Consensus mechanism of cryptocurrencies and their social and environmental effect

Cryptocurrencies, such as bitcoin, are based on blockchains. The blockchain is stored in many different nodes within a non-centralised network. The nodes have a consensus where all of them agree about the previous transactions that have been made in the past and they cannot be modified due to the cryptographical feature of the blockchain. This work explains how the consensus mechanism works in Bitcoin and in the future Ethereum 2.0, when a new block is added to the blockchain, which contains all the recent transaction, and this way, keeping track of the users states and balances and preventing “double spending” or other malicious attacks.

The process of adding a new block to the blockchain in bitcoin is called “mining” because the “miner”, the person who successfully adds the block, receives, as a reward, a specific number of coins, which are “artificially created”, in the same way real miners are wealthier when they mine precious metals from the earth.

The consensus mechanism used in bitcoin is called “proof- of-work”. The miner proves to the other nodes in the network that work has been done to create a new block. The other nodes verify his work and reach consensus to add this new block into the blockchain. The “work” that has been done for mining is to solve a “cryptographic puzzle”.

The way to solve a “cryptographic puzzle” is to find a specific number known as “nonce” which together with the block header (which contains a hash of all the transactions in the block) will hash (with SHA256) to a value that is lower than a given target. As the result of a hash function is unpredictable, the only way to find such a number is to try again and again different numbers. The work done by computing SHA256 of the block header together with possible nonces until the hash image is lower than the target, is the “work” in the consensus mechanism. If only one node in the network was used to mine bitcoins, it would take thousands of years to find this number, hence there are more than a million bitcoin miners around the globe who compete to find the cryptographic puzzle solution. It is expected that a new block will be added to the blockchain every 10 minutes. The competition between nodes and the difficult setting can regulate the time need to mine a new block, however the computation power used by all the miners only increases as new miners (and miner farms) are added to the network competing between each other. Moreover, the bitcoin miners use specific powerful equipment which is capable of calculate hashes in a very fast rate, which increase the need of electric power and electricity to cool them down.

Ethereum, the second largest cryptocurrency, uses “proof-of-work” as the consensus mechanism, similarly to bitcoin, however it has formally initiated the process to move to “proof-of-stake” consensus mechanism to become Ethereum 2.0. In “proof-of-stake”, there are no miners but “validators”. They do the job of transaction verification and new block addition, which is known as block minting or forging instead of mining. After a new block is added, others validate the block, this validation is known as “attesting”. In “proof-of-stake” there is no competition between users to become the “validator” of the block, the validator is chosen pseudo-randomly between the users who have left certain amount of coins in the network as “stake”. The higher the stake, the higher the probability to be chosen as “validator”. If the “validator” adds fraudulent transactions into the block, or the “attester” attest a fraudulent block, they may lose their stake, or part of it. For that reason, the fees gaining by the validator should be always smaller than the stake. This way, the network can trust on the validator and the attesters to reach consensus for only valid transactions. Once a node decides not to be a possible validator anymore, he receives back the stake plus the total fees he received by validating blocks, however this amount is released after a certain period of time, in case a fraudulent transaction is detected. There should be at least 128 validators, which form a committee, that propose and validate a block, and they should do this in a specific timeframe, a “slot”. Only one block could be created in that slot. Another time-frame exists, known as “epoch” which contains 32 slots. After each “epoch”, the committee is dismantled and a new one is created with other random participants.

We have learnt that the consensus mechanism in bitcoin, known as “proof-of-work” consumes huge amount of electric power which most of it is wasted as more than a million miners around the globe compete to solve the cryptographic puzzle first, but only one manages to be “miner” and receive the reward and the sum of the transaction fees. The latest research done by the University of Cambridge states that Bitcoin uses 129.22 terawatt-hours of electricity annually which is more than the total energy consumption of big countries such as Ukraine and Argentina. On one side, part of the consumed energy comes from renewable sources, however the leading bitcoin miner country is China, where two-thirds of its electricity comes from fossil fuel which add carbon dioxide to the atmosphere and hence increase the greenhouse effect in the planet.

On the other hand, “proof-of-stake”, which will be used in Ethereum 2.0 and it is used in other cryptocurrencies such as Peercoin, Lisk and Nxt, doesn’t need specific equipment and there is no competition between users, this lead to a significant reduction in the overall electricity consumption to reach consensus. In addition, “proof-of-stake” is more decentralized than “proof-of-work” where miners work together forming “pools” which hold great part of the network, this could potentially cause a 51% attach. This type of attack will be more improbable in “proof-of-stake”, hence we can conclude that “proof-of-stake” is more secure. However, there is a downside in “proof-of-stake”, it always benefits the users who have more stake, the richer users, this way, it generates more inequality in the society.

In conclusion, “proof-of-stake” has much more benefits than drawbacks, it improves the security, the scalability and the sustainability. And these are the reasons why Ethereum is investing money and time in moving to “proof-of-stake” from “proof-of-work”. In the same way, the latest developed cryptocurrencies work with this type of consensus mechanism.

References

Anonymous2021, Mar 06. High cost of digital currency. The Press. ISSN 01139762.

Antonopoulos, AM 2017, Mastering Bitcoin: Programming the Open Blockchain, O'Reilly Media, Incorporated, Sebastopol.

Chowdhury, N 2019, Inside Blockchain, Bitcoin, and Cryptocurrencies, Auerbach Publishers, Incorporated, Milton.

ethereum.org. 2021. Proof-of-stake (PoS) | ethereum.org. [online] Available at: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/> [Accessed 29 July 2021].

99 Bitcoins. 2021. What is Bitcoin Mining? How Does it Actually Work? (2021 Updated). [online] Available at: <https://99bitcoins.com/bitcoin-mining/> [Accessed 29 July 2021].