Blockchain basics: Introduction to distributed ledgers

Get to know this game-changing technology and IBM's contribution to it

Sloane Brakeville
Bhargav Perepa

December 15, 2016
(First published May 09, 2016)

Everyone is placing bets on how the blockchain technology will revolutionize the way organizations transact business. Let's look at how a blockchain network operates, what makes it unique, and how IBM is helping to advance the technology.

Everyone is placing bets on how blockchain will revolutionize the way organizations conduct their business transactions. Let's look at how a blockchain network operates, what makes it unique, and how IBM is helping to advance the technology. First, a little background is in order.

The role of ledgers

In today's connected and integrated world, economic activity takes place in business networks that span national, geographic, and jurisdictional boundaries. Business networks typically come together at marketplaces where producers, consumers, suppliers, partners, market makers/enablers, and other stakeholders own, control, and exercise their rights, privileges, and entitlements on objects of value known as ***assets***.

Assets can be tangible and physical, such as cars and homes, or intangible and virtual, such as stock certificates and patents. Asset ownership and transfer create value in a business network, and are known as ***transactions***.

Transactions typically involve various participants like buyers, sellers, and intermediaries (such as banks, auditors, or notaries) whose business agreements and contracts are recorded in ***ledgers***. A business typically uses multiple ledgers to keep track of asset ownership and asset transfers between participants in its various lines of businesses. Ledgers are the systems of record (SORs) for a business's economic activities and interests.

A typical ledger looks something like this:

LEDGER

ACCOUNT TYPE	CASH				
TRANSACTION DATE	TRANSACTION DETAIL	REFERENCE	DEBIT	CREDIT	BALANCE
1/1/16	Expenses for Jan	Ref#1	$100.00		$100.00
2/1/16	Tax withheld	Ref#2		$110.00	($10.00)

Problems with current business ledgers

Current business ledgers in use today are deficient in many ways. They are inefficient, costly, non-transparent, and subject to fraud and misuse. These problems stem from reliance on centralized, trust-based, third-party systems, such as financial institutions, clearinghouses, and other mediators of existing institutional arrangements.

These centralized, trust-based ledger systems lead to bottlenecks and slowdowns of transaction settlements. Lack of transparency, as well as susceptibility to corruption and fraud, lead to disputes. Having to resolve disputes and possibly reverse transactions or provide insurance for transactions is costly. These risks and uncertainties contribute to missed business opportunities.

Furthermore, out-of-sync copies of business ledgers on each network participant's own systems lead to faulty business decisions made on temporary, incorrect data. At best, the ability to make a fully informed decision is delayed while differing copies of the ledgers are resolved.

What is blockchain, exactly?

Blockchain terms and use cases

Get a handle on more blockchain terminology and all its potential uses in our "Blockchain glossary."

A blockchain is a tamper-proof, shared digital ledger that records transactions in a public or private peer-to-peer network. Distributed to all member nodes in the network, the ledger permanently records, in ***blocks***, the history of asset exchanges that take place between the peers in the network.

All the confirmed and validated transaction blocks are linked and chained from the beginning of the chain to the most current block, hence the name ***blockchain***. The blockchain thus acts as a single source of truth, and members in a blockchain network can view only those transactions that are relevant to them.

How does a blockchain network work?

Instead of relying on a third party, such as a financial institution, to mediate transactions, member nodes in a blockchain network use a consensus protocol to agree on ledger content, and cryptographic hashes and digital signatures to ensure the integrity of transactions.

Consensus ensures that the shared ledgers are exact copies, and lowers the risk of fraudulent transactions, because tampering would have to occur across many places at exactly the same time. ***Cryptographic hashes***, such as the SHA256 computational algorithm, ensure that any alteration to transaction input — even the most minuscule change — results in a different hash value being computed, which indicates potentially compromised transaction input. ***Digital signatures*** ensure that transactions originated from senders (signed with private keys) and not imposters.

The decentralized peer-to-peer blockchain network prevents any single participant or group of participants from controlling the underlying infrastructure or undermining the entire system. Participants in the network are all equal, adhering to the same protocols. They can be individuals, state actors, organizations, or a combination of all these types of participants.

