Fidelity DIGITAL ASSETS℠

SEPTEMBER 2022

The Ethereum Merge

What to Expect from the Biggest Protocol Change to the World's Second-Largest Digital Asset

Jack Neureuter Research Analyst
Daniel Gray Research Analyst

Introduction

One of the most anticipated events in the history of the digital asset industry is set to take place in September – The Ethereum Merge. This is expected to bring about a host of emerging investment narratives for crypto's second largest asset by market cap and largest smart contract platform.[i] In this piece, we'll provide key information related to The Ethereum Merge – including what proof-of-stake is, analysis of how and why the Ethereum network is transitioning to it, and what impact this milestone event may have on the network. For those who are new to the Ethereum ecosystem, we suggest first reading our primer, About Ethereum, to gain a more comprehensive understanding of the history, design, and use cases of the Ethereum network.

Key Takeaways:

- The Ethereum Merge, expected to take place on September 14, 2022,[ii] will transition the Ethereum network's consensus mechanism from proof-of-work to proof-of-stake.
- With staking, miners are replaced with validators posting collateral and attesting to transactions, and competition is replaced with randomization.
- The Merge is expected to have several potential benefits including decreasing Ethereum's energy consumption by over 99%, making the ether token (ETH) a yield-bearing asset, reducing the ether issuance rate, and increasing block time consistency.[1]
- It also comes with potential risks, including centralization concerns, technical challenges, and liquidity concerns for stakers; it may shift how ether is categorized, opening the possibility that it will be subject to securities laws.
- This milestone is not the end of Ethereum's evolution towards an eventual mature state. The next series of upgrades following this event will be centered around transaction speed and cost – known as scaling.[2]

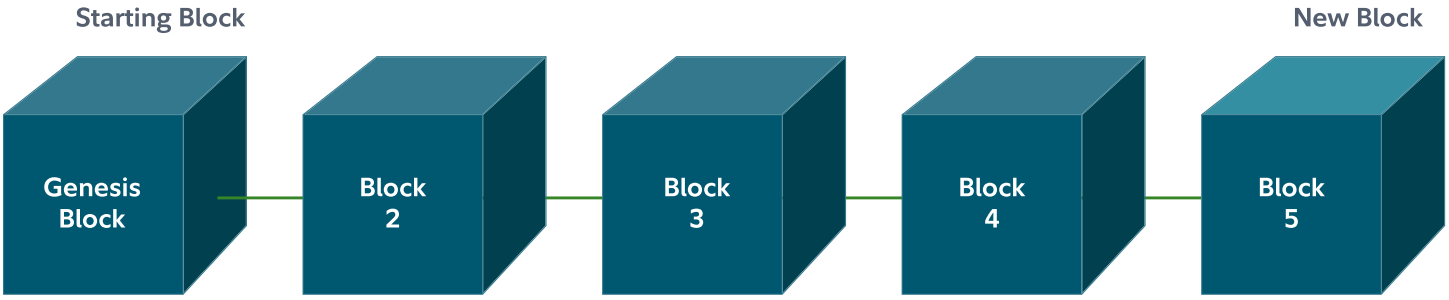
What is Proof-of-Work and Proof-of-Stake, what are the tradeoffs?

In order to understand The Merge, it is helpful to review how blockchains work and are organized. Remember that a blockchain is a special database or ledger which allows for historical records to be timestamped and agreed upon. Blockchains enable decentralized consensus, meaning there can be multiple copies of this identical ledger spread out across different computers and no one person controls the network. Each computer running the specific blockchain software and keeping a copy of the ledger is called a *node*. A node can also choose to be a *miner*, or in the perspective of a proof-of-stake network these miners become *"virtual miners"* or *validator nodes*, a participant that helps secure the network.

i At the time of writing, 8/10/2022, per CoinMetrics

ii Latest estimate as of 9/6/2022. At the time of writing, the latest *target* date is September 15, 2022 per The Ethereum Foundation blog and developer call. https://blog.ethereum.org/2022/08/12/finalized-no-36/

For this service, miners get to write new entries to the database (and also get a reward for doing this). These entries are bundled into batches called blocks, and they are linked together chronologically in a kind of chain, hence the term *blockchain*. Because there is no one person or entity in charge, these nodes therefore have to come to an agreement on what the true state of the ledger is and who gets to make new entries to the legitimate ledger. In other words, a *consensus mechanism* is needed.



