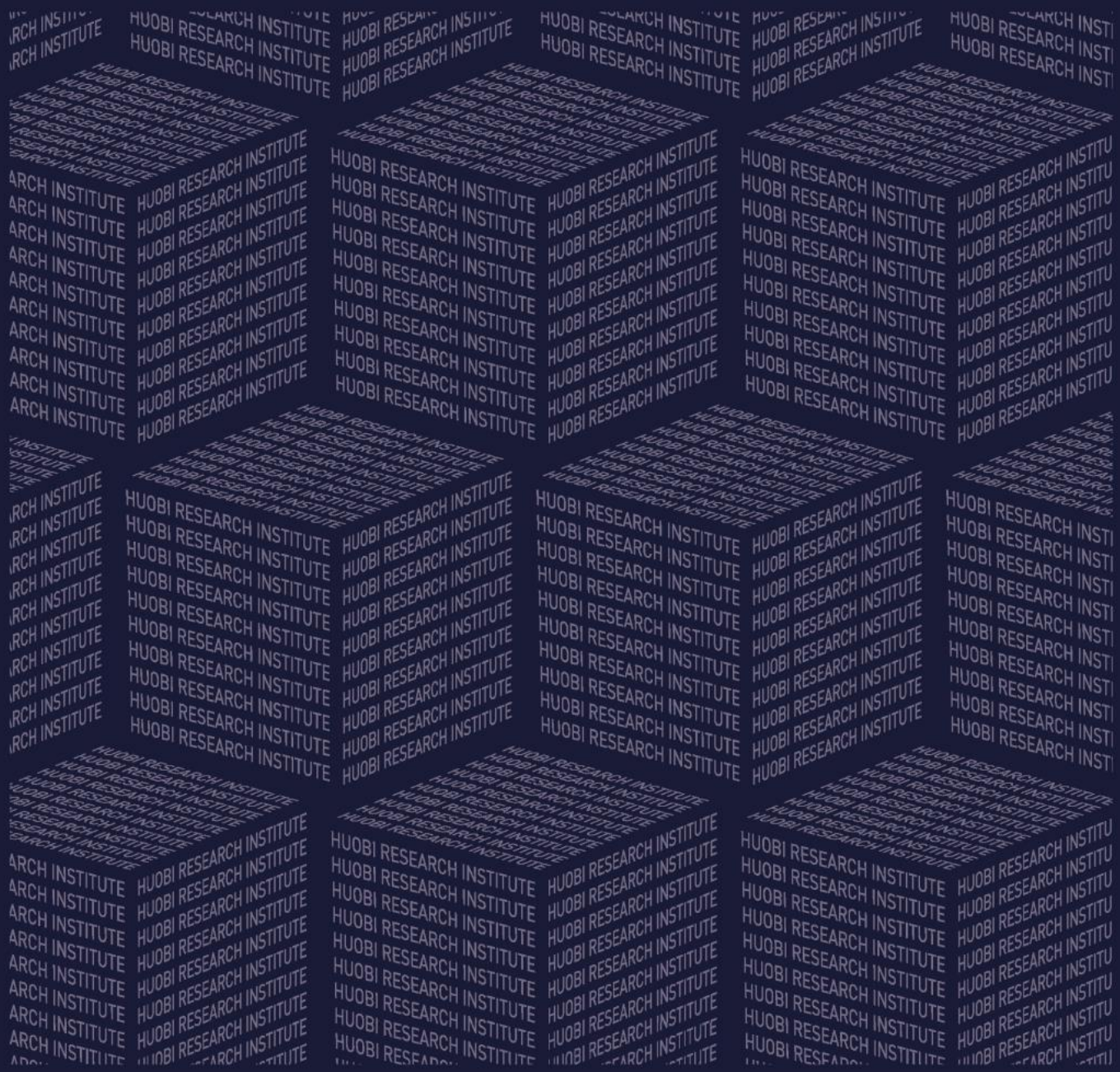

All You Need to Know about the Merge of Ethereum

Huobi Research

Authored by Huobi Research Institute researchers Barry Jiang and Tim Chen

Abstract

The current Ethereum Mainnet will complete the transition from proof-of-work to proof-of-stake by merging with the Beacon Chain, while preserving contract execution functions and full historical data with the current user state. The merge is not merely a response to the call for lower global carbon emissions, but also a critical step to lay the foundation for future upgrades including sharding.

After the Merge, changes will be seen in the network structure, block structure, consensus mechanism and state. The new block will carry the exterior of a Beacon block with contents from Ethereum proof-of-work (POW). The network will adopt an architecture in the form of a consensus layer and an execution layer (execution engine) to produce and synchronize blocks. The proof-of-stake (POS) consensus mechanism will be adopted in the new system where a verifiers' committee carries out the function of proposing and voting to form consensus upon certain blocks. The consensus and execution layers will be linked; and statelessness will also be introduced not only to help maintain the degree of decentralization, but also contribute to future sharding.

After the Merge, ETH may enter a deflationary state and the network will be more energy-efficient. On top of that, the competitive landscape for layer 1 chain will be redefined by the Merge to some extent: previous ETH miners will flock to other networks where extra hashrates could raise the price of corresponding tokens. Meanwhile, the Ethereum network will be upgraded by concentration on sharding after the Merge, and other POS layer 1 ecosystems will also experience distress.

With its scientific technical roadmap and an ambitious vision, Ethereum will see a gradual improvement in its performance after the Merge, sustaining its overall development. The previous POW network had to be aborted due to the difficulty bomb, and remains invalid even if a twin network is built by the miners - it will be volatile in absence of valuable assets, so hardforking is barely an issue. POS of Ethereum cannot solve the problem of "the rich getting richer", but the degree of decentralization is not undermined as the threshold is lower than that of POW. Maximal extractable value (MEV) still exists after the Merge. Even though some technical issues occurred during the Merge, it is still under control, while asset security is guaranteed.