At its core, the system records the chronological order of transactions with all nodes agreeing to the validity of transactions using the chosen consensus model. The result is transactions that are irreversible and agreed to by all members in the network.

What are the business benefits of blockchain?

In legacy business networks, all participants maintain their own ledgers with duplication and discrepancies that result in disputes, increased settlement times, and the need for intermediaries with their associated overhead costs. However, by using blockchain-based shared ledgers, where transactions cannot be altered once validated by consensus and written to the ledger, businesses can save time and costs while reducing risks. Blockchain technologies promise improved transparency among willing participants, automation, ledger customization, and improved trust in record keeping.

Blockchain consensus mechanisms provide the benefits of a consolidated, consistent dataset with reduced errors, near-real-time reference data, and the flexibility for participants to change the descriptions of the assets they own.

Because no one participating member owns the source of origin for information contained in the shared ledger, blockchain technologies lead to increased trust and integrity in the flow of transaction information among the participating members.

Immutability mechanisms of blockchain technologies lead to lowered cost of audit and regulatory compliance with improved transparency. And because contracts being executed on business networks using blockchain technologies are smart, automated, and final, businesses benefit from increased speed of execution, reduced costs, and less risk with timely settlements of contracts.

What's a good blockchain use case?

To determine whether your use case is a good fit for blockchain, ask yourself these questions:

1. Is a business network involved?
2. Is consensus used to validate transactions?
3. Is an audit trail, or provenance, required?

4. Must the record of transactions be immutable, or tamper proof?
5. Should dispute resolution be final?

If you answered yes to the first question and to at least one other, then your use case would benefit from blockchain technology. A network always needs to be involved for blockchain to be the right solution, but the network can take many forms. The network can be *between organizations*, such as a supply chain, or the network can be *within an organization*. Within an organization, a blockchain network could be used to share reference data between divisions or to create an audit or compliance network, for example. The network can also exist *between individuals*, who might need to store data, digital assets, or contracts on the blockchain, for example.

Introducing the Linux Foundation's Hyperledger Project

The Hyperledger Project is an open source, collaborative effort to create a blockchain for business-to-business (B2B) and business-to-customer (B2C) transactions. IBM was one of the founding members of the Hyperledger Project, donating 44,000 lines of blockchain code to what became the first project under incubation, Hyperledger Fabric.

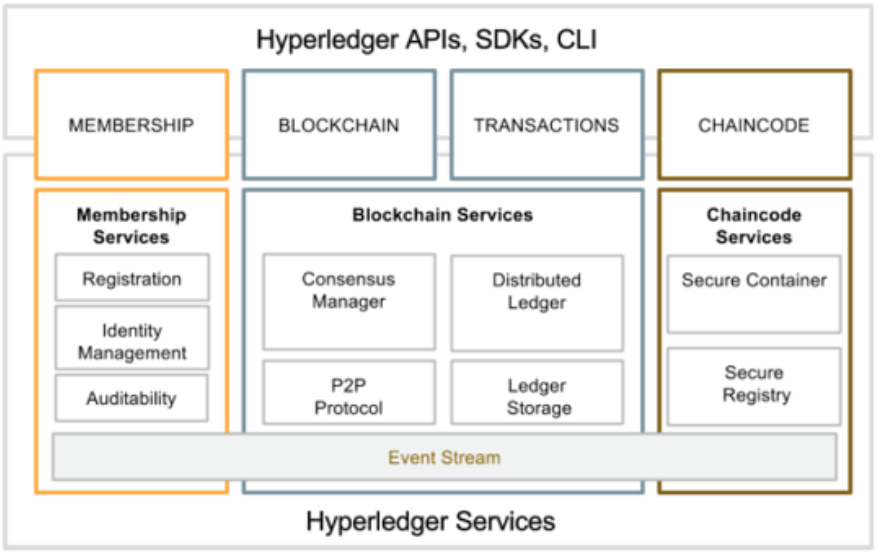
The goal of the Hyperledger Fabric is to create an open standard that can be applied to a variety of industry use cases involving B2B and B2C transactions. The primary goals of this effort are:

- Support a wide variety of industry use cases with different requirements
- Comply with regulatory regimes that exist today
- Support verified identities, and private and confidential transactions
- Support permissioned, shared ledgers
- Support performance, scaling, auditability, identity, security, and privacy
- Reduce costly computations involved in proof of work

To provide functionality and required capabilities, the Hyperledger Fabric is based on these concepts:

- Smart contracts
- Digital assets
- System of record repositories/stores
- Decentralized consensus-based network
- Pluggable consensus algorithms/models
- Cryptographic security

The Hyperledger Fabric architecture supports modularity, plug-and-play interoperability, and container technology for supporting smart contracts written in any popular language.



