A MESSARI REPORT

ETH 2.0: The Next Evolution of the Cryptoeconomy

An in-depth look at Ethereum's most critical network upgrade to date

MESSARI × BisonTrails

Table of Contents

Authors

Wilson Withiam

Senior Research Analyst at Messari

Wilson Withiam is a Senior Research Analyst at Messari who focuses on Ethereum and smart contract platforms. Before Messari, he was an analyst at Circle Research, where he was one half of the team focused on producing weekly updates and in-depth quarterly reports on cryptoassets. He also helped launch an organization dedicated to educating blockchain application developers. Wilson holds a degree in Kinesiology but abandoned med school to work with emerging technologies.

TWITTER: @WILSONWITHIAM

Ryan Watkins

Senior Research Analyst at Messari

Ryan is a Senior Research Analyst at Messari. Prior to joining Messari, Ryan worked as an investment banking analyst at Moelis & Company where he advised on Mergers & Acquisitions, Private Placements, and Restructurings across all industries with a focus in technology, media, and telecommunications. He previously held positions at Bank of America Merrill Lynch, and CastleOak Securities. Ryan holds a Bachelor of Science from Fordham University, where he studied Finance and Computer Science.

TWITTER: @RYANWATKINS_

Introduction

"Systems like Ethereum are a fundamentally new class of cryptoeconomic organisms – decentralized, jurisdictionless entities that exist entirely in cyberspace, maintained by a combination of cryptography, economics and social consensus."

- VITALIK BUTERIN[1]

In their most abstract form, blockchains are a new way of organizing economic, social, and political activity. Blockchains are an institutional technology - more similar to markets, corporations, and nation states, than just mere computing platforms[2]. Fundamentally, blockchains allow millions, if not billions of independent, diverse, and untrusting participants to coordinate on a global scale. And perhaps equally important, blockchains are sovereign entities, free from outside interference and unable to be shut down.

The first instantiation of blockchain technology was Bitcoin, which incentivizes participants to contribute computing resources towards maintaining a global ledger of transactions. This ledger is the ultimate source of truth containing a full history of who spent and who owns what. An innovation that alone created the world's first scarce digital asset, bitcoin.

Since the invention of Bitcoin, blockchain technology's use has been expanded beyond the maintenance of a transaction ledger. The most prominent example being Ethereum, which not only maintains a ledger of transactions but also stores and executes arbitrary code, opening up an infinite number of potential use cases.

Ethereum was birthed out of the idea that blockchains could power more than just decentralized money. Blockchains could, more expansively, power an entire decentralized economy. The ultimate vision for Ethereum was to become a world computer[3].

Seven years after conception and five years after mainnet launch, Ethereum now hosts tens of thousands of applications, $100+ billion in assets, and settles more than $1 trillion in transactions annually, making it arguably the most used blockchain in the world[4]. It also underpins a burgeoning ecosystem of composable and symbiotic decentralized finance protocols as well as the majority of the industry's stablecoin activity.

However Ethereum's progress is also the source of its challenges. Currently, Ethereum is only capable of handling a mere 15 transactions per second, making it unable to serve as a

[1]Vitalik Buterin, "**A Proof of Stake Design Philosophy**" Medium, Dec, 30, 2016 • [2]Sinclair Davidson, Primavera De Filippi, and Jason Potts, "**Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology**" Jul. 19, 2016 • [3]"**Ethereum: the World Computer**" Youtube, Jul. 30, 2015

globally scalable decentralized financial infrastructure. All it took was an uptick in on-chain activity spurred by the small scale speculative boom this past summer to push Ethereum to its limits. Ethereum is not ready for mainstream adoption under its current architecture.

In order for Ethereum to become a global decentralized financial infrastructure it will need to scale orders of magnitude. Fortunately, the Ethereum community has been working towards addressing this challenge since even before Ethereum launched.

That solution is called Ethereum 2.0 (ETH 2.0) - a long awaited network upgrade that will increase Ethereum's scalability, security, and energy efficiency without compromising on accessibility or decentralization.

ETH 2.0 is not just a major upgrade to the Ethereum blockchain; it is also a major upgrade to Etheurm's native asset ETH. ETH 2.0 will transform ETH as an asset, providing it with attributes of each of the three asset superclasses: capital assets, commodities, and stores of value - an unprecedented combination[5]. It will also fundamentally alter Ethereum's monetary policy, which while perpetually inflationary for security purposes, will likely see inflation of less than 1% annually if not even lower.

In this report, we will first explain what ETH 2.0 is, why it was created, and where it came from. We will then follow that overview with detailed breakdowns of each phase of Ethereum 2.0's multi phase rollout, outlining implications for users, investors, builders, researchers, and more.

2020: A Crypto Odyssey

[4]Ryan Watkins, "**Q3 Stablecoin Review: Ethereum's Economic Boom, Yield Farming, and the Rise of the Smart Dollar**" Messari, Oct 21, 2020
• [5]David Hoffman, "**Ether: The Triple Point Asset**" Bankless, Oct. 4, 2019

Part 1: Overview, Philosophy, and History

"People often ask, "What is Ethereum for?". Previous answers to this question often included the term "world computer", but despite some interesting examples, it's been difficult to answer this question at a more abstract level. I propose an answer to this question. I hereby propose, Ethereum is an unprecedented arena for playing cooperative games. And moreover, Ethereum enables powerful economic vehicles we don't yet understand."

- VIRGIL GRIFFITH[6]

Overview

ETH 2.0 is Ethereum's most ambitious system wide upgrade yet, and it will fundamentally change how Ethereum works. It is also the first time a major blockchain has attempted to rebuild itself from scratch under a new consensus mechanism while fully operational.[7]

At a high level there are three major components of ETH 2.0: Proof of Stake, Sharding, and the Beacon Chain.

Proof of Stake (PoS) is a category of consensus algorithms for public blockchains that depend on validator's economic stakes in the network as opposed to Proof of Work (PoW) consensus algorithms which depend on miners. ETH 2.0 will replace Ethereum's current PoW consensus mechanism with PoS with the aim to increase its security, increase its energy efficiency, reduce its centralization risk from miners,[8] and to ensure participation in the consensus process remains as maximally democratic and open as possible.

[6]Virgil Griffith, "**Ethereum is game changing technology, literally.**" Medium, Mar. 29, 2019 • [7]Viktor Bunin, "**Bison Trails Announces Support for Eth2**" Bison Trails, Jun. 29, 2020 • [8]"**Proof of Stake FAQs**" Ethereum Wiki

ETH 2.0 is designed for hundreds of thousands of validators to participate and anyone with 32 ETH will be able to run a validator without expensive infrastructure costs or strict maintenance requirements.

INSIGHTS FROM BISON TRAILS

"The transition to eth2 is incredibly important for the crypto ecosystem because it allows one of the most important and most adopted blockchains–with millions of users and tens of thousands of dapps–to introduce new scalability options for the protocol and that's a big deal."

–Joe Lallouz, CEO of Bison Trails

Sharding is a scaling solution that involves splitting the Ethereum blockchain into smaller pieces called shards, which run in parallel and ultimately link back to each other. Sharding is a type of horizontal scaling technique, which is an approach to scaling databases that involves spreading computing and storage capacity across multiple servers. In the world of blockchains sharding involves partitioning a blockchain across sub groups of nodes. Under ETH 2.0 the Ethereum blockchain will be divided into 64 parallel shards, which will each have a dynamic subset of nodes processing blocks of transactions. The reason why this is done is to ensure the demands to run a node remain low enough so that anyone can run a node using consumer hardware, while still increasing the scalability of the overall system. Sharding alone will scale throughput capacity by at least 64x greater than what is currently possible on the current PoW ETH chain.

The Beacon Chain ties PoS and sharding together, and serves as the central nervous system of ETH 2.0. It is where all the system level activity and orchestration happens.[9] The Beacon Chain stores and manages the registry of validators and their stakes, applies consensus rules, and stores references to shard states.

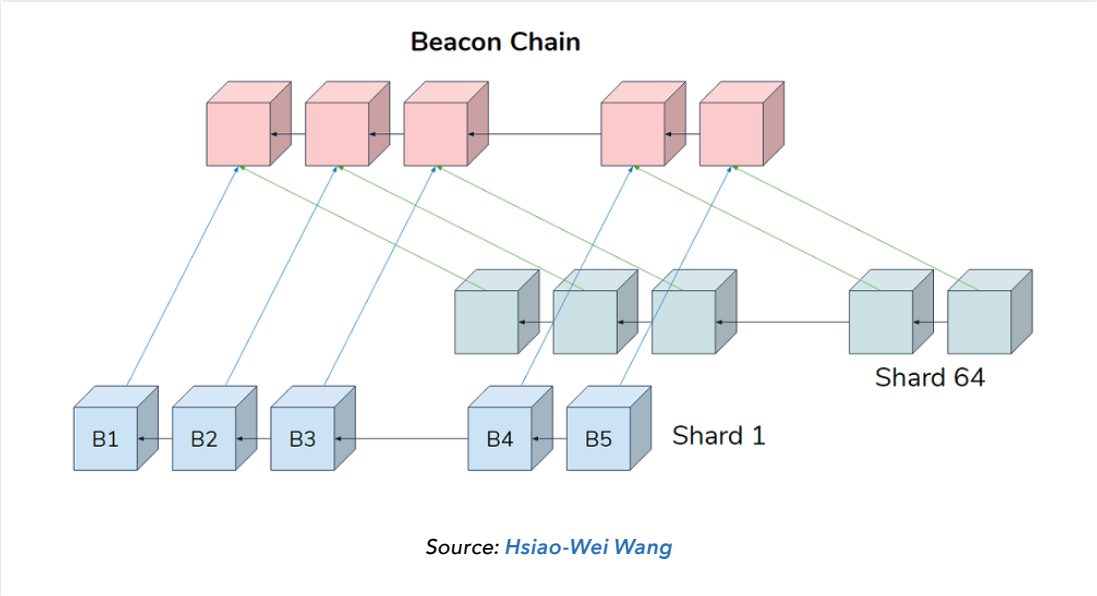
INSIGHTS FROM BISON TRAILS

The original sharding design called for 1024 shards, but came with the tradeoff that cross-shard communication would happen with a full epoch delay (6.4 minutes) which severely impacted dApp composability. This design was scrapped due to community feedback, which shows the strength of collaboration between community and protocol developers.

The Beacon Chain will be divided into slots - each of which is a chance for a block to be added to the Beacon Chain (and shards). Slots are further organized into epochs, which each contain 32 slots and serve as network checkpoints to help finalize transactions. In ETH 2.0's end state, every 12 seconds one Beacon Chain block and 64 shard blocks will be added when the system is running optimally. Each block will be

[9]Danny Ryan, "**The State of ETH2, June 2020**" Ethereum Blog, Jun. 2, 2020

proposed by a pseudorandomly selected validator (block proposer) and will be voted on by a pseudorandomly selected committee of validators called attesters (target 128 per committee).



Source: Hsiao-Wei Wang

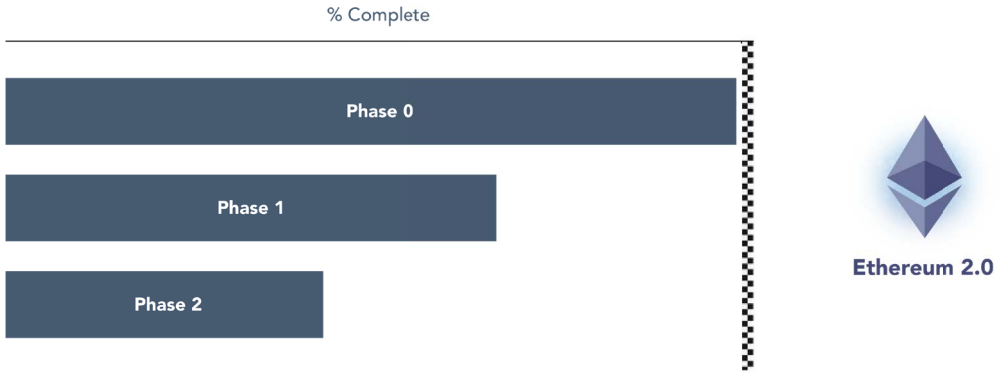
Finally, the heart of ETH 2.0 which makes the entire system possible, is Ether (ETH). ETH will not only be Ethereum's native store of value asset, and fuel for transactions, but will also be Ethereum's ultimate source of security from its role in the PoS system. Validators will be required to stake at least 32 ETH in order to participate in the consensus process. Validators will be rewarded for performing their duties adequately, penalized for failing to perform adequately, and slashed (have their stakes deleted) if they behave maliciously.

Due to the complexity involved in launching ETH 2.0 along with the fact that the community doesn't want to cause any disruptions to the current Ethereum chain (ETH 1.x) which already supports a bustling economy, ETH 2.0 will be launched in phases over a multi-year period. ETH 2.0 will first run in parallel with ETH 1.x, then eventually merge with ETH 1.x by merging ETH 1.x into ETH 2.0 as a shard. These phases have been divided into Phase 0, Phase 1, Phase 1.5, and Phase 2. It's important to note however, that despite the phases being numbered sequentially, the development of the phases will occur in parallel.

MESSARI

Ethereum 2.0 Development

Although the phases of Ethereum 2.0 are numbered sequentially, development of the phases will occur in parallel.



Note: Percentage completion is intended to be illustrative and not a precise estimate of completion • Source: Messari, Meeseeking

Phase 0 will launch the Beacon Chain and bootstrap ETH 2.0's PoS validator set. It will have limited functionality. (Estimated Arrival: December 2020).

INSIGHTS FROM BISON TRAILS

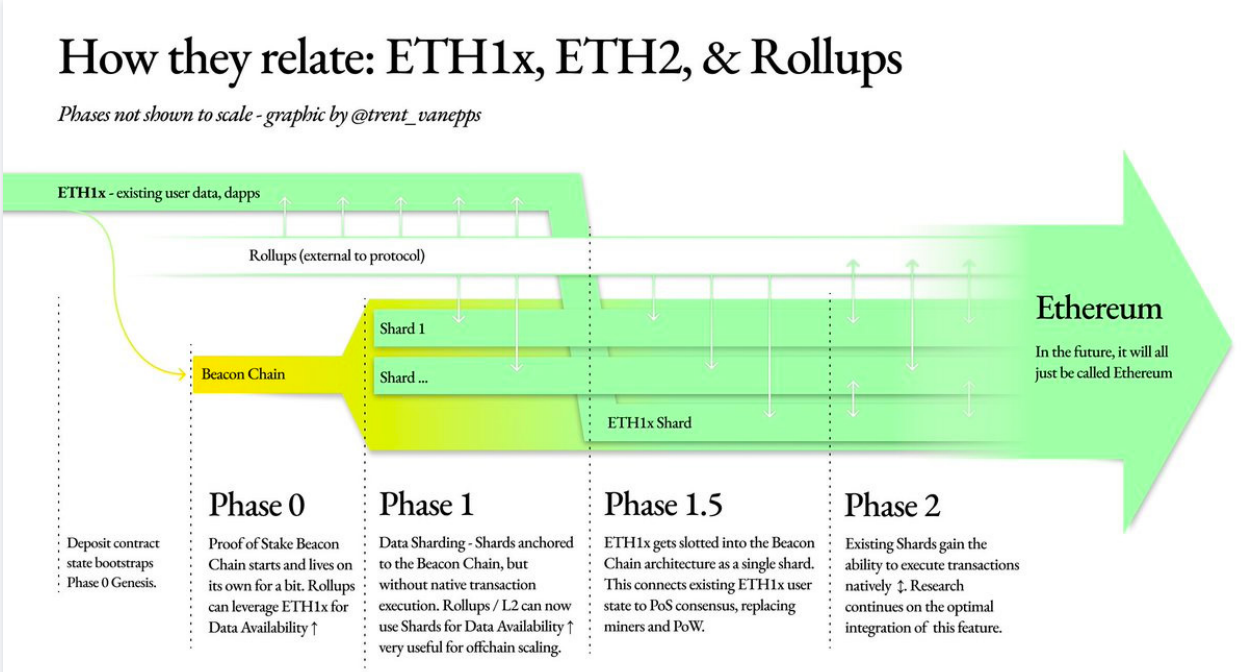
The Phase 0 Beacon Chain is not a testnet; it is a mainnet with limited functionality, with real consensus, opportunities, and consequences.

Phase 1 will extend ETH 2.0 PoS into 64 shard chains that will act as data availability layers. It will not support smart contracts. However, a few proposed upgrades to ETH 1.x will allow scaling solutions like rollups to verify data from ETH 2.0 shards and reduce their data bottlenecks. By combining rollups with 64 data shards in Phase 1, Ethereum could support a theoretical max of ~100,000 transactions per second. (Estimated Arrival: Q4 2021).

Phase 1.5 will transition ETH 1.x's current state (smart contract and transaction data) into a shard within the ETH 2.0 network. The state will remain the same; the merge simply swaps Ethereum's consensus layer from PoW to PoS. If the community elects to embrace a "rollup-centric future" and forgo smart contract execution capabilities within shards (except the ETH 1.x shard), this may be the final phase of ETH 2[10]. (Estimated Arrival: 2022).

[10]Vitalik Buterin, "**A rollup-centric ethereum roadmap**" Fellowship of Ethereum Magicians, Oct. 2, 2020

Phase 2 will unlock smart contract execution capabilities within shards and network state will be partitioned across some or all 64 shards. This stage will also introduce a new VM, Ethereum flavored WebAssembly or EWASM, that intends to bring usability and performance improvements for smart contract development. This is the final scheduled phase on ETH 2. (Estimated Arrival: 2023).

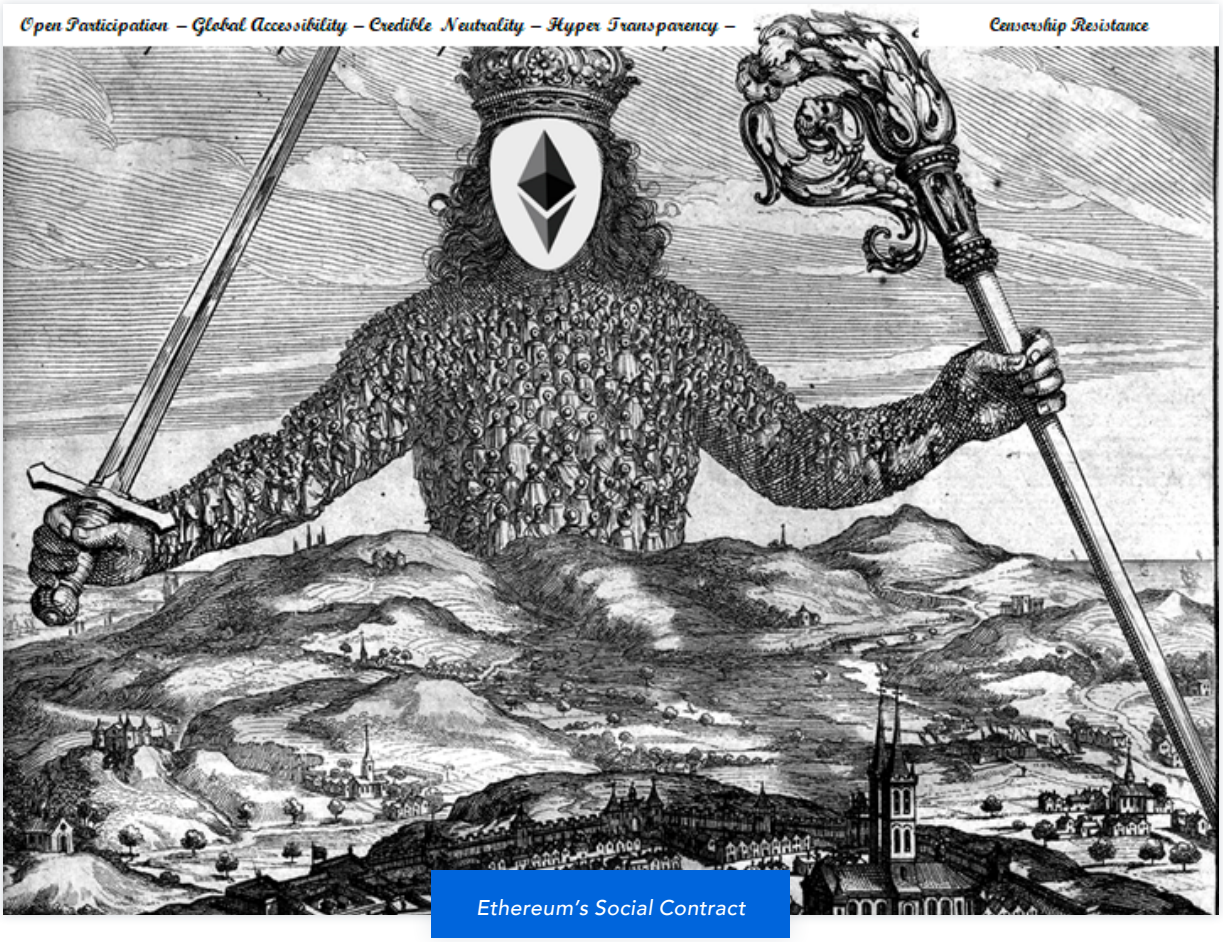


Source: Trent Vanepps

Philosophy

Ethereum is a new social contract for the global economy. It is a global public good that ensures open participation, borderless accessibility, credible neutrality, hyper transparency, and censorship-free economic interaction for anyone in the world regardless of who they are or where they come from. With Ethereum users and builders are sovereign and able to determine their own economic destinies.

Ethereum aims to be maximally democratic and open for users to participate, scalable for users to directly interact with, free of mining centralization risks, and energy efficient. What it refuses to sacrifice to achieve these properties is decentralization[11]. For Ethereum to uphold its social contract with its stakeholders it must be built upon firm principles that ensure Ethereum has the desired properties it promises.



Ethereum's Social Contract

[11] "**Designing Ethereum | Vitalik Buterin**" Bankless, Oct. 19, 2020

PRINCIPLES OF ETH 2.0 DESIGN

"The best protocols are protocols that work well under a variety of models and assumptions. It is important to have both layers of defense: economic incentives to discourage centralized cartels from acting anti-socially, and anti-centralization incentives to discourage cartels from forming in the first place."

- VITALIK BUTERIN[12]

ETH 2.0 was designed with five key principles in mind: simplicity, long-term stability, sufficiency, defense in depth, and full light-client verifiability[13].

Simplicity - PoS and sharding are inherently complex. Simplicity allows ETH 2.0 to minimize development costs, reduce its attack surface, and clearly convince users that protocol parameter choices are legitimate because they're easier to understand (key for credible neutrality).

