 'Org2.member', 'Org3.member')` requests one signature from each of the three principals.
- `OR('Org1.member', 'Org2.member')` requests one signature from either one of the two principals.
- `OR('Org1.member', AND('Org2.member', 'Org3.member'))` requests either one signature from a member of the `Org1` MSP or one signature from a member of the `Org2` MSP and one signature from a member of the `Org3` MSP.
- `OutOf(1, 'Org1.member', 'Org2.member')`, which resolves to the same thing as `OR('Org1.member', 'Org2.member')`.
- Similarly, `OutOf(2, 'Org1.member', 'B.member')` is equivalent to `AND('Org1.member', 'Org2.member')`.

7.5.3 Setting key-level endorsement policies

Setting regular chaincode-level endorsement policies is tied to the lifecycle of the corresponding chaincode. They can only be set or modified when instantiating or upgrading the corresponding chaincode on a channel.

In contrast, key-level endorsement policies can be set and modified in a more granular fashion from within a chaincode. The modification is part of the read-write set of a regular transaction.

The shim API provides the following functions to set and retrieve an endorsement policy for/from a regular key.

Note: `ep` below stands for the "endorsement policy", which can be expressed either by using the same syntax described above or by using the convenience function described below. Either method will generate a binary version of the endorsement policy that can be consumed by the basic shim API.

```
SetStateValidationParameter(key string, ep []byte) error
GetStateValidationParameter(key string) ([]byte, error)
```

For keys that are part of *Private data* in a collection the following functions apply:

```
SetPrivateDataValidationParameter(collection, key string, ep []byte) error
GetPrivateDataValidationParameter(collection, key string) ([]byte, error)
```

To help set endorsement policies and marshal them into validation parameter byte arrays, the shim provides convenience functions that allow the chaincode developer to deal with endorsement policies in terms of the MSP identifiers of organizations(KeyEndorsementPolicy):

```
type KeyEndorsementPolicy interface {
    // Policy returns the endorsement policy as bytes
    Policy() ([]byte, error)

    // AddOrgs adds the specified orgs to the list of orgs that are required
    // to endorse
    AddOrgs(roleType RoleType, organizations ...string) error

    // DelOrgs delete the specified channel orgs from the existing key-level␣
↪endorsement
    // policy for this KVS key. If any org is not present, an error will be returned.
    DelOrgs(organizations ...string) error

    // ListOrgs returns an array of channel orgs that are required to endorse changes
    ListOrgs() ([]string)
}
```

For example, to set an endorsement policy for a key where two specific orgs are required to endorse the key change, pass both org `MSPIDs` to `AddOrgs()`, and then call `Policy()` to construct the endorsement policy byte array that can be passed to `SetStateValidationParameter()`.

7.5.4 Validation

At commit time, setting a value of a key is no different from setting the endorsement policy of a key — both update the state of the key and are validated based on the same rules.

Validation	no validation parameter set	validation parameter set
modify value	check chaincode ep	check key-level ep
modify key-level ep	check chaincode ep	check key-level ep

As we discussed above, if a key is modified and no key-level endorsement policy is present, the chaincode-level endorsement policy applies by default. This is also true when a key-level endorsement policy is set for a key for the first time — the new key-level endorsement policy must first be endorsed according to the pre-existing chaincode-level endorsement policy.

If a key is modified and a key-level endorsement policy is present, the key-level endorsement policy overrides the chaincode-level endorsement policy. In practice, this means that the key-level endorsement policy can be either less restrictive or more restrictive than the chaincode-level endorsement policy. Because the chaincode-level endorsement policy must be satisfied in order to set a key-level endorsement policy for the first time, no trust assumptions have been violated.

If a key's endorsement policy is removed (set to nil), the chaincode-level endorsement policy becomes the default again.

If a transaction modifies multiple keys with different associated key-level endorsement policies, all of these policies need to be satisfied in order for the transaction to be valid.

7.6 Pluggable transaction endorsement and validation

7.6.1 Motivation

When a transaction is validated at time of commit, the peer performs various checks before applying the state changes that come with the transaction itself:

- Validating the identities that signed the transaction.
- Verifying the signatures of the endorsers on the transaction.
- Ensuring the transaction satisfies the endorsement policies of the namespaces of the corresponding chaincodes.

There are use cases which demand custom transaction validation rules different from the default Fabric validation rules, such as:

- **UTXO (Unspent Transaction Output):** When the validation takes into account whether the transaction doesn't double spend its inputs.
- **Anonymous transactions:** When the endorsement doesn't contain the identity of the peer, but a signature and a public key are shared that can't be linked to the peer's identity.

7.6.2 Pluggable endorsement and validation logic

Fabric allows for the implementation and deployment of custom endorsement and validation logic into the peer to be associated with chaincode handling in a pluggable manner. This logic can be either compiled into the peer as built in selectable logic, or compiled and deployed alongside the peer as a Golang plugin.

Recall that every chaincode is associated with its own endorsement and validation logic at the time of chaincode instantiation. If the user doesn't select one, the default built-in logic is selected implicitly. A peer administrator may alter the endorsement/validation logic that is selected by extending the peer's local configuration with the customization of the endorsement/validation logic which is loaded and applied at peer startup.

7.6.3 Configuration

Each peer has a local configuration (`core.yaml`) that declares a mapping between the endorsement/validation logic name and the implementation that is to be run.

The default logic are called `ESCC` (with the "E" standing for endorsement) and `VSCC` (validation), and they can be found in the peer local configuration in the `handlers` section:

```
handlers:
    endorsers:
      escc:
        name: DefaultEndorsement
    validators:
      vscc:
        name: DefaultValidation
```

When the endorsement or validation implementation is compiled into the peer, the `name` property represents the initialization function that is to be run in order to obtain the factory that creates instances of the endorsement/validation logic.

The function is an instance method of the `HandlerLibrary` construct under `core/handlers/library/library.go` and in order for custom endorsement or validation logic to be added, this construct needs to be extended with any additional methods.

Since this is cumbersome and poses a deployment challenge, one can also deploy custom endorsement and validation as a Golang plugin by adding another property under the `name` called `library`.

For example, if we have custom endorsement and validation logic which is implemented as a plugin, we would have the following entries in the configuration in `core.yaml`:

```
handlers:
    endorsers:
      escc:
        name: DefaultEndorsement
      custom:
        name: customEndorsement
        library: /etc/hyperledger/fabric/plugins/customEndorsement.so
    validators:
      vscc:
        name: DefaultValidation
      custom:
        name: customValidation
        library: /etc/hyperledger/fabric/plugins/customValidation.so
```

And we'd have to place the `.so` plugin files in the peer's local file system.

Note: Hereafter, custom endorsement or validation logic implementation is going to be referred to as "plugins", even if they are compiled into the peer.

7.6.4 Endorsement plugin implementation

To implement an endorsement plugin, one must implement the `Plugin` interface found in `core/handlers/endorsement/api/endorsement.go`:

```
// Plugin endorses a proposal response
type Plugin interface {
    // Endorse signs the given payload(ProposalResponsePayload bytes), and optionally␣
↪mutates it.
    // Returns:
    // The Endorsement: A signature over the payload, and an identity that is used to␣
↪verify the signature
```

(continues on next page)

(continued from previous page)

```
    // The payload that was given as input (could be modified within this function)
    // Or error on failure
    Endorse(payload []byte, sp *peer.SignedProposal) (*peer.Endorsement, []byte,␣
↪error)

    // Init injects dependencies into the instance of the Plugin
    Init(dependencies ...Dependency) error
}
```

An endorsement plugin instance of a given plugin type (identified either by the method name as an instance method of the `HandlerLibrary` or by the plugin `.so` file path) is created for each channel by having the peer invoke the `New` method in the `PluginFactory` interface which is also expected to be implemented by the plugin developer:

```
// PluginFactory creates a new instance of a Plugin
type PluginFactory interface {
    New() Plugin
}
```

The `Init` method is expected to receive as input all the dependencies declared under `core/handlers/endorsement/api/`, identified as embedding the `Dependency` interface.

After the creation of the `Plugin` instance, the `Init` method is invoked on it by the peer with the `dependencies` passed as parameters.

Currently Fabric comes with the following dependencies for endorsement plugins:

- `SigningIdentityFetcher`: Returns an instance of `SigningIdentity` based on a given signed proposal:

```
// SigningIdentity signs messages and serializes its public identity to bytes
type SigningIdentity interface {
    // Serialize returns a byte representation of this identity which is used to␣
↪verify
    // messages signed by this SigningIdentity
    Serialize() ([]byte, error)

    // Sign signs the given payload and returns a signature
    Sign([]byte) ([]byte, error)
}
```

- `StateFetcher`: Fetches a **State** object which interacts with the world state:

```
// State defines interaction with the world state
type State interface {
    // GetPrivateDataMultipleKeys gets the values for the multiple private data items␣
↪in a single call
    GetPrivateDataMultipleKeys(namespace, collection string, keys []string) ([][]byte,
↪ error)

    // GetStateMultipleKeys gets the values for multiple keys in a single call
    GetStateMultipleKeys(namespace string, keys []string) ([][]byte, error)

    // GetTransientByTXID gets the values private data associated with the given txID
    GetTransientByTXID(txID string) ([]*rwset.TxPvtReadWriteSet, error)

    // Done releases resources occupied by the State
    Done()
 }
```

7.6.5 Validation plugin implementation

To implement a validation plugin, one must implement the `Plugin` interface found in `core/handlers/validation/api/validation.go`:

```
// Plugin validates transactions
type Plugin interface {
    // Validate returns nil if the action at the given position inside the transaction
    // at the given position in the given block is valid, or an error if not.
    Validate(block *common.Block, namespace string, txPosition int, actionPosition␣
↪int, contextData ...ContextDatum) error

    // Init injects dependencies into the instance of the Plugin
    Init(dependencies ...Dependency) error
}
```

Each `ContextDatum` is additional runtime-derived metadata that is passed by the peer to the validation plugin. Currently, the only `ContextDatum` that is passed is one that represents the endorsement policy of the chaincode:

```
 // SerializedPolicy defines a serialized policy
type SerializedPolicy interface {
      validation.ContextDatum

      // Bytes returns the bytes of the SerializedPolicy
      Bytes() []byte
 }
```

A validation plugin instance of a given plugin type (identified either by the method name as an instance method of the `HandlerLibrary` or by the plugin `.so` file path) is created for each channel by having the peer invoke the `New` method in the `PluginFactory` interface which is also expected to be implemented by the plugin developer:

```
// PluginFactory creates a new instance of a Plugin
type PluginFactory interface {
    New() Plugin
}
```

The `Init` method is expected to receive as input all the dependencies declared under `core/handlers/validation/api/`, identified as embedding the `Dependency` interface.

After the creation of the `Plugin` instance, the **Init** method is invoked on it by the peer with the dependencies passed as parameters.

Currently Fabric comes with the following dependencies for validation plugins:

- `IdentityDeserializer`: Converts byte representation of identities into `Identity` objects that can be used to verify signatures signed by them, be validated themselves against their corresponding MSP, and see whether they satisfy a given **MSP Principal**. The full specification can be found in `core/handlers/validation/api/identities/identities.go`.
- `PolicyEvaluator`: Evaluates whether a given policy is satisfied:

```
// PolicyEvaluator evaluates policies
type PolicyEvaluator interface {
    validation.Dependency

    // Evaluate takes a set of SignedData and evaluates whether this set of␣
↪signatures satisfies
    // the policy with the given bytes
```

(continues on next page)

(continued from previous page)

```
    Evaluate(policyBytes []byte, signatureSet []*common.SignedData) error
}
```

- `StateFetcher`: Fetches a `State` object which interacts with the world state:

```
// State defines interaction with the world state
type State interface {
    // GetStateMultipleKeys gets the values for multiple keys in a single call
    GetStateMultipleKeys(namespace string, keys []string) ([][]byte, error)

    // GetStateRangeScanIterator returns an iterator that contains all the key-values␣
↪between given key ranges.
    // startKey is included in the results and endKey is excluded. An empty startKey␣
↪refers to the first available key
    // and an empty endKey refers to the last available key. For scanning all the␣
↪keys, both the startKey and the endKey
    // can be supplied as empty strings. However, a full scan should be used␣
↪judiciously for performance reasons.
    // The returned ResultsIterator contains results of type *KV which is defined in␣
↪protos/ledger/queryresult.
    GetStateRangeScanIterator(namespace string, startKey string, endKey string)␣
↪(ResultsIterator, error)

    // GetStateMetadata returns the metadata for given namespace and key
    GetStateMetadata(namespace, key string) (map[string][]byte, error)

    // GetPrivateDataMetadata gets the metadata of a private data item identified by␣
↪a tuple <namespace, collection, key>
    GetPrivateDataMetadata(namespace, collection, key string) (map[string][]byte,␣
↪error)

    // Done releases resources occupied by the State
    Done()
}
```

7.6.6 Important notes

- **Validation plugin consistency across peers:** In future releases, the Fabric channel infrastructure would guarantee that the same validation logic is used for a given chaincode by all peers in the channel at any given blockchain height in order to eliminate the chance of mis-configuration which would might lead to state divergence among peers that accidentally run different implementations. However, for now it is the sole responsibility of the system operators and administrators to ensure this doesn't happen.
- **Validation plugin error handling:** Whenever a validation plugin can't determine whether a given transaction is valid or not, because of some transient execution problem like inability to access the database, it should return an error of type **ExecutionFailureError** that is defined in `core/handlers/validation/api/validation.go`. Any other error that is returned, is treated as an endorsement policy error and marks the transaction as invalidated by the validation logic. However, if an `ExecutionFailureError` is returned, the chain processing halts instead of marking the transaction as invalid. This is to prevent state divergence between different peers.
- **Error handling for private metadata retrieval**: In case a plugin retrieves metadata for private data by making use of the `StateFetcher` interface, it is important that errors are handled as follows: `CollConfigNotDefinedError'' and ``InvalidCollNameError'', signalling that the specified collection does not exist, should be handled`

```
as deterministic errors and should not lead the plugin to return an
``ExecutionFailureError.
```

- **Importing Fabric code into the plugin**: Importing code that belongs to Fabric other than protobufs as part of the plugin is highly discouraged, and can lead to issues when the Fabric code changes between releases, or can cause inoperability issues when running mixed peer versions. Ideally, the plugin code should only use the dependencies given to it, and should import the bare minimum other than protobufs.

7.7 Access Control Lists (ACL)

7.7.1 What is an Access Control List?

Note: This topic deals with access control and policies on a channel administration level. To learn about access control within a chaincode, check out our chaincode for developers tutorial.

Fabric uses access control lists (ACLs) to manage access to resources by associating a **policy** — which specifies a rule that evaluates to true or false, given a set of identities — with the resource. Fabric contains a number of default ACLs. In this document, we'll talk about how they're formatted and how the defaults can be overridden.

But before we can do that, it's necessary to understand a little about resources and policies.

Resources

Users interact with Fabric by targeting a user chaincode, system chaincode, or an events stream source. As such, these endpoints are considered "resources" on which access control should be exercised.

Application developers need to be aware of these resources and the default policies associated with them. The complete list of these resources are found in `configtx.yaml`. You can look at a sample `configtx.yaml` file here.

The resources named in `configtx.yaml` is an exhaustive list of all internal resources currently defined by Fabric. The loose convention adopted there is `<component>/<resource>`. So `cscc/GetConfigBlock` is the resource for the `GetConfigBlock` call in the `CSCC` component.

Policies

Policies are fundamental to the way Fabric works because they allow the identity (or set of identities) associated with a request to be checked against the policy associated with the resource needed to fulfill the request. Endorsement policies are used to determine whether a transaction has been appropriately endorsed. The policies defined in the channel configuration are referenced as modification policies as well as for access control, and are defined in the channel configuration itself.

Policies can be structured in one of two ways: as `Signature` policies or as an `ImplicitMeta` policy.

`Signature` policies

These policies identify specific users who must sign in order for a policy to be satisfied. For example:

```
Policies:
  MyPolicy:
    Type: Signature
    Rule: "Org1.Peer OR Org2.Peer"
```

This policy construct can be interpreted as: *the policy named `MyPolicy` can only be satisfied by the signature of an identity with role of "a peer from Org1" or "a peer from Org2"*.

Signature policies support arbitrary combinations of `AND`, `OR`, and `NOutOf`, allowing the construction of extremely powerful rules like: "An admin of org A and two other admins, or 11 of 20 org admins".

`ImplicitMeta` policies

`ImplicitMeta` policies aggregate the result of policies deeper in the configuration hierarchy that are ultimately defined by `Signature` policies. They support default rules like "A majority of the organization admins". These policies use a different but still very simple syntax as compared to `Signature` policies: `<ALL|ANY|MAJORITY> <sub_policy>`.

For example: `ANY Readers` or `MAJORITY Admins`.

Note that in the default policy configuration `Admins` have an operational role. Policies that specify that only Admins — or some subset of Admins — have access to a resource will tend to be for sensitive or operational aspects of the network (such as instantiating chaincode on a channel). `Writers` will tend to be able to propose ledger updates, such as a transaction, but will not typically have administrative permissions. `Readers` have a passive role. They can access information but do not have the permission to propose ledger updates nor do can they perform administrative tasks. These default policies can be added to, edited, or supplemented, for example by the new `peer` and `client` roles (if you have `NodeOU` support).

Here's an example of an `ImplicitMeta` policy structure:

```
Policies:
  AnotherPolicy:
    Type: ImplicitMeta
    Rule: "MAJORITY Admins"
```

Here, the policy `AnotherPolicy` can be satisfied by the `MAJORITY` of `Admins`, where `Admins` is eventually being specified by lower level `Signature` policy.

Where is access control specified?

Access control defaults exist inside `configtx.yaml`, the file that `configtxgen` uses to build channel configurations.

Access control can be updated one of two ways, either by editing `configtx.yaml` itself, which will propagate the ACL change to any new channels, or by updating access control in the channel configuration of a particular channel.

7.7.2 How ACLs are formatted in `configtx.yaml`

ACLs are formatted as a key-value pair consisting of a resource function name followed by a string. To see what this looks like, reference this sample configtx.yaml file.

Two excerpts from this sample:

```
# ACL policy for invoking chaincodes on peer
peer/Propose: /Channel/Application/Writers
```

```
# ACL policy for sending block events
event/Block: /Channel/Application/Readers
```

These ACLs define that access to `peer/Propose` and `event/Block` resources is restricted to identities satisfying the policy defined at the canonical path `/Channel/Application/Writers` and `/Channel/Application/Readers`, respectively.

Updating ACL defaults in `configtx.yaml`

In cases where it will be necessary to override ACL defaults when bootstrapping a network, or to change the ACLs before a channel has been bootstrapped, the best practice will be to update `configtx.yaml`.

Let's say you want to modify the `peer/Propose` ACL default — which specifies the policy for invoking chaincodes on a peer – from `/Channel/Application/Writers` to a policy called `MyPolicy`.

This is done by adding a policy called `MyPolicy` (it could be called anything, but for this example we'll call it `MyPolicy`). The policy is defined in the `Application.Policies` section inside `configtx.yaml` and specifies a rule to be checked to grant or deny access to a user. For this example, we'll be creating a `Signature` policy identifying `SampleOrg.admin`.

```
Policies: &ApplicationDefaultPolicies
    Readers:
        Type: ImplicitMeta
        Rule: "ANY Readers"
    Writers:
        Type: ImplicitMeta
        Rule: "ANY Writers"
    Admins:
        Type: ImplicitMeta
        Rule: "MAJORITY Admins"
    MyPolicy:
        Type: Signature
        Rule: "OR('SampleOrg.admin')"
```

Then, edit the `Application: ACLs` section inside `configtx.yaml` to change `peer/Propose` from this:

```
peer/Propose: /Channel/Application/Writers
```

To this:

```
peer/Propose: /Channel/Application/MyPolicy
```

Once these fields have been changed in `configtx.yaml`, the `configtxgen` tool will use the policies and ACLs defined when creating a channel creation transaction. When appropriately signed and submitted by one of the admins of the consortium members, a new channel with the defined ACLs and policies is created.

Once `MyPolicy` has been bootstrapped into the channel configuration, it can also be referenced to override other ACL defaults. For example:

```
SampleSingleMSPChannel:
    Consortium: SampleConsortium
    Application:
        <<: *ApplicationDefaults
        ACLs:
            <<: *ACLsDefault
            event/Block: /Channel/Application/MyPolicy
```

This would restrict the ability to subscribe to block events to `SampleOrg.admin`.

If channels have already been created that want to use this ACL, they'll have to update their channel configurations one at a time using the following flow:

Updating ACL defaults in the channel config

If channels have already been created that want to use `MyPolicy` to restrict access to `peer/Propose` — or if they want to create ACLs they don't want other channels to know about — they'll have to update their channel configurations one at a time through config update transactions.

Note: Channel configuration transactions are an involved process we won't delve into here. If you want to read more about them check out our document on channel configuration updates and our "Adding an Org to a Channel" tutorial.

After pulling, translating, and stripping the configuration block of its metadata, you would edit the configuration by adding `MyPolicy` under `Application: policies`, where the `Admins`, `Writers`, and `Readers` policies already live.

```
"MyPolicy": {
  "mod_policy": "Admins",
  "policy": {
    "type": 1,
    "value": {
      "identities": [
        {
          "principal": {
            "msp_identifier": "SampleOrg",
            "role": "ADMIN"
          },
          "principal_classification": "ROLE"
        }
      ],
      "rule": {
        "n_out_of": {
          "n": 1,
          "rules": [
            {
              "signed_by": 0
            }
          ]
        }
      },
      "version": 0
    }
  },
  "version": "0"
},
```

Note in particular the `msp_identifer` and `role` here.

Then, in the ACLs section of the config, change the `peer/Propose` ACL from this:

```
"peer/Propose": {
  "policy_ref": "/Channel/Application/Writers"
```

To this:

```
"peer/Propose": {
  "policy_ref": "/Channel/Application/MyPolicy"
```

Note: If you do not have ACLs defined in your channel configuration, you will have to add the entire ACL structure.

Once the configuration has been updated, it will need to be submitted by the usual channel update process.

Satisfying an ACL that requires access to multiple resources

If a member makes a request that calls multiple system chaincodes, all of the ACLs for those system chaincodes must be satisfied.

For example, `peer/Propose` refers to any proposal request on a channel. If the particular proposal requires access to two system chaincodes that requires an identity satisfying `Writers` and one system chaincode that requires an identity satisfying `MyPolicy`, then the member submitting the proposal must have an identity that evaluates to "true" for both `Writers` and `MyPolicy`.

In the default configuration, `Writers` is a signature policy whose `rule` is `SampleOrg.member`. In other words, "any member of my organization". `MyPolicy`, listed above, has a rule of `SampleOrg.admin`, or "any admin of my organization". To satisfy these ACLs, the member would have to be both an administrator and a member of `SampleOrg`. By default, all administrators are members (though not all administrators are members), but it is possible to overwrite these policies to whatever you want them to be. As a result, it's important to keep track of these policies to ensure that the ACLs for peer proposals are not impossible to satisfy (unless that is the intention).

Migration considerations for customers using the experimental ACL feature

Previously, the management of access control lists was done in an `isolated_data` section of the channel creation transaction and updated via `PEER_RESOURCE_UPDATE` transactions. Originally, it was thought that the `resources` tree would handle the update of several functions that, ultimately, were handled in other ways, so maintaining a separate parallel peer configuration tree was judged to be unnecessary.

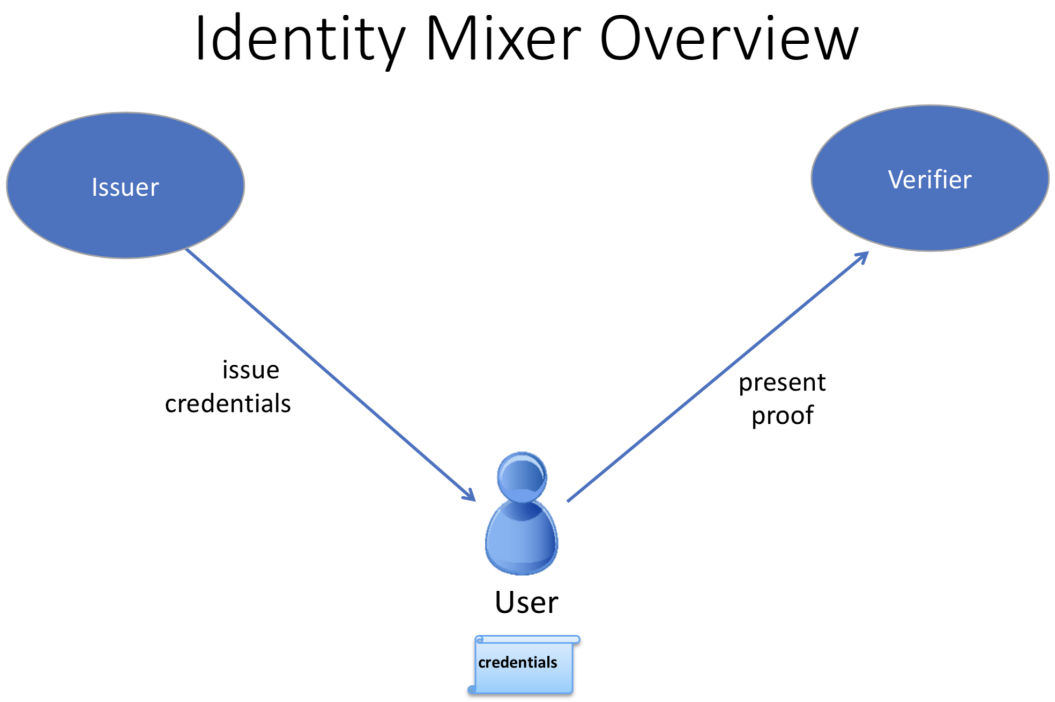
Migration for customers using the experimental resources tree in v1.1 is possible. Because the official v1.2 release does not support the old ACL methods, the network operators should shut down all their peers. Then, they should upgrade them to v1.2, submit a channel reconfiguration transaction which enables the v1.2 capability and sets the desired ACLs, and then finally restart the upgraded peers. The restarted peers will immediately consume the new channel configuration and enforce the ACLs as desired.

7.8 MSP Implementation with Identity Mixer

7.8.1 What is Idemix?

Idemix is a cryptographic protocol suite, which provides strong authentication as well as privacy-preserving features such as **anonymity**, the ability to transact without revealing the identity of the transactor, and **unlinkability**, the ability of a single identity to send multiple transactions without revealing that the transactions were sent by the same identity.

There are three actors involved in an Idemix flow: **user**, **issuer**, and **verifier**.



- An issuer certifies a set of user's attributes are issued in the form of a digital certificate, hereafter called "credential".
- The user later generates a "zero-knowledge proof" of possession of the credential and also selectively discloses only the attributes the user chooses to reveal. The proof, because it is zero-knowledge, reveals no additional information to the verifier, issuer, or anyone else.

As an example, suppose "Alice" needs to prove to Bob (a store clerk) that she has a driver's license issued to her by the DMV.

In this scenario, Alice is the user, the DMV is the issuer, and Bob is the verifier. In order to prove to Bob that Alice has a driver's license, she could show it to him. However, Bob would then be able to see Alice's name, address, exact age, etc. — much more information than Bob needs to know.

Instead, Alice can use Idemix to generate a "zero-knowledge proof" for Bob, which only reveals that she has a valid driver's license and nothing else.

So from the proof:

- Bob does not learn any additional information about Alice other than the fact that she has a valid license (anonymity).
- If Alice visits the store multiple times and generates a proof each time for Bob, Bob would not be able to tell from the proof that it was the same person (unlinkability).

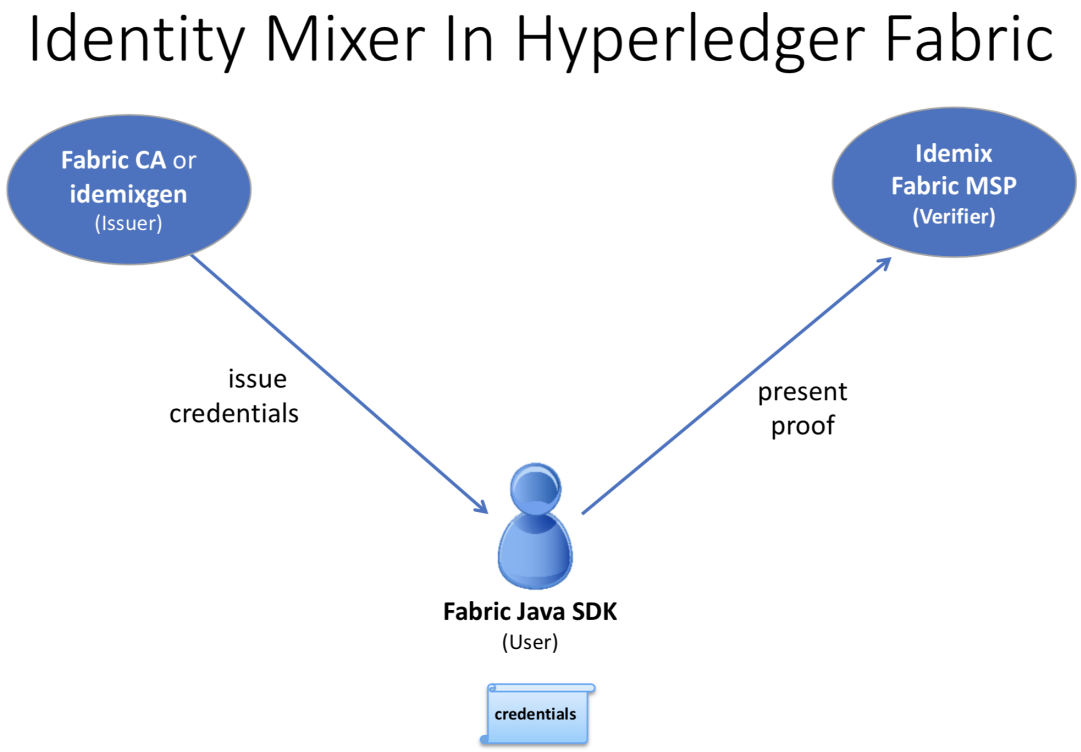
Idemix authentication technology provides the trust model and security guarantees that are similar to what is ensured by standard X.509 certificates but with underlying cryptographic algorithms that efficiently provide advanced privacy features including the ones described above. We'll compare Idemix and X.509 technologies in detail in the technical section below.

7.8.2 How to use Idemix

To understand how to use Idemix with Hyperledger Fabric, we need to see which Fabric components correspond to the user, issuer, and verifier in Idemix.

- The Fabric Java SDK is the API for the **user**. In the future, other Fabric SDKs will also support Idemix.
- Fabric provides two possible Idemix **issuers**:
  1. Fabric CA for production environments or development, and
  2. the *idemixgen* tool for development environments.
- The **verifier** is an Idemix MSP in Fabric.

In order to use Idemix in Hyperledger Fabric, the following three basic steps are required:



Compare the roles in this image to the ones above.

1. Consider the issuer.

   Fabric CA (version 1.3 or later) has been enhanced to automatically function as an Idemix issuer. When `fabric-ca-server` is started (or initialized via the `fabric-ca-server init` command), the following two files are automatically created in the home directory of the `fabric-ca-server`: `IssuerPublicKey` and `IssuerRevocationPublicKey`. These files are required in step 2.

   For a development environment and if you are not using Fabric CA, you may use ‘‘idemixgen‘‘to create these files.

2. Consider the verifier.

   You need to create an Idemix MSP using the `IssuerPublicKey` and `IssuerRevocationPublicKey` from step 1.

   For example, consider the following excerpt from configtx.yaml in the Hyperledger Java SDK sample:

```
- &Org1Idemix
    # defaultorg defines the organization which is used in the sampleconfig
    # of the fabric.git development environment
    name: idemixMSP1

    # id to load the msp definition as
    id: idemixMSPID1

    msptype: idemix
    mspdir: crypto-config/peerOrganizations/org3.example.com
```

The `msptype` is set to `idemix` and the contents of the `mspdir` directory (`crypto-config/peerOrganizations/org3.example.com/msp` in this example) contains the `IssuerPublicKey` and `IssuerRevocationPublicKey` files.

Note that in this example, `Org1Idemix` represents the Idemix MSP for `Org1` (not shown), which would also have an X509 MSP.

3. Consider the user. Recall that the Java SDK is the API for the user.

   There is only a single additional API call required in order to use Idemix with the Java SDK: the `idemixEnroll` method of the `org.hyperledger.fabric_ca.sdk.HFCAClient` class. For example, assume `hfcaClient` is your HFCAClient object and `x509Enrollment` is your `org.hyperledger.fabric.sdk.Enrollment` associated with your X509 certificate.

   The following call will return an `org.hyperledger.fabric.sdk.Enrollment` object associated with your Idemix credential.

```
IdemixEnrollment idemixEnrollment = hfcaClient.idemixEnroll(x509enrollment,
↪"idemixMSPID1");
```

   Note also that `IdemixEnrollment` implements the `org.hyperledger.fabric.sdk.Enrollment` interface and can, therefore, be used in the same way that one uses the X509 enrollment object, except, of course, that this automatically provides the privacy enhancing features of Idemix.

7.8.3 Idemix and chaincode

From a verifier perspective, there is one more actor to consider: chaincode. What can chaincode learn about the transactor when an Idemix credential is used?

The cid (Client Identity) library (for golang only) has been extended to support the `GetAttributeValue` function when an Idemix credential is used. However, as mentioned in the "Current limitations" section below, there are only two attributes which are disclosed in the Idemix case: `ou` and `role`.

If Fabric CA is the credential issuer:

- the value of the *ou* attribute is the identity's **affiliation** (e.g. "org1.department1");
- the value of the `role` attribute will be either 'member' or 'admin'. A value of 'admin' means that the identity is an MSP administrator. By default, identities created by Fabric CA will return the 'member' role. In order to create an 'admin' identity, register the identity with the `role` attribute and a value of `2`.

For an example of setting an affiliation in the Java SDK see this sample.

For an example of using the CID library in go chaincode to retrieve attributes, see this go chaincode.

7.8.4 Current limitations

The current version of Idemix does have a few limitations.

- **Fixed set of attributes**

  It not yet possible to issue or use an Idemix credential with custom attributes. Custom attributes will be supported in a future release.

  The following four attributes are currently supported:

  1. Organizational Unit attribute ("ou"):
  - Usage: same as X.509
  - Type: String
  - Revealed: always
  2. Role attribute ("role"):
  - Usage: same as X.509
  - Type: integer
  - Revealed: always
  3. Enrollment ID attribute
  - Usage: uniquely identify a user — same in all enrollment credentials that belong to the same user (will be used for auditing in the future releases)
  - Type: BIG
  - Revealed: never in the signature, only when generating an authentication token for Fabric CA
  4. Revocation Handle attribute
  - Usage: uniquely identify a credential (will be used for revocation in future releases)
  - Type: integer
  - Revealed: never

- **Revocation is not yet supported**

  Although much of the revocation framework is in place as can be seen by the presence of a revocation handle attribute mentioned above, revocation of an Idemix credential is not yet supported.

- **Peers do not use Idemix for endorsement**

  Currently, Idemix MSP is used by the peers only for signature verification. Signing with Idemix is only done via Client SDK. More roles (including a 'peer' role) will be supported by Idemix MSP.

7.8.5 Technical summary

Comparing Idemix credentials to X.509 certificates

The certificate/credential concept and the issuance process are very similar in Idemix and X.509 certs: a set of attributes is digitally signed with a signature that cannot be forged and there is a secret key to which a credential is cryptographically bound.

The main difference between a standard X.509 certificate and an Identity Mixer credential is the signature scheme that is used to certify the attributes. The signatures underlying the Identity Mixer system allow for efficient proofs of the possession of a signature and the corresponding attributes without revealing the signature and (selected) attribute

values themselves. We use zero-knowledge proofs to ensure that such "knowledge" or "information" is not revealed while ensuring that the signature over some attributes is valid and the user is in possession of the corresponding credential secret key.

Such proofs, like X.509 certificates, can be verified with the public key of the authority that originally signed the credential and cannot be successfully forged. Only the user who knows the credential secret key can generate the proofs about the credential and its attributes.

With regard to unlinkability, when an X.509 certificate is presented, all attributes have to be revealed to verify the certificate signature. This implies that all certificate usages for signing transactions are linkable.

To avoid such linkability, fresh X.509 certificates need to be used every time, which results in complex key management and communication and storage overhead. Furthermore, there are cases where it is important that not even the CA issuing the certificates is able to link all the transactions to the user.

Idemix helps to avoid linkability with respect to both the CA and verifiers, since even the CA is not able to link proofs to the original credential. Neither the issuer nor a verifier can tell whether two proofs were derived from the same credential (or from two different ones).

More details on the concepts and features of the Identity Mixer technology are described in the paper Concepts and Languages for Privacy-Preserving Attribute-Based Authentication.

Underlying cryptographic protocols

Idemix technology is built from a blind signature scheme that supports multiple messages and efficient zero-knowledge proofs of signature possession. All of the cryptographic building blocks for Idemix were published at the top conferences and journals and verified by the scientific community.

This particular Idemix implementation for Fabric uses a pairing-based signature scheme that was briefly proposed by Camenisch and Lysyanskaya and described in detail by Au et al.. The ability to prove knowledge of a signature in a zero-knowledge proof Camenisch et al. was used.

7.9 Identity Mixer MSP configuration generator (idemixgen)

This document describes the usage for the `idemixgen` utility, which can be used to create configuration files for the identity mixer based MSP. Two commands are available, one for creating a fresh CA key pair, and one for creating an MSP config using a previously generated CA key.

7.9.1 Directory Structure

The `idemixgen` tool will create directories with the following structure:

```
- /ca/
    IssuerSecretKey
    IssuerPublicKey
    RevocationKey
- /msp/
    IssuerPublicKey
    RevocationPublicKey
- /user/
    SignerConfig
```

The `ca` directory contains the issuer secret key (including the revocation key) and should only be present for a CA. The `msp` directory contains the information required to set up an MSP verifying idemix signatures. The `user` directory specifies a default signer.

7.9.2 CA Key Generation

CA (issuer) keys suitable for identity mixer can be created using command `idemixgen ca-keygen`. This will create directories `ca` and `msp` in the working directory.

