What is the Difference Between Public and Permissioned Blockchains?

Bitcoin is the most ambitious kind of blockchain. Anyone can use bitcoin's cryptographic keys, anyone can be a node and join the network, and anyone can become a miner to service the network and seek a reward. Miners can walk away from being a node, return if and when they feel like it, and get a full account of all network activity since they left.

Basically, anyone can read the chain, anyone can make legitimate changes and anyone can write a new block into the chain (as long as they follow the rules). Bitcoin is totally decentralized. It is also described as a 'censor-proof' blockchain.

For these reasons, it's known by its widest description, a public blockchain. But, this is not the only way to build a blockchain.

MorCryp

Blockchains can be built that require permission to read the information on the blockchain, that limit the parties who can transact on the blockchain and that set who can serve the network by writing new blocks into the chain.

For example, Ripple runs a permissioned blockchain. The startup determines who may act as transaction validator on their network, and it has included CGI, MIT and Microsoft as transaction validators, while also building its own nodes in different locations around the world.

A blockchain developer may choose to make the system of record available for everyone to read, but they may not wish to allow anyone to be a node, serving the network's security, transaction verification or mining. It's a mix-and-match situation that is reflected in the various ways entrepreneurs are experimenting with the technology.

MorCryp

With permissioned blockchains, this may or may not involve 'proof of work' or some other system requirement from the nodes. There is some politics around this, as there are those who consider private blockchains that do not use any proof of work (that is, blockchains with no mining) to not be blockchains at all, but simply shared ledgers.

MorCryp