Long-Term Stability - One of the dividing lines in the philosophy of blockchains is along the stability vs. evolution spectrum. The stability camp favors ossifying a blockchain so that it is more predictable to use and therefore, in theory, safer. It stems from the belief that stability is a necessity for any blockchain that truly wants to serve as critical public infrastructure, especially for things such as money. The evolution camp favors continually improving a blockchain so that it is more functional and robust. It stems from the belief that blockchain technology is in its infancy and there are many fundamental improvements to make before ossifying - evolution, for now, is critical. Ethereum so far has leaned more towards the evolution end of the spectrum, recognizing the infancy of blockchain technology and fundamental improvements it must make so that it can scale globally. However, ETH 2.0 is designed with the idea in mind that once built, there should be little need to change it for long periods of time, in order to achieve the stability necessary for Ethereum to serve as public infrastructure.

INSIGHTS FROM BISON TRAILS

In a mature state, the reward rate of eth2's global settlement layer may well become the base-rate for participation in Web3.0, and the benchmark to define the cost of trustless value transfer.

[12]Vitalik Buterin, "A Proof of Stake Design Philosophy" Medium, Dec. 30, 2016 • [13]Vitalik Buterin, "Serenity Design Rationale" Ethereum Foundation

Sufficiency - While blockchains cannot be too powerful, as greater power implies greater complexity and hence greater brittleness, blockchains must still be powerful enough for it to be possible to build layer 2 protocols on top of it that are neither centralized nor reliant on strong trust assumptions[14]. In order to achieve this blockchains must include an expressive (enough) programming language, scalable data availability and computation, and fast block times.

Defense in Depth - Blockchains must be fault tolerant and resilient to attacks and collusions, and in order to be so they must work well under a variety of possible security assumptions. A key way to achieve this is to design the system so that it is as decentralized as possible to prevent faults, collusions and attacks, and in the case where harmful collusion does take place, make it extremely expensive for those colluding and easy for non colluding participants to recover the system[15]. It is also important for participants validating the system to have skin in the game and for the system to hold individual contributors in a decision individually accountable for their contributions.

INSIGHTS FROM BISON TRAILS

Eth2's anti-correlation mechanisms have been designed to disincentivize centralization across all functional layers of the protocol including cloud, client and staking providers.

Full Light-Client Verifiability - Many users will only interact with the Ethereum blockchain through light clients - software that connects to full nodes in order to interact with the blockchain. Thus it's important for those users to be able to be sure that given some assumptions they can verify that the data in the full system is available and valid, even under a 51% attack.

PHILOSOPHY OF DECENTRALIZATION

According to the Bondareva–Shapley theorem, in cooperative game theory, which includes games that allow for the possibility of collusion, it is provable that there are large classes of games, such as majority games, that do not have any stable outcome. In majority games there is always the possibility that any subset of more than half of the agents could collude to capture a fixed reward and split it among themselves. Thus in order to create mechanisms that are stable, it is important to make it more difficult for agents to collude. And in the case of public blockchains, an important way of achieving this is through decentralization[16].

[14]Vitalik Buterin, "**Base Layers And Functionality Escape Velocity**" Vitalik's Website, Dec. 26, 2019 • [15]Vitalik Buterin, "**Coordination, Good and Bad**" Vitalik's Website, Sep. 11, 2020 • [16]Vitalik Buterin, "**Coordination, Good and Bad**" Vitalik's Website, Sep. 11, 2020

The purpose of decentralization is to make a blockchain resilient to faults, attacks, and collusion. This is not just an ideological appeal. The more trust minimized a blockchain is, the further it can scale itself to a global platform and as a consequence, attract a larger amount of capital and high value transactions[17].

Decentralization for public blockchains can be thought of across two dimensions: architectural and political. Architectural decentralization is about how many nodes a blockchain is made up of. While political decentralization is about how many people and entities control those nodes and how independent they are. For Ethereum this means validators, clients, developers, researchers, and users are diverse, independent, and geographically dispersed, and that knowledge of technical upgrades is democratized so everyone can evaluate and participate in discussions.

INSIGHTS FROM BISON TRAILS

Eth2 also intentionally omitted token-weighed on-chain governance, in contrast to most PoS blockchains, and will continue making decisions through rough consensus, helping it maintain its desired decentralization properties.

Decentralization in blockchains also conveniently makes it easy for non-colluding participants to coordinate forks that strip out colluding attackers and continue the system as is. Forking is trivial in the world of open-source software, with the primary challenge in doing so successfully typically being about gathering the legitimacy needed to coordinate all those who disagree with colluding attackers to follow along[18].

[17]David Hoffman, "**Global Public Goods and The Protocol Sink Thesis**" Bankless, Jul. 8, 2020 • [18]Vitalik Buterin, "**Coordination, Good and Bad**" Vitalik's Website, Sep. 11, 2020

PHILOSOPHY OF PROOF OF STAKE

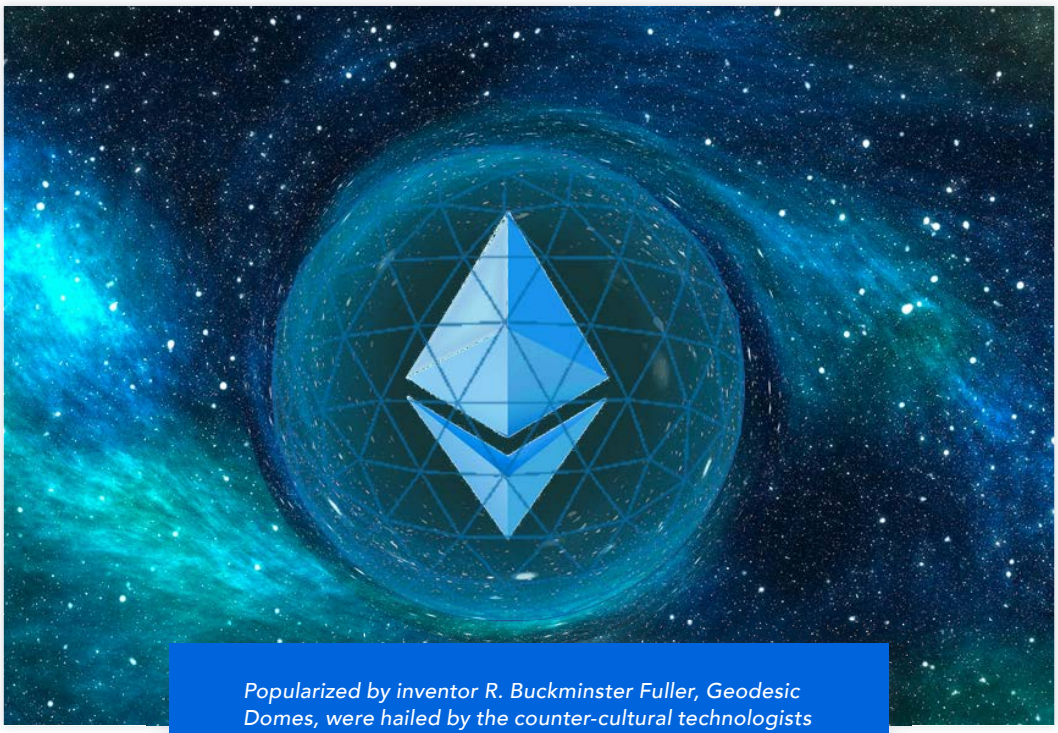
"Cryptography is truly special in the 21st century because cryptography is one of the very few fields where adversarial conflict continues to heavily favor the defender. Castles are far easier to destroy than build, islands are defendable but can still be attacked, but an average person's ECC keys are secure enough to resist even state-level actors. Cypherpunk philosophy is fundamentally about leveraging this precious asymmetry to create a world that better preserves the autonomy of the individual, and cryptoeconomics is to some extent an extension of that, except this time protecting the safety and liveness of complex systems of coordination and collaboration, rather than simply the integrity and confidentiality of private messages. Systems that consider themselves ideological heirs to the cypherpunk spirit should maintain this basic property, and be much more expensive to destroy or disrupt than they are to use and maintain."

- VITALIK BUTERIN[19]

Consensus mechanisms are critical for public blockchains. Nearly everything interesting that blockchains enable, such as digital scarcity and smart contracts, are impossible without sound consensus mechanisms. That's why Ethereum's shift to PoS was not taken lightly and has been a work in progress for nearly seven years now. PoS needs to be better than PoW, otherwise it is not worth abandoning a consensus mechanism that is tried and true.

There are three primary motivations for Ethereum moving to PoS: security, decentralization, and energy efficiency.

[19]Vitalik Buterin, "**A Proof of Stake Design Philosophy**" Medium, Dec. 30, 2016



Popularized by inventor R. Buckminster Fuller, Geodesic Domes, were hailed by the counter-cultural technologists of the 1970s for being highly resistant to external attack[20]

Security - At the core of PoS's security model is the idea that security comes from putting up economic value-at-loss[21]. Stakers may lose some, if not all, of their stake if they behave maliciously, serving as a major deterrent to launching attacks[22]. Such penalties, though rare, also make it much easier for PoS chains to recover from 51% attacks in the extreme case they do happen. In the event of a 51% attack, honest stakers can counter coordinate forks and delete the misbehaving stakers' stakes. This would be comparable to if a PoW blockchain burned down a malicious miner's ASIC farm for participating in a 51% attack[23]. 51% percent attacks in PoS are extremely expensive and ongoing 51% attacks are practically infeasible given that stakes are an internal accounting measure and can be deleted in the event a staker misbehaves.

Why this economic-value-at-loss matters and may make PoS more secure than Pow, is because of how large that economic-value-as-loss may be. Unlike ASIC based PoW blockchains, like Bitcoin, which require upfront capital costs in the form of ASICs, the capital costs PoS participants put up do not depreciate. Furthermore, given the low maintenance costs stakers pay to run validators and the fact that stakers can get their deposits back at any time after a short withdrawal period, the only cost stakers truly incur is an opportunity cost. These points are important because they theoretically make PoS stakers more willing to pay higher capital costs per a dollar of rewards, perhaps by an order of magnitude or more, thus raising the cost to attack the chain substantially[24].

[20]Jim Epstein, "**Bitcoin and the End of History**" Reason, Oct 28. 2020 • [21]Vitalik Buterin, "**A Proof of Stake Design Philosophy**" Medium, Dec. 30, 2016 • [22]Vitalik Buterin, "**A Proof of Stake Design Philosophy**" Medium, Dec. 30, 2016 • [23] "**Proof of Stake FAQs**" Ethereum Wiki • [24]Vitalik Buterin, "**Why Proof of Stake (Nov 2020)**" Vitalik's Website, Nov. 6, 2020

Decentralization - Mining centralization is an ever present risk in PoW blockchains and can be thought of across a couple of different dimensions: hash power centralization, manufacturer centralization, and geographic centralization. Regarding hash power centralization, running a mining operation is a capital intensive task that often requires significant investment to get into and be competitive. Furthermore, the mining business experiences economies of scale as it becomes less expensive to participate in on a unit basis as the business becomes larger - the most obvious example of this being that miners are able to negotiate bulk orders for ASICs and other equipment that lowers their unit costs.

Regarding manufacturer centralization, the supply side of the ASIC industry is extremely concentrated. In a January report, Token Insight estimated that the market share of the top four manufacturers in 2019 accounted for more than 95% of the total market share - with the overwhelming majority of activity taking place in China[25]. This geographic concentration is also present on the mining side as well. In 2019 CoinShares estimated that as much as 65% of Bitcoin hash power resides in China[26]. These two risks make mining much more exposed to censorship or interference, especially considering both mining farms and manufacturing facilities are large and difficult to hide (in contrast staking can be done on an ordinary laptop).

PoS avoids many of the above centralization risks by being more accessible to more participants. There are no economies of scale to PoS, the costs to participate in PoS are low, and ETH is widely dispersed after being distributed through PoW over the past five years. Plus rewards in PoS will be very low due to the reasons described above reducing the effects of current ETH holders theoretically having a perpetual claim on new issuance with little ongoing expenses.

Energy Efficiency - Finally, and perhaps the most simple of the three reasons, PoS is more energy efficient than PoW. Not only does PoS eliminate the need to burn enormous amounts of electricity (Bitcoin consumes more electricity than many small countries)[27], but it also achieves greater security per unit of cost as described above. Estimates are that it may only cost $120 a year to run a beacon node and validator client, which may be done using consumer hardware, as opposed to the high powered ASICs and large scale data centers often needed to mine PoW cryptocurrencies profitably[28].

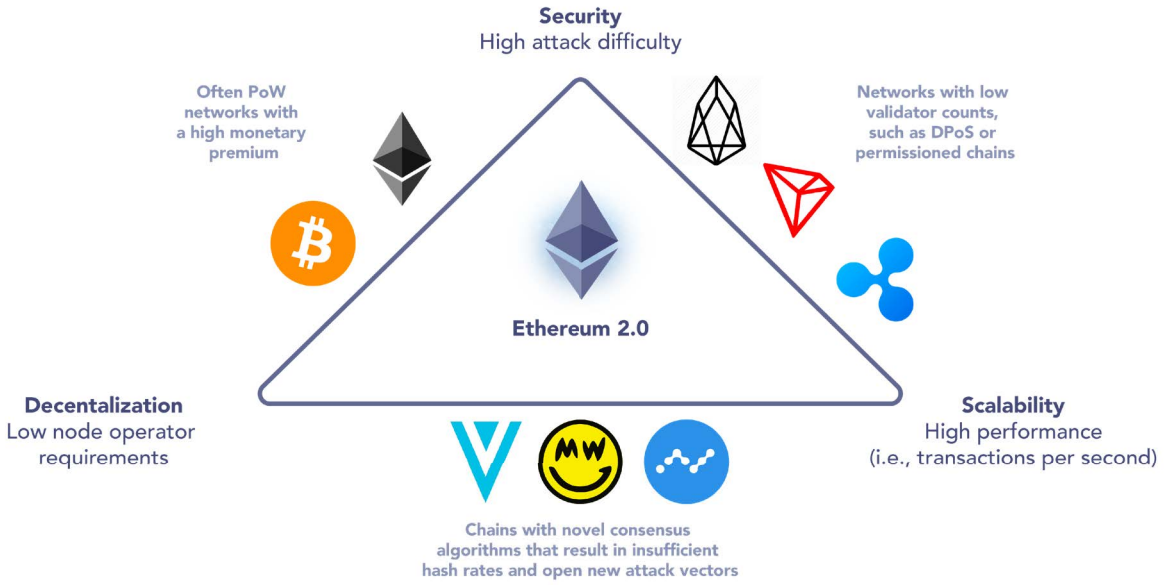
[25]Jennifer Wang, Johnson Xu, Wayne Zhao "**2019 Mining Industry Annual Research Report**" Token Insight, Jan. 2020 • [26]Christopher Bendiksen, Samuel Gibbons "**The Bitcoin Mining Network**" CoinShares, Dec. 3, 2019 • [27]James Vincent "**Bitcoin consumes more energy than Switzerland, according to new estimate**" The Verge, Jul. 4, 2019 • [28]Eric Conner, "**Eth 2.0 Economics**" EthHub

SHARDING

Scalability is important because it helps keep Ethereum open, allowing users to participate and interact without intermediaries. However, scaling blockchains is difficult because of a finicky relationship between decentralization, security, and scalability, that prevents blockchain systems from featuring all three properties. This is often referred to as the Scalability Trilemma. Historically, blockchains have only been able to achieve two of the three desired properties, and solving the Scalability Trilemma has been hailed as the holy grail of blockchains.

MESSARI

Mapping Blockchains According to the "Scalability Trilemma"



Source: Messari, Zooko Wilcox-O'Hearn, Ethereum GitHub, Arjun Balaji

Recognizing this challenge, Ethereum elected to pursue the path of sharding - a path that involves dividing Ethereum into 64 parallel shards, which each have a dynamic subset of nodes processing blocks of transactions. This was done to ensure the demands to run a node remain low enough so that anyone can do so using consumer hardware and Ethereum stays decentralized, while still increasing the scalability of the overall system.

For Ethereum, supernode requirements were a non-starter as it would make Ethereum more susceptible to centralization and collusion. Supernodes have high fixed costs, so fewer users can

participate. Furthermore high costs to run infrastructure make it more likely that nodes would run infrastructure with cloud computing providers (i.e AWS) - making Ethereum more exposed to central points of failure.

Base layer scalability for Ethereum was non-negotiable because Ethereum aims to ensure users can directly use the Ethereum blockchain without centralized intermediaries such as exchanges and other financial institutions. A future where Ethereum becomes a settlement layer for institutions and inaccessible to most users due to high fees would make this impossible. Access to the base layer is a necessity for self-sovereignty. And scaling is necessary to keep Ethereum accessible.

MONETARY POLICY

Ethereum's monetary policy is defined as "Minimum Necessary Issuance" - the minimum amount of issuance necessary to ensure Ethereum remains secure. Although such a monetary policy may seem subjective and prone to spurious adjustments, like any protocol parameter, Ethereum's monetary policy is enforced through social consensus. Any modifications to the monetary policy must be agreed upon by a wide range of stakeholders in the ecosystem - a feat that is far from easy. Since Ethereum's mainnet launch it has only modified its issuance twice, with both adjustments being to reduce issuance to these estimated minimums[29].

Ethereum opts for perpetual issuance and an uncapped supply because it prioritizes security over monetary idealism. Unlike deterministically issued and fixed supply cryptocurrencies, whose security budgets have been arbitrarily set is pursuit of "perfect money", Ethereum aims to issue enough ETH to ensure Ethereum remains secure now and into the future.

However, opting for perpetual issuance and an uncapped supply does not imply that Ethereum's monetary policy will be highly inflationary and unpredictable. A major component of Ethereum's shift to PoS is about lowering its issuance while maintaining the same level of network security. As discussed previously, PoS could provide an order of magnitude gain in security-per-cost and using this gain, Ethereum could dramatically reduce issuance while keeping its security level the same[30]. ETH 2.0's monetary policy will be dynamic, adjusting according to how much ETH is being staked, and will likely be well below 1%. Staking will also have the mutual benefit of making ETH a more productive asset, providing ETH with a native yield in addition to its store of value and commodity properties.

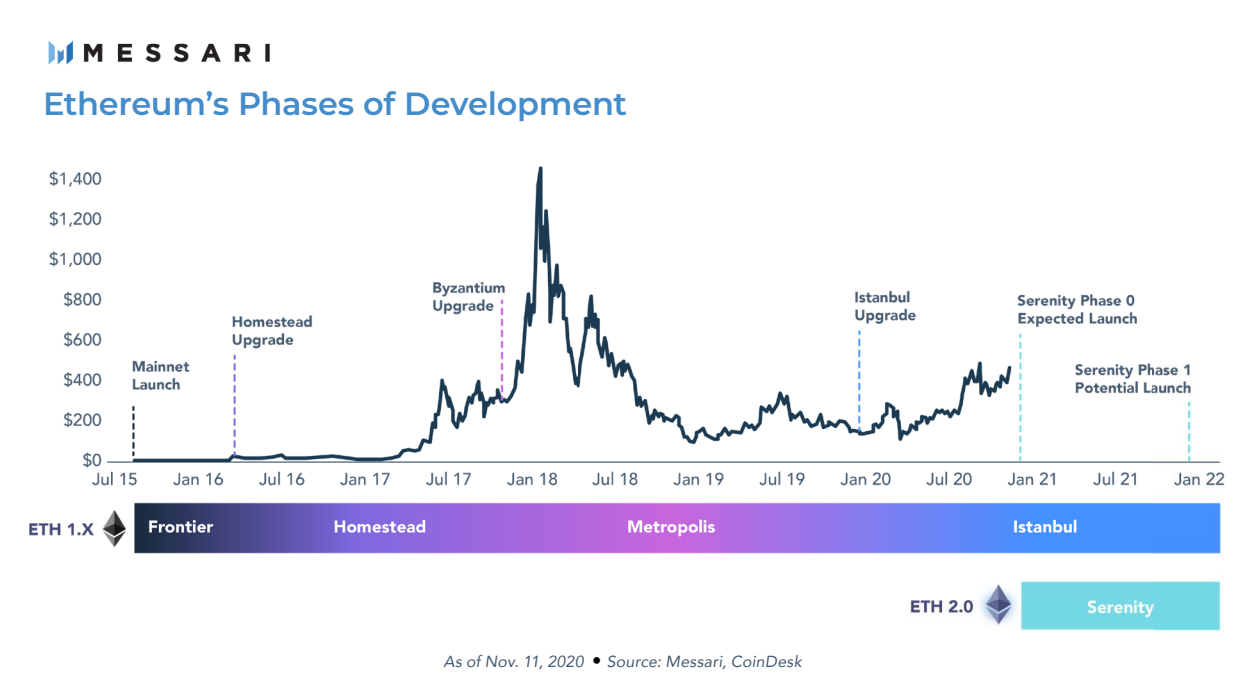
[29]Eric Conner, "**Monetary Policy**" EthHub • [30]Vitalik Buterin, "**Why Proof of Stake (Nov 2020)**" Vitalik's Website, Nov. 6, 2020

ETH validating	Max annual issuance	Max annual network issuance %	Max annual return rate (for validators)
1,000,000	181,019	0.17%	18.10%
3,000,000	313,534	0.30%	10.45%
10,000,000	572,433	0.54%	5.72%
30,000,000	991,483	0.94%	3.30%
100,000,000	1,810,193	1.71%	1.81%
134,217,728	2,097,152	1.56%	1.56%

Source: EthHub

History

The launch of ETH 2.0's Beacon Chain will usher in the Serenity era - the fourth and final stage in Ethereum's initial roadmap from 2015 that outlined the network's path to maturity[31]. The first stage, Frontier, marked the mainnet launch of Ethereum, while the following two phases (Homestead and Metropolis) each focused on adding the functionality and improvements required for Ethereum to realize its world computer aspirations. An additional phase, Istanbul, launched late in 2019 to bridge the gap between Metropolis and Serenity. But Serenity was by far the most ambitious of Ethereum's planned upgrades.

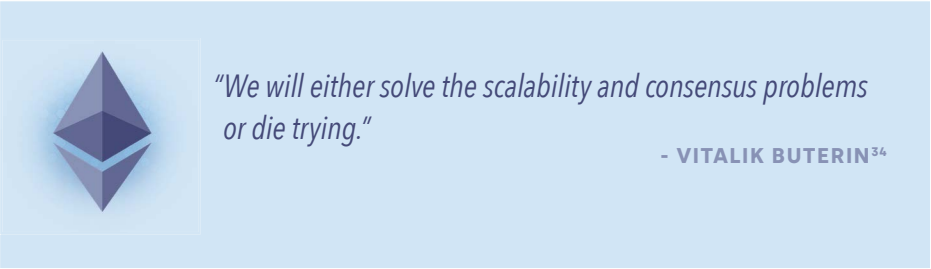


[31]Vinay Gupta, "The Ethereum Launch Process" Ethereum Foundation, Mar. 3, 2015

The original goal of Serenity was simple on paper - swap PoW for PoS, with the potential inclusion of some scalability enhancements. However, redesigning a network's consensus algorithm and architecture from the ground up is anything but simple in practice. Ethereum's rapid ascent in value and popularity in 2017 only narrowed the margin for error. With the existing network securing many billions of dollars worth of cryptoassets at current prices, the Silicon Valley cliche of "flying a plane while building it" befits what Serenity entails.

