IBM Blockchain Platform

Technical Overview

Published November 2017

IBM Blockchain

IBM

Introduction

This paper provides an overview of the capabilities of the IBM Blockchain Platform built on the Linux Foundation's Hyperledger Fabric and Hyperledger Composer. The IBM Blockchain Platform provides a managed, full stack blockchain-as-a-service (BaaS) offering delivered through the IBM Cloud, allowing members to develop, govern, and operate a network with the performance and security necessary for regulated industries. The IBM Blockchain Platform leverages Hyperledger Fabric to enable a new kind of distributed business network founded on the principles of finality, trust, and privacy.

1. **Data finality and consistency matters**
   When transactions are committed to the ledger they should not be removed or changed by the actions of a single party. Because Hyperledger Fabric does not fork, information appended to the blockchain will not change unless updated with another transaction. Transactions are only finalized when they are signed by the appropriate parties according to a flexible construct known as endorsement policies. Distributed ledger technology must enable co-development of a shared version of the truth for a specific business network.
2. **Trust is achieved through permissioned endorsements, not through anonymity**
   Unlike permission-less networks, Hyperledger Fabric and the IBM Blockchain Platform are not based on trust through anonymity. Participants to business networks should be known to the network, enabling distributed trust amongst a known business network. Regulatory requirements including HIPAA and GDPR often dictate certain information on participants and transactions in a network be known.

3. Privacy on the network
Although participants are known to the network, they should be able to transact with privacy and confidentiality on the network. Businesses require full confidence that both their transaction data and the transactions themselves are confidential. Hyperledger Fabric enables confidential communications through channels when information is not desired to be shared with the entire network.
A managed BaaS platform offers the fastest, simplest and most cost-effective way to run a decentralized network amongst a group of organizations. The IBM Blockchain platform offers the right tools and capabilities for Blockchain projects as they incubate and mature from experimental PoCs all the way to distributed multi-party production networks.

Architecture overview

The IBM Blockchain Platform builds on top of key open-source tools to provide the necessary infrastructure for developing, operating and governing enterprise solutions. Figure 1 outlines the end to end architecture of the IBM Blockchain Platform. This captures the experience from over 400 client engagements to provide a production-ready platform for enterprise blockchain networks. It is the only business-ready end to end platform to enable institutions to activate a decentralized blockchain network in record time. Numerous customers are using this architecture in their live networks today.