7.9.3 Adding a Default Signer

After generating the `ca` and `msp` directories with `idemixgen ca-keygen`, a default signer specified in the `user` directory can be added to the config with `idemixgen signerconfig`.

```
$ idemixgen signerconfig -h
usage: idemixgen signerconfig [<flags>]

Generate a default signer for this Idemix MSP

Flags:
    -h, --help               Show context-sensitive help (also try --help-long and --
↪help-man).
    -u, --org-unit=ORG-UNIT  The Organizational Unit of the default signer
    -a, --admin              Make the default signer admin
    -e, --enrollment-id=ENROLLMENT-ID
                             The enrollment id of the default signer
    -r, --revocation-handle=REVOCATION-HANDLE
                             The handle used to revoke this signer
```

For example, we can create a default signer that is a member of organizational unit "OrgUnit1", with enrollment identity "johndoe", revocation handle "1234", and that is an admin, with the following command:

```
idemixgen signerconfig -u OrgUnit1 --admin -e "johndoe" -r 1234
```

7.10 Error handling

7.10.1 General Overview

Hyperledger Fabric code should use the vendored package **github.com/pkg/errors** in place of the standard error type provided by Go. This package allows easy generation and display of stack traces with error messages.

7.10.2 Usage Instructions

github.com/pkg/errors should be used in place of all calls to `fmt.Errorf()` or `errors.New()`. Using this package will generate a call stack that will be appended to the error message.

Using this package is simple and will only require easy tweaks to your code.

First, you'll need to import **github.com/pkg/errors**.

Next, update all errors that are generated by your code to use one of the error creation functions (errors.New(), errors.Errorf(), errors.WithMessage(), errors.Wrap(), errors.Wrapf().

Note: See https://godoc.org/github.com/pkg/errors for complete documentation of the available error creation function. Also, refer to the General guidelines section below for more specific guidelines for using the package for Fabric code.

Finally, change the formatting directive for any logger or fmt.Printf() calls from `%s` to `%+v` to print the call stack along with the error message.

7.10.3 General guidelines for error handling in Hyperledger Fabric

- If you are servicing a user request, you should log the error and return it.
- If the error comes from an external source, such as a Go library or vendored package, wrap the error using errors.Wrap() to generate a call stack for the error.
- If the error comes from another Fabric function, add further context, if desired, to the error message using errors.WithMessage() while leaving the call stack unaffected.
- A panic should not be allowed to propagate to other packages.

7.10.4 Example program

The following example program provides a clear demonstration of using the package:

```
package main

import (
  "fmt"

  "github.com/pkg/errors"
)

func wrapWithStack() error {
  err := createError()
  // do this when error comes from external source (go lib or vendor)
  return errors.Wrap(err, "wrapping an error with stack")
}
func wrapWithoutStack() error {
  err := createError()
  // do this when error comes from internal Fabric since it already has stack trace
  return errors.WithMessage(err, "wrapping an error without stack")
}
func createError() error {
  return errors.New("original error")
}

func main() {
  err := createError()
  fmt.Printf("print error without stack: %s\n\n", err)
  fmt.Printf("print error with stack: %+v\n\n", err)
  err = wrapWithoutStack()
  fmt.Printf("%+v\n\n", err)
  err = wrapWithStack()
  fmt.Printf("%+v\n\n", err)
}
```

7.11 Logging Control

7.11.1 Overview

Logging in the `peer` application and in the `shim` interface to chaincodes is programmed using facilities provided by the `github.com/op/go-logging` package. This package supports

- Logging control based on the severity of the message
- Logging control based on the software *module* generating the message
- Different pretty-printing options based on the severity of the message

All logs are currently directed to `stderr`, and the pretty-printing is currently fixed. However global and module-level control of logging by severity is provided for both users and developers. There are currently no formalized rules for the types of information provided at each severity level, however when submitting bug reports the developers may want to see full logs down to the DEBUG level.

In pretty-printed logs the logging level is indicated both by color and by a 4-character code, e.g, "ERRO" for ERROR, "DEBU" for DEBUG, etc. In the logging context a *module* is an arbitrary name (string) given by developers to groups of related messages. In the pretty-printed example below, the logging modules "peer", "rest" and "main" are generating logs.

```
16:47:09.634 [peer] GetLocalAddress -> INFO 033 Auto detected peer address: 9.3.158.
↪178:7051
16:47:09.635 [rest] StartOpenchainRESTServer -> INFO 035 Initializing the REST␣
↪service...
16:47:09.635 [main] serve -> INFO 036 Starting peer with id=name:"vp1" , network␣
↪id=dev, address=9.3.158.178:7051, discovery.rootnode=, validator=true
```

An arbitrary number of logging modules can be created at runtime, therefore there is no "master list" of modules, and logging control constructs can not check whether logging modules actually do or will exist. Also note that the logging module system does not understand hierarchy or wildcarding: You may see module names like "foo/bar" in the code, but the logging system only sees a flat string. It doesn't understand that "foo/bar" is related to "foo" in any way, or that "foo/*" might indicate all "submodules" of foo.

7.11.2 peer

The logging level of the `peer` command can be controlled from the command line for each invocation using the `--logging-level` flag, for example

```
peer node start --logging-level=debug
```

The default logging level for each individual `peer` subcommand can also be set in the core.yaml file. For example the key `logging.node` sets the default level for the `node` subcommand. Comments in the file also explain how the logging level can be overridden in various ways by using environment variables.

Logging severity levels are specified using case-insensitive strings chosen from

```
CRITICAL | ERROR | WARNING | NOTICE | INFO | DEBUG
```

The full logging level specification for the `peer` is of the form

```
[<module>[,<module>...]=]<level>[:[<module>[,<module>...]=]<level>...]
```

A logging level by itself is taken as the overall default. Otherwise, overrides for individual or groups of modules can be specified using the

```
<module>[,<module>...]=<level>
```

syntax. Examples of specifications (valid for all of `--logging-level`, environment variable and core.yaml settings):

```
info                                          - Set default to INFO
warning:main,db=debug:chaincode=info          - Default WARNING; Override for main,db,
↪chaincode
chaincode=info:main=debug:db=debug:warning - Same as above
```

7.11.3 Go chaincodes

The standard mechanism to log within a chaincode application is to integrate with the logging transport exposed to each chaincode instance via the peer. The chaincode `shim` package provides APIs that allow a chaincode to create and manage logging objects whose logs will be formatted and interleaved consistently with the `shim` logs.

As independently executed programs, user-provided chaincodes may technically also produce output on stdout/stderr. While naturally useful for "devmode", these channels are normally disabled on a production network to mitigate abuse from broken or malicious code. However, it is possible to enable this output even for peer-managed containers (e.g. "netmode") on a per-peer basis via the CORE_VM_DOCKER_ATTACHSTDOUT=true configuration option.

Once enabled, each chaincode will receive its own logging channel keyed by its container-id. Any output written to either stdout or stderr will be integrated with the peer's log on a per-line basis. It is not recommended to enable this for production.

API

`NewLogger(name string) *ChaincodeLogger` - Create a logging object for use by a chaincode

`(c *ChaincodeLogger) SetLevel(level LoggingLevel)` - Set the logging level of the logger

`(c *ChaincodeLogger) IsEnabledFor(level LoggingLevel) bool` - Return true if logs will be generated at the given level

`LogLevel(levelString string) (LoggingLevel, error)` - Convert a string to a `LoggingLevel`

A `LoggingLevel` is a member of the enumeration

```
LogDebug, LogInfo, LogNotice, LogWarning, LogError, LogCritical
```

which can be used directly, or generated by passing a case-insensitive version of the strings

```
DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL
```

to the `LogLevel` API.

Formatted logging at various severity levels is provided by the functions

```
(c *ChaincodeLogger) Debug(args ...interface{})
(c *ChaincodeLogger) Info(args ...interface{})
(c *ChaincodeLogger) Notice(args ...interface{})
(c *ChaincodeLogger) Warning(args ...interface{})
(c *ChaincodeLogger) Error(args ...interface{})
(c *ChaincodeLogger) Critical(args ...interface{})

(c *ChaincodeLogger) Debugf(format string, args ...interface{})
```

(continues on next page)

(continued from previous page)

```
(c *ChaincodeLogger) Infof(format string, args ...interface{})
(c *ChaincodeLogger) Noticef(format string, args ...interface{})
(c *ChaincodeLogger) Warningf(format string, args ...interface{})
(c *ChaincodeLogger) Errorf(format string, args ...interface{})
(c *ChaincodeLogger) Criticalf(format string, args ...interface{})
```

The `f` forms of the logging APIs provide for precise control over the formatting of the logs. The non-`f` forms of the APIs currently insert a space between the printed representations of the arguments, and arbitrarily choose the formats to use.

In the current implementation, the logs produced by the `shim` and a `ChaincodeLogger` are timestamped, marked with the logger *name* and severity level, and written to `stderr`. Note that logging level control is currently based on the *name* provided when the `ChaincodeLogger` is created. To avoid ambiguities, all `ChaincodeLogger` should be given unique names other than "shim". The logger *name* will appear in all log messages created by the logger. The `shim` logs as "shim".

The default logging level for loggers within the Chaincode container can be set in the core.yaml file. The key `chaincode.logging.level` sets the default level for all loggers within the Chaincode container. The key `chaincode.logging.shim` overrides the default level for the `shim` module.

```
# Logging section for the chaincode container
logging:
  # Default level for all loggers within the chaincode container
  level:  info
  # Override default level for the 'shim' module
  shim:   warning
```

The default logging level can be overridden by using environment variables. `CORE_CHAINCODE_LOGGING_LEVEL` sets the default logging level for all modules. `CORE_CHAINCODE_LOGGING_SHIM` overrides the level for the `shim` module.

Go language chaincodes can also control the logging level of the chaincode `shim` interface through the `SetLoggingLevel` API.

`SetLoggingLevel(LoggingLevel level)` - Control the logging level of the shim

Below is a simple example of how a chaincode might create a private logging object logging at the `LogInfo` level.

```
var logger = shim.NewLogger("myChaincode")

func main() {

    logger.SetLevel(shim.LogInfo)
    ...
}
```

7.12 Securing Communication With Transport Layer Security (TLS)

Fabric supports for secure communication between nodes using TLS. TLS communication can use both one-way (server only) and two-way (server and client) authentication.

7.12.1 Configuring TLS for peers nodes

A peer node is both a TLS server and a TLS client. It is the former when another peer node, application, or the CLI makes a connection to it and the latter when it makes a connection to another peer node or orderer.

To enable TLS on a peer node set the following peer configuration properties:

- `peer.tls.enabled` = `true`
- `peer.tls.cert.file` = fully qualified path of the file that contains the TLS server certificate
- `peer.tls.key.file` = fully qualified path of the file that contains the TLS server private key
- `peer.tls.rootcert.file` = fully qualified path of the file that contains the certificate chain of the certificate authority(CA) that issued TLS server certificate

By default, TLS client authentication is turned off when TLS is enabled on a peer node. This means that the peer node will not verify the certificate of a client (another peer node, application, or the CLI) during a TLS handshake. To enable TLS client authentication on a peer node, set the peer configuration property `peer.tls.clientAuthRequired` to `true` and set the `peer.tls.clientRootCAs.files` property to the CA chain file(s) that contain(s) the CA certificate chain(s) that issued TLS certificates for your organization's clients.

By default, a peer node will use the same certificate and private key pair when acting as a TLS server and client. To use a different certificate and private key pair for the client side, set the `peer.tls.clientCert.file` and `peer.tls.clientKey.file` configuration properties to the fully qualified path of the client certificate and key file, respectively.

TLS with client authentication can also be enabled by setting the following environment variables:

- `CORE_PEER_TLS_ENABLED` = `true`
- `CORE_PEER_TLS_CERT_FILE` = fully qualified path of the server certificate
- `CORE_PEER_TLS_KEY_FILE` = fully qualified path of the server private key
- `CORE_PEER_TLS_ROOTCERT_FILE` = fully qualified path of the CA chain file
- `CORE_PEER_TLS_CLIENTAUTHREQUIRED` = `true`
- `CORE_PEER_TLS_CLIENTROOTCAS_FILES` = fully qualified path of the CA chain file
- `CORE_PEER_TLS_CLIENTCERT_FILE` = fully qualified path of the client certificate
- `CORE_PEER_TLS_CLIENTKEY_FILE` = fully qualified path of the client key

When client authentication is enabled on a peer node, a client is required to send its certificate during a TLS handshake. If the client does not send its certificate, the handshake will fail and the peer will close the connection.

When a peer joins a channel, root CA certificate chains of the channel members are read from the config block of the channel and are added to the TLS client and server root CAs data structure. So, peer to peer communication, peer to orderer communication should work seamlessly.

7.12.2 Configuring TLS for orderer nodes

To enable TLS on an orderer node, set the following orderer configuration properties:

- `General.TLS.Enabled` = `true`
- `General.TLS.PrivateKey` = fully qualified path of the file that contains the server private key
- `General.TLS.Certificate` = fully qualified path of the file that contains the server certificate
- `General.TLS.RootCAs` = fully qualified path of the file that contains the certificate chain of the CA that issued TLS server certificate

By default, TLS client authentication is turned off on orderer, as is the case with peer. To enable TLS client authentication, set the following config properties:

- `General.TLS.ClientAuthRequired = true`
- `General.TLS.ClientRootCAs` = fully qualified path of the file that contains the certificate chain of the CA that issued the TLS server certificate

TLS with client authentication can also be enabled by setting the following environment variables:

- `ORDERER_GENERAL_TLS_ENABLED = true`
- `ORDERER_GENERAL_TLS_PRIVATEKEY` = fully qualified path of the file that contains the server private key
- `ORDERER_GENERAL_TLS_CERTIFICATE` = fully qualified path of the file that contains the server certificate
- `ORDERER_GENERAL_TLS_ROOTCAS` = fully qualified path of the file that contains the certificate chain of the CA that issued TLS server certificate
- `ORDERER_GENERAL_TLS_CLIENTAUTHREQUIRED = true`
- `ORDERER_GENERAL_TLS_CLIENTROOTCAS` = fully qualified path of the file that contains the certificate chain of the CA that issued TLS server certificate

7.12.3 Configuring TLS for the peer CLI

The following environment variables must be set when running peer CLI commands against a TLS enabled peer node:

- `CORE_PEER_TLS_ENABLED = true`
- `CORE_PEER_TLS_ROOTCERT_FILE` = fully qualified path of the file that contains cert chain of the CA that issued the TLS server cert

If TLS client authentication is also enabled on the remote server, the following variables must to be set in addition to those above:

- `CORE_PEER_TLS_CLIENTAUTHREQUIRED = true`
- `CORE_PEER_TLS_CLIENTCERT_FILE` = fully qualified path of the client certificate
- `CORE_PEER_TLS_CLIENTKEY_FILE` = fully qualified path of the client private key

When running a command that connects to orderer service, like *peer channel <create|update|fetch>* or *peer chaincode <invoke|instantiate>*, following command line arguments must also be specified if TLS is enabled on the orderer:

- –tls
- –cafile <fully qualified path of the file that contains cert chain of the orderer CA>

If TLS client authentication is enabled on the orderer, the following arguments must be specified as well:

- –clientauth
- –keyfile <fully qualified path of the file that contains the client private key>
- –certfile <fully qualified path of the file that contains the client certificate>

7.12.4 Debugging TLS issues

Before debugging TLS issues, it is advisable to enable `GRPC debug` on both the TLS client and the server side to get additional information. To enable `GRPC debug`, set the environment variable `CORE_LOGGING_GRPC` to `DEBUG`.

If you see the error message `remote error: tls: bad certificate` on the client side, it usually means that the TLS server has enabled client authentication and the server either did not receive the correct client certificate

or it received a client certificate that it does not trust. Make sure the client is sending its certificate and that it has been signed by one of the CA certificates trusted by the peer or orderer node.

If you see the error message `remote error: tls: bad certificate` in your chaincode logs, ensure that your chaincode has been built using the chaincode shim provided with Fabric v1.1 or newer. If your chaincode does not contain a vendored copy of the shim, deleting the chaincode container and restarting its peer will rebuild the chaincode container using the current shim version.

7.13 Bringing up a Kafka-based Ordering Service

7.13.1 Caveat emptor

This document assumes that the reader generally knows how to set up a Kafka cluster and a ZooKeeper ensemble. The purpose of this guide is to identify the steps you need to take so as to have a set of Hyperledger Fabric ordering service nodes (OSNs) use your Kafka cluster and provide an ordering service to your blockchain network.

7.13.2 Big picture

Each channel maps to a separate single-partition topic in Kafka. When an OSN receives transactions via the `Broadcast` RPC, it checks to make sure that the broadcasting client has permissions to write on the channel, then relays (i.e. produces) those transactions to the appropriate partition in Kafka. This partition is also consumed by the OSN which groups the received transactions into blocks locally, persists them in its local ledger, and serves them to receiving clients via the `Deliver` RPC. For low-level details, refer to the document that describes how we came to this design — Figure 8 is a schematic representation of the process described above.

7.13.3 Steps

Let `K` and `Z` be the number of nodes in the Kafka cluster and the ZooKeeper ensemble respectively:

1. At a minimum, `K` should be set to 4. (As we will explain in Step 4 below, this is the minimum number of nodes necessary in order to exhibit crash fault tolerance, i.e. with 4 brokers, you can have 1 broker go down, all channels will continue to be writeable and readable, and new channels can be created.)
2. `Z` will either be 3, 5, or 7. It has to be an odd number to avoid split-brain scenarios, and larger than 1 in order to avoid single point of failures. Anything beyond 7 ZooKeeper servers is considered an overkill.

Then proceed as follows:

3. Orderers: **Encode the Kafka-related information in the network's genesis block.** If you are using `configtxgen`, edit `configtx.yaml` —or pick a preset profile for the system channel's genesis block— so that:
   (a) `Orderer.OrdererType` is set to `kafka`.
   (b) `Orderer.Kafka.Brokers` contains the address of *at least two* of the Kafka brokers in your cluster in `IP:port` notation. The list does not need to be exhaustive. (These are your bootstrap brokers.)
4. Orderers: **Set the maximum block size.** Each block will have at most *Orderer.AbsoluteMaxBytes* bytes (not including headers), a value that you can set in `configtx.yaml`. Let the value you pick here be `A` and make note of it — it will affect how you configure your Kafka brokers in Step 6.
5. Orderers: **Create the genesis block.** Use `configtxgen`. The settings you picked in Steps 3 and 4 above are system-wide settings, i.e. they apply across the network for all the OSNs. Make note of the genesis block's location.

6. Kafka cluster: **Configure your Kafka brokers appropriately.** Ensure that every Kafka broker has these keys configured:

   (a) `unclean.leader.election.enable = false` — Data consistency is key in a blockchain environment. We cannot have a channel leader chosen outside of the in-sync replica set, or we run the risk of overwriting the offsets that the previous leader produced, and —as a result— rewrite the blockchain that the orderers produce.

   (b) `min.insync.replicas = M` — Where you pick a value `M` such that `1 < M < N` (see `default.replication.factor` below). Data is considered committed when it is written to at least `M` replicas (which are then considered in-sync and belong to the in-sync replica set, or ISR). In any other case, the write operation returns an error. Then:

      i. If up to `N-M` replicas —out of the `N` that the channel data is written to— become unavailable, operations proceed normally.

      ii. If more replicas become unavailable, Kafka cannot maintain an ISR set of `M`, so it stops accepting writes. Reads work without issues. The channel becomes writeable again when `M` replicas get in-sync.

   (c) `default.replication.factor = N` — Where you pick a value `N` such that `N < K`. A replication factor of `N` means that each channel will have its data replicated to `N` brokers. These are the candidates for the ISR set of a channel. As we noted in the `min.insync.replicas section` above, not all of these brokers have to be available all the time. `N` should be set *strictly smaller* to `K` because channel creations cannot go forward if less than `N` brokers are up. So if you set `N = K`, a single broker going down means that no new channels can be created on the blockchain network — the crash fault tolerance of the ordering service is non-existent.

   Based on what we've described above, the minimum allowed values for `M` and `N` are 2 and 3 respectively. This configuration allows for the creation of new channels to go forward, and for all channels to continue to be writeable.

   (d) `message.max.bytes` and `replica.fetch.max.bytes` should be set to a value larger than `A`, the value you picked in `Orderer.AbsoluteMaxBytes` in Step 4 above. Add some buffer to account for headers — 1 MiB is more than enough. The following condition applies:

   ```
   Orderer.AbsoluteMaxBytes < replica.fetch.max.bytes <= message.max.bytes
   ```

   (For completeness, we note that `message.max.bytes` should be strictly smaller to `socket.request.max.bytes` which is set by default to 100 MiB. If you wish to have blocks larger than 100 MiB you will need to edit the hard-coded value in `brokerConfig.Producer.MaxMessageBytes` in `fabric/orderer/kafka/config.go` and rebuild the binary from source. This is not advisable.)

   (e) `log.retention.ms = -1`. Until the ordering service adds support for pruning of the Kafka logs, you should disable time-based retention and prevent segments from expiring. (Size-based retention —see `log.retention.bytes`— is disabled by default in Kafka at the time of this writing, so there's no need to set it explicitly.)

7. Orderers: **Point each OSN to the genesis block.** Edit `General.GenesisFile` in `orderer.yaml` so that it points to the genesis block created in Step 5 above. (While at it, ensure all other keys in that YAML file are set appropriately.)

8. Orderers: **Adjust polling intervals and timeouts.** (Optional step.)

   (a) The `Kafka.Retry` section in the `orderer.yaml` file allows you to adjust the frequency of the metadata/producer/consumer requests, as well as the socket timeouts. (These are all settings you would expect to see in a Kafka producer or consumer.)

   (b) Additionally, when a new channel is created, or when an existing channel is reloaded (in case of a just-restarted orderer), the orderer interacts with the Kafka cluster in the following ways:

      i. It creates a Kafka producer (writer) for the Kafka partition that corresponds to the channel.

ii. It uses that producer to post a no-op `CONNECT` message to that partition.

iii. It creates a Kafka consumer (reader) for that partition.

If any of these steps fail, you can adjust the frequency with which they are repeated. Specifically they will be re-attempted every `Kafka.Retry.ShortInterval` for a total of `Kafka.Retry.ShortTotal`, and then every `Kafka.Retry.LongInterval` for a total of `Kafka.Retry.LongTotal` until they succeed. Note that the orderer will be unable to write to or read from a channel until all of the steps above have been completed successfully.

9. **Set up the OSNs and Kafka cluster so that they communicate over SSL.** (Optional step, but highly recommended.) Refer to the Confluent guide for the Kafka cluster side of the equation, and set the keys under `Kafka.TLS` in `orderer.yaml` on every OSN accordingly.

10. **Bring up the nodes in the following order: ZooKeeper ensemble, Kafka cluster, ordering service nodes.**

7.13.4 Additional considerations

1. **Preferred message size.** In Step 4 above (see *Steps* section) you can also set the preferred size of blocks by setting the `Orderer.Batchsize.PreferredMaxBytes` key. Kafka offers higher throughput when dealing with relatively small messages; aim for a value no bigger than 1 MiB.

2. **Using environment variables to override settings.** When using the sample Kafka and Zookeeper Docker images provided with Fabric (see `images/kafka` and `images/zookeeper` respectively), you can override a Kafka broker or a ZooKeeper server's settings by using environment variables. Replace the dots of the configuration key with underscores — e.g. `KAFKA_UNCLEAN_LEADER_ELECTION_ENABLE=false` will allow you to override the default value of `unclean.leader.election.enable`. The same applies to the OSNs for their *local* configuration, i.e. what can be set in `orderer.yaml`. For example `ORDERER_KAFKA_RETRY_SHORTINTERVAL=1s` allows you to override the default value for `Orderer.Kafka.Retry.ShortInterval`.

7.13.5 Kafka Protocol Version Compatibility

Fabric uses the sarama client library and vendors a version of it that supports Kafka 0.10 to 1.0, yet is still known to work with older versions.

Using the `Kafka.Version` key in `orderer.yaml`, you can configure which version of the Kafka protocol is used to communicate with the Kafka cluster's brokers. Kafka brokers are backward compatible with older protocol versions. Because of a Kafka broker's backward compatibility with older protocol versions, upgrading your Kafka brokers to a new version does not require an update of the `Kafka.Version` key value, but the Kafka cluster might suffer a performance penalty while using an older protocol version.

7.13.6 Debugging

Set `General.LogLevel` to `DEBUG` and `Kafka.Verbose` in `orderer.yaml` to `true`.

CHAPTER 8

Commands Reference

8.1 peer

8.1.1 Description

The `peer` command has five different subcommands, each of which allows administrators to perform a specific set of tasks related to a peer. For example, you can use the `peer channel` subcommand to join a peer to a channel, or the `peer chaincode` command to deploy a smart contract chaincode to a peer.

8.1.2 Syntax

The `peer` command has five different subcommands within it:

```
peer chaincode [option] [flags]
peer channel   [option] [flags]
peer logging   [option] [flags]
peer node      [option] [flags]
peer version   [option] [flags]
```

Each subcommand has different options available, and these are described in their own dedicated topic. For brevity, we often refer to a command (`peer`), a subcommand (`channel`), or subcommand option (`fetch`) simply as a **command**.

If a subcommand is specified without an option, then it will return some high level help text as described in the `--help` flag below.

8.1.3 Flags

Each `peer` subcommand has a specific set of flags associated with it, many of which are designated *global* because they can be used in all subcommand options. These flags are described with the relevant `peer` subcommand.

The top level `peer` command has the following flags:

- `--help`

  Use `--help` to get brief help text for any `peer` command. The `--help` flag is very useful – it can be used to get command help, subcommand help, and even option help.

  For example

```
peer --help
peer channel --help
peer channel list --help
```

  See individual `peer` subcommands for more detail.

- `--logging-level <string>`

  This flag sets the logging level for a peer when it is started.

  There are six possible values for `<string>` : `debug`, `info`, `warning`, `error`, `panic`, and `fatal`.

  If `logging-level` is not explicitly specified, then it is taken from the `CORE_LOGGING_LEVEL` environment variable if it is set. If `CORE_LOGGING_LEVEL` is not set then the file `sampleconfig/core.yaml` is used to determined the logging level for the peer.

  You can find the current logging level for a specific component on the peer by running `peer logging getlevel <component-name>`.

- `--version`

  Use this flag to show detailed information about how the peer was built. This flag cannot be applied to `peer` subcommands or their options.

8.1.4 Usage

Here's some examples using the different available flags on the `peer` command.

- Using the `--help` flag on the `peer channel join` command.

```
peer channel join --help

Joins the peer to a channel.

Usage:
  peer channel join [flags]

Flags:
  -b, --blockpath string   Path to file containing genesis block

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded␣
↪X509 public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating␣
↪with the orderer endpoint
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides,␣
↪see core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
```

(continues on next page)

(continued from previous page)

```
      --tls                                    Use TLS when communicating with the␣
↪orderer endpoint
  -v, --version                                Display the build version for this␣
↪fabric peer
```

This shows brief help syntax for the `peer channel join` command.

- Using the `--version` flag on the `peer` command.

```
peer --version

peer:
 Version: 1.1.0-alpha
 Go version: go1.9.2
 OS/Arch: linux/amd64
 Experimental features: false
 Chaincode:
  Base Image Version: 0.4.5
  Base Docker Namespace: hyperledger
  Base Docker Label: org.hyperledger.fabric
  Docker Namespace: hyperledger
```

This shows that this peer was built using an alpha of Hyperledger Fabric version 1.1.0, compiled with GOLANG 1.9.2. It can be used on Linux operating systems with AMD64 compatible instruction sets.

8.2 peer chaincode

The `peer chaincode` command allows administrators to perform chaincode related operations on a peer, such as installing, instantiating, invoking, packaging, querying, and upgrading chaincode.

8.2.1 Syntax

The `peer chaincode` command has the following subcommands:

- install
- instantiate
- invoke
- list
- package
- query
- signpackage
- upgrade

The different subcommand options (install, instantiate...) relate to the different chaincode operations that are relevant to a peer. For example, use the `peer chaincode install` subcommand option to install a chaincode on a peer, or the `peer chaincode query` subcommand option to query a chaincode for the current value on a peer's ledger.

Each peer chaincode subcommand is described together with its options in its own section in this topic.

8.2.2 Flags

Each `peer chaincode` subcommand has both a set of flags specific to an individual subcommand, as well as a set of global flags that relate to all `peer chaincode` subcommands. Not all subcommands would use these flags. For instance, the `query` subcommand does not need the `--orderer` flag.

The individual flags are described with the relevant subcommand. The global flags are

- `--cafile <string>`

  Path to file containing PEM-encoded trusted certificate(s) for the ordering endpoint

- `--certfile <string>`

  Path to file containing PEM-encoded X509 public key to use for mutual TLS communication with the orderer endpoint

- `--keyfile <string>`

  Path to file containing PEM-encoded private key to use for mutual TLS communication with the orderer endpoint

- `-o` or `--orderer <string>`

  Ordering service endpoint specifed as `<hostname or IP address>:<port>`

- `--ordererTLSHostnameOverride <string>`

  The hostname override to use when validating the TLS connection to the orderer

- `--tls`

  Use TLS when communicating with the orderer endpoint

- `--transient <string>`

  Transient map of arguments in JSON encoding

- `--logging-level <string>`

  Default logging level and overrides, see `core.yaml` for full syntax

8.2.3 peer chaincode install

```
Package the specified chaincode into a deployment spec and save it on the peer's path.

Usage:
  peer chaincode install [flags]

Flags:
      --connectionProfile string       Connection profile that provides the necessary␣
↪connection information for the network. Note: currently only supported for␣
↪providing peer connection information
  -c, --ctor string                    Constructor message for the chaincode in JSON␣
↪format (default "{}")
  -h, --help                           help for install
  -l, --lang string                    Language the chaincode is written in (default
↪"golang")
  -n, --name string                    Name of the chaincode
  -p, --path string                    Path to chaincode
      --peerAddresses stringArray      The addresses of the peers to connect to
      --tlsRootCertFiles stringArray   If TLS is enabled, the paths to the TLS root␣
↪cert files of the peers to connect to. The order and number of certs specified␣
↪should match the --peerAddresses flag
```

(continues on next page)

(continued from previous page)

```
  -v, --version string                 Version of the chaincode specified in install/
↪instantiate/upgrade commands

Global Flags:
      --cafile string                        Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                      Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                           Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                 Timeout for client to connect (default 3s)
      --keyfile string                       Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                 Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                       Ordering service endpoint
      --ordererTLSHostnameOverride string    The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                  Use TLS when communicating with the␣
↪orderer endpoint
      --transient string                     Transient map of arguments in JSON␣
↪encoding
```

8.2.4 peer chaincode instantiate

```
Deploy the specified chaincode to the network.

Usage:
  peer chaincode instantiate [flags]

Flags:
  -C, --channelID string               The channel on which this command should be␣
↪executed
      --collections-config string      The fully qualified path to the collection␣
↪JSON file including the file name
      --connectionProfile string       Connection profile that provides the necessary␣
↪connection information for the network. Note: currently only supported for␣
↪providing peer connection information
  -c, --ctor string                    Constructor message for the chaincode in JSON␣
↪format (default "{}")
  -E, --escc string                    The name of the endorsement system chaincode␣
↪to be used for this chaincode
  -h, --help                           help for instantiate
  -l, --lang string                    Language the chaincode is written in (default
↪"golang")
  -n, --name string                    Name of the chaincode
      --peerAddresses stringArray      The addresses of the peers to connect to
  -P, --policy string                  The endorsement policy associated to this␣
↪chaincode
      --tlsRootCertFiles stringArray   If TLS is enabled, the paths to the TLS root␣
↪cert files of the peers to connect to. The order and number of certs specified␣
↪should match the --peerAddresses flag
  -v, --version string                 Version of the chaincode specified in install/
↪instantiate/upgrade commands
  -V, --vscc string                    The name of the verification system chaincode␣
↪to be used for this chaincode
```

(continues on next page)

(continued from previous page)

```
Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
      --transient string                    Transient map of arguments in JSON␣
↪encoding
```

8.2.5 peer chaincode invoke

```
Invoke the specified chaincode. It will try to commit the endorsed transaction to the␣
↪network.

Usage:
  peer chaincode invoke [flags]

Flags:
  -C, --channelID string               The channel on which this command should be␣
↪executed
      --connectionProfile string       Connection profile that provides the necessary␣
↪connection information for the network. Note: currently only supported for␣
↪providing peer connection information
  -c, --ctor string                    Constructor message for the chaincode in JSON␣
↪format (default "{}")
  -h, --help                           help for invoke
  -n, --name string                    Name of the chaincode
      --peerAddresses stringArray      The addresses of the peers to connect to
      --tlsRootCertFiles stringArray   If TLS is enabled, the paths to the TLS root␣
↪cert files of the peers to connect to. The order and number of certs specified␣
↪should match the --peerAddresses flag
      --waitForEvent                   Whether to wait for the event from each peer's␣
↪deliver filtered service signifying that the 'invoke' transaction has been␣
↪committed successfully
      --waitForEventTimeout duration   Time to wait for the event from each peer's␣
↪deliver filtered service signifying that the 'invoke' transaction has been␣
↪committed successfully (default 30s)

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
```

(continues on next page)

(continued from previous page)

```
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
      --transient string                    Transient map of arguments in JSON␣
↪encoding
```

8.2.6 peer chaincode list

```
Get the instantiated chaincodes in the channel if specify channel, or get installed␣
↪chaincodes on the peer

Usage:
  peer chaincode list [flags]

Flags:
  -C, --channelID string               The channel on which this command should be␣
↪executed
      --connectionProfile string       Connection profile that provides the necessary␣
↪connection information for the network. Note: currently only supported for␣
↪providing peer connection information
  -h, --help                           help for list
      --installed                      Get the installed chaincodes on a peer
      --instantiated                   Get the instantiated chaincodes on a channel
      --peerAddresses stringArray      The addresses of the peers to connect to
      --tlsRootCertFiles stringArray   If TLS is enabled, the paths to the TLS root␣
↪cert files of the peers to connect to. The order and number of certs specified␣
↪should match the --peerAddresses flag

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
      --transient string                    Transient map of arguments in JSON␣
↪encoding
```

(continues on next page)

(continued from previous page)

8.2.7 peer chaincode package

```
Package the specified chaincode into a deployment spec.

Usage:
  peer chaincode package [flags]

Flags:
  -s, --cc-package                  create CC deployment spec for owner endorsements␣
↪instead of raw CC deployment spec
  -c, --ctor string                 Constructor message for the chaincode in JSON␣
↪format (default "{}")
  -h, --help                        help for package
  -i, --instantiate-policy string   instantiation policy for the chaincode
  -l, --lang string                 Language the chaincode is written in (default
↪"golang")
  -n, --name string                 Name of the chaincode
  -p, --path string                 Path to chaincode
  -S, --sign                        if creating CC deployment spec package for owner␣
↪endorsements, also sign it with local MSP
  -v, --version string              Version of the chaincode specified in install/
↪instantiate/upgrade commands

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
      --transient string                    Transient map of arguments in JSON␣
↪encoding
```

8.2.8 peer chaincode query

```
Get endorsed result of chaincode function call and print it. It won't generate␣
↪transaction.

Usage:
  peer chaincode query [flags]
```

(continues on next page)

(continued from previous page)

```
Flags:
  -C, --channelID string               The channel on which this command should be␣
↪executed
      --connectionProfile string       Connection profile that provides the necessary␣
↪connection information for the network. Note: currently only supported for␣
↪providing peer connection information
  -c, --ctor string                    Constructor message for the chaincode in JSON␣
↪format (default "{}")
  -h, --help                           help for query
  -x, --hex                            If true, output the query value byte array in␣
↪hexadecimal. Incompatible with --raw
  -n, --name string                    Name of the chaincode
      --peerAddresses stringArray      The addresses of the peers to connect to
  -r, --raw                            If true, output the query value as raw bytes,␣
↪otherwise format as a printable string
      --tlsRootCertFiles stringArray   If TLS is enabled, the paths to the TLS root␣
↪cert files of the peers to connect to. The order and number of certs specified␣
↪should match the --peerAddresses flag

Global Flags:
      --cafile string                        Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                      Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                           Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                 Timeout for client to connect (default 3s)
      --keyfile string                       Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                 Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                       Ordering service endpoint
      --ordererTLSHostnameOverride string    The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                  Use TLS when communicating with the␣
↪orderer endpoint
      --transient string                     Transient map of arguments in JSON␣
↪encoding
```

8.2.9 peer chaincode signpackage

```
Sign the specified chaincode package

Usage:
  peer chaincode signpackage [flags]

Flags:
  -h, --help   help for signpackage

Global Flags:
      --cafile string                        Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                      Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                           Use mutual TLS when communicating with␣
↪the orderer endpoint
```

(continues on next page)

(continued from previous page)

```
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
      --transient string                    Transient map of arguments in JSON␣
↪encoding
```

8.2.10 peer chaincode upgrade

```
Upgrade an existing chaincode with the specified one. The new chaincode will␣
↪immediately replace the existing chaincode upon the transaction committed.

Usage:
  peer chaincode upgrade [flags]

Flags:
  -C, --channelID string               The channel on which this command should be␣
↪executed
      --collections-config string      The fully qualified path to the collection␣
↪JSON file including the file name
      --connectionProfile string       Connection profile that provides the necessary␣
↪connection information for the network. Note: currently only supported for␣
↪providing peer connection information
  -c, --ctor string                    Constructor message for the chaincode in JSON␣
↪format (default "{}")
  -E, --escc string                    The name of the endorsement system chaincode␣
↪to be used for this chaincode
  -h, --help                           help for upgrade
  -l, --lang string                    Language the chaincode is written in (default
↪"golang")
  -n, --name string                    Name of the chaincode
  -p, --path string                    Path to chaincode
      --peerAddresses stringArray      The addresses of the peers to connect to
  -P, --policy string                  The endorsement policy associated to this␣
↪chaincode
      --tlsRootCertFiles stringArray   If TLS is enabled, the paths to the TLS root␣
↪cert files of the peers to connect to. The order and number of certs specified␣
↪should match the --peerAddresses flag
  -v, --version string                 Version of the chaincode specified in install/
↪instantiate/upgrade commands
  -V, --vscc string                    The name of the verification system chaincode␣
↪to be used for this chaincode

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
```

(continues on next page)

(continued from previous page)

```
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
      --transient string                    Transient map of arguments in JSON␣
↪encoding
```

8.2.11 Example Usage

peer chaincode instantiate examples

Here are some examples of the `peer chaincode instantiate` command, which instantiates the chaincode named `mycc` at version `1.0` on channel `mychannel`:

- Using the `--tls` and `--cafile` global flags to instantiate the chaincode in a network with TLS enabled:

```
export ORDERER_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/
↪tlsca.example.com-cert.pem
peer chaincode instantiate -o orderer.example.com:7050 --tls --cafile $ORDERER_CA␣
↪-C mychannel -n mycc -v 1.0 -c '{"Args":["init","a","100","b","200"]}' -P "AND (
↪'Org1MSP.peer','Org2MSP.peer')"

2018-02-22 16:33:53.324 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 001␣
↪Using default escc
2018-02-22 16:33:53.324 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 002␣
↪Using default vscc
2018-02-22 16:34:08.698 UTC [main] main -> INFO 003 Exiting.....
```

- Using only the command-specific options to instantiate the chaincode in a network with TLS disabled:

```
peer chaincode instantiate -o orderer.example.com:7050 -C mychannel -n mycc -v 1.
↪0 -c '{"Args":["init","a","100","b","200"]}' -P "AND ('Org1MSP.peer','Org2MSP.
↪peer')"


2018-02-22 16:34:09.324 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 001␣
↪Using default escc
2018-02-22 16:34:09.324 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 002␣
↪Using default vscc
2018-02-22 16:34:24.698 UTC [main] main -> INFO 003 Exiting.....
```

peer chaincode invoke example

Here is an example of the `peer chaincode invoke` command:

- Invoke the chaincode named `mycc` at version `1.0` on channel `mychannel` on `peer0.org1.example.com:7051` and `peer0.org2.example.com:7051` (the peers defined by `--peerAddresses`), requesting to move 10 units from variable `a` to variable `b`:

```
peer chaincode invoke -o orderer.example.com:7050 -C mychannel -n mycc --
↪peerAddresses peer0.org1.example.com:7051 --peerAddresses peer0.org2.example.
↪com:7051 -c '{"Args":["invoke","a","b","10"]}'

2018-02-22 16:34:27.069 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 001␣
↪Using default escc
2018-02-22 16:34:27.069 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 002␣
↪Using default vscc
.
.
.
2018-02-22 16:34:27.106 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> DEBU 00a␣
↪ESCC invoke result: version:1 response:<status:200 message:"OK" > payload:"\n␣
↪\237mM\376? [\214\002 \332\204\035\275q\227\2132A\n\204&\2106\037W|\346
↪#\3413\274\022Y\nE\022\024\n\004lscc\022\014\n\n\n\004mycc\022\002\010\003\022-
↪\n\004mycc\022
↪%\n\007\n\001a\022\002\010\003\n\007\n\001b\022\002\010\003\032\007\n\001a\032\00290\032\010\n
↪"\013\022\004mycc\032\0031.0" endorsement:<endorser:"\n\007Org1MSP\022\262\006--
↪---BEGIN CERTIFICATE-----\nMIICLjCCAdWgAwIBAgIRAJYomxY2cqHA/fbRnH5a/
↪bwwCgYIKoZIzj0EAwIwczEL\nMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExFjAUBgNVBAcTDVNhbiBG\ncmF
↪/7JFDHATJXtLgJhkK5KosDdHuKLYbCqvge\n46u3AC16MZyJRvKBiw6jTTBLMA4GA1UdDwEB/
↪wQEAwIHgDAMBgNVHRMBAf8EAjAA\nMCsGA1UdIwQkMCKAIN7dJR9dimkFtkus0R5pAOlRz5SA3FB5t8Eaxl9A7lkgMAoG\
↪Xj3C8lA==\n-----END CERTIFICATE-----\n" signature:"0D\002 \022_
↪\342\350\344\231G&
↪\237\n\244\375\302J\220l\302\345\210\335D\250y\253P\0214:\221e\332@\002␣
↪\000\254\361\224\247\210\214L\277\370\222\213\217\301\r\341v\227\265\277\336\256^
↪\217\336\005y*\321\023\025\367" >
2018-02-22 16:34:27.107 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 00b␣
↪Chaincode invoke successful. result: status:200
2018-02-22 16:34:27.107 UTC [main] main -> INFO 00c Exiting.....
```

Here you can see that the invoke was submitted successfully based on the log message:

```
2018-02-22 16:34:27.107 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 00b␣
↪Chaincode invoke successful. result: status:200
```

A successful response indicates that the transaction was submitted for ordering successfully. The transaction will then be added to a block and, finally, validated or invalidated by each peer on the channel.

peer chaincode list example

Here are some examples of the `peer chaincode list` command:

- Using the `--installed` flag to list the chaincodes installed on a peer.

```
peer chaincode list --installed

Get installed chaincodes on peer:
Name: mycc, Version: 1.0, Path: github.com/hyperledger/fabric/examples/chaincode/
↪go/chaincode_example02, Id:␣
↪8cc2730fdafd0b28ef734eac12b29df5fc98ad98bdb1b7e0ef96265c3d893d61
2018-02-22 17:07:13.476 UTC [main] main -> INFO 001 Exiting.....
```

You can see that the peer has installed a chaincode called `mycc` which is at version `1.0`.

