A Report on Blockchain

Blockchain Technology

Blockchain technology is a way of documenting data on the internet. It packages data into blocks which are linked to form a chain with other blocks of similar information. Once the data is recorded in a block, it cannot be altered without having to change every block that came after it.

Distributed Ledgers

Distributed ledgers are recorded, transparent, and decentralized. Its data is time stamped, anyone can see the ledger of transactions, and the ledger exists on multiple computers, often referred to as nodes.

A block in a blockchain will contain data, a timestamp and a digital signature linked to the account that made the recording, and a unique identifying link (in the form of a hash) to the previous block in the chain.

Blockchain technology is a type of distributed ledgers. It supports a decentralized peer-to-peer network, a collective trust model among unknown peers, and a distributed immutable ledger of records of transactions.

Blockchain

Composition. Each block has a content and a header. The header contains data about the block and its ordering.

Block ordering. Each block references the previous block by its fingerprint, which is determined by the contents of the block. By ensuring that the fingerprints are consistent with the data and that they join up in a chain, then you can be sure that the block is internally consistent.

Peer-to-Peer

Peer-to-Peer is a way of distributing data in a network, where each peer has 100% of the data and updates are shared around. It is less efficient than client-server in such that data is replicated many times, and each change or addition to the data creates a lot of noise. However, peer-to-peer networks are more robust.

Consensus

With peer-to-peer models where each peer is updating at different speeds and have slightly different states, the problem of deciphering the *real* or *true* state of data arises. A common conflict is when multiple miners create blocks at roughly the same time—which block, then should count as the legitimate one?

Longest Chain Rule. In cases of multiple blocks, treat the longest chain as legitimate.

Consensus Algorithm

Terminologies. A *node* is a point of connection within a network. *Mining* is the process by which transactions are verified and added to the public ledger; the process of generating correct proofs in order to add a block to the blockchain. *Hash algorithms* are mathematical functions used in cryptography.

A consensus algorithm is a process used to achieve agreement on a single data value among distributed systems. It is designed to achieve reliability in a network involving multiple nodes. It is capable of two things: ensuring that the next block in a blockchain is the one and only version of the truth, and keeping powerful adversaries from derailing the system and successfully forking the chain.

Some criticisms on consensus algorithms are its need for big computational energy, that it does not scale well, and that the majority of mining is centralized in areas of the world where electricity is cheap.

Proof of Work

Proof of work is the kind of consensus algorithm that functions as a tool and is used to process blocks of transactions and add them to the blockchain; it is used for *block generation.* The individuals that participate in the mining process are known as miners. The proof of Work requires miners to solve complex cryptographic puzzles and receive block rewards.

In order to get to the block, miners must compete with other minters to find a correct hash (the answer to the PoW puzzle) for each hash function. How complex a puzzle is dependent on the *number of users, current power, and network load*. The hash of each block contains the hash of previous block.

Proof of Work is used in a lot of cryptocurrencies. The main benefits of PoW is that it is good defense for anti-Denial of Service attacks, and low impact of state on mining possibilities. PoW imposes limits on actions in the network. Efficient attacks require a lot of computational power and a lot of time to do calculations, therefor rendering it useless since the costs are too high.

The main disadvantage of PoW are huge expenditures,"uselessness" of computations, and 51% attack. Mining requires highly specialized computer hardware to run the complicated algorithm, and their calculations are not applicable anywhere else save for the block. They guarantee the security of the network at the cost of not being applied to the business, science or any other field. A 51% attack, or majority attack, is a case when a user or a group of users control the majority of the mining power. The attackers get enough power to control most events in the network. Although, 51% attack is not a profitable option: it requires an enormous amount of mining power, and gets the network considered compromised through public exposure. This leads to outflow of users and a drop on cryptocurrency price.

Proof of Stake

The proof of stake uses validators that depend on criteria based on their economic stake in the network. Validators are individuals that are chosen to generate a block. A validator generates a new block by sending a special type of transaction that locks up their deposit. This deposit serves as collateral for the block generation process. If the validator attemps to cheat and validate fraudulent transactions, their deposit is slashed. Validators that correctly validate blocks of transactions are returned their deposit and given a transaction fee for the validation process. A validator's economic state can include:

Relative Value is the percentage of the value of coins in a validator's wallet against the total value of coins on the network. The more coins a validator has in his wallet, the more likely of being selected to generate a block.

Coin age is the coint amount multiplied by the number of days that the coins have been held in a wallet.

One problem with this algorithm is the **Nothing at Stake Problem**. This problem describes an event in which two blocks are produced at the same time, and validators are incentivized to form blocks on top of both competing chains just ot be sure they are backing the chain that will eventually win out. The problem is that the convergence of the two chains might never occur, because staking does not induce the convergence of competing systems, since the same stake can be applied to multiple competing chains, which results in a risk-free way of validators to increase rewards. This may be overcome through the slashing strategy, where validators are penalized in the form of slashing a validator's deposit should they simultaneiously form blocks on multiple chains.

Proof of Burn

The miners of the Proof of Burn coins send coins to an unspendable address ("eater address") and thus taking them forever out of circulation (burning them). These transactions are recorded on the blockchain, ensuring that there's necessary proof that the coins cannot be spent again, and the user who burned the coins is issued a reward. Proof of Burn can also be seen as when a blockchain network applies several consensus mechanism algorithms to ensure that all participating nodes agree about the correct and valid state of the blockchain network.

Long term commitment. Burnt coins enables greater price stability for the coins because long-term investors are unlikely to sell or spend their coins.

Unsold Coins. During ICO sales, some companies burn their unused coins instead of selling them. This way, only the value received from the actual sale was uesd to develop their blockchain application.

Transaction Fees. A minor amount of a transaction can be burned. By doing this, user pays for the transaction, and the network benefits from the usage of Ripple because there is less and less of their cryptos in circulation, which then drive the price up.

New Coin Creation. Burning cryptocurrencies give value to newly created tokens.

Byzantine Fault Tolerance

Byzantine Fault Tolerance is the ability of a distributed computer network to function as desired and correctly reach a sufficient consensus despite malicious components of the system failing or propagating incorrect information to other peers. It’s objective is to mitigate the influence that these malicious nodes may have on the correct function of the network. As a a result, the right and correct consensus is reached by the honest nodes which are still in the system.

Practical BFT model focuses on providing a practical Byzantine state machine replication that tolerates Byzantine faults(malicious nodes). The assumption is that the amount of malicious nodes in the network cannot simultaneously equal or exceed a third of the overall nodes in the system.Each round of pBFT consensus comes down to 4 phases:

1. A client sends a request to the leader node to invoke a service
2. The leader node multicasts the request to the backup nodes
3. The nodes execute the request and then send a reply.
4. The client awaits for the replies with the same results and with a count of more than the maximum number of nodes that may be faulty. That reply will be the result of the operation.

The primary advantage is its ability to provide transaction finality without the need for Proof-of-Work models. If a proposed block is agreed upon by the nodes in a pBFT, then the block is final.

However, the pBFT model only works well in its classical form with small consensus group sizes due to the amount of communication required between nodes. It is also susceptible to sybil attacks, where a single party can create or manipulate a large number ofidentities, thus compromising the network. THis is mitigated against larger network sizes, but scalability and throughput ability is reduced with larger sizes as well.

Public and Private Blockchains

Blockchains can be ‘public’ in two senses: anyone, without permission granted by another authority, can write data, and anyone, without permission granted by another authority, can read data.

Consortium blockchains is a blockchain where the consensus process is controlled by a pre-selected set of nodes. The right to read the blockchain may be public or restricted to participants. These blockchains are considered to be partially decentralized.

Fully private blockchains are where permissions are kept centralized to one organization, and participants are known and “allowed” by the rest of the network.

References

[1] /@chainfundch, “Blockchain Basics 01: A Comprehensive Collection - Chainfund,” Medium, 05-Sep-2018. [Online]. Available: https://medium.com/chainfundch/week-1-a-comprehensive-collection-of-blockchain-basics-5c5403702e8a.

[2] /@coinbundle, “Consensus Algorithms - CoinBundle,” Medium, 10-Oct-2018. [Online]. Available: https://medium.com/coinbundle/consensus-algorithms-dfa4f355259d.

[3] Ethereum Foundation, “On Public and Private Blockchains,” Ethereum Blog. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

[4] A. Lewis and A. Lewis, “A Gentle Introduction to Blockchain Technology,” Bits on Blocks, 30-Oct-2018. [Online]. Available: https://bitsonblocks.net/2015/09/09/gentle-introduction-blockchain-technology/.

[5] T. K. Sharma, “How to Pick the Best Consensus Algorithm for Blockchain?,” Blockchain Council Blockchaincouncilorg. [Online]. Available: https://www.blockchain-council.org/blockchain/how-to-pick-the-best-consensus-algorithm-for-blockchain/.

[6] “What is Blockchain? » Explained Simple: Lisk Academy,” Lisk. [Online]. Available: https://lisk.io/academy/blockchain-basics/what-is-blockchain.

[7] “What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide,” Blockonomi, 11-May-2018. [Online]. Available: https://blockonomi.com/practical-byzantine-fault-tolerance/.