Proof-of-work and proof-of-stake are the most prevalent consensus mechanisms in today's public digital asset networks. Consensus mechanisms are required for decentralized networks to come to an agreement on the current state of the network.[3] Without a consensus, decentralized networks have limited ability to differentiate authentic transactions from illegitimate ones and thus have no accurate way of organizing the blockchain. Accurate record keeping has always been best practice, but when the data points on these cryptographic blockchains have a monetary value attached to them, ensuring data is frequently updated while remaining accurate becomes even more crucial. Having a consensus best positions the network to potentially defend against internal and external attacks, as the attacker would have to go against the consensus, allowing the other network participants to possibly identify and blacklist the dishonest user.[4] Note that an "attacker" is not necessarily malicious in nature. In the eyes of the network, this term can be applied to technical mistakes as well; however, these mistakes do not warrant as large of a penalty from the network.[5]

While proof-of-work and proof-of-stake both have the goal of consensus, they each achieve it in vastly different ways. Proof-of-work achieves consensus by requiring the expenditure of real-world energy or "work" to ensure miners are securing the network and only proposing new valid blocks.[6] Proposing illegitimate or inaccurate blocks requires the same amount of energy expenditure as a valid block but has none of the reward payout. Proof-of-work is often compared to real-world jobs. Bitcoin mining is analogous with many real-world jobs, but we will use mining precious metals as an example here for simplicity. You cannot find deposits of metals deep within the earth's crust without expending a large amount of energy, whether it is in the form of equipment to dig and move dirt or paying employees to do the work for you. If you were to mine a metal and then try and sell it as something it is not, you would have wasted your time, money, and potentially burned a connection. The same scenario is tantamount to bitcoin mining where trucks and equipment represent the bitcoin mining rigs, time is spent, and the network blacklists your IP address.

Proof-of-stake relies on a validator's potential loss of capital or "stake" to ensure they, the "virtual miners," are securing the network and only proposing new valid blocks.[7] Proposing faulty blocks has a financial penalty associated with it as well, known as slashing. Proof-of-stake does not require material real-world energy expenditure, only a signature verifying you have attested to the proposal of the new block. At first glance, it seems like this mechanism may not work as anyone can propose incorrect or faulty blocks at no cost. That's where the digital signature comes into play. Because a validator must digitally sign the proposed block, other validators can double check the proposal and agree or report the validator.[iii] However, if a mistake has been made, the other validators will report the block and the network penalizes the signer of the block, taking a portion of their staked funds as punishment before banning them from the network. While a potential attacker could take their remaining funds and spin up a new validator node, the penalties quickly add up, making attacks on proof-of-stake costly.

How does staking work?

Proof-of-stake consensus mechanisms produce new blocks by randomization and an economic stake to incentivize accuracy rather than the energy-intensive alternative that proof-of-work mechanisms use. Proof-of-stake systems pseudo-randomly select validators to propose new blocks while other nodes continuously cross-check each other for accuracy. To participate in this consensus mechanism, users are first required to prove that they are going to work accurately and reliably by posting collateral. This collateral is often referred to as a "stake." Each validator client stakes an effective balance of at least 32 ETH (roughly $61,000 today[8]) for the chance of proposing a new block. Staking more than 32 ETH as a validator does not increase the odds of being selected or the profitability of a node. In fact, it reduces the capital efficiency, or total yield, for the asset holder. Therefore, validators are incentivized to stake in 32 ETH lots when possible. If a validator is offline when selected for proposal, they risk being penalized. Pooled staking or centralized exchanges offer the ability for individuals with smaller balances to comingle their funds with other small holders and earn staking rewards (though this has the potential to create increased levels of centralization of the network). As we touched on briefly before, new blocks are proposed with a digital signature "etched" into the block. This means that every block has a verifiable proposer that will be held accountable for breaking the rules and accurate proposals will receive transaction tips and a reward paid out by the network.