The sheer level of difficulty is why ETH 2.0 has taken nearly seven years to turn what some have called "heretical voodoo magic" into a production-ready system[32]. Its imminent arrival is the culmination of countless research efforts dating back to 2013 that tackled two of crypto's toughest problems: PoW alternatives and blockchain scalability[33].

FROM SLASHER AND HYPERCUBES TO CASPER AND SHARDING (2013-2015)



Ethereum's Proof-of-Stake journey originated in 2013, when Vitalik Buterin began to openly question Proof-of-Work's sustainability. While Proof-of-Work's security guarantees were well-documented, Vitalik suggested it fell prey to mining centralization and energy wastefulness. In his mind, Proof-of-Stake was the future.

But back in Ethereum's early days, PoS had two fatal security flaws. The first was that PoS systems couldn't detect or discourage validators from supporting multiple forks (called "double-signing"), an issue now commonly known as the "nothing-at-stake problem." The second was that new clients joining the network also couldn't differentiate the correct chain from a malicious fork in the event of a long-range attack, where a malicious validator creates a competing fork that begins thousands of blocks in the past.

Blockchain scalability faced a similar uphill battle. As Vitalik noted in early 2014, "not a single [project had] managed to overcome the same core problem: that every single full node must process every single transaction."[35] The only solutions at that point involved introducing some

[32]Vlad Zamfir, "**The History of Casper -- Chapter 1**" Ethereum Foundation, Dec. 6, 2016 • [33]Vitalik Buterin, "**Problems**" GitHub, Aug. 25, 2014 • [34]Vitalik Buterin, **Reddit**, Jun. 14, 2014 • [35]Vitalik Buterin, "**Ethereum Scalability and Decentralization Updates**" Ethereum Foundation, Feb. 18, 2014

centralization, often in the form of so-called "supernodes" that exercised outsized control over transaction and fork selection. More elegant ideas that might preserve decentralization hadn't progressed beyond the theoretical stage.

Despite the challenges at hand, it took the Ethereum team about a year to uncover what would become the basis for ETH 2.0.

On the PoS front, Vitalik penned the concept for a staking protocol called Slasher in Jan. 2014, two months after sharing the first copy of the Ethereum whitepaper[36]. Slasher made an attempt to mitigate the nothing-at-stake problem by withholding a validator's reward if they signed blocks on competing forks. Several months later, this idea behind penalizing validators and holding them economically accountable would influence Ethereum Foundation researcher Vlad Zamfir to introduce the use of validator security deposits[37]. Whereas Slasher forced bad actors to forgo profit, a provably faulty node in Zamfir's scheme would lose their security deposit, which effectively closed the door on making double-signing profitable.

Overcoming long-range attacks proved to be more of a mental hurdle. Proof-of-Work blockchains like Bitcoin are objective - new nodes can determine whether a chain is a malicious fork or not in a protocol defined manner (in this case, the heaviest chain rule). Proof-of-Stake could never achieve this level of objectivity due to the threat of long range attacks. Therefore, new nodes or those reentering the network after a long layoff must authenticate a PoS chain through extra-protocol means ("social consensus"). Removing human influence is central to the blockchain movement, and requiring new nodes to rely on social means (block explorers or client teams) to authenticate the network was antithetical. But Vitalik and team felt PoS offered enough advantages over PoW that accepting a small level of subjectivity (later defined as "weak subjectivity") was a fair tradeoff[38]. According to Vitalik, a system was weakly subjective if it required new validators to rely on extra-protocol authentication means only once when they first joined the network.

In 2015, Vlad and Vitalik molded the ideas behind security-deposit based security and weakly subjective authentication to form the foundations of Capser, the PoS algorithm used in ETH 2.0. The name Casper came from its adapted use of Ethereum's GHOST protocol to order transactions, help achieve finality, and make it "friendly" to all validator types (large vs. small). Vlad announced that the first Caper specifications were in the works a mere two days after Ethereum's mainnet launch[39].

[36]Vitalik Buterin, "**Slasher: A Punitve Proof-of-Stake Algorithm**" Ethereum Foundation, Jan. 15, 2014 • [37]Vlad Zamfir, "**The History of Casper -- Chapter 1**" Ethereum Foundation, Dec. 6, 2016 • [38]Vitalik Buterin, "**Proof of Stake: How I Learned to Love Weak Subjectivity**" Ethereum Foundation, Nov. 25, 2014 • [39]Vlad Zamfir, "**Introducing Casper "the Friendly Ghost**" Ethereum Foundation, Aug. 1, 2015

Ethereum's research on blockchain scalability paralleled the progress on PoS in 2014. Vitalik and the rest of the team contemplated several strategies throughout the year, most prominently pushing the scaling responsibilities to applications[40], creating a mesh network of interconnected "sub-states" (called a hypercube[41], and adopting sidechains that use the main Ethereum chain as a central hub[42]. All of these approaches had undesirable tradeoffs. The application-specific strategy couldn't scale to all use cases, hypercubes had data availability and fragility issues, and the hub-and-spoke model introduced security concerns since smaller chains would be more susceptible to majority stake attacks. But each concept built on the lessons learned from prior attempts and showed a clear progression towards partitioning the network's workload across multiple sub groups of nodes.

By 2015, sharding had become a focal point for ETH 2.0[43]. There were some remaining questions on how a sharded network would manage changes in state across disparate chains and coordinated validator attacks on a single shard (solution: pseudorandom validator selection and security deposit penalties). But it had the desired property of reducing network workload on individual participants without relying on omnipotent nodes. Plus, sharding had the theoretical potential to increase the speed of transaction throughput from 10-20 tps (transactions per second) to 100,000. Vitalik captured the early design ideas for Ethereum's sharding architecture in the "Mauve Paper," which was one of the first attempts to define the technical specifications of ETH 2.0[44].

Ethereum-turned-Polkadot founder Gavin Wood also contributed towards the project's sharding research, releasing a proposal in 2015 that detailed an instance of sharding a network's data and state across many sub-chains, which he called Chain Fibers[45]. These sub-chains would plug into a single master chain that would coordinate validators to manage the security and communication between the various Chain Fibers. While Wood eventually pivoted this proposal into the foundation for Polkadot, the core concept behind it lives on in ETH 2.0's Beacon Chain, which serves as the sole coordination layer for shard chains.

[40]Vitalik Buterin, "**Scalability, Part 1: Building on Top**" Ethereum Foundation, Sep. 17, 2014 • [41]Vitalik Buterin, "**Scalability, Part 2: Hypercubes**" Ethereum Foundation, Oct. 21, 2014 • [42]Vitalik Buterin, "**Scalability, Part 3: On Metacoin History and Multichain**" Ethereum Foundation, Nov. 13, 2014 • [43]Vitalik Buterin, "**Vitalik's Research and Ecosystem Update**" Ethereum Foundation, Oct. 18, 2015 • [44]Vitalik Buterin, "**Ethereum.org 2.0 Mauve Paper**" Sep, 6, 2016 • [44]Gavin Wood, "**Blockchain Scalability: Chain-Fibers Redux**" Ethereum Foundation, Apr. 5, 2015

THE DARK AGES OF RESEARCH (2015-2017)

Ethereum Foundation research teams released the first Serenity proof-of-concept (PoC) in late-2015 and followed it up with two more over the course of 2016. These releases, which eventually set the foundation for the now-deprecated Pythereum ETH 2.0 client, contained the early features behind Casper and added the scaffolding necessary to deploy shards chains in a way that wouldn't disrupt the existing network.[46]

They also included various proposals to abstract away a few of the complexities within the network that bogged down user and developer experience. One such proposal that was gaining momentum but failed to make the initial PoCs was upgrading the network's virtual machine (the EVM) to a WebAssembly (WASM) based version.[47]

These PoCs illustrated what would come to define the next few years of research on ETH 2.0. The work endured by devoted Ethereum developers leading up to 2016 had helped determine how to solve the challenges associated with PoS and blockchain scalability. Researchers now had to convert those ground-breaking theories into prototypes and working products.

Vitalik noted that these middle years included several "failed attempts" at finalizing core features. Developers spent many months working on Casper's original consensus mechanism (called "Consensus by Bet") before scrapping it in favor of a less radical method. Scaling techniques like blockchain rent (ongoing payments for data storage to node operation costs) and quadratic sharding (a system built from shards of shards for unlimited scalability) received significant time and attention but never made it into the final design due to their complexity. Progress also stalled briefly when research teams directed resources away from Serenity to deal with the The DAO incident in June 2016 and the Shanghai DoS attacks later that Fall.[48]

The crypto gods weren't kind to ETH 2.0's progress in 2016, but Serenity research teams had no reason to rush their work. Network activity was consistently at low and manageable levels, and Ethereum was still progressing gradually toward its third planned phase, Metropolis. There wasn't a dire need to scale the network yet. Research teams working on Ethereum's next iteration had adequate buffer room to prioritize security and resiliency over timeliness.

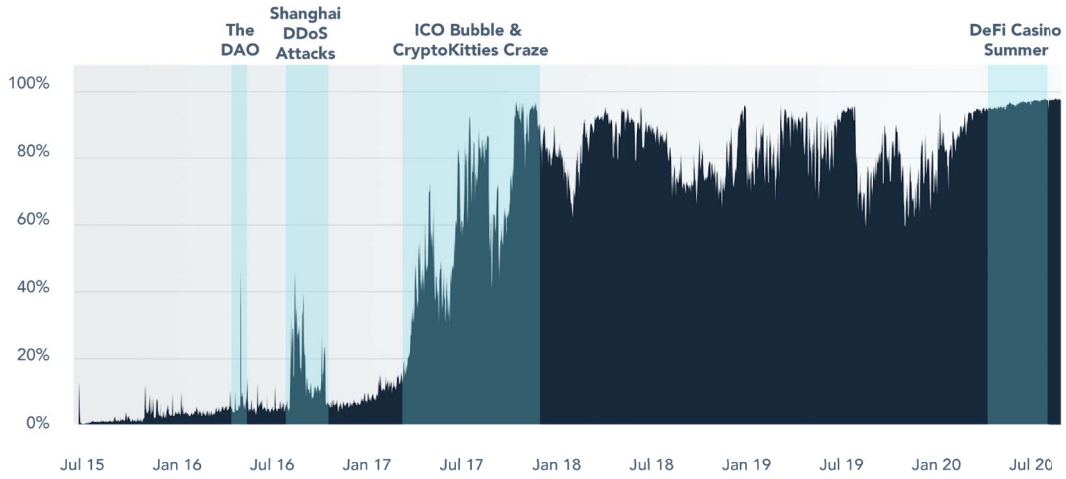
Then 2017 and the infamous ICO (initial coin offering) boom arrived. Investors and developers alike began using the network en masse to capitalize on rising ETH and token prices. The craze pushed Ethereum to limits, leading to skyrocketing fees and stunting the network's ability to process transactions in a timely manner. Scalability became a first-level priority almost overnight.

[46]Vitalik Buterin, "**Serenity PoC2**" Ethereum Foundation, Mar. 5, 2016 • [47]Vitalik Buterin, "**Vitalik's Research and Ecosystem Update**" Ethereum Foundation • [48]Vitalik Buterin, "**Devcon4 Keynote**" YouTube, Oct. 31, 2018

MESSARI

Percentage of Ethereum Block Space Used

The ICO Bubble in 2017 pushed Ethereum to its limits and made scalability an immediate priority.



As of Nov. 11, 2020 • Source: Etherscan

This breakout year affirmed the concerns that the network couldn't support world computer levels of activity in its current state. But it also affirmed the decision to spend the time and energy on reinventing the network's architecture. Ethereum needed Serenity now more than ever, and 2017's bull run supplied the Ethereum Foundation with enough motivation (and funding) to supercharge development efforts going forward.

During the year, Casper's design finally started to take shape. Vitalik released the first paper on ETH 2.0's official PoS algorithm, Casper FFG (Friendly Finality Gadget), in September 2017. Casper FFG got its name and core features by borrowing from Vlad Zamfir's work on PoS network design, which he eventually rolled out as a new family of consensus protocols and independent area of research called CBC (Correct by Construction) Casper.

Vitalik's amended Casper version featured a hybrid PoW and PoS mechanism with minimal slashing conditions. Vitalik and the team planned to deploy Casper FFG as a smart contract atop the existing Ethereum network where PoS validators would verify the work of PoW miners every 50 blocks.[49] The initial intent was to gradually introduce PoS to Ethereum and bootstrap a validator set while minimizing any disruptions to ongoing activity. This Frankenstein system would also make it easier to swap out PoW entirely further down the line. Employing Casper FFG as a so-called overlay network was a creative yet clunky approach that has since undergone significant strategic changes.

[49]Vitalik Buterin & Virgil Griffith, "**Casper the Friendly Finality Gadget**" Oct. 25, 2017

2017 ended with the release of a Casper FFG testnet and the first sharding design specification, indicating that there was some light at the end of the tunnel. After a few years of seemingly running in place, Serenity had some momentum heading into what would become the homestretch.

THE BEACON ERA (2018-2020)

Breakthroughs in research don't occur in a vacuum; they are the sum of the lessons learned and incremental achievements made along the way. But every major discovery often has a defining "Aha!" moment. That "Aha!" moment for ETH 2.0 came in June 2018, when a new proposal called to unite the Casper FFG and sharding designs.[50]

Until this proposal, Ethereum's Casper and sharding research groups operated independently. The Danny Ryan-led Casper FFG team was working towards the hybrid PoS and PoW vision laid out by Vitalik one year earlier, whereas the Justin Drake-led sharding unit had a separate roadmap for adding shard chains to Ethereum.

Despite their different objectives, both teams ran into similar issues trying to create feature-rich contracts within the limitations of Ethereum's internal computer (the EVM). They also shared several core design requirements, including validator deposits and slashing penalties, random number generators, and aggregate signatures.[51]

In light of these commonalities, developers deprecated the approach for building atop Ethereum 1.x and pivoted towards building Casper and sharding on an entirely new network, which they called the Beacon Chain. This shift in strategy would make it easier to integrate sharding with Casper later on, and it would isolate Ethereum's on-chain activity from any growing pains that might arise during the process. Both teams confirmed their commitment to the new direction by releasing a new multi-phase roadmap in which the initial step marked the launch of the Beacon Chain.

ETH 2.0 developers have adjusted the protocol slightly since the new plan took effect. In October 2019, they lowered the number of shard chains that Phase 1 (the second phase) would introduce from 1024 to 64, which simplified some design elements and lowered Phase 0 launch requirements.[52] Later that year, Vitalik proposed a solution for merging the existing Ethereum state (account balances and contract code) into a shard within the ETH 2.0 system, prompting the addition of a fourth phase to the roadmap (dubbed Phase 1.5).[53]

[50]Danny Ryan, "**Casper * Sharding**" Medium, Jun. 15, 2018 • [51]Ben Edgington, "**State of Ethereum Protocol #1**" Medium, Aug. 28, 2018 • [52]Vitalik Buterin, "**Eth2 shard chain simplification proposal**" HackMD, Oct. 1, 2019 • [53]Vitalik Buterin, "**Alternative proposal for early eth1 <-> eth2 merge**" EthResearch, Dec. 23, 2019

Despite these adjustments, the current vision for ETH 2.0 has remained largely unchanged. Without the need to account for a shifting landscape, research teams have been able to focus on formalizing the Beacon Chain's design for client and testnet development. But building sophisticated systems is complicated, which is why it took about a year to solidify the code and launch the first single-client testnet (managed by Prysmatic Labs).

Further testing and security audits also ate up months of time. Within the last year, Ethereum's research teams have administered several third-party audits on the essential pieces of code for Phase 0. They have also launched four different Beacon Chain replicas as testnets and completed three dry runs of the new network's launch process.

While the lengthy testnet period may have felt like a slow and, at times, arduous process, it gave ETH 2.0 developers enough confidence to declare the Beacon Chain mainnet-ready. ETH 2.0's first phase will launch on Dec. 1, 2020, almost seven years after Vitalik penned Ethereum's whitepaper.

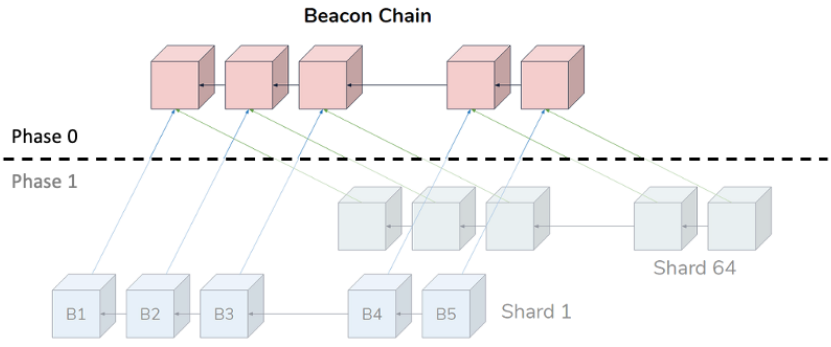
There's still plenty of work ahead, as the designs for ETH 2.0's subsequent phases are unfinished. But the launch of the Beacon Chain is a monumental milestone that marks the start of a new era in Ethereum's history: the future of the crypto economy.

Part 2: Phases and Implications

Phase 0

PHASE 0 OVERVIEW

Phase 0 marks the long-awaited launch of the Beacon Chain, the PoS layer at the core of ETH 2.0. The Beacon Chain is ETH 2.0's virtual central nervous system that coordinates block production, manages the registry of validators and their balances, and applies consensus rules (including the issuance of rewards and penalties). Later on, it will also serve as the anchor point for each of Phase 1's 64 shard chains.



*Source: **Hsiao-Wei Wang***

At a high level, Phase 0 is all about staking. The Beacon Chain's arrival will enable ETH holders to become an ETH 2.0 validator and earn income on their staked ETH. Beyond staking, the Beacon Chain will have limited functionality for the duration of Phase 0. There will be no transactions until Phase 1.5 and no smart contract support until Phase 2 (if ever). Phase 0's sole purpose is to bootstrap ETH 2.0's validator set and ensure that the network can securely support the features introduced in subsequent phases. Despite its minimalist, almost testnet-like feature set, the Beacon Chain will have real financial opportunities and consequences for stakers[54].

[54]Viktor Bunin, "**Bison Trails Announces Support for Eth2**" Bison Trails, Jun. 29, 2020

ETH 2.0's initial phase consists of two key pieces of infrastructure, with the most obvious one being the Beacon Chain. The second is the deposit contract, which will work with the Beacon Chain to turn ETH holders into stakers for the first time.

DEPOSIT CONTRACT

The process of becoming an ETH 2.0 validator begins at the deposit contract. The Beacon Chain will be a new network that runs parallel to the current Ethereum blockchain. This layer of separation will allow ETH 2.0 to launch and evolve without interrupting any ongoing activity on ETH 1.x. But it will require a cross-chain communication solution to onboard stakers onto the Beacon Chain. That's where the deposit contract comes in.

This contract, which is deployed on the ETH 1.x blockchain, is a one-way bridge between Ethereum and the Beacon Chain. Like its name suggests, the deposit contract accepts ETH deposits from aspiring stakers. If the deposit is valid, the ETH 2.0 clients will signal the Beacon Chain to mint an equivalent amount of ETH on ETH 2.0 and assign them to the correct account, which the depositor can then claim using their corresponding validator keys.

There are a few restrictions regarding what makes a deposit valid and what validators can do with their newly minted ETH 2.0 ETH. First, validator accounts require a minimum of 32 ETH to activate. This 32 ETH requirement was a deliberate design choice since acquiring this amount is relatively attainable (~$16,500 at current prices) but expensive enough to prevent the validator count from ballooning to a point that would cause network overhead issues.[55]

Stakers can send more than 32 ETH to the deposit contract.[56] However, any extra ETH won't have an impact on their potential returns or effectiveness as a validator.[57] For those looking to stake more than 32 ETH, it would be more efficient to create multiple validators with a balance of 32 ETH each. Stakers can manage several thousand validator accounts through a single ETH 2.0 client (also called a validator client); therefore, the increase in overhead for creating multiple validators is relatively minimal. As for accounts that don't meet the validator minimum, a range of services from professional validators and exchanges to decentralized staking protocols will likely offer to pool customer funds into 32 ETH batches and stake on their behalf.

[55]Vitalik Buterin, "**Serenity Design Rationale**" Ethereum Foundation • [56]Ben Edgington, "**The Genesis of a Beacon Chain**" HackMD, Jul. 31, 2020 • [57]Viktor Bunin, "**Bison Trails Announces Support for Eth2**" Bison Trails, Jun. 29, 2020

The second restriction is that the deposit contract is unidirectional. Once ETH goes into the deposit contract, the only course of action is to claim ETH 2.0 ETH and stake. These staked assets along with any inflation rewards will be completely immoble for the foreseeable future since the Beacon Chain won't be able to process transactions until Phase 1.5. ETH 2.0 researchers explored building a bidirectional bridge but determined it would put ETH 1.x at too great of a risk should any issues on ETH 2.0 arise. Making the deposit contract irreversible was a safer approach that "allowed for a quicker development cycle on ETH 2.0."[58]

INSIGHTS FROM BISON TRAILS

There's been much interest in making the bridge bi-directional, but this is a difficult engineering task because it requires the existing Ethereum chain to also keep track of the eth2 beacon chain. The decision was made to launch it as a one-way bridge to avoid unnecessarily delaying eth2 genesis. It also creates significant skin-in-the-game to eventually merge the two chains in Phase 1.5 to regain access to those funds.

While it was a conscious decision to side with security over user experience, the Ethereum community still recognizes that the indefinite lockup of validator funds is undesirable and could hinder adoption in its early phases. The possibility that developers solve this validator liquidity dilemma before Phase 1.5 is not out of the question. Researcher Justin Drake mentioned that one option could be a slow two-way bridge that operates on the order of several weeks to mitigate any onboarding or offboarding risks.[59] A more probable and immediate solution will come from service providers and protocols that allow customers to either borrow against or securitize their staked ETH on the ETH 1.x chain, as discussed in greater detail in the Staking Illiquidity and Staking Derivatives section below.

INSIGHTS FROM BISON TRAILS

Phase 0 requires long-term infrastructure commitments and trustworthy partners. Switching validator providers increases the risk of slashing, either as a result of double voting or surround votes. Professional providers are unlikely to take on this added risk, so evaluate your options carefully.

