Ethereum 2.0

PROOF OF STAKE

Ethereum 2.0 is a multi-year interconnected set of upgrades that make Ethereum more scalable, secure, and sustainable, while keeping its core ethos of decentralization. This report focuses on Phase 0 of Ethereum 2.0 which introduces the long-anticipated proof-of-stake to the Ethereum ecosystem, with the Beacon Chain coordinating the expanded networks of stakers with sharding coming in the next stage planned for 2022.

Kaveh Tehrani

May 2021

TABLE OF CONTENTS

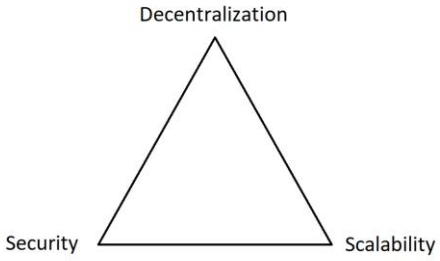
ETHEREUM 2.0

Ethereum 2.0 (Eth2) upgrades have been a long way in the making. Even though Ethereum shares many similarities with Bitcoin as it exists in its 1.0 iteration, the founding team led by Vitalik Buterin had long stated key upgrade, most notably the switch from proof-of-work to proof-of-stake, as early as 2014[1].

Eth2 upgrades make Ethereum more scalable, secure, and sustainable while enhancing its decentralization. Eth2 has started strong with the successful launch of the Beacon Chain that introduces the proof-of-stake to the Ethereum ecosystem. Proof-of-stake is a major step in addressing the Blockchain scalability trilemma which is the main challenge of decentralized scaling using proof-of-work consensus mechanism.

Ethereum's current chain is secure and decentralized, but it has been operating at the upper end of its scalability for some time now since Cryptokitties in 2017 congested the network and pushed it to its limits. As Decentralized Finance (DeFi) continues to grow at its exponential pace, it is ever more important to make Ethereum more scalable and bring down the transaction costs that are currently both too high and unpredictable to truly make Ethereum usable for all participants.

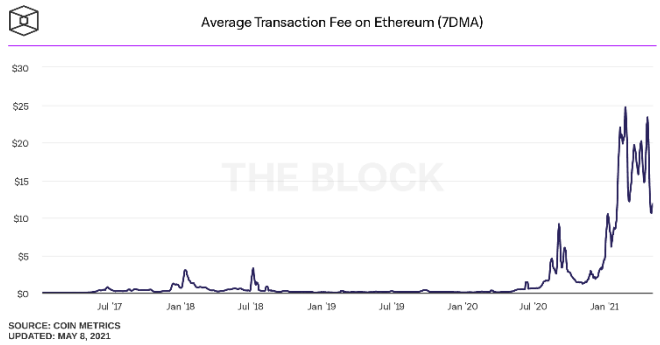
FIGURE 1 - SCALABILITY TRILEMMA - CHOOSE TWO

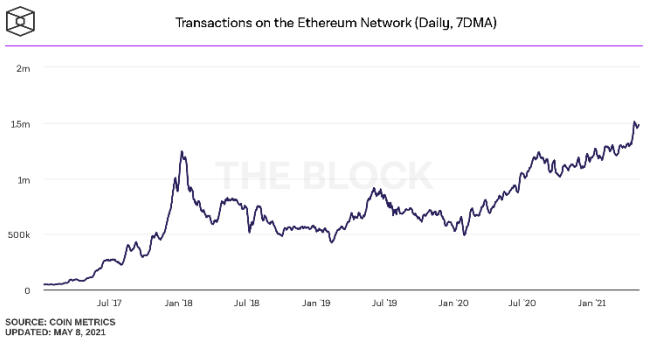


Scalability can be achieved by making the network more centralized. As DeFi has grown exponentially since 2020 with Eth2 still some time away, there has been a migration to other centralized chains such as Binance Smart Chain (BSC) where they have been able to scale up massively at the cost of substantial centralization, giving rise to the concept of Centralized Decentralized Finance (CeDeFi). BSC is compatible with the Ethereum Virtual Machine (EVM) which enables developers to port over their protocols with minimal effort. BSC has many parallels to the Ethereum's ecosystem with many protocols such as PancakeSwap are direct forks of existing DeFi protocols with minimal code changes.

Despite the current scalability issues and high transaction costs, Ethereum continues to enjoy most of the development in DeFi, and every indication thus far is for the Eth1/Eth2 merge to happen earlier than anticipated with sharding coming next.

FIGURE 2 - ETHEREUM TRANSACTIONS – GAS FEES ARE TOO HIGH AND VOLATILE





[1] For a comparison of Bitcoin to Ethereum, see Appendix A.

At its core, there are three components to Eth2 upgrades: The Beacon Chain which introduces proof-of-stake, the “merge” where mainnet merges with the Beacon Chain and phases out proof-of-work, and sharding which will drastically scale the capacity to process transactions and store data.

PHASE 0 -THE BEACON CHAIN

Phase 0 is all about the Beacon Chain which introduces proof-of-stake to the Ethereum ecosystem. The current chain will continue as a proof-of-work mainnet until “the merge” where Ethereum fully transitions to a proof-of-stake system by merging the current mainnet with the Beacon Chain. During the time where both the mainnet and Beacon Chain co-exist, stakers will be adding blocks to the Beacon Chain but this has no impact on the mainnet.

PHASE 1 - THE MERGE

The merge is a term being used to describe a period during the Phase 1 upgrade where the Eth1 and Eth2 blockchains are merged. After the merge, the Eth1 chain will run as the first shard of the Eth2 proof-of-stake blockchain.

PHASE 2 - SHARDING AND BEYOND

Originally planned for Phase 1, sharding is now part of Phase 2 with ongoing debate on its implementation and immediate necessity of sharding. Proof-of-stake upgrades with the advancement in a roll-up centric roadmap, will dictate how sharding unfolds.

WHAT IS STAKING?

