Top 6 technical advantages of Hyperledger Fabric for blockchain networks

What's unique about Hyperledger Fabric, why it matters to business networks, and how to start using it

Sharon Weed Cocco
Gari Singh

March 18, 2018

> Blockchain technology is already radically transforming industry operating models. When selecting a blockchain platform for your business needs, what are the most important attributes to consider? This top-6 list counts them down.

Ready to start building?

For the fastest start to developing your own blockchain solution based on Hyperledger Fabric, head over to the IBM Blockchain 101: Quick-start guide for developers.

Blockchain technology is already radically transforming industry operating models. When considering and evaluating blockchain platforms for your business use case, what are the most important attributes to consider? This article counts them down, and introduces you to Hyperledger Fabric, the open source engine for business blockchains.

IBM Blockchain runs on Hyperledger Fabric. Let the new IBM Blockchain Platform Starter Plan help you kick-start your blockchain network.

Introducing Hyperledger Fabric

Protecting the supply chain

Everledger, a global digital registry for diamonds, uses a Hyperledger Fabric blockchain to track conflict diamonds through the supply chain to protect suppliers, buyers, and shippers from theft and counterfeiting.

Learn how other industries are unlocking new business value with the power of IBM Blockchain built on Hyperledger Fabric.

To meet modern business demands, IBM joined with other companies to collaboratively develop an open source, production-ready, business blockchain framework, called **Hyperledger Fabric**™, one of the 8 Hyperledger® projects hosted by The Linux Foundation®.

Hyperledger Fabric supports distributed ledger solutions on permissioned networks for a wide range of industries. Its modular architecture maximizes the confidentiality, resilience, and flexibility of blockchain solutions.

159 engineers from 27 organizations contributed to Hyperledger Fabric v1.0. Version 1.1 is expected to be released soon.

1. Permissioned membership

Hyperledger Fabric is a framework for *permissioned networks*, where all participants have known identities. When considering a permissioned network, you should think about whether your blockchain use case needs to comply with data protection regulations. Many use cases — in the financial sector and healthcare industry, in particular — are subject to data protection laws that require knowing who the members of the network are and who is accessing specific data.

For example, consider a private equity company. By definition, a private equity is not publicly traded on the stock exchange, and its investors are typically venture capital firms, private equity firms, or angel investors. The participants in this network need to be known and have credibility in capital to invest to be able to participate in the blockchain.

2. Performance, scalability, and levels of trust

Hyperledger Fabric is built on a modular architecture that separates transaction processing into three phases: distributed logic processing and agreement ("chaincode"), transaction ordering, and transaction validation and commitment. This separation confers several advantages: Fewer levels of trust and verification are required across node types, and network scalability and performance are optimized.

To illustrate, let's look at the transaction flow in v1.0 of Hyperledger Fabric, shown in Figure 1. (Terms the figure are defined in the **Hyperledger Fabric glossary**.)

Starting at the left of the figure: **1)** The transaction proposal is submitted by an application to an endorsing peer. **2)** The Endorsement policies outline how many and/or what combination of endorsers are required to sign a proposal. The endorser executes the chaincode to simulate the proposal in the network peer, creating a read/write set. **3)** Then the endorsing peers send back the signed proposal responses (endorsements) to the application. **4)** The application submits the transactions and signatures to the ordering service, which **5)** creates a batch, or block, of transactions and delivers them to committing peers. **6)** When a committing peer receives a batch of transactions, for each transaction it **7)** validates that the endorsement policy was met and checks in the read/write sets to detect conflicting transactions. If both checks pass, the block is committed to the ledger, and the state updates for each transaction are reflected in the state database.

Figure 1. Transaction lifecycle in v1.0 of Hyperledger Fabric
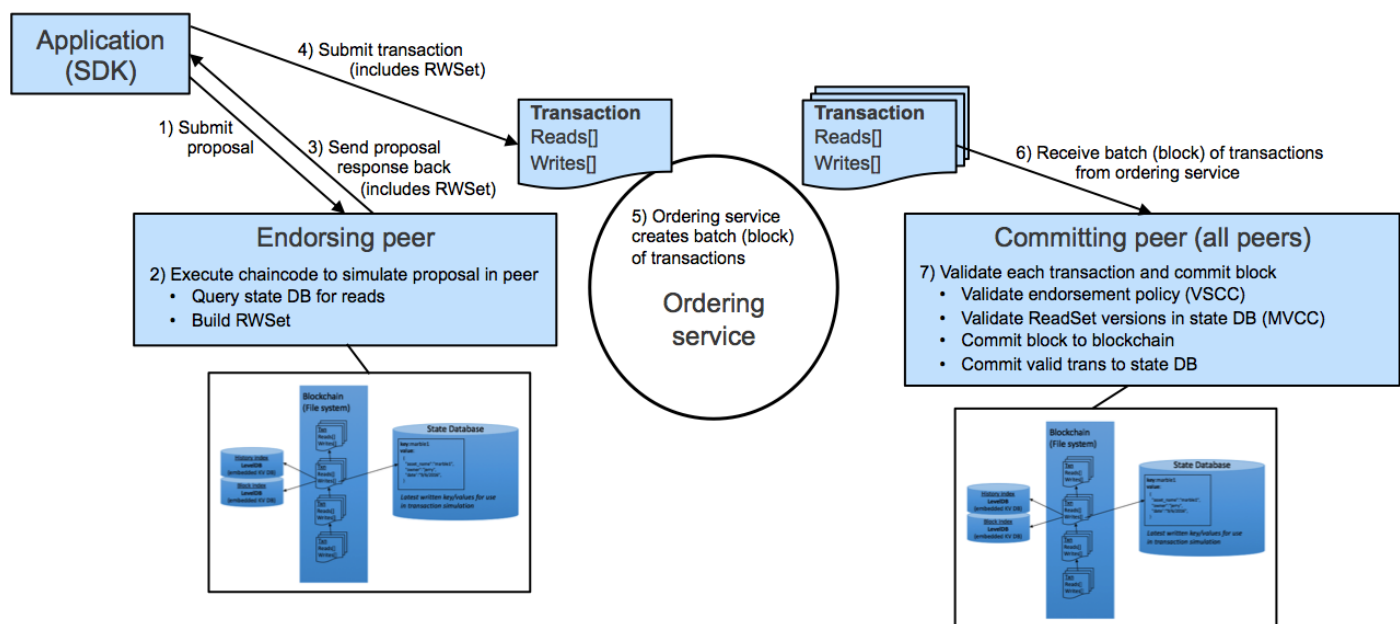
Because only the signatures and read/write set are being sent around the network with the new v1.0 architecture, the scalability and performance are optimized. In addition, because only the endorsers and the committers truly see the transaction, fewer levels of trust are required in different parts of the Blockchain system, offering more security.