BEACON CHAIN LAUNCH

The deposit contract also played a central role in the Beacon Chain's launch. This new network didn't come with a definitive genesis date. Instead, it could only launch once the deposit contract received at least 524,288 ETH (~$315 million at current prices), which at 32 ETH per validator equates to 16,384 validators at genesis. The Beacon Chain's genesis process gets slightly more complicated from here. At a high level, there was a seven day delay between the deposit contract reaching this threshold, but the earliest the Beacon Chain could

[58]Danny Ryan, "**eth2 quick update no. 4**" Ethereum Foundation, Nov. 21, 2019 • [59]Justin Drake, "**Ethereum Foundation ETH 2.0 Research Team AMA (Pt. 4)**" Reddit, Jul. 10, 2020

launch was on a predetermined "minimum genesis date," which was Dec. 1, 2020.[60] If the deposit contract didn't receive enough ETH one week before this date, the Beacon Chain would have remained dormant until more validators signaled their support.

Developers implemented this minimum validator requirement for genesis to serve as an extra security measure to ensure that the Beacon Chain has adequate validator support early on. It also acts as a defense against gatekeeping attacks, in which existing ETH 2.0 clients ignore valid staking deposits since each new validator added to the network decreases individual returns.[61] Some Ethereum community members were skeptical of this minimum threshold, deeming it too steep relative to the opportunity cost of an indefinite lockup period. With the crypto market on the rise and DeFi applications still offering favorable yields, ETH holders might prefer to keep their funds on hand in the near term.

The counter argument was that staking, trading, and liquidity mining might appeal to different personas and won't end up competing.[62] Staking could have a greater appeal to long term holders, whereas those with a shorter investment horizon might gravitate towards trading and DeFi applications. There was also a chance that the pent up demand for ETH staking and ETH 2.0 would become more relevant as the Beacon Chain's minimum genesis date drew near. If new DeFi protocols can attract hundreds of millions of dollars in mere hours, then the Beacon Chain shouldn't have an issue meeting its minimum validator requirement without any significant delays.

INSIGHTS FROM BISON TRAILS

Given the overall complexity of the endeavor, the early stages of Phase 0 will be concentrated on the 'ETH at stake' level as well as the deeper layers of the network (infrastructure providers & client software). This spells a very attractive opportunity for the brave early adopters that choose to swim alongside the innovators because rewards are shared between fewer parties.

It turns out that this counter theory was correct. The deposit contract surpassed 524,288 ETH deposits on Nov. 23, 2020, which confirmed the Beacon Chain would launch on Dec. 1, 2020 - its minimum genesis date. Reaching this minimum threshold was the first step. The total number of validators that join in Phase 0 will likely depend on ETH 2.0 staking yields, the market climate, and the launch of solutions to the validator illiquidity dilemma, as discussed in the Staking Illiquidity and Staking Derivatives section below.

[60]Ben Edgington, "**The Genesis of a Beacon Chain**" HackMD, Jul. 31, 2020 • [61]Mikera Quintyne-Collins, "**Potential attack on the beacon chain by rational validators: The Gatekeeping Attack**" GitHub, Mar. 22, 2019 • [62]Anthony Sassano, "**To Stake or Not to Stake**" The Daily Gwei, Jul. 21, 2020

BEACON CHAIN CONSENSUS

The Beacon Chain will be Etheruem's new PoS blockchain. It will manage all validator deposits and eventually serve as the base security and coordination layer for Phase 1's 64 shard chains.

From an architectural perspective, the Beacon Chain consists of epochs that break down further into slots. A slot is a 12 second window for a block to be added to the network, and an epoch is 32 slots, which amounts to six minutes and 24 seconds per epoch. In Phase 0, ETH 2.0 consists of only one chain, the Beacon Chain; therefore, slots will contain a single block. Once Phase 1 arrives and introduces 64 shard chains, slots will be an opportunity to add one Beacon Chain block and 64 shard blocks to the network. The first slot in every epoch generally serves as a network checkpoint, which helps finalize previously added blocks (make them essentially irreversible) and directs new clients towards the right chain in the event of a fork.

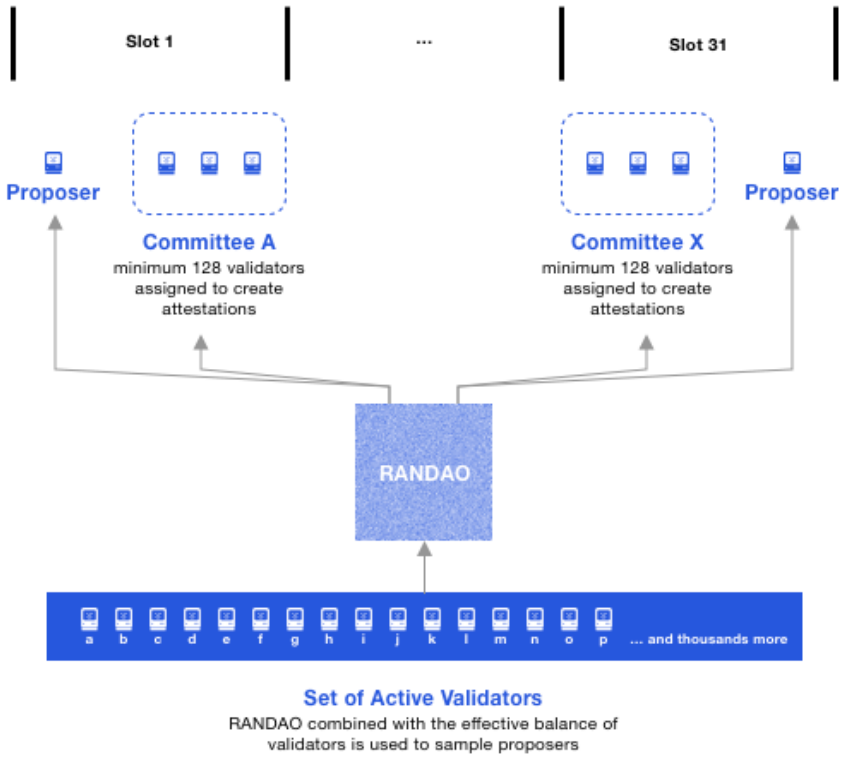
Block production on the Beacon Chain differs significantly from Ethereum's PoW network. Whereas PoW involves miners competing individually in a winner-take-all scenario, ETH 2.0's PoS system is more collaborative. A subset of Beacon Chain validators (think of them as virtual miners) votes on new blocks and every participant earns a reward for their contribution.

For each slot, the Beacon Chain uses a random sampling mechanism called a RANDAO to pseudorandomly select one validator to propose a block. It uses the same sampling mechanism to also pseudorandomly select a group (or multiple groups) of validators called attestors that will vote on the validity of the newly proposed block. Votes are weighed by an attester's staking balance. A single group of attesters represents a committee, and each committee has a target membership of 128 validators. By using random sampling, the network effectively eliminates the chance that a minority attestor (one that owns less than 66% of all network stake) can win a majority share of a committee and manipulate the block production process.[63]

INSIGHTS FROM BISON TRAILS

Supporting hundreds of thousands, and even millions, of validators is extremely difficult due to the sheer amount of signature volume required for consensus. This is why BLS signatures, which enable easy and efficient signature aggregation, are a key component of eth2.

[63]Vitalik Buterin, "Serenity Design Rationale" Ethereum Foundation



Source: Joseph Chow

Attesters abide by two different processes defined by ETH 2.0's PoS consensus rules. The first process is LMD GHOST (Last Message Driven Greediest Heaviest Observed SubTree), which adds new blocks and determines the head of the chain by choosing the fork that has the most votes. The second, Casper FFG (Casper, the Friendly Finality Gadget), finalizes blocks, as in it makes the final decision on which blocks are part of the chain.[64] Each validator attestation contains an LMD GHOST vote to add a new Beacon Chain block and a Casper FFG vote that points to the current epoch's checkpoint. As defined by Casper FFG, if a checkpoint receives support from two-thirds of network validators, all blocks in that epoch get "justified." These blocks will become finalized once the following epoch's checkpoint also gets justified. The time from block creation to finalization will typically be just shy of 13 minutes (12 minutes and 48 seconds to be exact).[65]

The distinction between the LMD GHOST and Casper FFG becomes important in the event of an attack or if a large number of validators are offline. Finalization requires two-thirds of network validators to remain active. If voting activity falls below this threshold, which could signal an attack, Casper FFG will stop finalizing blocks, but new block production will continue through LMD GHOST.[66] Once the network regains stability and validators can vote consistently again, Casper FFG will resume its finality responsibilities, including the finalization of the valid blocks generated during its hiatus. These two algorithms coordinate to keep the Beacon Chain alive even when the network is operating suboptimally.

[64]Carl Beekhuizen, "Two ghosts in a trench coat" Ethereum Foundation, Feb. 12, 2020 • [65]Joseph Chow, "The Beacon Chain Ethereum 2.0 explainer you need to read first" Ethos Dev, May. 23, 2020 • [66]Carl Beekhuizen, "Two ghosts in a trench coat" Ethereum Foundation, Feb. 12, 2020

The Beacon Chain uses an intricate system of validator rewards and penalties to avoid suboptimal execution while encouraging honest voting practices and high uptimes. Validators receive rewards for both producing and attesting (LMD GHOST and Casper FFG votes) blocks that receive super-majority support. Attestations for blocks that get finalized are worth even more. But missed votes or votes for blocks that don't get finalized result in penalties (removal of staked balance) in proportion to the rewards they would have obtained for executing those responsibilities adequately.[67]

Since missed attestations might be common, these types of penalties are relatively minor and act more like negative rewards. If a validator is online greater than ~54% of the time, it should break even. Validators that fall below this mark, however, could be at risk of losing a portion of their stake. If a validator's staked balance falls below 16 ETH due to penalties, they will be forced to exit the network. Since Phase 0 doesn't support transactions, disqualified validators won't be able to withdraw their remaining balance until Phase 1.5. However, stakers can prevent deactivations due to penalties by topping up their accounts with new ETH to keep their balance above 16 ETH.[68]

Acts such as double signing (voting for two blocks in the same epoch) or surround voting (attesting conflicting checkpoints on separate occasions) result in heavier punishments called slashings. Slashable offenses are often deliberate or a consequence of a poorly operated validator client and won't affect validators that correctly follow the protocol unless its corresponding client contains an unfortunate bug. Slashings typically result in the loss of at least 1/32 of a validators balance, but these losses are amplified if other validators commit a punishable act in the same epoch.[69] These mass slashings, referred to as correlated slashings, are a security measure to discourage and inhibit coordinated network attacks. Validators also police each other and can receive a reward (called a whistleblower's reward) for reporting slashable offenses.

INSIGHTS FROM BISON TRAILS

For Phase 0, slashable offences need not be discovered immediately. Eth2 allows for a window of time between an offence being committed and the inclusion of a slashing proof, that can be arbitrarily long.

The Beacon Chain has one final penalty mechanism called the inactivity leak. This penalty scheme only occurs when the network fails to reach finality for more than four epochs, which means more than one-third of validators have been offline for almost an hour. In response, the Beacon Chain issues a penalty to inactive validators (active validators remain unharmed) that increases quadratically until a checkpoint gets finalized. These mounting penalties either incentivize offline validators to come back and remain online or drain inactive accounts to a forced exit. By enforcing network activity, the inactivity leak helps the network resume finality by restoring the balance of online to offline validators.

[67]Joseph Chow, "**The Beacon Chain Ethereum 2.0 explainer you need to read first**" Ethos Dev, May. 23, 2020 • [68]Viktor Bunin, "**Bison Trails Announces Support for Eth2**" Bison Trails, Jun. 29, 2020 • [69]Joseph Chow "**The Beacon Chain Ethereum 2.0 explainer you need to read first**" Ethos Dev, May. 23, 2020

STAKING ECONOMICS AND IMPLICATIONS FOR ETH

Validators are rewarded for performing adequately, penalized for performing inadequately, and potentially slashed for behaving maliciously. However, yields are just one side of the profit equation. In addition to rewards and penalties, which will determine the headline yield validators will receive, validators must also consider various costs.

Costs include capital acquisition costs (minimum 32 ETH needed to stake), opportunity costs (stakers are unable to withdraw their stake until Phase 1.5), and infrastructure costs (validator clients and beacon nodes). There are a variety of ways of approaching these costs that include doing everything yourself, outsourcing infrastructure to staking-as-a-service providers and exchanges, or pooling resources (both ETH and infrastructure) to validate. The 32 ETH minimum requirement costs ~$16,500 at current prices, and rough estimates on the infrastructure side are that it will cost just $120 a year to run a beacon node and validator client, which may be done using consumer hardware.[70]

More specifically what will determine the headline yield is a combination of staking participation and validator uptime. The Beacon Chain needs at least 524,288 ETH staked to launch - at which point validators would be earning ~23% per year. However, depending on the rate of adoption that yield may drop considerably. Participation will likely start low, with primarily ideological and long-term oriented ETH holders being the first to lock funds in the deposit contract as they will be most willing to assume the early risks and accept the opportunity cost of having their ETH locked until Phase 1.5. But over time as users become more comfortable with the risks of staking, and service providers become better able to satisfy stakers needs (like liquidity), adoption should increase.

According to ConsenSys, the rate of staking participation for ETH 2.0 where it will match the security of ETH 1.x will be just under 16 million ETH. At this point validators would be earning a theoretical max of 4.4% per year. Although it may be a long time before that target is reached if at all before Phase 1.5.

INSIGHTS FROM BISON TRAILS

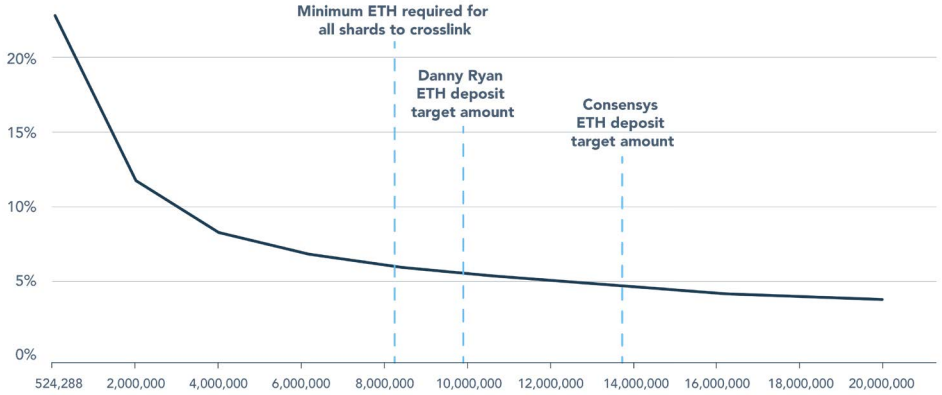
Proof of stake represents a new type of digital work agreement between the protocol and its participants. Validators are lenders of capital, labor, and security, while receiving periodic rewards for their contribution to public infrastructure.

[70]Eric Conner, "**Eth 2.0 Economics**" EthHub

MESSARI

Ethereum Validator Yields

Assuming 100% validator uptime, staking yields will likely be in the 4%-6% range at scale.



Note: Assumes starting supply of 113,000,000 ETH. Also assumes 100% validator uptime - the theoretical maximum. • Source: Messari, Consensys

The above analysis assumes 100% validator uptime, but of course validator uptime is highly unlikely to be 100%. The next table provides sensitivity around network wide validator uptimes to provide a fuller picture of what rewards may look like.

MESSARI

Ethereum 2.0 Validator Yields

VALIDATOR ISSUANCE — **Average Network % Online**

Total ETH Staked (Network)	70%	75%	80%	85%	90%	92%	94%	96%	98%	100%
524,288	16.5%	17.6%	18.7%	19.8%	20.9%	21.3%	21.7%	22.1%	22.5%	23.0%
2,000,000	8.4%	9.0%	9.6%	10.1%	10.7%	10.9%	11.1%	11.3%	11.5%	11.8%
4,000,000	6.0%	6.4%	6.8%	7.2%	7.5%	7.7%	7.9%	8.0%	8.2%	8.3%
6,000,000	4.9%	5.2%	5.5%	5.8%	6.2%	6.3%	6.4%	6.5%	6.7%	6.8%
8,000,000	4.2%	4.5%	4.8%	5.1%	5.3%	5.4%	5.6%	5.7%	5.8%	5.9%
10,000,000	3.8%	4.0%	4.3%	4.5%	4.8%	4.9%	5.0%	5.1%	5.2%	5.3%
12,000,000	3.4%	3.7%	3.9%	4.1%	4.4%	4.4%	4.5%	4.6%	4.7%	4.8%
14,000,000	3.2%	3.4%	3.6%	3.8%	4.0%	4.1%	4.2%	4.3%	4.4%	4.4%
16,000,000	3.0%	3.2%	3.4%	3.6%	3.8%	3.9%	3.9%	4.0%	4.1%	4.2%
18,000,000	2.8%	3.0%	3.2%	3.4%	3.6%	3.6%	3.7%	3.8%	3.8%	3.9%
20,000,000	2.7%	2.9%	3.0%	3.2%	3.4%	3.4%	3.5%	3.6%	3.7%	3.7%
22,000,000	2.5%	2.7%	2.9%	3.1%	3.2%	3.3%	3.4%	3.4%	3.5%	3.5%
24,000,000	2.4%	2.6%	2.8%	2.9%	3.1%	3.1%	3.2%	3.3%	3.3%	3.4%
26,000,000	2.3%	2.5%	2.7%	2.8%	3.0%	3.0%	3.1%	3.1%	3.2%	3.3%
28,000,000	2.3%	2.4%	2.6%	2.7%	2.9%	2.9%	3.0%	3.0%	3.1%	3.1%
30,000,000	2.2%	2.3%	2.5%	2.6%	2.8%	2.8%	2.9%	2.9%	3.0%	3.0%
32,000,000	2.1%	2.3%	2.4%	2.5%	2.7%	2.7%	2.8%	2.8%	2.9%	2.9%
40,000,000	1.9%	2.0%	2.1%	2.3%	2.4%	2.4%	2.5%	2.5%	2.6%	2.6%
50,000,000	1.7%	1.8%	1.9%	2.0%	2.1%	2.2%	2.2%	2.3%	2.3%	2.4%
60,000,000	1.5%	1.6%	1.7%	1.8%	1.9%	2.0%	2.0%	2.1%	2.1%	2.1%
70,000,000	1.4%	1.5%	1.6%	1.7%	1.8%	1.8%	1.9%	1.9%	2.0%	2.0%
80,000,000	1.3%	1.4%	1.5%	1.6%	1.7%	1.7%	1.8%	1.8%	1.8%	1.9%
90,000,000	1.3%	1.3%	1.4%	1.5%	1.6%	1.6%	1.7%	1.7%	1.7%	1.8%
100,000,000	1.2%	1.3%	1.4%	1.4%	1.5%	1.5%	1.6%	1.6%	1.6%	1.7%
110,000,000	1.1%	1.2%	1.3%	1.4%	1.4%	1.5%	1.5%	1.5%	1.6%	1.6%

Source: Consensys

More holistically, PoS will make ETH a significantly more productive asset than it was under PoW. On the current PoW chain ETH possesses store of value and commodity properties from its use as money and gas. On the new Beacon Chain, ETH will also possess capital asset properties from its use in PoS. Recall that validators are required to stake 32 ETH as collateral to register their node on the network in order to participate in consensus. In this capacity ETH will function as a type of hybrid-perpetual bond with debt and equity like characteristics.[71] In return for behaving honestly and securing the Ethereum blockchain, stakers will be rewarded a perpetual, though variable, ETH-denominated yield derived from new issuance and transaction fees. New issuance would be paid by Ethereum itself, while transaction fees would be paid by users. Although it is important to note that the payout of this yield will be deferred until the Phase 1.5 ETH 1.x merger, when stakers will finally be able to withdraw their deposits and claim their rewards. Additionally, until Phase 1.5, that yield will only come from new issuance, not transaction fees.

INSIGHTS FROM BISON TRAILS

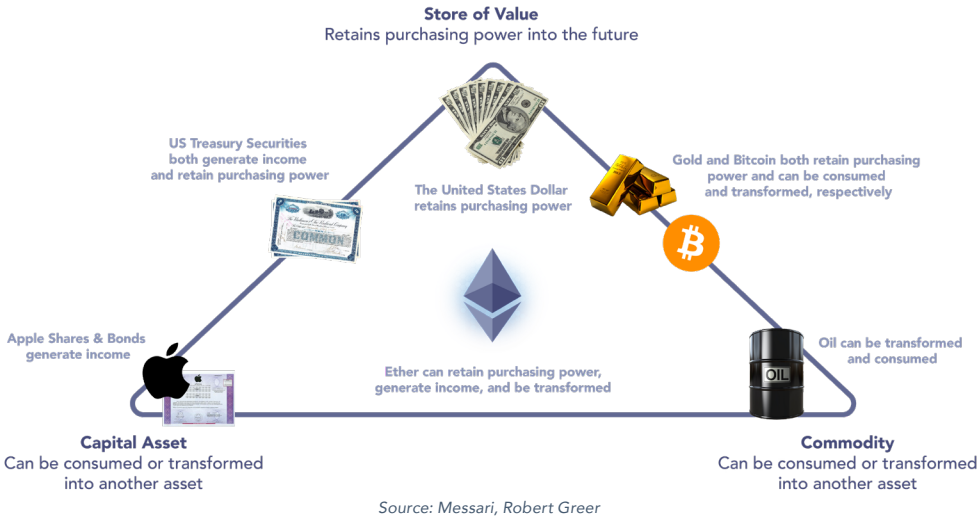
Average validator uptime is a crucial metric because it impacts rewards and penalties. It can trigger the inactivity leak to help the network find finality. It also serves as an anti-DDoS mechanism to disincentivize validators from knocking other validators offline, as doing so will also decrease the average reward rate experienced by the online validators.

The combination of the three properties will provide ETH with a unique combination of asset class properties.[72]

MESSARI

Asset Superclass Triangle

All assets can be grouped into three classes: capital assets, commodities, and stores of value.
Ether may be the first member of all three classes, ever.



Source: Messari, Robert Greer

[71]Colin Myers and Mara Schmiedt, "The Internet Bond: Digital Work Agreements in the Web3.0 Era" Aug. 2020 • [72]Chris Burniske and Adam White, "Bitcoin: Ringing the Bell For a New Asset Class" ARK Invest, Jan. 16, 2017

In ETH 2.0, ETH will be both the most integral and productive asset in Ethereum's economy. In ETH 2.0 ETH can be:

- Staked to produce yield for securing Ethereum
- Transformed into blockspace through transaction fees (an especially direct relationship when EIP 1559 is implemented and the majority of transaction fees are burned)
- Stored and transferred as Ethereum's native (and thus most trust minimized) store of value asset

The combination of the three may create a constant tug of war for ETH demanded by each use case. This will be especially apparent until Phase 1.5 considering that ETH deposited to stake will be locked, creating a temporary supply sink.