How Proof-Of-Stake Aims to Defend Against Attacks

Unlike proof-of-work, proof-of-stake does not require immense amounts of energy to propose new blocks. This opens the network to a variety of attacks, most notably, equivocation. Validators can propose new blocks that are essentially costless to produce. This allows for an unlimited number of blocks to be created at the same time, causing the chain to split. To address this problem, Ethereum uses a mechanism called "slashing." All blocks require a digital signature to be proposed; when multiple blocks are proposed the

iii When two-thirds of validators agree, consensus is reached, the block is validated, and the proposer gets a reward in the form of transaction "tips" and newly minted ether (the token native to the Ethereum network).

validators are there watching, ensuring that everything is accurate and operational. When multiple blocks are proposed at the same time, a whistleblowing validator can easily use the signed blocks as proof to the network that someone acted incorrectly. The network in turn slashes the dishonest proposer's stake, taking a percentage (based on the infraction) of their locked 32 ETH and irrevocably forcing them off the network. As a reward, both the new proposer and the whistleblowing validator receive a payment from the network. It is not the purpose of this paper to explore in detail the proof-of-stake security vulnerabilities or Ethereum's incentivization strategies, but block rewards, slashing, forced exits, and whistleblower rewards having been embedded as economic incentives and defense mechanisms have kept the current proof-of-stake network going, block after block, so far.[9]

	Proof-of-Work	Proof-of-Stake
What is it?	A consensus mechanism that uses "work" performed by computers that expend electricity and prove said work. In other words, it regulates the state of the blockchain.	A consensus mechanism that does not require "work" to be performed, but instead delegates control of the network to owners/stakers of the token.
Commonly Cited Advantages	• Fair • Decentralized • Mining is scalable • Longest track record of any blockchain successfully defending against attacks to the network • Security (and value) anchored to physics	• No energy use • No expensive and depreciating hardware needed • No geographic/physical footprint needed • Provides yield mechanism • Allows scalability of transactions with future network upgrades such as sharding[iv]
Commonly Cited Disadvantages and Risks	• Requires energy use • Requires hardware that becomes obsolete • Geographic footprint necessary • 51% attack risk[10]	• Governance risk – network control given to owners of tokens, potential centralization risks • More complex to implement than proof-of-work[11] • Younger, "less battle-tested" than proof-of-work[12] • 51% attack risk and additional potential vulnerabilities or bad actor actions[13]

Ethereum's Road to Proof-of-Stake

Ethereum's transition to proof-of-stake has been a long time coming. The Ethereum network's original founders have discussed the idea of transitioning the protocol's governance mechanism since before a single block was minted on its blockchain back in 2014. Vitalik Buterin, one of the network's most notable co-founders, wrote, "We may choose later on to adopt alternative consensus strategies, such as hybrid proof-of-stake, so future patches may reduce the issuance rate lower."[14]

The Merge, the name given to the upcoming transition of Ethereum from proof-of-work to proof-of-stake, is the outcome of multiple years of research and development intended to provide a series of potential

iv Per the Ethereum organization website, sharding is the process of splitting a database horizontally to spread the load. https://ethereum.org/en/upgrades/sharding/

benefits to the network.[15] With many upgrades repeatedly pushed back time and time again, we now have insight into more concrete dates. Ethereum's merge is expected to take place around September 14, 2022, based on the currently planned upgrade timeline for the Mainnet chain of Ethereum.[16]

To understand how we arrived here, let's take a brief look back at Ethereum's proof-of-stake journey.