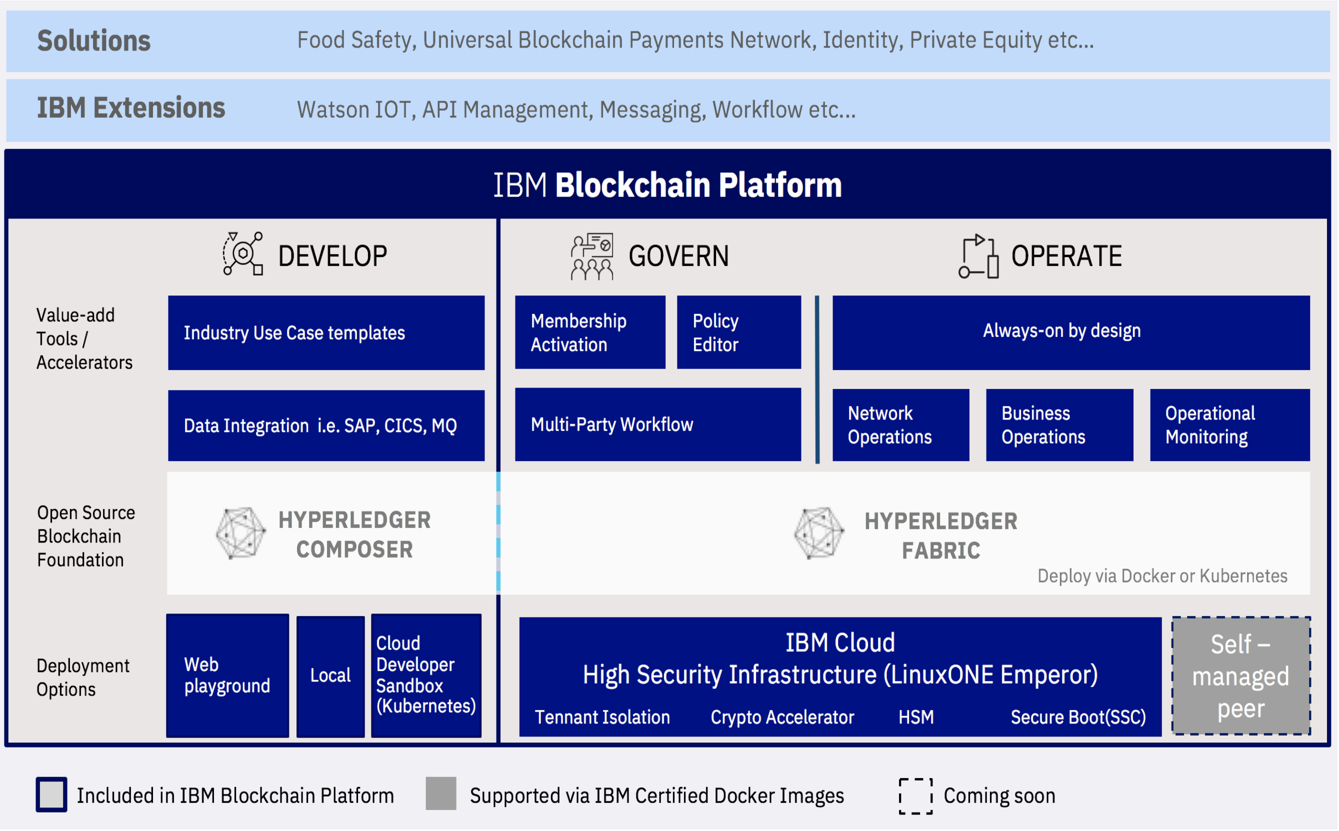
Solutions
Food Safety, Universal Blockchain Payments Network, Identity, Private Equity etc...
IBM Extensions
Watson IOT, API Management, Messaging, Workflow etc...
IBM Blockchain Platform
DEVELOP
GOVERN
OPERATE
Value-add Tools / Accelerators
Industry Use Case templates
Data Integration i.e. SAP, CICS, MQ
Membership Activation
Policy Editor
Multi-Party Workflow
Always-on by design
Network Operations
Business Operations
Operational Monitoring
Open Source Blockchain Foundation
HYPERLEDGER COMPOSER
HYPERLEDGER FABRIC
Deploy via Docker or Kubernetes
Deployment Options
Web playground
Local
Cloud Developer Sandbox (Kubernetes)
IBM Cloud
High Security Infrastructure (LinuxONE Emperor)
Tennant Isolation
Crypto Accelerator
HSM
Secure Boot(SSC)
Self – managed peer
Included in IBM Blockchain Platform
Supported via IBM Certified Docker Images
Coming soon

Figure 1. IBM BLOCKCHAIN PLATFORM

Develop

The first step in recognizing value of transactional business networks is enabling developers to materialize innovative business ideas. The IBM Blockchain Platform allows developers to leverage common tools and languages to model, build, test, and deploy their business applications to a distributed business network.

The platform enables developers to:

- Ensure close alignment across business and technology to significantly reduce blockchain application develop time via a unique modeling language
- Quickly build blockchain skills within existing bench of programmers by leveraging popular tools and languages such as JavaScript and REST.
- Flexibly learn and develop in preferred environment with an open and modern toolset.

The IBM Blockchain Platform builds on top of two open-source code bases governed by the Linux Foundation's Hyperledger: Hyperledger Fabric and Hyperledger Composer. Hyperledger Composer serves as the foundation for modeling business use-cases using common programming languages and tools on top of Hyperledger Fabric.

Hyperledger Composer

Hyperledger Composer is the framework to build blockchain based applications that reflect the core structures of business networks. This framework enables developers to:

- Model business networks
- Expose blockchain data and business logic via auto-generated REST APIs
- Create applications that consume blockchain data

Hyperledger Composer includes a powerful Object-Oriented domain specific language, used to specify a business model, including the structure of assets, participants and transactions. The domain model is used across Hyperledger Composer for code generation, type validation, user interface generation, API generation, amongst other things.

Hyperledger Composer contains a series of code libraries, data models and runtime, developer tools, and a web-based developer environment designed to expedite learning and adoption. All of these capabilities bring speed and efficiency while reducing risk during the application development process.

Hyperledger Composer is designed around a collection of artifacts that is a high-level abstraction over the functional primitives of Hyperledger Fabric, including DSL based duchess main models for defining the assets and relationships, JavaScript based functions for the business logic (a.k.a smart contract), and declarative expression of access control rules over the domain models. The IBM Blockchain Platform builds on Hyperledger Composer to allow developers to easily go from building to deploying applications onto live decentralized business networks in a secure and repeatable fashion.

