Towards the Future of Ethereum with Proof-of-Stake

Choosing a Central Authority in Distributed Ledger Systems

In distributed ledger systems, there is no single, pre-determined central authority (CA) for deciding upon the world state. If the system *permanently* assigns this role to a specific network participant, he can unilaterally censor transactions and even halt the network. To mitigate this centralization issue, the selection of the CA should not be deterministic. For example, in blockchain systems, a mechanism must randomly pick a participant as the CA for each new block to be proposed. However, when randomly selecting a network participant, it must be made sure that someone cannot increase their chance of getting selected by creating new identities (i.e., Sybil attack), as this is usually free. Hence, the probability of getting selected must be bound to a *scarce resource*.

To establish a block proposer selection mechanism that is not susceptible to Sybil attacks, Ethereum utilizes *Proof-of-Work* (PoW). In PoW, the scarce resource is computational power. To become the next block proposer (or "miner" as it is called in PoW systems), a participant must solve a complex hash puzzle, as this proves that computational power has been expended. The miner who solves this puzzle first and propagates his block to the network is awarded the block reward (2 ETH fixed reward + transaction fees). Due to this economic incentive, mining has been a popular activity in the Ethereum community. Currently, the cumulative computational power of Ethereum miners produces approximately 900 terahashes per second. However, this has a *pernicious* impact on the environment as computation on mining hardware requires a large amount of power. According to Digiconomist, Ethereum's current carbon footprint is around 43.24 Mt per year, which is comparable to the annual carbon footprint of Hong Kong. Moreover, Ethereum's annual electrical energy consumption is similar to Chile's annual consumption (77 Tw/h).

An Alternative Approach

Like PoW, *Proof-of-Stake* (PoS) is another mechanism blockchains utilize for choosing the next block proposer in a Sybil attack-resistant way. In PoS, the network members who want to participate in block production must *stake* money to the protocol. Unlike, PoW, PoS does not require the participants to solve a complex puzzle. Thus, no mining hardware is required. Instead, participants are financially involved (in case of misbehavior, the protocol can slash the stake). Due to that, PoS chains consume significantly less energy than PoW chains.

The Vision of Ethereum

In 2015, Ethereum launched to be a *decentralized*, *scalable*, and *secure* chain. With the growing demand, transaction fees climbed up, and the disk space required for running an Ethereum client increased rapidly. Keeping the chain secure with PoW has also become a problem due to its detrimental environmental impact. One way to scale while not giving up security guarantees would have been to become more centralized. However, Ethereum did not want to compromise its decentralization which is critical for the network's *transparency* and *trustlessness*.

To tackle this problem bounded by the *scalability trilemma*, Ethereum developed an elaborate upgrade plan. While the scalability issue will be addressed with sharding and layer-2 solutions (e.g., rollups), to achieve a sustainable and secure chain, Ethereum decided to switch to PoS. Using PoS was, in fact, the goal since the beginning but wasn't adopted initially due to its complexity and bootstrapping issues (check this article by Vitalik Buterin, written in 2014). With PoS, Ethereum aims to reach the following goals:

- Making Ethereum greener by reducing energy consumption by **99.95**%
- Becoming more **secure against colluding attacks** (e.g., 51% attack) with the slashing mechanism
- Increasing the involvement in the protocol by **decreasing the barrier of entry** (running mining hardware requires more overhead and can quickly become more expensive than staking)
- Lowering the ETH issuance by 90% (compared to PoW-Ethereum) in order to make Ethereum **deflationary**, thus, increasing its value over time (this movement already began with EIP-1559)

Note: *PoS, by itself, won't cause a dramatic improvement in the transaction throughput of Ethereum as the block time won't change significantly. However, it lays the infrastructure that will enable the implementation of the planned scaling solutions.*

The Beacon Chain and The Merge

Ethereum planned the transition to PoS in two steps instead of a single major step due to the significance of the change. The first of these steps was the launch of the *Beacon Chain* back in December 2020. The Ethereum community deployed the Beacon Chain as a separate, independent chain from the Mainnet of Ethereum. The Beacon Chain is a PoS chain projected to become the new *consensus layer* of Ethereum. Under the new architecture, the Beacon Chain will be responsible for producing blocks and reaching an agreement about the correct state of the chain, while the transactions and the contracts (i.e., EVM operations) will get executed on the current Ethereum Mainnet, which will become the *execution layer*.