STAKING ILLIQUIDITY AND STAKING DERIVATIVES

As discussed in the overview section, becoming a validator in ETH 2.0 requires sending at least 32 ETH to the deposit contract on the ETH 1.x chain. This transaction is a one way transfer with the deposited ETH being locked up until Phase 1.5 when the ETH 1.x chain merges into ETH 2.0 as a shard. While estimates are that Phase 1.5 may be anywhere from 18 - 36 months out, practically speaking, stakers will have their ETH locked up indefinitely as they await Phase 1.5 to come. As a result stakers face a significant opportunity cost locking up their ETH for this period.

Recognizing the illiquidity and opportunity costs stakers face, multiple solutions have emerged that will allow stakers to gain liquidity and capital efficiency on their staked ETH. Secured lending solutions have emerged that allow stakers to borrow against their staked ETH positions, such as Liquid Stake which allows stakers to borrow USDC against their ETH if they deposit through Liquid Stake.[73] More broadly a variety of firms and protocols have emerged that may allow users to securitize their staked ETH for liquidity. These ETH derivatives ("DETH" - it's not as scary as it sounds), will have a claim on the underlying staked ETH, and allow stakers to gain additional productivity on their assets. DETH could be issued by exchanges and staking pools and will allow stakers to rehypothecate their staked ETH for additional use in DeFi.

Yet, not all DETH will be made equal. Each organization that creates DETH may differ in validator uptimes, security practices, and trustworthiness that will determine underlying rewards, penalties, and custodial risks.[74] As a result users may prefer to use a handful of solutions over others. Further making this scenario likely are secondary market liquidity

[73]Andrey Shevchenko, "**LiquidStake set to unlock liquidity for ETH 2.0 Phase 0 stakers**" CoinTelegraph, Nov. 11, 2020 • [74]"**Liquid Staking Research Report**" ChorusOne, Jun. 2020

considerations. Liquidity has strong network effects, and if the fiat-backed stablecoins are any indicator of what's to come, the market may likely settle upon a couple of DETH solutions.[75] Exchanges are particularly well positioned for this market as they are already among the largest holders of ETH and issuers of wrapped assets. Exchanges are fundamentally in the game of capital aggregation and already are racing to offer ancillary services outside of trading in pursuit of this end goal.[76] There's little doubt they will jump at this opportunity.

But it's not just centralized providers jumping at the opportunity - which is a good thing because staking concentration with centralized providers could threaten Ethereum's PoS security. Decentralized solutions such as Rocket Pool and StaFi will create two sided marketplaces for staking that will match stakers and validators. These protocols will allow users to pool their ETH together to stake, then allocate that pooled ETH to validators to stake. The value proposition for stakers is reducing the 32 ETH barrier to entry, outsourcing infrastructure requirements, gaining liquidity on their stake, and supporting the decentralization of Ethereum. The value proposition for validators is the ability to scale their operations without needing to purchase their own ETH for each validator they run.

These decentralized staking solutions will also create a flavor of DETH that will depend not on the validator uptimes, security practices, and trustworthiness of a single provider, rather the validator uptimes, security practices, and trustworthiness of a pool of providers, which diversifies the risk. This flavor of DETH would resemble securitized products like mortgage-backed securities. Just like mortgage-backed securities (MBS) represent the value of an aggregation of many loans, staking derivatives pool staking positions into a single package and then tokenizes them.[77]

MESSARI

Decentralized Staking Protocols as Investment Banks

Decentralized staking protocols pool staking positions into a single package then tokenizes them - resembling the securitization process for MBS.

Note: "DETH" is short for "Staked Ethereum Derivative" • Source: Messari

[75]Dan Elitzer, "**The DETH of Ethereum**" Medium, Dec. 12, 2020 • [76]Kyle Samani, "**Exchanges are Open Finance**" Multicoin Capital, Oct. 29, 2020 • [77]Alex Evans and Tarun Chitra, "**What PoS and DeFi can learn from mortgage-backed securities**" Medium, Nov.15, 2020

With how large the addressable market will be for these ETH staking derivatives, there will be many additional financial services built atop them. Not only will DETH products be available for use in many existing DeFi protocols, but DETH products could be further packaged into ETF-like index products, swap products that allow stakers to fix their yield and traders to speculate on yield, and other structured products (such as combining DETH with put options on the underlying token to create fixed income products).[78] The design space is wide open in this respect and may even introduce unforeseen behaviors into staking.

It is also important to caveat that while these protocols may decentralize validator infrastructure for users, they still carry custodial risk. RocketPool for example, as designed currently, will be custodial until after Phase 1.5. However, the team is working on a solution alongside the Ethereum Foundation to enable trust minimized withdrawals, which would remove this custodial risk.

The ETH derivatives space as a whole is understandably still very early, but should play a much larger role following the launch of the Beacon Chain.

MONETARY POLICY IMPLICATIONS FOR ETH

As discussed in the overview, validators will be rewarded newly issued ETH for performing their duties adequately, and the amount of rewards validators will be issued overall will be proportional to how much ETH is staked. Until Phase 1.5 when ETH 1.x is merged into ETH 2.0 as a shard chain (estimated 2022), issuance from the Beacon Chain will be incremental to issuance from ETH 1.x. The result is that overall issuance for Ethereum will increase slightly once the Beacon Chain launches.

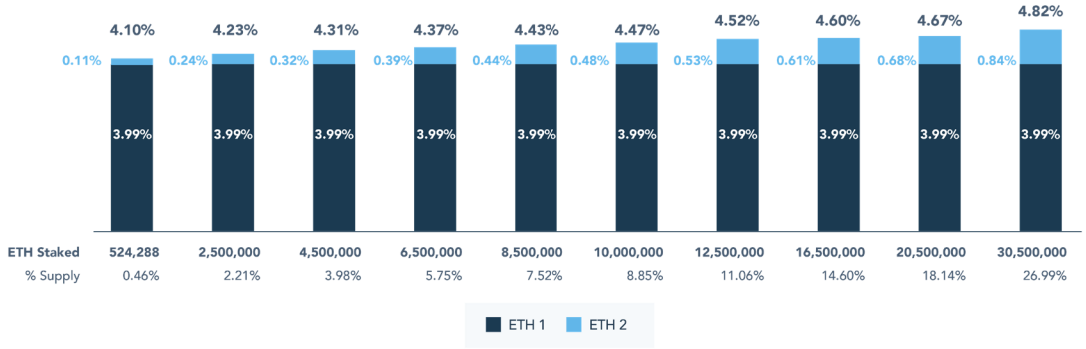
However, this incremental issuance from the Beacon Chain will more than likely be de minimis, and will not decidedly impact ETH's properties as a store of value - especially considering it's just temporary. Even under extremely aggressive staking participation rate assumptions for this period leading up to Phase 1.5 (30.5 million ETH) incremental issuance may only reach as high at 0.84% per year. To put that in perspective, ConsenSys' target staking participation rate for Phases 1+ that will achieve the same level of security as the ETH 1.x chain will be ~16 million ETH.[79]

[78]"**Liquid Staking Research Report**" ChorusOne, Jun. 2020 • [79]Tanner Hoban and Thomas Borgers, "**Ethereum 2.0 Economic Review**" ConsenSys, Jul. 16, 2020

MESSARI

Ethereum Annual Issuance Rate until Phase 1.5 ETH 1 Merge

Assuming 100% validator uptime, Ethereum's total issuance will only be affected marginally, even with high staking participation.



Note: Assumes starting supply of 113,000,000 ETH. Also assumes flat participation for each column shown. • Source: Messari, Consensys

Further reducing the potential issuance of ETH 2.0 until Phase 1.5 are the likely shape of the staking adoption curve, validator performance, and transaction fee burns (EIP 1559). Staking participation will likely start low and increase over time as holders gradually become more comfortable with the Beacon Chain and deposit more ETH into the deposit contract. What this means is that issuance could be extremely low in the early months following the Beacon Chain launch before reaching their theoretical maximums outlined in the above chart. Validator performance will affect issuance given that for every 1% of validators offline, total issuance will be cut by ~3%. And if more than 33% of validators go offline at once, this will lead to finality leaking which will incur extra penalties for offline validators.[80] Finally, EIP 1559, a proposal to restructure how users bid for Ethereum blockspace that will burn ETH transaction fees, may reduce issuance for ETH 1.x when implemented, which will offset the incremental issuance from the Beacon Chain. The result of these three factors is that net issuance from ETH 2.0 could be significantly lower than what's projected on the above chart.

ROLLUP-CENTRIC ETHEREUM VS LAYER 1 COMPETITORS

Phase 0 is for stakers and little else. Its whole purpose is to bootstrap network security and test ETH 2.0's consensus model in a live environment. Both are critical steps for ensuring the network's sustainability, but outside of producing new blocks and earning rewards, Phase 0's functionality will be almost non-existent.

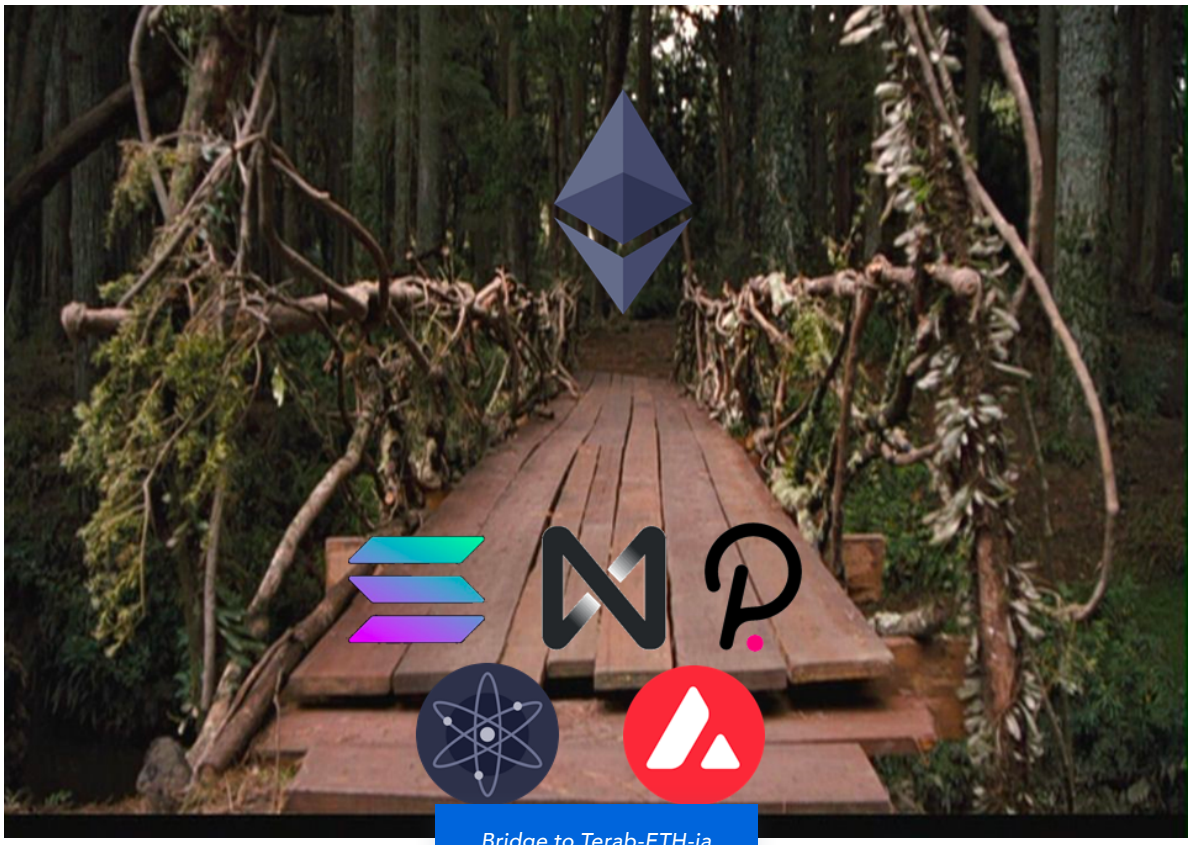
With basic transaction functionality 1-2 years away, ETH 2.0 can't be a near-term scaling solution for the current network. This gap between now and more feature-rich stages puts Ethereum in

[80]Eric Conner, "**Monetary Policy**" EthHub

precarious position while presenting its low-fee, low-latency competitors with an opportunity to eat into Ethereum's monopoly on smart contract developers and DeFi applications.

Most new Layer-1s have built their platforms partially based on the premise that developers and new retail users will grow tired of Ethereum's unpredictable and, at times, unforgiving fee market. Their strategy is not wrong. Many users and developers are still reeling from the profit-sucking ETH fees they paid during the DeFi bull market this summer. Those impacted by unrelenting high costs will inevitably explore alternative platforms with better transaction throughput and lower fees if they aren't already.

It's easy to write off these new networks, as they are miles behind Ethereum in terms of developer firepower, financial middleware, and tradeable tokens. But the competition in this market is just getting started. Nearly every high-profile Ethereum competitor has launched or will launch by the end of 2020, and most are closer to maturity than ETH 2.0 is to reaching subsequent phases. Several new networks are also nearing completion on bridges to Ethereum (Near's Rainbow Bridge, Cosmos' Peggy, or Solana's Wormhole) or EVM-compatible chains (Avalanche's Athereum or Polkadot's Moonbeam) that offer familiar development environments for Ethereum applications and minimal switching costs.



Bridge to Terab-ETH-ia

Ethereum developers recognize the current need for scalability, which is why they have been strong advocates of Layer-2 scaling technology. In general, these second layer solutions facilitate transactions through off-chain means before bundling and submitting them as a single transaction to the base layer. By batching transactions, Layer-1s can significantly improve the number of transactions they process per block while theoretically providing similar security guarantees upon settlement. Off-chain transactions also don't bog down the underlying network with excess data and computing requests.

Of all the proposed Layer-2 technologies, rollups have quickly become the go-to scaling solution due to their ability to run smart contracts.[81] They provide a more complete solution than Plasma chains or state channels, which can't support application development, and better security assumptions than sidechains, which often rely on independent consensus mechanisms. With their rise in popularity, there's now a burgeoning ecosystem of various rollup flavors, from Optimism's Optimistic Ethereum to Matter Labs' zkSync.[82] Each comes with a different set of advantages and trust assumptions that will likely cater to different use cases.

Rollups present the most promising case for scaling Ethereum in the near and mid-term future. They also give Ethereum a path to scalability that rivals the timeline of new Layer-1s reaching maturity. Ethereum competitors aren't racing to beat ETH 2.0; they're in a much tighter race against a viable rollup solution.

Rollups are still a few months away from reaching a production-ready stage. Optimism's OVM and Offchain Labs' Arbitrum recently released public testnets and both expect to launch on mainnet in near feature. But they are already starting to see the benefits from their close ties with the Ethereum community, where members tend to support their own. DeFi darling Synthetix deployed the first application on Optimism's public testnet[83], and some suspect Uniswap will follow suit.

It is likely that big name DeFi apps won't stray too far from Ethereum and will end up on some version of a rollup, if they move from the base layer at all. Ethereum competitors may not receive the same treatment despite offering similar technical advantages. On a level playing field, community sentiment and financial incentives will be the deciding factor.

There's still ample opportunity outside of Ethereum, and new Layer-1s can stand out by targeting niche sectors (think Flow and gaming) and bringing radically different designs to the table (the unparalleled flexibility afforded by modular frameworks like Polkadot and Cosmos). As for which approach will prevail, only time will tell. But if rollups pan out, Ethereum should be able to maintain its virtual monopoly on DeFi applications while ETH 2.0 remains in an incubation stage.

[81]Vitalik Buterin, "**A rollup-centric ethereum roadmap**" Fellowship of Ethereum Magicians, Oct. 2, 2020 • [82]Daniel Goldman, "**The State of Optimistic Rollup**" Medium, Feb. 20, 2020 • [83]Ethereum Optimism, "**Light at the end of the tunnel**" Medium, Sep. 24, 2020

ROLLUP-CENTRIC ETHEREUM IMPLICATIONS FOR APPLICATIONS

As discussed in the above section on rollups vs. other Layer-1 networks, ETH 2.0's lengthy roadmap will likely lead the community to rely on rollups as a near-term scaling strategy. Rollups won't only have implications for the Layer-1 platform race, they'll also be central to how applications determine their product strategy going forward.

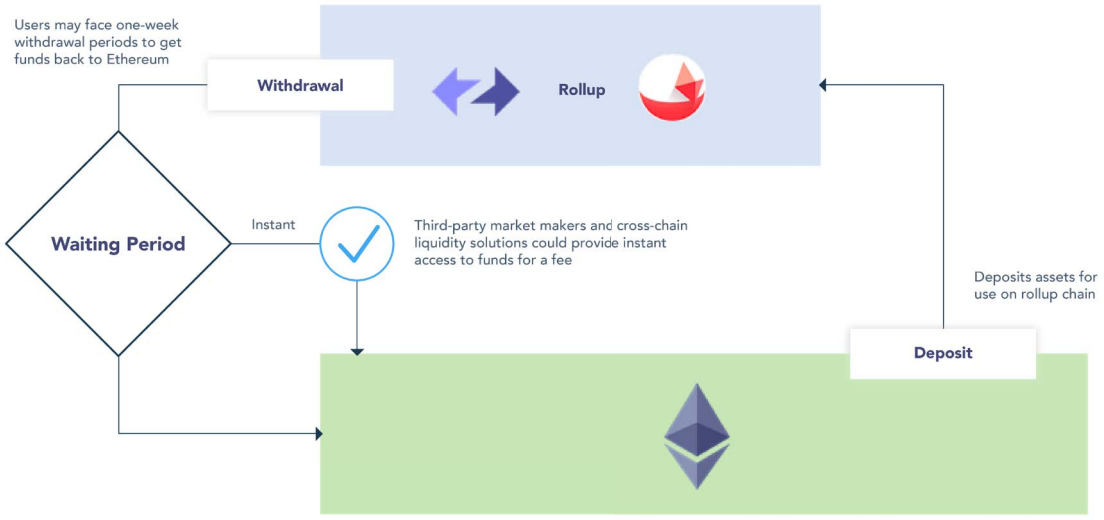
From a developer's perspective, the cost of moving to a rollup is minimal. A rollup like the one Optimism is building will be able to support near-replicas of a protocol's existing contracts. These new contracts can run parallel to their mainnet counterparts, which enables applications to keep their current user base and liquidity while simultaneously offering a low-fee option.[84]

Despite the relatively low barrier to entry, rollups come with a few tradeoffs. First, users face a lengthy wait of up to one week when looking to withdraw from a rollup back to the base layer.[85] This temporary lockup enables onlookers to challenge the validity of transactions packed into each fraud proof. It's an important security measure, but the opportunity cost of waiting for the network to confirm withdrawal transactions might lead some users to avoid rollups altogether.

MESSARI

Rollup Overview

Rollups can only facilitate cross-chain transactions on an asynchronous basis.



Source: Messari, Daniel Goldman

[84]Daniel Goldman, "**When DeFi meets Rollup**" Bankless, Apr. 16, 2020 • [85]Alex Gluchowski, "**Evaluating Ethereum L2 Scaling Solutions: A Comparison Framework**" Medium, Jun. 12, 2020

Second, rollups can only facilitate cross-chain transactions on an asynchronous basis (as in not in the same block), which breaks the composability standards that have enabled Ethereum's DeFi sector to flourish. Composability is the core attribute that allows smart contracts to easily reference each other and unlocks the ability to create more complex products like flash loans. Rollups don't pose any restrictions on intra-rollup composability, but if previously interconnected applications end up on different rollups, their contracts won't be able to call on each other in a timely manner. In the world of crypto finance, latency is already an issue and any transaction restrictions (like withdrawal periods) could be a deal breaker.

Neither challenge is insurmountable. Third-party market makers can accelerate the rollup withdrawal period by providing instant access to locked funds for a fee. As Nic Carter suggests, this proposed solution would create "a tiered system, with lengthier finality from the "free version" of a Rollup exit, and shorter finality in the paid, accelerated version."[86] It also has the unintended consequence of turning these intermediary marker makers into the gatekeepers of rollup systems. A more crypto-friendly but potentially complex solution would be to use cross-chain liquidity networks like THORChain to bridge Layer-1 and Layer-2 liquidity. These networks introduce a new set of security assumptions, and most are still in the development stage. However, their use could circumvent rollup withdrawal and composability restrictions without relying on a single intermediary.

For the foreseeable future, rollups will be isolated hubs of composable activity with cross-rollup activity only happening on an asynchronous basis. The result of this, combined with the fact that many rollup solutions are just now launching, means that the first protocols to move to rollups may have significant competitive advantages over ones that don't. Furthermore, ones that move to the same rollup in some sense are effectively forming partnerships to maintain composability in this more scalable environment, which could lead to synergies between such cooperating protocols.[87]

Ethereum may look very different a year from now. There could be one giant rollup that hosts all of the composability-reliant DeFi protocols (albeit at the expense of some scalability gains), while several others are more application specific and cater use cases like gaming, NFTs, or order book DEXs.[88] The rate at which Ethereum transitions to this rollup centered framework depends on when (or if) the foundational DeFi building blocks like Uniswap or Compound make a move. Once these major protocols go, the rest are likely to follow.

[86]Nic Carter, "**Public blockchain fee cyclicality and negative feedback loops**" Medium, Oct. 5, 2020 • [87]Ryan Watkins, "**DeFi Citadels: How DeFi Protocols Create and Capture Value**" Messari, Oct. 27, 2020 • [88]Daniel Goldman, "**When DeFi meets Rollup**" Bankless, Apr. 16, 2020

CLIENT DIVERSITY

A blockchain client is any node on a network that can parse and verify block data. Every network relies on clients to provide a gateway into the blockchain, enabling users to submit transactions and produce new blocks. Since public blockchains are open source by design, any developer can create a new version of a client in the programming language of their choice.

Most chains rely heavily on a single client implementation, with the most prominent example being Bitcoin Core's 98% network share over other Bitcoin clients.[89] Ethereum strives to eliminate this concentration. The community advocates for greater client diversity to prevent a single version from commanding a majority share of the market. This multi-client approach can increase the probability of cross-client consensus discrepancies (which leads to inadvertent yet costly forks). But it presents some clear advantages in terms of security and decentralization.

An attack that targets a chain's top client will cripple a network dominated by a single implementation (a point of centralization), whereas a multi-client chain can fall back on its remaining implementations to avoid a stoppage in block production. This resiliency was on display back in 2016 when a series of DoS (Denial of Service) attacks brought down Ethereum's Geth and Parity clients at separate intervals. Ethereum suffered some momentary congestion but never stopped producing blocks since the attacks didn't impact both clients at the same time.