Top Coder Challenge

Hyperledger Composer was recently used in a Topcoder challenge, for non-blockchain developers to model specific regulations for a decentralized business network. The challenge received over 100 registrants with winning submissions involving medical device provenance and registration, oil import regulations, ferry and passenger boat registration and HUD approved loan and property sales. Developers easily grasped the business modeling language to create sample applications to deploy onto business networks to automate regulatory compliance. More information on the challenge can be found on the Topcoder website [1]

Developer tooling

Developers have multiple options for building and testing their applications before deploying to live business networks. The IBM Blockchain Platform enables developers to quickly and easily align business requirements and accelerate blockchain application development for free with a cloud sandbox and interactive playground that turns any programmer into a blockchain developer. These tools are designed to turn a business design into code in your preferred environment:

1. Try online: Leverage Hyperledger Composer, an open source development tool to learn key blockchain concepts, create network definitions, and leverage reusable industry models and smart contract libraries
2. Install on Laptop: After exploring online, leverage certified Docker images of Hyperledger Fabric and Hyperledger Composer.
3. Develop Together on Cloud: Developing on the cloud allows for all members of your ecosystem to collaborate, share code and view playbacks of your running Blockchain network. This feature utilizes IBM's Container Service, using Docker and Kubernetes to quickly stand-up Blockchain test networks, with free and fee options.

Industry Use Cases

With the IBM Blockchain Platform there is no need for developers to start from scratch. The platform provides developers with a number of simple industry use case scenarios for them to start their exploration with. Additional industry use cases will be added in the future but as of the time of this writing, IBM provides use cases for supply chain, financial services, automotive, real estate, food safety, identity, and international trade.

Simple Integration with Existing Business Data (SOR)

IBM believes that many businesses will want to integrate their blockchain operations with many of their current data sets. To help make this integration easier for the application development, IBM is providing API's to aid integration with Systems of Record through Hyperledger Composer REST API server. Hyperledger Composer also leverages Node-Red to model business flows, as well as LoopBack to assist with routing data flows.

The IBM Blockchain Platform supports a range of development options to enable alignment of business needs with technical capabilities. This is done without the need to separately integrate multiple protocols and platforms after learning vulnerable programming languages for smart contacts.

Govern

Perhaps the most important feature to decentralized business networks is clear and effective governance definitions, models, and tools. The IBM Blockchain Platform provides key features to ensure that networks are created with a well-defined model, and update as needed without restarting the entire network.

Initiating and governing a blockchain network across a group of members once it is operational can take significant amounts of coordination, time and effort. The ability to properly govern a blockchain network is often overlooked and underestimated. Proper governance ultimately ensures the network is in compliance, removes uncertainly and risk of your business obligational (embodied in the smart contracts), ensures privacy and confidentiality of different classes of transactions (embodied in channels) and affords a vetting process to introduce new members.

Key benefits to governance provided with the IBM Blockchain Platform:

- Democratic management tools allows members of the network to collectively manage the rules and policies governing the decentralized business network
- Dynamic management environment allows members to be added to the network as it grows and new smart contracts become available
- Pre-built tools for faster on-boarding, customization, and activation

The IBM Blockchain Platform introduces the first set of integrated tools to allow teams to enforce change management of the network across the cohorts via customizable democratic policies.

Activation Tool

Decentralized business networks constantly change as new participants and transactions are created. Activation tools allow members to easily increase the size of the network, set up new smart contracts, and create channels within a broader business network.

Policy Editor

Core components of a blockchain network such as consensus, membership policy, smart contract, and transaction channels must be supported in a flexible and democratic manner. The Policy Editor within the IBM Blockchain Platform allows members (all or some) of a decentralized business network to collaboratively update the policies that govern the network.

Multi-party Workflow Tool

Network members require visibility in how parties are interacting on the network. The IBM Blockchain Platform provides a workflow tool with a member activity panel, showing integrated and customized notifications, and secure signature collection for policy voting.

Network model

As is the case with traditional business networks, different participants serve different business purposes. The IBM Blockchain Platform enables participants to be configured in specific roles, subject to governance policies in line with the business purpose. Members in a decentralized business network on the IBM Blockchain Platform can serve any combination of roles as a participant, member, user, member-provider, or member-consumer. Each member can operate multiple peers depending on their business needs as well as participate in different networks. Communication "Channels" can be configured so that only specified members are able to view certain confidential data. Members are able to submit and make updates to their copy of the ledger through the consensus and ordering cluster. Applications with the proper identity certificates are likely to be the main user interface for transacting on the network.

Operate

Decentralized business networks handling mission critical applications and transactional data need to be built on a platform that supports secure and scalable "Always-on" operation and updates. The IBM Blockchain Platform enables members to deploy and operate decentralized networks with a production-ready, security hardened service.