The first major accomplishment towards transitioning the protocol to proof-of-stake took place on December 1st, 2020 with the launch of the Beacon Chain.[17] This proof-of-stake chain has been running parallel to the proof-of-work Ethereum Mainnet ever since and is designed to act as the central hub of Ethereum's consensus after The Merge takes place. Today, users on Mainnet are able to lock up their funds on the proof-of-stake chain, effectively burning their proof-of-work ether in order to start securing the chain as well as receive rewards for proposing new blocks. Once The Merge is complete though, the proof-of-work and proof-of-stake chains will combine to become one singular proof-of-stake chain. A later planned network upgrade will allow staked Ethereum to be withdrawn, though this is not expected to take place until roughly 6-12 months after The Merge.

Developers have been testing the consensus mechanism transition of several test chains in preparation for the real event. The first major test took place on Ethereum's Ropsten Testnet and was completed in early June of this year (2022). This marked the first successful attempt proving that a switch from proof-of-work to proof-of-stake was not only possible, but well within grasp. The next attempt was made with the Sepolia testnet which took place later that month. Although each of these tests revealed a series of different issues that needed to be tweaked, they largely were accepted as successful merge attempts and have increased confidence levels associated with the actual merge. The final merge, Goerli, took place in the first few weeks of August and successfully transitioned from proof-of-work to proof-of-stake. The official Mainnet merge is targeted to take place on or around September 14, as of the time of writing.[18]

When The Merge actually happens, the transition to proof-of-stake will officially be complete, changing how blocks are created and how new ether is minted and issued. There are many steps along the way and The Merge will be a multi-day, even potentially multi-week, process involving two separate hard forks and network upgrades, which will not be backwards compatible.

Switching to proof-of-stake will be the largest change to a digital asset network to-date. If the Mainnet merge is successful, a great deal of new features and potential investment narratives will emerge around Ethereum.

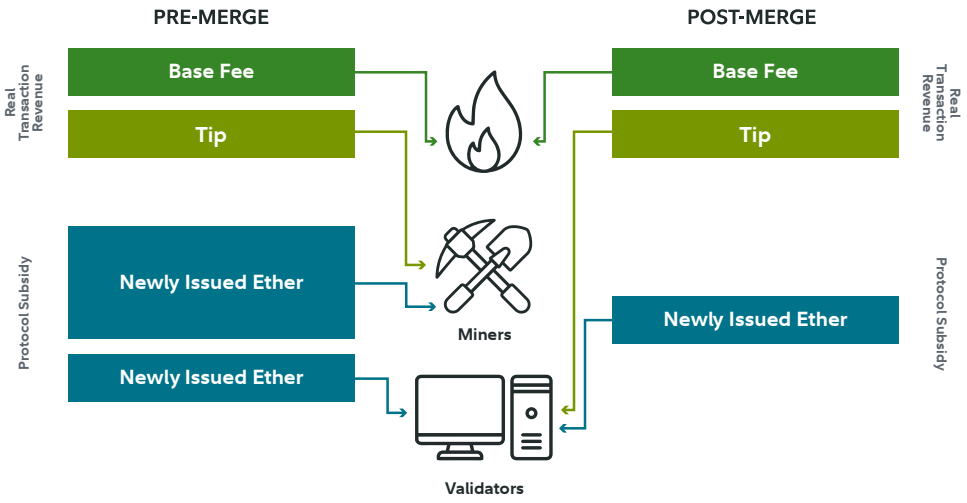
Potential Benefits of the Merge

Given The Merge is the most significant development in the history of the Ethereum network, the investment thesis for the ether token arguably should evolve as well, in addition to some of the network's features or characteristics. Below we outline some of the ways The Merge may impact the way the asset is viewed.

