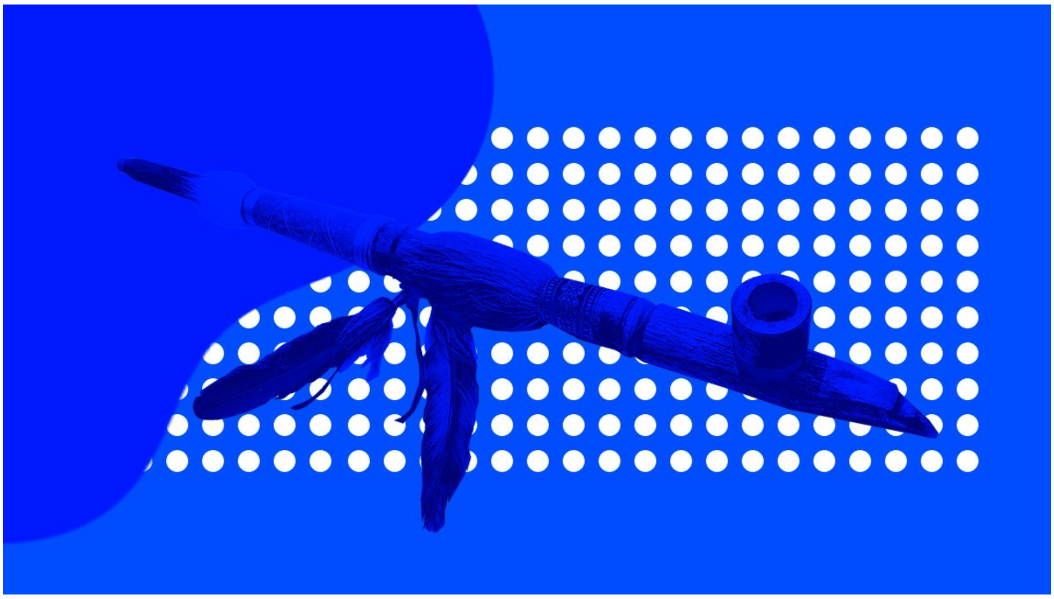
Gleb Kostarev Follow
PR #blockchain #cryptocurrency #fintech
Jul 31, 2017 · 5 min read

Review of blockchain consensus mechanisms



Cryptocurrencies use distributed ledgers or blockchains to record information—primarily about the balance of every address for value transfer platforms (like bitcoin and most cryptocurrencies), though the approach can be extended to any kind of information. Key to the operation of the blockchain is that the network should collectively agree on the contents of the ledger: instead of authority for keeping accounts being centralised in one entity, like a bank, it is shared amongst everyone.

This requires that the network maintains consensus around the information recorded on the blockchain. How this consensus is achieved impacts the security and economic parameters of the protocol. Here are five examples of how it's done.

1. Proof of Work (PoW)

Proof of work is the first distributed consensus mechanism, pioneered by bitcoin's pseudonymous creator, Satoshi Nakamoto. Many cryptocurrencies followed suit, including Ethereum. In PoW, all the computers in the network that are tasked with maintaining the security of the blockchain—known as Miners in bitcoin—work to solve a puzzle consisting of a mathematical function called a hash. This task is straightforward (for a computer) but extremely repetitive, and therefore computationally expensive. Computers compete to find a hash with specific properties. The computer that finds the answer first —the proof that they have done the necessary work—is allowed to add a new block of transactions to the blockchain. They are rewarded with a tranche of newly-minted bitcoins (currently 12.5 BTC per block, or roughly every 10 minutes), plus all of the small transaction fees users have paid to send coins.

PoW operates on the principle that it is expensive to add a tranche of new transactions to the blockchain, but very easy to check if the transactions are valid due to the transparent nature of the ledger. Miners collectively verify the entire blockchain, and transactions aren't considered to be fully 'confirmed' until several new blocks have been added on top of them. If a malicious actor tries to spend coins fraudulently, those transactions will be ignored by the rest of the network. The only way that an attacker could commit such a fraud is to possess a huge amount of computational power, such that they could mine block after block, winning the proof of work competition time after time. This is known as a '51% attack' due to the need to possess more than half of total network hashrate. The reality is that no miner has such a proportion of total hashing power. Thus attempting such a fraud is 1) extremely expensive (since it costs as much as the hardware and energy required, plus the opportunity cost of not supporting the valid version of the blockchain and receiving rewards in return) and 2) extremely unlikely to succeed. Consequently it is better (i.e. more profitable) for miners to remain honest.