In September 2022, the Ethereum Mainnet will be *merged* with the Beacon Chain, carrying over all the historical transaction and state data. The merge is triggered by reaching a particular total terminal difficulty instead of block height to prevent malicious entities from mining empty blocks to pull the merge date sooner than planned. Once the merge occurs, the current Mainnet will stop running PoW and only execute transactions, while the Beacon Chain will become the new consensus engine of Ethereum. However, this won't affect how end-users interact with Ethereum. This separation of execution and consensus layers is to achieve better *modularity*.

For the last 1.5 years, the Beacon Chain has been operating independently from the Ethereum Mainnet, gathering block proposers (called "validators") and, thus, collecting stakes. It launched sooner than its full usage such that there was enough time for staking and extensive testing without stopping the Mainnet (remember that bootstrapping is one of the main problems in PoS). With the increasing number of validators and total staked amount, the security of the Ethereum protocol also improves as decentralization becomes better and

financial involvement on the network grows. To become a validator on the Beacon Chain, one has to stake 32 ETH to the protocol. In return, validators get rewarded for building new blocks and attesting to blocks built by other validators. Based on the numbers on BeaconScan, Etherscan's block explorer for the Beacon Chain, there are 423,431 active validators and 13M ETH (> $22B) locked in the protocol.

Block Production and Security Post Merge

In the current Ethereum Mainnet, the block time depends on the mining puzzle's difficulty.[1] After the merge, the block time will be *fixed* to 12 seconds. To achieve this property, Ethereum divides the time into *epochs* and *slots,* where each epoch contains 32 slots, and every slot lasts 12 seconds. The protocol randomly selects a validator for each slot to propose a block. In case of misbehavior, such as proposing multiple blocks in a single slot, the respective validator gets penalized (i.e., stake slashed). Also, a set of validators (committee) are chosen at every slot to vote on the validity of the proposed block (at least 2/3 must agree). Any validator submitting contradicting votes is also penalized. A block becomes *finalized* after two epochs.

While the new mechanism has improvements over the PoW-Ethereum (e.g., faster, deterministic finality, resiliency towards misbehaving, etc.), it also has its issues. One of them is the *centralization of validators*. Currently, exchanges and staking pools (Lido, Coinbase, Kraken, and Binance) hold the most stake in the new protocol. Lido owns around 1/3 of the total stake, according to the numbers on Glassnode. In theory, this poses a real threat to the consensus stability of Ethereum, as Lido can potentially become a CA and use its power to extract MEV through history rewriting or censorship.[2] However, in practice, it is not expected for Lido or any other significant players to behave maliciously due to their reputation and the power they hold.

What's Next for Ethereum?

Once the transition to PoS is complete, Ethereum's roadmap includes significant upgrade packages taking place in parallel. One of them is *the surge* which aims to achieve better scalability by breaking down the main chain into many smaller chains (i.e., sharding). Currently, danksharding is one of the discussed actualizations of sharding on Ethereum. If implemented, it will enable low-cost layer-2 solutions, thus, better transaction throughput.

The verge is another upgrade package in Ethereum's roadmap, which introduces the Verkle trees. A Verkle tree is much like a Merkle tree, but it is more efficient due to the size of the proofs it provides. Through Verkle trees, Ethereum aims to enable stateless clients that do not have to store the entire Ethereum state but just use proofs to do block execution and validation. This upgrade will contribute to the decentralization of Ethereum by lowering the cost of starting up a full node.

The other two upgrade packages are *the purge* and *the splurge*. While the latter is about various interesting upgrades (e.g., Proposer Builder Separation (PBS)), the former eliminates the historical data over one-year-old. The purge will reduce the congestion on the network and lower the hardware requirements for running a full node. With lighter and faster clients,

Ethereum plans to increase the number of transactions it processes per second. Since the historical data is still necessary for some applications like block explorers (and for keeping a consistent history), Ethereum is looking for off-chain solutions to make the purged data accessible. Although the discussion is still ongoing (see EIP-4444), alternatives include using InterPlanetary File System (IPFS) or torrent magnet links.

Closing Words

Ethereum strives to achieve a secure and scalable network while not compromising its decentralization. The transition to PoS is the first significant upgrade toward realizing this plan. After the merge, a series of upgrades still await us. As the community, we should be aware of what's ahead as these changes will shape the future of Ethereum and, potentially, the future of the blockchain ecosystem.

[1] Currently, the block time is around 13-14 seconds.
[2] To mitigate an issue like this, Vitalik suggests minority user-activated soft forks where the honest community can choose to follow a minority chain and remove the malicious entity from the system.