- Using the `--instantiated` in combination with the `-C` (channel ID) flag to list the chaincodes instantiated on a channel.

```
peer chaincode list --instantiated -C mychannel

Get instantiated chaincodes on channel mychannel:
Name: mycc, Version: 1.0, Path: github.com/hyperledger/fabric/examples/chaincode/
↪go/chaincode_example02, Escc: escc, Vscc: vscc
2018-02-22 17:07:42.969 UTC [main] main -> INFO 001 Exiting.....
```

You can see that chaincode `mycc` at version `1.0` is instantiated on channel `mychannel`.

peer chaincode package example

Here is an example of the `peer chaincode package` command, which packages the chaincode named `mycc` at version `1.1`, creates the chaincode deployment spec, signs the package using the local MSP, and outputs it as `ccpack.out`:

```
  peer chaincode package ccpack.out -n mycc -p github.com/hyperledger/fabric/examples/
↪chaincode/go/chaincode_example02 -v 1.1 -s -S
  .
  .
  .
  2018-02-22 17:27:01.404 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 003␣
↪Using default escc
  2018-02-22 17:27:01.405 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 004␣
↪Using default vscc
  .
  .
  .
  2018-02-22 17:27:01.879 UTC [chaincodeCmd] chaincodePackage -> DEBU 011 Packaged␣
↪chaincode into deployment spec of size <3426>, with args = [ccpack.out]
  2018-02-22 17:27:01.879 UTC [main] main -> INFO 012 Exiting.....
```

peer chaincode query example

Here is an example of the `peer chaincode query` command, which queries the peer ledger for the chaincode named `mycc` at version `1.0` for the value of variable `a`:

- You can see from the output that variable `a` had a value of 90 at the time of the query.

```
peer chaincode query -C mychannel -n mycc -c '{"Args":["query","a"]}'

2018-02-22 16:34:30.816 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 001␣
↪Using default escc
2018-02-22 16:34:30.816 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 002␣
↪Using default vscc
Query Result: 90
```

peer chaincode signpackage example

Here is an example of the `peer chaincode signpackage` command, which accepts an existing signed package and creates a new one with signature of the local MSP appended to it.

```
peer chaincode signpackage ccwith1sig.pak ccwith2sig.pak
Wrote signed package to ccwith2sig.pak successfully
2018-02-24 19:32:47.189 EST [main] main -> INFO 002 Exiting.....
```

peer chaincode upgrade example

Here is an example of the `peer chaincode upgrade` command, which upgrades the chaincode named `mycc` at version `1.0` on channel `mychannel` to version `1.1`, which contains a new variable `c`:

- Using the `--tls` and `--cafile` global flags to upgrade the chaincode in a network with TLS enabled:

```
export ORDERER_CA=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/
↪tlsca.example.com-cert.pem
peer chaincode upgrade -o orderer.example.com:7050 --tls --cafile $ORDERER_CA -C␣
↪mychannel -n mycc -v 1.2 -c '{"Args":["init","a","100","b","200","c","300"]}' -
↪P "AND ('Org1MSP.peer','Org2MSP.peer')"
.
.
.
2018-02-22 18:26:31.433 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 003␣
↪Using default escc
2018-02-22 18:26:31.434 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 004␣
↪Using default vscc
2018-02-22 18:26:31.435 UTC [chaincodeCmd] getChaincodeSpec -> DEBU 005 java␣
↪chaincode enabled
2018-02-22 18:26:31.435 UTC [chaincodeCmd] upgrade -> DEBU 006 Get upgrade␣
↪proposal for chaincode <name:"mycc" version:"1.1" >
.
.
.
2018-02-22 18:26:46.687 UTC [chaincodeCmd] upgrade -> DEBU 009 endorse upgrade␣
↪proposal, get response <status:200 message:"OK" payload:"\n\004mycc\022\0031.
↪1\032\004escc\"\004vscc*,
↪\022\014\022\n\010\001\022\002\010\000\022\002\010\001\032\r\022\013\n\007Org1MSP\020\003\032\
↪\261g(^
↪v\021\220\240\332\251\014\204V\210P\310o\231\271\036\301\022\032\205fC[|=\215\372\223\022␣
↪\311b\025?
↪\323N\343\325\032\005\365\236\001XKj\004E\351\007\247\265fu\305j\367\331\275\253\307R\032␣
↪\014H#\014\272!#\345\306s\323\371\350\364\006.
↪\000\356\230\353\270\263\215\217\303\256\220i^\277\305\214: \375\200zY\275\203}
↪\375\244\205\035\340\226]l!uE\334\273\214\214\020\303\3474\360\014\234-
↪\006\315B\031\022\010\022\006\010\001\022\002\010\000\032\r\022\013\n\007Org1MSP\020\001
↪" >
.
.
.
2018-02-22 18:26:46.693 UTC [chaincodeCmd] upgrade -> DEBU 00c Get Signed envelope
2018-02-22 18:26:46.693 UTC [chaincodeCmd] chaincodeUpgrade -> DEBU 00d Send␣
↪signed envelope to orderer
2018-02-22 18:26:46.908 UTC [main] main -> INFO 00e Exiting.....
```

- Using only the command-specific options to upgrade the chaincode in a network with TLS disabled:

```
peer chaincode upgrade -o orderer.example.com:7050 -C mychannel -n mycc -v 1.2 -c
↪'{"Args":["init","a","100","b","200","c","300"]}' -P "AND ('Org1MSP.peer',
↪'Org2MSP.peer')"
```

(continues on next page)

(continued from previous page)

```
.
.
.
2018-02-22 18:28:31.433 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 003␣
↪Using default escc
2018-02-22 18:28:31.434 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 004␣
↪Using default vscc
2018-02-22 18:28:31.435 UTC [chaincodeCmd] getChaincodeSpec -> DEBU 005 java␣
↪chaincode enabled
2018-02-22 18:28:31.435 UTC [chaincodeCmd] upgrade -> DEBU 006 Get upgrade␣
↪proposal for chaincode <name:"mycc" version:"1.1" >
.
.
.
2018-02-22 18:28:46.687 UTC [chaincodeCmd] upgrade -> DEBU 009 endorse upgrade␣
↪proposal, get response <status:200 message:"OK" payload:"\n\004mycc\022\0031.
↪1\032\004escc\"\004vscc*,
↪\022\014\022\n\010\001\022\002\010\000\022\002\010\001\032\r\022\013\n\007Org1MSP\020\003\032\
↪\261g(^
↪v\021\220\240\332\251\014\204V\210P\310o\231\271\036\301\022\032\205fC[|=\215\372\223\022␣
↪\311b\025?
↪\323N\343\325\032\005\365\236\001XKj\004E\351\007\247\265fu\305j\367\331\275\253\307R\032␣
↪\014H#\014\272!#\345\306s\323\371\350\364\006.
↪\000\356\230\353\270\263\215\217\303\256\220i^\277\305\214: \375\200zY\275\203}
↪\375\244\205\035\340\226]l!uE\334\273\214\214\020\303\3474\360\014\234-
↪\006\315B\031\022\010\022\006\010\001\022\002\010\000\032\r\022\013\n\007Org1MSP\020\001
↪" >
.
.
.
2018-02-22 18:28:46.693 UTC [chaincodeCmd] upgrade -> DEBU 00c Get Signed envelope
2018-02-22 18:28:46.693 UTC [chaincodeCmd] chaincodeUpgrade -> DEBU 00d Send␣
↪signed envelope to orderer
2018-02-22 18:28:46.908 UTC [main] main -> INFO 00e Exiting.....
```


8.3 peer channel

The `peer channel` command allows administrators to perform channel related operations on a peer, such as joining a channel or listing the channels to which a peer is joined.

8.3.1 Syntax

The `peer channel` command has the following subcommands:

- create
- fetch
- getinfo
- join
- list

- signconfigtx
- update

8.3.2 peer channel

```
Operate a channel: create|fetch|join|list|update|signconfigtx|getinfo.

Usage:
  peer channel [command]

Available Commands:
  create       Create a channel
  fetch        Fetch a block
  getinfo      get blockchain information of a specified channel.
  join         Joins the peer to a channel.
  list         List of channels peer has joined.
  signconfigtx Signs a configtx update.
  update       Send a configtx update.

Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
  -h, --help                                help for channel
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint

Global Flags:
      --logging-level string   Default logging level and overrides, see core.yaml for␣
↪full syntax

Use "peer channel [command] --help" for more information about a command.
```

8.3.3 peer channel create

```
Create a channel and write the genesis block to a file.

Usage:
  peer channel create [flags]

Flags:
  -c, --channelID string     In case of a newChain command, the channel ID to create.␣
↪It must be all lower case, less than 250 characters long and match the regular␣
↪expression: [a-z][a-z0-9.-]*
  -f, --file string          Configuration transaction file generated by a tool such␣
↪as configtxgen for submitting to orderer
```

(continues on next page)

(continued from previous page)

```
  -h, --help                 help for create
      --outputBlock string   The path to write the genesis block for the channel.␣
↪(default ./<channelID>.block)
  -t, --timeout duration     Channel creation timeout (default 5s)

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
```

8.3.4 peer channel fetch

```
Fetch a specified block, writing it to a file.

Usage:
  peer channel fetch <newest|oldest|config|(number)> [outputfile] [flags]

Flags:
  -c, --channelID string   In case of a newChain command, the channel ID to create.␣
↪It must be all lower case, less than 250 characters long and match the regular␣
↪expression: [a-z][a-z0-9.-]*
  -h, --help               help for fetch

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
```

8.3.5 peer channel getinfo

```
get blockchain information of a specified channel. Requires '-c'.

Usage:
  peer channel getinfo [flags]

Flags:
  -c, --channelID string   In case of a newChain command, the channel ID to create.␣
↪It must be all lower case, less than 250 characters long and match the regular␣
↪expression: [a-z][a-z0-9.-]*
  -h, --help               help for getinfo

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
```

8.3.6 peer channel join

```
Joins the peer to a channel.

Usage:
  peer channel join [flags]

Flags:
  -b, --blockpath string   Path to file containing genesis block
  -h, --help               help for join

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
```

(continues on next page)

(continued from previous page)

```
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
```

8.3.7 peer channel list

```
List of channels peer has joined.

Usage:
  peer channel list [flags]

Flags:
  -h, --help   help for list

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
      --keyfile string                      Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                      Ordering service endpoint
      --ordererTLSHostnameOverride string   The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                 Use TLS when communicating with the␣
↪orderer endpoint
```

8.3.8 peer channel signconfigtx

```
Signs the supplied configtx update file in place on the filesystem. Requires '-f'.

Usage:
  peer channel signconfigtx [flags]

Flags:
  -f, --file string   Configuration transaction file generated by a tool such as␣
↪configtxgen for submitting to orderer
  -h, --help          help for signconfigtx

Global Flags:
      --cafile string                       Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                     Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                          Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                Timeout for client to connect (default 3s)
```

(continues on next page)

(continued from previous page)

```
      --keyfile string                       Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                 Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                       Ordering service endpoint
      --ordererTLSHostnameOverride string    The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                  Use TLS when communicating with the␣
↪orderer endpoint
```

8.3.9 peer channel update

```
Signs and sends the supplied configtx update file to the channel. Requires '-f', '-o',
↪ '-c'.

Usage:
  peer channel update [flags]

Flags:
  -c, --channelID string   In case of a newChain command, the channel ID to create.␣
↪It must be all lower case, less than 250 characters long and match the regular␣
↪expression: [a-z][a-z0-9.-]*
  -f, --file string        Configuration transaction file generated by a tool such as␣
↪configtxgen for submitting to orderer
  -h, --help               help for update

Global Flags:
      --cafile string                        Path to file containing PEM-encoded␣
↪trusted certificate(s) for the ordering endpoint
      --certfile string                      Path to file containing PEM-encoded X509␣
↪public key to use for mutual TLS communication with the orderer endpoint
      --clientauth                           Use mutual TLS when communicating with␣
↪the orderer endpoint
      --connTimeout duration                 Timeout for client to connect (default 3s)
      --keyfile string                       Path to file containing PEM-encoded␣
↪private key to use for mutual TLS communication with the orderer endpoint
      --logging-level string                 Default logging level and overrides, see␣
↪core.yaml for full syntax
  -o, --orderer string                       Ordering service endpoint
      --ordererTLSHostnameOverride string    The hostname override to use when␣
↪validating the TLS connection to the orderer.
      --tls                                  Use TLS when communicating with the␣
↪orderer endpoint
```

8.3.10 Example Usage

peer channel create examples

Here's an example that uses the `--orderer` global flag on the `peer channel create` command.

- Create a sample channel `mychannel` defined by the configuration transaction contained in file `./createchannel.txn`. Use the orderer at `orderer.example.com:7050`.

```
peer channel create -c mychannel -f ./createchannel.txn --orderer orderer.example.
↪com:7050

2018-02-25 08:23:57.548 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and␣
↪orderer connections initialized
2018-02-25 08:23:57.626 UTC [channelCmd] InitCmdFactory -> INFO 019 Endorser and␣
↪orderer connections initialized
2018-02-25 08:23:57.834 UTC [channelCmd] readBlock -> INFO 020 Received block: 0
2018-02-25 08:23:57.835 UTC [main] main -> INFO 021 Exiting.....
```

Block 0 is returned indicating that the channel has been successfully created.

Here's an example of the `peer channel create` command option.

- Create a new channel `mychannel` for the network, using the orderer at ip address `orderer.example.com:7050`. The configuration update transaction required to create this channel is defined the file `./createchannel.txn`. Wait 30 seconds for the channel to be created.

```
  peer channel create -c mychannel --orderer orderer.example.com:7050 -f ./
↪createchannel.txn -t 30s

  2018-02-23 06:31:58.568 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser␣
↪and orderer connections initialized
  2018-02-23 06:31:58.669 UTC [channelCmd] InitCmdFactory -> INFO 019 Endorser␣
↪and orderer connections initialized
  2018-02-23 06:31:58.877 UTC [channelCmd] readBlock -> INFO 020 Received block: 0
  2018-02-23 06:31:58.878 UTC [main] main -> INFO 021 Exiting.....

  ls -l

  -rw-r--r-- 1 root root 11982 Feb 25 12:24 mychannel.block
```

You can see that channel `mychannel` has been successfully created, as indicated in the output where block 0 (zero) is added to the blockchain for this channel and returned to the peer, where it is stored in the local directory as `mychannel.block`.

Block zero is often called the *genesis block* as it provides the starting configuration for the channel. All subsequent updates to the channel will be captured as configuration blocks on the channel's blockchain, each of which supersedes the previous configuration.

peer channel fetch example

Here's some examples of the `peer channel fetch` command.

- Using the `newest` option to retrieve the most recent channel block, and store it in the file `mychannel.block`.

```
peer channel fetch newest mychannel.block -c mychannel --orderer orderer.example.
↪com:7050

2018-02-25 13:10:16.137 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and␣
↪orderer connections initialized
2018-02-25 13:10:16.144 UTC [channelCmd] readBlock -> INFO 00a Received block: 32
2018-02-25 13:10:16.145 UTC [main] main -> INFO 00b Exiting.....

ls -l

-rw-r--r-- 1 root root 11982 Feb 25 13:10 mychannel.block
```

You can see that the retrieved block is number 32, and that the information has been written to the file `mychannel.block`.

- Using the `(block number)` option to retrieve a specific block – in this case, block number 16 – and store it in the default block file.

```
peer channel fetch 16  -c mychannel --orderer orderer.example.com:7050

2018-02-25 13:46:50.296 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and␣
↪orderer connections initialized
2018-02-25 13:46:50.302 UTC [channelCmd] readBlock -> INFO 00a Received block: 16
2018-02-25 13:46:50.302 UTC [main] main -> INFO 00b Exiting.....

ls -l

-rw-r--r-- 1 root root 11982 Feb 25 13:10 mychannel.block
-rw-r--r-- 1 root root  4783 Feb 25 13:46 mychannel_16.block
```

You can see that the retrieved block is number 16, and that the information has been written to the default file `mychannel_16.block`.

For configuration blocks, the block file can be decoded using the `configtxlator` command. See this command for an example of decoded output. User transaction blocks can also be decoded, but a user program must be written to do this.

peer channel getinfo example

Here's an example of the `peer channel getinfo` command.

- Get information about the local peer for channel `mychannel`.

```
peer channel getinfo -c mychannel

2018-02-25 15:15:44.135 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and␣
↪orderer connections initialized
Blockchain info: {"height":5,"currentBlockHash":"JgK9lcaPUNmFb5Mp1qe1SVMsx3o/
↪22Ct4+n5tejcXCw=","previousBlockHash":
↪"f81ZXoAn3gF86zrFq7L1DzW2aKuabH9Ow6SIE5Y04a4="}
2018-02-25 15:15:44.139 UTC [main] main -> INFO 006 Exiting.....
```

You can see that the latest block for channel `mychannel` is block 5. You can also see the crytographic hashes for the most recent blocks in the channel's blockchain.

peer channel join example

Here's an example of the `peer channel join` command.

- Join a peer to the channel defined in the genesis block identified by the file `./mychannel.genesis.block`. In this example, the channel block was previously retrieved by the `peer channel fetch` command.

```
peer channel join -b ./mychannel.genesis.block

2018-02-25 12:25:26.511 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and␣
↪orderer connections initialized
2018-02-25 12:25:26.571 UTC [channelCmd] executeJoin -> INFO 006 Successfully␣
↪submitted proposal to join channel
2018-02-25 12:25:26.571 UTC [main] main -> INFO 007 Exiting.....
```

You can see that the peer has successfully made a request to join the channel.

peer channel list example

Here's an example of the `peer channel list` command.

- List the channels to which a peer is joined.

```
peer channel list

2018-02-25 14:21:20.361 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and␣
↪orderer connections initialized
Channels peers has joined:
mychannel
2018-02-25 14:21:20.372 UTC [main] main -> INFO 006 Exiting.....
```

You can see that the peer is joined to channel `mychannel`.

peer channel signconfigtx example

Here's an example of the `peer channel signconfigtx` command.

- Sign the `channel update` transaction defined in the file `./updatechannel.txn`. The example lists the configuration transaction file before and after the command.

```
ls -l

-rw-r--r--  1 anthonyodowd  staff   284 25 Feb 18:16 updatechannel.tx

peer channel signconfigtx -f updatechannel.tx

2018-02-25 18:16:44.456 GMT [channelCmd] InitCmdFactory -> INFO 001 Endorser and␣
↪orderer connections initialized
2018-02-25 18:16:44.459 GMT [main] main -> INFO 002 Exiting.....

ls -l

-rw-r--r--  1 anthonyodowd  staff  2180 25 Feb 18:16 updatechannel.tx
```

You can see that the peer has successfully signed the configuration transaction by the increase in the size of the file `updatechannel.tx` from 284 bytes to 2180 bytes.

peer channel update example

Here's an example of the `peer channel update` command.

- Update the channel `mychannel` using the configuration transaction defined in the file `./updatechannel.txn`. Use the orderer at ip address `orderer.example.com:7050` to send the configuration transaction to all peers in the channel to update their copy of the channel configuration.

```
peer channel update -c mychannel -f ./updatechannel.txn -o orderer.example.
↪com:7050

2018-02-23 06:32:11.569 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and␣
↪orderer connections initialized
2018-02-23 06:32:11.626 UTC [main] main -> INFO 010 Exiting.....
```

At this point, the channel `mychannel` has been successfully updated.

8.4 peer version

The `peer version` command displays the version information of the peer. It displays version, Go version, OS/architecture, if experimental features are turned on, and chaincode information. For example:

```
peer:
  Version: 1.1.0-beta-snapshot-a6c3447e
  Go version: go1.9.2
  OS/Arch: linux/amd64
  Experimental features: true
  Chaincode:
   Base Image Version: 0.4.5
   Base Docker Namespace: hyperledger
   Base Docker Label: org.hyperledger.fabric
   Docker Namespace: hyperledger
```

8.4.1 Syntax

```
Print current version of the fabric peer server.

Usage:
  peer version [flags]

Flags:
  -h, --help   help for version

Global Flags:
      --logging-level string   Default logging level and overrides, see core.yaml for␣
↪full syntax
```


8.5 peer logging

The `peer logging` subcommand allows administrators to dynamically view and configure the log levels of a peer.

8.5.1 Syntax

The `peer logging` command has the following subcommands:

- getlevel
- setlevel
- revertlevels

The different subcommand options (getlevel, setlevel, and revertlevels) relate to the different logging operations that are relevant to a peer.

Each peer logging subcommand is described together with its options in its own section in this topic.

8.5.2 peer logging

```
Log levels: getlevel|setlevel|revertlevels.

Usage:
  peer logging [command]

Available Commands:
  getlevel     Returns the logging level of the requested module logger.
  revertlevels Reverts the logging levels to the levels at the end of peer startup.
  setlevel     Sets the logging level for all modules that match the regular␣
↪expression.

Flags:
  -h, --help   help for logging

Global Flags:
      --logging-level string   Default logging level and overrides, see core.yaml for␣
↪full syntax

Use "peer logging [command] --help" for more information about a command.
```

8.5.3 peer logging getlevel

```
Returns the logging level of the requested module logger. Note: the module name␣
↪should exactly match the name that is displayed in the logs.

Usage:
  peer logging getlevel <module> [flags]

Flags:
  -h, --help   help for getlevel

Global Flags:
      --logging-level string   Default logging level and overrides, see core.yaml for␣
↪full syntax
```

8.5.4 peer logging revertlevels

```
Reverts the logging levels to the levels at the end of peer startup

Usage:
  peer logging revertlevels [flags]

Flags:
  -h, --help   help for revertlevels

Global Flags:
      --logging-level string   Default logging level and overrides, see core.yaml for␣
↪full syntax
```

8.5.5 peer logging setlevel

```
Sets the logging level for all modules that match the regular expression.

Usage:
  peer logging setlevel <module regular expression> <log level> [flags]

Flags:
  -h, --help   help for setlevel

Global Flags:
      --logging-level string   Default logging level and overrides, see core.yaml for␣
↪full syntax
```

8.5.6 Example Usage

peer logging getlevel example

Here is an example of the `peer logging getlevel` command:

- To get the log level for module `peer`:

```
peer logging getlevel peer

2018-02-22 19:10:08.633 UTC [cli/logging] getLevel -> INFO 001 Current log level␣
↪for peer module 'peer': DEBUG
2018-02-22 19:10:08.633 UTC [main] main -> INFO 002 Exiting.....
```

Set Level Usage

Here are some examples of the `peer logging setlevel` command:

- To set the log level for modules matching the regular expression `peer` to log level `WARNING`:

```
peer logging setlevel peer warning
2018-02-22 19:14:51.217 UTC [cli/logging] setLevel -> INFO 001 Log level set for␣
↪peer modules matching regular expression 'peer': WARNING
2018-02-22 19:14:51.217 UTC [main] main -> INFO 002 Exiting.....
```

- To set the log level for modules that match the regular expression `^gossip` (i.e. all of the `gossip` logging submodules of the form `gossip/<submodule>`) to log level `ERROR`:

```
peer logging setlevel ^gossip error

2018-02-22 19:16:46.272 UTC [cli/logging] setLevel -> INFO 001 Log level set for␣
↪peer modules matching regular expression '^gossip': ERROR
2018-02-22 19:16:46.272 UTC [main] main -> INFO 002 Exiting.....
```

Revert Levels Usage

Here is an example of the `peer logging revertlevels` command:

- To revert the log levels to the start-up values:

```
peer logging revertlevels

2018-02-22 19:18:38.428 UTC [cli/logging] revertLevels -> INFO 001 Log levels␣
↪reverted to the levels at the end of peer startup.
2018-02-22 19:18:38.428 UTC [main] main -> INFO 002 Exiting.....
```


8.6 peer node

The `peer node` command allows an administrator to start a peer node or check the status of a peer node.

8.6.1 Syntax

The `peer node` command has the following subcommands:

- start
- status

8.6.2 peer node start

```
Starts a node that interacts with the network.

Usage:
  peer node start [flags]

Flags:
  -h, --help                help for start
  -o, --orderer string      Ordering service endpoint (default "orderer:7050")
      --peer-chaincodedev   Whether peer in chaincode development mode

Global Flags:
      --logging-level string   Default logging level and overrides, see core.yaml for␣
↪full syntax
```

8.6.3 peer node status

```
Returns the status of the running node.

Usage:
  peer node status [flags]

Flags:
  -h, --help   help for status

Global Flags:
      --logging-level string   Default logging level and overrides, see core.yaml for␣
↪full syntax
```

8.6.4 Example Usage

peer node start example

The following command:

```
peer node start --peer-chaincodedev
```

starts a peer node in chaincode development mode. Normally chaincode containers are started and maintained by peer. However in chaincode development mode, chaincode is built and started by the user. This mode is useful during chaincode development phase for iterative development. See more information on development mode in the chaincode tutorial.

8.7 configtxgen

The `configtxgen` command allows users to create and inspect channel config related artifacts. The content of the generated artifacts is dictated by the contents of `configtx.yaml`.

8.7.1 Syntax

The `configtxgen` tool has no sub-commands, but supports flags which can be set to accomplish a number of tasks.

8.7.2 configtxgen

```
Usage of configtxgen:
  -asOrg string
        Performs the config generation as a particular organization (by name), only␣
↪including values in the write set that org (likely) has privilege to set
  -channelID string
        The channel ID to use in the configtx
  -configPath string
        The path containing the configuration to use (if set)
  -inspectBlock string
        Prints the configuration contained in the block at the specified path
  -inspectChannelCreateTx string
        Prints the configuration contained in the transaction at the specified path
  -outputAnchorPeersUpdate string
        Creates an config update to update an anchor peer (works only with the␣
↪default channel creation, and only for the first update)
  -outputBlock string
        The path to write the genesis block to (if set)
  -outputCreateChannelTx string
        The path to write a channel creation configtx to (if set)
  -printOrg string
        Prints the definition of an organization as JSON. (useful for adding an org␣
↪to a channel manually)
  -profile string
        The profile from configtx.yaml to use for generation. (default
↪"SampleInsecureSolo")
  -version
        Show version information
```

8.7.3 Usage

Output a genesis block

Write a genesis block to `genesis_block.pb` for channel `orderer-system-channel` for profile `SampleSingleMSPSoloV1_1`.

```
configtxgen -outputBlock genesis_block.pb -profile SampleSingleMSPSoloV1_1 -channelID␣
↪orderer-system-channel
```

Output a channel creation tx

Write a channel creation transaction to `create_chan_tx.pb` for profile `SampleSingleMSPChannelV1_1`.

```
configtxgen -outputCreateChannelTx create_chan_tx.pb -profile␣
↪SampleSingleMSPChannelV1_1 -channelID application-channel-1
```

Inspect a genesis block

Print the contents of a genesis block named `genesis_block.pb` to the screen as JSON.

```
configtxgen -inspectBlock genesis_block.pb
```

Inspect a channel creation tx

Print the contents of a channel creation tx named `create_chan_tx.pb` to the screen as JSON.

```
configtxgen -inspectChannelCreateTx create_chan_tx.pb
```

Print an organization definition

Construct an organization definition based on the parameters such as MSPDir from `configtx.yaml` and print it as JSON to the screen. (This output is useful for channel reconfiguration workflows, such as adding a member).

```
configtxgen -printOrg Org1
```

Output anchor peer tx

Output a configuration update transaction to `anchor_peer_tx.pb` which sets the anchor peers for organization Org1 as defined in profile SampleSingleMSPChannelV1_1 based on `configtx.yaml`.

```
configtxgen -outputAnchorPeersUpdate anchor_peer_tx.pb -profile␣
↪SampleSingleMSPChannelV1_1 -asOrg Org1
```

8.7.4 Configuration

The `configtxgen` tool's output is largely controlled by the content of `configtx.yaml`. This file is searched for at `FABRIC_CFG_PATH` and must be present for `configtxgen` to operate.

This configuration file may be edited, or, individual properties may be overridden by setting environment variables, such as `CONFIGTX_ORDERER_ORDERERTYPE=kafka`.

For many `configtxgen` operations, a profile name must be supplied. Profiles are a way to express multiple similar configurations in a single file. For instance, one profile might define a channel with 3 orgs, and another might define one with 4 orgs. To accomplish this without the length of the file becoming burdensome, `configtx.yaml` depends on the standard YAML feature of anchors and references. Base parts of the configuration are tagged with an anchor like `&OrdererDefaults` and then merged into a profile with a reference like `<<: *OrdererDefaults`. Note, when `configtxgen` is operating under a profile, environment variable overrides do not need to include the profile prefix and may be referenced relative to the root element of the profile. For instance, do not specify `CONFIGTX_PROFILE_SAMPLEINSECURESOLO_ORDERER_ORDERERTYPE`, instead simply omit the profile specifics and use the `CONFIGTX` prefix followed by the elements relative to the profile name such as `CONFIGTX_ORDERER_ORDERERTYPE`.

Refer to the sample `configtx.yaml` shipped with Fabric for all possible configuration options. You may find this file in the `config` directory of the release artifacts tar, or you may find it under the `sampleconfig` folder if you are building from source.

8.8 configtxlator

The `configtxlator` command allows users to translate between protobuf and JSON versions of fabric data structures and create config updates. The command may either start a REST server to expose its functions over HTTP or may be utilized directly as a command line tool.

8.8.1 Syntax

The `configtxlator` tool has five sub-commands, as follows:

- start
- proto_encode
- proto_decode
- compute_update
- version

8.8.2 configtxlator start

```
usage: configtxlator start [<flags>]

Start the configtxlator REST server

Flags:
  --help               Show context-sensitive help (also try --help-long and
                       --help-man).
```

(continues on next page)

(continued from previous page)

```
  --hostname="0.0.0.0"  The hostname or IP on which the REST server will listen
  --port=7059           The port on which the REST server will listen
```

8.8.3 configtxlator proto_encode

```
usage: configtxlator proto_encode --type=TYPE [<flags>]

Converts a JSON document to protobuf.

Flags:
  --help                Show context-sensitive help (also try --help-long and
                        --help-man).
  --type=TYPE           The type of protobuf structure to encode to. For
                        example, 'common.Config'.
  --input=/dev/stdin    A file containing the JSON document.
  --output=/dev/stdout  A file to write the output to.
```

8.8.4 configtxlator proto_decode

```
usage: configtxlator proto_decode --type=TYPE [<flags>]

Converts a proto message to JSON.

Flags:
  --help                Show context-sensitive help (also try --help-long and
                        --help-man).
  --type=TYPE           The type of protobuf structure to decode from. For
                        example, 'common.Config'.
  --input=/dev/stdin    A file containing the proto message.
  --output=/dev/stdout  A file to write the JSON document to.
```

8.8.5 configtxlator compute_update

```
usage: configtxlator compute_update --channel_id=CHANNEL_ID [<flags>]

Takes two marshaled common.Config messages and computes the config update which
transitions between the two.

Flags:
  --help                    Show context-sensitive help (also try --help-long and
                            --help-man).
  --original=ORIGINAL       The original config message.
  --updated=UPDATED         The updated config message.
  --channel_id=CHANNEL_ID   The name of the channel for this update.
  --output=/dev/stdout      A file to write the JSON document to.
```

8.8.6 configtxlator version

```
usage: configtxlator version

Show version information

Flags:
  --help  Show context-sensitive help (also try --help-long and --help-man).
```

8.8.7 Examples

Decoding

Decode a block named `fabric_block.pb` to JSON and print to stdout.

```
configtxlator proto_decode --input fabric_block.pb --type common.Block
```

Alternatively, after starting the REST server, the following curl command performs the same operation through the REST API.

```
curl -X POST --data-binary @fabric_block.pb "${CONFIGTXLATOR_URL}/protolator/decode/
↪common.Block"
```

Encoding

Convert a JSON document for a policy from stdin to a file named `policy.pb`.

```
configtxlator proto_encode --type common.Policy --output policy.pb
```

Alternatively, after starting the REST server, the following curl command performs the same operation through the REST API.

```
curl -X POST --data-binary /dev/stdin "${CONFIGTXLATOR_URL}/protolator/encode/common.
↪Policy" > policy.pb
```

Pipelines

Compute a config update from `original_config.pb` and `modified_config.pb` and decode it to JSON to stdout.

```
configtxlator compute_update --channel_id testchan --original original_config.pb --
↪updated modified_config.pb | configtxlator proto_decode --type common.ConfigUpdate
```

Alternatively, after starting the REST server, the following curl commands perform the same operations through the REST API.

```
curl -X POST -F channel=testchan -F "original=@original_config.pb" -F
↪"updated=@modified_config.pb" "${CONFIGTXLATOR_URL}/configtxlator/compute/update-
↪from-configs" | curl -X POST --data-binary /dev/stdin "${CONFIGTXLATOR_URL}/
↪protolator/encode/common.ConfigUpdate"
```

8.8.8 Additional Notes

The tool name is a portmanteau of *configtx* and *translator* and is intended to convey that the tool simply converts between different equivalent data representations. It does not generate configuration. It does not submit or retrieve configuration. It does not modify configuration itself, it simply provides some bijective operations between different views of the configtx format.

There is no configuration file `configtxlator` nor any authentication or authorization facilities included for the REST server. Because `configtxlator` does not have any access to data, key material, or other information which might be considered sensitive, there is no risk to the owner of the server in exposing it to other clients. However, because the data sent by a user to the REST server might be confidential, the user should either trust the administrator of the server, run a local instance, or operate via the CLI.