Blockchain is a technology that solves the problem of **duplication** in how the original internet was designed. Blockchain at its core is a distributed database where all nodes on the network must agree on the state of the system. This is achieved using a consensus mechanism. Bitcoin as the first and most well-known use case of the blockchain technology, pioneered the proof-of-work consensus mechanism. There are several well-known issues with the proof-of-work consensus mechanism, and Ethereum has long stated its desire to switch to proof-of-stake.

Staking is the process of actively participating in validating transactions on a proof-of-stake blockchain. Participants need to ***stake*** a minimum-required balance in order to be able to validate transactions and earn staking reward. In Eth2, the minimum required balance is 32 ETH with no incremental reward for any higher balance.

PROOF-OF-STAKE

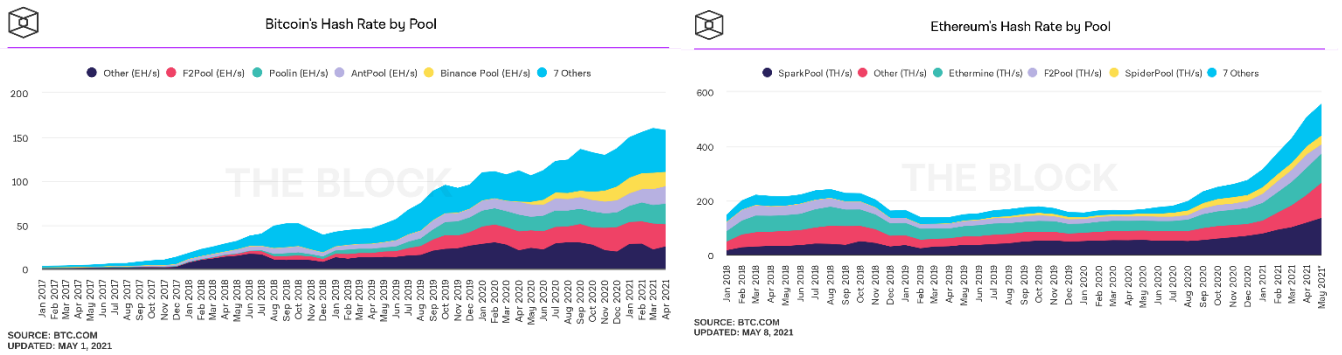
ADVANTAGES VS. PROOF-OF-WORK

DECENTRALIZATION

Despite Bitcoin's vision of a decentralized peer-to-peer network, the mining of Bitcoin over years has become increasingly centralized due to two reasons: 1- hashrate is purely a function of hardware capability with large economies of scale, and 2- required energy use for proof-of-work consensus mechanism favouring geographies with subsidized and economical energy.

This runs counter to the ethos of its original vision where mining on consumer-grade computers was the primary method of earning coins. Today nearly the entirety of Bitcoin mining happens on ASIC mining chips specifically targeted at its SHA-256 hash function, or on mining pools. The chances of an individual mining any major proof-of-work on a consumer-grade computer is almost null.

FIGURE 3 - HISTORICAL MINING POOLS – PROOF-OF-WORK MINING HAS INCREASINGLY BECOME CENTRALIZED



Source: theblockcrypto.com

Unlike proof-of-work, where at its core is a simple grid search to find the required nonce, validators do not need significant amount of computational power because they are not competing. Instead they are selected and simply need to create the block when called upon, or validate proposed blocks created by other nodes. This validation is known as attesting. There are rewards for both proposing new blocks and attestations, with a penalty system known as slashing for malicious activity.

The odds of being selected for validation is proportional to value staked in a **linear** scale. This contrasts with proof-of-work where there are enormous economies of scale as evidenced in concentration of hashing power on ASIC farms in regions with subsidized electricity.

ENHANCED SECURITY

The cost of a majority attack is drastically higher in a proof-of-stake mechanism. A majority attack requires at least 51% of the network's **value**, which is costly to acquire and likely not worth the cost given that any hint of a malicious participant achieving supermajority status is likely to crumble the value of the chain itself.

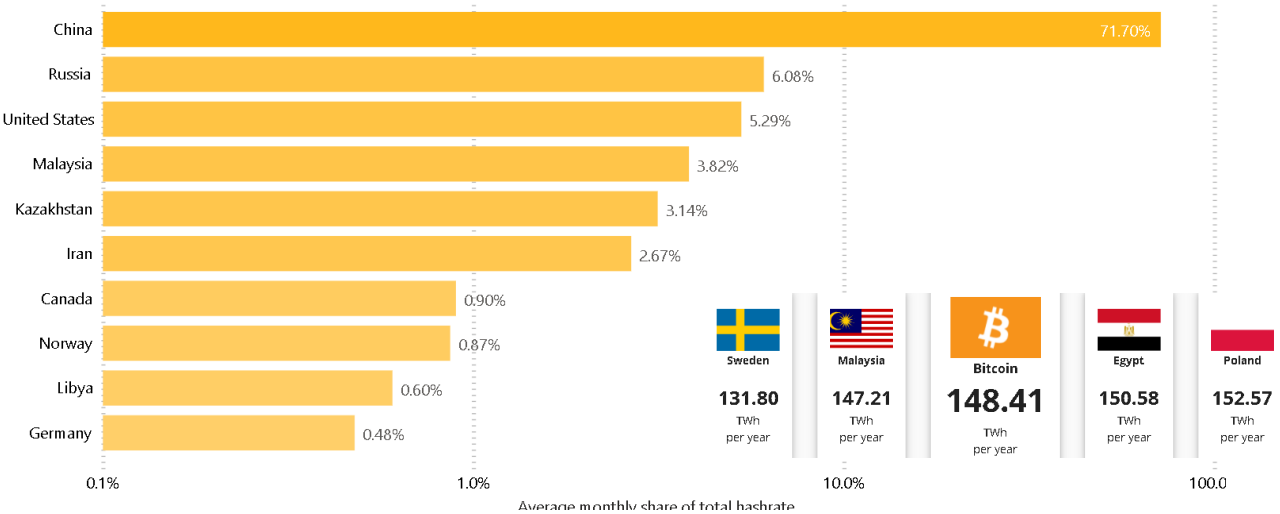
Furthermore, proof-of-stake cannot be repeated on other blockchains without first accumulating the required threshold itself. In proof-of-work, with sufficient hashing power, any blockchain on proof-of-work is a potential target and the hashrate is fully mobile from one target to the next. The **only** requirement in a proof-of-work majority attack is sufficient hashrate accumulated directly via hardware. Stated another way, the only way to secure a proof-of-work network is maintaining sufficient hashrate. Given the centralization of hashing power and economic incentives to mine whatever is the most profitable, this is a difficult feat to achieve.