Beyond resiliency, the multi-client approach can attract a more diverse set of ideas, algorithms, and even user bases because each client team has different perspectives and design goals. These outcomes feed into Ethereum's penchant for evolution and continuous improvement over absolute stability and ossification. Clients written in Python, Go, or Java (among others) also open the doors to those respective programming language communities, which can "snowball" into a robust ecosystem of tools and contributors that span multiple languages. As Danny Ryan pointed out, "the multi-client paradigm reinforces the gravitational well that is Ethereum."[90]

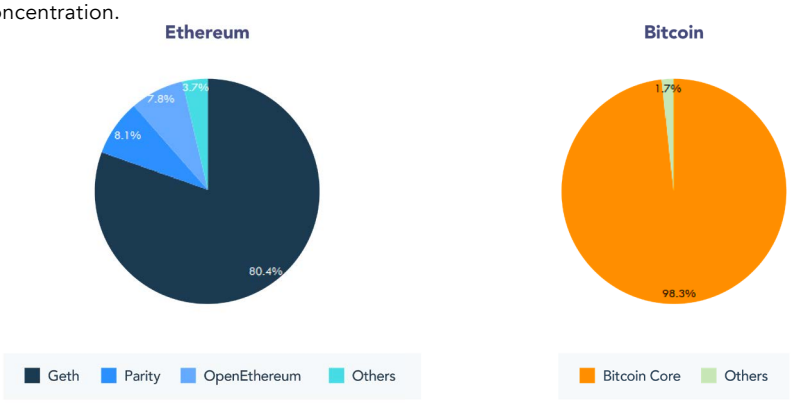
At the moment, client distribution on the existing Ethereum network is unhealthy. Over 80% of active nodes are running Geth.[91] Some developers attribute Geth's current dominance to its first mover advantage, which may have led the Ethereum Foundation to support a wide variety of ETH 2.0 client teams early on to avoid a similar scenario.

[89]"**Bitcoin Nodes Summary**" Coin Dance, Nov. 13, 2020 • [90]Danny Ryan, "**The State of Eth2, June 2020**" Ethereum Foundation, Jun. 2, 2020 • [91]"**Ethereum Mainnet Statistics**" Ethernodes, Nov. 14, 2020

MESSARI

Client Diversity

Most chains including Ethereum rely heavily on a single client implementation. Ethereum 2.0 strives to eliminate this concentration.



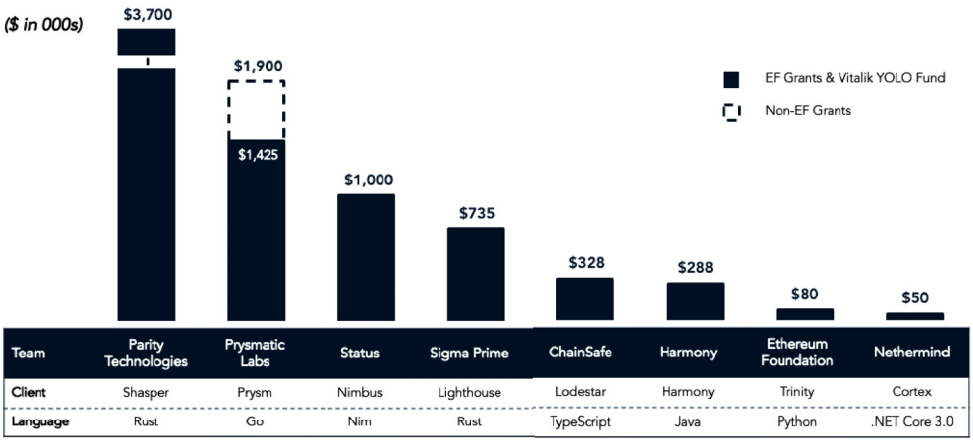
Source: Coin Dance, ethermodes

Since the start of 2018, the Ethereum Foundation has issued or co-funded over $7.6 million in grants to eight different ETH 2.0 clients teams, a total that is likely much higher when accounting for other undisclosed grant amounts. Various Ethereum Foundation members have also contributed to client teams, including Vitalik Buterin unexpectedly giving 1,000 ETH each to Prysmatic Labs, Sigma Prime, and ChainSafe in December 2018.[92] A ninth client, Teku, is being developed by ConsenSys subsidiary PegaSys.

MESSARI

Grant funding received by Ethereum 2.0 client teams

The Thereum Foundation has granted over $7.6 million (and likely much more) into ETH 2.0 client teams since 2018.



Team	Parity Technologies	Prysmatic Labs	Status	Sigma Prime	ChainSafe	Harmony	Ethereum Foundation	Nethermind
Client	Shasper	Prysm	Nimbus	Lighthouse	Lodestar	Harmony	Trinity	Cortex
Language	Rust	Go	Nim	Rust	TypeScript	Java	Python	.NET Core 3.0

Note: Parity received a $5M grant but suspended payments in Dec 2019 when it redirected all operations to Polkadot development. • *Source: Ethereum Foundation, EthHub*

The grant spree has paid off. There are four viable clients that are ready for the Beacon Chain's launch (Prysm, Teku, Lighthouse, and Nimbus), a respectable turnout as some teams have expectedly underdelivered or discontinued development efforts. However, client

[92]Vitalik Buterin, Twitter, Dec. 18, 2018

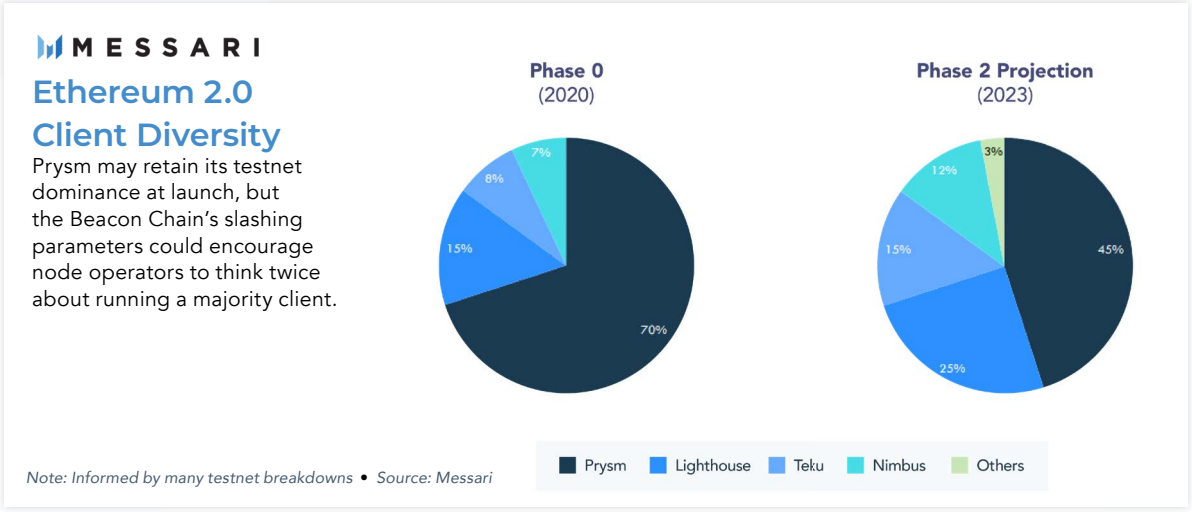
distribution on the Phase 0 multi-client testnets was still top heavy, with 65-80% of the network running on Prysm at various times.[93] It begs the question whether a true multi-client setup with equitable distribution is realistic or if one client will always instill more confidence in node operators and become the default option.

INSIGHTS FROM BISON TRAILS

A validator in eth2 Phase 0 gets rewarded for keeping good uptime and getting votes included as fast as possible. In order to see more client diversity, the protocol could reward more types of positive behavior, such as the efficient aggregation of attestation.

Ethereum is not going down without a fight and has carried its "solve scalability and consensus or die trying" mindsight into its quest for client diversity. Part of the community's strategy has been encouraging a network-first ideology. Danny Ryan didn't mince words when he said "if there is more than one viable and secure client, it is an [operator's] duty to run minority client software to promote a healthy" network.[94] ETH 2.0 developers have also built the Beacon Chain to disincentivize running a majority client. Inactivity penalties and slashing rates ramp up if more nodes get slashed or knocked offline at the same time. A critical mistake or bug in a majority client almost guarantees that those validators will lose a portion (or in extreme cases, all) of their security deposit, while validators running alternative client software will remain largely unscathed.[95]

There's a good chance that Prysm retains its Beacon Chain dominance at launch. Prysm has a strong team backing it in Prysmatic Labs, and it doesn't hurt that they have received more grant funding than any other active ETH 2.0 client team. But the Beacon Chain's slashing parameters could encourage node operators to think twice about running a majority client. Additional initiatives, such as a cross-client standard for easily porting between client types without losing all of any data, could further enhance client diversity over time.

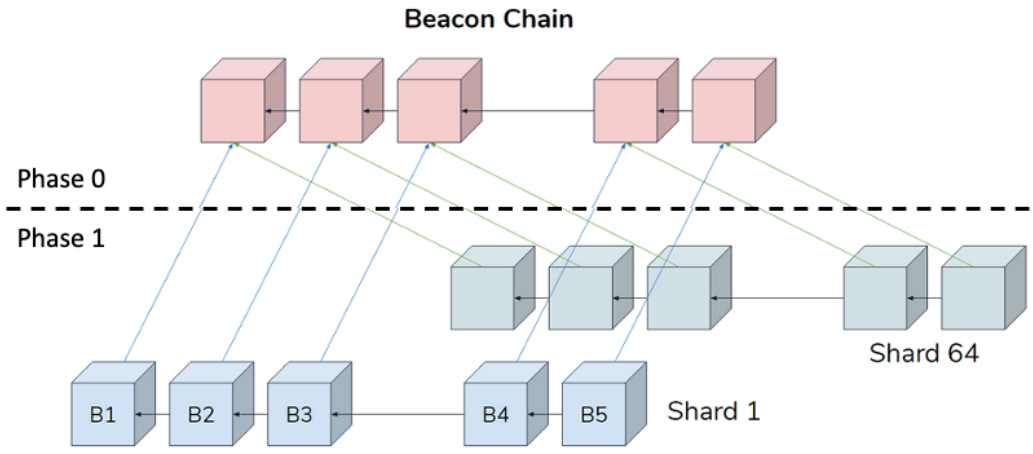


[93]Raul Jordan, "Eth2 Medalla Testnet Incident" Medium, Aug. 18, 2020 • [94]Danny Ryan, "The State of Eth2, June 2020" Ethereum Foundation, Jun. 2, 2020 • [95]Carl Beekhuizen, "Validated, staking on eth2: #5 - Why client diversity matters" Ethereum Foundation, Aug. 21, 2020

Phase 1 & 1.5

PHASE 1 OVERVIEW

While Phase 0 is all about staking and fortifying the foundation of ETH 2.0, Phase 1 will unveil the network's long-term scaling solution: sharding. Sharding involves splitting a blockchain into smaller, identical pieces, called shards, which each contain a subset of a blockchain's nodes. A blockchain can then spread processing capacity across these parallel shards to increase the system's overall transaction throughput, avoiding the need for each node to process and store every on-chain interaction. Phase 1 will introduce 64 of these shards, essentially scaling the throughput capacity of ETH 2.0 64x beyond what is possible on the Ethereum's current PoW chain. Yet, despite the added feature, ETH 2.0 node operator costs should remain relatively low since nodes will process only a subset of the network's total activity at a given time.



Source: Hsiao-Wei Wang

Phase 1 is simply the marriage of ETH 2.0's primary objectives, staking and sharding. It involves extending ETH 2.0's PoS consensus logic across these 64 new shard chains. Each shard will anchor into the Beacon Chain, where Beacon Chain validators will take turns creating and validating new shard blocks before linking them to the rest of the network.

Like the Beacon Chain in Phase 0, shards in Phase 1 won't have the ability to process transactions or support smart contracts - although they will be able to serve as data storage layers for rollups, as discussed in the rollup-centric Ethereum section below. But their limited feature set will prevent the consensus process from becoming overly complex. From

this perspective, Phase 1 is simply an extension of Phase 0 as it's also all about coming to consensus, although with 64 additional moving parts.[96]

ETH 2.0's consensus process will essentially remain the same between Phase 0 and Phase 1, but there will be some slight differences to account for shard security and linking shard blocks to the Beacon Chain.

First, the use of RANDAO to pseudorandomly assign block proposers and attesters will become even more essential to the security of the system. Each ETH 2.0 slot will now be an opportunity to add one Beacon Chain block and 64 different shard blocks to the network. Reaching a consensus on up to 65 blocks in a timely manner is a massive coordination effort that requires the network to spread validators across all 65 chains. By breaking validation responsibilities into smaller groups, ETH 2.0 could potentially increase the chance a staker (or group of stakers) with multiple validators could gain a majority share of influence over an individual shard and mount an attack.

However, RANDAO aims to eliminate this risk as it randomly shuffles the validator committees assigned to each shard every block. According to Joseph Chow, RANDAO's per block pseudorandom selection process makes it "mathematically improbable that an attack controlling less than one-third of all validators can attack a single shard."[97] In short, only a validator with greater than a 33% share of all network stake can pose a threat to the network, but even then, the chance of being able to execute an attack is minute.

The second slight difference in Phase 1 consensus is the addition of crosslinks. A crosslink is a reference between the Beacon Chain and a shard. It allows Beacon Chain validators to "learn about" and determine the head of referenced shards (differentiate between the "true" chain and forks) without having to store each chain's entire state.[98] Validator committees are responsible for voting on and forming these cross-chain bonds. Therefore, an ETH 2.0 slot can also represent an opportunity to add a block and 64 crosslinks to the Beacon Chain. Once linked to the Beacon Chain, shards follow the same fork choice and chain finality rules established in Phase 0.

Crosslinks also enable shards to communicate with other chains in the system. Any communication between different shards occurs on an asynchronous basis, meaning that cross-shard transactions don't happen all at once (essentially, in the same block). Since synchronous transactions are the foundation of smart contract composability on Ethereum, several developer teams are researching how to bring synchronicity to cross-shard transactions on ETH 2.0.[99]

[96]Danny Ryan, "**The State of Eth2, June 2020**" Ethereum Foundation, Jun. 2, 2020 • [97]Joseph Chow, "**The Beacon Chain Ethereum 2.0 explainer you need to read first**" Ethos Dev, May. 23, 2020 • [98]Eric Conner, "**Ethereum 2.0 Phases**" EthHub • [99]Eric Conner, "**Ethereum 2.0 Phases**" EthHub

Phase 1 may also introduce an amended version of EIP 1559 - a proposal to restructure how users bid for blockspace that will improve UX and burn a large portion of ETH transaction fees - to ETH 2.0. EIP 1559 could significantly lower Ethereum's net issuance, as discussed in the section on Monetary Policy Implications for ETH below. Since the Beacon Chain and its data shards won't support transactions until Phase 1.5, ETH 2.0 won't have any need for this new fee market during Phase 1. But its introduction in Phase 1 sets the foundation for complimentary fee markets between ETH 1.x and ETH 2.0 once the two merge in the following phase.[100]

PHASE 1.5 OVERVIEW

ETH 1.x and ETH 2.0 will exist as separate chains likely for the duration of Serenity's first two phases. This separation enables ETH 2.0 to evolve and resolve any issues without disturbing the applications and assets running on the current network. But eventually, these applications and tokens must find their way over to the new network for Ethereum to achieve its scalability goals and permanently move on from PoW. Determining the optimal route for merging Ethereum into a single, unified network is the basis of Phase 1.5.

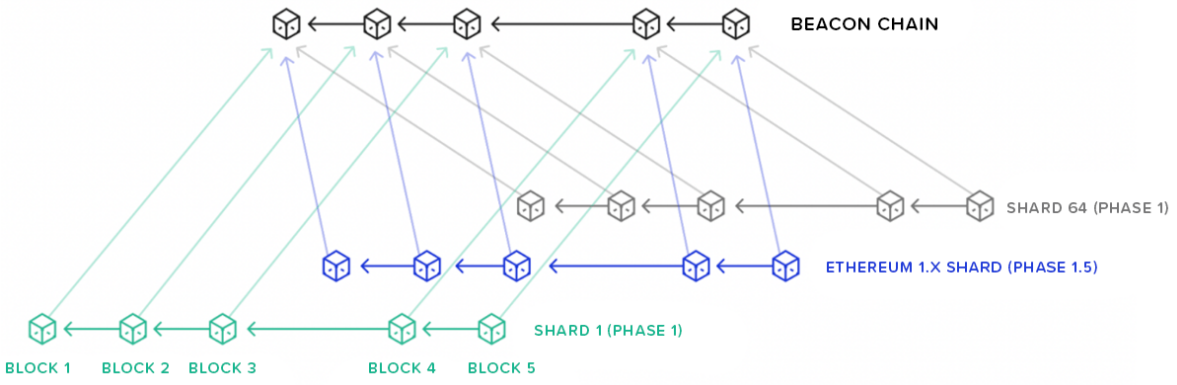
The integration of ETH 1.x into ETH 2.0 comes with two important implications. First, it officially marks the end of PoW and the point at which ETH 2.0 becomes Ethereum.[101] From Phase 1.5 on, Ethereum will only use PoS to generate new blocks and validate transactions. The old PoW chain will continue to exist after the merge, but it will have a temporary lifespan since Ethereum developers have encoded a function (called the difficulty bomb) that will make mining permanently impractical at a future block height. Second, Phase 1.5 realigns Ethereum as a single network with one native token, which will allow the Beacon Chain and shards to safely unlock transactions. Once transactions are live, Beacon Chain validators will be able to withdraw their staking deposits and rewards for the first time.

INSIGHTS FROM BISON TRAILS

Some believe the merge will be contentious, or that miners will continue the proof of work Ethereum chain post-merge, treating it like a fork. But given that the merge is unlikely until there is sufficient community buy-in and rough consensus, we believe these fears are wildly overblown.

Research discussions on how to merge Ethereum old and new have zeroed in on integrating ETH 1.x as a shard within the ETH 2.0 system, as first outlined by Vitalik in October 2019. He later simplified this plan in December 2019 to potentially accelerate the development cycle. Since this proposal came after ETH 2.0 had a familiar roadmap, the Ethereum community has aptly named it Phase 1.5.

[100]Danny Ryan, "**Ethereum Foundation ETH 2.0 Research Team AMA (Pt. 5)**" Reddit, Nov. 18, 2020 • [101]Danny Ryan, "**The State of Eth2, June 2020**" Ethereum Foundation, Jun. 2, 2020



Source: Bison Trails

At a high level, Vitalik's latest scheme involves swapping Ethereum's consensus layer from PoW to PoS, while keeping the execution layer (app layer) intact. This transition might require some heavy lifting at the protocol layer to get ETH 1.x and ETH 2.0 clients to coordinate state execution and block production responsibilities, respectively.[102] But at the surface, it should look similar to previous Ethereum upgrades.[103] This approach should remove the need to actively migrate any assets or code, making the transition almost seamless from a developer and user perspective.

Phase 1.5 is still in the research and development stage, and its roadmap is subject to change. But Vitalik recently indicated that this phase could have a more aggressive development timeline. For instance, ETH 2.0 teams could try to run ETH 1.x transactions on the Beacon Chain rather than waiting for Phase 1 to integrate them into a shard. There's also a push to build an ETH 2.0 "light client" - software that connects to full nodes to interact with a blockchain - inside of ETH 1.x, which would give the Beacon Chain the ability to interact with the current Ethereum network. According to Vitalik, if these experiments prove successful, there's a chance the ETH 1.x and ETH 2.0 merge could happen before Phase 1.[104] While it is an optimistic suggestion, the fact ETH 2.0's core features are being developed in parallel might mean the rollout of different phases is more fluid than initially anticipated.

Phase 1.5 could also become the final scheduled upgrade on ETH 2.0's roadmap due to the recent rise of rollups, as discussed in the Rollup-centric Ethereum section below. Vitalik and others have surmised that rollups layered on top of Phase 1 shards could provide a suitable long-term scaling solution well before Phase 2 arrives. In response, ETH 2.0 research teams have de-emphasized their work on Phase 2 because this final phase might be unnecessary given the potential lack of demand. Despite the shift in focus, Phase 2 is still on the roadmap, but there's a possibility Ethereum eventually accepts a "phase 1.5 and done" approach.[105]

[102]Danny Ryan, "**Eth1+eth2 client relationship**" EthResearch, Apr. 7, 2020 • [103]Vitalik Buterin, "**The eth1 -> eth2 transition**" EthResearch, Oct. 9, 2019 • [104]Vitalik Buterin, "**Ethereum Foundation ETH 2.0 Research Team AMA (Pt. 5)**" Reddit, Nov. 18, 2020 • [105]Vitalik Buterin, "**A rollup-centric ethereum roadmap**" Ethereum Magicians, Oct. 2, 2020

MONETARY POLICY IMPLICATIONS FOR ETH

As detailed in the Phase 0 section, issuance from the Beacon Chain will be incremental to issuance from ETH 1.x. This will cause overall ETH issuance to increase slightly until Phase 1.5 when ETH 1.x is merged into ETH 2.0 as a shard chain. However, when the merger is complete, the once incremental issuance from ETH 2.0 will become the only issuance for Ethereum, and it is very likely Ethereum's annual issuance rate will be well below 1%. Assuming ConsenSys's target staking participation number of ~16 million ETH and 100% validator uptime, Ethereum's annual issuance rate would be 0.6%.

