PoW to PoS Transition: Early Lessons from Ethereum's Merge

Abstract—**Ethereum is a decentralized technology that powers the cryptocurrency Ether and many other decentralized applications. It was launched in 2015 with a Proof of Work (PoW) consensus mechanism, in which miners compete to solve mathematical puzzles to validate transactions and add them to the blockchain. In 2020, Ethereum began its transition to a new consensus mechanism called Proof of Stake (PoS). This mechanism relies on validator nodes, rather than miners, to validate transactions and add them to the blockchain. Validator nodes are chosen based on the number of Ether (the native cryptocurrency of Ethereum) they hold and are willing to stake or lock up as collateral. The transition to PoS was initiated with the launch of the Ethereum 2.0 beacon chain, which coordinates the validator nodes' activities and manages the Ethereum blockchain's state. The transition to PoS is expected to provide several benefits, including increased scalability, reduced energy consumption, and improved security. This paper evaluates the transition from PoW to PoS by defining metrics that provide a basis for observing and analyzing these benefits. Our results attest to Ethereum's claims of the expected benefits and show that such a smooth transition is indeed possible and beneficial for other blockchains.**

I. Introduction

Blockchain technology has garnered significant attention in recent years as a potential solution to issues of trust and centralization in various industries. In particular, the development of decentralized, peer-to-peer (P2P) cryptocurrencies, such as Bitcoin and Ethereum, has introduced a new approach to the age-old problem of confidence in people and institutions.

Bitcoin, the first successful implementation of blockchain technology, was introduced in 2009. It utilizes a decentralized, open-source, immutable ledger that is append-only and employs cryptography to reduce security risks. A chain of hash references connects the blocks containing transactions, and the majority of blockchain holders' acceptance of newly proposed blocks determines whether a consensus can be established on the kinds of blocks and transactions that may be included in the blockchain [1]. This characteristic results in a system where the software is hardwired with consensus and participants in the consensus mechanism receive rewards.

Ethereum, another well-known decentralized cryptocurrency, was launched in 2015 with a Proof of Work (PoW) consensus mechanism. This mechanism relies on miners to complete complicated mathematical puzzles to validate transactions and add them to the blockchain. Over the years, Ethereum has undergone several iterations and updates, including the Homestead and Metropolis releases, which added additional functionality to the PoW blockchain.

In 2020, Ethereum began transitioning to a new consensus mechanism known as Proof-of-Stake (PoS). This mechanism relies on validator nodes, rather than miners, to validate transactions and add them to the blockchain. The transition was initiated with the launch of the Serenity Phase 0, which laid the groundwork for the Beacon Chain and validator nodes. The Beacon Chain ran parallel to the mainnet, and was used for testing and coordinating among validators, but did not support transactions, store user data, or execute smart contracts.

On September 15, 2022, the Beacon Chain was merged with the mainnet in an event known as "The Merge" [2]. This marked the end of Ethereum's PoW era and the official start of its PoS era, becoming the first-ever smooth protocol transition at such a scale, without any downtime. Thus, this observational study aims to provide an in-depth analysis of the claims made in favor of Ethereum's transition to PoS, in an effort to understand whether other cryptocurrency or blockchain models should make the same transition as well. To this end, we identify metrics that are essential to empirically understand the advantages and disadvantages of such a transition for blockchains in general.

This paper will analyze the Ethereum blockchain on various metrics before and after The Merge. The operation of the PoW and PoS consensus processes is covered in Section II. Section III describes the measures we'll use to evaluate the Ethereum blockchain's performance. The data sources and data gathering techniques that we employed in our article to analyze metrics like energy usage, total daily block rewards, and the number of validators joining the network in relation to the price of Ethereum are discussed in Section IV. Section V covers the possible danger of a 51% attack and focuses on the critical security vulnerabilities connected to centralization. We wrap up the impact of The Merge on the Ethereum blockchain in Section VI.

II. Ethereum

A. Background

The Merge is one of the most significant events in the history of blockchain technology. The redesigned system, dubbed "The Merge," will do away with the requirement for cryptocurrency miners and massive mining farms, who previously powered the blockchain via a system referred to as PoW. In its place, a PoS mechanism has been adopted, which randomly selects "validators" to approve transactions in exchange for a modest payment.