8.9 cryptogen

`cryptogen` is an utility for generating Hyperledger Fabric key material. It is provided as a means of preconfiguring a network for testing purposes. It would normally not be used in the operation of a production network.

8.9.1 Syntax

The `cryptogen` command has five subcommands, as follows:

- help
- generate
- showtemplate
- extend
- version

8.9.2 cryptogen help

```
usage: cryptogen [<flags>] <command> [<args> ...]

Utility for generating Hyperledger Fabric key material

Flags:
  --help  Show context-sensitive help (also try --help-long and --help-man).

Commands:
  help [<command>...]
    Show help.

  generate [<flags>]
    Generate key material

  showtemplate
    Show the default configuration template

  version
```

(continues on next page)

(continued from previous page)

```
    Show version information

  extend [<flags>]
    Extend existing network
```

8.9.3 cryptogen generate

```
usage: cryptogen generate [<flags>]

Generate key material

Flags:
  --help                    Show context-sensitive help (also try --help-long
                            and --help-man).
  --output="crypto-config"  The output directory in which to place artifacts
  --config=CONFIG           The configuration template to use
```

8.9.4 cryptogen showtemplate

```
usage: cryptogen showtemplate

Show the default configuration template

Flags:
  --help  Show context-sensitive help (also try --help-long and --help-man).
```

8.9.5 cryptogen extend

```
usage: cryptogen extend [<flags>]

Extend existing network

Flags:
  --help                   Show context-sensitive help (also try --help-long and
                           --help-man).
  --input="crypto-config"  The input directory in which existing network place
  --config=CONFIG          The configuration template to use
```

8.9.6 cryptogen version

```
usage: cryptogen version

Show version information

Flags:
  --help  Show context-sensitive help (also try --help-long and --help-man).
```

8.9.7 Usage

Here's an example using the different available flags on the `cryptogen extend` command.

```
    cryptogen extend --input="crypto-config" --config=config.yaml

    org3.example.com
```

Where config.yaml adds a new peer organization called `org3.example.com`

8.10 Service Discovery Command Line Interface (discover)

The discovery service has its own Command Line Interface (CLI) which uses a YAML configuration file to persist properties such as certificate and private key paths, as well as MSP ID.

The `discover` command has the following subcommands:

- saveConfig
- peers
- config
- endorsers

And the usage of the command is shown below:

```
usage: discover [<flags>] <command> [<args> ...]

Command line client for fabric discovery service

Flags:
  --help                    Show context-sensitive help (also try --help-long and --
↪help-man).
  --configFile=CONFIGFILE   Specifies the config file to load the configuration from
  --peerTLSCA=PEERTLSCA     Sets the TLS CA certificate file path that verifies the␣
↪TLS peer's certificate
  --tlsCert=TLSCERT         (Optional) Sets the client TLS certificate file path that␣
↪is used when the peer enforces client authentication
  --tlsKey=TLSKEY           (Optional) Sets the client TLS key file path that is used␣
↪when the peer enforces client authentication
  --userKey=USERKEY         Sets the user's key file path that is used to sign␣
↪messages sent to the peer
  --userCert=USERCERT       Sets the user's certificate file path that is used to␣
↪authenticate the messages sent to the peer
  --MSP=MSP                 Sets the MSP ID of the user, which represents the CA(s)␣
↪that issued its user certificate

Commands:
  help [<command>...]
    Show help.

  peers [<flags>]
    Discover peers

  config [<flags>]
```

(continues on next page)

(continued from previous page)

```
    Discover channel config

  endorsers [<flags>]
    Discover chaincode endorsers

  saveConfig
    Save the config passed by flags into the file specified by --configFile
```

8.10.1 Persisting configuration

To persist the configuration, a config file name should be supplied via the flag `--configFile`, along with the command `saveConfig`:

```
discover --configFile conf.yaml --peerTLSCA tls/ca.crt --userKey msp/keystore/
↪ea4f6a38ac7057b6fa9502c2f5f39f182e320f71f667749100fe7dd94c23ce43_sk --userCert msp/
↪signcerts/User1\@org1.example.com-cert.pem  --MSP Org1MSP saveConfig
```

By executing the above command, configuration file would be created:

```
$ cat conf.yaml
version: 0
tlsconfig:
  certpath: ""
  keypath: ""
  peercacertpath: /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪peerOrganizations/org1.example.com/users/User1@org1.example.com/tls/ca.crt
  timeout: 0s
signerconfig:
  mspid: Org1MSP
  identitypath: /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪peerOrganizations/org1.example.com/users/User1@org1.example.com/msp/signcerts/
↪User1@org1.example.com-cert.pem
  keypath: /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/
↪peerOrganizations/org1.example.com/users/User1@org1.example.com/msp/keystore/
↪ea4f6a38ac7057b6fa9502c2f5f39f182e320f71f667749100fe7dd94c23ce43_sk
```

When the peer runs with TLS enabled, the discovery service on the peer requires the client to connect to it with mutual TLS, which means it needs to supply a TLS certificate. The peer is configured by default to request (but not to verify) client TLS certificates, so supplying a TLS certificate isn't needed (unless the peer's `tls.clientAuthRequired` is set to `true`).

When the discovery CLI's config file has a certificate path for `peercacertpath`, but the `certpath` and `keypath` aren't configured as in the above - the discovery CLI generates a self-signed TLS certificate and uses this to connect to the peer.

When the `peercacertpath` isn't configured, the discovery CLI connects without TLS , and this is highly not recommended, as the information is sent over plaintext, un-encrypted.

8.10.2 Querying the discovery service

The discoveryCLI acts as a discovery client, and it needs to be executed against a peer. This is done via specifying the `--server` flag. In addition, the queries are channel-scoped, so the `--channel` flag must be used.

The only query that doesn't require a channel is the local membership peer query, which by default can only be used by administrators of the peer being queried.

The discover CLI supports all server-side queries:

- Peer membership query
- Configuration query
- Endorsers query

Let's go over them and see how they should be invoked and parsed:

8.10.3 Peer membership query:

```
$ discover --configFile conf.yaml peers --channel mychannel  --server peer0.org1.
↪example.com:7051
[
    {
        "MSPID": "Org2MSP",
        "LedgerHeight": 5,
        "Endpoint": "peer0.org2.example.com:7051",
        "Identity": "-----BEGIN CERTIFICATE-----
↪\nMIICKTCCAc+gAwIBAgIRANK4WBck5gKuzTxVQIwhYMUwCgYIKoZIzj0EAwIwczEL\nMAkGA1UEBhMCVVMxEzARBgNVBAgTCk
↪ecJNvdAV2zmSx5Sf2qospVAH1MYCHyudDEvkiRuBPgmCdOdwJsE0g+h\nz0nZdKq6/
↪X+jTTBLMA4GA1UdDwEB/
↪wQEAwIHgDAMBgNVHRMBAf8EAjAAMCsGA1Ud\nIwQkMCKAIFZMuZfUtY6n2iyxaVr3rl+x5lU0CdG9x7KAeYydQGTMMAoGCCqGSM
↪LJ7j3I9NEPQ/B1BpnJP+UNPnGO2peVrM/
↪mJ1nVgIgS1ZA\nA1tsxuDyllaQuHx2P+P9NDFdjXx5T08lZhxuWYM=\n-----END CERTIFICATE-----\n
↪",
        "Chaincodes": [
            "mycc"
        ]
    },
    {
        "MSPID": "Org2MSP",
        "LedgerHeight": 5,
        "Endpoint": "peer1.org2.example.com:7051",
        "Identity": "-----BEGIN CERTIFICATE-----
↪\nMIICKDCCAc+gAwIBAgIRALnNJzplCrYy4Y8CjZtqL7AwCgYIKoZIzj0EAwIwczEL\nMAkGA1UEBhMCVVMxEzARBgNVBAgTCk
↪YMn1hS6sM+bFDgkJKalG7s9Hg3URF0aGpy51R\nU+4F9Muo+XajTTBLMA4GA1UdDwEB/
↪wQEAwIHgDAMBgNVHRMBAf8EAjAAMCsGA1Ud\nIwQkMCKAIFZMuZfUtY6n2iyxaVr3rl+x5lU0CdG9x7KAeYydQGTMMAoGCCqGSM
↪ExunQ==\n-----END CERTIFICATE-----\n",
        "Chaincodes": [
            "mycc"
        ]
    },
    {
        "MSPID": "Org1MSP",
        "LedgerHeight": 5,
        "Endpoint": "peer0.org1.example.com:7051",
        "Identity": "-----BEGIN CERTIFICATE-----
↪\nMIICKDCCAc6gAwIBAgIQP18LeXtEXGoN8pTqzXTHZTAKBggqhkjOPQQDAjBzMQsw\nCQYDVQQGEwJVUzETMBEGA1UECBMKQ2
↪1Rg/ynSk\nNNItaMlaCDZOaQvxJEl6o3fqx1PVFlfXE4NarY3OO1N3YZI41hWWoXksSwJu/
↪35S\nM7wMEzw+3KNNMEswDgYDVR0PAQH/BAQDAgeAMAwGA1UdEwEB/
↪wQCMAAwKwYDVR0j\nBCQwIoAgcecTOxTes6rfgyxHH6KIW7hsRAw2bhP9ikCHkvtv/
↪RcwCgYIKoZIzj0E\nAwIDSAAwRQIhAKiJEv79XBmr8gGY6kHrGL0L3sq95E7IsCYzYdAQHj+DAiBPcBTg\nRuA0/
↪/Kq+3aHJ2T0KpKHqD3FfhZZolKDkcrkwQ==\n-----END CERTIFICATE-----\n",
        "Chaincodes": [
            "mycc"
        ]
```

(continues on next page)

(continued from previous page)

```
    },
    {
        "MSPID": "Org1MSP",
        "LedgerHeight": 5,
        "Endpoint": "peer1.org1.example.com:7051",
        "Identity": "-----BEGIN CERTIFICATE-----
↪\nMIICJzCCAc6gAwIBAgIQO7zMEHlMfRhnP6Xt65jwtDAKBggqhkjOPQQDAjBzMQsw\nCQYDVQQGEwJVUzETMBEGA1UECBMKQ2
↪Q2g\nRHw5rk3SYw+OMFw9jNbsJJyC5ttJRvc12Dn7lQ8ZR9hW1vLQ3NtqO/
↪couccDJcHg\nt47iHBNadaNNMEswDgYDVR0PAQH/BAQDAgeAMAwGA1UdEwEB/
↪wQCMAAwKwYDVR0j\nBCQwIoAgcecTOxTes6rfgyxHH6KIW7hsRAw2bhP9ikCHkvtv/
↪RcwCgYIKoZIzj0E\nAwIDRwAwRAIgGHGtRVxcFVeMQr9yRlebs23OXEECNo6hNqd/
↪4ChLwwoCIBFKFd6t\nlL5BVzVMGQyXWcZGrjFgl4+fDrwjmMe+jAfa\n-----END CERTIFICATE-----\n
↪",
        "Chaincodes": null
    }
]
```

As seen, this command outputs a JSON containing membership information about all the peers in the channel that the peer queried possesses.

The `Identity` that is returned is the enrollment certificate of the peer, and it can be parsed with a combination of `jq` and `openssl`:

```
$ discover --configFile conf.yaml peers --channel mychannel  --server peer0.org1.
↪example.com:7051  | jq .[0].Identity | sed "s/\\\n/\n/g" | sed "s/\"//g"  | openssl␣
↪x509 -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            55:e9:3f:97:94:d5:74:db:e2:d6:99:3c:01:24:be:bf
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, ST=California, L=San Francisco, O=org2.example.com, CN=ca.org2.
↪example.com
        Validity
            Not Before: Jun  9 11:58:28 2018 GMT
            Not After : Jun  6 11:58:28 2028 GMT
        Subject: C=US, ST=California, L=San Francisco, OU=peer, CN=peer0.org2.example.
↪com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:f5:69:7a:11:65:d9:85:96:65:b7:b7:1b:08:77:
                    43:de:cb:ad:3a:79:ec:cc:2a:bc:d7:93:68:ae:92:
                    1c:4b:d8:32:47:d6:3d:72:32:f1:f1:fb:26:e4:69:
                    c2:eb:c9:45:69:99:78:d7:68:a9:77:09:88:c6:53:
                    01:2a:c1:f8:c0
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:
                ␣
↪keyid:8E:58:82:C9:0A:11:10:A9:0B:93:03:EE:A0:54:42:F4:A3:EF:11:4C:82:B6:[illegible]E:24:AB:13:82:
```

(continues on next page)

(continued from previous page)

```
    Signature Algorithm: ecdsa-with-SHA256
         30:44:02:20:29:3f:55:2b:9f:7b:99:b2:cb:06:ca:15:3f:93:
         a1:3d:65:5c:7b:79:a1:7a:d1:94:50:f0:cd:db:ea:61:81:7a:
         02:20:3b:40:5b:60:51:3c:f8:0f:9b:fc:ae:fc:21:fd:c8:36:
         a3:18:39:58:20:72:3d:1a:43:74:30:f3:56:01:aa:26
```

8.10.4 Configuration query:

The configuration query returns a mapping from MSP IDs to orderer endpoints, as well as the `FabricMSPConfig` which can be used to verify all peer and orderer nodes by the SDK:

```
$ discover --configFile conf.yaml config --channel mychannel  --server peer0.org1.
↪example.com:7051
{
    "msps": {
        "OrdererOrg": {
            "name": "OrdererMSP",
            "root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNMekNDQWRhZ0F3SUJBZ0lSQU1pWkxUb3RmMHR6VTRzNUdIdkQ0UjR3Q2
↪"
            ],
            "admins": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNDVENDQWJDZ0F3SUJBZ0lRR2wzTjhaSzRDekRRQmZqYVpwMVF5VEFLQn
↪"
            ],
            "crypto_config": {
                "signature_hash_family": "SHA2",
                "identity_identifier_hash_function": "SHA256"
            },
            "tls_root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNORENDQWR1Z0F3SUJBZ0lRZDdodzFIaHNZTXI2a25ETWJrZThTakFLQn
↪"
            ]
        },
        "Org1MSP": {
            "name": "Org1MSP",
            "root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWVxZ0F3SUJBZ0lSQU1nN2VETnhwS0t0ZGl0TDRVNDRZMUl3Q2
↪"
            ],
            "admins": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNLakNDQWRDZ0F3SUJBZ0lRRTRFK0tqSHgwdTlzRSsxZUgrL1dOakFLQn
↪"
            ],
            "crypto_config": {
                "signature_hash_family": "SHA2",
                "identity_identifier_hash_function": "SHA256"
            },
            "tls_root_certs": [
```

(continues on next page)

(continued from previous page)

```
↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNTVENDQWUrZ0F3SUJBZ0lRZlRWTE9iTENVUjdxVEY3Z283UXgvakFLQn
↪"
            ],
            "fabric_node_ous": {
                "enable": true,
                "client_ou_identifier": {
                    "certificate":
↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWVxZ0F3SUJBZ0lSQU1nN2VETnhwS0t0ZGl0TDRVNDRZMUl3Q2
↪",
                    "organizational_unit_identifier": "client"
                },
                "peer_ou_identifier": {
                    "certificate":
↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWVxZ0F3SUJBZ0lSQU1nN2VETnhwS0t0ZGl0TDRVNDRZMUl3Q2
↪",
                    "organizational_unit_identifier": "peer"
                }
            }
        },
        "Org2MSP": {
            "name": "Org2MSP",
            "root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWVxZ0F3SUJBZ0lSQUx2SWV2KzE4Vm9LZFR2V1RLNCtaZ2d3Q2
↪"
            ],
            "admins": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNLVENDQWRDZ0F3SUJBZ0lRU1lpeE1vdmpoM1N2c25WMmFUOXl1REFLQn
↪"
            ],
            "crypto_config": {
                "signature_hash_family": "SHA2",
                "identity_identifier_hash_function": "SHA256"
            },
            "tls_root_certs": [

↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNTakNDQWZEZ0F3SUJBZ0lSQUtoUFFxUGZSYnVpSktqL0JRanQ3RXN3Q2
↪"
            ],
            "fabric_node_ous": {
                "enable": true,
                "client_ou_identifier": {
                    "certificate":
↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWVxZ0F3SUJBZ0lSQUx2SWV2KzE4Vm9LZFR2V1RLNCtaZ2d3Q2
↪",
                    "organizational_unit_identifier": "client"
                },
                "peer_ou_identifier": {
                    "certificate":
↪"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWVxZ0F3SUJBZ0lSQUx2SWV2KzE4Vm9LZFR2V1RLNCtaZ2d3Q2
↪",
                    "organizational_unit_identifier": "peer"
                }
            }
        },
```

(continues on next page)

(continued from previous page)

```
        "Org3MSP": {
            "name": "Org3MSP",
            "root_certs": [
                "CgJPVQoEUm9sZQoMRW5yb2xsbWVudElEChBSZXZvY2F0aW9uSGFuZGxlEkQKIKoEXcq/
↪psdYnMKCiT79N+dS1hM8k+SuzU1blOgTuN++EiBe2m3E+FjWLuQGMNRGRrEVTMqTvC4A/
↪5jvCLv2ja1sZxpECiDBbI0kwetxAwFzHwb1hi8TlkGW3OofvuVzfFt9VlewcRIgyvsxG5/
↪THdWyKJTdNx8Gle2hoCbVF0Y1/
↪DQESBjGOGciRAog25fMyWps+FLOjzj1vIsGUyO457ri3YMvmUcycIH2FvQSICTtzaFvSPUiDtNtAVz+uetuB9kfmjUdUSQxjyXU
↪uaJMuVph7Dy/
↪icgnAtVYHShET41O0Eh3Q5BIgy5q9VMQrch9VW5yajhY8dH1uA593gKd5kBqGdLfiXzAiRAogAnUYq/
↪kwKzFfmIm/
↪W4nZxi1kjG2C8NRjsYYBkeAOQ6wSIGyX5GGmwgvxgXXehNWBfijyNIJALGRVhO8YtBqr+vnrKogBCiDHR1XQsDbpcBoZFJ09V9
↪wwC+tq3oBIgSWT/
↪peiO2BI0DecypKfgMpVR8DWXl8ZHSrPISsL3Mc8aINem9+BOezLwFKCbtVH1KAHIRLyyiNP+TkIKW6x9RkThIiAbIJCYU6O02EE
↪1lHxV0vtWdIsKCTLx2EZmDJECiCPXeyUyFzPS3iFv8CQUOLCPZxf6buZS5JlM6EE/
↪gCRaxIgmF9GKPLLmEoA77+AU3J8Iwnu9pBxnaHtUlyf/F9p30c6RAogG7ENKWlOZ4aF0HprqXAjl++Iao7/
↪iE8xeVcKRlmfq1ASIGtmmavDAVS2bw3zClQd4ZBD2DrqCBO9NPOcLNB0IWeIQiCjxTdbmcuBNINZYWe+5fWyI1oY9LavKzDVkdH
↪PRAmBaeTQLXdbMxIthxM2gw+Zkc5+IJEWX"
            ],
            "intermediate_certs": [
                "CtgCCkQKIP0UVivtH8NlnRNrZuuu6jpaj2ZbEB4/
↪secGS57MfbINEiDSJweLUMIQSW12jugBQG81lIQflJWvi7vi925u+PU/
↪+xJECiDgOGdNbAiGSoHmTjKhT22fqUqYLIVh+JBHetm4kF4skhIg9XTWRkUqtsfYKENzPgm7ZUSmCHNF8xH7Vnhuc1EpAUgaINw
↪cIiCnlRj+mfNVAJGKthLgQBB/
↪JKM14NbUeutyJtTgrmDDiCogme25qGvxJfgQNnzldMMicVyiI6YMfnoThAUyqsTzyXkqIAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
↪El+BA2fOV0wyJxXKIjpgx+ehOEBTKqxPPJeSogAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAESIFYUenRvjbmEh+37Y
↪gwzULTJbCAoVg9XfCiROs4cU5oSv4Q80iYWtonAnvsSIE6mYFdzisBU21rhxjfYE7kk3Xjih9A1idJp7TSjfmorGiBwIEbnxUKj
↪yIgBVTjvNOIwpBC7qZJKX6yn4tMvoCCGpiz4BKBEUqtBJsaZzBlAjBwZ4WXYOttkhsNA2r94gBfLUdx/
↪4VhW4hwUImcztlau1T14UlNzJolCNkdiLc9CqsCMQD6OBkgDWGq9UlhkK9dJBzU+RElcZdSfVV1hDbbqt+lFRWOzzEkZ+BXCR1k
↪"
            ],
            "admins": [

↪"LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUhZd0VBWUhLb1pJemowQ0FRWUZLNEVFQUNJRFlnQUVUYk13SEZteEpEMWR3Sj
↪"
            ]
        }
    },
    "orderers": {
        "OrdererOrg": {
            "endpoint": [
                {
                    "host": "orderer.example.com",
                    "port": 7050
                }
            ]
        }
    }
}
```

It's important to note that the certificates here are base64 encoded, and thus should decoded in a manner similar to the following:

```
$ discover --configFile conf.yaml config --channel mychannel  --server peer0.org1.
↪example.com:7051 | jq .msps.OrdererOrg.root_certs[0] | sed "s/\"//g" | base64 --
↪decode | openssl x509 -text -noout
```

(continues on next page)

(continued from previous page)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            c8:99:2d:3a:2d:7f:4b:73:53:8b:39:18:7b:c3:e1:1e
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, ST=California, L=San Francisco, O=example.com, CN=ca.example.com
        Validity
            Not Before: Jun  9 11:58:28 2018 GMT
            Not After : Jun  6 11:58:28 2028 GMT
        Subject: C=US, ST=California, L=San Francisco, O=example.com, CN=ca.example.
↪com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:28:ac:9e:51:8d:a4:80:15:0a:ff:ae:c9:61:d6:
                    08:67:b0:15:c3:c7:99:46:61:63:0a:10:a6:42:6a:
                    b0:af:14:0c:c0:e2:5b:b4:a1:c3:f0:07:7e:5b:7c:
                    c4:b2:95:13:95:81:4b:6a:b9:e3:87:a4:f3:2c:7c:
                    ae:00:91:9e:32
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Certificate Sign, CRL Sign
            X509v3 Extended Key Usage:
                Any Extended Key Usage
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:

↪60:9D:F2:30:26:CE:8F:65:81:41:AD:96:15:0E:24:8D:A0:9D:C5:79:C1:17:BF:FE:E5:1B:FB:75:50:10:A6:4C
    Signature Algorithm: ecdsa-with-SHA256
         30:44:02:20:3d:e1:a7:6c:99:3f:87:2a:36:44:51:98:37:11:
         d8:a0:47:7a:33:ff:30:c1:09:a6:05:ec:b0:53:53:39:c1:0e:
         02:20:6b:f4:1d:48:e0:72:e4:c2:ef:b0:84:79:d4:2e:c2:c5:
         1b:6f:e4:2f:56:35:51:18:7d:93:51:86:05:84:ce:1f
```

8.10.5 Endorsers query:

To query for the endorsers of a chaincode call, additional flags need to be supplied:

- The `--chaincode` flag is mandatory and it provides the chaincode name(s). To query for a chaincode-to-chaincode invocation, one needs to repeat the `--chaincode` flag with all the chaincodes.
- The `--collection` is used to specify private data collections that are expected to used by the chaincode(s). To map from thechaincodes passed via `--chaincode` to the collections, the following syntax should be used: `collection=CC:Collection1,Collection2,...`.

For example, to query for a chaincode invocation that results in both cc1 and cc2 to be invoked, as well as writes to private data collection col1 by cc2, one needs to specify: `--chaincode=cc1 --chaincode=cc2 --collection=cc2:col1`

Below is the output of an endorsers query for chaincode **mycc** when the endorsement policy is `AND('Org1.peer', 'Org2.peer')`:

```
$ discover --configFile conf.yaml endorsers --channel mychannel  --server peer0.org1.
↪example.com:7051 --chaincode mycc
[
    {
        "Chaincode": "mycc",
        "EndorsersByGroups": {
            "G0": [
                {
                    "MSPID": "Org1MSP",
                    "LedgerHeight": 5,
                    "Endpoint": "peer0.org1.example.com:7051",
                    "Identity": "-----BEGIN CERTIFICATE-----
↪\nMIICKDCCAc+gAwIBAgIRANTiKfUVHVGnrYVzEy1ZSKIwCgYIKoZIzj0EAwIwczEL\nMAkGA1UEBhMCVVMxEzARBgNVBAgTCk
↪k\n/CtORCDPQ02jTTBLMA4GA1UdDwEB/
↪wQEAwIHgDAMBgNVHRMBAf8EAjAAMCsGA1Ud\nIwQkMCKAIOBdQLF+cMWa6e1p2CpOEx7SHUinzVvd55hLm7w6v72oMAoGCCqGSM
↪zwD08t7hJxNe8MwgP8/48fAiBiC0cr\nu99oLsRNCFB7R3egyKg1YYao0KWTrr1T+rK9Bg==\n-----END␣
↪CERTIFICATE-----\n"
                }
            ],
            "G1": [
                {
                    "MSPID": "Org2MSP",
                    "LedgerHeight": 5,
                    "Endpoint": "peer1.org2.example.com:7051",
                    "Identity": "-----BEGIN CERTIFICATE-----
↪\nMIICKDCCAc+gAwIBAgIRAIs6fFxk4Y5cJxSwTjyJ9A8wCgYIKoZIzj0EAwIwczEL\nMAkGA1UEBhMCVVMxEzARBgNVBAgTCk
↪cq\n0cGrMKR93vKjTTBLMA4GA1UdDwEB/
↪wQEAwIHgDAMBgNVHRMBAf8EAjAAMCsGA1Ud\nIwQkMCKAII5YgskKERCpC5MD7qBUQvSj7xFMgrb5zhCiHiSrE4KgMAoGCCqGSM
↪OidQ2SBR7OZyMAzgXc5nAabWZpdkuQ==\n-----END CERTIFICATE-----\n"
                },
                {
                    "MSPID": "Org2MSP",
                    "LedgerHeight": 5,
                    "Endpoint": "peer0.org2.example.com:7051",
                    "Identity": "-----BEGIN CERTIFICATE-----\nMIICJzCCAc6gAwIBAgIQVek/
↪l5TVdNvi1pk8ASS+vzAKBggqhkjOPQQDAjBzMQsw\nCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEWMBQGA1UEBxMNU
↪BAQDAgeAMAwGA1UdEwEB/
↪wQCMAAwKwYDVR0j\nBCQwIoAgjliCyQoREKkLkwPuoFRC9KPvEUyCtvnOEKIeJKsTgqAwCgYIKoZIzj0E\nAwIDRwAwRAIgKT9V
↪yu/CH9yDajGDlYIHI9GkN0MPNWAaom\n-----END CERTIFICATE-----\n"
                }
            ]
        },
        "Layouts": [
            {
                "quantities_by_group": {
                    "G0": 1,
                    "G1": 1
                }
            }
        ]
    }
]
```

8.10.6 Not using a configuration file

It is possible to execute the discovery CLI without having a configuration file, and just passing all needed configuration as commandline flags. The following is an example of a local peer membership query which loads administrator credentials:

```
$ discover --peerTLSCA tls/ca.crt --userKey msp/keystore/
↪cf31339d09e8311ac9ca5ed4e27a104a7f82f1e5904b3296a170ba4725ffde0d_sk --userCert msp/
↪signcerts/Admin\@org1.example.com-cert.pem --MSP Org1MSP --tlsCert tls/client.crt --
↪tlsKey tls/client.key peers --server peer0.org1.example.com:7051
[
    {
        "MSPID": "Org1MSP",
        "Endpoint": "peer1.org1.example.com:7051",
        "Identity": "-----BEGIN CERTIFICATE-----
↪\nMIICJzCCAc6gAwIBAgIQO7zMEHlMfRhnP6Xt65jwtDAKBggqhkjOPQQDAjBzMQsw\nCQYDVQQGEwJVUzETMBEGA1UECBMKQ2F
↪Q2g\nRHw5rk3SYw+OMFw9jNbsJJyC5ttJRvc12Dn7lQ8ZR9hW1vLQ3NtqO/
↪couccDJcHg\nt47iHBNadaNNMEswDgYDVR0PAQH/BAQDAgeAMAwGA1UdEwEB/
↪wQCMAAwKwYDVR0j\nBCQwIoAgcecTOxTes6rfgyxHH6KIW7hsRAw2bhP9ikCHkvtv/
↪RcwCgYIKoZIzj0E\nAwIDRwAwRAIgGHGtRVxcFVeMQr9yRlebs23OXEECNo6hNqd/
↪4ChLwwoCIBFKFd6t\nlL5BVzVMGQyXWcZGrjFgl4+fDrwjmMe+jAfa\n-----END CERTIFICATE-----\n
↪",
    },
    {
        "MSPID": "Org1MSP",
        "Endpoint": "peer0.org1.example.com:7051",
        "Identity": "-----BEGIN CERTIFICATE-----
↪\nMIICKDCCAc6gAwIBAgIQP18LeXtEXGoN8pTqzXTHZTAKBggqhkjOPQQDAjBzMQsw\nCQYDVQQGEwJVUzETMBEGA1UECBMKQ2F
↪1Rg/ynSk\nNNItaMlaCDZOaQvxJEl6o3fqx1PVFlfXE4NarY3OO1N3YZI41hWWoXksSwJu/
↪35S\nM7wMEzw+3KNNMEswDgYDVR0PAQH/BAQDAgeAMAwGA1UdEwEB/
↪wQCMAAwKwYDVR0j\nBCQwIoAgcecTOxTes6rfgyxHH6KIW7hsRAw2bhP9ikCHkvtv/
↪RcwCgYIKoZIzj0E\nAwIDSAAwRQIhAKiJEv79XBmr8gGY6kHrGL0L3sq95E7IsCYzYdAQHj+DAiBPcBTg\nRuA0/
↪/Kq+3aHJ2T0KpKHqD3FfhZZolKDkcrkwQ==\n-----END CERTIFICATE-----\n",
    },
    {
        "MSPID": "Org2MSP",
        "Endpoint": "peer0.org2.example.com:7051",
        "Identity": "-----BEGIN CERTIFICATE-----
↪\nMIICKTCCAc+gAwIBAgIRANK4WBck5gKuzTxVQIwhYMUwCgYIKoZIzj0EAwIwczEL\nMAkGA1UEBhMCVVMxEzARBgNVBAgTCk
↪ecJNvdAV2zmSx5Sf2qospVAH1MYCHyudDEvkiRuBPgmCdOdwJsE0g+h\nz0nZdKq6/
↪X+jTTBLMA4GA1UdDwEB/
↪wQEAwIHgDAMBgNVHRMBAf8EAjAAMCsGA1Ud\nIwQkMCKAIFZMuZfUtY6n2iyxaVr3rl+x5lU0CdG9x7KAeYydQGTMMAoGCCqGSM
↪LJ7j3I9NEPQ/B1BpnJP+UNPnGO2peVrM/
↪mJ1nVgIgS1ZA\nA1tsxuDyllaQuHx2P+P9NDFdjXx5T08lZhxuWYM=\n-----END CERTIFICATE-----\n
↪",
    },
    {
        "MSPID": "Org2MSP",
        "Endpoint": "peer1.org2.example.com:7051",
        "Identity": "-----BEGIN CERTIFICATE-----
↪\nMIICKDCCAc+gAwIBAgIRALnNJzplCrYy4Y8CjZtqL7AwCgYIKoZIzj0EAwIwczEL\nMAkGA1UEBhMCVVMxEzARBgNVBAgTCk
↪YMn1hS6sM+bFDgkJKalG7s9Hg3URF0aGpy51R\nU+4F9Muo+XajTTBLMA4GA1UdDwEB/
↪wQEAwIHgDAMBgNVHRMBAf8EAjAAMCsGA1Ud\nIwQkMCKAIFZMuZfUtY6n2iyxaVr3rl+x5lU0CdG9x7KAeYydQGTMMAoGCCqGSM
↪ExunQ==\n-----END CERTIFICATE-----\n",
    }
]
```

8.11 Fabric-CA Commands

The Hyperledger Fabric CA is a Certificate Authority (CA) for Hyperledger Fabric. The commands available for the fabric-ca client and fabric-ca server are described in the links below.

8.11.1 Fabric-CA Client

The fabric-ca-client command allows you to manage identities (including attribute management) and certificates (including renewal and revocation).

More information on `fabric-ca-client` commands can be found here.

8.11.2 Fabric-CA Server

The fabric-ca-server command allows you to initialize and start a server process which may host one or more certificate authorities.

More information on `fabric-ca-server` commands can be found here.

CHAPTER 9

Architecture Reference

9.1 Architecture Explained

The Hyperledger Fabric architecture delivers the following advantages:

- **Chaincode trust flexibility.** The architecture separates *trust assumptions* for chaincodes (blockchain applications) from trust assumptions for ordering. In other words, the ordering service may be provided by one set of nodes (orderers) and tolerate some of them to fail or misbehave, and the endorsers may be different for each chaincode.
- **Scalability.** As the endorser nodes responsible for particular chaincode are orthogonal to the orderers, the system may *scale* better than if these functions were done by the same nodes. In particular, this results when different chaincodes specify disjoint endorsers, which introduces a partitioning of chaincodes between endorsers and allows parallel chaincode execution (endorsement). Besides, chaincode execution, which can potentially be costly, is removed from the critical path of the ordering service.
- **Confidentiality.** The architecture facilitates deployment of chaincodes that have *confidentiality* requirements with respect to the content and state updates of its transactions.
- **Consensus modularity.** The architecture is *modular* and allows pluggable consensus (i.e., ordering service) implementations.

Part I: Elements of the architecture relevant to Hyperledger Fabric v1

1. System architecture
2. Basic workflow of transaction endorsement
3. Endorsement policies

   Part II: Post-v1 elements of the architecture

4. Ledger checkpointing (pruning)

9.1.1 1. System architecture

The blockchain is a distributed system consisting of many nodes that communicate with each other. The blockchain runs programs called chaincode, holds state and ledger data, and executes transactions. The chaincode is the central element as transactions are operations invoked on the chaincode. Transactions have to be "endorsed" and only endorsed transactions may be committed and have an effect on the state. There may exist one or more special chaincodes for management functions and parameters, collectively called *system chaincodes*.

1.1. Transactions

Transactions may be of two types:

- *Deploy transactions* create new chaincode and take a program as parameter. When a deploy transaction executes successfully, the chaincode has been installed "on" the blockchain.
- *Invoke transactions* perform an operation in the context of previously deployed chaincode. An invoke transaction refers to a chaincode and to one of its provided functions. When successful, the chaincode executes the specified function - which may involve modifying the corresponding state, and returning an output.

As described later, deploy transactions are special cases of invoke transactions, where a deploy transaction that creates new chaincode, corresponds to an invoke transaction on a system chaincode.

Remark: *This document currently assumes that a transaction either creates new chaincode or invokes an operation provided by *one* already deployed chaincode. This document does not yet describe: a) optimizations for query (read-only) transactions (included in v1), b) support for cross-chaincode transactions (post-v1 feature).**

1.2. Blockchain datastructures

1.2.1. State

The latest state of the blockchain (or, simply, *state*) is modeled as a versioned key-value store (KVS), where keys are names and values are arbitrary blobs. These entries are manipulated by the chaincodes (applications) running on the blockchain through `put` and `get` KVS-operations. The state is stored persistently and updates to the state are logged. Notice that versioned KVS is adopted as state model, an implementation may use actual KVSs, but also RDBMSs or any other solution.

More formally, state `s` is modeled as an element of a mapping `K -> (V X N)`, where:

- `K` is a set of keys
- `V` is a set of values
- `N` is an infinite ordered set of version numbers. Injective function `next: N -> N` takes an element of `N` and returns the next version number.

Both `V` and `N` contain a special element (empty type), which is in case of `N` the lowest element. Initially all keys are mapped to (,). For `s(k)=(v,ver)` we denote `v` by `s(k).value`, and `ver` by `s(k).version`.

KVS operations are modeled as follows:

- `put(k,v)` for `k K` and `v V`, takes the blockchain state `s` and changes it to `s'` such that `s'(k)=(v, next(s(k).version))` with `s'(k')=s(k')` for all `k'!=k`.
- `get(k)` returns `s(k)`.

State is maintained by peers, but not by orderers and clients.

State partitioning. Keys in the KVS can be recognized from their name to belong to a particular chaincode, in the sense that only transaction of a certain chaincode may modify the keys belonging to this chaincode. In principle, any

chaincode can read the keys belonging to other chaincodes. *Support for cross-chaincode transactions, that modify the state belonging to two or more chaincodes is a post-v1 feature.*

1.2.2 Ledger

Ledger provides a verifiable history of all successful state changes (we talk about *valid* transactions) and unsuccessful attempts to change state (we talk about *invalid* transactions), occurring during the operation of the system.

Ledger is constructed by the ordering service (see Sec 1.3.3) as a totally ordered hashchain of *blocks* of (valid or invalid) transactions. The hashchain imposes the total order of blocks in a ledger and each block contains an array of totally ordered transactions. This imposes total order across all transactions.

Ledger is kept at all peers and, optionally, at a subset of orderers. In the context of an orderer we refer to the Ledger as to `OrdererLedger`, whereas in the context of a peer we refer to the ledger as to `PeerLedger`. `PeerLedger` differs from the `OrdererLedger` in that peers locally maintain a bitmask that tells apart valid transactions from invalid ones (see Section XX for more details).

Peers may prune `PeerLedger` as described in Section XX (post-v1 feature). Orderers maintain `OrdererLedger` for fault-tolerance and availability (of the `PeerLedger`) and may decide to prune it at anytime, provided that properties of the ordering service (see Sec. 1.3.3) are maintained.

The ledger allows peers to replay the history of all transactions and to reconstruct the state. Therefore, state as described in Sec 1.2.1 is an optional datastructure.

1.3. Nodes

Nodes are the communication entities of the blockchain. A "node" is only a logical function in the sense that multiple nodes of different types can run on the same physical server. What counts is how nodes are grouped in "trust domains" and associated to logical entities that control them.

There are three types of nodes:

1. **Client** or **submitting-client**: a client that submits an actual transaction-invocation to the endorsers, and broadcasts transaction-proposals to the ordering service.
2. **Peer**: a node that commits transactions and maintains the state and a copy of the ledger (see Sec, 1.2). Besides, peers can have a special **endorser** role.
3. **Ordering-service-node** or **orderer**: a node running the communication service that implements a delivery guarantee, such as atomic or total order broadcast.

The types of nodes are explained next in more detail.

1.3.1. Client

The client represents the entity that acts on behalf of an end-user. It must connect to a peer for communicating with the blockchain. The client may connect to any peer of its choice. Clients create and thereby invoke transactions.

As detailed in Section 2, clients communicate with both peers and the ordering service.

1.3.2. Peer

A peer receives ordered state updates in the form of *blocks* from the ordering service and maintain the state and the ledger.

Peers can additionally take up a special role of an **endorsing peer**, or an **endorser**. The special function of an *endorsing peer* occurs with respect to a particular chaincode and consists in *endorsing* a transaction before it is committed. Every chaincode may specify an *endorsement policy* that may refer to a set of endorsing peers. The policy defines the necessary and sufficient conditions for a valid transaction endorsement (typically a set of endorsers' signatures), as described later in Sections 2 and 3. In the special case of deploy transactions that install new chaincode the (deployment) endorsement policy is specified as an endorsement policy of the system chaincode.

1.3.3. Ordering service nodes (Orderers)

The *orderers* form the *ordering service*, i.e., a communication fabric that provides delivery guarantees. The ordering service can be implemented in different ways: ranging from a centralized service (used e.g., in development and testing) to distributed protocols that target different network and node fault models.

Ordering service provides a shared *communication channel* to clients and peers, offering a broadcast service for messages containing transactions. Clients connect to the channel and may broadcast messages on the channel which are then delivered to all peers. The channel supports *atomic* delivery of all messages, that is, message communication with total-order delivery and (implementation specific) reliability. In other words, the channel outputs the same messages to all connected peers and outputs them to all peers in the same logical order. This atomic communication guarantee is also called *total-order broadcast*, *atomic broadcast*, or *consensus* in the context of distributed systems. The communicated messages are the candidate transactions for inclusion in the blockchain state.

Partitioning (ordering service channels). Ordering service may support multiple *channels* similar to the *topics* of a publish/subscribe (pub/sub) messaging system. Clients can connect to a given channel and can then send messages and obtain the messages that arrive. Channels can be thought of as partitions - clients connecting to one channel are unaware of the existence of other channels, but clients may connect to multiple channels. Even though some ordering service implementations included with Hyperledger Fabric support multiple channels, for simplicity of presentation, in the rest of this document, we assume ordering service consists of a single channel/topic.

Ordering service API. Peers connect to the channel provided by the ordering service, via the interface provided by the ordering service. The ordering service API consists of two basic operations (more generally *asynchronous events*):

TODO add the part of the API for fetching particular blocks under client/peer specified sequence numbers.

- `broadcast(blob)`: a client calls this to broadcast an arbitrary message `blob` for dissemination over the channel. This is also called `request(blob)` in the BFT context, when sending a request to a service.
- `deliver(seqno, prevhash, blob)`: the ordering service calls this on the peer to deliver the message `blob` with the specified non-negative integer sequence number (`seqno`) and hash of the most recently delivered blob (`prevhash`). In other words, it is an output event from the ordering service. `deliver()` is also sometimes called `notify()` in pub-sub systems or `commit()` in BFT systems.

Ledger and block formation. The ledger (see also Sec. 1.2.2) contains all data output by the ordering service. In a nutshell, it is a sequence of `deliver(seqno, prevhash, blob)` events, which form a hash chain according to the computation of `prevhash` described before.

Most of the time, for efficiency reasons, instead of outputting individual transactions (blobs), the ordering service will group (batch) the blobs and output *blocks* within a single `deliver` event. In this case, the ordering service must impose and convey a deterministic ordering of the blobs within each block. The number of blobs in a block may be chosen dynamically by an ordering service implementation.

In the following, for ease of presentation, we define ordering service properties (rest of this subsection) and explain the workflow of transaction endorsement (Section 2) assuming one blob per `deliver` event. These are easily extended to blocks, assuming that a `deliver` event for a block corresponds to a sequence of individual `deliver` events for each blob within a block, according to the above mentioned deterministic ordering of blobs within a block.

Ordering service properties

The guarantees of the ordering service (or atomic-broadcast channel) stipulate what happens to a broadcasted message and what relations exist among delivered messages. These guarantees are as follows:

1. **Safety (consistency guarantees)**: As long as peers are connected for sufficiently long periods of time to the channel (they can disconnect or crash, but will restart and reconnect), they will see an *identical* series of delivered `(seqno, prevhash, blob)` messages. This means the outputs (`deliver()` events) occur in the *same order* on all peers and according to sequence number and carry *identical content* (`blob` and `prevhash`) for the same sequence number. Note this is only a *logical order*, and a `deliver(seqno, prevhash, blob)` on one peer is not required to occur in any real-time relation to `deliver(seqno, prevhash, blob)` that outputs the same message at another peer. Put differently, given a particular `seqno`, *no* two correct peers deliver *different* `prevhash` or `blob` values. Moreover, no value `blob` is delivered unless some client (peer) actually called `broadcast(blob)` and, preferably, every broadcasted blob is only delivered *once*.

   Furthermore, the `deliver()` event contains the cryptographic hash of the data in the previous `deliver()` event (`prevhash`). When the ordering service implements atomic broadcast guarantees, `prevhash` is the cryptographic hash of the parameters from the `deliver()` event with sequence number `seqno-1`. This establishes a hash chain across `deliver()` events, which is used to help verify the integrity of the ordering service output, as discussed in Sections 4 and 5 later. In the special case of the first `deliver()` event, `prevhash` has a default value.

2. **Liveness (delivery guarantee)**: Liveness guarantees of the ordering service are specified by a ordering service implementation. The exact guarantees may depend on the network and node fault model.

   In principle, if the submitting client does not fail, the ordering service should guarantee that every correct peer that connects to the ordering service eventually delivers every submitted transaction.

To summarize, the ordering service ensures the following properties:

- *Agreement.* For any two events at correct peers `deliver(seqno, prevhash0, blob0)` and `deliver(seqno, prevhash1, blob1)` with the same `seqno`, `prevhash0==prevhash1` and `blob0==blob1`;
- *Hashchain integrity.* For any two events at correct peers `deliver(seqno-1, prevhash0, blob0)` and `deliver(seqno, prevhash, blob)`,`prevhash = HASH(seqno-1||prevhash0||blob0)`.
- *No skipping*. If an ordering service outputs `deliver(seqno, prevhash, blob)` at a correct peer *p*, such that `seqno>0`, then *p* already delivered an event `deliver(seqno-1, prevhash0, blob0)`.
- *No creation*. Any event `deliver(seqno, prevhash, blob)` at a correct peer must be preceded by a `broadcast(blob)` event at some (possibly distinct) peer;
- *No duplication (optional, yet desirable)*. For any two events `broadcast(blob)` and `broadcast(blob')`, when two events `deliver(seqno0, prevhash0, blob)` and `deliver(seqno1, prevhash1, blob')` occur at correct peers and `blob == blob'`, then `seqno0==seqno1` and `prevhash0==prevhash1`.
- *Liveness*. If a correct client invokes an event `broadcast(blob)` then every correct peer "eventually" issues an event `deliver(*, *, blob)`, where `*` denotes an arbitrary value.

9.1.2 2. Basic workflow of transaction endorsement

In the following we outline the high-level request flow for a transaction.

Remark: *Notice that the following protocol *does not* assume that all transactions are deterministic, i.e., it allows for non-deterministic transactions.**

2.1. The client creates a transaction and sends it to endorsing peers of its choice

To invoke a transaction, the client sends a PROPOSE message to a set of endorsing peers of its choice (possibly not at the same time - see Sections 2.1.2. and 2.3.). The set of endorsing peers for a given chaincodeID is made available to client via peer, which in turn knows the set of endorsing peers from endorsement policy (see Section 3). For example, the transaction could be sent to *all* endorsers of a given chaincodeID. That said, some endorsers could be offline, others may object and choose not to endorse the transaction. The submitting client tries to satisfy the policy expression with the endorsers available.

In the following, we first detail PROPOSE message format and then discuss possible patterns of interaction between submitting client and endorsers.

2.1.1. PROPOSE message format

The format of a PROPOSE message is <PROPOSE,tx,[anchor]>, where tx is a mandatory and anchor optional argument explained in the following.

- tx=<clientID,chaincodeID,txPayload,timestamp,clientSig>, where
  - clientID is an ID of the submitting client,
  - chaincodeID refers to the chaincode to which the transaction pertains,
  - txPayload is the payload containing the submitted transaction itself,
  - timestamp is a monotonically increasing (for every new transaction) integer maintained by the client,
  - clientSig is signature of a client on other fields of tx.

  The details of txPayload will differ between invoke transactions and deploy transactions (i.e., invoke transactions referring to a deploy-specific system chaincode). For an **invoke transaction**, txPayload would consist of two fields
  - txPayload = <operation, metadata>, where
    - operation denotes the chaincode operation (function) and arguments,
    - metadata denotes attributes related to the invocation.

  For a **deploy transaction**, txPayload would consist of three fields
  - txPayload = <source, metadata, policies>, where
    - source denotes the source code of the chaincode,
    - metadata denotes attributes related to the chaincode and application,
    - policies contains policies related to the chaincode that are accessible to all peers, such as the endorsement policy. Note that endorsement policies are not supplied with txPayload in a deploy transaction, but txPayload of a deploy contains endorsement policy ID and its parameters (see Section 3).
- anchor contains *read version dependencies*, or more specifically, key-version pairs (i.e., anchor is a subset of KxN), that binds or "anchors" the PROPOSE request to specified versions of keys in a KVS (see Section 1.2.). If the client specifies the anchor argument, an endorser endorses a transaction only upon *read* version numbers of corresponding keys in its local KVS match anchor (see Section 2.2. for more details).

Cryptographic hash of tx is used by all nodes as a unique transaction identifier tid (i.e., tid=HASH(tx)). The client stores tid in memory and waits for responses from endorsing peers.

2.1.2. Message patterns

The client decides on the sequence of interaction with endorsers. For example, a client would typically send <PROPOSE, tx> (i.e., without the anchor argument) to a single endorser, which would then produce the version dependencies (anchor) which the client can later on use as an argument of its PROPOSE message to other endorsers. As another example, the client could directly send <PROPOSE, tx> (without anchor) to all endorsers of its choice. Different patterns of communication are possible and client is free to decide on those (see also Section 2.3.).

2.2. The endorsing peer simulates a transaction and produces an endorsement signature

On reception of a <PROPOSE,tx,[anchor]> message from a client, the endorsing peer epID first verifies the client's signature clientSig and then simulates a transaction. If the client specifies anchor then endorsing peer simulates the transactions only upon read version numbers (i.e., readset as defined below) of corresponding keys in its local KVS match those version numbers specified by anchor.

Simulating a transaction involves endorsing peer tentatively *executing* a transaction (txPayload), by invoking the chaincode to which the transaction refers (chaincodeID) and the copy of the state that the endorsing peer locally holds.

As a result of the execution, the endorsing peer computes *read version dependencies* (readset) and *state updates* (writeset), also called *MVCC+postimage info* in DB language.

Recall that the state consists of key-value pairs. All key-value entries are versioned; that is, every entry contains ordered version information, which is incremented each time the value stored under a key is updated. The peer that interprets the transaction records all key-value pairs accessed by the chaincode, either for reading or for writing, but the peer does not yet update its state. More specifically:

- Given state s before an endorsing peer executes a transaction, for every key k read by the transaction, pair (k,s(k).version) is added to readset.
- Additionally, for every key k modified by the transaction to the new value v', pair (k,v') is added to writeset. Alternatively, v' could be the delta of the new value to previous value (s(k).value).

If a client specifies anchor in the PROPOSE message then client specified anchor must equal readset produced by endorsing peer when simulating the transaction.

Then, the peer forwards internally tran-proposal (and possibly tx) to the part of its (peer's) logic that endorses a transaction, referred to as **endorsing logic**. By default, endorsing logic at a peer accepts the tran-proposal and simply signs the tran-proposal. However, endorsing logic may interpret arbitrary functionality, to, e.g., interact with legacy systems with tran-proposal and tx as inputs to reach the decision whether to endorse a transaction or not.

If endorsing logic decides to endorse a transaction, it sends <TRANSACTION-ENDORSED, tid, tran-proposal,epSig> message to the submitting client(tx.clientID), where:

- tran-proposal := (epID,tid,chaincodeID,txContentBlob,readset,writeset),

  where txContentBlob is chaincode/transaction specific information. The intention is to have txContentBlob used as some representation of tx (e.g., txContentBlob=tx.txPayload).
- epSig is the endorsing peer's signature on tran-proposal

Else, in case the endorsing logic refuses to endorse the transaction, an endorser *may* send a message (TRANSACTION-INVALID, tid, REJECTED) to the submitting client.

Notice that an endorser does not change its state in this step, the updates produced by transaction simulation in the context of endorsement do not affect the state!

2.3. The submitting client collects an endorsement for a transaction and broadcasts it through ordering service

The submitting client waits until it receives "enough" messages and signatures on `(TRANSACTION-ENDORSED, tid, *, *)` statements to conclude that the transaction proposal is endorsed. As discussed in Section 2.1.2., this may involve one or more round-trips of interaction with endorsers.

The exact number of "enough" depend on the chaincode endorsement policy (see also Section 3). If the endorsement policy is satisfied, the transaction has been *endorsed*; note that it is not yet committed. The collection of signed `TRANSACTION-ENDORSED` messages from endorsing peers which establish that a transaction is endorsed is called an *endorsement* and denoted by `endorsement`.

If the submitting client does not manage to collect an endorsement for a transaction proposal, it abandons this transaction with an option to retry later.

For transaction with a valid endorsement, we now start using the ordering service. The submitting client invokes ordering service using the `broadcast(blob)`, where `blob=endorsement`. If the client does not have capability of invoking ordering service directly, it may proxy its broadcast through some peer of its choice. Such a peer must be trusted by the client not to remove any message from the `endorsement` or otherwise the transaction may be deemed invalid. Notice that, however, a proxy peer may not fabricate a valid `endorsement`.

2.4. The ordering service delivers a transactions to the peers

When an event `deliver(seqno, prevhash, blob)` occurs and a peer has applied all state updates for blobs with sequence number lower than `seqno`, a peer does the following:

- It checks that the `blob.endorsement` is valid according to the policy of the chaincode (`blob.tran-proposal.chaincodeID`) to which it refers.
- In a typical case, it also verifies that the dependencies (`blob.endorsement.tran-proposal.readset`) have not been violated meanwhile. In more complex use cases, `tran-proposal` fields in endorsement may differ and in this case endorsement policy (Section 3) specifies how the state evolves.

Verification of dependencies can be implemented in different ways, according to a consistency property or "isolation guarantee" that is chosen for the state updates. **Serializability** is a default isolation guarantee, unless chaincode endorsement policy specifies a different one. Serializability can be provided by requiring the version associated with *every* key in the `readset` to be equal to that key's version in the state, and rejecting transactions that do not satisfy this requirement.

- If all these checks pass, the transaction is deemed *valid* or *committed*. In this case, the peer marks the transaction with 1 in the bitmask of the `PeerLedger`, applies `blob.endorsement.tran-proposal.writeset` to blockchain state (if `tran-proposals` are the same, otherwise endorsement policy logic defines the function that takes `blob.endorsement`).
- If the endorsement policy verification of `blob.endorsement` fails, the transaction is invalid and the peer marks the transaction with 0 in the bitmask of the `PeerLedger`. It is important to note that invalid transactions do not change the state.

Note that this is sufficient to have all (correct) peers have the same state after processing a deliver event (block) with a given sequence number. Namely, by the guarantees of the ordering service, all correct peers will receive an identical sequence of `deliver(seqno, prevhash, blob)` events. As the evaluation of the endorsement policy and evaluation of version dependencies in `readset` are deterministic, all correct peers will also come to the same conclusion whether a transaction contained in a blob is valid. Hence, all peers commit and apply the same sequence of transactions and update their state in the same way.

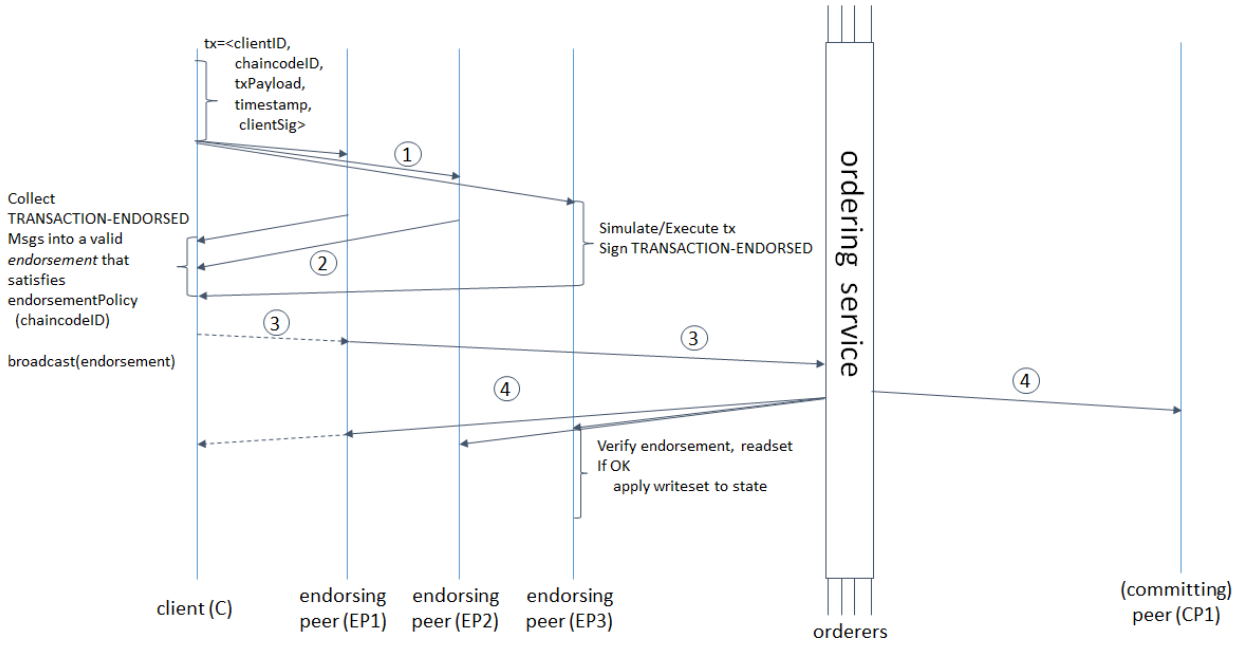


Figure 1. Illustration of one possible transaction flow (common-case path).

9.1.3 3. Endorsement policies

3.1. Endorsement policy specification

An **endorsement policy**, is a condition on what *endorses* a transaction. Blockchain peers have a pre-specified set of endorsement policies, which are referenced by a `deploy` transaction that installs specific chaincode. Endorsement policies can be parametrized, and these parameters can be specified by a `deploy` transaction.

To guarantee blockchain and security properties, the set of endorsement policies **should be a set of proven policies** with limited set of functions in order to ensure bounded execution time (termination), determinism, performance and security guarantees.

Dynamic addition of endorsement policies (e.g., by `deploy` transaction on chaincode deploy time) is very sensitive in terms of bounded policy evaluation time (termination), determinism, performance and security guarantees. Therefore, dynamic addition of endorsement policies is not allowed, but can be supported in future.

3.2. Transaction evaluation against endorsement policy

A transaction is declared valid only if it has been endorsed according to the policy. An invoke transaction for a chaincode will first have to obtain an *endorsement* that satisfies the chaincode's policy or it will not be committed. This takes place through the interaction between the submitting client and endorsing peers as explained in Section 2.

Formally the endorsement policy is a predicate on the endorsement, and potentially further state that evaluates to TRUE or FALSE. For deploy transactions the endorsement is obtained according to a system-wide policy (for example, from the system chaincode).

An endorsement policy predicate refers to certain variables. Potentially it may refer to:

1. keys or identities relating to the chaincode (found in the metadata of the chaincode), for example, a set of endorsers;
2. further metadata of the chaincode;

3. elements of the `endorsement` and `endorsement.tran-proposal`;
4. and potentially more.

The above list is ordered by increasing expressiveness and complexity, that is, it will be relatively simple to support policies that only refer to keys and identities of nodes.

The evaluation of an endorsement policy predicate must be deterministic. An endorsement shall be evaluated locally by every peer such that a peer does *not* need to interact with other peers, yet all correct peers evaluate the endorsement policy in the same way.

3.3. Example endorsement policies

The predicate may contain logical expressions and evaluates to TRUE or FALSE. Typically the condition will use digital signatures on the transaction invocation issued by endorsing peers for the chaincode.

Suppose the chaincode specifies the endorser set `E = {Alice, Bob, Charlie, Dave, Eve, Frank, George}`. Some example policies:

- A valid signature from on the same `tran-proposal` from all members of E.
- A valid signature from any single member of E.
- Valid signatures on the same `tran-proposal` from endorsing peers according to the condition `(Alice OR Bob) AND (any two of: Charlie, Dave, Eve, Frank, George)`.
- Valid signatures on the same `tran-proposal` by any 5 out of the 7 endorsers. (More generally, for chaincode with `n > 3f` endorsers, valid signatures by any `2f+1` out of the `n` endorsers, or by any group of *more* than `(n+f)/2` endorsers.)
- Suppose there is an assignment of "stake" or "weights" to the endorsers, like `{Alice=49, Bob=15, Charlie=15, Dave=10, Eve=7, Frank=3, George=1}`, where the total stake is 100: The policy requires valid signatures from a set that has a majority of the stake (i.e., a group with combined stake strictly more than 50), such as `{Alice, X}` with any `X` different from George, or `{everyone together except Alice}`. And so on.
- The assignment of stake in the previous example condition could be static (fixed in the metadata of the chaincode) or dynamic (e.g., dependent on the state of the chaincode and be modified during the execution).
- Valid signatures from (Alice OR Bob) on `tran-proposal1` and valid signatures from `(any two of: Charlie, Dave, Eve, Frank, George)` on `tran-proposal2`, where `tran-proposal1` and `tran-proposal2` differ only in their endorsing peers and state updates.

How useful these policies are will depend on the application, on the desired resilience of the solution against failures or misbehavior of endorsers, and on various other properties.

9.1.4 4 (post-v1). Validated ledger and `PeerLedger` checkpointing (pruning)

4.1. Validated ledger (VLedger)

To maintain the abstraction of a ledger that contains only valid and committed transactions (that appears in Bitcoin, for example), peers may, in addition to state and Ledger, maintain the *Validated Ledger (or VLedger)*. This is a hash chain derived from the ledger by filtering out invalid transactions.

The construction of the VLedger blocks (called here *vBlocks*) proceeds as follows. As the `PeerLedger` blocks may contain invalid transactions (i.e., transactions with invalid endorsement or with invalid version dependencies), such transactions are filtered out by peers before a transaction from a block becomes added to a vBlock. Every peer does this by itself (e.g., by using the bitmask associated with `PeerLedger`). A vBlock is defined as a block without the

invalid transactions, that have been filtered out. Such vBlocks are inherently dynamic in size and may be empty. An illustration of vBlock construction is given in the figure below.

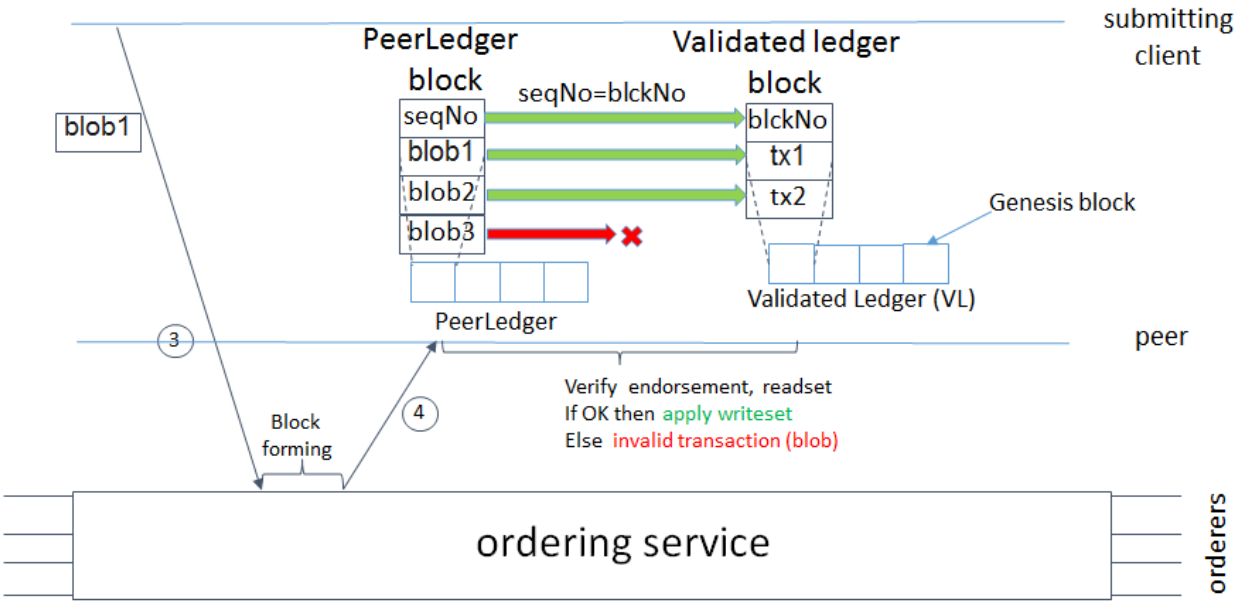


Figure 2. Illustration of validated ledger block (vBlock) formation from ledger (PeerLedger) blocks.

vBlocks are chained together to a hash chain by every peer. More specifically, every block of a validated ledger contains:

- The hash of the previous vBlock.
- vBlock number.
- An ordered list of all valid transactions committed by the peers since the last vBlock was computed (i.e., list of valid transactions in a corresponding block).
- The hash of the corresponding block (in `PeerLedger`) from which the current vBlock is derived.

All this information is concatenated and hashed by a peer, producing the hash of the vBlock in the validated ledger.

4.2. `PeerLedger` Checkpointing

The ledger contains invalid transactions, which may not necessarily be recorded forever. However, peers cannot simply discard `PeerLedger` blocks and thereby prune `PeerLedger` once they establish the corresponding vBlocks. Namely, in this case, if a new peer joins the network, other peers could not transfer the discarded blocks (pertaining to `PeerLedger`) to the joining peer, nor convince the joining peer of the validity of their vBlocks.

To facilitate pruning of the `PeerLedger`, this document describes a *checkpointing* mechanism. This mechanism establishes the validity of the vBlocks across the peer network and allows checkpointed vBlocks to replace the discarded `PeerLedger` blocks. This, in turn, reduces storage space, as there is no need to store invalid transactions. It also reduces the work to reconstruct the state for new peers that join the network (as they do not need to establish validity of individual transactions when reconstructing the state by replaying `PeerLedger`, but may simply replay the state updates contained in the validated ledger).

4.2.1. Checkpointing protocol

Checkpointing is performed periodically by the peers every *CHK* blocks, where *CHK* is a configurable parameter. To initiate a checkpoint, the peers broadcast (e.g., gossip) to other peers message `<CHECKPOINT,blocknohash, blockno,stateHash,peerSig>`, where `blockno` is the current blocknumber and `blocknohash` is its respective hash, `stateHash` is the hash of the latest state (produced by e.g., a Merkle hash) upon validation of block `blockno` and `peerSig` is peer's signature on `(CHECKPOINT,blocknohash,blockno,stateHash)`, referring to the validated ledger.

A peer collects `CHECKPOINT` messages until it obtains enough correctly signed messages with matching `blockno`, `blocknohash` and `stateHash` to establish a *valid checkpoint* (see Section 4.2.2.).

Upon establishing a valid checkpoint for block number `blockno` with `blocknohash`, a peer:

- if `blockno>latestValidCheckpoint.blockno`, then a peer assigns `latestValidCheckpoint=(blocknohash,blockno)`,
- stores the set of respective peer signatures that constitute a valid checkpoint into the set `latestValidCheckpointProof`,
- stores the state corresponding to `stateHash` to `latestValidCheckpointedState`,
- (optionally) prunes its `PeerLedger` up to block number `blockno` (inclusive).

4.2.2. Valid checkpoints

Clearly, the checkpointing protocol raises the following questions: *When can a peer prune its ''PeerLedger''? How many ''CHECKPOINT'' messages are "sufficiently many"?*. This is defined by a *checkpoint validity policy*, with (at least) two possible approaches, which may also be combined:

- *Local (peer-specific) checkpoint validity policy (LCVP).* A local policy at a given peer *p* may specify a set of peers which peer *p* trusts and whose `CHECKPOINT` messages are sufficient to establish a valid checkpoint. For example, LCVP at peer *Alice* may define that *Alice* needs to receive `CHECKPOINT` message from Bob, or from *both Charlie* and *Dave*.
- *Global checkpoint validity policy (GCVP).* A checkpoint validity policy may be specified globally. This is similar to a local peer policy, except that it is stipulated at the system (blockchain) granularity, rather than peer granularity. For instance, GCVP may specify that:
  - each peer may trust a checkpoint if confirmed by *11* different peers.
  - in a specific deployment in which every orderer is collocated with a peer in the same machine (i.e., trust domain) and where up to *f* orderers may be (Byzantine) faulty, each peer may trust a checkpoint if confirmed by *f+1* different peers collocated with orderers.

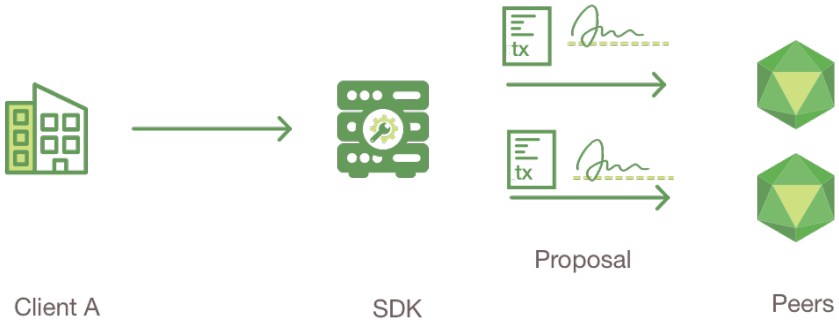
9.2 Transaction Flow

This document outlines the transactional mechanics that take place during a standard asset exchange. The scenario includes two clients, A and B, who are buying and selling radishes. They each have a peer on the network through which they send their transactions and interact with the ledger.

Assumptions

This flow assumes that a channel is set up and running. The application user has registered and enrolled with the organization's certificate authority (CA) and received back necessary cryptographic material, which is used to authenticate to the network.

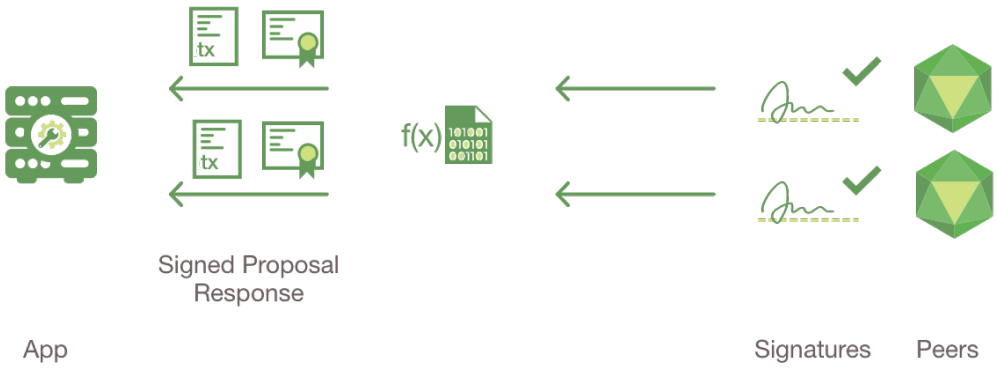
The chaincode (containing a set of key value pairs representing the initial state of the radish market) is installed on the peers and instantiated on the channel. The chaincode contains logic defining a set of transaction instructions and the agreed upon price for a radish. An endorsement policy has also been set for this chaincode, stating that both `peerA` and `peerB` must endorse any transaction.



1. **Client A initiates a transaction**

What's happening? - Client A is sending a request to purchase radishes. The request targets `peerA` and `peerB`, who are respectively representative of Client A and Client B. The endorsement policy states that both peers must endorse any transaction, therefore the request goes to `peerA` and `peerB`.

Next, the transaction proposal is constructed. An application leveraging a supported SDK (Node, Java, Python) utilizes one of the available API's which generates a transaction proposal. The proposal is a request to invoke a chaincode function so that data can be read and/or written to the ledger (i.e. write new key value pairs for the assets). The SDK serves as a shim to package the transaction proposal into the properly architected format (protocol buffer over gRPC) and takes the user's cryptographic credentials to produce a unique signature for this transaction proposal.



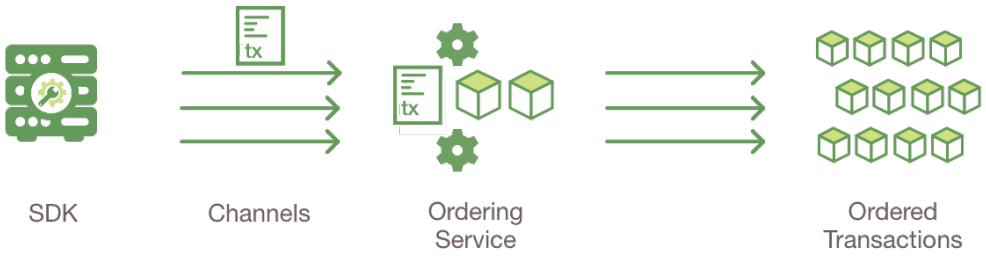
2. **Endorsing peers verify signature & execute the transaction**

The endorsing peers verify (1) that the transaction proposal is well formed, (2) it has not been submitted already in the past (replay-attack protection), (3) the signature is valid (using MSP), and (4) that the submitter (Client A, in the example) is properly authorized to perform the proposed operation on that channel (namely, each endorsing peer ensures that the submitter satisfies the channel's *Writers* policy). The endorsing peers take the transaction proposal inputs as arguments to the invoked chaincode's function. The chaincode is then executed against the current state database to produce transaction results including a response value, read set, and write set. No updates are made to the ledger at this point. The set of these values, along with the endorsing peer's signature is passed back as a "proposal response" to the SDK which parses the payload for the application to consume.

Note: The MSP is a peer component that allows peers to verify transaction requests arriving from clients and to sign transaction results (endorsements). The writing policy is defined at channel creation time and determines which users are entitled to submit a transaction to that channel.

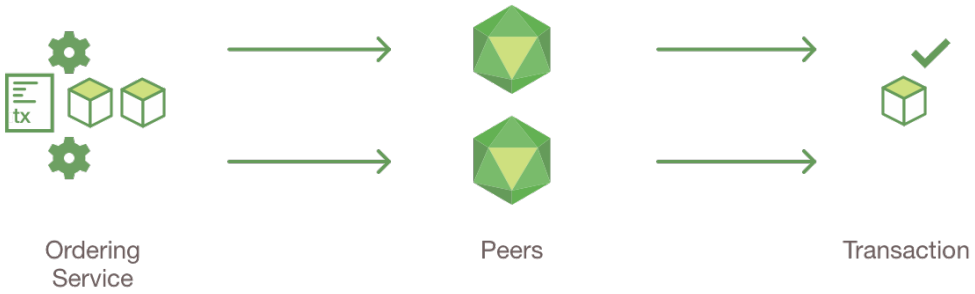
3. **Proposal responses are inspected**

The application verifies the endorsing peer signatures and compares the proposal responses to determine if the proposal responses are the same. If the chaincode only queried the ledger, the application would inspect the query response and would typically not submit the transaction to Ordering Service. If the client application intends to submit the transaction to Ordering Service to update the ledger, the application determines if the specified endorsement policy has been fulfilled before submitting (i.e. did peerA and peerB both endorse). The architecture is such that even if an application chooses not to inspect responses or otherwise forwards an unendorsed transaction, the endorsement policy will still be enforced by peers and upheld at the commit validation phase.



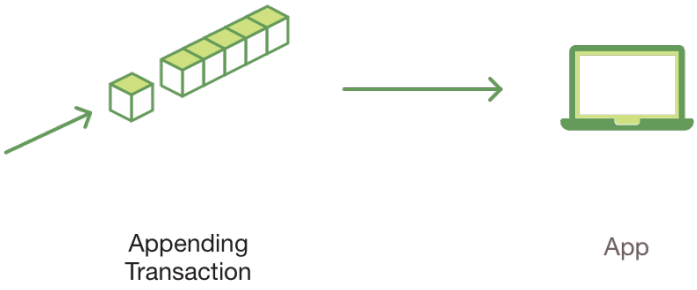
4. **Client assembles endorsements into a transaction**

The application "broadcasts" the transaction proposal and response within a "transaction message" to the Ordering Service. The transaction will contain the read/write sets, the endorsing peers signatures and the Channel ID. The Ordering Service does not need to inspect the entire content of a transaction in order to perform its operation, it simply receives transactions from all channels in the network, orders them chronologically by channel, and creates blocks of transactions per channel.



5. **Transaction is validated and committed**

The blocks of transactions are "delivered" to all peers on the channel. The transactions within the block are validated to ensure endorsement policy is fulfilled and to ensure that there have been no changes to ledger state for read set variables since the read set was generated by the transaction execution. Transactions in the block are tagged as being valid or invalid.



6. **Ledger updated**

Each peer appends the block to the channel's chain, and for each valid transaction the write sets are committed to current state database. An event is emitted, to notify the client application that the transaction (invocation) has been immutably appended to the chain, as well as notification of whether the transaction was validated or invalidated.

Note: See the *sequence diagram* to better understand the transaction flow.

9.3 Hyperledger Fabric SDKs

Hyperledger Fabric intends to offer a number of SDKs for a wide variety of programming languages. The first two delivered are the Node.js and Java SDKs. We hope to provide Python, REST and Go SDKs in a subsequent release.

- Hyperledger Fabric Node SDK documentation.
- Hyperledger Fabric Java SDK documentation.

9.4 Service Discovery

9.4.1 Why do we need service discovery?

In order to execute chaincode on peers, submit transactions to orderers, and to be updated about the status of transactions, applications connect to an API exposed by an SDK.

However, the SDK needs a lot of information in order to allow applications to connect to the relevant network nodes. In addition to the CA and TLS certificates of the orderers and peers on the channel – as well as their IP addresses and port numbers – it must know the relevant endorsement policies as well as which peers have the chaincode installed (so the application knows which peers to send chaincode proposals to).

Prior to v1.2, this information was statically encoded. However, this implementation is not dynamically reactive to network changes (such as the addition of peers who have installed the relevant chaincode, or peers that are temporarily offline). Static configurations also do not allow applications to react to changes of the endorsement policy itself (as might happen when a new organization joins a channel).

In addition, the client application has no way of knowing which peers have updated ledgers and which do not. As a result, the application might submit proposals to peers whose ledger data is not in sync with the rest of the network, resulting in transaction being invalidated upon commit and wasting resources as a consequence.

The **discovery service** improves this process by having the peers compute the needed information dynamically and present it to the SDK in a consumable manner.

9.4.2 How service discovery works in Fabric

The application is bootstrapped knowing about a group of peers which are trusted by the application developer/administrator to provide authentic responses to discovery queries. A good candidate peer to be used by the client application is one that is in the same organization.

The application issues a configuration query to the discovery service and obtains all the static information it would have otherwise needed to communicate with the rest of the nodes of the network. This information can be refreshed at any point by sending a subsequent query to the discovery service of a peer.

The service runs on peers – not on the application – and uses the network metadata information maintained by the gossip communication layer to find out which peers are online. It also fetches information, such as any relevant endorsement policies, from the peer's state database.

With service discovery, applications no longer need to specify which peers they need endorsements from. The SDK can simply send a query to the discovery service asking which peers are needed given a channel and a chaincode ID. The discovery service will then compute a descriptor comprised of two objects:

1. **Layouts**: a list of groups of peers and a corresponding amount of peers from each group which should be selected.

2. **Group to peer mapping**: from the groups in the layouts to the peers of the channel. In practice, each group would most likely be peers that represent individual organizations, but because the service API is generic and ignorant of organizations this is just a "group".

The following is an example of a descriptor from the evaluation of a policy of `AND(Org1, Org2)` where there are two peers in each of the organizations.