On June 9, the Ethereum Ropsten testnet completed its merge, which was the first merge practice based on testnet. After the transition of Ropsten, Goerli and Sepolia will also be transformed to POS. The much-anticipated merge of Mainnet Ethereum and the Beacon Chain will take place between August and November. With the Merge, ETH's inflation rate will be around -2% from 4%. The redemption of Beacon Chain is expected immediately following the first hardfork (likely 6 months after the Merge). The arrival of the Merge is imminent.

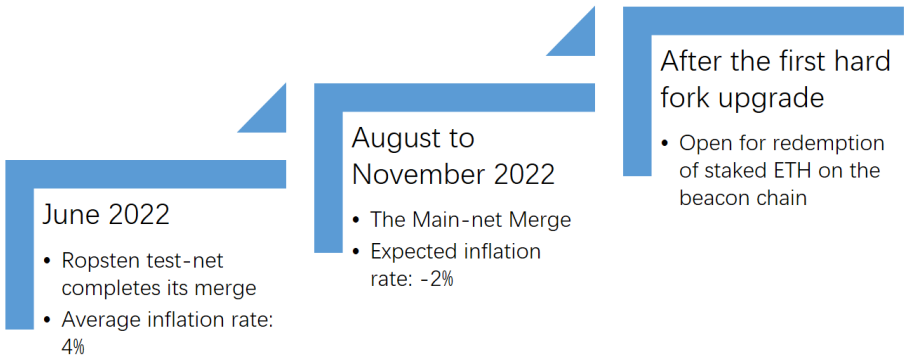

Figure 1: Timeline of the Merge

Source: Huobi Research

The Merge has been mentioned by many sources, but few provided a comprehensive view. In this article, a comprehensive view will be given in terms of the significance of the Merge, technical principle of implementation, influence on the industry and possible risks.

1. What is the Merge?

Two networks are live in the current Ethereum: one is our old friend, Ethereum blockchain network, which is powered by POW; the other is Beacon Chain (also called ETH 2.0 earlier), which is enforced by POS. Beacon Chain has maintained its stature after launch, with a steady increase in ETH staked in smart contracts, up to the current 13 million.

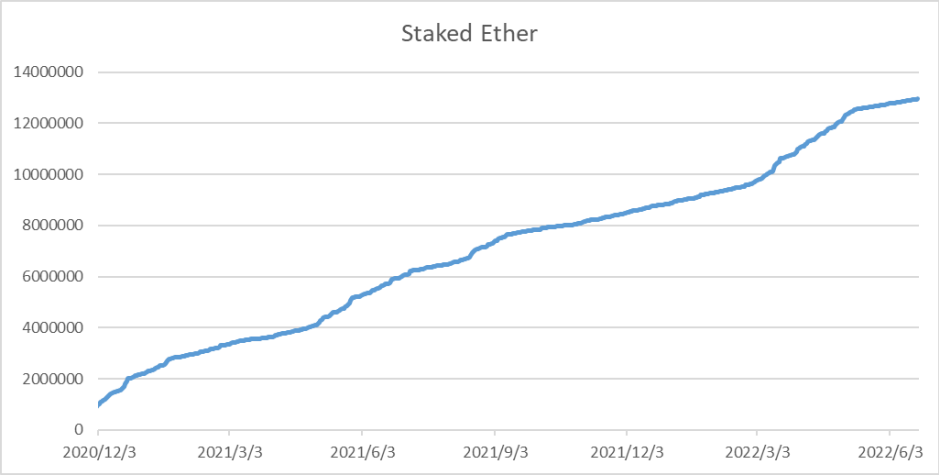

Figure 2: Amount of ETH Staked in Beacon Chain

Source: beaconcha.in

The Merge stands for the merger of the Ethereum blockchain and Beacon Chain. It is not a simple mathematical combination case. Instead, it is an integration and upgrade of the two: trimming the unwanted from the two that may undermine the long-term development of Ethereum, while preserving and combining the desirable parts.

That said, POW will be isolated from Ethereum Mainnet while retaining and transporting the function of smart contract execution, full historical data and current user status to Beacon Chain powered by POS. It is not merely a normal upgrade of forking, but a major change in the consensus mechanism.

Figure 3: What is the Merge

Source: ethmerge

POS verifiers will replace POW miners during the Merge. When it happens, Beacon nodes will monitor the current POW chain and measure a predetermined difficulty threshold value, which is called TERMINAL_TOTAL_DIFFICULTY: any block with a difficulty level over the threshold value will be marked as the final POW block. From then on, blocks generated and verified by verifiers on Beacon Chain will all be POS blocks, signaling the completion of the Merge.

If any technical issue occurs during the process, the network may become unavailable briefly. However, assets will remain safe no matter where they are stored as no consensus is present on the network – thus no theft can take place. Exchanges may disable deposits and withdrawals during the Merge, so users who are concerned with potential forced liquidation due to price volatility during the process may wish to make a deposit in advance.

In comparison with the Merge, the previous plan had intended to support 64 sharded chains on Beacon Chain with independent Ethereum POW operations for another 3-5 years, where users can migrate at free will. Therefore, no such merge even exists. However, the Merge adopts the Ethereum Mainnet without POW as the first sharded chain of Beacon Chain, and integrates the two thereafter. Meanwhile, users and applications are migrated to the POS Ethereum network. The Merge now stands as the most viable route, as the previous plan's technical route with various sharded chains was associated with the unprecedented challenge of developing sharded chain in the short term. Conversely, the Merge could inherit the previous execution layer, which requires less effort. At the same time, there will be minimal impact on users in terms of discernible change; their transition costs are minimal.

