# Blockchain Technology

The State of the art for Blockchain technology can be seen in the changes to the Ethereum platform that are being developed and rolled out starting in 2020, primarily to try and increase the number of transactions per second that the platform can achieve. In “Blockchain: State of the art ” [1] From 2017, the author concludes that they will be watching for technical developments in proof of stake and sharding, as well as the formalized recognition of crypto currencies and the development of projects to use blockchains.

The launch of Ethereum 2.0 is currently expected around July 2020 [2], and features several changes to make the platform more robust and scalable. In an interview with cointelegraph.com one of the co-founders of Ethereum, Vitalik Buterin, outlined the two phase of introducing Ethereum 2.0 [3] The first phase will involve changing from a Proof of Work model to a Proof of Stake model. The second phase will introduce the concept of sharding the data on the blockchain, which is a concept to reduce the barriers to scalability of the platform.

The transition to proof of stake from proof of work is a change to the consensus mechanism used by the blockchain platform, and the means that a third party is avoided when confirming transactions on the chain and preventing double spend of value. The proof of work system is based upon advanced cryptography which creates output from equations that is unique and immutable. This has been the basis for the majority of blockchain systems and was proposed in the original Bitcoin system of Satoshi Nakamoto. However some of the major drawbacks to the computational complexity in proof of work systems is the computational power required in the calculations causing large electricity costs and limiting the number of transactions that can be processed in a given amount of time. The mathematical problems must be brute forced to be initially solved, and the design of the system varies the complexity of the problem depending on the available computational power on the network. Another major flaw in proof of work systems is that theoretically if someone can control 51% or more of the computational power of the network, they could manipulate the result of the verification of the transactions, and destroy the immutability of the previous blocks by recalculating them.

In a proof of stake model there is still cryptographic computation, however the load is reduced. Rather than having to compete to be the first to solve a computational problem, any party that wants to create the next block on the chain has to invest an amount of value for the blockchain that they are bidding to verify. These parties can be referred to as verifiers as they are solving the small computational puzzles that are the transactions that are to be added to the block. The reward for producing the next block on the chain is the value of the transaction fees generated by the activity of others using the platform. The chance of winning the transaction fees is based on how many coins have been staked and the percentage of the total pool that they represent. This avoids the theoretical issue of someone controlling 51% of the computational power of the network as brute force is no longer the governing factor in determining who creates the new blocks on the chain. The system relies on it being highly unlikely for someone to control the majority of the value on the platform. As a disincentive to poor verification or fraudulent verification of transactions which would harm the network, parties risk losing the value that they have staked, making it economically unfeasible to endanger the network.

In the second phase of the implementation of Ethereum 2.0 a process called sharding will be used to break the database into pieces and distribute the pieces across the nodes of the network. This is applying a concept used in managing large centralized databases to achieve scale and manage traffic loads. In terms of the Ethereum blockchain it would involve splitting the network into segments or shards which would hold a set of the account balances and smart contracts of the broader network. Rather than each node having to run the entire ledger, they only need to maintain a smaller section, which allows for the transaction validation to occur in parallel rather than in a linear fashion. This allows for the rate of transactions to be increased and the platform become more practical for long term widespread adoption.

The move to Proof of Stake rather than Proof of Work will also assist in allowing the Ethereum blockchain to be sharded. [4] In a Proof of Work chain, validation of transactions needs the history of transactions, but a sharded database only has part of the history. There are concepts such as a “proof chain” proposed by Peter Todd [5] where the integrity of transactions can be determined without access to the whole database. While this can produce a system that could validate transactions on the client side, the complexity of the system does increase greatly. With Proof of Stake the validation of the sharded chain is made easier because the work required is only required to be done on a proportion of the total number of transactions. [6]

In order to coordinate a sharded Blockchain, a separate chain is used for maintenance and assignment of nodes into their shards. This is referred to as the Beacon chain for Ethereum. The beacon chain uses randomness for shard assignment, manages stake processing and has snapshotting abilities. [7]

The Impact of the changes proposed in Ethereum 2.0 is going to depend on if it solves the speed and scalability issues inherent in current blockchain implementations [8] As the changes are going to be delivered in phases, there is a lengthy rollout period of the Ethereum 2.0 roadmap. Each phase of the roadmap will need to be rolled out before developer can start to build the applications that will make use of the features. There is also a significant amount of the future roadmap that is actually still in the research stages, with no guarantee that the changes will work to improve the speed of the system to the three to six seconds for a transaction.

In a major change such as Ethereum 2.0, there is also a question of what happens with the value of the coins that are currently in the system, as they need to be transferred over to the new technology, or replaced by something new. There are several issues with creating a link between the two versions, but if there is a linking in the future, there may need to be manual intervention to reverse transfers of value from the 2.0 chain to the older version if the Ethereum 2.0 chain is broken. [9] It is however likely that the two chains will operate for several years before they are merged together.

The effects of these changes on individuals will depend on the success of the changes. Blockchain technology has received a significant amount of interest outside of developers and researchers, but this has had more to do with the media coverage of large dollar values of bitcoin that actual changes to people day to day lives. A potential negative effect of Blockchains for individuals is that the mining of coins requires significant financial investments, and will exacerbate the differences between the haves and the have-nots. This is regardless of proof of work or proof of stake systems, as the proof of work requires large inputs of computing power to compete, and proof of stake requires value to gain a share of the rewards.

References

[1] <https://fr.linkedin.com/pulse/blockchain-state-art-prospective-simon-polrot?trk=related_artice_%26amp%3Bamp%3Bquot%3BBlockchain%26amp%3Bamp%3Bquot%3B%E2%80%8B%3A%20State%20of%20the%20Art%20and%20Prospective_article-card_title>

[2] <https://www.coinspeaker.com/developers-ethereum-2-launch/>

[3] <https://cointelegraph.com/news/vitalik-buterin-reveals-ethereum-20-roadmap-to-cointelegraph>

[4] <https://thenextweb.com/hardfork/2019/01/18/explainer-blockchain-sharding-beginners/>

[5] <https://petertodd.org/2015/why-scaling-bitcoin-with-sharding-is-very-hard>

[6] <https://thenextweb.com/hardfork/2019/01/18/explainer-blockchain-sharding-beginners/>

[7] <https://hackernoon.com/sharding-and-the-scaling-of-a-blockchain-xz1kq30j0>

[8] <https://blog.sfox.com/ethereum-2-0-what-the-next-three-years-of-ethereum-will-look-like-b366a46f9704>

[9] <https://www.coindesk.com/5-takeaways-on-ethereum-2-0-from-vitaliks-beast-mode-blog-posts>