MESSARI

Ethereum 2.0 Annual Issuance

NETWORK ISSUANCE — Average Network % Online

Total ETH Staked (Network)

	70%	75%	80%	85%	90%	92%	94%	96%	98%	100%
524,288	0.0%	0.0%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%
2,000,000	0.1%	0.1%	0.1%	0.1%	0.2%	0.2%	0.2%	0.2%	0.2%	0.2%
4,000,000	0.1%	0.1%	0.1%	0.2%	0.2%	0.2%	0.2%	0.3%	0.3%	0.3%
6,000,000	0.1%	0.1%	0.2%	0.2%	0.3%	0.3%	0.3%	0.3%	0.3%	0.4%
8,000,000	0.1%	0.2%	0.2%	0.3%	0.3%	0.3%	0.3%	0.4%	0.4%	0.4%
10,000,000	0.1%	0.2%	0.2%	0.3%	0.3%	0.4%	0.4%	0.4%	0.4%	0.5%
12,000,000	0.1%	0.2%	0.3%	0.3%	0.4%	0.4%	0.4%	0.5%	0.5%	0.5%
14,000,000	0.1%	0.2%	0.3%	0.3%	0.4%	0.4%	0.5%	0.5%	0.5%	0.6%
16,000,000	0.2%	0.2%	0.3%	0.4%	0.4%	0.5%	0.5%	0.5%	0.6%	0.6%
18,000,000	0.2%	0.2%	0.3%	0.4%	0.5%	0.5%	0.5%	0.6%	0.6%	0.6%
20,000,000	0.2%	0.2%	0.3%	0.4%	0.5%	0.5%	0.6%	0.6%	0.6%	0.7%
22,000,000	0.2%	0.3%	0.3%	0.4%	0.5%	0.5%	0.6%	0.6%	0.7%	0.7%
24,000,000	0.2%	0.3%	0.4%	0.4%	0.5%	0.6%	0.6%	0.6%	0.7%	0.7%
26,000,000	0.2%	0.3%	0.4%	0.5%	0.6%	0.6%	0.6%	0.7%	0.7%	0.8%
28,000,000	0.2%	0.3%	0.4%	0.5%	0.6%	0.6%	0.7%	0.7%	0.7%	0.8%
30,000,000	0.2%	0.3%	0.4%	0.5%	0.6%	0.6%	0.7%	0.7%	0.8%	0.8%
32,000,000	0.2%	0.3%	0.4%	0.5%	0.6%	0.7%	0.7%	0.7%	0.8%	0.8%
40,000,000	0.2%	0.3%	0.5%	0.6%	0.7%	0.7%	0.8%	0.8%	0.9%	0.9%
50,000,000	0.3%	0.4%	0.5%	0.6%	0.8%	0.8%	0.9%	0.9%	1.0%	1.0%
60,000,000	0.3%	0.4%	0.6%	0.7%	0.8%	0.9%	1.0%	1.0%	1.1%	1.1%
70,000,000	0.3%	0.5%	0.6%	0.8%	0.9%	1.0%	1.0%	1.1%	1.2%	1.2%
80,000,000	0.3%	0.5%	0.6%	0.8%	1.0%	1.0%	1.1%	1.2%	1.2%	1.3%
90,000,000	0.4%	0.5%	0.7%	0.9%	1.0%	1.1%	1.2%	1.2%	1.3%	1.4%
100,000,000	0.4%	0.6%	0.7%	0.9%	1.1%	1.2%	1.2%	1.3%	1.4%	1.5%
110,000,000	0.4%	0.6%	0.8%	0.9%	1.1%	1.2%	1.3%	1.4%	1.5%	1.5%

Source: Consensys

Still, there is a significant factor that may reduce this issuance rate even further. EIP 1559 – a proposal to restructure how users bid for Ethereum blockspace that will burn ETH transaction fees - could bring Ethereum's net issuance significantly lower and possibly negative. Assuming 20 million ETH will be staking (four million more than ConsenSys's target participation target). Ethereum's issuance would be ~2,000 ETH per day. To put that in perspective, Ethereum's median daily transaction fees so far in 2020 has been ~2,100 ETH per day, and throughout the second half of 2020 since DeFi took off and on-chain activity boomed, ~5,700 ETH per day.

MESSARI

Ethereum Daily Fees

Median daily Ethereum fees have been ~2,000 ETH throughout 2020, with a huge uptick during the DeFi boom over the summer.

Source: CoinMetrics

Although ETH 2.0 will scale transaction throughput substantially, thus alleviating fees per transaction, it would be surprising if ETH 2.0 generated less fees overall given the sheer number of paying transactions it could be processing. Regardless, it doesn't take much fees for issuance to drop below zero with how low issuance already is.

MESSARI

Ethereum 2.0 Annual Issuance Net of Burns

NETWORK ISSUANCE (NET OF BURN) — **ETH Burned Daily**

Total ETH Staked (Network)

	500	1,000	1,500	2,000	2,500	3,000	4,000	5,000	7,500	10,000
524,288	-0.1%	-0.2%	-0.4%	-0.5%	-0.7%	-0.9%	-1.2%	-1.5%	-2.3%	-3.1%
2,000,000	0.0%	-0.1%	-0.3%	-0.4%	-0.6%	-0.8%	-1.1%	-1.4%	-2.2%	-3.0%
4,000,000	0.1%	0.0%	-0.2%	-0.4%	-0.5%	-0.7%	-1.0%	-1.3%	-2.1%	-2.9%
6,000,000	0.2%	0.0%	-0.1%	-0.3%	-0.4%	-0.6%	-0.9%	-1.3%	-2.1%	-2.9%
8,000,000	0.3%	0.1%	-0.1%	-0.2%	-0.4%	-0.6%	-0.9%	-1.2%	-2.0%	-2.8%
10,000,000	0.3%	0.1%	0.0%	-0.2%	-0.3%	-0.5%	-0.8%	-1.2%	-2.0%	-2.8%
12,000,000	0.3%	0.2%	0.0%	-0.1%	-0.3%	-0.5%	-0.8%	-1.1%	-1.9%	-2.7%
14,000,000	0.4%	0.2%	0.1%	-0.1%	-0.3%	-0.4%	-0.7%	-1.1%	-1.9%	-2.7%
16,000,000	0.4%	0.3%	0.1%	-0.1%	-0.2%	-0.4%	-0.7%	-1.0%	-1.8%	-2.6%
18,000,000	0.5%	0.3%	0.1%	0.0%	-0.2%	-0.3%	-0.7%	-1.0%	-1.8%	-2.6%
20,000,000	0.5%	0.3%	0.2%	0.0%	-0.1%	-0.3%	-0.6%	-1.0%	-1.8%	-2.6%
22,000,000	0.5%	0.4%	0.2%	0.0%	-0.1%	-0.3%	-0.6%	-0.9%	-1.7%	-2.5%
24,000,000	0.6%	0.4%	0.2%	0.1%	-0.1%	-0.2%	-0.6%	-0.9%	-1.7%	-2.5%
26,000,000	0.6%	0.4%	0.3%	0.1%	-0.1%	-0.2%	-0.5%	-0.9%	-1.7%	-2.5%
28,000,000	0.6%	0.5%	0.3%	0.1%	0.0%	-0.2%	-0.5%	-0.8%	-1.6%	-2.5%
30,000,000	0.6%	0.5%	0.3%	0.2%	0.0%	-0.2%	-0.5%	-0.8%	-1.6%	-2.4%
32,000,000	0.7%	0.5%	0.3%	0.2%	0.0%	-0.1%	-0.5%	-0.8%	-1.6%	-2.4%
40,000,000	0.8%	0.6%	0.4%	0.3%	0.1%	0.0%	-0.4%	-0.7%	-1.5%	-2.3%
50,000,000	0.9%	0.7%	0.6%	0.4%	0.2%	0.1%	-0.3%	-0.6%	-1.4%	-2.2%
60,000,000	1.0%	0.8%	0.7%	0.5%	0.3%	0.2%	-0.2%	-0.5%	-1.3%	-2.1%
70,000,000	1.1%	0.9%	0.7%	0.6%	0.4%	0.3%	-0.1%	-0.4%	-1.2%	-2.0%
80,000,000	1.2%	1.0%	0.8%	0.7%	0.5%	0.3%	0.0%	-0.3%	-1.1%	-1.9%
90,000,000	1.2%	1.1%	0.9%	0.7%	0.6%	0.4%	0.1%	-0.2%	-1.0%	-1.8%
100,000,000	1.3%	1.1%	1.0%	0.8%	0.7%	0.5%	0.2%	-0.1%	-1.0%	-1.8%
110,000,000	1.4%	1.2%	1.1%	0.9%	0.7%	0.6%	0.3%	-0.1%	-0.9%	-1.7%

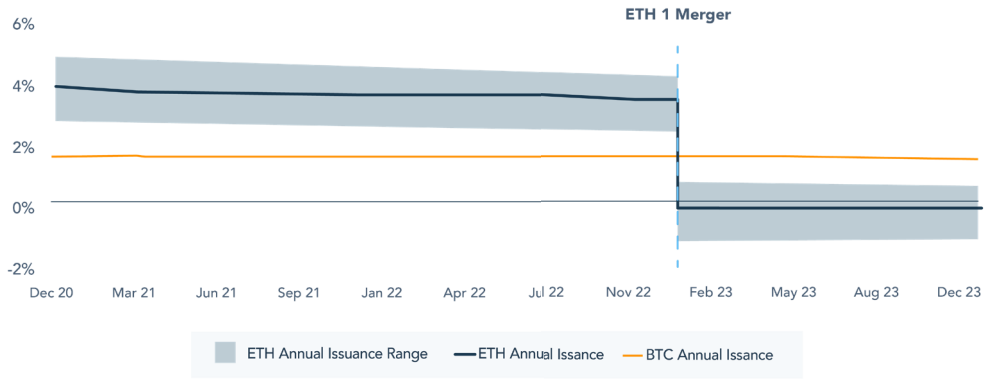
Note: Analysis assumes 100% validator uptime • Source: Consensys

Plotting these above analyses on a time series chart illustrates how significant the drop in annual issuance rate will be once ETH 1.x merges into ETH 2.0. At this point Ethereum's annual issuance would be well below Bitcoin's annual issuance rate of 1.7%.

MESSARI

Ethereum Net Annual Issuance Rate Throughout Transition to ETH 2.0

Ethereum's net annual issuance will drop substantially following the Phase 1.5 ETH 1 to ETH 2 merger.



Note: Issuance rnage includes ETH transaction fee burns at the bottom end. Top end of range assumes 30 million ETH staking, bottom end assumes 10 million ETH staking. • Source: Messari, Consensys

Beyond the fact that Ethereum's issuance will be extremely low, what may be more important is that it is sustainable. Recall from the ETH 2.0 philosophy section that Ethereum's monetary policy is defined as "Minimum Necessary Issuance" - the minimum amount of issuance necessary to ensure Ethereum remains secure. Rather than set its security budget arbitrarily like many fixed supply cryptocurrencies do in pursuit of monetary idealism, Ethereum prioritizes security. It just so happens that Ethereum's shift to PoS and its implementation of EIP 1559 transaction fee burns, also lower issuance as well. It is very likely that once ETH 1.x merges into ETH 2, Ethereum will not only be the most secure blockchain, but also the one with the most credibly low monetary policy.

INSIGHTS FROM BISON TRAILS

Proof of stake is criticized by some for potential centralizing effects–since tokens can generate rewards in perpetuity–but by keeping the inflation low, eth2 effectively negates that concern. By Vitalik's calculations, "it would likely take over a century for the level of concentration to double, and on such time scales other pressures (people wanting to spend their money, distributing their money to charity or among their children, etc.) are likely to dominate."

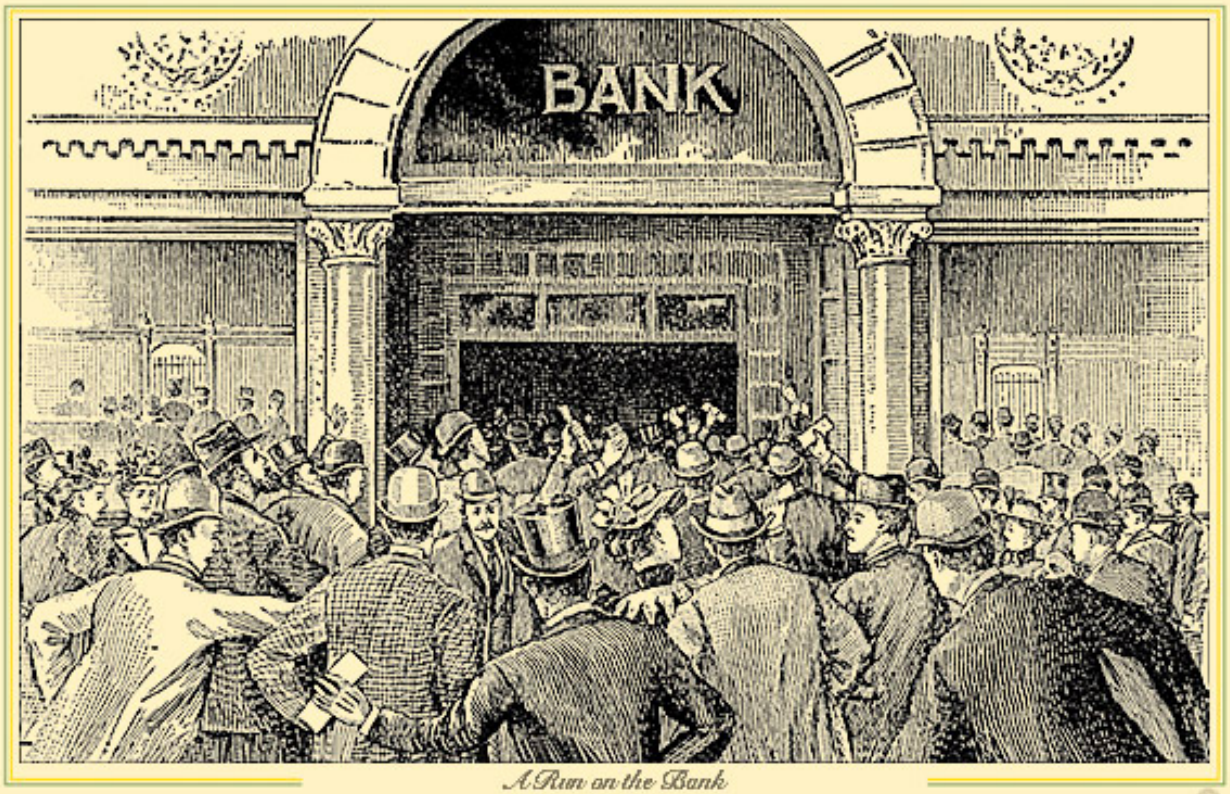
STAKING VS DEFI

As discussed in the overview section in Phase 1.5, becoming a validator will no longer require users to make a one way deposit and lock up their funds for an indefinite period of time. Instead stakers will be able to more freely deposit and withdraw their ETH. Validators will be able to "voluntarily exit" after serving for 2,048 epochs (~9 days). And once this period has passed, stakers will be able to withdraw their funds in around 27 hours (~36 days for slashed validators).[106] This added withdrawal functionality will introduce slightly different behaviors for stakers in comparison to pre-Phase 1.5 staking.

[106]Joseph Chow "**The Beacon Chain Ethereum 2.0 explainer you need to read first**" Ethos Dev, May. 23, 2020

One potentially important dynamic that will be present in Phase 1.5 that will not be in prior phases is the competition between staking and DeFi yields. Gauntlet Networks CEO Tarun Chitra, explored this dynamic in a 2019 paper titled "Competitive equilibria between staking and on-chain lending." In the paper Chitra demonstrated that it is possible for on-chain lending smart contracts to cannibalize network security in PoS systems assuming stakers behave rationally.

Chitra states that "when the yield provided by these contracts is more attractive than the inflation rate provided from staking, stakers will tend to remove their staked tokens and lend them out, thus reducing network security."[107] In other words, the paper describes a kind of neo bank-run where stakers suddenly withdraw their stakes from the protocol in pursuit of more attractive yields. The most important conclusion from his work was PoS chains cannot safely use deflationary monetary policy and instead must have adaptive monetary policy.



[107]Tarun Chitra, "**Competitive equilibria between staking and on-chain lending**" Feb. 5 ,2020

Luckily, ETH 2.0's monetary policy is adaptive and has a self-correcting negative feedback mechanism that prevents staked ETH from falling too low. As illustrated in the Phase 0 section on staking economics, reward rates in ETH 2.are proportional to the amount of ETH deposited (technically 1/sqrt of the amount deposited), so if deposits fall extremely low reward rates rise extremely high to incentivize more people to stake.[108] Further mitigating this effect is that stakers will likely not face a binary decision on whether to stake or lend their ETH in DeFi. The existence of staking derivatives will allow stakers to get additional productivity on their staked ETH through rehypothecation. If yields in DeFi are high, stakers may potentially be able to take advantage of those yields through putting their staked ETH derivatives to work in DeFi.

Beyond the security implications of staking vs DeFi, there's also investment implications of staking vs DeFi. Staking and DeFi fundamentally offer two different products which carry different risks that will factor into the decision whether to do one or the other. Beyond the systemic risk of the Ethereum blockchain failing, which every asset on Ethereum assumes, staked ETH just assumes the risks of validator performance. On the other hand, ETH deposited in DeFi assumes smart contract risk, liquidity risk, solvency risk, and composability risk from interconnectedness of DeFi protocols. In short the use cases serve two different purposes and competition between them may not be as simple as who offers the higher yields.

STAKING IMPLICATIONS ON ETH

As discussed in the Phase 0 section, validators are required to stake 32 ETH as collateral to register their node on the network in order to participate in consensus and earn yield. This opportunity to earn native yield on ETH will transform ETH as an asset, providing it with capital asset properties in addition to its properties as a commodity and store of value. Phase 1.5 furthers transformation of ETH as an asset, adding two key additional features to staking:

- The ability to withdraw your stake and claim rewards
- The opportunity to earn transaction fees

Staking provides ETH with bond-like characteristics in that it is a type of digital agreement where Ethereum acts as a bond issuer and stakers act as bond holders. Just like a typical vanilla bond, stakers provide capital up front to Ethereum and Ethereum pays stakers periodic rewards. The major difference is that stakers can redeem their ETH back on command as opposed to having to wait until a maturity date. This feature is similar to an embedded put option on the bond that provides the right, not the obligation, to demand early repayment of the principal.

[107]Vitalik Buterin, **Twitter**, Apr. 5, 2020

Building upon this idea of ETH as a bond is the fact that Ethereum's risk characteristics are similar to a sovereign bond. In staking, Etherum, the issuer, pays out stakers, the bond holders, in its own native currency, and the reason why Ethereum issues this agreement in the first place is to raise capital for security (recall that Ethereum is secured by staker's economic-value-at-loss). The relationship can be analogized to a nation state that issues bonds to pay for its defense budget and in return pays bond holders additional currency that it creates. The holder of that bond is perceived to hold the risk-free rate of that country in the sense that a government whose bond is issued in its own currency has no default risk because it can always print more currency.

Of course in practice, risk-free rate of return does not truly exist, as every investment carries at least a small amount of risk. Sovereign bonds, although often not assuming any default risk nominally, can practically default by inflating their currency too much to pay off their debt. Ethereum is similar in that it can guarantee to pay out stakers so long as the Ethereum blockchain remains alive because it pays stakers in its own currency. The difference being that Ethereum's payments are programmatic, and not guaranteed by a government but rather a sovereign blockchain.

INSIGHTS FROM BISON TRAILS

This approximation to a sovereign bond with a resulting risk free rate counteracts some of the risk of very attractive DeFi application returns incentivizing ETH holders to stop staking, resulting in lower security for the system. Just like in the traditional finance system, there will always be long-term players looking for low risk rewards, which in the case of eth2 is likely to be staking.

Source: Bankless

The above description of ETH as a bond may be especially powerful when ETH holders stake through decentralized staking protocols that diversify the performance risk of validators. Otherwise stakers assume idiosyncratic risk in the performance of their validator. In this more direct staking scenario ETH can be considered a contractor license bond, whereby in exchange for stakers posting ETH as collateral to register as a validator on Ethereum stakers receive a "license" to support consensus operations on-chain, and by obtaining this license, the validator agrees to adhere to the network's rules, which is to behave honestly and guarantee continued operations. Failure to meet those

requirements or behaving maliciously runs the risk of incurring penalties, forfeitures and/or lose the right to participate.[109]

However, Ethereum's bond-like characteristics are only half the picture. Two key features that make ETH equity-like as well are its perpetual nature and its claim on Ethereum's transaction fees. Unlike bonds which have maturity dates at which time bond holders are paid back their principal, stakers can stake their ETH and receive yield forever. In this capacity ETH can be considered a perpetual bond, which is practically treated like equity because Ethereum can pay out stakers forever. Of course though, unlike equity staked ETH does not have any voting power and rewards are non-discretionary, hence the perpetual bond moniker.

ETH's claim on transaction fees is a slightly more direct comparison to equity. Although EIP 1559 will likely burn the majority of transaction fees, some portion of fees will be paid to stakers. One of the first building blocks of EIP 1559 is a minimum fee called BASEFEE, which is levied by the protocol. The second building block is GAS_PREMIUM, otherwise known as "tip", which acts as an additional incentive for validators to include your transaction in the next block. The final building block is FEECAP which represents the most a user is willing to pay for inclusion in a block, including the tip. The entirety of BASEFEE is burned, while the tip is paid to stakers.[110] The latter component is important because it is an incremental reward stakers receive in addition to new issuance. In this function ETH acts like equity in that it has a claim on future fees from users demanding to transact on the Ethereum blockchain. And ETH can in part be valued as a function of those fees.

Taking many of the above points into consideration is why Colin Myers and Mara Schmiedt of ConsenSys and Bison Trails, respectively, eschewed attempting to box ETH into one asset class or another. Instead they astutely articulated that staking will make ETH function as a type of unique hybrid-perpetual bond with debt and equity like characteristics, declaring ETH alternatively as "The Internet Bond".

"The Internet bond is an entirely new asset for financial markets. It allows anyone in the world to invest, participate, and profit off an open-sourced, decentralized digital economy."[111]

ROLLUP-CENTRIC ETHEREUM WITH SHARDS AS DATA AVAILABILITY LAYERS

As discussed in the Phase 0 sections on rollups, ETH 2.0's lengthy roadmap will likely lead the community to rely on rollups as a near and mid-term scaling strategy. The key improvement to rollups' ability to scale Ethereum in Phase 1 is the introduction of sharding, which as discussed entails splitting Ethereum into 64 smaller, identical pieces, called shards.

[109]Colin Myers and Mara Schmiedt, "**The Internet Bond: Digital Work Agreements in the Web3.0 Era**" Aug. 2020 • [110]Hasu and Georgios Konstantopoulos, "**Analysis of EIP-1559**" Jun. 10, 2020 • [111]Colin Myers and Mara Schmiedt, "**The Internet Bond: Digital Work Agreements in the Web3.0 Era**" Aug. 2020

In Phase 1 these shards will each contain a subset of nodes and can be used to spread storage capacity across parallel shards in order to increase the system's overall transaction throughput. This boosted data storage via shards will provide the foundation for what Vitalik has promoted as a "rollip-centric future" for Ethereum. In this "rollup-centric future," Ethereum base-layer scaling would primarily focus on scaling how much data blocks can hold rather than how much on-chain computation they can perform. And by combining rollups with 64 data shards in Phase 1, Ethereum could support a theoretical max of ~100,000 transactions per second.[112]

Underpinning this strategy is scaling data availability for rollups, whose key limiting factor for scalability is how much data blocks can store. The most important benefit to this strategy is that scalability could come to Ethereum much quicker than if Ethereum were to wait until Phase 2, which is still years out. Optimistically, Phase 1 could arrive as soon as next year, meaning orders of magnitude more scalability for Ethereum could arrive in the near-future.