2. Why the Merge?

POS in Ethereum cannot be achieved without the Merge. It serves two major purposes: the realization of sharding and savings in energy consumption.

2.1 POS is conducive to sharding

Ethereum's major drawback is its poor performance, which was exposed in 2017 on the blockchain game CryptoKitties. To lift its performance, the Ethereum community submitted proposals on hierarchy and sharding. ETH 2.0 (currently known as Beacon Chain) emerged as a result: to improve TPS from 15 to 15,000 by processing multiple transactions on sharded chains at the same time. Due to technical constraints, the total shard count was reduced from 1024 to 64, but the idea of sharding has never been off the table.

Although Beacon Chain is in place to assign and coordinate verifiers to various sharded chains in Ethereum's technical structure, the system would not operate the same way under different consensus mechanisms. For POS, the system requires the staking of 32 ETHs to acquire commensurate voting rights and staking benefits (without forfeiture). Tycoon verifiers may distribute funds to various accounts to become small verifiers in disguise, in order to receive more benefits. In other words, even if one holds a considerable amount of ETH, his or her holdings will be diluted to various sharded chains randomly; it is nearly impossible to receive higher voting rights in a single chain. Thus, verifiers are always in a state of balance within each chain. Unless there is a staking of 51% of the whole network, nothing could undermine the security of the network. For POW, miners are verifiers. Mining rigs are in the hands of miners, which could be connected or disconnected any time at their will. That is to say, the hashrate is unknown, which could vary within a short time period. If a giant miner

concentrates the hashrate to 0.51% of the whole network, he or she could take control of a sharded chain and undermine its security. For a safer sharding structure, POW must be replaced by POS.

2.2 POS is energy-friendly

According to Digiconomist, Ethereum has made progress when viewed against the energy consumption of Bitcoin mining. However, energy consumption of Ethereum mining (POW) still exceeds 44.46 TWH, which is equivalent to the annual energy consumption of Finland or Sweden. Each transaction costs 84 KWH in electricity, which could supply a household for 2.8 days. Under POS, the system does not require verifiers to repeatedly complete hash calculations with energy input; energy consumption will be reduced by more than 99.95% to maintain the network, improving energy efficiency by over 2,000 times. Each transaction only takes 35 KWH electricity, which is similar to the energy consumption for watching television for 20 minutes.

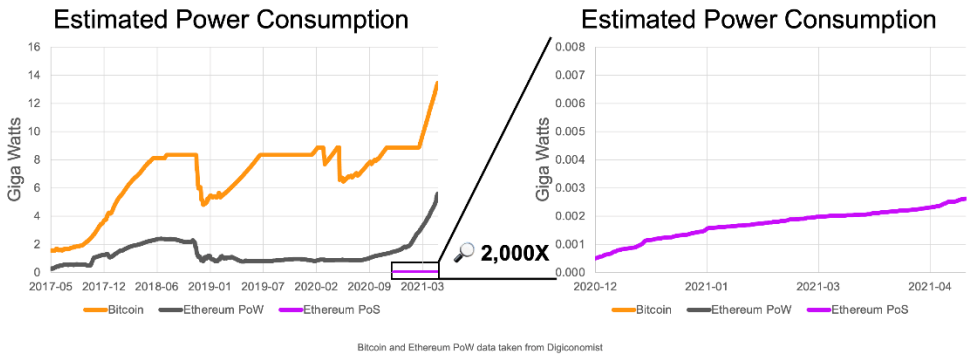

Figure 4: Comparison of energy consumption in Bitcoin mining, Ethereum POW, and Ethereum POS

Source: blog.ethereum.org

3. Changes after the Merge

3.1 Block Structure

In whole, blocks after the Merge can be viewed as the interior of Ethereum POW blocks coated by the exterior Beacon Chain blocks. Currently, the Beacon Chain only exerts POS actions on blank blocks, including the serial number of slots, father block root, state root, attestation, deposit contract root and validator slashing, etc. These actions share one characteristic in common: from the user perspective, no transactions, such as sending ETH or interacting with other contracts, are involved, so it is merely the provision of a 'shape'. The content is also called Execution Payloads after the Merge, namely the relevant information of execution, i.e., the transfers of Ethereum and interactions of smart contracts provided by the execution layer (previous POW nodes). The execution and consensus layers could be conflated at the block level.

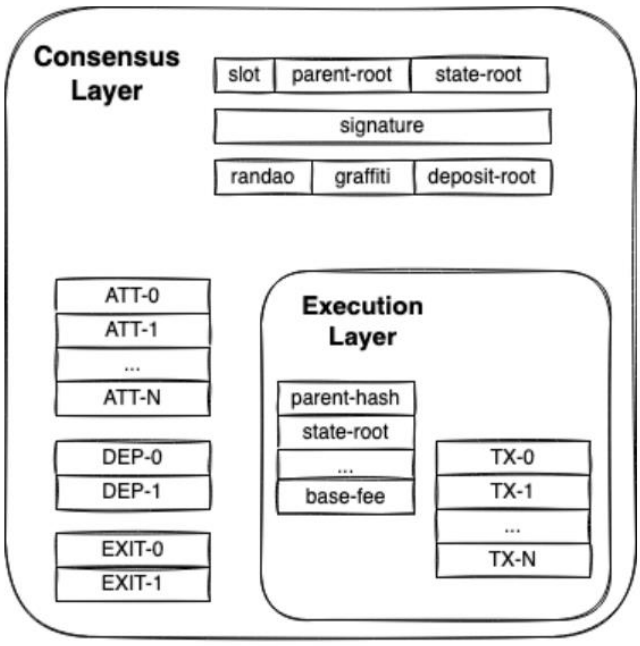

Figure 5: Ethereum block structure after the Merge

Source: Ethereum foundation blog

As POW is no longer in use, dynamic block strings related to POW, such as

difficulty, mixHash, nonce, ommers, ommerHash, will be automatically modified to 0 or other constant values; the length of extraData will also be limited to within 32 bytes.

