100 XP

Blockchain types

5 minutes

A blockchain can be public or private. The distinction determines who can participate in the blockchain network.

Public

What if you wanted a network where you trusted no one? Anyone with Internet access can join your blockchain network. No onboarding is required and you don't have to ask an authority for permission.

A public blockchain is decentralized with no single authority on the network. All transactions in the blockchain are visible by any node on the network.

The first blockchain network was created for Bitcoin. The Bitcoin blockchain network is public. All transactions can be viewed by anyone. For example, you can view the latest Bitcoin blocks and transactions using a block explorer .

The consensus algorithms for public blockchains use cryptocurrency as a reward to validate blocks. Public blockchains may also charge a cryptocurrency fee for validating transactions. Public blockchain privacy is limited. If you wanted to keep your transaction private, you should only share your public key with the other participant in the transaction.

Private

What if we had some trust of the participants in the blockchain network? The information stored in the blockchain would only be accessible to participants invited to the blockchain network. Private networks are *semi-trusted* networks. In a private network, there is an agreement between all participants about how they will leverage the blockchain.

A consortium blockchain is a private blockchain but authority is distributed and acts in the best interests of the network.

In our scenario, we want transaction privacy from the public. Consortium blockchains can restrict who has authority to participate in consensus. Trust is enforced by restricting only the participants be involved in validation. The group of participants is called a consortium. Consensus algorithms for consortium blockchains can use authority rather than cryptocurrency.

We may also want privacy of some data. For example, all parties would know a product was transported but details about the shipment could be kept private. Since we use multiple shipping companies, the details about the shipments could be kept private between two of the parties. Competing shipment companies would only know that the transaction happened and could not see the details about the shipment.

Blockchain protocols

There are several blockchain protocols. The most well known is Bitcoin. The Bitcoin blockchain network was created for Bitcoin cryptocurrency. The primary function of the Bitcoin blockchain network is to store Bitcoin value. Value can be transferred from one to another in a trustless way.

Ethereum is a general use protocol. Ethereum extends what Bitcoin had created to provide a protocol that would allow small programs to be written, as well as simple value transfers. The net effect is the ability to add logic and code instead of simple fixed value transfers.

If you are going to use blockchain for your own solution, consider a general use protocol like Ethereum and Hyperledger Fabric. They are programmable blockchains that can be used for several scenarios. General use protocols use smart contracts to encode business logic and state. In this module, we focus on the Ethereum protocol.

Next unit: When to use blockchain

Continue >