```
Layouts: [
     QuantitiesByGroup: {
       "Org1": 1,
       "Org2": 1,
     }
],
EndorsersByGroups: {
  "Org1": [peer0.org1, peer1.org1],
  "Org2": [peer0.org2, peer1.org2]
}
```

In other words, the endorsement policy requires a signature from one peer in Org1 and one peer in Org2. And it provides the names of available peers in those orgs who can endorse (`peer0` and `peer1` in both Org1 and in Org2).

The SDK then selects a random layout from the list. In the example above, the endorsement policy is Org1 `AND` Org2. If instead it was an `OR` policy, the SDK would randomly select either Org1 or Org2, since a signature from a peer from either Org would satisfy the policy.

After the SDK has selected a layout, it selects from the peers in the layout based on a criteria specified on the client side (the SDK can do this because it has access to metadata like ledger height). For example, it can prefer peers with higher ledger heights over others – or to exclude peers that the application has discovered to be offline – according to the number of peers from each group in the layout. If no single peer is preferable based on the criteria, the SDK will randomly select from the peers that best meet the criteria.

Capabilities of the discovery service

The discovery service can respond to the following queries:

- **Configuration query**: Returns the `MSPConfig` of all organizations in the channel along with the orderer endpoints of the channel.
- **Peer membership query**: Returns the peers that have joined the channel.
- **Endorsement query**: Returns an endorsement descriptor for given chaincode(s) in a channel.
- **Local peer membership query**: Returns the local membership information of the peer that responds to the query. By default the client needs to be an administrator for the peer to respond to this query.

Special requirements

When the peer is running with TLS enabled the client must provide a TLS certificate when connecting to the peer. If the peer isn't configured to verify client certificates (clientAuthRequired is false), this TLS certificate can be self-signed.

9.5 Channels

A Hyperledger Fabric `channel` is a private "subnet" of communication between two or more specific network members, for the purpose of conducting private and confidential transactions. A channel is defined by members (organizations), anchor peers per member, the shared ledger, chaincode application(s) and the ordering service node(s). Each

transaction on the network is executed on a channel, where each party must be authenticated and authorized to transact on that channel. Each peer that joins a channel, has its own identity given by a membership services provider (MSP), which authenticates each peer to its channel peers and services.

To create a new channel, the client SDK calls configuration system chaincode and references properties such as `anchor peers`, and members (organizations). This request creates a `genesis block` for the channel ledger, which stores configuration information about the channel policies, members and anchor peers. When adding a new member to an existing channel, either this genesis block, or if applicable, a more recent reconfiguration block, is shared with the new member.

Note: See the *Channel Configuration (configtx)* section for more details on the properties and proto structures of config transactions.

The election of a `leading peer` for each member on a channel determines which peer communicates with the ordering service on behalf of the member. If no leader is identified, an algorithm can be used to identify the leader. The consensus service orders transactions and delivers them, in a block, to each leading peer, which then distributes the block to its member peers, and across the channel, using the `gossip` protocol.

Although any one anchor peer can belong to multiple channels, and therefore maintain multiple ledgers, no ledger data can pass from one channel to another. This separation of ledgers, by channel, is defined and implemented by configuration chaincode, the identity membership service and the gossip data dissemination protocol. The dissemination of data, which includes information on transactions, ledger state and channel membership, is restricted to peers with verifiable membership on the channel. This isolation of peers and ledger data, by channel, allows network members that require private and confidential transactions to coexist with business competitors and other restricted members, on the same blockchain network.

9.6 Capability Requirements

Because Fabric is a distributed system that will usually involve multiple organizations (sometimes in different countries or even continents), it is possible (and typical) that many different versions of Fabric code will exist in the network. Nevertheless, it's vital that networks process transactions in the same way so that everyone has the same view of the current network state.

This means that every network – and every channel within that network – must define a set of what we call "capabilities" to be able to participate in processing transactions. For example, Fabric v1.1 introduces new MSP role types of "Peer" and "Client". However, if a v1.0 peer does not understand these new role types, it will not be able to appropriately evaluate an endorsement policy that references them. This means that before the new role types may be used, the network must agree to enable the v1.1 `channel` capability requirement, ensuring that all peers come to the same decision.

Only binaries which support the required capabilities will be able to participate in the channel, and newer binary versions will not enable new validation logic until the corresponding capability is enabled. In this way, capability requirements ensure that even with disparate builds and versions, it is not possible for the network to suffer a state fork.

9.6.1 Defining Capability Requirements

Capability requirements are defined per channel in the channel configuration (found in the channel's most recent configuration block). The channel configuration contains three locations, each of which defines a capability of a different type.

Capability Type	Canonical Path	JSON Path
Channel	/Channel/Capabilities	.channel_group.values.Capabilities
Orderer	/Channel/Orderer/Capabilities	.channel_group.groups.Orderer.values.Capabilities
Application	/Channel/Application/Capabilities	.channel_group.groups.Application.values. Capabilities

- **Channel:** these capabilities apply to both peer and orderers and are located in the root `Channel` group.
- **Orderer:** apply to orderers only and are located in the `Orderer` group.
- **Application:** apply to peers only and are located in the `Application` group.

The capabilities are broken into these groups in order to align with the existing administrative structure. Updating orderer capabilities is something the ordering orgs would manage independent of the application orgs. Similarly, updating application capabilities is something only the application admins would manage. By splitting the capabilities between "Orderer" and "Application", a hypothetical network could run a v1.6 ordering service while supporting a v1.3 peer application network.

However, some capabilities cross both the 'Application' and 'Orderer' groups. As we saw earlier, adding a new MSP role type is something both the orderer and application admins agree to and need to recognize. The orderer must understand the meaning of MSP roles in order to allow the transactions to pass through ordering, while the peers must understand the roles in order to validate the transaction. These kinds of capabilities – which span both the application and orderer components – are defined in the top level "Channel" group.

Note: It is possible that the channel capabilities are defined to be at version v1.3 while the orderer and application capabilities are defined to be at version 1.1 and v1.4, respectively. Enabling a capability at the "Channel" group level does not imply that this same capability is available at the more specific "Orderer" and "Application" group levels.

9.6.2 Setting Capabilities

Capabilities are set as part of the channel configuration (either as part of the initial configuration – which we'll talk about in a moment – or as part of a reconfiguration).

Note: We have a two documents that talk through different aspects of channel reconfigurations. First, we have a tutorial that will take you through the process of *Adding an Org to a Channel*. And we also have a document that talks through *Updating a Channel Configuration* which gives an overview of the different kinds of updates that are possible as well as a fuller look at the signature process.

Because new channels copy the configuration of the Orderer System Channel by default, new channels will automatically be configured to work with the orderer and channel capabilities of the Orderer System Channel and the application capabilities specified by the channel creation transaction. Channels that already exist, however, must be reconfigured.

The schema for the Capabilities value is defined in the protobuf as:

```
message Capabilities {
      map<string, Capability> capabilities = 1;
}

message Capability { }
```

As an example, rendered in JSON:

```
{
    "capabilities": {
        "V1_1": {}
    }
}
```

Capabilities in an Initial Configuration

In the `configtx.yaml` file distributed in the `config` directory of the release artifacts, there is a `Capabilities` section which enumerates the possible capabilities for each capability type (Channel, Orderer, and Application).

The simplest way to enable capabilities is to pick a v1.1 sample profile and customize it for your network. For example:

```
SampleSingleMSPSoloV1_1:
    Capabilities:
        <<: *GlobalCapabilities
    Orderer:
        <<: *OrdererDefaults
        Organizations:
            - *SampleOrg
        Capabilities:
            <<: *OrdererCapabilities
    Consortiums:
        SampleConsortium:
            Organizations:
                - *SampleOrg
```

Note that there is a `Capabilities` section defined at the root level (for the channel capabilities), and at the Orderer level (for orderer capabilities). The sample above uses a YAML reference to include the capabilities as defined at the bottom of the YAML.

When defining the orderer system channel there is no Application section, as those capabilities are defined during the creation of an application channel. To define a new channel's application capabilities at channel creation time, the application admins should model their channel creation transaction after the `SampleSingleMSPChannelV1_1` profile.

```
SampleSingleMSPChannelV1_1:
     Consortium: SampleConsortium
     Application:
         Organizations:
             - *SampleOrg
         Capabilities:
             <<: *ApplicationCapabilities
```

Here, the Application section has a new element `Capabilities` which references the `ApplicationCapabilities` section defined at the end of the YAML.

Note: The capabilities for the Channel and Orderer sections are inherited from the definition in the ordering system channel and are automatically included by the orderer during the process of channel creation.

9.7 CouchDB as the State Database

9.7.1 State Database options

State database options include LevelDB and CouchDB. LevelDB is the default key-value state database embedded in the peer process. CouchDB is an optional alternative external state database. Like the LevelDB key-value store, CouchDB can store any binary data that is modeled in chaincode (CouchDB attachment functionality is used internally for non-JSON binary data). But as a JSON document store, CouchDB additionally enables rich query against the chaincode data, when chaincode values (e.g. assets) are modeled as JSON data.

Both LevelDB and CouchDB support core chaincode operations such as getting and setting a key (asset), and querying based on keys. Keys can be queried by range, and composite keys can be modeled to enable equivalence queries against multiple parameters. For example a composite key of `owner,asset_id` can be used to query all assets owned by a certain entity. These key-based queries can be used for read-only queries against the ledger, as well as in transactions that update the ledger.

If you model assets as JSON and use CouchDB, you can also perform complex rich queries against the chaincode data values, using the CouchDB JSON query language within chaincode. These types of queries are excellent for understanding what is on the ledger. Proposal responses for these types of queries are typically useful to the client application, but are not typically submitted as transactions to the ordering service. In fact, there is no guarantee the result set is stable between chaincode execution and commit time for rich queries, and therefore rich queries are not appropriate for use in update transactions, unless your application can guarantee the result set is stable between chaincode execution time and commit time, or can handle potential changes in subsequent transactions. For example, if you perform a rich query for all assets owned by Alice and transfer them to Bob, a new asset may be assigned to Alice by another transaction between chaincode execution time and commit time, and you would miss this "phantom" item.

CouchDB runs as a separate database process alongside the peer, therefore there are additional considerations in terms of setup, management, and operations. You may consider starting with the default embedded LevelDB, and move to CouchDB if you require the additional complex rich queries. It is a good practice to model chaincode asset data as JSON, so that you have the option to perform complex rich queries if needed in the future.

Note: The key for a CouchDB JSON document cannot begin with an underscore ("_"). Also, a JSON document cannot use the following field names at the top level. These are reserved for internal use.

- `Any field beginning with an underscore, "_"`
- `~version`

9.7.2 Using CouchDB from Chaincode

Chaincode queries

Most of the chaincode shim APIs can be utilized with either LevelDB or CouchDB state database, e.g. `GetState`, `PutState`, `GetStateByRange`, `GetStateByPartialCompositeKey`. Additionally when you utilize CouchDB as the state database and model assets as JSON in chaincode, you can perform rich queries against the JSON in the state database by using the `GetQueryResult` API and passing a CouchDB query string. The query string follows the CouchDB JSON query syntax.

The marbles02 fabric sample demonstrates use of CouchDB queries from chaincode. It includes a `queryMarblesByOwner()` function that demonstrates parameterized queries by passing an owner id into chaincode. It then queries the state data for JSON documents matching the docType of "marble" and the owner id using the JSON query syntax:

```
{"selector":{"docType":"marble","owner":<OWNER_ID>}}
```

CouchDB pagination

Fabric supports paging of query results for rich queries and range based queries. APIs supporting pagination allow the use of page size and bookmarks to be used for both range and rich queries.

If a pagesize is specified using the paginated query APIs (`GetStateByRangeWithPagination`, `GetStateByPartialCompositeKeyWithPagination()`, and `GetQueryResultWithPagination()`), a set of results will be returned along with a bookmark. The bookmark can be used with a follow on query to receive the next "page" of results.

All chaincode queries are bound by `totalQueryLimit` (default 100000) from `core.yaml`. This is the maximum number of results that chaincode will iterate through and return to the client, in order to avoid accidental or malicious long-running queries.

An example using pagination is included in the *Using CouchDB* tutorial.

Note: Regardless of whether chaincode uses paginated queries or not, the peer will query CouchDB in batches based on `internalQueryLimit` (default 1000) from `core.yaml`. This behavior ensures reasonably sized result sets are passed between the peer and CouchDB, and is transparent to chaincode and requires no additional configuration.

CouchDB indexes

Indexes in CouchDB are required in order to make JSON queries efficient and are required for any JSON query with a sort. Indexes can be packaged alongside chaincode in a `/META-INF/statedb/couchdb/indexes` directory. Each index must be defined in its own text file with extension `*.json` with the index definition formatted in JSON following the CouchDB index JSON syntax. For example, to support the above marble query, a sample index on the `docType` and `owner` fields is provided:

```
{"index":{"fields":["docType","owner"]},"ddoc":"indexOwnerDoc", "name":"indexOwner",
↪"type":"json"}
```

The sample index can be found here.

Any index in the chaincode's `META-INF/statedb/couchdb/indexes` directory will be packaged up with the chaincode for deployment. When the chaincode is both installed on a peer and instantiated on one of the peer's channels, the index will automatically be deployed to the peer's channel and chaincode specific state database (if it has been configured to use CouchDB). If you install the chaincode first and then instantiate the chaincode on the channel, the index will be deployed at chaincode **instantiation** time. If the chaincode is already instantiated on a channel and you later install the chaincode on a peer, the index will be deployed at chaincode **installation** time.

Upon deployment, the index will automatically be utilized by chaincode queries. CouchDB can automatically determine which index to use based on the fields being used in a query. Alternatively, in the selector query the index can be specified using the `use_index` keyword.

The same index may exist in subsequent versions of the chaincode that gets installed. To change the index, use the same index name but alter the index definition. Upon installation/instantiation, the index definition will get re-deployed to the peer's state database.

If you have a large volume of data already, and later install the chaincode, the index creation upon installation may take some time. Similarly, if you have a large volume of data already and instantiate a subsequent version of the chaincode, the index creation may take some time. Avoid calling chaincode functions that query the state database at these times

as the chaincode query may time out while the index is getting initialized. During transaction processing, the indexes will automatically get refreshed as blocks are committed to the ledger.

9.7.3 CouchDB Configuration

CouchDB is enabled as the state database by changing the `stateDatabase` configuration option from goleveldb to CouchDB. Additionally, the `couchDBAddress` needs to configured to point to the CouchDB to be used by the peer. The username and password properties should be populated with an admin username and password if CouchDB is configured with a username and password. Additional options are provided in the `couchDBConfig` section and are documented in place. Changes to the *core.yaml* will be effective immediately after restarting the peer.

You can also pass in docker environment variables to override core.yaml values, for example `CORE_LEDGER_STATE_STATEDATABASE` and `CORE_LEDGER_STATE_COUCHDBCONFIG_COUCHDBADDRESS`.

Below is the `stateDatabase` section from *core.yaml*:

```
state:
  # stateDatabase - options are "goleveldb", "CouchDB"
  # goleveldb - default state database stored in goleveldb.
  # CouchDB - store state database in CouchDB
  stateDatabase: goleveldb
  # Limit on the number of records to return per query
  totalQueryLimit: 10000
  couchDBConfig:
     # It is recommended to run CouchDB on the same server as the peer, and
     # not map the CouchDB container port to a server port in docker-compose.
     # Otherwise proper security must be provided on the connection between
     # CouchDB client (on the peer) and server.
     couchDBAddress: couchdb:5984
     # This username must have read and write authority on CouchDB
     username:
     # The password is recommended to pass as an environment variable
     # during start up (e.g. LEDGER_COUCHDBCONFIG_PASSWORD).
     # If it is stored here, the file must be access control protected
     # to prevent unintended users from discovering the password.
     password:
     # Number of retries for CouchDB errors
     maxRetries: 3
     # Number of retries for CouchDB errors during peer startup
     maxRetriesOnStartup: 10
     # CouchDB request timeout (unit: duration, e.g. 20s)
     requestTimeout: 35s
     # Limit on the number of records per each CouchDB query
     # Note that chaincode queries are only bound by totalQueryLimit.
     # Internally the chaincode may execute multiple CouchDB queries,
     # each of size internalQueryLimit.
     internalQueryLimit: 1000
     # Limit on the number of records per CouchDB bulk update batch
     maxBatchUpdateSize: 1000
     # Warm indexes after every N blocks.
     # This option warms any indexes that have been
     # deployed to CouchDB after every N blocks.
     # A value of 1 will warm indexes after every block commit,
     # to ensure fast selector queries.
     # Increasing the value may improve write efficiency of peer and CouchDB,
     # but may degrade query response time.
     warmIndexesAfterNBlocks: 1
```

CouchDB hosted in docker containers supplied with Hyperledger Fabric have the capability of setting the CouchDB username and password with environment variables passed in with the `COUCHDB_USER` and `COUCHDB_PASSWORD` environment variables using Docker Compose scripting.

For CouchDB installations outside of the docker images supplied with Fabric, the local.ini file of that installation must be edited to set the admin username and password.

Docker compose scripts only set the username and password at the creation of the container. The *local.ini* file must be edited if the username or password is to be changed after creation of the container.

Note: CouchDB peer options are read on each peer startup.

9.8 Peer channel-based event services

9.8.1 General overview

In previous versions of Fabric, the peer event service was known as the event hub. This service sent events any time a new block was added to the peer's ledger, regardless of the channel to which that block pertained, and it was only accessible to members of the organization running the eventing peer (i.e., the one being connected to for events).

Starting with v1.1, there are two new services which provide events. These services use an entirely different design to provide events on a per-channel basis. This means that registration for events occurs at the level of the channel instead of the peer, allowing for fine-grained control over access to the peer's data. Requests to receive events are accepted from identities outside of the peer's organization (as defined by the channel configuration). This also provides greater reliability and a way to receive events that may have been missed (whether due to a connectivity issue or because the peer is joining a network that has already been running).

9.8.2 Available services

- `Deliver`

This service sends entire blocks that have been committed to the ledger. If any events were set by a chaincode, these can be found within the `ChaincodeActionPayload` of the block.

- `DeliverFiltered`

This service sends "filtered" blocks, minimal sets of information about blocks that have been committed to the ledger. It is intended to be used in a network where owners of the peers wish for external clients to primarily receive information about their transactions and the status of those transactions. If any events were set by a chaincode, these can be found within the `FilteredChaincodeAction` of the filtered block.

Note: The payload of chaincode events will not be included in filtered blocks.

9.8.3 How to register for events

Registration for events from either service is done by sending an envelope containing a deliver seek info message to the peer that contains the desired start and stop positions, the seek behavior (block until ready or fail if not ready). There are helper variables `SeekOldest` and `SeekNewest` that can be used to indicate the oldest (i.e. first) block or the newest (i.e. last) block on the ledger. To have the services send events indefinitely, the `SeekInfo` message should include a stop position of `MAXINT64`.

Note: If mutual TLS is enabled on the peer, the TLS certificate hash must be set in the envelope's channel header.

By default, both services use the Channel Readers policy to determine whether to authorize requesting clients for events.

9.8.4 Overview of deliver response messages

The event services send back `DeliverResponse` messages.

Each message contains one of the following:

- status – HTTP status code. Both services will return the appropriate failure code if any failure occurs; otherwise, it will return `200 - SUCCESS` once the service has completed sending all information requested by the `SeekInfo` message.
- block – returned only by the `Deliver` service.
- filtered block – returned only by the `DeliverFiltered` service.

A filtered block contains:

- channel ID.
- number (i.e. the block number).
- array of filtered transactions.
- transaction ID.
  - type (e.g. `ENDORSER_TRANSACTION`, `CONFIG`.
  - transaction validation code.
- **filtered transaction actions.**
  - **array of filtered chaincode actions.**
    - chaincode event for the transaction (with the payload nilled out).

9.8.5 SDK event documentation

For further details on using the event services, refer to the SDK documentation.

9.9 Private Data

Note: This topic assumes an understanding of the conceptual material in the documentation on private data.

9.9.1 Private data collection definition

A collection definition contains one or more collections, each having a policy definition listing the organizations in the collection, as well as properties used to control dissemination of private data at endorsement time and, optionally, whether the data will be purged.

The collection definition gets deployed to the channel at the time of chaincode instantiation (or upgrade). If using the peer CLI to instantiate the chaincode, the collection definition file is passed to the chaincode instantiation using the `--collections-config` flag. If using a client SDK, check the SDK documentation for information on providing the collection definition.

Collection definitions are composed of five properties:

- `name`: Name of the collection.
- `policy`: The private data collection distribution policy defines which organizations' peers are allowed to persist the collection data expressed using the `Signature` policy syntax, with each member being included in an `OR` signature policy list. To support read/write transactions, the private data distribution policy must define a broader set of organizations than the chaincode endorsement policy, as peers must have the private data in order to endorse proposed transactions. For example, in a channel with ten organizations, five of the organizations might be included in a private data collection distribution policy, but the endorsement policy might call for any three of the organizations to endorse.
- `requiredPeerCount`: Minimum number of peers (across authorized organizations) that each endorsing peer must successfully disseminate private data to before the peer signs the endorsement and returns the proposal response back to the client. Requiring dissemination as a condition of endorsement will ensure that private data is available in the network even if the endorsing peer(s) become unavailable. When `requiredPeerCount` is `0`, it means that no distribution is **required**, but there may be some distribution if `maxPeerCount` is greater than zero. A `requiredPeerCount` of `0` would typically not be recommended, as it could lead to loss of private data in the network if the endorsing peer(s) becomes unavailable. Typically you would want to require at least some distribution of the private data at endorsement time to ensure redundancy of the private data on multiple peers in the network.
- `maxPeerCount`: For data redundancy purposes, the maximum number of other peers (across authorized organizations) that each endorsing peer will attempt to distribute the private data to. If an endorsing peer becomes unavailable between endorsement time and commit time, other peers that are collection members but who did not yet receive the private data at endorsement time, will be able to pull the private data from peers the private data was disseminated to. If this value is set to `0`, the private data is not disseminated at endorsement time, forcing private data pulls against endorsing peers on all authorized peers at commit time.
- `blockToLive`: Represents how long the data should live on the private database in terms of blocks. The data will live for this specified number of blocks on the private database and after that it will get purged, making this data obsolete from the network. To keep private data indefinitely, that is, to never purge private data, set the `blockToLive` property to `0`.

Here is a sample collection definition JSON file, containing an array of two collection definitions:

```
[
 {
    "name": "collectionMarbles",
    "policy": "OR('Org1MSP.member', 'Org2MSP.member')",
    "requiredPeerCount": 0,
    "maxPeerCount": 3,
    "blockToLive":1000000
 },
 {
    "name": "collectionMarblePrivateDetails",
    "policy": "OR('Org1MSP.member')",
    "requiredPeerCount": 0,
    "maxPeerCount": 3,
    "blockToLive":3
 }
]
```

This example uses the organizations from the BYFN sample network, `Org1` and `Org2` . The policy in the

`collectionMarbles` definition authorizes both organizations to the private data. This is a typical configuration when the chaincode data needs to remain private from the ordering service nodes. However, the policy in the `collectionMarblePrivateDetails` definition restricts access to a subset of organizations in the channel (in this case `Org1`). In a real scenario, there would be many organizations in the channel, with two or more organizations in each collection sharing private data between them.

Endorsement

Since private data is not included in the transactions that get submitted to the ordering service, and therefore not included in the blocks that get distributed to all peers in a channel, the endorsing peer plays an important role in disseminating private data to other peers of authorized organizations. This ensures the availability of private data in the channel's collection, even if endorsing peers become unavailable after their endorsement. To assist with this dissemination, the `maxPeerCount` and `requiredPeerCount` properties in the collection definition control the degree of dissemination at endorsement time.

If the endorsing peer cannot successfully disseminate the private data to at least the `requiredPeerCount`, it will return an error back to the client. The endorsing peer will attempt to disseminate the private data to peers of different organizations, in an effort to ensure that each authorized organization has a copy of the private data. Since transactions are not committed at chaincode execution time, the endorsing peer and recipient peers store a copy of the private data in a local `transient store` alongside their blockchain until the transaction is committed.

How private data is committed

When authorized peers do not have a copy of the private data in their transient data store at commit time (either because they were not an endorsing peer or because they did not receive the private data via dissemination at endorsement time), they will attempt to pull the private data from another authorized peer, *for a configurable amount of time* based on the peer property `peer.gossip.pvtData.pullRetryThreshold` in the peer configuration `core.yaml` file.

Note: The peers being asked for private data will only return the private data if the requesting peer is a member of the collection as defined by the private data dissemination policy.

Considerations when using `pullRetryThreshold`:

- If the requesting peer is able to retrieve the private data within the `pullRetryThreshold`, it will commit the transaction to its ledger (including the private data hash), and store the private data in its state database, logically separated from other channel state data.
- If the requesting peer is not able to retrieve the private data within the `pullRetryThreshold`, it will commit the transaction to it's blockchain (including the private data hash), without the private data.
- If the peer was entitled to the private data but it is missing, then that peer will not be able to endorse future transactions that reference the missing private data - a chaincode query for a key that is missing will be detected (based on the presence of the key's hash in the state database), and the chaincode will receive an error.

Therefore, it is important to set the `requiredPeerCount` and `maxPeerCount` properties large enough to ensure the availability of private data in your channel. For example, if each of the endorsing peers become unavailable before the transaction commits, the `requiredPeerCount` and `maxPeerCount` properties will have ensured the private data is available on other peers.

Note: For collections to work, it is important to have cross organizational gossip configured correctly. Refer to our documentation on *Gossip data dissemination protocol*, paying particular attention to the section on "anchor peers".

9.9.2 Referencing collections from chaincode

A set of shim APIs are available for setting and retrieving private data.

The same chaincode data operations can be applied to channel state data and private data, but in the case of private data, a collection name is specified along with the data in the chaincode APIs, for example `PutPrivateData(collection,key,value)` and `GetPrivateData(collection,key)`.

A single chaincode can reference multiple collections.

How to pass private data in a chaincode proposal

Since the chaincode proposal gets stored on the blockchain, it is also important not to include private data in the main part of the chaincode proposal. A special field in the chaincode proposal called the `transient` field can be used to pass private data from the client (or data that chaincode will use to generate private data), to chaincode invocation on the peer. The chaincode can retrieve the `transient` field by calling the GetTransient() API. This `transient` field gets excluded from the channel transaction.

9.9.3 Considerations when using private data

Querying Private Data

Private collection data can be queried just like normal channel data, using shim APIs:

- `GetPrivateDataByRange(collection, startKey, endKey string)`
- `GetPrivateDataByPartialCompositeKey(collection, objectType string, keys []string)`

And for the CouchDB state database, JSON content queries can be passed using the shim API:

- `GetPrivateDataQueryResult(collection, query string)`

Limitations:

- Clients that call chaincode that executes range or rich JSON queries should be aware that they may receive a subset of the result set, if the peer they query has missing private data, based on the explanation in Private Data Dissemination section above. Clients can query multiple peers and compare the results to determine if a peer may be missing some of the result set.
- Chaincode that executes range or rich JSON queries and updates data in a single transaction is not supported, as the query results cannot be validated on the peers that don't have access to the private data, or on peers that are missing the private data that they have access to. If a chaincode invocation both queries and updates private data, the proposal request will return an error. If your application can tolerate result set changes between chaincode execution and validation/commit time, then you could call one chaincode function to perform the query, and then call a second chaincode function to make the updates. Note that calls to GetPrivateData() to retrieve individual keys can be made in the same transaction as PutPrivateData() calls, since all peers can validate key reads based on the hashed key version.
- Note that private data collections only define which organization's peers are authorized to receive and store private data, and consequently implies which peers can be used to query private data. Private data collections do not by themselves limit access control within chaincode. For example if non-authorized clients are able to invoke chaincode on peers that have access to the private data, the chaincode logic still needs a means to enforce access control as usual, for example by calling the GetCreator() chaincode API or using the client identity chaincode library .

9.9.4 Using Indexes with collections

The topic *CouchDB as the State Database* describes indexes that can be applied to the channel's state database to enable JSON content queries, by packaging indexes in a `META-INF/statedb/couchdb/indexes` directory at chaincode installation time. Similarly, indexes can also be applied to private data collections, by packaging indexes in a `META-INF/statedb/couchdb/collections/<collection_name>/indexes` directory. An example index is available here.

Private Data Purging

To keep private data indefinitely, that is, to never purge private data, set `blockToLive` property to `0`.

Recall that prior to commit, peers store private data in a local transient data store. This data automatically gets purged when the transaction commits. But if a transaction was never submitted to the channel and therefore never committed, the private data would remain in each peer's transient store. This data is purged from the transient store after a configurable number blocks by using the peer's `peer.gossip.pvtData.transientstoreMaxBlockRetention` property in the peer `core.yaml` file.

9.9.5 Upgrading a collection definition

If a collection is referenced by a chaincode, the chaincode will use the prior collection definition unless a new collection definition is specified at upgrade time. If a collection configuration is specified during the upgrade, a definition for each of the existing collections must be included, and you can add new collection definitions.

Collection updates becomes effective when a peer commits the block that contains the chaincode upgrade transaction. Note that collections cannot be deleted, as there may be prior private data hashes on the channel's blockchain that cannot be removed.

9.10 Read-Write set semantics

This document discusses the details of the current implementation about the semantics of read-write sets.

9.10.1 Transaction simulation and read-write set

During simulation of a transaction at an `endorser`, a read-write set is prepared for the transaction. The `read set` contains a list of unique keys and their committed versions that the transaction reads during simulation. The `write set` contains a list of unique keys (though there can be overlap with the keys present in the read set) and their new values that the transaction writes. A delete marker is set (in the place of new value) for the key if the update performed by the transaction is to delete the key.

Further, if the transaction writes a value multiple times for a key, only the last written value is retained. Also, if a transaction reads a value for a key, the value in the committed state is returned even if the transaction has updated the value for the key before issuing the read. In another words, Read-your-writes semantics are not supported.

As noted earlier, the versions of the keys are recorded only in the read set; the write set just contains the list of unique keys and their latest values set by the transaction.

There could be various schemes for implementing versions. The minimal requirement for a versioning scheme is to produce non-repeating identifiers for a given key. For instance, using monotonically increasing numbers for versions can be one such scheme. In the current implementation, we use a blockchain height based versioning scheme in which the height of the committing transaction is used as the latest version for all the keys modified by the transaction. In this scheme, the height of a transaction is represented by a tuple (txNumber is the height of the transaction within

the block). This scheme has many advantages over the incremental number scheme - primarily, it enables other components such as statedb, transaction simulation and validation for making efficient design choices.

Following is an illustration of an example read-write set prepared by simulation of a hypothetical transaction. For the sake of simplicity, in the illustrations, we use the incremental numbers for representing the versions.

```
<TxReadWriteSet>
  <NsReadWriteSet name="chaincode1">
    <read-set>
      <read key="K1", version="1">
      <read key="K2", version="1">
    </read-set>
    <write-set>
      <write key="K1", value="V1"
      <write key="K3", value="V2"
      <write key="K4", isDelete="true"
    </write-set>
  </NsReadWriteSet>
<TxReadWriteSet>
```

Additionally, if the transaction performs a range query during simulation, the range query as well as its results will be added to the read-write set as `query-info`.

9.10.2 Transaction validation and updating world state using read-write set

A `committer` uses the read set portion of the read-write set for checking the validity of a transaction and the write set portion of the read-write set for updating the versions and the values of the affected keys.

In the validation phase, a transaction is considered `valid` if the version of each key present in the read set of the transaction matches the version for the same key in the world state - assuming all the preceding `valid` transactions (including the preceding transactions in the same block) are committed (*committed-state*). An additional validation is performed if the read-write set also contains one or more query-info.

This additional validation should ensure that no key has been inserted/deleted/updated in the super range (i.e., union of the ranges) of the results captured in the query-info(s). In other words, if we re-execute any of the range queries (that the transaction performed during simulation) during validation on the committed-state, it should yield the same results that were observed by the transaction at the time of simulation. This check ensures that if a transaction observes phantom items during commit, the transaction should be marked as invalid. Note that the this phantom protection is limited to range queries (i.e., `GetStateByRange` function in the chaincode) and not yet implemented for other queries (i.e., `GetQueryResult` function in the chaincode). Other queries are at risk of phantoms, and should therefore only be used in read-only transactions that are not submitted to ordering, unless the application can guarantee the stability of the result set between simulation and validation/commit time.

If a transaction passes the validity check, the committer uses the write set for updating the world state. In the update phase, for each key present in the write set, the value in the world state for the same key is set to the value as specified in the write set. Further, the version of the key in the world state is changed to reflect the latest version.

9.10.3 Example simulation and validation

This section helps with understanding the semantics through an example scenario. For the purpose of this example, the presence of a key, `k`, in the world state is represented by a tuple `(k,ver,val)` where `ver` is the latest version of the key `k` having `val` as its value.

Now, consider a set of five transactions `T1, T2, T3, T4, and T5`, all simulated on the same snapshot of the world state. The following snippet shows the snapshot of the world state against which the transactions are simulated and the sequence of read and write activities performed by each of these transactions.