At the core of a proof-of-stake security model is the idea of **economic value-at-loss**. Stakers can lose their stake for malicious behaviour, and bad behaviour is punished via a mechanism called slashing. This penalty system introduces a **disincentive** into the network that is missing in blockchains using proof-of-work consensus mechanism.

ENVRIONMENT FRIENDLY

One of the main criticisms of Bitcoin is the environmental impact applicable to any proof-of-work coin including Eth1. Bitcoin mining consumes more energy than several countries[1], many of which are dependent on non-renewal energy sources.

FIGURE 4 - AVERAGE MONTHLY HASHRATE BREAKDOWN BY COUNTRY



Source: cbeci.org
Note: 2019 to Q1 2021

[1] digiconomist.net/bitcoin-energy-consumption/

SUPPORT FOR SHARDING

Proof-of-stake offers much stronger support for shard chains which is a critical part of scaling Ethereum's roadmap after the merge of Eth1/Eth2. Proof-of-work's dependence on massive hashrates to ensure its security makes sharding effectively a non-starter given the hashrate would be divided among different shard chains.

REDUCING CONFLICTS OF INTEREST

In a proof-of-work blockchain the interest of miners and users of the blockchain are conflicting. Miners earn block rewards as well as fees, and benefit from higher transaction costs. Meanwhile high transaction costs are a disincentive to the users of the blockchain and make development on the network more costly. Proof-of-stake largely eliminates this conflict by better aligning the economic incentives of validators with the chain's use case as programmable money.

This conflict of interest is one of the reasons that Bitcoin's reliance on proof-of-work potentially makes it unstable once all 21m coins have been mined and there are no more block rewards for miners resulting in a substantial drop in network's hashrate.

DISADVANTAGES VS. PROOF-OF-WORK

ACQUISITION

In a proof-of-work blockchain coins are mined, i.e., earned by participating in the network to verify transactions. One major drawback of a proof-of-stake is that stakes can only be accumulated by purchasing from an entity who has them. This means that new entrants to the Eth2 can only run a validator node by buying the required 32 ETH to run a validator, which at current prices nearing 4k USD is a high barrier to entry.

ONE-WAY TRANSACTION

Most proof-of-stake chains have a lock-up period for their staking mechanism. Eth2 staking currently has no definitive end date but it is expected to happen in early 2022 where Eth1/Eth2 merge. Until then, the locked-up ETH is not available at all, though some staking services have wrapped tokens available for interim liquidity.

SLASHING

Slashing is the penalty system in a proof-of-stake to reduce the stake of malicious validators, either intentionally or unintentionally. This introduces a level of anxiety given that the transactions are one-way and setting up a standalone validator requires a fair amount of technical knowledge. Thus far, a

significant number of slashings have been due to technical issues or redundant setups using duplicate keys that were actually intended as backup validators.

LIMITED TRACK RECORD

Eth2 is one of the most ambitious system-wide upgrades in the history of blockchains and fundamentally changes how the Ethereum ecosystem works. It is also the first time a major blockchain has attempted a full revamp into a new consensus mechanism while staying fully operational. There are several unknowns that are still under development, but the start has been extremely promising.

CUSTODY

Participants without the required 32 ETH or desire to set up a standalone validator themselves, will have to participate via a staking pool which means they do not have direct custody of their keys and need to rely on the competence and integrity of their pool operator.

TECHNOLOGICAL UPKEEP

Running a standalone validator requires an initial upfront cost which is fully attainable via consumer-grade hardware. Validators however need to also be maintained for upkeep which requires a stable and always-on internet connection. Offline validators can get slashed for extended periods of inactivity. Those without the desire to maintain a physical system with near 100% uptime can run their validator on a node in the cloud, however this is somewhat discouraged as cloud solutions are centralized and can introduce a single point of failure into the system.

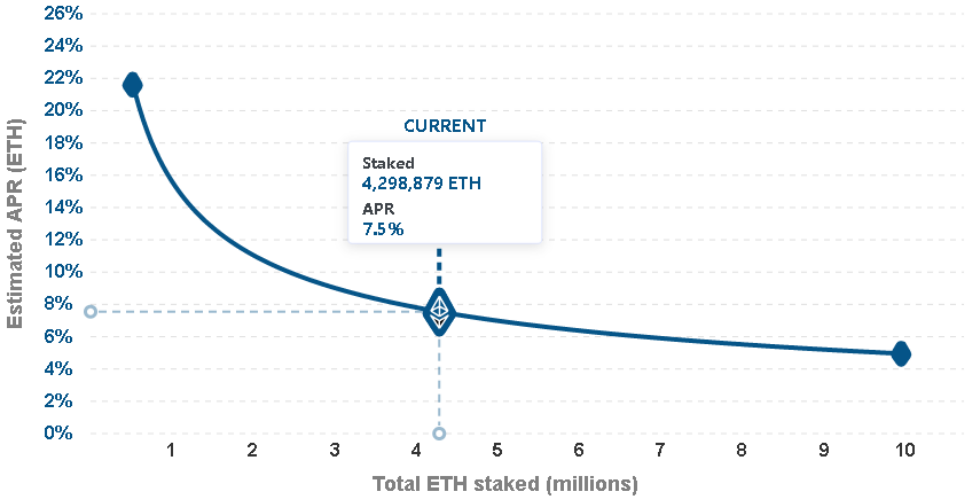
WHY STAKE?

ECONOMIC INCENTIVES

Validators earn staking rewards for validating transactions on the blockchain. The initial incentives were quite high to attract a critical mass in order to successfully launch the Beacon Chain. There is a drop in staking rewards as more ETH gets staked levelling off around 5% as shown in the Figure 5 below.