You can learn more at the Hyperledger Project, in the Hyperledger Whitepaper, and in the Hyperledger Fabric documentation on GitHub.

Enterprise blockchain requirements

We believe that blockchain is a truly disruptive technology that can transform business networks. We also believe that this innovation has to happen in the open, collaborating with other technology companies and industries. To this end, IBM continues to contribute code to the Hyperledger Project.

From IBM's perspective, industrial-grade blockchain technologies have the following characteristics:

- A **shared, permissioned ledger** is the append-only system of record (SOR) and single source of truth. It is visible to all participating members of the business network.
- A **consensus protocol** agreed to by all participating members of the business network ensures that the ledger is updated only with network-verified transactions.
- **Cryptography** ensures tamper-proof security, authentication, and integrity of transactions.
- **Smart contracts** encapsulate participant terms of agreements for the business that takes place on the network; they are stored on the validating nodes in the blockchain and triggered by transactions.

In addition to these attributes, enterprise blockchain technology needs to meet key industry requirements such as performance, verified identifies, and private and confidential transactions. In addition to these attributes, enterprise blockchain technology needs to meet key industry requirements such as performance, verified identifies, and private and confidential transactions. Hyperledger Fabric has been architected to meet these needs. It is also designed with a pluggable consensus model, allowing businesses to select an optimal algorithm for their networks.

How do I get started?

IBM offers flexible platforms and secure infrastructure to help you design, deploy, and manage your blockchain networks. Learn about IBM Blockchain solutions, and see how you can start using blockchain in your business today.

IBM Blockchain on Bluemix

With the free Blockchain service on IBM Bluemix, you can create your own blockchain network with validating nodes and a security service. From there, you can deploy smart contracts (also called chaincode), see results, and build applications.

Start your free Bluemix trial and try Blockchain on Bluemix. Follow the step-by-step instructions in IBM Blockchain 101: Quick-start guide for developers to experiment with your own blockchain network in a secure cloud environment.

IBM-signed and tested images from Docker Hub

Alternatively, you can set up and run a blockchain network using IBM-signed Docker images and Docker Compose files. The images have been tested for functionality, stability, and performance, and you can deploy them in any environment you choose. IBM offers technical support for this configuration for purchase.

Get the images on Docker Hub, and learn more.

Other offerings

IBM offers a high-security environment for enterprise deployments. Networks run in isolation on secure infrastructure that prevents any backdoor access or tampering.

IBM also offers the Watson IoT™ Platform with its built-in capability for adding selected Internet of Things data to a private blockchain. This allows IoT devices to send data to private blockchain ledgers for inclusion in shared transactions with tamper-resistant records.

Learn more about IBM Blockchain solutions.

Conclusion

Blockchain technologies represent a fundamentally new way to transact business. They usher in a robust and smart next generation of applications for the registry and exchange of physical, virtual, tangible, and intangible assets. Thanks to the key concepts of cryptographic security,

decentralized consensus, and a shared public ledger (with its properly controlled and permissioned visibility), blockchain technologies can profoundly change the way we organize our economic, social, political, and scientific activities.

Acknowledgments

The authors are grateful for contributions from Nitin Gaur, Joshua Horton, and Nikhil Gupta, who reviewed the content and provided constructive suggestions. Additionally, they thank Scott Sloan, Sujatha Perepa, and the rest of the IBM Technical Sales Leadership Council (TSLC) team for connecting as one unified IBM Blockchain team.

Related topics

- Blockchain developer center
- Blockchain 101: Quick-start guide for developers
- Blockchain network plan on Bluemix (free)
- Blockchain learning path (3 courses for developers)
- Blockchain videos on developerWorks TV
- Hyperledger Fabric
- Hyperledger Project on GitHub
- Hyperledger Project on Slack