The second benefit of this strategy is that it will provide open space for layer 2 protocols to innovate and fund development - a benefit for Ethereum's long-term sustainability. Because creating rollups is permissionless, many different teams, including teams that are not close to the current core development process, could participate in designing execution environments for Ethereum. Furthermore rollups could more freely experiment with public goods funding mechanisms, either directly through fee capture or indirectly through a token, without the controversy Ethereum would experience attempting to do so at the base layer.

Moving most computational needs to layer 2s could also ultimately make ETH 2.0 safer, because sharding data availability is much less risky and complex than sharding EVM computation. Vitalik suggests this could help Ethereum distinguish itself as having a stronger security model than other sharded layer 2 chains, which are all working towards implementing sharded execution of some form. ETH 2.0 would instead just be powerful enough to have functionality escape velocity, but not too much to increase brittleness.[113]

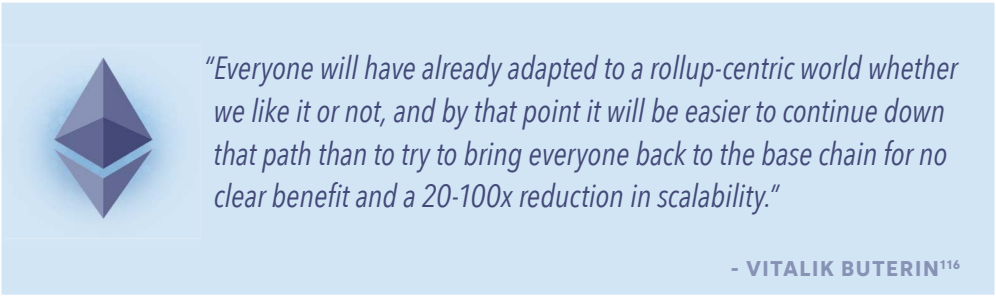
Of course this path is not without its challenges and drawbacks. The main downside to the rollup approach is the potential loss of developer network effects because there are many different rollups with fundamentally different internal execution environments. Although, it is possible that rollups could quickly move toward one set of standards being dominant, with some other standards catering toward niche communities.[114]

Additionally, there will need to be significant work done to adapt Ethereum to a world where users' primary accounts, balances, assets, etc are entirely inside rollups. Among this work

[112]Vitalik Buterin, "**A rollup-centric ethereum roadmap**" Ethereum Magicians, Oct. 2, 2020 • [113]Vitalik Buterin, "**A rollup-centric ethereum roadmap**" Ethereum Magicians, Oct. 2, 2020 • [114]Vitalik Buterin, "**Ethereum Foundation ETH 2.0 Research Team AMA (Pt. 5)**" Reddit, Nov. 18, 2020

is the need to integrate layer 2 protocol into wallets, improve the process for cross-layer 2 transfers, and speed up layer 2 withdrawal times.[115] None of these problems are impossible to solve, and some may be even easy to solve, but adapting the ecosystem's infrastructure for rollups may just take time.

A rollup-centric future could mean that Phase 1.5 becomes the final scheduled upgrade on ETH 2.0's roadmap. Because rollups layered on top of Phase 1 shards could provide a suitable long-term scaling solution well before Phase 2 arrives, research teams have begun to de-emphasized their work on Phase 2. As highlighted previously, sharded chains with data storage could already provide a theoretical max of ~100,000 transactions per second. Thus the demand for Phase 2 sharded chains with native computation, which provides ~1,000-5,000 TPS may be scarce.



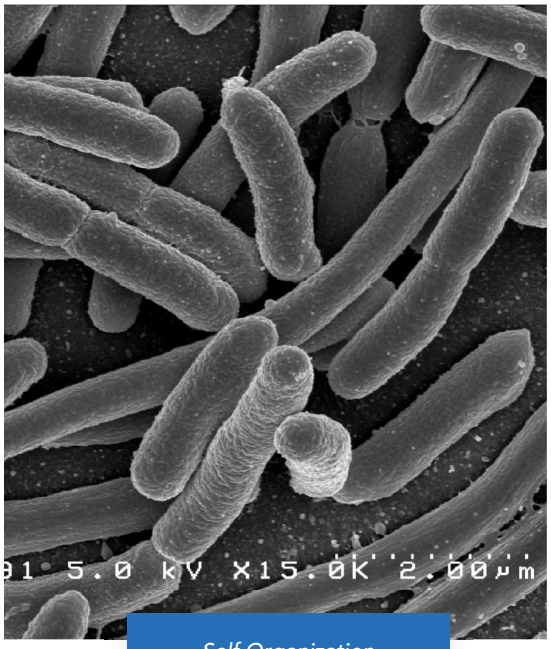
Despite this shift in focus, Phase 2 is still on the roadmap, and is still being worked towards, but there's a possibility Ethereum eventually accepts a "phase 1.5 and done" approach. ETH 2.0's long-term future would instead be as a single high-security execution shard that everyone processes, plus a scalable data availability layer.[117]

[115]Vitalik Buterin, "A rollup-centric ethereum roadmap" Ethereum Magicians, Oct. 2, 2020 • [116]Vitalik Buterin, "A rollup-centric ethereum roadmap" Ethereum Magicians, Oct. 2, 2020 • [117]Vitalik Buterin, "A rollup-centric ethereum roadmap" Ethereum Magicians, Oct. 2, 2020

Phase 2 & Beyond

PHASE 2 OVERVIEW

The broad vision for Phase 2 involves adding functionality to the Beacon Chain and remaining shards in the ETH 2.0 system. Each shard will transition from an open data container to a smart contract execution layer, enabling developers to deploy existing or new applications on shards other than the ETH 1.x version. If Phase 0 symbolizes the introduction of ETH 2.0's central nervous system while Phase 1 adds the skeletal infrastructure, Phase 2 represents the muscular anatomy that allows ETH 2.0 to execute a task in response to external stimuli (smart contract calls), and quite literally self organize.



Self Organization

ETH 2.0 research teams have floated several ideas regarding what form this upgrade could take, with most suggesting to replace Ethereum's current execution engine, the EVM, with a more efficient one. The EVM is a lightweight virtual machine (VM) that emphasizes correctness, an essential characteristic when state changes are immutable and the execution process is decentralized. But it is clunky in practice, which can hinder overall performance. By prioritizing correctness over performances, it appears as if the EVM has been designed "for theoretical purity, rather than practical use."[118]

The top candidate to replace the EVM is eWASM, a modified version of WebAssembly specifically designed for Ethereum. Unlike the EVM, eWASM optimizes for performance and offers support for writing contracts in multiple, more common programming languages, which could provide further scalability and developer experience improvements. eWASM is also part of the larger WASM family of virtual machines that are becoming popular among new Layer-1 blockchains. If Ethereum makes the switch to eWASM, it would make the network more compatible with WASM-based networks and expand the opportunities for cross-chain communication and use cases.

However, eWASM may face an uphill battle trying to overcome the EVM's current developer network effects. At the moment, the EVM is the current standard for blockchain development, and its use has been so strong that other Layer-1s have either added or are looking to add

[118]Rachel-Rose O'Leary, "**EVM 2.0: Inside the Race to Replace the Heart of Ethereum**" CoinDesk, Sep. 16, 2018

EVM support to attract developers. Sticking with EVM in the long run could give Ethereum a leg up on competitors as it would force them to continuously comply with Ethereum's standards. Ethereum researchers tend to have a more pragmatic approach that favors progression and open collaboration, but they are even starting to question whether eWASM's potential efficiency gains are worth ditching the EVM's sizeable library of developer tools.[119]

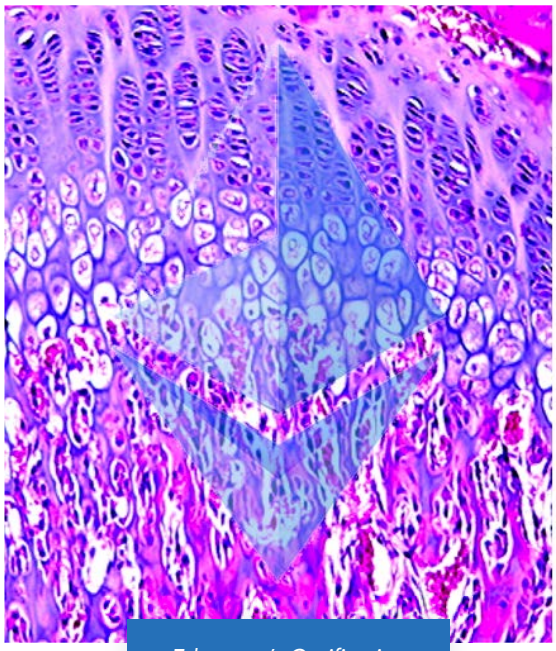
The conversation on potential Phase 2 upgrades has also included stateless clients and the concept of individual "execution environments" (EEs). A stateless client is node software that can validate blocks without having to store a chain's entire state history locally. Their ability to dramatically reduce node storage requirements and state growth (how quickly a blockchain grows in size) has led the Ethereum Foundation to accelerate research efforts on statelessness for both ETH 1.x and ETH 2.0 chains.[120] Now that they are a priority, Ethereum might offer support for stateless clients before Phase 2 arrives. In comparison, EEs would enable developers to create a custom environment for their specific application development needs, abstracting away the fixed rules of most smart contract execution layers.[121] But some ETH 2.0 developers have started to doubt whether their potential value is worth the complexity cost. Instead, the Ethereum Foundation might direct its efforts towards integrating a single, shared VM (such as eWASM) across all shard chains.[122]

stateless clients and the concept of individual "execution environments" (EEs). A stateless client is node software that can validate blocks without having to store a chain's entire state history locally. Their ability to dramatically reduce node storage requirements and state growth (how quickly a blockchain grows in size) has led the Ethereum Foundation to make "Stateless Ethereum" a major area of research. In comparison,

All of these proposed upgrades, including eWASM, are in the R&D stage. While there is a general vision for what Phase 2 might look like, it is the least defined out of the other ETH 2.0 phases and by far the furthest from completion. There's also the possibility that the scope of Phase 2 gets dialed back or, in the extreme case, removed from the roadmap altogether. If Ethereum's "rollup-centric future" strategy is successful, as discussed in the Rollup-centric Ethereum section above, it could replace the need for Phase 2 and lead Ethereum to accept a "Phase 1.5 and done" approach.[123] The less extreme scenario is if only a few shards (in the 4-8 range) become smart contract executions layers while the rest remain data containers for rollups. Either way, with rollups stealing the spotlight, the Ethereum Foundation has "de-emphasized" development efforts on Phase 2 as it is no longer a priority.[124]

[119]Danny Ryan, "**Ethereum Foundation ETH 2.0 Research Team AMA (Pt. 5)**" Reddit, Nov. 18, 2020 • [120]Danny Ryan, "**The State of Eth2, June 2020**" Ethereum Foundation, Jun. 2, 2020 • [121]Robert Drost, "**Eth2 - Beyond the Beacon Chain**" ConsenSys, Jul. 19, 2019 • [122]Danny Ryan, "**Ethereum Foundation ETH 2.0 Research Team AMA (Pt. 5)**" Reddit, Nov. 18, 2020 • [123]Vitalik Buterin, "**A rollup-centric ethereum roadmap**" Ethereum Magicians, Oct. 2, 2020 • [124]Vitalik Buterin, "**Ethereum Foundation ETH 2.0 Research Team AMA (Pt. 5)**" Reddit, Nov. 18, 2020

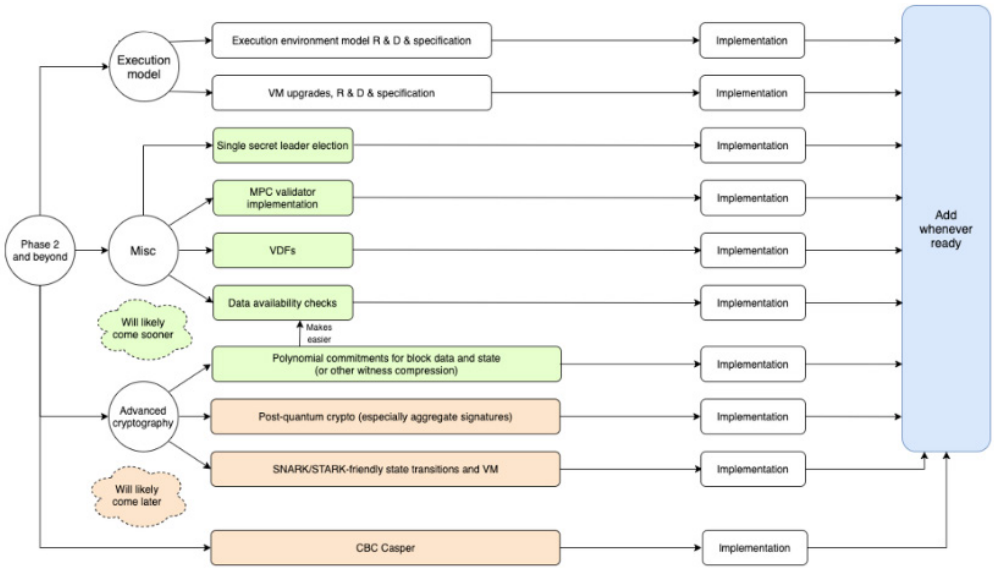
BEYOND PHASE 2



Ethereum's Ossification

Ossification can sometimes be conflated with never evolving. However, in the true spirit of the word ossification, Ethereum will not halt evolution altogether. Rather it will continue to improve its skeletal infrastructure, albeit more slowly than it has evolved so far in its life. If Ethereum Phase 2 solidifies the constitution of ETH 2.0, then additional changes down the road to Ethereum's skeletal infrastructure are like constitutional amendments.

One of the most powerful sovereigns ever, the United States of America, has only made 27 amendments to it's constitution in its 244 year existence. Each amendment being an admission that no organizational mechanism can be designed perfectly, and organizational mechanisms may always have to evolve to survive. And who ultimately decides how the organizational mechanisms are designed is not the constitution itself, but the people who empower it. People evolve over time. Thus similarly the people who lead Ethereum's development efforts won't completely halt evolution after Phase 2 (or Phase 1.5, whichever comes first). The ETH 2.0 roadmap includes several more advanced features that developers, and if by consent, the community, would like to add to Ethereum's skeletal infrastructure further down the line.



Source: Vitalik Buterin's Ethereum Roadmap for ETH 2.0 and Beyond

POLYNOMIAL COMMITMENTS

Polynomial commitments are one of several "Beyond Phase 2" research efforts that focus on making Ethereum more data efficient. They aim to replace the use of Merkle trees to dramatically reduce storage requirements on network clients.

In Ethereum, a Merkle tree is a proof (a small data set that represents a much larger data set) that references the network's transaction history.[125] Clients use these proofs to verify and store the chain's state, but without them, running a client would be impractical due to the excessive storage requirements. Any improvements to the size of state proofs like Merkle trees would make running a client even easier. That's where polynomial commitments, which Vitalik calls "magic math," can help out.[126]

Based on Vitalik's research, Danny Ryan estimates that polynomial commitments could reduce the weight (size) of state proofs by 50-500x.[127] With this potential level of data efficiency, magic math could be a breakthrough in the research on stateless clients, which are discussed in more detail in the Phase 2 Overview section above. Polynomial commitments are still very new to Ethereum and will likely take years of research alongside stateless clients before these theoretical improvements become practical solutions.

ZK-SNARK/STARK FRIENDLY VIRTUAL MACHINE

While the plan to replace the EVM with eWASM has lost momentum (as discussed in the Phase 2 Overview section above), some ETH 2.0 researchers agree that Ethereum will eventually require an upgrade to its smart contract execution layer (also referred to as a virtual machine or VM). In their eyes, the ideal successor to the EVM would be zk-SNARK or STARK friendly virtual machine.[128]

zk-SNARKs and STARKs are both cryptographic proofs that allow one to prove a statement (or possession of an asset) is true without ever revealing the statement (the owner of that asset). zk-SNARKs are what Zcash uses to enable private transactions, as ZEC holders can prove ownership over their assets without revealing their address or account balance.[129] zk-SNARK and STARK friendly VMs would extend this privacy preserving capability to smart contract execution, enabling developers to build and run applications without revealing the actual code. Any transactions that flow in and out of these applications would also remain private.

[125]William Foxley, "**Why Polynomial Commitments Might Be a 'Breakthrough' for Ethereum 2.0**" CoinDesk, Mar. 23, 2020 • [126]Vitalik Buterin, "**Using polynomial commitments to replace state roots**" EthResearch, Mar. 10, 2020 • [127]Danny Ryan, "**eth2 quick update no. 9**" Ethereum Foundation, Mar. 17, 2020 • [128]Vitalik Buterin, "**Ethereum Foundation ETH 2.0 Research Team AMA (Pt. 5)**" Reddit, Nov. 18, 2020 • [129]"**What are zk-SNARKs?**" Zcash Website, Sep. 21, 2018

Ethereum's radical transparency is a valuable asset, in that every inch of code and every transaction are fully auditable. But a fully transparent blockchain where any user could surveill another user may change the relationship between the surveilling user and the surveilled user by the simple fact of a user knowing they are being observed.[130] Privacy is important in ensuring the most powerful users don't interfere with weaker users' pursuit of self-sovereignty.

CBC CASPER

In the distant future, Ethereum could look to upgrade its Proof of Stake (PoS) algorithm from Casper FFG to CBC (Correct by Construction) Casper. These two variations of Casper are sister protocols that originated from Vlad Zamfir's early work on PoS network design. Both share some core characteristics, such as the use of LMD GHOST to determine the head of a chain. But CBC Casper arguably has a more complex design, which is what led Ethereum researchers to use Casper FFG for the Beacon Chain.

Despite its complexity, CBC Casper remains on the Ethereum roadmap because it offers some clear advantages over Casper FFG in terms of finality and flexibility. In FFG, the chain selection rule and finality algorithm are two different components that work together to create and finalize blocks, respectively (as discussed in the Phase 0 Overview section). According to Vitalik, this design is "awkward" and likely the reason ETH 2.0 will take about 13 minutes to finalize transactions.[131]

In comparison, CBC Casper combines these two algorithms. CBC also offers subjective finality, which allows node operators to individually select when they consider a block to be final. This process is an intra-protocol version of how exchanges select confirmation times for assets they support.[132] The more coherent and flexible design of CBC Casper enables it to finalize blocks faster than Casper FFG.

[130]Chris Burniske, "**Zcash Thesis**" Placeholder, Sep. 15, 2020 • [131]Vitalik Buterin, "**A CBC Casper Tutorial**" Vitalik's Website, Dec. 5, 2018 • [132]Ryuya Nakamura, "**CBC Casper and formal verification**" Medium, Apr. 24, 2019

Conclusion

"The Ethereum ecosystem has a resolute goal of being a stable and dependable system in the long run, but if you are here in Ethereum today, you should be here not because you believe the current rules (economic or technical) deserve to be protected and stabilized at all costs, but because you believe in where the ecosystem is going. In two years the main task will be to stabilize and cherish what we will have built. Until then, participation in Ethereum is unavoidably in part a prediction that the roadmap is a good one and that once this upgrading process ends we actually will get to a place where the network is efficient and stable and powerful and capable of being the base of significant parts of the global economy."

-VITALIK BUTERIN[133]

Conservatism vs Progressivism; one of the oldest debates in political philosophy, and one in which public blockchain communities cannot escape. Blockchain conservatives favor ossifying a blockchain so that it is stable and predictable - two essential properties for any blockchain aiming to serve as critical public infrastructure for things such as money. Blockchain progressives on the other hand, are unsatisfied with the status quo and favor evolving a blockchain so that it is more functional and performant. Ethereum has so far leaned more towards the progressive end of the spectrum, believing that blockchain technology is in its infancy and there are many fundamental improvements Ethereum must make before ossifying if it is to truly scale globally. But this progressivism has also been the primary source of Ethereum's criticisms.

For many critics Ethereum is too unstable to serve as the base layer infrastructure of an economy. It's constantly upgrading itself, constantly changing its narrative, and constantly pushing back it's "overly-ambitious" roadmap. And these critics aren't entirely wrong. Ethereum has always been a work in progress and is still it today.

[133]Vitalik Buterin, "**Ethereum Foundation ETH 2.0 Research Team AMA (Pt. 5)**" Reddit, Nov. 18, 2020

However, stopping analysis there would be missing the forest for the trees. With the coming launch of the Beacon Chain, stability is in sight, and Ethereum is now taking its first big step towards fulfilling a vision seven years in the making. ETH 2.0 is no longer the long-fabled but always out of reach upgrade that promises to bring Ethereum to the world. It is now Ethereum's present.

INSIGHTS FROM BISON TRAILS

"With millions of users, tens of thousands of dApps and companies, and billions of dollars of value involved with the protocol, the transition to eth2 will be no easy feat. As a platform providing validators for the earliest adopters to join the network, we're excited to power such a historic moment."

–Joe Lallouz, CEO of Bison Trails

ETH 2.0 could allow Ethereum to truly live up to its vision of providing a new social contract for the global economy founded upon open participation, borderless accessibility, credible neutrality, hyper transparency, and censorship-free interaction. ETH 2.0 will achieve this through scaling Ethereum orders of magnitude, increasing its security, reducing its energy waste, and maximizing its accessibility, all without sacrificing the crucial property of decentralization.

Furthemore, ETH 2.0 will not only transform Ethereum the blockchain, it will also transform ETH the asset. The introduction of staking will make ETH a significantly more productive asset than it was under PoW, providing ETH with native yield generating opportunities in addition to its current use as gas and money on Ethereum. The combination will provide ETH with an unprecedented combination of attributes from each of the three asset superclasses: capital assets, commodities, and stores of value, respectively. And it may also create a constant tug of war for ETH demanded by each use case.

With Ethereum's latest and strongest narrative to date, DeFi, pushing Ethereum to its limits as excitement and opportunity in the markets nears 2017 levels again, it's hard not to wish ETH 2.0 couldn't have come sooner. It would be much more ideal if when people use Ethereum this cycle it felt like it was ready for mainstream adoption. Yet what matters now is not that Ethereum isn't perfect today, rather it's that Ethereum continues to strive to be perfect tomorrow. Eventually ETH 2.0 will stabilize. But building the foundation for an institution meant to last hundreds of years takes time. The most important thing is that the Ethereum community keeps moving forward.

"The best time to plant a tree was twenty years ago. The second-best time is now"

-CHINESE PROVERB

About Messari

Messari is the industry's leading market intelligence company focused on the digital asset ecosystem. Our **tools** and **research** solutions provide customers with actionable insights to confidently make decisions in the fast-moving cryptoasset space. Since our inception in 2017, we've built strong relationships with the industry's top thinkers, investors, and builders from today's most promising projects. Learn more at **messari.io**.

Disclaimers

MESSARI