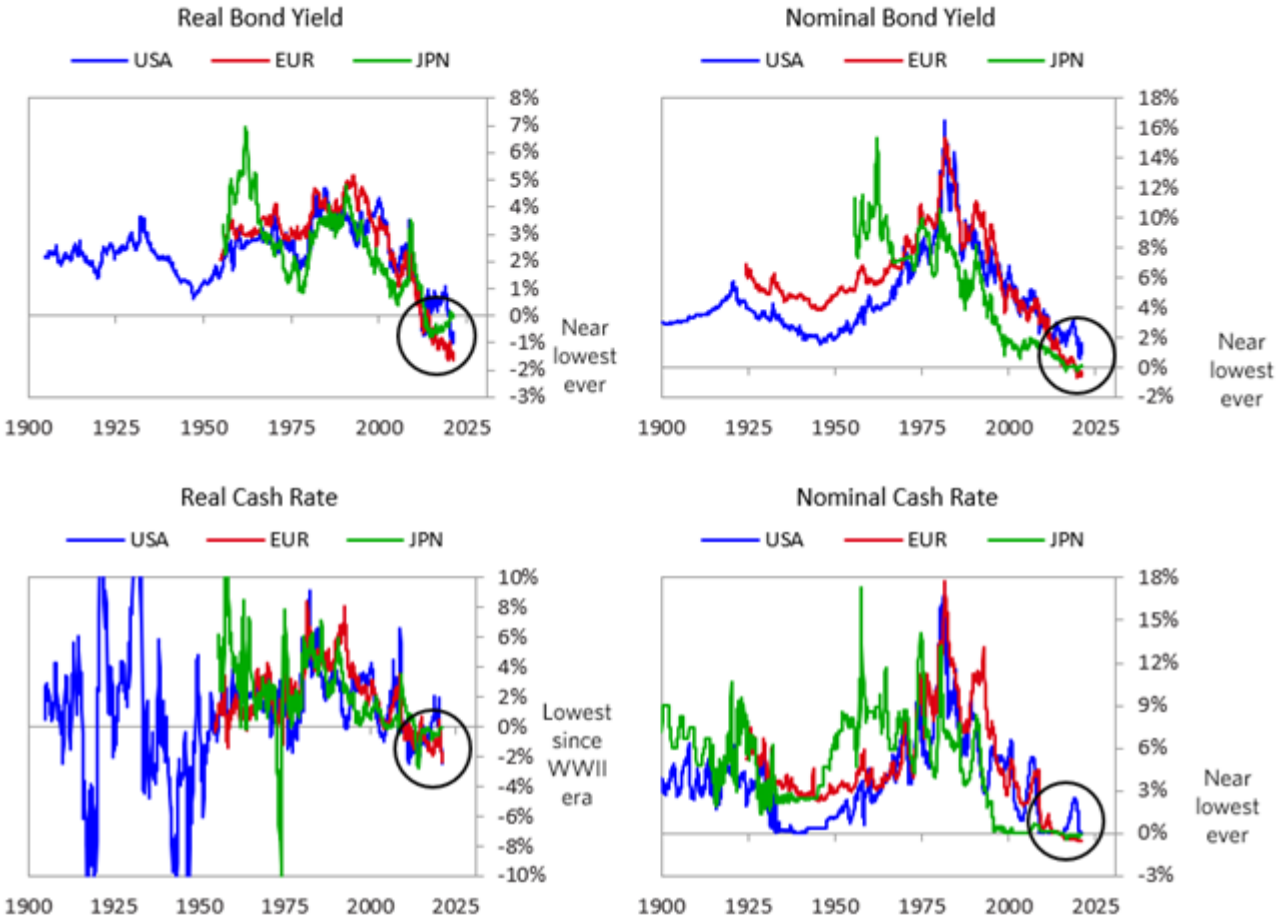
This is a healthy return from a macro perspective in a world where nearly every major developed world has negative real yields far out into the yield curve, with negative nominal rates in parts of Western Europe on bank balances including ordinary citizens' saving deposits. Furthermore, low nominal yields are priced to stay for extended periods of time making allocation to fixed-income a difficult choice in portfolio construction going forward.

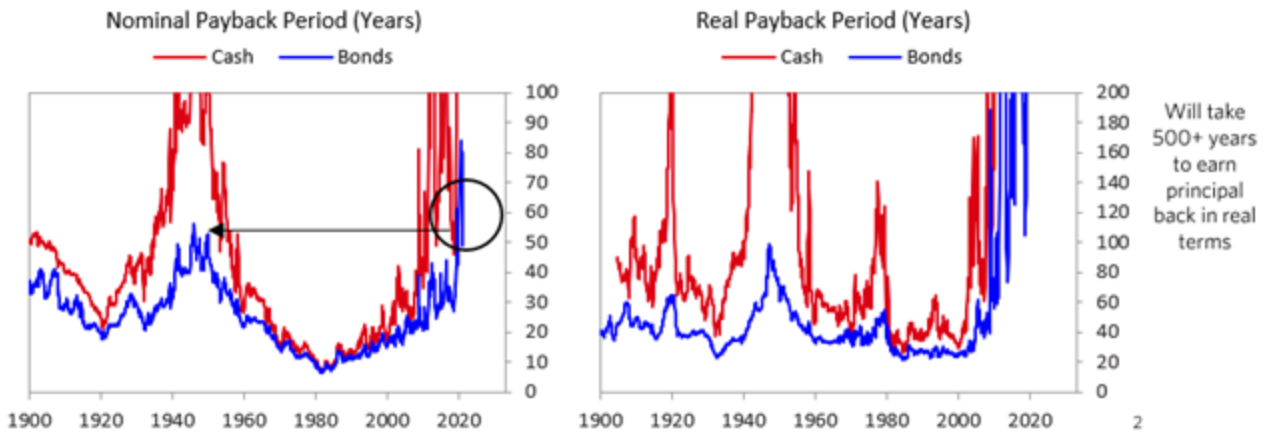
FIGURE 5 - ETH2 STAKING AND REWARDS



Source: launchpad.ethereum.org

FIGURE 6 - YIELDS AROUND THE WORLD ARE AT HISTORICAL LOWS AND PRICED TO STAY LOW





Source: ***Bridgewater Associates***

While not the focus of this report, one can certainly see the appeal of a well-defined monetary policy mandated by code in a world that has been in a perpetual and deepening monetary easing cycle with several unintended side effects including inflation of almost every asset class at the expense of future expected returns.