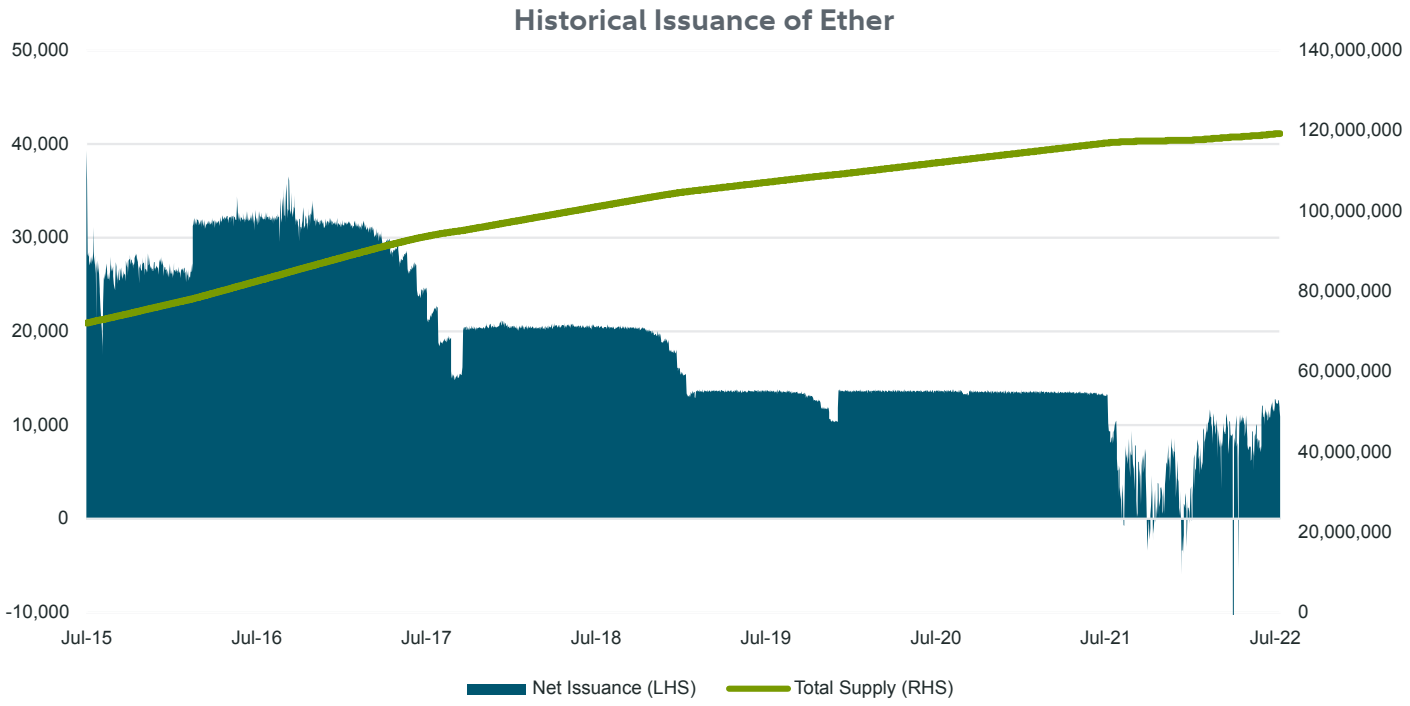
Reduction in Energy Consumption – Energy consumption for proof-of-work chains is a nuanced topic. It is simply an undeniable fact that proof-of-work chains do require a meaningful level of energy consumption. After all, that is an intentional design, with a number of possible advantages due to this linkage to real-world energy use. It is not the purpose of this paper to explore the tradeoffs between different consensus mechanisms, but instead we simply point out that Ethereum's switch to proof-of-stake will reduce its energy consumption by an estimated 99.95%.[19] This may have a positive reinforcing effect for those who feel strongly about the environmental impact resulting from the usage of blockchains.

