
10TH FEBRUARY 2023

Ethereum's Shanghai-Capella Upgrade

Since its inception in December 2020, Ethereum network validators have voluntarily locked their ETH on the Beacon chain without a solid timeline for the addition of a withdrawal function. The upcoming Shanghai-Capella will mark an end to that era, granting validators access to their ETH, alongside the rewards already earned for their validating duties. In this report we explore the details of the forecasted withdrawal process and its possible consequences on ETH supply.

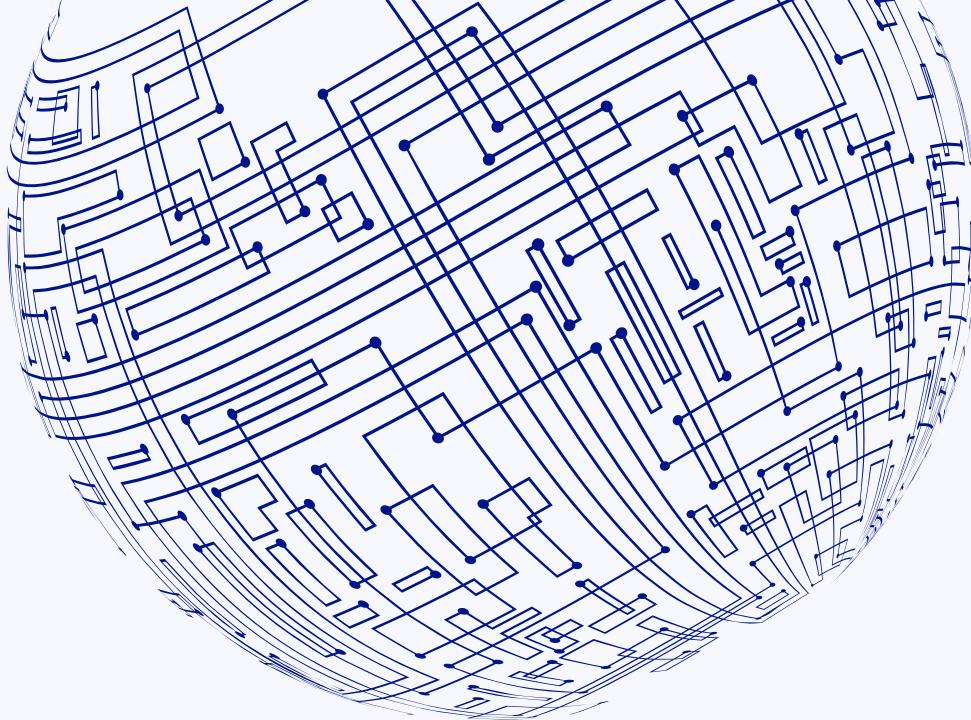


Table of contents

What is it?	3
The Staking Process	5
The Unstaking Process	6
Possible Implications	8
Other Upgrades	10
Conclusion	11

What is it?

The upcoming update to the Ethereum network's protocol is actually a pair of updates, named *Shanghai* and *Capella*. These are updates to the part of the Ethereum network that performs computation and transactions, the *Execution chain*, and the part of the network that controls the production and validation of new blocks, the *Beacon chain*, respectively. By *Execution chain*, we mean the part of the network that prior to the *Merge* handled both consensus (through mining) and execution (updating balances, changing internal states of smart contracts). More on the distinction between the two parts of the network can be found in our [article](#) that details the *Merge*, which resulted in the divorce of these two processes into two layers.

The *Shanghai* upgrade is a hard fork to the Execution layer of the network, the *Execution chain*, that is intended to implement a series of changes to some operations of the Ethereum network. Its most important update will allow validators to withdraw their staked ETH tokens for the first time since the Beacon Chain's inception in December 2020. When the network switched from Proof of Work mining to using the Beacon chain to control block production in September 2022, the Ethereum foundation set a tentative deadline to have withdrawals to be activated in the next update to the network.

Recently, that timeline was narrowed to some date in March 2023, pending the successful completion of several tests. The foundation's recent efforts reflect their commitment to achieving this goal in the originally promised time frame, going as far as postponing other upgrades originally scheduled to be deployed in Shanghai in order to prioritise the activation of withdrawals. Note that validators can currently pause their validating duties, effectively "un-staking" their ETH without withdrawing it. The *Shanghai* update allows *withdrawable* users (which we discuss later) to withdraw their ETH from the Beacon chain.