Field	Constant value
ommersHash	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
difficulty	0
mixHash	0x0000000000000000000000000000000000000000000000000000000000000000
nonce	0x0000000000000000
ommers	[ ]

Table 1: Changes in poW-related fields

Source: EIP-3675

The consensus layer (Beacon nodes) still verifies all strings in current Beacon blocks, but contents in the blocks are now in the hands of the execution layer (current POW) to be verified.

3.2 Network Structure

After the Merge, the network structure will be modified. Ethereum employs the structure of a consensus layer and an execution layer (execution engine) to generate and synchronize blocks. Previously, the two P2P networks were mutually exclusive. After the Merge, they have to collaborate and coordinate while remaining independent.

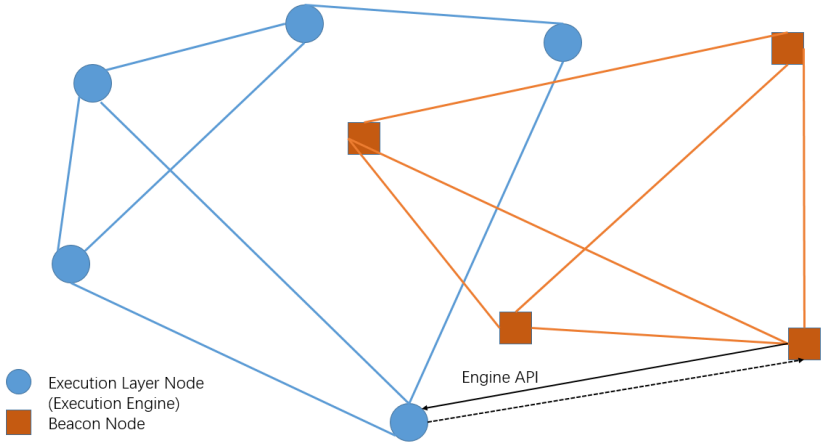

Figure 5: Ethereum block structure after the Merge

Source: Huobi Research

Transfers and calls of smart contract are packed, radioed and executed by the execution engine (previous ETH full nodes), with tips from the GAS fees staying in the execution engine. The primary goal of the execution layer is to establish communication with the execution engine, facilitating the generation or verification of Execution Payloads, and creating full Beacon blocks thereafter based on the consent from Beacon nodes. The engine API serves as the bridge between the two networks: The consensus layer captures contents to be consented from the execution engine via this venue, and calls for other execution engine nodes to validate the legitimacy of the transactions. After reaching consensus, the latest network state will be transmitted to the execution engine through the same channel, and the execution engine syncs with the state henceforth. In other words, the consensus layer helps the previous POW network to reach consensus.

As stated above, there will be a hierarchical relationship after the Merge. The consensus layer is similar to a commander, whereas the execution layer is the soldier. The following eth2 client chart explicitly demonstrates this relationship. This hierarchical relationship will ignite changes in the consensus mechanism and state.

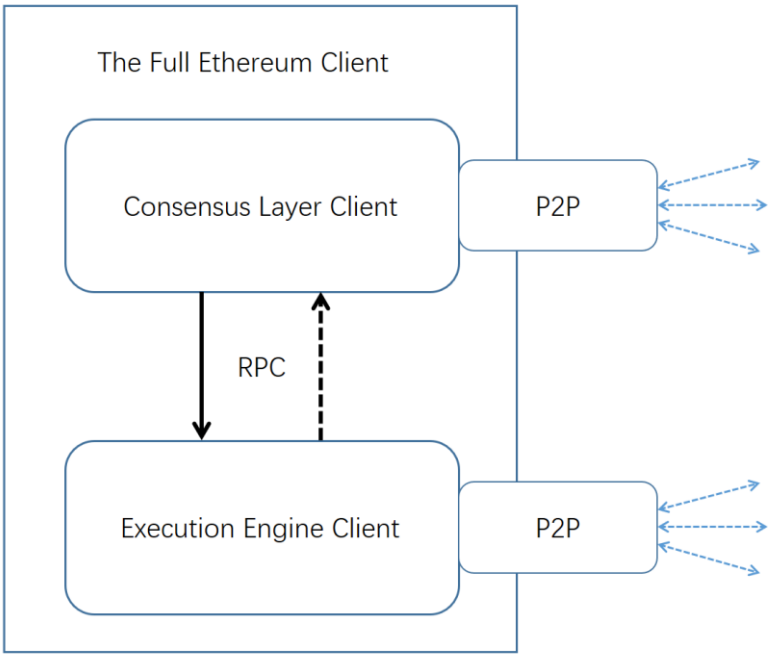

Figure 6: Structure of eth2 client

Source: ethresearch

3.3 Consensus Mechanism

The purpose of the Merge is to change the consensus mechanism. The Ethereum Beacon Chain will adopt POS where the committee of verifiers propose and vote to reach consensus on a certain block.

After the Merge, the timing unit of a block will be in the form of a slot and epoch. A slot is created every 12 seconds, and every epoch pack consists of 32 slots. An epoch is a fixed time period where verifiers will be re-assigned at the end of this period.

To become a verifier and get voting rights, users must stake at least 32 ETHs. As of June 20, there are over 403,000 verifiers. For consensus to be more efficient, the number needs to be smaller. The rule of Ethereum is that for every epoch, verifiers will be randomly assigned to 32 committees, ensuring that every committee consists of at least 128 verifiers. The system assigns 1 verifier to each slot using a random algorithm, RANDAO, and randomly selects a committee for this slot at the same time. This verifier is responsible for proposing the block, and the committee is in charge of the verification and voting towards the proposal. Once the vote passes, a block is produced, and the proposer receives rewards; otherwise, not only will the rewards be unavailable, the security deposit will also be forfeited. The same applies to the average verifier: rewards will be available if rules are properly followed, and penalties await for saboteurs. Eligibility to become a verifier will end once the 32 ETHs in staking fall to less than 16 ETHs.

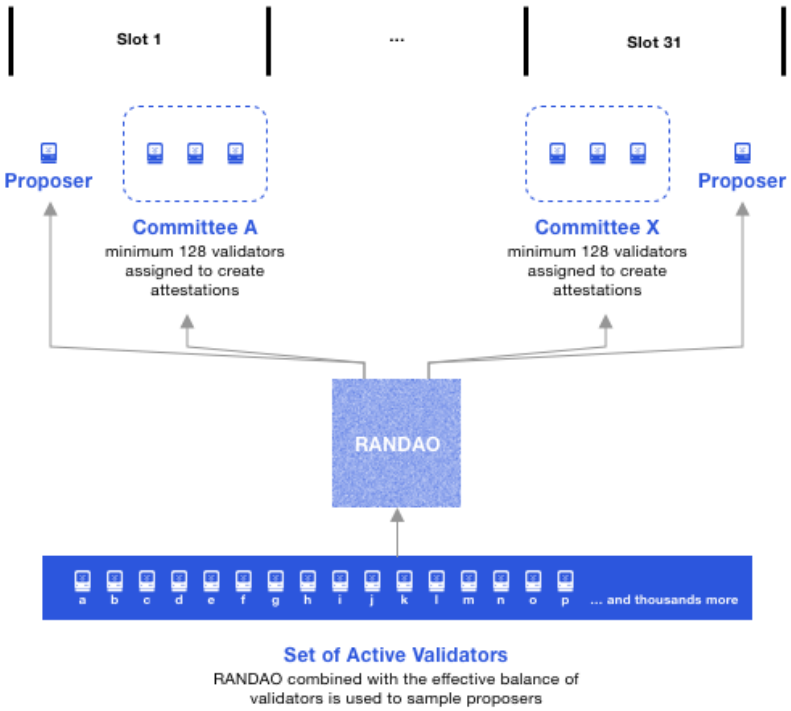

Figure 7: Ethereum POS consensus mechanism

Source: ethos.dev

The random selection process of verifiers and committees barely differs from

that of Beacon Chain before the Merge. The only difference after the Merge is that the consensus after the Merge must contain consensus on Execution Payloads. In future, when more shards are available on Ethereum, i.e., 4 shards, each committee will be divided into 4 equal shares to participate in voting of each shard.

3.4 State

Statelessness becomes a remarkable characteristic after the Merge as the change in network changes the state of network.

To begin with, Ethereum adopts an account mode, where each account consists of user state and contract state. State, in short, is the specific appearance of the system at a specific time, including account balance, the hash of contract codes or stored data. Full Ethereum state documents all accounts and the associated account balance, as well as historical records of all smart contracts that were deployed and executed in EVM. There is only one state for a block on the main chain after a consensus is reached by various nodes. Moreover, the state of the system continues to develop along with confirmation on new blocks. To be more specific, the node which produces a block needs to access and check current state of the system, record a new state after execution, and sync with other nodes in the network. Other client nodes need to verify and execute the transaction inside the block to ensure a consensus is always in place in the network.

As more new users and applications will be on Ethereum, more new data will be generated, and the state data of accounts will grow without limits. For nodes, it is nearly unrealistic to store all the state data in memory. If hard drives were to be considered, it may be too slow for a mechanical hard drive to read data, which results in difficulty in syncing the latest data with nodes, whereas solid

state drives are not cost-effective. In the long run, the issue of state inflation will require the nodes to have larger storage and stronger performance, which levels up the threshold of nodes operations.

To tackle the issue of state inflation, the community proposed two possible solutions: state rent and statelessness. The former imposed continuous rents to contracts which preserved state, otherwise the availability would end. It is complicated in practice: On one hand, the proper rent collection method cannot be determined; on the other it is hard to say who can be the legitimate recipient of the rent. As such, the exploration of state rents has been halted. The latter proposal enables the verification process of all transactions and states without the presence of actual storage of any states in light client.

The question boils down to one of why statelessness is so crucial for POS Ethereum? First, the threshold for hardware would be too high for nodes if it is simply adding the function of eth1 execution and all states to all Beacon clients. Taking into account the increasing difficulty of full nodes operation, the degree of centralization is exacerbated on Ethereum. The POS Ethereum aims to engage all nodes, either with all states or none at all to participate in the verification to maintain cyber security, which also brings about a high degree of decentralization in the network.

What's more, statelessness is a prerequisite for sharding. Ethereum may have several shards in the future, and each shard will consist of accounts and a contract state deployed on it. Each shard randomly selects verifiers to form a committee; that being said, if statelessness is absent, verifiers must possess all state data from all shards, which could overwhelm the average verifier. Sharding could mitigate the poor performance of Ethereum, while statelessness cements the highly decentralized Ethereum network. Statelessness is crucial in setting the stage for future updates, and it is a major technical upgrade.

With statelessness, Ethereum after the Merge would have 3 types of nodes/clients:

1. Clients without an ETH1 execution engine
2. Clients with an ETH1 execution engine with statelessness
3. Clients with an ETH1 execution engine with full state

The first type of client is lightest because it could only participate in reaching a consensus, but is unable to verify transactions from the execution layer. It exists to supervise other types of nodes on the consensus layer. The third type of client is fully functional with all states, executing capability and consenting capability – in other words, a full node. The number of the third type of client will be small as the investments required could be huge in data storge, hardware and tokens for staking. The second type of client wins in terms of statelessness, in that it calls for data from execution engines with state and verifies the validity of the transaction using its own execution power. Thanks to the cost savings for state storage, the second type of clients may be more common in the network.

4. Characteristics of the Merge

4.1 Certainty in time needed to produce new block

Ethereum will not enable blocks to be produced by adjusting the difficulty to increase the competitiveness for miners. In any case, each block can be produced after each slot, which takes 12 seconds. The benefits are:

- User experience is enhanced. For on-chain transactions, the user must wait for miners to pack. When the time needed to produce a block is known, one could easily estimate which block may consist of the transaction data at a certain time period, and thus predict the time needed to complete a transaction.
- For some DeFi protocols, the release of tokens relies on the number of blocks generated on Ethereum Mainnet, i.e., for every 1,000 blocks, 1

token would be released. That is to say, under the previous model even the time period to produce a block was around 14 seconds. When the network faced congestion, the time needed to produce a block became uncertain, which resulted in the erratic release of tokens for some DeFi protocols.

- More accurate planning for future upgrades. Based on past experience, each upgrade took place at a certain height of blocks. For example, the Berlin Upgrade happened at the height of 12,244,000 blocks. However, the specific plan was consistently postponed due to variations in the time taken to produce new blocks, which led to the community's dissatisfaction with the development team. If the time to produce a block is certain, it may alleviate the situation.

4.2 Lower threshold for client

As mentioned earlier, state inflation has made verification of the blocks even harder, which imposes stricter requirements on hardware. After the Merge, Ethereum enables the light nodes, which were unable to save the full network state before, to participate in the network and verify all transactions and state proofs. That is to say a mega miner is no more a must for nodes; devices at the service level are sufficient enough to participate in the verification network.

4.3 Seamless transition to POS

By the natural design of the development team, the Merge provides a seamless transition to POS for clients who will become the execution layer. For end users and developers, the execution layer is where most interactions with Ethereum take place, and most functions (for instance, EVM, state and execution method, etc.) and APIs will not change as a result of the Merge. As someone said, the Merge may be completed after one takes nap, and no one would even notice.

5. Possible Influences

No words may be enough to accurately describe the significance of the Merge for Ethereum. Although the performance bottleneck cannot be immediately resolved, all ambitions and the technical route of Ethereum must be built from this stage. As the first step on the voyage, the Merge is of far-reaching significance.

5.1 Deflation

As mentioned, the Merge will move Ethereum from POW to POS, stopping the production of new blocks under the current POW. This puts an end to traditional mining rewards. Any incremental ETH in the system can only be minted by participating in the POS verification process as nodes; this will greatly reduce the total supply of ETH. From the graph below, the issuance of ETH is expected to plummet when Ethereum moves to POS. Further, even when the Merge is completed, the system will not release any locked ETH in staking. By design, the first unlock of ETH will be granted after the first hardfork when the Merge is completed, which will be months later. Meanwhile, the system imposes a strict quota on the daily amount to unlock and the total number of applicants to prevent large-scale dumping.

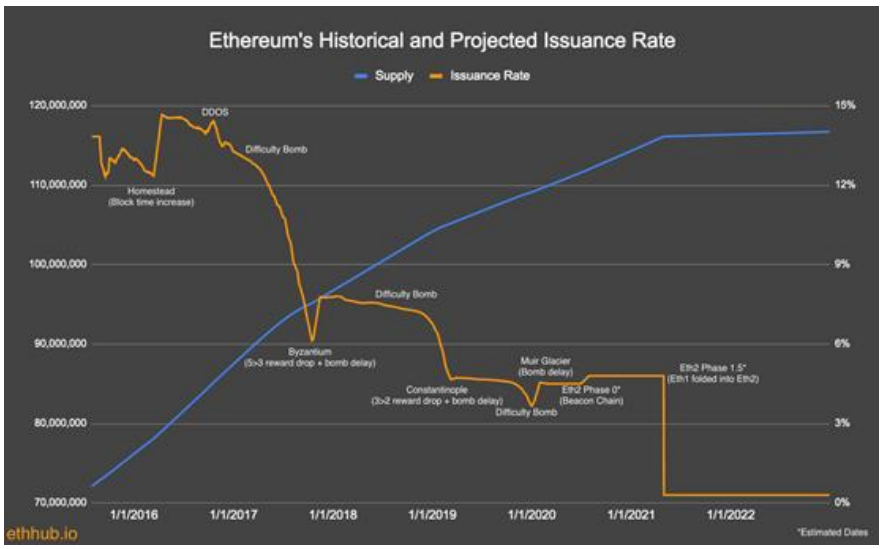

Figure 8: Historical ETH issuance vs predicted issuance rate

Source: ethhub.io

While the supply of ETH is cut, its net destruction rate is increasing. According to current data, the supply of ETH will grow to around 500,000, but due to the launch of EIP-1559, around 2.9 million (and possibly more) will be destroyed when the market is hot. From the two perspectives above, ETH will see deflation eventually, even without the demand from POS staking and protocols in the ecosystem.

Figure 9: Amount of expected issuance and destruction after the Merge

Source: ultrasound.money

Since the rule of supply reduction is analogous to the rule of Bitcoin halving, the community named it “triple halving”: Bitcoin needs three halving to reach the supply reduction effect of ETH by the Merge. From historical data, Bitcoin halving is closely tied to the crypto market life cycle: when the new supply of Bitcoin halved, its remaining liquidity on the secondary market was drained slowly, causing its price to rise and create a bull market. Similarly, as the

cryptocurrency with the second largest market capitalization, ETH's deflation may boost the market like what Bitcoin did.

However, the unlock may cause distress to ETH holders, which could take place before the unlock, accompanied by the short-term pressure of price cuts.

5.2 Energy savings

Although Bitcoin's success is convincing proof of POW's nearly impeccable credentials, miners use an enormous amount of energy to repeatedly calculate the sole hash that may become an asset. Given the current global emphasis on lower-carbon activities, POS may be just the solution.

5.3 Influence on layer 1 chains' competitive landscape

The Merge will eventually affect the current competitive landscape of layer 1 chains to some extent. Due to the existence of the difficulty bomb, time consumption will increase faster after the Merge. Theoretically, miner nodes are still able to mine by forking, but they must accept the trade-off between limited returns and continuously rising costs – which means giving up on Ethereum. Alternatives are also limited: To mine on similar POW chains, or sell mining devices for liquidity and invest in POS. For other POW chains, the influx of miners and hashrate may improve the current situation in the ecosystem and boost the price of tokens. For other POS chains, even though Ethereum has been accused of many drawbacks, no one could deny that the Ethereum community still dominates the industry and the security is top-of-the-line. After the Merge, shortages of Ethereum would start to be resolved, the thriving layer 2 ecosystems would further lower on-chain transaction costs, not to mention the integration of sharding would improve the network operational efficiency at large. The rising demand for Ethereum would eventually eat away at other ecosystems.

6. Risks of the Merge

6.1 Will there be a hardfork?

Recall that the current Ethereum is a product of hardfork. Will history repeat itself with this large-scale upgrade similar to the hardfork event of ETC? Based on current facts, Ethereum follows a scientific technical route and its legendary vision, which will greatly improve its performance and draw sufficient participation for more sustainable future development. On the other hand, the difficulty bomb would force POW miners to retreat from their original battlefield of Ethereum Mainnet. The community adheres to the Merge at a high level, so not a single strong voice for fork is heard from any joint miner groups.

Assuming that miners could simulate a new analogous network to Ethereum, for example ETH Legacy which is identical to POW Ethereum but without the difficulty bomb, the new network would face several strong competitors long before the launch. These include Ethereum and other layer 1 chains, and this challenge is additional to the issue of insufficient assets. After forking, ETH has to duplicate the whole ledger of Ethereum. Not only will the forked tokens emerge (for example, ETL), derivatives from other assets must also be dealt with, such as WBTC, USDC, DAI, LINK, BAYC, CryptoPunks, etc. No matter where the assets were issued, whether the issuing institutions are centralized or decentralized, only the uniqueness of the assets matters as only assets on one network will be recognized. To be more specific, only assets on POS Ethereum would be recognized by the issuing institutions as the bona-fide assets. Obviously, ETH Legacy or other similar entities are more likely to have an early demise due to poor performance, insufficient assets, and weak consensus.

In conclusion, a hardfork is less likely to take place after the Merge.

6.2 Will the degree of centralization be intensified?

Some may be concerned with the degree of centralization after the Merge. The POS consensus mechanism naturally vests those with large holdings with more interests – in other words, more voting rights, which signals more control over the network. The issue is not unique to POS: in POW, miners with higher hashrate could buy more hashrate with rewards from mining, increasing the chances for a block to be successfully generated. As such, POS does not solve the problem, nor does it exacerbate the situation.

The tremendous growth of Lido has drawn skeptics. Lido is a large-scale staking pool which accounts for over one-third of the whole network. Some claim that if another Lido presence were to be assembled, that presence would be capable of taking control of the whole network. What's worth noticing is that Lido is not controlled by any single entity. Lido has 30 node operators internally, which is mutually exclusive to each other or Lido. These operators are top-tiered node operators with accountable records and legal entities to pursue right to recourse; they must pass the vote of the DAO and remain under the surveillance of the DAO at all times. So, a single equation of Lido to a centralized mining pool is invalid. On the contrary, the continuous efforts on decentralization let Lido prevail in the competition with CEX mining pool. That said, the risk of monopoly power or collusion power taking over the network is not as high as commonly thought.

As mentioned, no mining devices or mining fields are necessary under POS, which lowered the barrier to entry for common users. From this perspective, Ethereum would be more decentralized under POS than under POW.

In summary, the stepping up of centralization is not a major concern.

6.3 Will MEV be eliminated?

MEV stands for Miner Extractable Value, inherently an action of arbitrage by miners when a new block is generated – similar to front-running in traditional financial trading. Specifically, as the room of on-chain block is limited, submission of transactions would enter mempool first and wait to be packed by miners. For miners, the right to decide the order of these transactions to be processed and on-chain lies in their hands. Normally, miners decide by the amount of GAS fee to be received: transactions with more GAS fees receive priority to be processed sooner. As a result, the priority of on-chain transaction processing depends not on the time of submission but how much GAS fees users are willing to offer; extra profits from this activity to miners are MEV.

When it changes to POS, the procedure for processing does not vary much. The execution engine takes the place of the miners to decide the order, which is, in effect, the same group of people. Therefore, the issue of MEV is not solved.

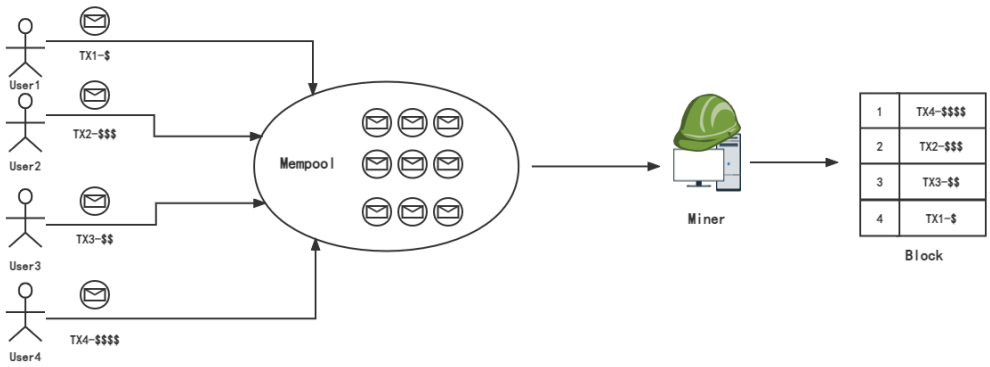

Figure 10: Processing order of transactions by miners

Source: Huobi Research

6.4 How risky is it from a technical perspective?

To rule out possible technical risks, the team implemented several shadow forking and testnet merge. Potential risks were exposed during the test.

Information leaked by an insider pointed to 14% of the verifiers being malfunctional during the merge on Ropsten testnet at the beginning of June, mostly triggered by incorrect node configuration. The situation was handled in a timely manner.

On June 22, the 7th shadow forking of Ethereum Mainnet encountered obstacles: 20% of the nodes went offline upon the activation after the merge, and more after. The glitch mainly came from the storage format of Besu Client; the team is currently working on the solution.

A shadow forking is to conduct a test merge between a forked network from an existing mainnet or testnet and a new test Beacon Chain. As few activities will be seen on the brand new testnet, data need to be "borrowed" to simulate activities for the purpose of a pressure test on the merge. This will test the team's hypothesis on the state sync and state upgrade to see if it is correct. In the most recent shadow forking, Ropsten testnet was the "borrowed" network. When the shadow forking for Ropsten testnet is completed, another shadow forking test on mainnet needs to be conducted. A successful shadow forking test signals foreseeable technical risk minimization in the Merge. The meticulous approach taken by the current merge team means they will conduct sufficient experiments before the Merge to minimize all risks.

Admittedly, the actual merge will somewhat differ from the test, and uncertainty remains in the actual process i.e. unexpected bugs in the client or an external attack. The team needs to deliberate all possible solutions in response to any unexpected events, which could be seen as the last line of defense. We believe all professional cyber security teams will collaborate closely to monitor the whole procedure to prevent any potential risk, as well as to provide active solutions in time.

References

[1]. https://tim.mirror.xyz/sR23jU02we6zXRgsF_oTUkttL83S3vyn05vJWnnp-Lc

[2]. https://ethresear.ch/t/eth1-eth2-client-relationship/7248

[3]. https://blog.ethereum.org/2021/11/29/how-the-merge-impacts-app-layer/

[4]. https://blog.lido.fi/the-road-to-trustless-ethereum-staking/

About Huobi Research Institute

Huobi Blockchain Application Research Institute (referred to as "Huobi Research Institute") was established in April 2016. Since March 2018, it has been committed to comprehensively expanding the research and exploration of various fields of blockchain. As the research object, the research goal is to accelerate the research and development of blockchain technology, promote the application of blockchain industry, and promote the ecological optimization of the blockchain industry. The main research content includes industry trends, technology paths, application innovations in the blockchain field, Model exploration, etc. Based on the principles of public welfare, rigor and innovation, Huobi Research Institute will carry out extensive and in-depth cooperation with governments, enterprises, universities and other institutions through various forms to build a research platform covering the complete industrial chain of the blockchain. Industry professionals provide a solid theoretical basis and trend judgments to promote the healthy and sustainable development of the entire blockchain industry.

Official website：

https://research.huobi.com/

Consulting email:

research@huobi.com

Twitter: @Huobi_Research

https://twitter.com/Huobi_Research

Medium: Huobi Research

https://medium.com/huobi-research

Disclaimer

1. The author of this report and his organization do not have any relationship that affects the objectivity, independence, and fairness of the report with other third parties involved in this report.

2. The information and data cited in this report are from compliance channels. The sources of the information and data are considered reliable by the author, and necessary verifications have been made for their authenticity, accuracy and completeness, but the author makes no guarantee for their authenticity, accuracy or completeness.

3. The content of the report is for reference only, and the facts and opinions in the report do not constitute business, investment and other related recommendations. The author does not assume any responsibility for the losses caused by the use of the contents of this report, unless clearly stipulated by laws and regulations. Readers should not only make business and investment decisions based on this report, nor should they lose their ability to make independent judgments based on this report.

4. The information, opinions and inferences contained in this report only reflect the judgments of the researchers on the date of finalizing this report. In the future, based on industry changes and data and information updates, there is the possibility of updates of opinions and judgments.

5. The copyright of this report is only owned by Huobi Blockchain Research Institute. If you need to quote the content of this report, please indicate the source. If you need a large amount of reference, please inform in advance (see "About Huobi Blockchain Research Institute" for contact information) and use it within the allowed scope. Under no circumstances shall this report be quoted, deleted or modified contrary to the original intent.