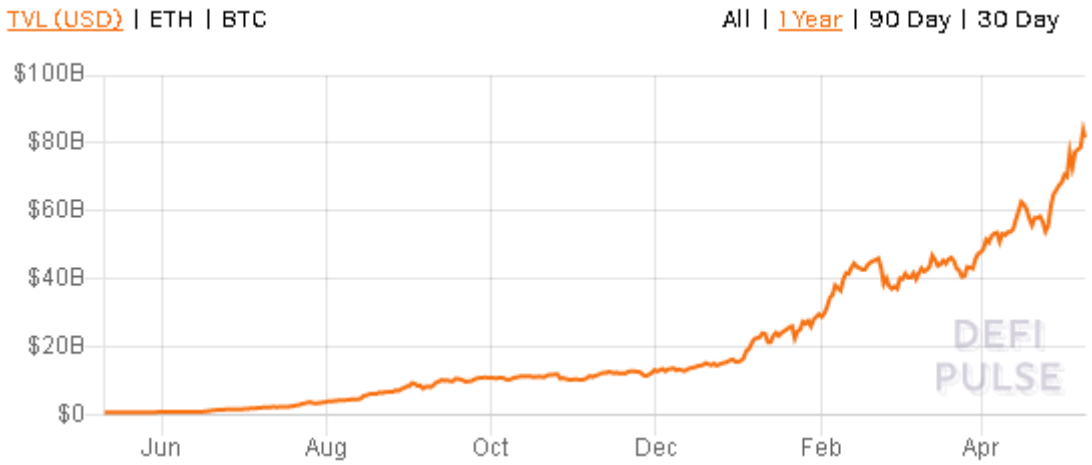
STAKING AS A PUBLIC GOOD

Staking in Ethereum is thought of a public good in the ecosystem. In return for helping to secure the network and lending infrastructure, stakers earn rewards in the process with strong incentives offered to early adopters.

Staking makes Ethereum significantly greener by phasing out proof-of-work and helps accrue value to the protocol in the Web 3.0 design. This is a critical departure in how we have utilized the internet since its inception, as there has been virtually no value accrued to the protocol, but enormous value has been accrued to the application layer. The internet came out of government defense research institutions and virtually no attempt was made to monetize any of the protocols such as HTTP, TCP/IP, SMTP/POP3/IMAP, etc. despite the enormous amount of public benefit they have provided. This is summarized in the concept of "Fat Protocols" which is not well-understood by those who have not taken the time to understand blockchain's value proposition.

DeFi Summer was ignited by the introduction of Compound's governance token and has seen widespread adoption since . DeFi's success is testament to the robustness and validity of fat protocols and a shift away from platforms in Web 2.0, e.g., Facebook and Google, where the user is the product with no value accrued to the user with minimal control in governance or the protocol's direction.

FIGURE 7 - TOTAL VALUE LOCKED IN DEFI



Source: ***DeFi Pulse***

STAKING VS. DEFI

After the Eth1/Eth2 merge, becoming a validator will no longer require an indefinite lock-up. Stakers will be able to move freely and with the advent of yield-farming there will be a natural comparison between staking and yield-farming yields.

As shown in Figure 5, there is a natural mechanism to incentivise staking and prevent staked ETH from falling too low and making majority attacks too easy to achieve. Beyond this security vs. reward trade-off, there is an investment implication whereby investing in DeFi is fundamentally a different product.

There is a systematic risk of the Ethereum ecosystem entirely collapsing which affects every asset on the blockchain. Staking ETH on the network solely assumes the risk of validator performance. ETH locked into a DeFi protocol, however, assumes smart contract risk, liquidity risk, and frictional costs transacting on the network, which in theory should command a higher risk premium for assuming the additional risks not present in staking.

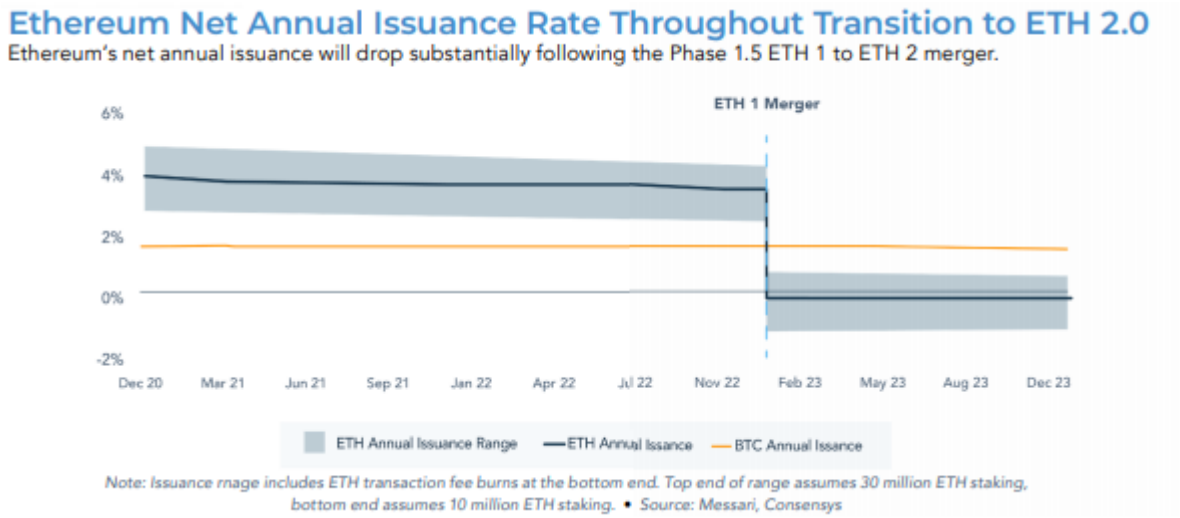
IMPACT ON THE ETH PRICE

Ethereum's monetary policy is defined as "Minimum Necessary Issuance" which is defined as the minimum issuance required to secure the network. Recall that in a proof-of-work consensus mechanism, a high hash rate is the **only** defense against a majority attack and can only be incentivized with high rewards offered to the miners who are economical participants and agnostic to the blockchain given that they have little skin in any chain. Ethereum is estimated to be overpaying significantly for this security given that the network's security supersedes all other requirements.