Operating System

The core operating system of the IBM Blockchain Platform is Hyperledger Fabric. The back end operating environment of the network is driven by the service plan selected by network founders. Founders interested in the Enterprise and Enterprise + options can leverage the high security LinuxONE infrastructure while Entry plans can use more flexible options. Hyperledger announced the production-ready version of Hyperledger Fabric 1.0 in July of 2017. Hyperledger Fabric v1.0 benefited from the contribution of 159 developers from 28 organizations, built by the enterprise community, for the enterprise community. Hyperledger's Technical Steering Committee drove community involvement and contribution in line with the needs of enterprise adoption, enabling modularity, scalability, and consensus for production networks.

Hyperledger Fabric provides core features to address specific needs of a permissions blockchain network with organizational membership from businesses large and small. Hyperledger Fabric is built with modularity throughout the architecture to allow a variety of implementations on cryptography, identity, consensus algorithms, smart contract languages and other aspects to be easily swapped based on the needs of the consortium. Hyperledger Fabric provides a strong foundation for building decentralized business networks without the need to create a patchwork of disparate solutions.

Modularity

Blockchain networks must be able to incorporate a wide range of new and existing "pluggable" features depending on the enterprise and industry. As a result, Hyperledger Fabric was developed to be modular in order to support future-proof networks as new features emerge. Key features of Hyperledger Fabric are designed to be modular:

- Consensus: Supports any voting-based consensus algorithms for crash fault tolerance and byzantine fault tolerance. Currently shipped with Apache Kafka based implementation, with others under development such as one based on Raft and one based on BFT-SMaRt
- Database: State database options include LevelDB and CouchDB with additional options under development
- Membership services: Currently implemented based on Public Key Infrastructure, with a zero-knowledge proof based implementation coming soon

Modularity in Hyperledger Fabric allows the IBM Blockchain Platform to leverage industry leading security practices to serve production-ready networks.

Scalability

Organizations across sectors demand solutions that scale as they move past initial explorations and proof-of-concepts. Hyperledger Fabric was built to support growing business networks which need to dynamically add participants and support increasing transaction processing.

Many aspects of scalability depend on network configuration of consensus, membership, or security. Modular platforms support the ability to configure a network to support needed throughput numbers. However, Hyperledger Fabric is able to scale to support throughput for use-cases specific to enterprise needs. Current networks are seeing thousands of transactions per second.

Scalability means more than just throughput. Network growth requires that new participants are easily able to join and transact on the network. Hyperledger Fabric separates participant roles into endorsers and committers. This means that participants that just want a copy of the ledger can join as committers who update their copy of the ledger without being burdened with endorsing transactions

Finally, Hyperledger Fabric introduces the concept of channels, enabling participants to transact with complete confidentiality and participate in numerous channels with specific business partners.

These features are further enhanced within the IBM Blockchain Platform through governance and network configuration tooling (as discussed later in the paper). Decentralized business networks require a platform which supports the ability to dynamically add participants, assets, and transactions.

Consensus

Perhaps the most important feature to the security, scalability, and maturity of any blockchain protocol is a clearly-defined and implemented consensus algorithm. Selecting the appropriate consensus algorithm is vital to enabling distributed trust within a decentralized business network.

As mentioned above, consensus in Hyperledger Fabric is designed to be pluggable to fit specific enterprise use-cases. For example, development networks with limited security needs may be suited for a SOLO consensus model that allows a single node to validate all transactions. Production networks are much more likely to require crash and byzantine fault tolerant consensus algorithms. Hyperledger Fabric enables both.

Hyperledger Fabric currently supports voting based consensus algorithms in permissioned networks. The combination of voting and permissions enables network operation with better performance than many public, byzantine fault tolerant, networks. The absence of unknown actors requires that burdensome consensus algorithms are not required. Apache Kafka is provided out of the box and supports crash fault tolerance so a network will continue to function in the event of a partial network crash. Other consensus algorithms include BFT-SMaRt and SBFT
(Simplified Byzantine Fault Tolerance) to tolerate malicious actions in consensus. Hyperledger published a detailed comparison of the different Hyperledger Frameworks, including Hyperledger Fabric. [3]

Hyperledger Fabric's success to date is driven by the massive amount of community support it has received through Hyperledger. Open governance of the code base with a clear purpose has allowed it to emerge as the industry leading protocol for enterprise production networks.