Yield Generation – Ethereum's shift to proof-of-stake makes ether an asset which can earn interest for holders in the form of staking. This yield generation has the potential to increase the total return for ether holders and may make the asset more attractive to prospective investors. Yield, or a form of cash flow paid to asset holders, is a feature that is a familiar concept from traditional markets. This makes traditional financial valuation modeling possible (such as discounted-cash-flow modeling) based on an investor's assumed future network usage, fee accrual, and discount rate. In this way, ether becomes similar to owning both a native token – usable on the Ethereum blockchain – and a non-depreciating miner on a proof-of-work blockchain (yield-bearing validator on a proof-of-stake chain). The Beacon Chain currently pays investors a yield of between 3-5%[20] depending on the number of validators, but some estimates for post-merge yields are as high as nearly 7%.[21]

Increased Rate of Deflation – The Ethereum network altered its monetary policy in August 2021 with the introduction of EIP-1559 via the London Hard Fork.[22] This resulted in the network charging what amounted to two types of fees – one which would be burnt (removed from existence similar to a share buyback in the equity world), known as the base fee, and the other, known as the tip, which would incentivize the networks miners. Payments to miners also come in two forms – block rewards (inflation) and those tips from transactions.[23] Prior to The Merge, new ether is issued to incentivize both miners, approximately 13,000 ether minted per day, and validators, approximately 1,600 ether minted per day, to validate transactions.[24] Post-Merge, payments of new ether to miners will no longer be made, driving down the rate of newly issued ether and directing both block rewards and transaction tips to Ethereum stakers. Previously, Ethereum has gone through periods of net burning (deflation) when more ether is burned through transactions than minted via block rewards. The Merge is expected to increase this potential deflationary (net burning) impact because of a reduction in block rewards (issuance) that are currently being



paid to miners. The new issuance schedule will decrease from roughly 5 million ether created per year (or approximately a 4% annual inflation rate) to being controlled by an equation derived from the amount of ether staked. The anticipated inflation rate is expected to drop roughly 90% to an estimated level of 0.50%, depending on the total amount of ether staked.[25]



Data Source: Coin Metrics, as of 08/09/2022.

Block Time Consistency And (Minor) Speed Increase – Ethereum's block time predictability will increase as a result of the move to proof-of-stake. Consistent block times can help increase the certainty of transaction settlement times when interacting with a blockchain or an application on one. In proof-of-work, a "competition" ensues where miners compete for the privilege of adding or writing the next block to the chain or ledger, which will average towards an intended block speed as a result of the network's adjusting ruleset. For Ethereum, this average has been roughly every 13 seconds, but there is typically a level of variance for these blocks. Upon moving to proof-of-stake, these block times will come virtually every 12 seconds.[v] This will slightly decrease block times and greatly increase block time consistency.

A Major Milestone Complete, Time for Ethereum to Scale – The Ethereum foundation, community, and developers have been focused on the transition of the network's consensus mechanism from proof-of-work to proof-of-stake for years now. When this historic event takes place, it's not just an important milestone for the network but, in a sense, the start of a new era for the Ethereum blockchain. Over time, and assuming that The Merge is completed successfully, developer resources will likely shift their focus from transitioning the network's consensus mechanism towards the next set of goals for the Ethereum network to grow – particularly scaling.

v Except for when, "a slot is missed either because a validator is offline or because they do not submit a block in time. In practice, this currently happens in <1% of slots." https://blog.ethereum.org/2021/11/29/how-the-merge-impacts-app-layer/

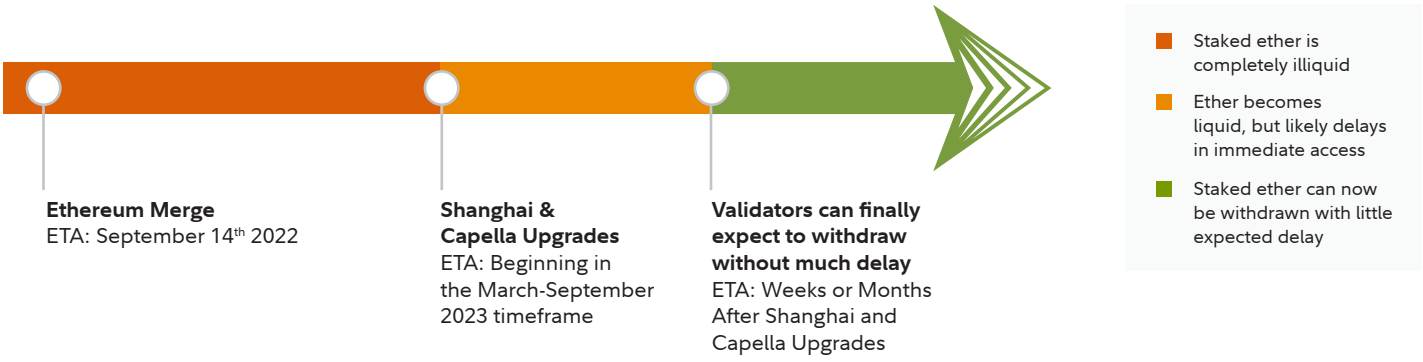
Risks Associated with The Merge

While The Merge is considered by many to have several positive impacts on the network, a large change to the protocol does not come without risks as well. Below we outline several potential risks market participants should be aware of.

Potential Technical Challenges – The Merge consists of two hard forks, requires node operators to operate two separate software clients, and necessitates the coordination of thousands of individuals across the globe. To assume that everything will go perfectly is presumptuous at best, especially as The Merge has been delayed multiple times in the past due to additional testing and validation needed.[26]

Centralization and Proof-of-Stake Concerns – Users of Ethereum have relied upon an entirely different consensus mechanism throughout the network's history. Wealth, in the form of more ether tokens, has historically not been correlated to one's ability to govern or alter the network. Upon transitioning to proof-of-stake, this will likely no longer be the case. This may lead to some concerns surrounding the network's initial token allocations to developers and early adopters, who could theoretically band together to alter the protocol if tokens were concentrated through a few individuals. Additionally, the need to stake 32 ETH, and the complexity involved in doing such, will add to the likelihood that many retail holders may utilize centralized staking services, which could create large holdings of ether among a few institutions.

Liquidity Timeline of Staked Ether – As of the time of this writing, over 14 million ether tokens are staked on the Ethereum Beacon Chain.[27] This ether, and any additional ether that is staked over the coming months before and after The Merge, will not be liquid and cannot be withdrawn until separate network upgrades take place at a future, yet-to-be-determined date. These network upgrade, known as the Shanghai and Capella upgrades, are not expected to take place for at least another 6-12 months[vi] following the completion of The Merge.[28] Additionally, due to varying rate limits, only about six full validators will be able to exit per epoch (every 6.4 minutes), which means a maximum of around 1,350 validators or roughly 43,200 ether can gain liquidity out of their staked position in a 24-hour period. This means that there may be an exit queue that forms causing further delay, conceivably adding many more weeks or months to the validator's timeline of when their position is withdrawn.



vi While it is expected to take place within 12 months post-Merge, there is a chance that the update will take longer and staked ether will remain locked up.

Might Ether Be More Likely to Be Deemed a Security Post-Merge? – The Merge changes the fundamental dynamics of the ether token and investors' expectations of holding such a token. The process of creating decentralization via a wealth staking mechanism and paying a yield to validators introduces different considerations that did not previously exist, which some have argued may alter the way the asset is viewed under the United States' "Howey Test."[vii] Regulators have yet to make any concrete distinction on which digital assets are or are not securities and the impacts to crypto markets when they do remain relatively unknown.

Beyond The Merge

The Merge is certainly a milestone event for Ethereum, but it is not the end of the aggressive roadmap laid out by the network's community. Ethereum's co-founder Vitalik Buterin has said, "Ethereum can be up to being 55% complete after the 'merge'... we're getting close, which is really amazing."[29]

The Merge represents the first major milestone of a five stage roadmap laid out by the network's developers. The next stated endeavor for the Ethereum network will be to focus on scaling the protocol. This will be attempted in multiple ways, including a plan to shard the network's main consensus chain into 64 individual chains, which then roll back up to the one master Beacon Chain. This would likely help lower transaction fees and network congestion, but the timeline for when these upgrades will occur remains ambiguous right now.