With the switch to proof-of-stake, the rate of issuance significantly goes down as hashrate is no longer relevant for securing the network as shown in the estimate in Figure 8 post merging of Eth1/Eth2.

The current annual network issuance is approximately 4.5%. After the merge, this rate is expected to drop well below 1%. The rate will be dependent on the amount of ETH locked with sufficient incentives in place to make majority attacks economically infeasible.

FIGURE 8 - ETHEREUM NET ANNUAL ISSUANCE FORECAST



There are three forces that impact the price of ETH with the launch of Eth2 upgrades.

First, there is a period of co-existence where Eth1 and Eth2 are both operational and issuance on the Beacon Chain is incremental to the system. The effect of this issuance thus far is minimal, given that it is temporary, well conveyed in advance, and requires a lock-up of 32 ETH per validator which effectively reduces publicly available float for trading.

Second, the expected drop-off in issuance combined with the upcoming EIP-1559 (i.e., London Fork) affecting Eth1, is a significant reduction in the net issuance rate of ETH and will be a deflationary force in pushing up the price of ETH.

Third, the Ethereum's capacity for processing transactions is expected to grow significantly even before the introduction of sharding. This is expected to incentivise further use of Ethereum as the platform of choice for DeFi developers, decreasing transaction costs but massively increasing total volume resulting in higher overall transaction costs which accrue to the ETH holders and stakers.

HOW TO STAKE

The staking mechanism in Eth2's proof-of-stake has been designed to address short-comings of proof-of-work in terms of scalability without compromising decentralization and security.

The hardware requirements as covered previously are near the low-end of the spectrum and most consumer-grade hardware can run a standalone validator. It is important to keep in mind the ethos of decentralization while choosing a staking mechanism. While turnkey solutions do exist, the future health of any decentralized ecosystem, including Ethereum 2.0, depends on a vast network of decentralized nodes that do not introduce any single point of failure.

As the price of Ethereum has significantly increased in 2021, the 32 ETH requirement is a much higher hurdle to new entrants than the technical / knowledge requirements. With ETH price nearing 4k USD, the entry cost is likely out of reach for most new entrants versus when the requirements were finalized in early 2020 with ETH averaging ~200 USD.

SOLO STAKING / RUNNING A VALIDATOR

Given the importance of decentralization in the Ethereum's ecosystem, solo staking on a physical hardware is the route that was envisioned when staking methodology and requirements were designed. Staking Eth2 is significantly easier both logistically and operationally given that technological requirements are far lower than both proof-of-work and other similar chains operating on proof-of-stake consensus mechanism.

Staking Eth2 can be done on most consumer-grade hardware at the moment including single-board computers such as Raspberry Pis. The requirements are likely to go up slightly as the storage and computational requirements expand rendering single-board computer obsolete in a couple of years time.

A popular solution that can scale easily as required with no physical hardware requirement is staking on the cloud. That said, cloud services in general are heavily centralized and introduce a central choke point into the ecosystem and as such they are not recommended if motives for staking include enhancing the blockchain and contributing to the health of its ecosystem[1].

STAKING IN A POOL

Staking pools are primarily used by participants who do not have 32 ETH or do not want to commit to running a validator for themselves with the required upkeep. Staking pools provide this service for a fee. Some also provide secondary liquidity in the form of tokenized staked ETH.

[1] There have been several instances of AWS outages impacting large swaths of the internet as web hosting solutions have become centralized over time.

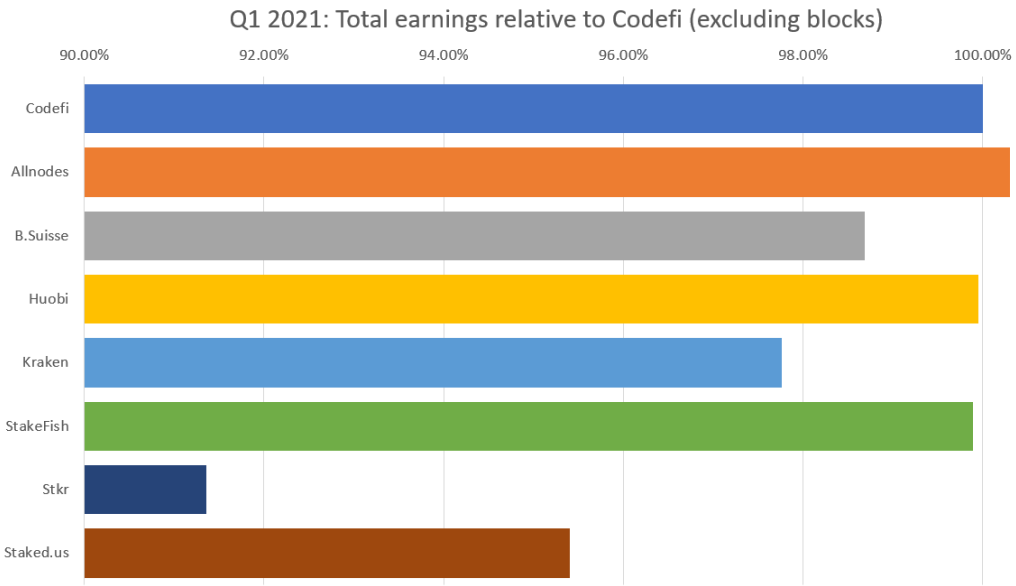
A non-comprehensive list of staking services can be found here. Some exchanges such as Kraken also offer staking services.