```
World state: (k1,1,v1), (k2,1,v2), (k3,1,v3), (k4,1,v4), (k5,1,v5)
T1 -> Write(k1, v1'), Write(k2, v2')
T2 -> Read(k1), Write(k3, v3')
T3 -> Write(k2, v2'')
T4 -> Write(k2, v2'''), read(k2)
T5 -> Write(k6, v6'), read(k5)
```

Now, assume that these transactions are ordered in the sequence of T1,..,T5 (could be contained in a single block or different blocks)

1. `T1` passes validation because it does not perform any read. Further, the tuple of keys `k1` and `k2` in the world state are updated to `(k1,2,v1'), (k2,2,v2')`
2. `T2` fails validation because it reads a key, `k1`, which was modified by a preceding transaction - `T1`
3. `T3` passes the validation because it does not perform a read. Further the tuple of the key, `k2`, in the world state is updated to `(k2,3,v2'')`
4. `T4` fails the validation because it reads a key, `k2`, which was modified by a preceding transaction `T1`
5. `T5` passes validation because it reads a key, `k5,` which was not modified by any of the preceding transactions

Note: Transactions with multiple read-write sets are not yet supported.

9.11 Gossip data dissemination protocol

Hyperledger Fabric optimizes blockchain network performance, security, and scalability by dividing workload across transaction execution (endorsing and committing) peers and transaction ordering nodes. This decoupling of network operations requires a secure, reliable and scalable data dissemination protocol to ensure data integrity and consistency. To meet these requirements, Fabric implements a **gossip data dissemination protocol**.

9.11.1 Gossip protocol

Peers leverage gossip to broadcast ledger and channel data in a scalable fashion. Gossip messaging is continuous, and each peer on a channel is constantly receiving current and consistent ledger data from multiple peers. Each gossiped message is signed, thereby allowing Byzantine participants sending faked messages to be easily identified and the distribution of the message(s) to unwanted targets to be prevented. Peers affected by delays, network partitions, or other causes resulting in missed blocks will eventually be synced up to the current ledger state by contacting peers in possession of these missing blocks.

The gossip-based data dissemination protocol performs three primary functions on a Fabric network:

1. Manages peer discovery and channel membership, by continually identifying available member peers, and eventually detecting peers that have gone offline.
2. Disseminates ledger data across all peers on a channel. Any peer with data that is out of sync with the rest of the channel identifies the missing blocks and syncs itself by copying the correct data.
3. Bring newly connected peers up to speed by allowing peer-to-peer state transfer update of ledger data.

Gossip-based broadcasting operates by peers receiving messages from other peers on the channel, and then forwarding these messages to a number of randomly selected peers on the channel, where this number is a configurable constant. Peers can also exercise a pull mechanism rather than waiting for delivery of a message. This cycle repeats, with the result of channel membership, ledger and state information continually being kept current and in sync. For dissemination of new blocks, the **leader** peer on the channel pulls the data from the ordering service and initiates gossip dissemination to peers in its own organization.

9.11.2 Leader election

The leader election mechanism is used to **elect** one peer per each organization which will maintain connection with ordering service and initiate distribution of newly arrived blocks across peers of its own organization. Leveraging leader election provides system with ability to efficiently utilize bandwidth of the ordering service. There are two possible operation modes for leader election module:

1. **Static** – system administrator manually configures one peer in the organization to be the leader, e.g. one to maintain open connection with the ordering service.
2. **Dynamic** – peers execute a leader election procedure to select one peer in an organization to become leader, pull blocks from the ordering service, and disseminate blocks to the other peers in the organization.

Static leader election

Using static leader election allows to manually define a set of leader peers within the organization, it's possible to define a single node to be a leader or all available peers, it should be taken into account that - making too many peers to connect to the ordering service might lead to inefficient bandwidth utilization. To enable static leader election mode, configure the following parameters within the section of `core.yaml`:

```
peer:
    # Gossip related configuration
    gossip:
        useLeaderElection: false
        orgLeader: true
```

Alternatively these parameters could be configured and overridden with environmental variables:

```
export CORE_PEER_GOSSIP_USELEADERELECTION=false
export CORE_PEER_GOSSIP_ORGLEADER=true
```

Note: The following configuration will keep peer in **stand-by** mode, i.e. peer will not try to become a leader:

```
export CORE_PEER_GOSSIP_USELEADERELECTION=false
export CORE_PEER_GOSSIP_ORGLEADER=false
```

2. Setting `CORE_PEER_GOSSIP_USELEADERELECTION` and `CORE_PEER_GOSSIP_USELEADERELECTION` with `true` value is ambiguous and will lead to an error.
3. In static configuration organization admin is responsible to provide high availability of the leader node in case for failure or crashes.

Dynamic leader election

Dynamic leader election enables organization peers to **elect** one peer which will connect to the ordering service and pull out new blocks. Leader is elected for set of peers for each organization independently.

Elected leader is responsible to send the **heartbeat** messages to the rest of the peers as an evidence of liveness. If one or more peers won't get **heartbeats** updates during period of time, they will initiate a new round of leader election procedure, eventually selecting a new leader. In case of a network partition in the worst case there will be more than one active leader for organization thus to guarantee resiliency and availability allowing the organization's peers to continue making progress. After the network partition is healed one of the leaders will relinquish its leadership, therefore in steady state and in no presence of network partitions for each organization there will be **only** one active leader connecting to the ordering service.

Following configuration controls frequency of the leader **heartbeat** messages:

```
peer:
    # Gossip related configuration
    gossip:
        election:
            leaderAliveThreshold: 10s
```

In order to enable dynamic leader election, the following parameters need to be configured within `core.yaml`:

```
peer:
    # Gossip related configuration
    gossip:
        useLeaderElection: true
        orgLeader: false
```

Alternatively these parameters could be configured and overridden with environmental variables:

```
export CORE_PEER_GOSSIP_USELEADERELECTION=true
export CORE_PEER_GOSSIP_ORGLEADER=false
```

9.11.3 Anchor peers

Anchor peers are used by gossip to make sure peers in different organizations know about each other.

When a configuration block that contains an update to the anchor peers is committed, peers reach out to the anchor peers and learn from them about all of the peers known to the anchor peer(s). Once at least one peer from each organization has contacted an anchor peer, the anchor peer learns about every peer in the channel. Since gossip communication is constant, and because peers always ask to be told about the existence of any peer they don't know about, a common view of membership can be established for a channel.

For example, let's assume we have three organizations—*A*, *B*, *C*— in the channel and a single anchor peer—*peer0.orgC*— defined for organization *C*. When *peer1.orgA* (from organization *A*) contacts *peer0.orgC*, it will tell it about *peer0.orgA*. And when at a later time *peer1.orgB* contacts *peer0.orgC*, the latter would tell the former about *peer0.orgA*. From that point forward, organizations *A* and *B* would start exchanging membership information directly without any assistance from *peer0.orgC*.

As communication across organizations depends on gossip in order to work, there must be at least one anchor peer defined in the channel configuration. It is strongly recommended that every organization provides its own set of anchor peers for high availability and redundancy. Note that the anchor peer does not need to be the same peer as the leader peer.

9.11.4 Gossip messaging

Online peers indicate their availability by continually broadcasting "alive" messages, with each containing the **public key infrastructure (PKI)** ID and the signature of the sender over the message. Peers maintain channel membership by collecting these alive messages; if no peer receives an alive message from a specific peer, this "dead" peer is eventually purged from channel membership. Because "alive" messages are cryptographically signed, malicious peers can never impersonate other peers, as they lack a signing key authorized by a root certificate authority (CA).

In addition to the automatic forwarding of received messages, a state reconciliation process synchronizes **world state** across peers on each channel. Each peer continually pulls blocks from other peers on the channel, in order to repair its own state if discrepancies are identified. Because fixed connectivity is not required to maintain gossip-based data dissemination, the process reliably provides data consistency and integrity to the shared ledger, including tolerance for node crashes.

Because channels are segregated, peers on one channel cannot message or share information on any other channel. Though any peer can belong to multiple channels, partitioned messaging prevents blocks from being disseminated to peers that are not in the channel by applying message routing policies based on peers' channel subscriptions.

Note: 1. Security of point-to-point messages are handled by the peer TLS layer, and do not require signatures. Peers are authenticated by their certificates, which are assigned by a CA. Although TLS certs are also used, it is the peer certificates that are authenticated in the gossip layer. Ledger blocks are signed by the ordering service, and then delivered to the leader peers on a channel.

2. Authentication is governed by the membership service provider for the peer. When the peer connects to the channel for the first time, the TLS session binds with the membership identity. This essentially authenticates each peer to the connecting peer, with respect to membership in the network and channel.

CHAPTER 10

Frequently Asked Questions

10.1 Endorsement

Endorsement architecture:

Question How many peers in the network need to endorse a transaction?

Answer The number of peers required to endorse a transaction is driven by the endorsement policy that is specified at chaincode deployment time.

Question Does an application client need to connect to all peers?

Answer Clients only need to connect to as many peers as are required by the endorsement policy for the chaincode.

10.2 Security & Access Control

Question How do I ensure data privacy?

Answer There are various aspects to data privacy. First, you can segregate your network into channels, where each channel represents a subset of participants that are authorized to see the data for the chaincodes that are deployed to that channel.

Second, you can use private-data to keep ledger data private from other organizations on the channel. A private data collection allows a defined subset of organizations on a channel the ability to endorse, commit, or query private data without having to create a separate channel. Other participants on the channel receive only a hash of the data. For more information refer to the *Using Private Data in Fabric* tutorial. Note that the key concepts topic also explains when to use private data instead of a channel.

Third, as an alternative to Fabric hashing the data using private data, the client application can hash or encrypt the data before calling chaincode. If you hash the data then you will need to provide a means to share the source data. If you encrypt the data then you will need to provide a means to share the decryption keys.

Fourth, you can restrict data access to certain roles in your organization, by building access control into the chaincode logic.

Fifth, ledger data at rest can be encrypted via file system encryption on the peer, and data in-transit is encrypted via TLS.

Question Do the orderers see the transaction data?

Answer No, the orderers only order transactions, they do not open the transactions. If you do not want the data to go through the orderers at all, then utilize the private data feature of Fabric. Alternatively, you can hash or encrypt the data in the client application before calling chaincode. If you encrypt the data then you will need to provide a means to share the decryption keys.

10.3 Application-side Programming Model

Question How do application clients know the outcome of a transaction?

Answer The transaction simulation results are returned to the client by the endorser in the proposal response. If there are multiple endorsers, the client can check that the responses are all the same, and submit the results and endorsements for ordering and commitment. Ultimately the committing peers will validate or invalidate the transaction, and the client becomes aware of the outcome via an event, that the SDK makes available to the application client.

Question How do I query the ledger data?

Answer Within chaincode you can query based on keys. Keys can be queried by range, and composite keys can be modeled to enable equivalence queries against multiple parameters. For example a composite key of (owner,asset_id) can be used to query all assets owned by a certain entity. These key-based queries can be used for read-only queries against the ledger, as well as in transactions that update the ledger.

If you model asset data as JSON in chaincode and use CouchDB as the state database, you can also perform complex rich queries against the chaincode data values, using the CouchDB JSON query language within chaincode. The application client can perform read-only queries, but these responses are not typically submitted as part of transactions to the ordering service.

Question How do I query the historical data to understand data provenance?

Answer The chaincode API `GetHistoryForKey()` will return history of values for a key.

Question How to guarantee the query result is correct, especially when the peer being queried may be recovering and catching up on block processing?

Answer The client can query multiple peers, compare their block heights, compare their query results, and favor the peers at the higher block heights.

10.4 Chaincode (Smart Contracts and Digital Assets)

Question Does Hyperledger Fabric support smart contract logic?

Answer Yes. We call this feature *Chaincode*. It is our interpretation of the smart contract method/algorithm, with additional features.

A chaincode is programmatic code deployed on the network, where it is executed and validated by chain validators together during the consensus process. Developers can use chaincodes to develop business contracts, asset definitions, and collectively-managed decentralized applications.

Question How do I create a business contract?

Answer There are generally two ways to develop business contracts: the first way is to code individual contracts into standalone instances of chaincode; the second way, and probably the more efficient way, is to use chaincode to create decentralized applications that manage the life cycle of one or multiple types of business contracts, and let end users instantiate instances of contracts within these applications.

Question How do I create assets?

Answer Users can use chaincode (for business rules) and membership service (for digital tokens) to design assets, as well as the logic that manages them.

There are two popular approaches to defining assets in most blockchain solutions: the stateless UTXO model, where account balances are encoded into past transaction records; and the account model, where account balances are kept in state storage space on the ledger.

Each approach carries its own benefits and drawbacks. This blockchain technology does not advocate either one over the other. Instead, one of our first requirements was to ensure that both approaches can be easily implemented.

Question Which languages are supported for writing chaincode?

Answer Chaincode can be written in any programming language and executed in containers. Currently, Golang, node.js and java chaincode are supported.

It is also possible to build Hyperledger Fabric applications using Hyperledger Composer.

Question Does the Hyperledger Fabric have native currency?

Answer No. However, if you really need a native currency for your chain network, you can develop your own native currency with chaincode. One common attribute of native currency is that some amount will get transacted (the chaincode defining that currency will get called) every time a transaction is processed on its chain.

10.5 Differences in Most Recent Releases

Question Where can I find what are the highlighted differences between releases?

Answer The differences between any subsequent releases are provided together with the *Releases*.

Question Where to get help for the technical questions not answered above?

Answer Please use StackOverflow.

10.6 Ordering Service

Question I have an ordering service up and running and want to switch consensus algorithms. How do I do that?

Answer This is explicitly not supported.

Question What is the orderer system channel?

Answer The orderer system channel (sometimes called ordering system channel) is the channel the orderer is initially bootstrapped with. It is used to orchestrate channel creation. The orderer system channel defines consortia and the initial configuration for new channels. At channel creation time, the organization definition in the consortium, the `/Channel` group's values and policies, as well as the `/Channel/Orderer` group's values and policies, are all combined to form the new initial channel definition.

Question **If I update my application channel, should I update my orderer system channel?**

Answer Once an application channel is created, it is managed independently of any other channel (including the orderer system channel). Depending on the modification, the change may or may not be desirable to port to other channels. In general, MSP changes should be synchronized across all channels, while policy changes are more likely to be specific to a particular channel.

Question **Can I have an organization act both in an ordering and application role?**

Answer Although this is possible, it is a highly discouraged configuration. By default the `/Channel/Orderer/BlockValidation` policy allows any valid certificate of the ordering organizations to sign blocks. If an organization is acting both in an ordering and application role, then this policy should be updated to restrict block signers to the subset of certificates authorized for ordering.

Question **I want to write a consensus implementation for Fabric. Where do I begin?**

Answer A consensus plugin needs to implement the `Consenter` and `Chain` interfaces defined in the consensus package. There are two plugins built against these interfaces already: solo and kafka. You can study them to take cues for your own implementation. The ordering service code can be found under the orderer package.

Question **I want to change my ordering service configurations, e.g. batch timeout, after I start the network, what should I do?**

Answer This falls under reconfiguring the network. Please consult the topic on *configtxlator*.

10.6.1 Solo

Question **How can I deploy Solo in production?**

Answer Solo is not intended for production. It is not, and will never be, fault tolerant.

10.6.2 Kafka

Question **How do I remove a node from the ordering service?**

Answer This is a two step-process:

1. Add the node's certificate to the relevant orderer's MSP CRL to prevent peers/clients from connecting to it.
2. Prevent the node from connecting to the Kafka cluster by leveraging standard Kafka access control measures such as TLS CRLs, or firewalling.

Question **I have never deployed a Kafka/ZK cluster before, and I want to use the Kafka-based ordering service. How do I proceed?**

Answer The Hyperledger Fabric documentation assumes the reader generally has the operational expertise to setup, configure, and manage a Kafka cluster (see *Caveat emptor*). If you insist on proceeding without such expertise, you should complete, *at a minimum*, the first 6 steps of the Kafka Quickstart guide before experimenting with the Kafka-based ordering service. You can also consult this sample configuration file for a brief explanation of the sensible defaults for Kafka/ZooKeeper.

Question **Where can I find a Docker composition for a network that uses the Kafka-based ordering service?**

Answer Consult the end-to-end CLI example.

Question **Why is there a ZooKeeper dependency in the Kafka-based ordering service?**

Answer Kafka uses it internally for coordination between its brokers.

Question **I'm trying to follow the BYFN example and get a "service unavailable" error, what should I do?**

Answer Check the ordering service's logs. A "Rejecting deliver request because of consenter error" log message is usually indicative of a connection problem with the Kafka cluster. Ensure that the Kafka cluster is set up properly, and is reachable by the ordering service's nodes.

10.6.3 BFT

Question **When is a BFT version of the ordering service going to be available?**

Answer No date has been set. We are working towards a release during the 1.x cycle, i.e. it will come with a minor version upgrade in Fabric. Track FAB-33 for updates.

CHAPTER 11

Contributions Welcome!

We welcome contributions to Hyperledger in many forms, and there's always plenty to do!

First things first, please review the Hyperledger Code of Conduct before participating. It is important that we keep things civil.

11.1 Maintainers

Active Maintainers

Name	Gerrit	GitHub	RocketChat	email
Artem Barger	c0rwin	c0rwin	c0rwin	bartem@il.ibm.com
Binh Nguyen	binhn	binhn	binhn	binh1010010110@gmail.com
Chris Ferris	ChristopherFerris	christo4ferris	cbf	chris.ferris@gmail.com
Dave Enyeart	denyeart	denyeart	dave.enyeart	enyeart@us.ibm.com
Gari Singh	mastersingh24	mastersingh24	garisingh	gari.r.singh@gmail.com
Greg Haskins	greg.haskins	ghaskins	ghaskins	gregory.haskins@gmail.com
Jason Yellick	jyellick	jyellick	jyellick	jyellick@us.ibm.com
Jonathan Levi	JonathanLevi	hacera	JonathanLevi	jonathan@hacera.com
Keith Smith	smithbk	smithbk	smithbk	bksmith@us.ibm.com
Kostas Christidis	kchristidis	kchristidis	kostas	kostas@gmail.com
Manish Sethi	manish-sethi	manish-sethi	manish-sethi	manish.sethi@gmail.com
Matthew Sykes	sykesm	sykesm	sykesm	sykesmat@us.ibm.com
Srinivasan Muralidharan	muralisr	muralisrini	muralisr	srinivasan.muralidharan99@gmail.com
Yacov Manevich	yacovm	yacovm	yacovm	yacovm@il.ibm.com

Release Managers

Name	Gerrit	GitHub	RocketChat	email
Chris Ferris	ChristopherFerris	christo4ferris	cbf	chris.ferris@gmail.com
Dave Enyeart	denyeart	denyeart	dave.enyeart	enyeart@us.ibm.com
Gari Singh	mastersingh24	mastersingh24	garisingh	gari.r.singh@gmail.com

Retired Maintainers

Gabor Hosszu	hgabre	gabre	hgabor	gabor@digitalasset.com
Sheehan Anderson	sheehan	srderson	sheehan	sranderson@gmail.com
Tamas Blummer	TamasBlummer	tamasblummer	tamas	tamas@digitalasset.com
Jim Zhang	jimthematrix	jimthematrix	jimthematrix	jim_the_matrix@hotmail.com
Yaoguo Jiang	jiangyaoguo	jiangyaoguo	jiangyaoguo	jiangyaoguo@gmail.com

11.2 Using Jira to understand current work items

This document has been created to give further insight into the work in progress towards the Hyperledger Fabric v1 architecture based on the community roadmap. The requirements for the roadmap are being tracked in Jira.

It was determined to organize in sprints to better track and show a prioritized order of items to be implemented based on feedback received. We've done this via boards. To see these boards and the priorities click on **Boards -> Manage Boards**:

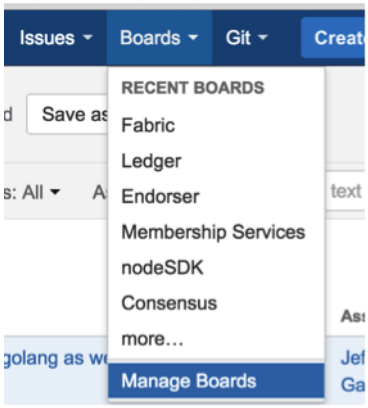


Fig. 1: Jira boards

Now on the left side of the screen click on **All boards**:

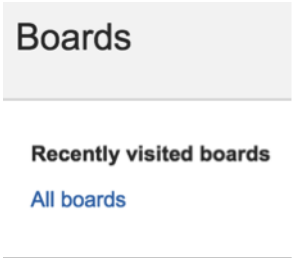


Fig. 2: Jira boards

On this page you will see all the public (and restricted) boards that have been created. If you want to see the items with current sprint focus, click on the boards where the column labeled **Visibility** is **All Users** and the column **Board type** is labeled **Scrum**. For example the **Board Name** Consensus:

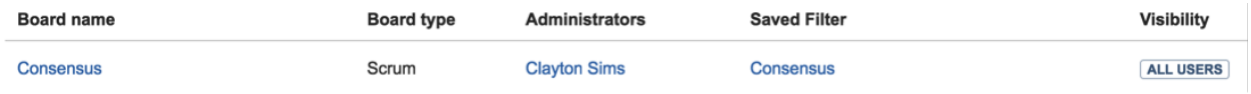


Fig. 3: Jira boards

When you click on Consensus under **Board name** you will be directed to a page that contains the following columns:

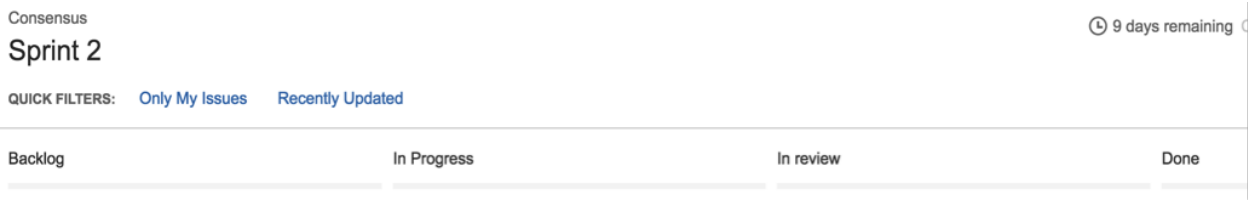


Fig. 4: Jira boards

The meanings to these columns are as follows:

- Backlog – list of items slated for the current sprint (sprints are defined in 2 week iterations), but are not currently in progress
- In progress – items currently being worked by someone in the community.
- In Review – items waiting to be reviewed and merged in Gerrit
- Done – items merged and complete in the sprint.

If you want to see all items in the backlog for a given feature set, click on the stacked rows on the left navigation of the screen:

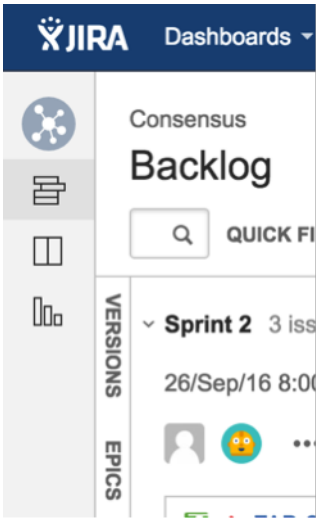


Fig. 5: Jira boards

This shows you items slated for the current sprint at the top, and all items in the backlog at the bottom. Items are listed in priority order.

If there is an item you are interested in working on, want more information or have questions, or if there is an item that you feel needs to be in higher priority, please add comments directly to the Jira item. All feedback and help is very much appreciated.

11.3 Setting up the development environment

11.3.1 Overview

Prior to the v1.0.0 release, the development environment utilized Vagrant running an Ubuntu image, which in turn launched Docker containers as a means of ensuring a consistent experience for developers who might be working with varying platforms, such as macOS, Windows, Linux, or whatever. Advances in Docker have enabled native support on the most popular development platforms: macOS and Windows. Hence, we have reworked our build to take full advantage of these advances. While we still maintain a Vagrant based approach that can be used for older versions of macOS and Windows that Docker does not support, we strongly encourage that the non-Vagrant development setup be used.

Note that while the Vagrant-based development setup could not be used in a cloud context, the Docker-based build does support cloud platforms such as AWS, Azure, Google and IBM to name a few. Please follow the instructions for Ubuntu builds, below.

11.3.2 Prerequisites

- Git client
- Go - version 1.10.x
- (macOS) Xcode must be installed
- Docker - 17.06.2-ce or later
- Docker Compose - 1.14.0 or later
- Pip
- (macOS) you may need to install gnutar, as macOS comes with bsdtar as the default, but the build uses some gnutar flags. You can use Homebrew to install it as follows:

```
brew install gnu-tar --with-default-names
```

- (macOS) Libtool. You can use Homebrew to install it as follows:

```
brew install libtool
```

- (only if using Vagrant) - Vagrant - 1.9 or later
- (only if using Vagrant) - VirtualBox - 5.0 or later
- BIOS Enabled Virtualization - Varies based on hardware
- Note: The BIOS Enabled Virtualization may be within the CPU or Security settings of the BIOS

11.3.3 `pip`

```
pip install --upgrade pip
```

11.3.4 Steps

Set your GOPATH

Make sure you have properly setup your Host's GOPATH environment variable. This allows for both building within the Host and the VM.

In case you installed Go into a different location from the standard one your Go distribution assumes, make sure that you also set GOROOT environment variable.

Note to Windows users

If you are running Windows, before running any `git clone` commands, run the following command.

```
git config --get core.autocrlf
```

If `core.autocrlf` is set to `true`, you must set it to `false` by running

```
git config --global core.autocrlf false
```

If you continue with `core.autocrlf` set to `true`, the `vagrant up` command will fail with the error:

```
./setup.sh: /bin/bash^M: bad interpreter: No such file or directory
```

Cloning the Hyperledger Fabric source

Since Hyperledger Fabric is written in `Go`, you'll need to clone the source repository to your $GOPATH/src directory. If your $GOPATH has multiple path components, then you will want to use the first one. There's a little bit of setup needed:

```
cd $GOPATH/src
mkdir -p github.com/hyperledger
cd github.com/hyperledger
```

Recall that we are using `Gerrit` for source control, which has its own internal git repositories. Hence, we will need to clone from *Gerrit*. For brevity, the command is as follows:

```
git clone ssh://LFID@gerrit.hyperledger.org:29418/fabric && scp -p -P 29418␣
↪LFID@gerrit.hyperledger.org:hooks/commit-msg fabric/.git/hooks/
```

Note: Of course, you would want to replace `LFID` with your own *Linux Foundation ID*.

Bootstrapping the VM using Vagrant

If you are planning on using the Vagrant developer environment, the following steps apply. **Again, we recommend against its use except for developers that are limited to older versions of macOS and Windows that are not supported by Docker for Mac or Windows.**

```
cd $GOPATH/src/github.com/hyperledger/fabric/devenv
vagrant up
```

Go get coffee... this will take a few minutes. Once complete, you should be able to `ssh` into the Vagrant VM just created.

```
vagrant ssh
```

Once inside the VM, you can find the source under `$GOPATH/src/github.com/hyperledger/fabric`. It is also mounted as `/hyperledger`.

11.3.5 Building Hyperledger Fabric

Once you have all the dependencies installed, and have cloned the repository, you can proceed to *build and test* Hyperledger Fabric.

11.3.6 Notes

NOTE: Any time you change any of the files in your local fabric directory (under `$GOPATH/src/github.com/hyperledger/fabric`), the update will be instantly available within the VM fabric directory.

NOTE: If you intend to run the development environment behind an HTTP Proxy, you need to configure the guest so that the provisioning process may complete. You can achieve this via the *vagrant-proxyconf* plugin. Install with `vagrant plugin install vagrant-proxyconf` and then set the VAGRANT_HTTP_PROXY and VAGRANT_HTTPS_PROXY environment variables *before* you execute `vagrant up`. More details are available here: https://github.com/tmatilai/vagrant-proxyconf/

NOTE: The first time you run this command it may take quite a while to complete (it could take 30 minutes or more depending on your environment) and at times it may look like it's not doing anything. As long you don't get any error messages just leave it alone, it's all good, it's just cranking.

NOTE to Windows 10 Users: There is a known problem with vagrant on Windows 10 (see hashicorp/vagrant#6754). If the `vagrant up` command fails it may be because you do not have the Microsoft Visual C++ Redistributable package installed. You can download the missing package at the following address: http://www.microsoft.com/en-us/download/details.aspx?id=8328

NOTE: The inclusion of the miekg/pkcs11 package introduces an external dependency on the ltdl.h header file during a build of fabric. Please ensure your libtool and libltdl-dev packages are installed. Otherwise, you may get a ltdl.h header missing error. You can download the missing package by command: `sudo apt-get install -y build-essential git make curl unzip g++ libtool`.

11.4 Building Hyperledger Fabric

The following instructions assume that you have already set up your *development environment*.

To build Hyperledger Fabric:

```
cd $GOPATH/src/github.com/hyperledger/fabric
make dist-clean all
```

11.4.1 Running the unit tests

Use the following sequence to run all unit tests

```
cd $GOPATH/src/github.com/hyperledger/fabric
make unit-test
```

To run a subset of tests, set the TEST_PKGS environment variable. Specify a list of packages (separated by space), for example:

```
export TEST_PKGS="github.com/hyperledger/fabric/core/ledger/..."
make unit-test
```

To run a specific test use the `-run RE` flag where RE is a regular expression that matches the test case name. To run tests with verbose output use the `-v` flag. For example, to run the `TestGetFoo` test case, change to the directory containing the `foo_test.go` and call/execute

```
go test -v -run=TestGetFoo
```

11.4.2 Running Node.js Client SDK Unit Tests

You must also run the Node.js unit tests to ensure that the Node.js client SDK is not broken by your changes. To run the Node.js unit tests, follow the instructions here.

11.5 Building outside of Vagrant

It is possible to build the project and run peers outside of Vagrant. Generally speaking, one has to 'translate' the vagrant setup file to the platform of your choice.

11.5.1 Building on Z

To make building on Z easier and faster, this script is provided (which is similar to the setup file provided for vagrant). This script has been tested only on RHEL 7.2 and has some assumptions one might want to re-visit (firewall settings, development as root user, etc.). It is however sufficient for development in a personally-assigned VM instance.

To get started, from a freshly installed OS:

```
sudo su
yum install git
mkdir -p $HOME/git/src/github.com/hyperledger
cd $HOME/git/src/github.com/hyperledger
git clone http://gerrit.hyperledger.org/r/fabric
source fabric/devenv/setupRHELonZ.sh
```

From this point, you can proceed as described above for the Vagrant development environment.

```
cd $GOPATH/src/github.com/hyperledger/fabric
make peer unit-test
```

11.5.2 Building on Power Platform

Development and build on Power (ppc64le) systems is done outside of vagrant as outlined *here*. For ease of setting up the dev environment on Ubuntu, invoke this script as root. This script has been validated on Ubuntu 16.04 and assumes certain things (like, development system has OS repositories in place, firewall setting etc) and in general can be improvised further.

To get started on Power server installed with Ubuntu, first ensure you have properly setup your Host's GOPATH environment variable. Then, execute the following commands to build the fabric code:

```
mkdir -p $GOPATH/src/github.com/hyperledger
cd $GOPATH/src/github.com/hyperledger
git clone http://gerrit.hyperledger.org/r/fabric
sudo ./fabric/devenv/setupUbuntuOnPPC64le.sh
cd $GOPATH/src/github.com/hyperledger/fabric
make dist-clean all
```

11.5.3 Building on Centos 7

You will have to build CouchDB from source because there is no package available from the distribution. If you are planning a multi-orderer arrangement, you will also need to install Apache Kafka from source. Apache Kafka includes both Zookeeper and Kafka executables and supporting artifacts.

```
export GOPATH={directory of your choice}
mkdir -p $GOPATH/src/github.com/hyperledger
FABRIC=$GOPATH/src/github.com/hyperledger/fabric
git clone https://github.com/hyperledger/fabric $FABRIC
cd $FABRIC
git checkout master # <-- only if you want the master branch
export PATH=$GOPATH/bin:$PATH
make native
```

If you are not trying to build for docker, you only need the natives.

11.6 Configuration

Configuration utilizes the viper and cobra libraries.

There is a **core.yaml** file that contains the configuration for the peer process. Many of the configuration settings can be overridden on the command line by setting ENV variables that match the configuration setting, but by prefixing with *'CORE_'*. For example, logging level manipulation through the environment is shown below:

```
CORE_PEER_LOGGING_LEVEL=CRITICAL peer
```

11.7 Requesting a Linux Foundation Account

Contributions to the Hyperledger Fabric code base require a Linux Foundation account — follow the steps below to create one if you don't already have one.

11.7.1 Creating a Linux Foundation ID

1. Go to the Linux Foundation ID website.
2. Select the option `I need to create a Linux Foundation ID`, and fill out the form that appears.
3. Wait a few minutes, then look for an email message with the subject line: "Validate your Linux Foundation ID email".
4. Open the received URL to validate your email address.
5. Verify that your browser displays the message `You have successfully validated your e-mail address`.

6. Access Gerrit by selecting `Sign In`, and use your new Linux Foundation account ID to sign in.

11.7.2 Configuring Gerrit to Use SSH

Gerrit uses SSH to interact with your Git client. If you already have an SSH key pair, you can skip the part of this section that explains how to generate one.

What follows explains how to generate an SSH key pair in a Linux environment — follow the equivalent steps on your OS.

First, create an SSH key pair with the command:

```
ssh-keygen -t rsa -C "John Doe john.doe@example.com"
```

Note: This will ask you for a password to protect the private key as it generates a unique key. Please keep this password private, and DO NOT enter a blank password.

The generated SSH key pair can be found in the files `~/.ssh/id_rsa` and `~/.ssh/id_rsa.pub`.

Next, add the private key in the `id_rsa` file to your key ring, e.g.:

```
ssh-add ~/.ssh/id_rsa
```

Finally, add the public key of the generated key pair to the Gerrit server, with the following steps:

1. Go to Gerrit.
2. Click on your account name in the upper right corner.
3. From the pop-up menu, select `Settings`.
4. On the left side menu, click on `SSH Public Keys`.
5. Paste the contents of your public key `~/.ssh/id_rsa.pub` and click `Add key`.

Note: The `id_rsa.pub` file can be opened with any text editor. Ensure that all the contents of the file are selected, copied and pasted into the `Add SSH key` window in Gerrit.

Note: The SSH key generation instructions operate on the assumption that you are using the default naming. It is possible to generate multiple SSH keys and to name the resulting files differently. See the ssh-keygen documentation for details on how to do that. Once you have generated non-default keys, you need to configure SSH to use the correct key for Gerrit. In that case, you need to create a `~/.ssh/config` file modeled after the one below.

```
host gerrit.hyperledger.org
 HostName gerrit.hyperledger.org
 IdentityFile ~/.ssh/id_rsa_hyperledger_gerrit
 User <LFID>
```

where <LFID> is your Linux Foundation ID and the value of IdentityFile is the name of the public key file you generated.

Warning: Potential Security Risk! Do not copy your private key `~/.ssh/id_rsa`. Use only the public `~/.ssh/id_rsa.pub`.

11.7.3 Checking Out the Source Code

Once you've set up SSH as explained in the previous section, you can clone the source code repository with the command:

```
git clone ssh://<LFID>@gerrit.hyperledger.org:29418/fabric fabric
```

You have now successfully checked out a copy of the source code to your local machine.

11.8 Working with Gerrit

Follow these instructions to collaborate on Hyperledger Fabric through the Gerrit review system.

Please be sure that you are subscribed to the mailing list and of course, you can reach out on chat if you need help.

Gerrit assigns the following roles to users:

- **Submitters**: May submit changes for consideration, review other code changes, and make recommendations for acceptance or rejection by voting +1 or -1, respectively.
- **Maintainers**: May approve or reject changes based upon feedback from reviewers voting +2 or -2, respectively.
- **Builders**: (e.g. Jenkins) May use the build automation infrastructure to verify the change.

Maintainers should be familiar with the *review process*. However, anyone is welcome to (and encouraged!) review changes, and hence may find that document of value.

11.8.1 Git-review

There's a **very** useful tool for working with Gerrit called git-review. This command-line tool can automate most of the ensuing sections for you. Of course, reading the information below is also highly recommended so that you understand what's going on behind the scenes.

11.8.2 Getting deeper into Gerrit

A comprehensive walk-through of Gerrit is beyond the scope of this document. There are plenty of resources available on the Internet. A good summary can be found here. We have also provided a set of *Best Practices* that you may find helpful.

11.8.3 Working with a local clone of the repository

To work on something, whether a new feature or a bugfix:

1. Open the Gerrit Projects page
2. Select the project you wish to work on.
3. Open a terminal window and clone the project locally using the `Clone with git hook` URL. Be sure that `ssh` is also selected, as this will make authentication much simpler:

```
git clone ssh://LFID@gerrit.hyperledger.org:29418/fabric && scp -p -P 29418␣
↪LFID@gerrit.hyperledger.org:hooks/commit-msg fabric/.git/hooks/
```

Note: If you are cloning the fabric project repository, you will want to clone it to the `$GOPATH/src/github.com/hyperledger` directory so that it will build, and so that you can use it with the Vagrant *development environment*.

4. Create a descriptively-named branch off of your cloned repository

```
cd fabric
git checkout -b issue-nnnn
```

5. Commit your code. For an in-depth discussion of creating an effective commit, please read *this document on submitting changes*.

```
git commit -s -a
```

Then input precise and readable commit msg and submit.

6. Any code changes that affect documentation should be accompanied by corresponding changes (or additions) to the documentation and tests. This will ensure that if the merged PR is reversed, all traces of the change will be reversed as well.

11.8.4 Submitting a Change

Currently, Gerrit is the only method to submit a change for review.

Note: Please review the *guidelines* for making and submitting a change.

11.8.5 Using git review

Note: if you prefer, you can use the *git-review* tool instead of the following. e.g.

Add the following section to `.git/config`, and replace `<USERNAME>` with your gerrit id.

```
[remote "gerrit"]
    url = ssh://<USERNAME>@gerrit.hyperledger.org:29418/fabric.git
    fetch = +refs/heads/*:refs/remotes/gerrit/*
```

Then submit your change with `git review`.

```
$ cd <your code dir>
$ git review
```

When you update your patch, you can commit with `git commit --amend`, and then repeat the `git review` command.

11.8.6 Not using git review

See the *directions for building the source code*.

When a change is ready for submission, Gerrit requires that the change be pushed to a special branch. The name of this special branch contains a reference to the final branch where the code should reside, once accepted.

For the Hyperledger Fabric repository, the special branch is called `refs/for/master`.

To push the current local development branch to the gerrit server, open a terminal window at the root of your cloned repository:

```
cd <your clone dir>
git push origin HEAD:refs/for/master
```

If the command executes correctly, the output should look similar to this:

```
Counting objects: 3, done.
Writing objects: 100% (3/3), 306 bytes | 0 bytes/s, done.
Total 3 (delta 0), reused 0 (delta 0)
remote: Processing changes: new: 1, refs: 1, done
remote:
remote: New Changes:
remote:   https://gerrit.hyperledger.org/r/6 Test commit
remote:
To ssh://LFID@gerrit.hyperledger.org:29418/fabric
* [new branch]      HEAD -> refs/for/master
```

The gerrit server generates a link where the change can be tracked.

11.9 Reviewing Using Gerrit

- **Add**: This button allows the change submitter to manually add names of people who should review a change; start typing a name and the system will auto-complete based on the list of people registered and with access to the system. They will be notified by email that you are requesting their input.
- **Abandon**: This button is available to the submitter only; it allows a committer to abandon a change and remove it from the merge queue.
- **Change-ID**: This ID is generated by Gerrit (or system). It becomes useful when the review process determines that your commit(s) have to be amended. You may submit a new version; and if the same Change-ID header (and value) are present, Gerrit will remember it and present it as another version of the same change.
- **Status**: Currently, the example change is in review status, as indicated by "Needs Verified" in the upper-left corner. The list of Reviewers will all emit their opinion, voting +1 if they agree to the merge, -1 if they disagree. Gerrit users with a Maintainer role can agree to the merge or refuse it by voting +2 or -2 respectively.

Notifications are sent to the email address in your commit message's Signed-off-by line. Visit your Gerrit dashboard, to check the progress of your requests.

The history tab in Gerrit will show you the in-line comments and the author of the review.

11.10 Viewing Pending Changes

Find all pending changes by clicking on the `All --> Changes` link in the upper-left corner, or open this link.

If you collaborate in multiple projects, you may wish to limit searching to the specific branch through the search bar in the upper-right side.

Add the filter *project:fabric* to limit the visible changes to only those from Hyperledger Fabric.

List all current changes you submitted, or list just those changes in need of your input by clicking on `My --> Changes` or open this link

11.11 Submitting a Change to Gerrit

Carefully review the following before submitting a change to the Hyperledger Fabric code base. These guidelines apply to developers that are new to open source, as well as to experienced open source developers.

11.11.1 Change Requirements

This section contains guidelines for submitting code changes for review. For more information on how to submit a change using Gerrit, please see *Working with Gerrit*.

All changes to Hyperledger Fabric are submitted as Git commits via Gerrit. Each commit must contain:

- a short and descriptive subject line that is 55 characters or fewer, followed by a blank line,
- a change description with the logic or reasoning for your changes, followed by a blank line,
- a Signed-off-by line, followed by a colon (Signed-off-by:), and
- a Change-Id identifier line, followed by a colon (Change-Id:). Gerrit won't accept patches without this identifier.

A commit with the above details is considered well-formed.

Note: You don't need to supply the Change-Id identifier for a new commit; this is added automatically by the `commit-msg` Git hook associated with the repository. If you subsequently amend your commit and resubmit it, using the same Change-Id value as the initial commit will guarantee that Gerrit will recognize that subsequent commit as an amended commit with respect to the earlier one.

All changes and topics sent to Gerrit must be well-formed. In addition to the above mandatory content in a commit, a commit message should include:

- **what** the change does,
- **why** you chose that approach, and
- **how** you know it works — for example, which tests you ran.

Commits must *build cleanly* when applied on top of each other, thus avoiding breaking bisectability. Each commit should address a single identifiable JIRA issue and should be logically self-contained. For example, one commit might fix whitespace issues, another commit might rename a function, while a third commit could change some code's functionality.

A well-formed commit is illustrated below in detail:

```
[FAB-XXXX] purpose of commit, no more than 55 characters

You can add more details here in several paragraphs, but please keep
each line less than 80 characters long.

