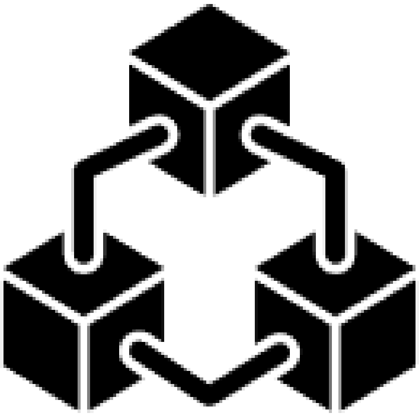
IEEE STC Blockchain

September 2022
Volume 1, Issue 3



Blockchain Fundamentals

By Lars Andreassen Jaatun, UiS

What is Blockchain?

To put it in terms as simple as possible, a blockchain is an unchangeable transaction history. Individual transactions are grouped together in *blocks* together with a hash referring to the previous block and a timestamp. The transactions in question may consist of transferring assets from one member of the network to the other (like transferring Bitcoins or Ethereum), or changing the state of some asset owned by a member (through custom smart contracts).

Bitcoin and Ethereum are two famous examples of public blockchains, i.e. the blockchain is available to anyone who is interested, all members have equal access to the blockchain, and all members participate in validating the order of transactions (otherwise known as "consensus"). Some of the controversy tied to blockchain comes from consensus protocols, especially in the case of Bitcoin and Ethereum. Their consensus protocol ("proof-of-work") uses a lot of processing power and rewards the users proportionally to how much processing power they allocate for the consensus protocol (this is what is referred to as mining). A study from 2020 estimated that for every USD of bitcoin created in the USA, there were environmental damages equivalent to almost 0.5 USD (!)

When a new block is added to the blockchain it refers to the preceding block. If you wanted to change the transaction history within the previous block, due to the hash referring to the previous block you would have to generate a new block for the subsequent block. In addition to this, in bitcoin the majority accepts the longest chain as the valid chain, so you would have to perform this work faster than the rest of the network; you would need more than 50% of all the physical mining resources in the network. This is the 51% attack. The reason this is generally accepted as a non-risk, is that it is deemed less profitable to spend your resources attacking the blockchain than actually just mining.

Other than decentralized currency without the fees that come with centralized banking, the use cases of blockchain centre around smart contracts which empower organizations and corporations to formulate contracts as code which fulfil themselves automatically. This would result in faster fulfilment (less bureaucracy = more efficacy), as well as decreased costs (no TTP = no extra fee).

Consensus

What is “proof-of-work”?

“Proof-of-work” is the consensus protocol used to validate, order and assemble bitcoin and (at the time of writing) Ethereum transactions into blocks for the blockchain.

Bitcoin is a public permissionless blockchain, which means it is accessible to anyone wishing to connect to it. When everyone is free to connect to and make transactions on the network, to avoid duplicate transactions and other malicious acts you need a way to be able to verify and validate correct transactions. This is what proof-of-work aims to do.

When proposing a block you first assemble some transactions (in this case, bitcoin transactions), the hash of the previous block, and a nonce (a number that doesn’t do anything other than change the hash of the block). To create the block, you must find a hash for the block that begins with a certain number of 0 bytes by incrementing the nonce (the more 0s, the heavier the computation), this is what is known as the difficulty. There might be multiple proposed blocks for each addition to the blockchain, but the first block that satisfies the difficulty is added. While it is possible to have multiple parallel blockchains, in the long run the longest chain will prevail. This makes the act of adding a block to the blockchain a democratic process between all members of the blockchain network, in that the majority of processing power decides the next block.

What is “proof-of-stake”?

“Proof-of-stake” is another consensus mechanism for blockchain. “Proof-of-stake” is at the time of writing not in widespread use, but is included in the roadmap for Ethereum 2.0.

As with “proof-of-work”, “proof-of-stake” is a mechanism to establish a consensus about the order and validity of transactions within the blockchain, however the approach is different. Instead of awarding the block to the agent with the most computing power, the miners “stake” at least 48 ETH (at the time of writing equivalent to over €10 000) to gain the ability to validate block monetary stake of assets for block validation instead of processing power is to further de-incentivize fraud, as you can end up losing your stake. Additionally, the blockchain is designed to make it more lucrative play by the rules than against them. If you do not have enough ETH to fulfil this requirement, you can join a pool together with other miners.

“Proof-of-stake” differs from “proof-of-work” in that there is no significant computing power expended to create and validate blocks. Nodes that stake their ETH are randomly chosen to either create or validate blocks, without all the hassle of calculating a difficult hash.

Consensus

The 51% attack is perhaps the biggest problem with public consensus mechanisms and there is at the time of writing no way to prevent this completely, multiple successful attacks have been committed on various public blockchains. With “proof-of-stake”, the 51% attack with “proof-of-work” becomes less likely because of the penalties that can be doled out to peers who endorse malicious blocks. If a peer in the blockchain endorses a malicious block, the peer risks losing their entire stake, which as previously mentioned is a lot of money. In addition to this, “proof-of-stake” penalizes being disconnected, thereby increasing availability of the system.

These are the main arguments for switching over to “proof-of-stake” for Ethereum, but it has yet to be proven that it works in real life. At the time of writing, there are no blockchains on the scale of Ethereum and Bitcoin that use “proof-of-stake”, so whether the switch pays off or not will be interesting to see.

What is a Smart contract?

Within blockchain technology, one of the most attractive points for business applications are smart contracts. They enable businesses to write code instead of physical contracts, and these coded contracts are automatically fulfilled when conditions agreed upon by both parties are fulfilled. This has the potential to decrease costs for both parties, as well as time spent on bureaucracy. This however is not the only use case for smart contracts.

As well as being used for legal contracts between corporations, smart contracts can be applied in numerous fashions within blockchain networks to run distributed applications on multiple clients.

Smart contracts are not limited to transferring assets (e.g. cryptocurrency) from one party to the next, but can also be used to change states of programmatic objects defined within the application. A very simple example is a car ownership application. In the application, there are multiple cars owned by different people. One person initiates a transaction to buy a car, and another person initiates a transaction to sell this car to the person. The smart contract takes the input from the peers and completes the trade by changing the state of the car object, changing ownership from one person to the next, all without making any physical transfers between users of the application.