EXTERNAL SOLUTIONS

There are few institutional staking solutions available with ConsenSys Codefi – currently the most well-known platform to be operating. Building solutions internally is relatively capital and technology intensive given that there is **no incremental** return past the 32 ETH deposited. The only way to generate incremental returns is to initiate a validator with 32 ETH staked.

A natural assumption is that institutional-grade custody solution providers over time will provide staking services, such as Gemini. Wallet providers like Ledger already provide staking solutions for other digital assets. There are also funds specifically aimed at staking such as Staked for ETH which provide turnkey solutions for a fee.

FIGURE 9 - RELATIVE REWARDS EARNED FROM ATTESTING BY STAKING SERVICES



Source: ***ConsenSys***

CONCLUSION

Eth2 upgrades are a major step toward making the Ethereum ecosystem more scalable, secure, and sustainable. The first step is the introduction of proof-of-stake via the launch of the Beacon Chain.

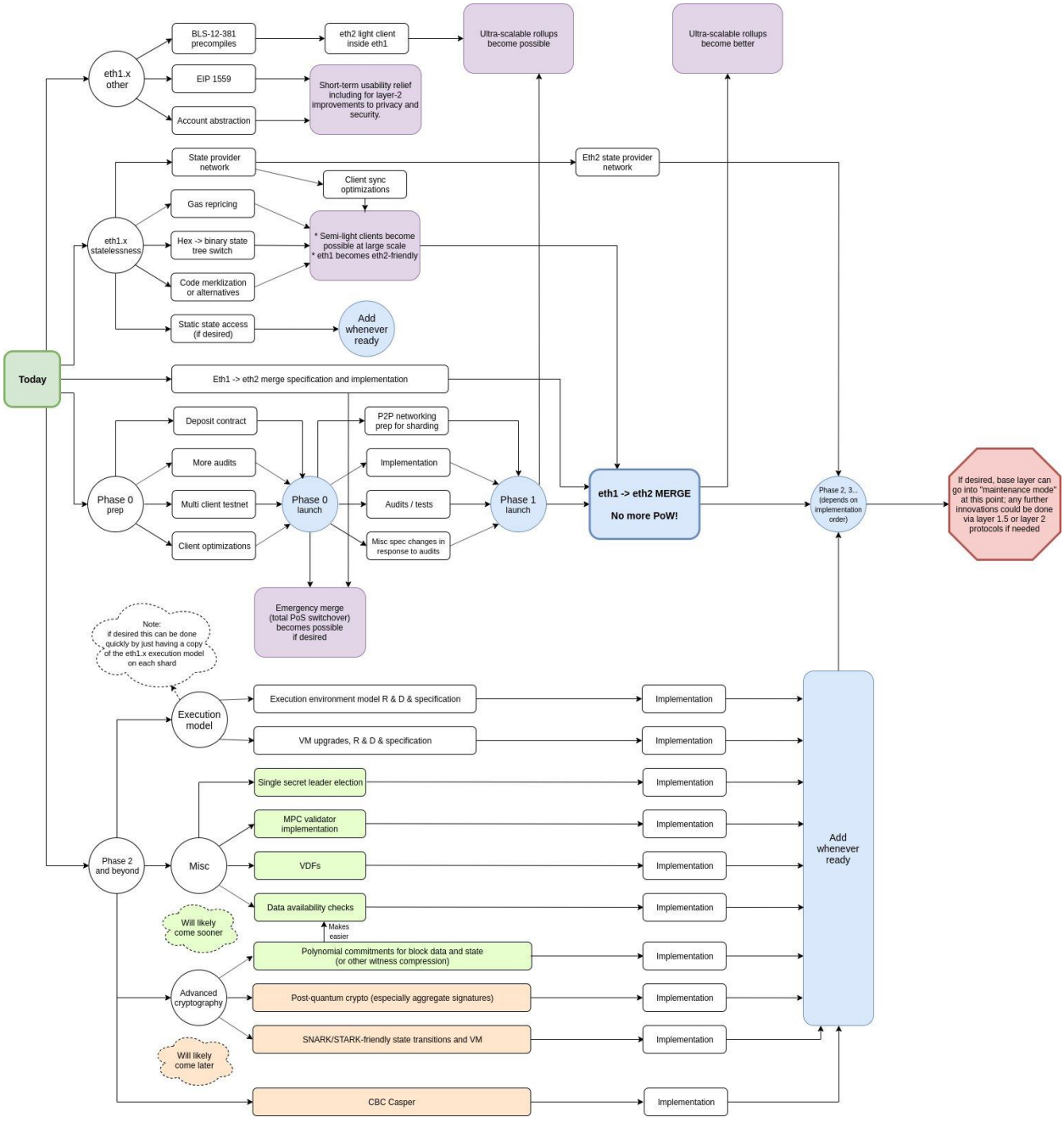
Critical to the proof-of-stake consensus mechanism is the adoption of staking which has been substantial with 4.3m ETH staked (circulating supply of 115m) by a total of ~133k validators with majority running the minimum required 32 ETH staked.

Staking is a natural evolution of one's journey in the Ethereum ecosystem. Bitcoin is the gateway for most into the blockchain universe and will likely continue to operate as an unbiased value layer, i.e., digital gold for a long time to come. Ethereum however is where the bulk of development has been in the last few years and has only accelerated with the exponential growth of DeFi.

Eth2 upgrades are off to a great start, having only launched in December 2020 after a long period of planning. There are still several unknowns, but the launch of Beacon Chain already has been successful enough to move up the anticipated date of Eth1/Eth2 merging. Phase 1 and 2 will consolidate Eth1/Eth2, phase out proof-of-work, and introduce sharding which will substantially raise Ethereum's capacity for transactions while lowering fees, in effect providing a blockchain usable globally by anyone with as little as a smartphone connected to the internet.

Staking Ethereum provides a great way contribute to the advancement of the Ethereum ecosystem while earning attractive economic rewards along the away and is a natural progression for any long-term holder that believes in the value of the protocol over the long run.

