Top 6 reasons to use the IBM Blockchain service for distributed business networks

With the IBM Blockchain service beta on Hyperledger Fabric version 1.0, create secure, dynamic blockchain networks managed by innovative governance tooling

Steve Cerveny
Sharon Weed Cocco

March 20, 2017

With the IBM Blockchain service beta on Hyperledger Fabric version 1.0, you can easily set up an enterprise-grade blockchain network optimized for security, performance, resiliency, monitoring, upgradeability, and support. The service provides dynamic management of network components, including governance tooling with multiple levels of isolation to protect your data in a highly secured blockchain network.

Sign up for the Blockchain service beta on Bluemix:

1. Visit the Blockchain service page in Bluemix.
3. Click Create. On the form, sign up with your company name and reason for giving the beta a try.

The open source Hyperledger Fabric version 1.0 is now available and full of new features. It's also the foundation for a new beta release of the IBM Blockchain service for high-security business networks.

With the IBM Blockchain service beta on Hyperledger Fabric version 1.0, you can easily set up an enterprise-grade blockchain network optimized for security, performance, resiliency, monitoring, upgradeability, and support. The service provides dynamic management of network components, including governance tooling with multiple isolation levels at the hardware and software level to protect your data in a highly secured blockchain network.

1. Distributed business networks

You might imagine that bootstrapping an enterprise-grade blockchain network would be a complex process, requiring a lot of information and coordination to set up the hardware and software. And
you'd be right! Setting up a network with all the certificates, the members of the network, and the governance required is quite complex, but the IBM Blockchain service beta on Hyperledger Fabric Version 1.0 makes it easy. In a few minutes, you can create a blockchain network, invite participants to join the network, add new channels, and set up the operating rules for the network.

2. Managed Blockchain service

The IBM Blockchain service beta was built based on hundreds of proof of concepts and clients' production networks, which led to a hardened stack of software and hardware, preconfigured for blockchain best practices.

The IBM Blockchain service ensures uptime by providing native resilience. The architecture eliminates single points of failure and adds redundancy to the blockchain network. The ordering service is crash fault tolerant; and 2 peers are automatically provided per member for high availability purposes.

A dashboard monitor provides built-in monitoring and support for simplified asset lifecycle management. Members of the network can see an overview of the blockchain environment, including information about peers, logs, ledger state, channels, and chaincode. This allows you to manage the network and understand asset status at any time.

And because it's a managed service, version updates to the underlying Fabric are automatically applied.

3. Built on Hyperledger Fabric v1.0

Hyperledger Fabric v1.0 brings increased performance, scalability, and levels of trust. Network scalability and performance are increased based on the smaller payload structure of read/write sets, while levels of trust are managed based on having a reduced set of endorsers and committers who can execute the transaction.

In addition, channels were introduced in Hyperledger Fabric v1.0, which helps ensure that data goes only to the parties that need to know, providing data partitioning for data that must be protected at all costs. With the Blockchain service beta, users with the right permissions now have screens that easily allow for installing and instantiating chaincode for channels, and for seeing members who are in the channels that they participate in.

To further explain, chaincode is software that encapsulates the business logic and transactional instructions for creating and modifying assets; it runs in a Docker container associated with any peer that needs to interact with it. Chaincode is first installed on a peer's filesystem for a peer that
will participate in exchanging assets state changes (read/write). Chaincode is then instantiated on a specific channel that contains a list of members. Each channel represents a subset of members that are authorized to see the data for the chaincode instantiated on that channel.

If you are not on a channel, you can't see the data, nor can you see the information in the Blockchain service user interface. Each channel has a unique ledger, and users must properly authenticate in order to perform read/write operations against this data for that channel. Multiple channels can be set up with varying lists of permissioned users. Managing the installation and instantiation of chaincode as well as member participation in channels is made easier through the governance and user interface of the Blockchain service for Hyperledger Fabric version 1.0.

Because the IBM Bluemix service beta is built on Hyperledger Fabric v1.0, these features and a wealth of new capabilities can be leveraged.

4. Governance tooling

The IBM Blockchain service is introducing governance tooling, which helps members to democratically operate a distributed network. As an example of a governance policy, network members may want to set rules to determine how members join the network. Do all members need to agree to have another member join? Do 50% of the members decide to have a member join the network? Network governance is embodied in governance policies like these. A policy editor is available within the IBM Blockchain service to help set the democratic policies for lifecycle tasks.

Based on this governance tooling and policies for who has appropriate access, resource screens are provided to help manage resources for the Certificate Authority, the peers, and ordering service. As an example, in the resource screens, those who have permission can access logs that can be useful in debugging blockchain applications on particular channels.

5. Highly secured environment

The IBM Blockchain service runs in an isolated and highly secured environment. The embedded operating system and all the Fabric components are run in multiple Secure Service Containers (SSC). The Secure Service Container provides advanced cryptology, security, and reliability by encapsulating the operating systems with a secure boot container, encrypting appliance disks, providing tamper protection, and protecting memory. It can be configured to be EAL5 compliant and certified. All these capabilities help to protect highly sensitive and regulated data.

For the IBM Blockchain service for high-security business networks, a virtual appliance was created based on the Secure Service Container. In this appliance, data access is controlled, and access to the embedded Operating System is disabled. Firmware disables access to the memory to prevent data from being dumped. The appliance is booted with a secure boot architecture that ensures that code has not been tampered with. All of the appliance image is signed and encrypted. The appliance is only decrypted in memory, and the encryption keys are protected by Hardware and Firmware means, so administrators do not have access to them. Administrators, including service administrators, cannot access or modify the chaincode, the endorsers, the ordering service, the committer, or the blockchain network.
In addition to these features, HSM (Hardware Security Module) safeguards and manages 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. The IBM Blockchain service has HSM support with the highest FIPS-level compliance.

6. Dedicated, high-performance compute

The IBM Blockchain service has endorsers, ordering services, and committers that run with dedicated resource inside multiple isolated environments. Communication between peers takes place over a high-speed network where communication is highly secure with no data leakage. In addition, communication is accelerated, thanks to advanced cryptographic technology, where operations are more performant with respect to hashing, encryption, and digital signatures.

Next steps

- Build your enterprise-grade blockchain network on Hyperledger v1.0. Take the first step and sign up for the Blockchain service beta on Bluemix.
  To sign up for the beta:
  1. Visit the Blockchain service page.
  3. Click Create. On the form, sign up with your company name and reason for giving the beta a try.

- To work with IBM and many other developers from startups to enterprises on Hyperledger Fabric, join the community.

- A quick way to develop applications on Hyperledger Fabric is to use the new open-source tool, Fabric Composer. Fabric Composer abstracts the details from Hyperledger Fabric and makes it easy to:
  - Build and test a blockchain business network
  - Develop applications to interact with your network
  - Integrate existing systems with your network

  Get an overview of Fabric Composer, and follow the Quickstart. When you complete the Quickstart, you'll have a running local instance of Hyperledger Fabric and a deployed business network, ready for app development.

- Find tutorials, courses, videos, blogs, and more resources for developers in the Blockchain Developer Center.
Related topics

- Blockchain Developer Center
- Hyperledger Fabric documentation
- Hyperledger community
- Hyperledger discussion channels

© Copyright IBM Corporation 2017
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)