2. Proof of Stake

Due to the amount of computational power required, PoW is costly and energy intensive. A whole industry has grown up around creating custom chips designed only for mining. Proof of stake (PoS) is an alternative approach that has gained popularity in recent years and that requires no specialist hardware. In PoW, hashrate determines how likely a participant is to add the next block of transactions to the blockchain. In PoS, the participant's coin stake determines their likelihood. That is, each network node is linked to an address, and the more coins that address holds, the more likely it is that they will mine (or 'stake', in this instance) the next block. It is like a lottery: the winner is determined by chance, but the more coins (lottery tickets) they have, the greater the odds. An attacker who wants to make a fraudulent transaction would need over 50% of coins to process the required transactions reliably; buying these would push the price up and make such an endeavour prohibitively expensive.

The PoS system was pioneered by Nxt. Because it is not energy-intensive, like PoW, the costs do not need reimbursing in the same way as they do for bitcoin. Thus PoS systems are well suited to platforms where there is a static coin supply, without inflation from block rewards. Stakers' rewards consist only of transaction fees. This is the approach taken by most crowdsale-funded platforms, where tokens are distributed based on investment, and diluting this with more coins would be viewed unfavourably.

Proof of stake is now a well-established consensus mechanism, but is not often used in its original form. Two variations, LPoS and DPoS, offer certain advantages.

3. Leased Proof of Stake (LPoS)

In classic PoS, holders with small balances are unlikely to stake a block —just as small miners with low hashrate are unlikely to mine a block in bitcoin. It may be many years before a small holder is lucky enough to generate a block. This means that many holders with low balances don't run a node, and leave maintaining the network to a limited number of larger players. Since network security is better when there are more participants, it is important to incentivise these smaller holders to take part.

LPoS achieves this by allowing holders to lease their balances to staking nodes. The leased funds remain in the full control of the holder, and can be moved or spent at any time (at which point the lease ends). Leased coins increase the 'weight' of the staking node, increasing its chances of being allowed to add a block of transactions to the blockchain. Any rewards received are shared proportionally with the leasers. This is the approach taken by Waves.

4. Delegated Proof of Stake (DPoS)

A similar but different approach is taken by BitShares and a number of other platforms. With DPoS, coin holders use their balances to elect a list of nodes that will have the opportunity to stake blocks of new transactions and add them to the blockchain. This engages all coin holders, though may not reward them directly in the same way as LPoS does. Holders can also vote on changes to network parameters, giving them greater influence and ownership over the network.

5. Proof of Importance (PoI)

A final variation on these consensus mechanisms is PoI. The first cryptocurrency platform to implement this was NEM. With PoI, it is not simply coin balance that matters. NEM's consensus system is based on the idea that productive network activity, not just the amount of coins, should be rewarded. The odds of staking a block are a function of a number of factors, including balance, reputation (determined by a separate purpose-designed system), and the number of transactions made to and from that address. This provides a more holistic picture of a 'useful' network member.

There are many variations on these broad approaches, and some platforms use a combination of PoW and PoS—often using the first to distribute coins, and then shifting to the second at a later point to maintain the network. Another approach is to use Masternodes in conjunction with PoW mining, as is the case with DASH and Crown.

These help to process transactions and receive a share of the block rewards from miners' activity.

In all cases, the aim of the consensus approach is to secure the network, predominantly through economic means: it should be too expensive to attack the network, and more profitable to help protect it.

Join Wavescommunity: http://wavescommunity.com/
Join Waves News channel: https://t.me/wavesnews
Join Waves twitter: http://twitter.com/wavesplatform
Join Waves Facebook: https://www.facebook.com/wavesplatform/