HOW WILL THE UPGRADE BE IMPLEMENTED

Just like in previous updates to the network, like the [Merge](#) or the [London](#) upgrade, the *Shanghai* update will be completed using a *hard fork*. This requires every node that is listening to or validating on the network to install a new version of the Ethereum network *client*. By *client*, we mean the program that each node runs locally in order to interact with the rest of the network. There are multiple versions of Ethereum clients, released by different third party providers, but each promises to implement the rules and logic of the open-source Ethereum protocol as defined by the Ethereum foundation.

Once a final version of the updated protocol is defined by the Ethereum foundation, each client provider will release an updated version of their clients containing both the new and old versions of the protocol. For all blocks after an agreed block height (the length of the blockchain from a block to the first block on the chain), each node on the network will begin using the updated version of the protocol. This ensures that the history of the network will remain unchanged. As the updated protocol will only apply to blocks with a higher block height than the agreed number, nodes will use the previous version of the rules should the chain be reverted to a block before the switch. This ensures that the network is in agreement on when the new rules apply.

TESTS

In preparation for the update to the network, the Ethereum foundation has created copies of the live Ethereum network on which to test their changes. This is achieved by configuring a small set of nodes (both validators and non-validating nodes) to branch off of the main network on an agreed-upon block. That side chain has the same history as the main chain (until the block that they branched from) and allows developers to simulate the planned network upgrades on separate chains and fix any bugs they might encounter. This process is called shadow forking, find more about it [here](#).

By *shadow forking* the main Ethereum chain, its developers have launched a series of public testnets available for developers to test their smart contracts on the proposer version of the network. Shandong, the first public testnet, was launched on the 14th of October 2022, which activated 5 planned upgrades but did not include Beacon Chain withdrawal functionality. Zhejiang, launched on the 1st of February, allows developers to test all the EIP's included in the final Shanghai-Capella update. This includes a simulation of the hard fork that will switch nodes from following the current version of the Ethereum protocol to the updated version, scheduled for the 7th February 2023. After the hard fork on the test net, users would be able to test the withdrawal processes with ETH that lives on that test chain, but which is not communicable with the live Ethereum network.

The Staking Process

Users can stake ETH on the Beacon chain in order to perform the work of validating new blocks and contributing to the security of the blockchain. In return, stakers earn rewards for doing their jobs “correctly” and are punished with penalties if they perform this dishonestly or “incorrectly”. This feature is available right now, and has been since long before the Ethereum network began listening to the Beacon chain to reach consensus on new blocks. However, until the *Shanghai* update, users will be unable to withdraw the ETH that they stake (including rewards and penalties).

To take part in this process, a user must have the software required to validate and propose new blocks (execution and consensus clients) running on their system. They must also generate a public key and private key pair that the Beacon chain can use to track the new validator. Once this is completed, the user must deposit 32 ETH to the [Beacon chain deposit smart contract](#) and include their public key (and some other [credentials](#)) as a data input to the transaction.

The successful deposit causes a “receipt” to be emitted on the Execution chain, formally known as a *Log*. That receipt contains data inducing the amount the user has deposited, and registers their deposit on the Beacon chain. The Beacon chain reads these logs from the Execution chain and includes the new staker in an activation queue. That action is processed on the Beacon chain as a transaction, much like how the functions of smart contracts are executed on the Execution chain.

The incoming validator is then placed in a queue of other incoming validators. This queue is processed in a first-in, first-out manner, with a minimum of 4 new validators admitted to the Beacon chain each epoch (6.4 minutes), or the entire queue if it is fewer than 4 validators long.

The upper bound of new validators added in each epoch is dependent on the existing number of validators currently operating on the Beacon chain. The higher the number of existing validators, the higher the cap on new validators admitted. The fewer validators that exist onchain, the fewer that can graduate from the queue per epoch. Currently, the size of the active validator set means that this limit is set to 6 validators per epoch. More details about this feature can be found [here](#).

ETH IN THE DEPOSIT SMART CONTRACT

The ETH that validators send to the Beacon chain smart contract will remain there forever as the smart contract was not written to have withdrawal capabilities and cannot be updated. Instead, the record of the validator’s balance for the duration of their staking lifetime, adding rewards and taking penalties, before approving the final withdrawable balance will be handled separately by the Beacon chain.

This means that the Execution layer balance of the Beacon chain smart contract will be an ever increasing count of the amount of ETH staked by validators. This balance should be discounted from the circulating supply of ETH on the network, as the following description of the unstaking process shows.

The Un-Staking Process

Following the update, validators will have the ability to make 2 types of withdrawals: a partial withdrawal, and a full withdrawal. For both, validators must also have been active for 2048 epochs (~9 days at 12 seconds per slot, and 32 slots per epoch) before they are able to signal their desire to exit.

EXITED

In a full withdrawal, the validator must first halt their participation in validating duties. They can do that by sending a *VoluntaryExit* transaction to the Beacon chain, which we can think of as calling a function on a smart contract. If they have been active for 2048 epochs and not been penalised for dishonest behaviour in that time, the *VoluntaryExit* function determines two separate epochs in the future: the first is when the exiting validator will be considered “*Exited*” (they are no longer validating).

Validators that signal their exits are susceptible to the same queuing mechanism that applies to validators entering the Beacon chain, described in the section above. If a large number of validators send *VoluntaryExit* signals at the same time, then the network will adjust our validators “*Exited*” epoch to match the currently allowed validator entry/exit rate. At the current rate of 6 validators exiting per epoch a maximum of 1350 validators can exit per day, which equates to 43,200 ETH being retired from validating to prepare it for withdrawal.

EXITED AND WITHDRAWABLE

In a full withdrawal, the validator must first halt their participation in validating duties. They can do that by sending a *VoluntaryExit* transaction to the Beacon chain, which we can think of as calling a function on a smart contract. If they have been active for 2048 epochs and not been penalised for dishonest behaviour in that time, the *VoluntaryExit* function determines two separate epochs in the future: the first is when the exiting validator will be considered “*Exited*” (they are no longer validating).

Validators that signal their exits are susceptible to the same queuing mechanism that applies to validators entering the Beacon chain, described in the section above. If a large number of validators send *VoluntaryExit* signals at the same time, then the network will adjust our validators “*Exited*” epoch to match the currently allowed validator entry/exit rate. At the current rate of 6 validators exiting per epoch a maximum of 1350 validators can exit per day, which equates to 43,200 ETH being retired from validating to prepare it for withdrawal.

FINAL WITHDRAWAL QUEUE

Once a validator is considered *Exited* and *Withdrawable*, they can send a final transaction to initiate the withdrawal. When validators submit either full or partial withdrawal requests they get added to a single withdrawal queue. The network will only process 16 withdrawals per block, by including the first 16 withdrawal requests in the queue adhering to a first-in first-out rule. This results in approximately ~115k validators (that are already *Exited* and *Withdrawable*) being able to withdraw on any given day.

When withdrawals are processed, new ETH that was previously not in circulation will be minted to the validators specified withdrawal address. As previously mentioned, this new ETH will not be removed from the Beacon Chain Deposit Contract that the validator initially deposited their stake. An important thing to note is that none of the transactions required to complete the un-staking process incur a gas cost to the validator. Fuller implementation details of the validation lifecycle can be found [here](#).

Possible Implications

Both the staked ETH and the increase in supply of ETH as a result of staking rewards to validators since the Beacon chain's inception has not yet entered spot markets. That ETH is still locked up on the Beacon chain until withdrawals are enabled. This means that there is a possibility that the Shanghai update's unlock will dramatically increase token supply, as (at the time of writing) there are 1,116 validators who are able to withdraw following the unlock.

The limit set on the final withdrawal queue exiting the Beacon chain means that at most 16 validators can leave per slot. Assuming that each is a full withdrawal (validators will need to be "*Exited and Withdrawable*"), and that each validator's staking balance is 32 ETH (a reasonable assumption given the discrete 32 ETH validator nodes, but [other analyses](#) differ), this translates to a maximum of 3,686,400 ETH per day. However, this unlock rate is only possible whilst there is a backlog of more than 6 validators in the final withdrawal queue. Once that backlog has been cleared, only 6 validators will be able to join it each epoch according to the exit limits set per epoch. At this rate and with the above assumptions, 43,200.

IN THE LONG TERM

However, we should not discount this backlog of users waiting to withdraw immediately represents less than 1% of the 500,000 validators. This group chose to collectively lock up more than 16M ETH (\$26.8B at \$1,673 per token) without a guaranteed date for withdrawals. We believe that it is likely that the unlock ultimately results in an *increase* in staked ETH, as stakers will feel more comfortable locking up their ETH with the knowledge that it is recoverable.

We also believe that the successful addition of withdrawals is likely to fortify that belief in the network, causing a net inflow of new stakers in the medium-to-long term. The operating costs of participating as a validator are much lower than mining on a Proof of Work chain. As a result, validators will not face pressure to withdraw their staked position in order to cover the computation costs. This reinforces our belief as to why validators are unlikely to embark on a mass exodus following the enabling of withdrawals.

IN THE SHORT TERM

In the short term however, we believe that a large subset of validators will want to perform partial withdrawals on their beacon chain balances which may cause a net outflow of ETH from the Beacon Chain. Validators are incentivised to perform partial withdrawals on their Beacon Chain balances because the proportion of their balance above 32 ETH earns no yield on the Beacon Chain. By not performing partial withdrawals, the validators are essentially forfeiting access to their ETH with no added benefit.

To add to this, we believe that users who wish to stake their ETH will not immediately do so, and will instead wait to observe whether or not the withdrawal process proceeds smoothly. These two phenomena, in the short term, likely stunt the inflow of ETH into the beacon chain.

LIQUID STAKING TOKENS

Liquid staking tokens have become one of the most popular ways for users to stake ETH on the Beacon chain, allowing users to trade their staked positions using a tokenized version of their staked ETH. These are likely to remain a popular staking method as they facilitate pooled staking, similar to the mining pools that dominate Bitcoin's hashrate. Liquid staking providers lower the entry barrier to staking and allow users with less than 32 ETH (~\$52K on 09/02/23) to earn staking rewards.

In addition, they will continue to allow for a quicker unwinding of staking position - users can sell their tokenized staking position directly for ETH in an onchain spot exchange instead of completing the full withdrawal process outlined above which may take much longer, at the cost of gas fees paid for their *Execution layer* transactions.

Other Upgrades

As previously mentioned, the Shanghai/Capella upgrade includes a series of upgrades outside the activation of beacon chain withdrawals. Other notable upgrades are mentioned below.

WARM COINBASE - EIP-3651

This upgrade is primarily focused towards enabling users to optimise . It allows the user to set some initial gas fee to be paid to the miner and then increase or decrease this gas fee should some conditions be met. This upgrade particularly assists MEV searchers who wish to optimise their costs by dynamically adjusting their fees, which would otherwise have to be a fixed value. More on searchers and their involvement in MEV can be found in our [article](#).

PUSH0 INSTRUCTION- EIP-3855

This upgrade aims to reduce the average size of smart contracts by adding a fundamental instruction, PUSH0, which allows the addition of 0's to bytes. Smart contracts need to do this for various reasons. Before this upgrade, other non dedicated instructions were used to pad 0's to bytes, but would comparatively cost more gas than using a dedicated instruction. This upgrade plans to introduce this dedicated instruction which will help Ethereum developers reduce gas costs when deploying their smart contracts on the network.

Conclusion

The coming Shanghai/Capella upgrade will mark another significant milestone in the Ethereum foundation's roadmap for the future of the Ethereum Network. For over two years, validators have willingly staked their ETH on the network without access to it, a point that this upgrade aims to directly address. We believe that the success of this upgrade will, in the medium-to-long term, result in more ETH locked up in the Beacon Chain as investors look for sources of yield on their tokens. We believe that the knowledge that their tokens being recoverable will solve the final sticking point for the participation of many as-yet unstaked ETH holders.

AUTHORS



AHMAD MUSTAFKA KIDA

Data Analyst

ahmad.kida@blockscholes.com



ANDREW MELVILLE

Research Analyst

andrew.melville@blockscholes.com



Block Scholes Ltd.



27 Old Gloucester Street
London WC1N 3AX



research@blockscholes.com

SUBSCRIBE TO OUR PLATFORM