B. Proof of Work

PoW is a consensus mechanism that was first implemented by Satoshi Nakamoto to secure the Bitcoin network against double-spending attacks and to ensure the veracity of transactions without the need for a central authority. In the PoW system, miners are responsible for validating transactions and creating cryptographically-linked blocks through the use of hash functions. To create a block, miners must perform a significant amount of computational work as the block's hash must meet a certain threshold set by the network. This threshold is determined by the total network hash rate, which represents the combined computational power of all miners on the network. The process of creating a block is known as "mining." Once a block has been created, it is broadcast to other miners who verify its validity. If most miners confirm that the block is valid, it is added to the blockchain, representing the consensus reached within the network. Although PoW has been widely adopted to secure networks, it has also been criticized for its high energy consumption and slow consensus times.

C. Proof of Stake

The Ethereum blockchain recently switched from a PoW to a PoS consensus mechanism in an effort to address the shortcomings of PoW. In PoS, validators are chosen at random based on the amount of tokens they have staked on the network. This eliminates the need for energy-intensive puzzle-solving and incentivizes validators to act in the best interests of the network to maintain their stake and continue to be chosen as validators. The PoS consensus mechanism offers several advantages over PoW. It is more scalable, allowing the Ethereum network to process more transactions per second. It is also more energy efficient, requiring less electricity to power the validation process, leading to lower transaction fees and faster confirmation times for users. The transition from PoW to PoS has significantly improved the Ethereum blockchain in terms of scalability and energy efficiency, and has also eliminated the need for mining farms, addressing concerns about the environmental impact of the cryptocurrency industry.

D. Benefits of the merge

Since the integration, Ethereum's energy usage has dropped by 99 percent. Proof Stake gives network control to users who "stake" cryptocurrency on the network, rendering attacks both monetarily impossible and self-defeating. Moreover, staking is more accessible to regular Ethereum users than mining, which required a significant initial investment and labor to set up huge mining rigs to participate in the PoW consensus mechanism.

III. Evaluation Metrics

In this paper, we will analyze the Ethereum network using several metrics. The first metric we will examine is energy consumption. To measure this, we will analyze the average daily energy consumption of the Ethereum network before and after a specific event, such as the "merge," to compare the network's energy consumption at different points in time and understand how it has changed. The second metric we will analyze is total daily block rewards, which is the total amount of ETH rewarded to miners/validators on a daily basis. By tracking this metric, we can understand how rewards are distributed among network participants and how they may have changed over time.

The third metric we will analyze is the number of new validators entering the network, or what we will refer to as delta. We will compare this metric with the price of Ethereum on corresponding days to understand how changes in the number of validators may impact the price of the cryptocurrency. Finally, we will examine the degree of centralization in the Ethereum network by calculating the percentage of the top stake-holding entities whose stake amounts to 51% of the stake in the network. This allows us to understand the concentration of power within the network.

IV. Case Study

A. Data Collection

Since the paper compares the Ethereum blockchain before and after the merge, time-scale data has been collected from multiple credible sources. Data Collection methods include web scraping using python scripts and running SQL queries on the Dune analytical platform. The energy consumption data was scraped from digiconomist.net for May 1, 2022- Nov 25, 2022 [3]. The cumulative number of validators on the Beacon Chain smart contract were scraped from beaconscan.com for the time frame Dec 1, 2020, to Nov 26, 2022 [4]. The data for the price of Ethereum was extracted from ethereumprice.org for the time frame Dec 1, 2020, to Nov 26, 2022 [5]. Furthermore, the block creation reward data was scraped from etherscan.org for the time frame Dec 1, 2020, to Nov 26, 2022 [6]. Finally, the stake amounts of the top 1000 and top 11 stakeholders were retrieved from the Dune analytical platform [7] [8].