APPENDIX A – ETHEREUM 2.0 APPROXIMATE ROADMAP



Source: https://twitter.com/VitalikButerin/status/1240365047421054976 annotated version at https://notes.ethereum.org/KMsYUL1pTomNS_gLevDlpA?view
Note: The roadmap since then has prioritized eth1/eth2 merge over sharding

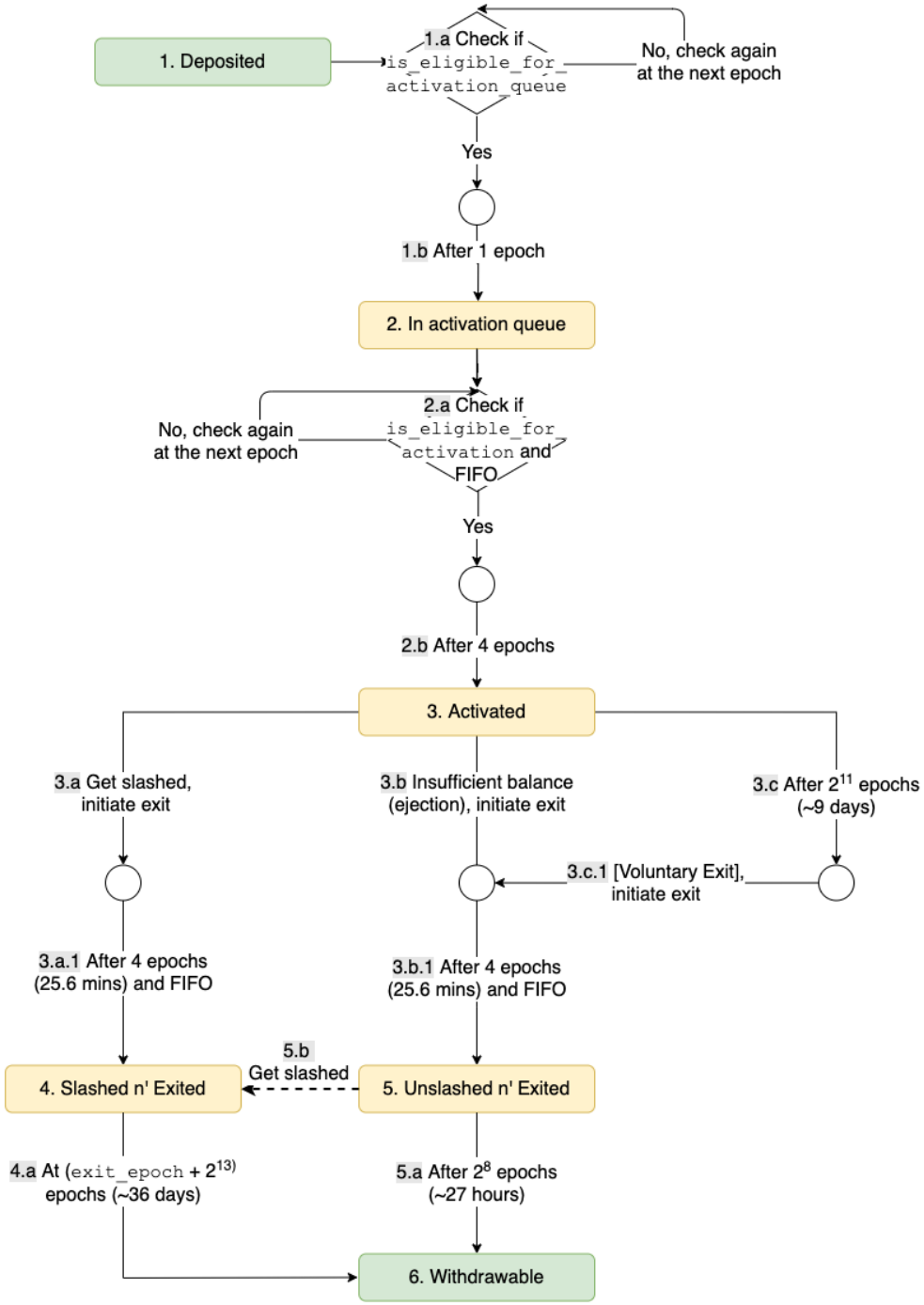
APPENDIX B – BITCOIN VS. ETHEREUM

Ethereum 1.0 is in many ways similar to Bitcoin today. Ethereum's roadmap however from its inception included a roadmap emphasising scalability and reliability with proof-of-stake as a critical component via the long-anticipated Casper upgrade.

	Bitcoin ₿	Ethereum
Founders	• Satoshi Nakamoto (pseudonym) • "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008 • First transaction in January 2009	• 2-5 depending on how you count • Vitalik Buterin is the most well-known • Initial release via an ICO in 2014
Purpose	• Pioneered the Blockchain technology with Bitcoin as its first use case • Digital currency for transferring value	• Programmable money via smart contract build using Blockchain technology enabling decentralized applications
Mining	• Proof of work	• Proof of work at inception, with intention to switch to proof-of-stake stated upfront
Transaction Fees	• Build-in reward system with halving mechanism built into code (~4 years) • Miner incentives via fees and block rewards (block rewards persist until all 21m coins are mined)	• Gas system with varying transaction costs depending on network's state of supply/demand • Balancing act between too high fees or too low fees while balancing network security
Block Size[1]	• 1MB block size, roughly 1 block every 10 minutes • Joint constraint acts as a bottleneck	• There is no maximum block size • Blocks are bound by gas limits • Block size has increased over time with current blocks averaging ~50kb
Economics	• Hard cap at **21m coins** with ~19m coined thus far • Unchangeable without a hard fork	• Monetary Policy based on Minimum Necessary Issuance • Ethereum's current yearly network issuance is approximately 4.5% with 2 Ether per block and an additional 1.75 Ether per uncle block (plus fees) being rewarded to miners. • **There is no fixed supply**

[1] There is no topic more charged than block size in Bitcoin, resulting in several high-profile and controversial disagreements resulting in hard forks, notably Bitcoin Cash.

APPENDIX C – VALIDATOR LIFECYCLE



Source: *https://notes.ethereum.org/7CFxjwMgQSWOHIxLgJP2Bw#A-note-on-Ethereum-20-phase-0-validator-lifecycle*