ROBINSONS, LAWYERS

羅本信律師行

Distributed Ledgers, Blockchain and Consensus Mechanisms

September 2021

A ledger is a book that has rules to determine entry and striking of its contents. A distributed ledger is a replicated, shared, and synchronized ledger spread across multiple locations. The database is spread across multiple nodes on a peer-to-peer network, with each node operating independently with consensus mechanisms working throughout the network to ensure cohesiveness.[1]

A blockchain is a type of Distributed Ledger that is authenticated by mass collaboration based on collective self-interest. The authentication of a blockchain is done by the creation of blocks which are cryptographically hashed and linked (chained) with the previous block. Due to the hashed links, blockchains are immutable, since a previous block cannot be changed without invalidating all later blocks.[2] To ensure all blocks are the same on the network, consensus mechanisms allow all nodes to independently agree on the blocks without trusting each other.[3] Private blockchains need not use a consensus mechanism, instead they use less computationally intensive error checking. Consensus mechanisms exist to prevent sockpuppetry (fraudulent creation of fact verification actors) from commandeering a network by effectively making a hostile takeover prohibitively expensive.[4]

Consensus mechanisms

Consensus mechanisms are the system whereby the blockchain maintains its own validity across all nodes in the network. The several mechanisms in use or postulated are:

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[2] https://doi.org/10.1016/bs.adcom.2020.08.011

[3] ibid.

[4] https://ethereum.org/en/developers/docs/consensus-mechanisms/

- Proof of Work (PoW): the primary method used today, it involves computers performing computation heavy hash puzzles to compete over who gets to create the new block and earn the associated reward. The people who perform this are known as miners.
- Proof of Stake (PoS): a less popular system that is believed to be the future of blockchain; instead of relying on expensive computations PoS relies on stakes in the network to determine who creates blocks. The exact mechanism that a large network (Ethereum) would need to implement PoS is not yet known, but it will likely be and loosely be based on staking coins where the more coins staked as a percentage of total staked, the more blocks the stakeholder can validate, and therefore the more coins that stakeholder can earn (from the block rewards). Consider this analogous to property-based voting.
- Proof of Capacity: an alternative to PoW where instead of computational power, computer storage is used. It can be thought of as somewhat analogous to the lottery where the more storage space you have the more tickets you have so the better chance you have to win. There is some computation used in the system for the plotting of the drives and the actual creation of the block, but it uses far less energy than PoW.
- Proof of Authority (PoA): PoA is utilized in permissioned or semi-permissioned networks, where a central authority determines who has the right to create new blocks. This removes the advantages of decentralisation and lack of key vulnerability to a blockchain, but requires far less power and gives faster transaction time.

In general, consensus mechanisms can be thought of as a way to ensure the sincerity of the parties involved. This is generally done by showing a vested interest in the network through staked or spent resources. Then the network randomly selects an individual based on the amount of sincerity shown to create the next block. The decision is important since the person who validates the block has the ability to choose which transactions get entered into the ledger. A 51% percent attack refers to the scenario whereby an individual actor gains control of the majority of the "votes" meaning they can prevent and roll back transactions, or in some cases change the network.[5] [6]

Nevertheless, a 51% attacker cannot move all assets directly. Control of assets that exist on the blockchain along with identity are inextricably linked, both being tied to the private key. The blockchain can be thought of as a vast land filled with transparent vaults, each vault completely indestructible save for a private key. These vaults are known as wallets, serving both as an identification and a repository; private keys are numbers between 1 and 2^256. Each private key is attached to a public key where the assets are assigned; and crypto assets are moved by an

[5] https://www.bloomberg.com/news/articles/2021-08-04/crypto-coin-bitcoin-sv-appears-to-have-suffered-a-51-attack
[6] https://www.fxempire.com/education/article/51-attack-explained-the-attack-on-a-blockchain-513887

instruction signed with their respective private key. The link between private keys and public keys is a function, which is impossible to reverse computationally. This means that an attacker would still need a private key encrypted instruction to move another wallet's funds. That being said, an attacker could just rollback the block which assigned one the funds (this grows more difficult with the passage of time).[7]

The reason blockchain is touted as secure despite the potential for risk is simple: it's hard to have 51% of the proofing resource. The most common kind, PoW relies on computational power and while smaller cryptocurrencies are vulnerable to 51% attacks[8] for larger coins like Bitcoin or Ethereum such an attack would require a massive amount of resources. PoS is a little different. PoA has several vulnerabilities but it is unlikely anyone who held 51% would exploit their position, since the value of their stake would plummet. In general consensus mechanisms do not make the network immutable, but instead practically immutable and too costly to change. The value of cryptocurrency is strongly tied to how difficult it is to take over because the incentives are to maintain the functioning blockchain, and if it was easy to take over then the coin would likely have already been exploited.

Contributed by: Dr. James Lau and Mr. Charlton Diesch, Averell

ROBINSONS, Lawyers

羅本信律師行

Suite 1702-3, West Tower, Shun Tak Centre, 168 Connaught Road Central, Hong Kong
香港干諾道中168號信德中心西座1702-3室
網址 Website: www.RobinsonsLawyers.com
電郵 Email: service@RobinsonsLawyers.com

[7] https://news.ycombinator.com/item?id=18849961
[8] https://www.crypto51.app/