CrushCrypto

What is Proof of Work?

Educational Series

September 18, 2018

Overview

- There are many protocols that regulate how nodes on a blockchain achieve consensus, and currently the most popular is proof-of-work. A blockchain-based proof-of-work system was first implemented with the release of Bitcoin in 2009, although the concept originated in the 1990s.
- Proof-of-work is a consensus mechanism that relies on a difficult computational task to secure the network from malicious actors. A proof-of-work system has miners: computers that compete to solve the difficult task first. Whichever miner solves it first broadcasts the result to the other miners, who can easily verify that the task has been solved correctly.
- The system is called proof-of-work because that is what miners are providing – the winner computer is finding a piece of data that proves a sufficient amount of computational work has been done to get the right output.

Overview (continued)

- In a proof-of-work system, the more computational power a miner has, the greater chance they have of winning the competition with other miners. The more miners there are competing to find the winning piece of data, the more secure the network becomes.
- Cryptocurrencies that use a proof-of-work system include Bitcoin (and all forks of Bitcoin), Ethereum, Ethereum Classic, Litecoin, Monero, Dash, Zcash, Decred, and more.

History

- Bitcoin was the first popularized implementation of proof-of-work, but the concept has been around for much longer. The idea was first proposed in a 1993 academic journal by Cynthia Dwork and Moni Naor, although the name “proof-of-work” was coined by Markus Jakobsson in 1999.
- In 1997, Adam Back proposed Hashcash – a proof-of-work system used to limit email spam and denial of service (DoS) attacks. It worked by requiring a stamp in the form of textual encoding to be added to the header of an email to prove the sender has used a modest amount of CPU time to calculate the stamp prior to sending.
- The idea was that spammers, who rely on sending many emails with no cost per message, would stop sending spam if each email they sent had a small computational cost. This was one of the first practical implementations of a proof-of-work system.

How does it work?

- On a proof-of-work blockchain, while transactional data is being added to the current block by nodes, other computers called miners are attempting to crack a code that validates the block.
- The mining process is comparable to guessing a random long password – the more computing power you have, the faster you can make guesses thus giving you a better chance to validate the current block. The code is generated through a cryptographic algorithm called hashing, and there is no way to crack the code without trying random combinations through repetition.
- After validation, the "winning" miner broadcasts the result and the other miners on the network can prove that the code is correct. At this point the data in the block is sealed and miners move on attempting to guess the next block's code.

Incentivization

- People are incentivized to use their computers as miners through automatically distributed block rewards: the miner that correctly guesses a block's code receives an allocation of new coins tied to that block. The inflation rate is programmed into the blockchain and there is no other way to mint new coins.
- The winning miner also receives the transaction fees used by every transaction in the block they validated. Incentivization in a proof-of-work system is extremely important because miners are the main actors in protecting the network from malicious actors.

Incentivization (continued)

- Considering there can only be one winner and the number of miners has grown over time, the odds of a single machine guessing the correct code is astronomically low. People have got around this by creating mining pools: networks where people commit their computing power to a pool of other miners.
- If the pool mines a block, the block reward is proportionally split based on how much computing power each machine provided. This has kept the barrier to entry low for proof-of-work mining.

Example of network security

- Someone wants to send out a malicious transaction on the blockchain to credit their wallet with 10 BTC from a random user's wallet. They broadcast the faulty transaction on their copy of the blockchain, and for it to be accepted as valid, they would have to mine the current block, in turn creating a new fork of the chain that credits them 10 BTC.
- If they don't mine the block, the miner that does would broadcast their version of the block with its valid data, not including the faulty transaction.
- Even if they succeed in getting their transaction into a confirmed block, (1) they must continue to solve blocks faster than the rest of the non-malicious miners, and (2) other miners agree that this chain is the valid one.

Network security

- In general, there are two principles to guide which chain is the legitimate chain for a coin – the chain with the most blocks, and/or the chain with the most accumulated mining difficulty.
- To outpace the networks miners over time, 51% of all the networks computing power is required. This is called a 51% attack and is the main security vulnerability in blockchain systems. It's also the reason why a blockchain becomes more secure as the number of miners goes up.

Additional resources

- https://en.bitcoin.it/wiki/Proof_of_work
- https://hackernoon.com/consensus-mechanisms-explained-pow-vs-pos-89951c66ae10
- https://bitcoin.stackexchange.com/questions/8031/what-are-bitcoin-miners-really-solving
- https://cointelegraph.com/explained/proof-of-work-explained

CrushCrypto