For example, in the capital market, with equity-backed securities or debt being bought and sold, transaction volume has increased, due to a growing number of participants. Increased transactions require improved scalability and performance, which v1.0 of Hyperledger Fabric provides, due in part to splitting out the chaincode execution.

Splitting out the chaincode execution also enables dynamic growth in the network. In v1.0 of Hyperledger Fabric, peers can be added dynamically and programmatically, rather than statically as in v0.6. For example, suppose a company that manages foreign exchange rates has a new bank to add to the network. With Hyperledger Fabric v1.0, they can do this programmatically.

3. Data on a need-to-know basis

Businesses, due to competitiveness, protection laws, and regulation on confidentiality of personal data dictate the need for privacy of certain data elements, which can be achieved through data partitioning on the blockchain. Channels, supported in Hyperledger Fabric, allow for data to go to only the parties that need to know.

For example, many financial entities express concern over competitors seeing even the number of transactions being processed. Some financial institutions do not consider cryptography "enough" to protect their data. Given that some financial instruments can take 10 years or more to come to value, the risk of cryptography breaks over time could allow private information to become public. Channels help provide a data-partitioning capability where only those that need to know the data will see the number of transactions and the data itself.

4. Rich queries over an immutable distributed ledger

The ledger is the sequenced record of state transitions for the blockchain application. Each transaction results in a set of asset key-value pairs that are committed to the ledger as creates, updates, or deletes. The immutable source of truth for v1.0 is appended into the file system of the peer, which also has LevelDB embedded.

LevelDB has, by default, a key value database and supports keyed queries, composite key queries, and key range queries. If you also need complex, rich queries, CouchDB supports the basic capabilities of LevelDB, and adds the full data-rich queries. With optional support of a document database such as CouchDB, the content is JSON and fully queryable, where the data model is compatible with existing key/value programming model. As a result, the application changes are not required when modeling chaincode data as JSON when utilizing CouchDB.

This JSON format helps minimize the work required to produce simple reports and perform audit functions. For example, in supply-chain scenarios, you can use JSON document style to help outline specific data for goods and transportation entities. You can easily produce a report on an asset for the different locations and transportation entities that were used in delivery to the asset's final destination.

5. Modular architecture supporting plug-in components

The modularity of Hyperledger Fabric architecture enables network designers to plug in their preferred implementations for components, which is an advantage. One of the most requested areas for modularity is "bring your own identity." Some multi-company networks already have identity management and want to reuse instead of rebuild. Other components of the architecture that can be easily plugged in include consensus or encryption, where some countries have their own encryption standards.

6. Protection of digital keys and sensitive data

HSM (Hardware Security Module) support is vital for safeguarding and managing digital keys for strong authentication. Hyperledger Fabric provides modified and unmodified PKCS11 for key generation, which supports cases like identity management that need more protection. For scenarios dealing with identity management, HSM increases the protection of keys and sensitive data.

Next steps

Dive deeper in the Hyperledger Fabric project overview and latest documentation.

Get a sneak peek at new features planned for the next Hyperledger Fabric release in this Preview of coming attractions: Hyperledger Fabric v1.1.

Learn more about developing, governing, and operating a Hyperledger Fabric business blockchain on the IBM Blockchain Platform. You can kick-start your first pilot solutions on the new Starter Plan, which includes all the latest Hyperledger Fabric functionality.

Join the Hyperledger community and work with IBM and many other developers, from startups to enterprises, on contributing to Hyperledger Fabric. Connect with experts and find answers in the discussion channels.

Hear how Hyperledger executive director Brian Behlendorf demystifies distributed ledgers in There's more to blockchain than dodgy cryptocurrencies.

Stay in the know with the Blockchain Newsletter from developerWorks. Check out the current issue and subscribe.