Change-Id: IF7b6ac513b2eca5f2bab9728ebd8b7e504d3cebe1
Signed-off-by: Your Name <commit-sender@email.address>
```

The name in the `Signed-off-by:` line and your email must match the change authorship information. Make sure your personal `.gitconfig` file is set up correctly.

When a change is included in the set to enable other changes, but it will not be part of the final set, please let the reviewers know this.

11.11.2 Check that your change request is validated by the CI process

To ensure stability of the code and limit possible regressions, we use a Continuous Integration (CI) process based on Jenkins which triggers a build on several platforms and runs tests against every change request being submitted. It is your responsibility to check that your CR passes these tests. No CR will ever be merged if it fails the tests and you shouldn't expect anybody to pay attention to your CRs until they pass the CI tests.

To check on the status of the CI process, simply look at your CR on Gerrit, following the URL that was given to you as the result of the push in the previous step. The History section at the bottom of the page will display a set of actions taken by "Hyperledger Jobbuilder" corresponding to the CI process being executed.

Upon completion, "Hyperledger Jobbuilder" will add to the CR a *+1 vote* if successful and a *-1 vote* otherwise.

In case of failure, explore the logs linked from the CR History. If you spot a problem with your CR, amend your commit and push it to update it, which will automatically kick off the CI process again.

If you see nothing wrong with your CR, it might be that the CI process simply failed for some reason unrelated to your change. In that case you may want to restart the CI process by posting a reply to your CR with the simple content "reverify". Check the CI management page for additional information and options on this.

11.12 Reviewing a Change

1. Click on a link for incoming or outgoing review.
2. The details of the change and its current status are loaded:

- **Status:** Displays the current status of the change. In the example below, the status reads: Needs Verified.
- **Reply:** Click on this button after reviewing to add a final review message and a score, -1, 0 or +1.
- **Patch Sets:** If multiple revisions of a patch exist, this button enables navigation among revisions to see the changes. By default, the most recent revision is presented.
- **Download:** This button brings up another window with multiple options to download or checkout the current changeset. The button on the right copies the line to your clipboard. You can easily paste it into your git interface to work with the patch as you prefer.

Underneath the commit information, the files that have been changed by this patch are displayed.

3. Click on a filename to review it. Select the code base to differentiate against. The default is `Base` and it will generally be what is needed.
4. The review page presents the changes made to the file. At the top of the review, the presentation shows some general navigation options. Navigate through the patch set using the arrows on the top right corner. It is possible to go to the previous or next file in the set or to return to the main change screen. Click on the yellow sticky pad to add comments to the whole file.

The focus of the page is on the comparison window. The changes made are presented in green on the right versus the base version on the left. Double click to highlight the text within the actual change to provide feedback on a specific section of the code. Press *c* once the code is highlighted to add comments to that section.

5. After adding the comment, it is saved as a *Draft*.
6. Once you have reviewed all files and provided feedback, click the *green up arrow* at the top right to return to the main change page. Click the `Reply` button, write some final comments, and submit your score for the patch set. Click `Post` to submit the review of each reviewed file, as well as your final comment and score. Gerrit sends an email to the change-submitter and all listed reviewers. Finally, it logs the review for future reference. All individual comments are saved as *Draft* until the `Post` button is clicked.

11.13 Gerrit Recommended Practices

This document presents some best practices to help you use Gerrit more effectively. The intent is to show how content can be submitted easily. Use the recommended practices to reduce your troubleshooting time and improve participation in the community.

11.13.1 Browsing the Git Tree

Visit Gerrit then select `Projects --> List --> SELECT-PROJECT --> Branches`. Select the branch that interests you, click on `gitweb` located on the right-hand side. Now, `gitweb` loads your selection on the Git web interface and redirects appropriately.

11.13.2 Watching a Project

Visit Gerrit, then select `Settings`, located on the top right corner. Select `Watched Projects` and then add any projects that interest you.

11.13.3 Commit Messages

Gerrit follows the Git commit message format. Ensure the headers are at the bottom and don't contain blank lines between one another. The following example shows the format and content expected in a commit message:

Brief (no more than 50 chars) one line description.

Elaborate summary of the changes made referencing why (motivation), what was changed and how it was tested. Note also any changes to documentation made to remain consistent with the code changes, wrapping text at 72 chars/line.

Jira: FAB-100
Change-Id: LONGHEXHASH
Signed-off-by: Your Name your.email@example.org
AnotherExampleHeader: An Example of another Value

The Gerrit server provides a precommit hook to autogenerate the Change-Id which is one time use.

Recommended reading: How to Write a Git Commit Message

11.13.4 Avoid Pushing Untested Work to a Gerrit Server

To avoid pushing untested work to Gerrit.

Check your work at least three times before pushing your change to Gerrit. Be mindful of what information you are publishing.

11.13.5 Keeping Track of Changes

- Set Gerrit to send you emails:
- Gerrit will add you to the email distribution list for a change if a developer adds you as a reviewer, or if you comment on a specific Patch Set.

- Opening a change in Gerrit's review interface is a quick way to follow that change.
- Watch projects in the Gerrit projects section at `Gerrit`, select at least *New Changes, New Patch Sets, All Comments* and *Submitted Changes*.

Always track the projects you are working on; also see the feedback/comments mailing list to learn and help others ramp up.

11.13.6 Topic branches

Topic branches are temporary branches that you push to commit a set of logically-grouped dependent commits:

To push changes from `REMOTE/master` tree to Gerrit for being reviewed as a topic in **TopicName** use the following command as an example:

$ git push REMOTE HEAD:refs/for/master/TopicName

The topic will show up in the review `UI` and in the `Open Changes List`. Topic branches will disappear from the master tree when its content is merged.

11.13.7 Creating a Cover Letter for a Topic

You may decide whether or not you'd like the cover letter to appear in the history.

1. To make a cover letter that appears in the history, use this command:

```
git commit --allow-empty
```

Edit the commit message, this message then becomes the cover letter. The command used doesn't change any files in the source tree.

2. To make a cover letter that doesn't appear in the history follow these steps:

- Put the empty commit at the end of your commits list so it can be ignored without having to rebase.
- Now add your commits

```
git commit ...
git commit ...
git commit ...
```

- Finally, push the commits to a topic branch. The following command is an example:

```
git push REMOTE HEAD:refs/for/master/TopicName
```

If you already have commits but you want to set a cover letter, create an empty commit for the cover letter and move the commit so it becomes the last commit on the list. Use the following command as an example:

```
git rebase -i HEAD~#Commits
```

Be careful to uncomment the commit before moving it. `#Commits` is the sum of the commits plus your new cover letter.

11.13.8 Finding Available Topics

```
$ ssh -p 29418 gerrit.hyperledger.org gerrit query \ status:open project:fabric␣
↪branch:master \
| grep topic: | sort -u
```

- gerrit.hyperledger.org Is the current URL where the project is hosted.
- *status* Indicates the topic's current status: open , merged, abandoned, draft, merge conflict.
- *project* Refers to the current name of the project, in this case fabric.
- *branch* The topic is searched at this branch.
- *topic* The name of an specific topic, leave it blank to include them all.
- *sort* Sorts the found topics, in this case by update (-u).

11.13.9 Downloading or Checking Out a Change

In the review UI, on the top right corner, the **Download** link provides a list of commands and hyperlinks to checkout or download diffs or files.

We recommend the use of the *git review* plugin. The steps to install git review are beyond the scope of this document. Refer to the git review documentation for the installation process.

To check out a specific change using Git, the following command usually works:

```
git review -d CHANGEID
```

If you don't have Git-review installed, the following commands will do the same thing:

```
git fetch REMOTE refs/changes/NN/CHANGEIDNN/VERSION \ && git checkout FETCH_HEAD
```

For example, for the 4th version of change 2464, NN is the first two digits (24):

```
git fetch REMOTE refs/changes/24/2464/4 \ && git checkout FETCH_HEAD
```

11.13.10 Using Draft Branches

You can use draft branches to add specific reviewers before you publishing your change. The Draft Branches are pushed to `refs/drafts/master/TopicName`

The next command ensures a local branch is created:

```
git checkout -b BRANCHNAME
```

The next command pushes your change to the drafts branch under **TopicName**:

```
git push REMOTE HEAD:refs/drafts/master/TopicName
```

11.13.11 Using Sandbox Branches

You can create your own branches to develop features. The branches are pushed to the `refs/sandbox/USERNAME/BRANCHNAME` location.

These commands ensure the branch is created in Gerrit's server.

```
git checkout -b sandbox/USERNAME/BRANCHNAME
git push --set-upstream REMOTE HEAD:refs/heads/sandbox/USERNAME/BRANCHNAME
```

Usually, the process to create content is:

- develop the code,
- break the information into small commits,
- submit changes,
- apply feedback,
- rebase.

The next command pushes forcibly without review:

```
git push REMOTE sandbox/USERNAME/BRANCHNAME
```

You can also push forcibly with review:

```
git push REMOTE HEAD:ref/for/sandbox/USERNAME/BRANCHNAME
```

11.13.12 Updating the Version of a Change

During the review process, you might be asked to update your change. It is possible to submit multiple versions of the same change. Each version of the change is called a patch set.

Always maintain the **Change-Id** that was assigned. For example, there is a list of commits, **c0...c7**, which were submitted as a topic branch:

```
git log REMOTE/master..master

c0
...
c7

git push REMOTE HEAD:refs/for/master/SOMETOPIC
```

After you get reviewers' feedback, there are changes in **c3** and **c4** that must be fixed. If the fix requires rebasing, rebasing changes the commit Ids, see the rebasing section for more information. However, you must keep the same Change-Id and push the changes again:

```
git push REMOTE HEAD:refs/for/master/SOMETOPIC
```

This new push creates a patches revision, your local history is then cleared. However you can still access the history of your changes in Gerrit on the `review UI` section, for each change.

It is also permitted to add more commits when pushing new versions.

11.13.13 Rebasing

Rebasing is usually the last step before pushing changes to Gerrit; this allows you to make the necessary *Change-Ids*. The *Change-Ids* must be kept the same.

- **squash:** mixes two or more commits into a single one.
- **reword:** changes the commit message.

- **edit:** changes the commit content.
- **reorder:** allows you to interchange the order of the commits.
- **rebase:** stacks the commits on top of the master.

11.13.14 Rebasing During a Pull

Before pushing a rebase to your master, ensure that the history has a consecutive order.

For example, your `REMOTE/master` has the list of commits from **a0** to **a4**; Then, your changes **c0...c7** are on top of **a4**; thus:

```
git log --oneline REMOTE/master..master

a0
a1
a2
a3
a4
c0
c1
...
c7
```

If `REMOTE/master` receives commits **a5**, **a6** and **a7**. Pull with a rebase as follows:

```
git pull --rebase REMOTE master
```

This pulls **a5-a7** and re-apply **c0-c7** on top of them:

```
$ git log --oneline REMOTE/master..master
a0
...
a7
c0
c1
...
c7
```

11.13.15 Getting Better Logs from Git

Use these commands to change the configuration of Git in order to produce better logs:

```
git config log.abbrevCommit true
```

The command above sets the log to abbreviate the commits' hash.

```
git config log.abbrev 5
```

The command above sets the abbreviation length to the last 5 characters of the hash.

```
git config format.pretty oneline
```

The command above avoids the insertion of an unnecessary line before the Author line.

To make these configuration changes specifically for the current Git user, you must add the path option `--global` to `config` as follows:

11.14 Coding guidelines

11.14.1 Coding Golang

We code in Go™ and strictly follow the best practices and will not accept any deviations. You must run the following tools against your Go code and fix all errors and warnings: - golint - go vet - goimports

API Documentation

The API documentation for Hyperledger Fabric's Golang APIs is available in GoDoc.

11.15 Generating gRPC code

If you modify any `.proto` files, run the following command to generate/update the respective `.pb.go` files.

```
cd $GOPATH/src/github.com/hyperledger/fabric
make protos
```

11.16 Adding or updating Go packages

Hyperledger Fabric uses Go Vendoring for package management. This means that all required packages reside in the `$GOPATH/src/github.com/hyperledger/fabric/vendor` folder. Go will use packages in this folder instead of the GOPATH when the `go install` or `go build` commands are executed. To manage the packages in the `vendor` folder, we use dep.

11.17 Install prerequisites

Before we begin, if you haven't already done so, you may wish to check that you have all the *prerequisites* installed on the platform(s) on which you'll be developing blockchain applications and/or operating Hyperledger Fabric.

11.18 Getting a Linux Foundation account

In order to participate in the development of the Hyperledger Fabric project, you will need a *Linux Foundation account*. You will need to use your LF ID to access to all the Hyperledger community development tools, including Gerrit, Jira and the Wiki (for editing, only).

11.19 Getting help

If you are looking for something to work on, or need some expert assistance in debugging a problem or working out a fix to an issue, our community is always eager to help. We hang out on Chat, IRC (#hyperledger on freenode.net) and the mailing lists. Most of us don't bite :grin: and will be glad to help. The only silly question is the one you don't ask. Questions are in fact a great way to help improve the project as they highlight where our documentation could be clearer.

11.20 Reporting bugs

If you are a user and you have found a bug, please submit an issue using JIRA. Before you create a new JIRA issue, please try to search the existing items to be sure no one else has previously reported it. If it has been previously reported, then you might add a comment that you also are interested in seeing the defect fixed.

Note: If the defect is security-related, please follow the Hyperledger security bug reporting process.

If it has not been previously reported, create a new JIRA. Please try to provide sufficient information for someone else to reproduce the issue. One of the project's maintainers should respond to your issue within 24 hours. If not, please bump the issue with a comment and request that it be reviewed. You can also post to the relevant Hyperledger Fabric channel in Hyperledger Rocket Chat. For example, a doc bug should be broadcast to `#fabric-documentation`, a database bug to `#fabric-ledger`, and so on...

11.21 Submitting your fix

If you just submitted a JIRA for a bug you've discovered, and would like to provide a fix, we would welcome that gladly! Please assign the JIRA issue to yourself, then you can submit a change request (CR).

Note: If you need help with submitting your first CR, we have created a brief tutorial for you.

11.22 Fixing issues and working stories

Review the issues list and find something that interests you. You could also check the "help-wanted" list. It is wise to start with something relatively straight forward and achievable, and that no one is already assigned. If no one is assigned, then assign the issue to yourself. Please be considerate and rescind the assignment if you cannot finish in a reasonable time, or add a comment saying that you are still actively working the issue if you need a little more time.

11.23 Reviewing submitted Change Requests (CRs)

Another way to contribute and learn about Hyperledger Fabric is to help the maintainers with the review of the CRs that are open. Indeed maintainers have the difficult role of having to review all the CRs that are being submitted and evaluate whether they should be merged or not. You can review the code and/or documentation changes, test the changes, and tell the submitters and maintainers what you think. Once your review and/or test is complete just reply to the CR with your findings, by adding comments and/or voting. A comment saying something like "I tried it on

system X and it works" or possibly "I got an error on system X: xxx " will help the maintainers in their evaluation. As a result, maintainers will be able to process CRs faster and everybody will gain from it.

Just browse through the open CRs on Gerrit to get started.

11.24 Making Feature/Enhancement Proposals

Review JIRA. to be sure that there isn't already an open (or recently closed) proposal for the same function. If there isn't, to make a proposal we recommend that you open a JIRA Epic, Story or Improvement, whichever seems to best fit the circumstance and link or inline a "one pager" of the proposal that states what the feature would do and, if possible, how it might be implemented. It would help also to make a case for why the feature should be added, such as identifying specific use case(s) for which the feature is needed and a case for what the benefit would be should the feature be implemented. Once the JIRA issue is created, and the "one pager" either attached, inlined in the description field, or a link to a publicly accessible document is added to the description, send an introductory email to the hyperledger-fabric@lists.hyperledger.org mailing list linking the JIRA issue, and soliciting feedback.

Discussion of the proposed feature should be conducted in the JIRA issue itself, so that we have a consistent pattern within our community as to where to find design discussion.

Getting the support of three or more of the Hyperledger Fabric maintainers for the new feature will greatly enhance the probability that the feature's related CRs will be merged.

11.25 Setting up development environment

Next, try *building the project* in your local development environment to ensure that everything is set up correctly.

11.26 What makes a good change request?

- One change at a time. Not five, not three, not ten. One and only one. Why? Because it limits the blast area of the change. If we have a regression, it is much easier to identify the culprit commit than if we have some composite change that impacts more of the code.
- Include a link to the JIRA story for the change. Why? Because a) we want to track our velocity to better judge what we think we can deliver and when and b) because we can justify the change more effectively. In many cases, there should be some discussion around a proposed change and we want to link back to that from the change itself.
- Include unit and integration tests (or changes to existing tests) with every change. This does not mean just happy path testing, either. It also means negative testing of any defensive code that it correctly catches input errors. When you write code, you are responsible to test it and provide the tests that demonstrate that your change does what it claims. Why? Because without this we have no clue whether our current code base actually works.
- Unit tests should have NO external dependencies. You should be able to run unit tests in place with `go test` or equivalent for the language. Any test that requires some external dependency (e.g. needs to be scripted to run another component) needs appropriate mocking. Anything else is not unit testing, it is integration testing by definition. Why? Because many open source developers do Test Driven Development. They place a watch on the directory that invokes the tests automagically as the code is changed. This is far more efficient than having to run a whole build between code changes. See this definition of unit testing for a good set of criteria to keep in mind for writing effective unit tests.
- Minimize the lines of code per CR. Why? Maintainers have day jobs, too. If you send a 1,000 or 2,000 LOC change, how long do you think it takes to review all of that code? Keep your changes to < 200-300 LOC, if

possible. If you have a larger change, decompose it into multiple independent changes. If you are adding a bunch of new functions to fulfill the requirements of a new capability, add them separately with their tests, and then write the code that uses them to deliver the capability. Of course, there are always exceptions. If you add a small change and then add 300 LOC of tests, you will be forgiven;-) If you need to make a change that has broad impact or a bunch of generated code (protobufs, etc.). Again, there can be exceptions.

Note: Large change requests, e.g. those with more than 300 LOC are more likely than not going to receive a -2, and you'll be asked to refactor the change to conform with this guidance.

- Do not stack change requests (e.g. submit a CR from the same local branch as your previous CR) unless they are related. This will minimize merge conflicts and allow changes to be merged more quickly. If you stack requests your subsequent requests may be held up because of review comments in the preceding requests.
- Write a meaningful commit message. Include a meaningful 50 (or less) character title, followed by a blank line, followed by a more comprehensive description of the change. Each change MUST include the JIRA identifier corresponding to the change (e.g. [FAB-1234]). This can be in the title but should also be in the body of the commit message. See the *complete requirements* for an acceptable change request.

Note: That Gerrit will automatically create a hyperlink to the JIRA item. e.g.

```
[FAB-1234] fix foobar() panic

Fix [FAB-1234] added a check to ensure that when foobar(foo string)
is called, that there is a non-empty string argument.
```

Finally, be responsive. Don't let a change request fester with review comments such that it gets to a point that it requires a rebase. It only further delays getting it merged and adds more work for you - to remediate the merge conflicts.

11.27 Communication

We use RocketChat for communication and Google Hangouts™ for screen sharing between developers. Our development planning and prioritization is done in JIRA, and we take longer running discussions/decisions to the mailing list.

11.28 Maintainers

The project's *maintainers* are responsible for reviewing and merging all patches submitted for review and they guide the over-all technical direction of the project within the guidelines established by the Hyperledger Technical Steering Committee (TSC).

11.28.1 Becoming a maintainer

This project is managed under an open governance model as described in our charter. Projects or sub-projects will be lead by a set of maintainers. New sub-projects can designate an initial set of maintainers that will be approved by the top-level project's existing maintainers when the project is first approved. The project's maintainers will, from time-to-time, consider adding or removing a maintainer. An existing maintainer can submit a change set to the *MAINTAINERS.rst* file. A nominated Contributor may become a Maintainer by a majority approval of the proposal by

the existing Maintainers. Once approved, the change set is then merged and the individual is added to (or alternatively, removed from) the maintainers group. Maintainers may be removed by explicit resignation, for prolonged inactivity (3 or more months), or for some infraction of the code of conduct or by consistently demonstrating poor judgement. A maintainer removed for inactivity should be restored following a sustained resumption of contributions and reviews (a month or more) demonstrating a renewed commitment to the project.

11.29 Legal stuff

Note: Each source file must include a license header for the Apache Software License 2.0. See the template of the license header.

We have tried to make it as easy as possible to make contributions. This applies to how we handle the legal aspects of contribution. We use the same approach—the Developer's Certificate of Origin 1.1 (DCO)—that the Linux® Kernel community uses to manage code contributions.

We simply ask that when submitting a patch for review, the developer must include a sign-off statement in the commit message.

Here is an example Signed-off-by line, which indicates that the submitter accepts the DCO:

```
Signed-off-by: John Doe <john.doe@example.com>
```

You can include this automatically when you commit a change to your local git repository using `git commit -s`.

CHAPTER 12

Glossary

Terminology is important, so that all Hyperledger Fabric users and developers agree on what we mean by each specific term. What is a smart contract for example. The documentation will reference the glossary as needed, but feel free to read the entire thing in one sitting if you like; it's pretty enlightening!

12.1 Anchor Peer

Used by gossip to make sure peers in different organizations know about each other.

When a configuration block that contains an update to the anchor peers is committed, peers reach out to the anchor peers and learn from them about all of the peers known to the anchor peer(s). Once at least one peer from each organization has contacted an anchor peer, the anchor peer learns about every peer in the channel. Since gossip communication is constant, and because peers always ask to be told about the existence of any peer they don't know about, a common view of membership can be established for a channel.

For example, let's assume we have three organizations—*A*, *B*, *C*— in the channel and a single anchor peer—*peer0.orgC*— defined for organization *C*. When *peer1.orgA* (from organization *A*) contacts *peer0.orgC*, it will tell it about *peer0.orgA*. And when at a later time *peer1.orgB* contacts *peer0.orgC*, the latter would tell the former about *peer0.orgA*. From that point forward, organizations *A* and *B* would start exchanging membership information directly without any assistance from *peer0.orgC*.

As communication across organizations depends on gossip in order to work, there must be at least one anchor peer defined in the channel configuration. It is strongly recommended that every organization provides its own set of anchor peers for high availability and redundancy.

12.2 ACL

An ACL, or Access Control List, associates access to specific peer resources (such as system chaincode APIs or event services) to a *Policy* (which specifies how many and what types of organizations or roles are required). The ACL is part of a channel's configuration. It is therefore persisted in the channel's configuration blocks, and can be updated using the standard configuration update mechanism.

An ACL is formatted as a list of key-value pairs, where the key identifies the resource whose access we wish to control, and the value identifies the channel policy (group) that is allowed to access it. For example `lscc/GetDeploymentSpec: /Channel/Application/Readers` defines that the access to the life cycle chaincode `GetDeploymentSpec` API (the resource) is accessible by identities which satisfy the `/Channel/Application/Readers` policy.

A set of default ACLs is provided in the `configtx.yaml` file which is used by configtxgen to build channel configurations. The defaults can be set in the top level "Application" section of `configtx.yaml` or overridden on a per profile basis in the "Profiles" section.

12.3 Block

A block contains an ordered set of transactions. It is cryptographically linked to the preceding block, and in turn it is linked to be subsequent blocks. The first block in such a chain of blocks is called the **genesis block**. Blocks are created by the ordering system, and validated by peers.

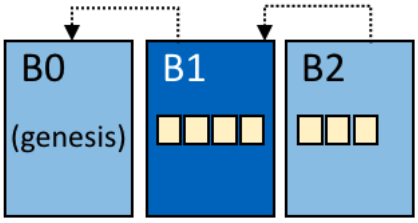


Fig. 1: Block B1 is linked to block B0. Block B2 is linked to block B1.

12.4 Chain

The ledger's chain is a transaction log structured as hash-linked blocks of transactions. Peers receive blocks of transactions from the ordering service, mark the block's transactions as valid or invalid based on endorsement policies and concurrency violations, and append the block to the hash chain on the peer's file system.

12.5 Chaincode

See *Smart-Contract*.

12.6 Channel

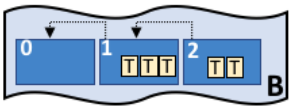


Fig. 2: Blockchain B contains blocks 0, 1, 2.

A channel is a private blockchain overlay which allows for data isolation and confidentiality. A channel-specific ledger is shared across the peers in the channel, and transacting parties must be properly authenticated to a channel in order to interact with it. Channels are defined by a *Configuration-Block*.

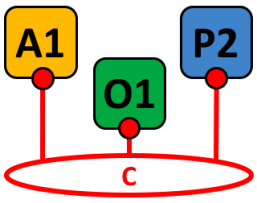


Fig. 3: Channel C connects application A1, peer P2 and ordering service O1.

12.7 Commitment

Each *Peer* on a channel validates ordered blocks of transactions and then commits (writes/appends) the blocks to its replica of the channel *Ledger*. Peers also mark each transaction in each block as valid or invalid.

12.8 Concurrency Control Version Check

Concurrency Control Version Check is a method of keeping state in sync across peers on a channel. Peers execute transactions in parallel, and before commitment to the ledger, peers check that the data read at execution time has not changed. If the data read for the transaction has changed between execution time and commitment time, then a Concurrency Control Version Check violation has occurred, and the transaction is marked as invalid on the ledger and values are not updated in the state database.

12.9 Configuration Block

Contains the configuration data defining members and policies for a system chain (ordering service) or channel. Any configuration modifications to a channel or overall network (e.g. a member leaving or joining) will result in a new configuration block being appended to the appropriate chain. This block will contain the contents of the genesis block, plus the delta.

12.10 Consensus

A broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block.

12.11 Consortium

A consortium is a collection of non-orderer organizations on the blockchain network. These are the organizations that form and join channels and that own peers. While a blockchain network can have multiple consortia, most blockchain networks have a single consortium. At channel creation time, all organizations added to the channel must be part of a consortium. However, an organization that is not defined in a consortium may be added to an existing channel.

12.12 Current State

See *World-State*.

12.13 Dynamic Membership

Hyperledger Fabric supports the addition/removal of members, peers, and ordering service nodes, without compromising the operationality of the overall network. Dynamic membership is critical when business relationships adjust and entities need to be added/removed for various reasons.

12.14 Endorsement

Refers to the process where specific peer nodes execute a chaincode transaction and return a proposal response to the client application. The proposal response includes the chaincode execution response message, results (read set and write set), and events, as well as a signature to serve as proof of the peer's chaincode execution. Chaincode applications have corresponding endorsement policies, in which the endorsing peers are specified.

12.15 Endorsement policy

Defines the peer nodes on a channel that must execute transactions attached to a specific chaincode application, and the required combination of responses (endorsements). A policy could require that a transaction be endorsed by a minimum number of endorsing peers, a minimum percentage of endorsing peers, or by all endorsing peers that are assigned to a specific chaincode application. Policies can be curated based on the application and the desired level of resilience against misbehavior (deliberate or not) by the endorsing peers. A transaction that is submitted must satisfy the endorsement policy before being marked as valid by committing peers. A distinct endorsement policy for install and instantiate transactions is also required.

12.16 Hyperledger Fabric CA

Hyperledger Fabric CA is the default Certificate Authority component, which issues PKI-based certificates to network member organizations and their users. The CA issues one root certificate (rootCert) to each member and one enrollment certificate (ECert) to each authorized user.

12.17 Genesis Block

The configuration block that initializes the ordering service, or serves as the first block on a chain.

12.18 Gossip Protocol

The gossip data dissemination protocol performs three functions: 1) manages peer discovery and channel membership; 2) disseminates ledger data across all peers on the channel; 3) syncs ledger state across all peers on the channel. Refer to the *Gossip* topic for more details.

12.19 Initialize

A method to initialize a chaincode application.

12.20 Install

The process of placing a chaincode on a peer's file system.

12.21 Instantiate

The process of starting and initializing a chaincode application on a specific channel. After instantiation, peers that have the chaincode installed can accept chaincode invocations.

12.22 Invoke

Used to call chaincode functions. A client application invokes chaincode by sending a transaction proposal to a peer. The peer will execute the chaincode and return an endorsed proposal response to the client application. The client application will gather enough proposal responses to satisfy an endorsement policy, and will then submit the transaction results for ordering, validation, and commit. The client application may choose not to submit the transaction results. For example if the invoke only queried the ledger, the client application typically would not submit the read-only transaction, unless there is desire to log the read on the ledger for audit purpose. The invoke includes a channel identifier, the chaincode function to invoke, and an array of arguments.

12.23 Leading Peer

Each *Organization* can own multiple peers on each channel that they subscribe to. One or more of these peers should serve as the leading peer for the channel, in order to communicate with the network ordering service on behalf of the organization. The ordering service delivers blocks to the leading peer(s) on a channel, who then distribute them to other peers within the same organization.

12.24 Ledger

A ledger consists of two distinct, though related, parts – a "blockchain" and the "state database", also known as "world state". Unlike other ledgers, blockchains are **immutable** – that is, once a block has been added to the chain, it cannot be changed. In contrast, the "world state" is a database containing the current value of the set of key-value pairs that have been added, modified or deleted by the set of validated and committed transactions in the blockchain.

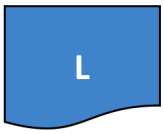


Fig. 4: A Ledger, 'L'

It's helpful to think of there being one **logical** ledger for each channel in the network. In reality, each peer in a channel maintains its own copy of the ledger – which is kept consistent with every other peer's copy through a process called **consensus**. The term **Distributed Ledger Technology** (**DLT**) is often associated with this kind of ledger – one that is logically singular, but has many identical copies distributed across a set of network nodes (peers and the ordering service).

12.25 Member

See *Organization*.

12.26 Membership Service Provider

The Membership Service Provider (MSP) refers to an abstract component of the system that provides credentials to clients, and peers for them to participate in a Hyperledger Fabric network. Clients use these credentials to authenticate their transactions, and peers use these credentials to authenticate transaction processing results (endorsements). While strongly connected to the transaction processing components of the systems, this interface aims to have membership services components defined, in such a way that alternate implementations of this can be smoothly plugged in without modifying the core of transaction processing components of the system.

Fig. 5: An MSP, 'ORG.MSP'

12.27 Membership Services

Membership Services authenticates, authorizes, and manages identities on a permissioned blockchain network. The membership services code that runs in peers and orderers both authenticates and authorizes blockchain operations. It is a PKI-based implementation of the Membership Services Provider (MSP) abstraction.

12.28 Ordering Service

A defined collective of nodes that orders transactions into a block. The ordering service exists independent of the peer processes and orders transactions on a first-come-first-serve basis for all channel's on the network. The ordering service is designed to support pluggable implementations beyond the out-of-the-box SOLO and Kafka varieties. The ordering service is a common binding for the overall network; it contains the cryptographic identity material tied to each *Member*.

12.29 Organization

Also known as "members", organizations are invited to join the blockchain network by a blockchain service provider. An organization is joined to a network by adding its Membership Service Provider (*MSP*) to the network. The MSP defines how other members of the network may verify that signatures (such as those over transactions) were generated by a valid identity, issued by that organization. The particular access rights of identities within an MSP are governed by policies which are also agreed upon when the organization is joined to the network. An organization can be as large as a multi-national corporation or as small as an individual. The transaction endpoint of an organization is a *Peer*. A collection of organizations form a *Consortium*. While all of the organizations on a network are members, not every organization will be part of a consortium.

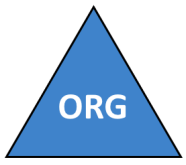


Fig. 6: An organization, 'ORG'

12.30 Peer

A network entity that maintains a ledger and runs chaincode containers in order to perform read/write operations to the ledger. Peers are owned and maintained by members.

Fig. 7: A peer, 'P'

12.31 Policy

Policies are expressions composed of properties of digital identities, for example: `Org1.Peer OR Org2.Peer`. They are used to restrict access to resources on a blockchain network. For instance, they dictate who can read from or write to a channel, or who can use a specific chaincode API via an *ACL*. Policies may be defined in `configtx.yaml` prior to bootstrapping an ordering service or creating a channel, or they can be specified when instantiating chaincode on a channel. A default set of policies ship in the sample `configtx.yaml` which will be appropriate for most networks.

12.32 Private Data

Confidential data that is stored in a private database on each authorized peer, logically separate from the channel ledger data. Access to this data is restricted to one or more organizations on a channel via a private data collection definition. Unauthorized organizations will have a hash of the private data on the channel ledger as evidence of the transaction data. Also, for further privacy, hashes of the private data go through the *Ordering-Service*, not the private data itself, so this keeps private data confidential from Orderer.

12.33 Private Data Collection (Collection)

Used to manage confidential data that two or more organizations on a channel want to keep private from other organizations on that channel. The collection definition describes a subset of organizations on a channel entitled to store a set of private data, which by extension implies that only these organizations can transact with the private data.

12.34 Proposal

A request for endorsement that is aimed at specific peers on a channel. Each proposal is either an instantiate or an invoke (read/write) request.

12.35 Query

A query is a chaincode invocation which reads the ledger current state but does not write to the ledger. The chaincode function may query certain keys on the ledger, or may query for a set of keys on the ledger. Since queries do not change ledger state, the client application will typically not submit these read-only transactions for ordering, validation, and commit. Although not typical, the client application can choose to submit the read-only transaction for ordering, validation, and commit, for example if the client wants auditable proof on the ledger chain that it had knowledge of specific ledger state at a certain point in time.

12.36 Software Development Kit (SDK)

The Hyperledger Fabric client SDK provides a structured environment of libraries for developers to write and test chaincode applications. The SDK is fully configurable and extensible through a standard interface. Components, including cryptographic algorithms for signatures, logging frameworks and state stores, are easily swapped in and out of the SDK. The SDK provides APIs for transaction processing, membership services, node traversal and event handling.

Currently, the two officially supported SDKs are for Node.js and Java, while three more – Python, Go and REST – are not yet official but can still be downloaded and tested.

12.37 Smart Contract

A smart contract is code – invoked by a client application external to the blockchain network – that manages access and modifications to a set of key-value pairs in the *World State*. In Hyperledger Fabric, smart contracts are referred to as chaincode. Smart contract chaincode is installed onto peer nodes and instantiated to one or more channels.

12.38 State Database

Current state data is stored in a state database for efficient reads and queries from chaincode. Supported databases include levelDB and couchDB.

12.39 System Chain

Contains a configuration block defining the network at a system level. The system chain lives within the ordering service, and similar to a channel, has an initial configuration containing information such as: MSP information, policies, and configuration details. Any change to the overall network (e.g. a new org joining or a new ordering node being added) will result in a new configuration block being added to the system chain.

The system chain can be thought of as the common binding for a channel or group of channels. For instance, a collection of financial institutions may form a consortium (represented through the system chain), and then proceed to create channels relative to their aligned and varying business agendas.

12.40 Transaction

Invoke or instantiate results that are submitted for ordering, validation, and commit. Invokes are requests to read/write data from the ledger. Instantiate is a request to start and initialize a chaincode on a channel. Application clients gather invoke or instantiate responses from endorsing peers and package the results and endorsements into a transaction that is submitted for ordering, validation, and commit.

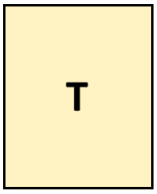


Fig. 8: A transaction, 'T'

12.41 World State

Also known as the "current state", the world state is a component of the HyperLedger Fabric *Ledger*. The world state represents the latest values for all keys included in the chain transaction log. Chaincode executes transaction proposals against world state data because

the world state provides direct access to the latest value of these keys rather than having to calculate them by traversing the entire transaction log. The world state will change every time the value of a key changes (for example, when the ownership of a car – the "key" – is transferred from one owner to another – the "value") or when a new key is added (a car is created). As a result, the world state is critical to a transaction flow, since the current state of a key-value pair must be known before it can be changed. Peers commit the latest values to the ledger world state for each valid transaction included in a processed block.

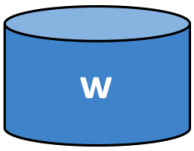


Fig. 9: The World State, 'W'

CHAPTER 13

Releases

Hyperledger Fabric releases are documented on the Fabric github page.

CHAPTER 14

Still Have Questions?

We try to maintain a comprehensive set of documentation for various audiences. However, we realize that often there are questions that remain unanswered. For any technical questions relating to Hyperledger Fabric not answered here, please use StackOverflow. Another approach to getting your questions answered to send an email to the mailing list (hyperledger-fabric@lists.hyperledger.org), or ask your questions on RocketChat (an alternative to Slack) on the #fabric or #fabric-questions channel.

Note: Please, when asking about problems you are facing tell us about the environment in which you are experiencing those problems including the OS, which version of Docker you are using, etc.

CHAPTER 15

Status

Hyperledger Fabric is in the *Active* state. For more information on the history of this project see our wiki page. Information on what *Active* entails can be found in the Hyperledger Project Lifecycle document.

Note: If you have questions not addressed by this documentation, or run into issues with any of the tutorials, please visit the *Still Have Questions?* page for some tips on where to find additional help.