High Security Infrastructure

As mentioned above, the choice of infrastructure is tied to the service plan selected. The IBM Blockchain Platform Enterprise and Enterprise + plans leverage industry-leading security through LinuxOne Emperor to ensure that all code and data are encrypted at all times, tampered virtual machines (VM's) will not start, and no admin or privileged access occurs. Code is executed within IBM Secured Services Containers (SSCs) which protect the security of the ledger. SSC's ensure:

- Tenants are isolated from each other
- Protection from insider attacks or compromised credentials by removing privileged access
- Data encryption keys are private and data is inaccessible even to IBM under court order
- Trusted Boot Loading for tamper proof code execution

The IBM Blockchain Platform meets the highest FIPS 140-2 Level 4 standard for hardware security modules(HSM).

Additionally, the IBM Blockchain Platform's "Always-on" design supports network updates while operational and has optimized performance on the world's fastest Linux compute. Each of these features is backed by IBM's deep Hyperledger Fabric expertise with 24x7x365 coverage for technical blockchain support baked directly into the console.

Specific tools and capabilities were included to make network operation easier. These include:

- Dashboards for monitoring and managing the resources on the network
- Lifecycle Management for seamless upgrades of the full code stack without pausing the network.
- 24/7 Technical Support integrated into the portal
- Hardened security stack with no privileged access, malware and tamper resistance, 100% disk encryption and HSM key protection.

Network Operations

The IBM Blockchain Platform enables founders to initiate, invite, and configure a network with a simple user interface.

Initiating a network creates 3 ordering peers, and two certificate authorities. This provides a founder with a ready to use foundation for creating their business network. Founders can then invite additional participants to the network using any number of peers. Participants will receive email notifications of their invite so that they can easily join the network.

The Network Operations user interface also enables a founder to configure core network components such as identity verification and channel creation. This helps to ensure that only permissioned users access the network, and confidential transactions are enabled via channels.

Business Operations

The IBM Blockchain Platform provides a user interface to support business operations in an active blockchain network. Updates are made without the need to take down the network or halt operations.

Smart contracts represent a core feature of a blockchain network by automating the exchange of information and assets. Users of the IBM Blockchain Platform are easily able to deploy and upgrade smart contracts across the network through a single user interface. Additionally, users are able to edit the policies of a channel which govern consensus.

Operational Monitoring

Users require the ability to monitor the activity on a network as it grows in terms of transactions and participants. The IBM Blockchain Platform provides both a Network Traffic Dashboard and Network Health Monitor. These dashboards enable proactive adjustment to network operations and clearly defines resource consumption within the network.

Network membership

The cost of a blockchain network is shared across its members. To participate in the network each member must operate one or more peers which enables them to transact and represents their copy of the shared ledger. The IBM Blockchain Platform allows members to manage their peers by selecting from four membership plans based on the ecosystem's needs for compute performance and isolation:

1. Entry Plan: Hourly Charge w/basic service levels (available in 2018)
2. Enterprise Plan: Monthly subscription with advanced service levels, ready for production networks (available now)
3. Enterprise Plus Plan: Dedicated compute for performance and isolation available via a monthly subscription plan (available in 2018)
4. Self-Managed Plan: Signed and Certified images of Hyperledger Fabric you can install on your own infrastructure. Can be connected to a network hosted on the IBM Blockchain Platform (available in 2018)

Each membership options includes all the platform tools to develop and govern a complete blockchain network and the tools to operate 1 blockchain peer.

Hybrid Deployment

It is also worth noting that self-managed deployments of Hyperledger Fabric are supported by the IBM Blockchain Platform via IBM Certified Docker images. This enables network peers to be configured via private data centers, IBM Softlayer, AWS, or Azure depending on the business need.
Specifically, IBM will support a Developer Sandbox and self-managed network, configurable in multiple deployment environments. The IBM Blockchain Platform will serve as the control center for the operation of blockchain networks with various deployment options.

Conclusion

The past year has seen an incredible amount of blockchain innovation from a diverse range of organizations. This innovation has been fostered by open-source organizations bringing together institutions and developers to make blockchain ready for enterprise.

The IBM Blockchain Platform represents the next step in this innovation by enabling production networks to be built, governed, and operated through an easy to use interface built on an enterprise-ready protocol. It is easy to get started building your use-case, application, or network today using a free introduction.

For more information: http://www.ibm.com/blockchain/platform
For developers to get started: https://developer.ibm.com/blockchain/sandbox/

IBM **Blockchain**

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
October 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

[1] www.topcoder.com/challenge details/30057924/?type=develop

[2] www.hyperledger.org/announcements/2017/07/11/hyperledger-announces-production-ready-hyperledger-fabric-1-0

[3] www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf