The difference between public and private blockchain

ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain

May 31, 2017

May 31, 2017 | Written by: Praveen Jayachandran

Categorized: Blockchain development | Blockchain explained | Blockchain identity

Share this post:

There are a number of explanations on what blockchain is and what exactly is the difference between Bitcoin and blockchain, but another area where I get many questions, is the difference between public and private blockchain.

The similarities of public and private blockchain

Many flavors of blockchain have evolved over the years and the terminology is often misconstrued. This is easy to do because public and private blockchain have many similarities:

- Both are decentralized peer-to-peer networks, where each participant maintains a replica of a shared append-only ledger of digitally signed transactions.
- Both maintain the replicas in sync through a protocol referred to as consensus.
- Both provide certain guarantees on the immutability of the ledger, even when some participants are faulty or malicious.

So, how are they different?

Public blockchain and known participants

The sole distinction between public and private blockchain is related to who is allowed to participate in the network, execute the *consensus* protocol and maintain the shared ledger. A public blockchain network is completely open and anyone can join and participate in the network. The network typically has an incentivizing mechanism to encourage more participants to join the network. Bitcoin is one of the largest public blockchain networks in production today.

One of the drawbacks of a public blockchain is the substantial amount of computational power that is necessary to maintain a distributed ledger at a large scale. More specifically, to achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of work to ensure all are in sync.

Another disadvantage is the openness of public blockchain, which implies little to no privacy for transactions and only supports a weak notion of security. Both of these are important considerations for enterprise use cases of blockchain.

What's your potential blockchain ROI?

Private blockchain and enterprise

A private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter. Businesses who set up a private blockchain, will generally set up a *permissioned* network. This places restrictions on who is allowed to participate in the network, and only in certain transactions. Participants need to obtain an invitation or *permission* to join. The access control mechanism could vary: existing participants could decide future entrants; a regulatory authority could issue licenses for participation; or a consortium could make the decisions instead. Once an entity has joined the network, it will play a role in maintaining the blockchain in a decentralized manner.

Watch Video At: https://youtu.be/eS39tn5Cy20

The Linux Foundation's Hyperledger Fabric is an example of a permissioned blockchain framework implementation and one of the Hyperledger projects hosted by The Linux Foundation. It has been designed ground up to cater to these enterprise requirements.

This type of permissioned blockchain model offers the ability to leverage more than 30 years of technical literature to realize significant benefits. Digital identity in particular, is fundamental for most industry use cases, be it handling supply chain challenges, disrupting the financial industry, or facilitating security-rich patient/provider data exchanges in healthcare. Only the entities participating in a particular transaction will have knowledge and access to it — other entities will have no access to it. Permissioned blockchains also permit a couple of orders of magnitude greater scalability in terms of transactional throughput.

The next steps on your blockchain journey

The immense promise and accelerated development of permissioned blockchain technology, combined with intense business interest from a wide range of industries, is acting as a perfect stimulant for more and more enterprises to start rolling out blockchain networks into production. I envision these permissioned networks will soon directly or indirectly influence every facet of human enterprise.

Learn more about IBM Blockchain and possible applications for your business. Also, be sure to sign up for the developerWorks newsletter and join the community to stay up to date on exciting blockchain developments:

Learn more about blockchain today

Praveen Jayachandran
Research Scientist and Manager, Blockchain and Smart Contracts, Master Inventor, IBM Research

bitcoin and blockchain blockchain blockchain and enterprise blockchain and finance blockchain and healthcare blockchain network Consensus consensus protocol digital identity Hyperledger hyperledger fabric IBM Blockchain permissioned network Praveen Jayachandran private blockchain public and private blockchain public blockchain public vs private blockchain supply chain the linux foundation

Previous Post

Going big and going global: IBM Blockchain at Consensus

Next Post

Blockchain Technology Summit: Across the industries