What The Merge Is and Is Not

Confusion surrounding such a monumental event is common. To summarize, below is a recap of what is and is not changing as a result of The Merge.

What Is Changing:

- Ethereum is removing its reliance on energy intensive miners.
- Ether, the token native to the Ethereum network, is becoming a yield-bearing asset for holders who choose to run a validator or to delegate to one.
- Ethereum will have a far lower ether token issuance rate after The Merge which, when combined with the network's burning of base fees, creates the potential for a consistent net reduction in total token supply.
- Ethereum will have more consistent block times.

What Is Not Changing:

- Ethereum will not gain large improvements in the cost or speed of transactions. Scaling is not the focus of The Merge and will likely be the focus of subsequent upgrades in 2023 or 2024.

vii The Howey Test refers to a U.S. Supreme Court case helpful in determining if a transaction represents an investment contract, and therefore should be considered a security. - https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets

- Ethereum is not creating two separate ETH 1.0 and ETH 2.0 chains. The current proof-of-work "execution layer" will be merged with the current proof-of-stake Beacon Chain "consensus layer" to become one single Ethereum chain.
- Those staking on the Beacon Chain will still not be eligible to withdraw their either post-Merge. A separate set of upgrades, which is estimated to take place 6-12 months after The Merge, would allow staked ether to be withdrawn from their validator.[30]
- Ethereum will not be considered "completed" because of The Merge. There are many future upgrades planned on its roadmap.

---

[1] https://ethereum.org/en/energy-consumption/

[2] https://ethereum.org/en/upgrades/vision/

[3] https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/

[4] https://blog.staked.us/blog/eth2-post-mortem

[5] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/gasper/#incentives-and-slashing

[6] https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/#top

[7] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[8] As of 8/11/2022 according to Coin Metrics

[9] https://ethereum.org/en/upgrades/beacon-chain/

[10] See the bitcoin whitepaper at https://bitcoin.org/bitcoin.pdf

[11] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#pros-and-cons

[12] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#pros-and-cons

[13] For example, long-range attacks, short-range "reorg" attacks, and others; see: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#pos-and-security

[14] https://blog.ethereum.org/2014/07/22/launching-the-ether-sale/

[15] https://ethereum.org/en/upgrades/merge/

[16] https://blog.ethereum.org/2022/08/12/finalized-no-36/

[17] https://www.coindesk.com/tech/2020/12/01/ethereum-20-beacon-chain-goes-live-as-world-computer-begins-long-awaited-overhaul/

[18] https://blog.ethereum.org/2022/08/12/finalized-no-36/

[19] https://blog.ethereum.org/2021/05/18/country-power-no-more/

[20] As of 08/12/22 according to https://www.stakingrewards.com/earn/ethereum-2-0/

[21] Updated as of July 27, 2022 https://www.coinbase.com/institutional/research-insights/research/market-intelligence/eth-staking-post-merge-yield-estimates-and-risk

[22] https://cointelegraph.com/news/ethereum-london-hard-fork-goes-live

[23] https://consensys.net/blog/quorum/what-is-eip-1559-how-will-it-change-ethereum/

[24] https://ethereum.org/en/upgrades/merge/issuance/

[25] https://ethereum.org/en/upgrades/merge/issuance/

[26] https://cointelegraph.com/news/ethereum-dev-confirms-perpetual-date-for-pos-merge

[27] https://ethereum.org/en/staking/

[28] https://ethereum.org/en/upgrades/merge/

[29] https://fortune.com/2022/07/21/vitalik-buterin-ethereum-merge-ethcc-paris/

[30] https://ethereum.org/en/upgrades/merge/

1047653.1.0