B. Graphs and Analysis

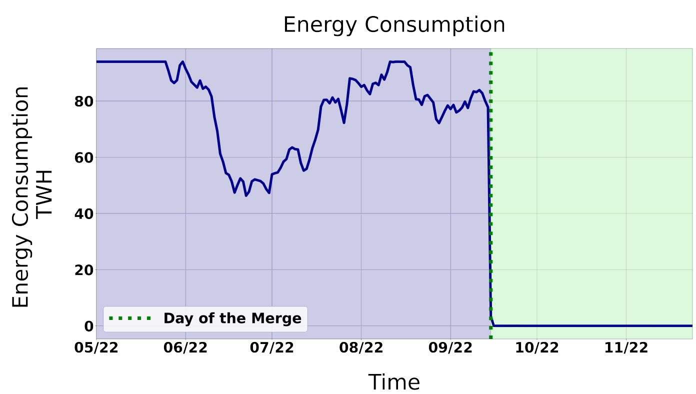

Fig. 1. Ethereum Energy Consumption

1) Energy Consumption: Fig1 displays Ethereum networks energy consumption before the merge, which stands at around 100 TWH which has now dropped to 0.014 TWH. This indicates a drop of 99.95% in the Ethereum network's energy consumption because a PoS system's energy consumption is much lower, as validators do not need to run resource-intensive mining equipment to participate in the consensus process.

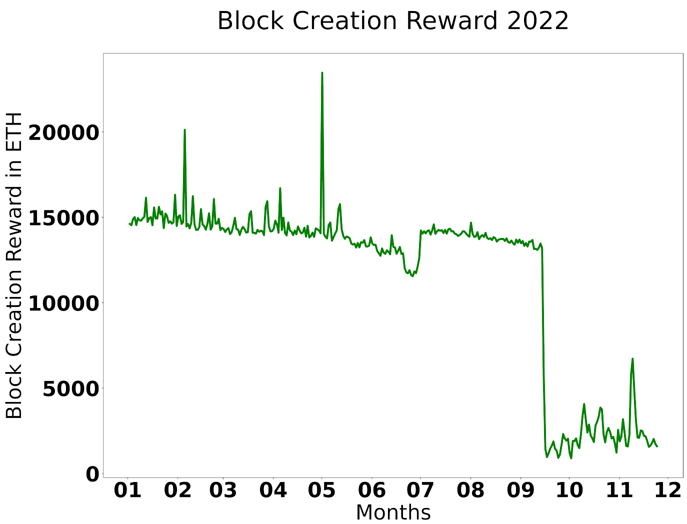

Fig. 2. Block Reward

2) Block Rewards: Under the PoW model, miners competed to solve complex mathematical puzzles to validate transactions and add them to the blockchain. The miner that successfully solved the puzzle received a reward of 2 ETH plus transaction costs. Under the PoS model, a validator is chosen randomly for every epoch, along with 127 attestors. The validator is responsible for verifying all transactions and including them in a block. As a result, the block reward has significantly decreased. For example, on September 14, 2022, the total block reward was 13,200 ETH, but on September 16, 2022, the day after the PoS transition, the total block reward dropped to 1,435 ETH. This shows an ≈89.13% decrease in the amount of Ether issued by the network over 48 hours, which is in accordance with Ethereum's claim of dropping the total new ETH issuance by ≈88.7%. Thus, if an average gas price of at least 16 gwei is observed for a given day, it effectively offsets the 1,700 ETH that is issued to validators and brings net ETH inflation to zero or less for that day. [9]. This drop in the block reward is a result of the change in the consensus mechanism and the elimination of miner fees.

The PoS model allows for improved scalability and energy efficiency, but it also requires a reduction in rewards for participating in the network. This is evident in the significant decrease in the block reward observed after the transition to PoS.

3) Validators in contrast to ETH Price: Fig. 3 compares Ethereum's price and the number of new validators entering the network daily. A general trend can be observed in the data, with the number of new validators entering the network increasing as Ethereum's price drops. This suggests an inverse relationship between Ethereum's price and the number of new validators entering the network.

One possible explanation for this relationship is that validators are confident in the recovery of Ethereum's price. As

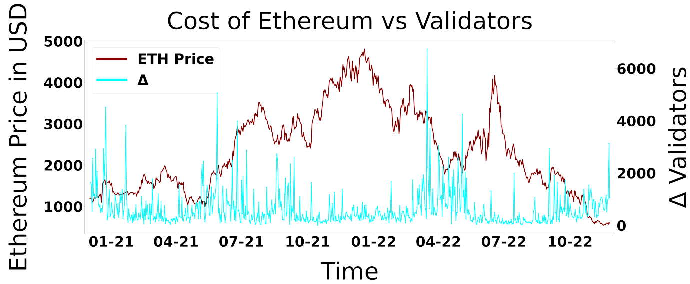

Fig. 3. Change in number of validators per day VS Ethereum prices

the price drops, validators may see it as an opportunity to buy and stake Ethereum at a lower cost, with the expectation that the price will eventually recover and their stakes will not go to waste. This trend is particularly evident in December 2021, and January 2022, when Ethereum's price was at its highest and the number of new validators entering the network was at its lowest.

Additionally, the influx of new validators may contribute to a spike in Ethereum's price as people buy Ethereum for staking purposes in addition to its use as a gas fee and investment following the switch to Proof-of-Stake (PoS). However, it is important to acknowledge this analysis's assumptions and potential limitations. One major assumption is that most of the new validators entering the network have bought Ethereum as the price dropped and did not hold their entire staked amount before the price decline. This assumption may not hold in all cases, and further research is needed to confirm the validity of this relationship.

Despite these limitations, the observed inverse relationship between Ethereum's price and the number of new validators entering the network is a significant finding that sheds light on the confidence that validators have in recovering Ethereum's price and their commitment to strengthening the network's security. This relationship holds important implications for the future of Ethereum and the broader cryptocurrency market.

4) Degree of Centralization: The use of staking pools in Ethereum has raised concerns about the potential for centralization. In late 2020, the rapid growth of Yearn.finance's yETH vault, which amassed over 137,000 ETH in its first day, sparked fears of a 51% attack. Although the maximum amount that a single validator can stake is 32 ETH, entities can operate multiple validator nodes that follow their rules and ideology, effectively functioning as a single large validator. This has led to concerns about the concentration of power in the hands of a few large staking pools. To assess this issue, we have analyzed the current distribution of stakes among staking pools, major exchanges, and standalone validators using data from the Dune Analytical Platform.

Figure 4 shows the division of market share held by the top 1000 stakeholders in the Beacon Chain smart contract. At the time of writing, LIDO DAO holds 29.3% of the total market share (37.7% of the total Ethereum staked by the top

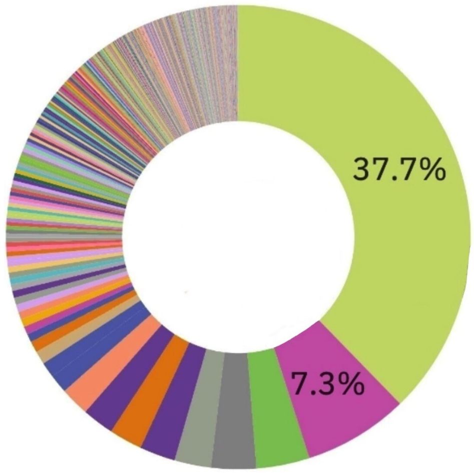

Fig. 4. Degree of Centralization

1000 stakeholders) followed by Kraken with 5.6% and so on.

TABLE I
MAJOR STAKE HOLDERS IN ETHEREUM

Entity	Stake (ETH)	Number of Validators	Marketshare(%)
LIDO	4605152	143911	29.30
Kraken	890624	27832	5.66
Staked.US	451904	14122	2.87
Figment	381952	11936	2.43
Kraken	310336	9698	1.97
Bitcoin Suisse	303968	9499	1.93
stakefish	280704	8772	1.78
0xeFE9a82d56cd965D7B332c7aC1feB15c53Cd4340	270144	8442	1.72
Binance 23	247488	7734	1.57
0xeEE27662c2B8EBa3CD936A23F039F3189633e4C8	158176	4943	1.00
0xFA5f9EAa65FFb2A75de092eB7f3fc84FC86B5b18	131584	4112	0.84
	8032096		**51.11**

Table 1 shows the top 11 stakeholding entities from 90,413 as of December 13, 2022. These entities hold over 51% of the total staked ether. Owing to the Annual Percentage Yield (APY), it is frequently argued that PoS is a rich-get-richer scheme because those with higher stakes will continue to compound their wealth and, if reinvested, will lead to increasing centralization [10]. However, it is to note that the APY is the same for all staking entities, and such compounding will apply to all such entities as well. This means that unless more Ethereum is bought and staked by any entity, the percentages in the table will remain constant.

V. DISCUSSION

This section discusses potential threats to Ethereum following its transition, which includes an analysis of increasing centralization and 51% attacks.

A. Increasing Centralization

As discussed above, the APY does not lead to increasing centralization as the percentage stakes remain constant (assuming that they are staked for the same amount of time). Then how exactly are larger stakeholders more likely to grow their stake faster than others if not by the yield?

The probability of being chosen to produce a block in an Epoch is directly proportional to the number of ETH staked, when chosen the validators can use MEV (Maximal Extractable Value) to maximize their block rewards. Maximal extractable value (MEV) is the value validators can extract from users through certain trading activities on decentralized exchanges. This extraction is facilitated by the settlement mechanism of decentralized ledgers, which allows orders to be organized in batches and exposed before they are settled. This allows validators to suggest a series of trades dependent on one another and to front-run other participants in the network.

One example of this is arbitrage across decentralized exchanges. Automated market makers (AMMs), a class of decentralized exchanges, allow users to purchase and sell tokens without the involvement of a third party. The market maker, a piece of code running on a blockchain, depends on arbitrageurs to return the token's price to the market price. However, validators can take advantage of this by front-running the arbitrageurs, executing their own transactions ahead of the arbitrageurs to benefit from the opportunity.

Validators can also engage in back-running or sandwich deals, where they place sell or buy orders after or before a transaction that affects the market price. These transactions are found using a complex algorithm and often have high gas fees to encourage instant block inclusion, resulting in the validator making a huge sum on each MEV block. In this way, they are able to extract value from other users on the network. It is important to note that this behavior is not necessarily malicious but rather a result of decentralized exchanges' design and the way transactions are settled on the underlying blockchain. MEV is often referred to as the "Invisible Tax" in crypto.

The entities with the higher market share will have more opportunities for MEV and generate greater revenue from MEV and transaction fees combined. When reinvested, this amount will allow the entities to grow their stakeholder percentage substantially, leading to increased centralization.

B. 51 Percent Attacks

One of the primary reasons for entirely shifting to a PoS protocol was the added inherent security which discourages 51% attacks (wherein a staking entity gains 51% of the total staked Ethereum and hence control over the network). There are two major guards against this: firstly, the attacker is a stakeholder – if the attack succeeds, then the value of Ethereum in the open market would drop as people would start to lose confidence in the protocol's security. (However, a potential profitable 51% attacking pattern called the Short-Selling Attack is still possible, which will be discussed in a later section). Thus, the value of the attacker's stake would drastically depreciate. The built-in stake-slashing mechanism is the second discouraging factor: the attacker's stake would be immediately slashed in the event of an attack. For other, more difficult-to-detect attacks, such as censoring other users, the community can coordinate on a minority UASF; UASF stands for User Activated Soft Fork, in which the attacker's funds are again largely destroyed.

For a 51% attack, the attacker needs 51% of the total Ethereum staked (which amounts to 12.9% of the Ethereum in circulation).

1) Recovery: Vitalik argues that a 51% attack would be easier to recover from in a PoS protocol [11]. In a proof-of-work system, if a chain gets 51% attacked, the only viable response in practice is to wait it out until the attacker loses interest. However, this does not address the possibility of a more dangerous type of attack called a spawn camping attack, where the attacker repeatedly attacks the chain with the goal of rendering it useless. Furthermore, a persistent attacker may easily make the chain permanently unusable. In fact, after the initial attack, the attacker's costs may become very low as honest miners will stop participating in the network due to the lack of rewards.

In contrast, a PoS protocol recovers much quicker as there is no explicit hard fork needed to 'delete coins' (in the case of automated slashing). Even a UASF recovers faster than a traditional PoW protocol recovery, as all that is required is coordinating on the USAF to select a minority block.

Overall, attacking a PoS chain the first time will be expensive for the attacker, and the community can recover within a few days. Subsequent attacks will also be costly, as the attacker will need to acquire new coins to replace the destroyed ones. This makes the game highly asymmetric and unfavorable for the attacker.

2) Short-Selling Attack: A short selling attack is a type of 51% attack that can be carried out on a proof-of-stake (PoS) based cryptocurrency. In this attack, the attacker first acquires a majority stake in the cryptocurrency by holding a large number of coins and staking them in the system. Next, the attacker carries out short selling, which involves selling a large amount of the cryptocurrency in the market, causing its market value to decrease. The attacker then proceeds to sabotage the cryptocurrency system, causing its market value to decrease further. Finally, the attacker buys back the cryptocurrency they shorted, gaining the value of the depreciation. This attack is profitable if the amount of cryptocurrency shorted is greater than the attacker's majority stake. Derivatives such as futures, options, and swaps can also be used in this attack, increasing the potential profit but also introducing additional risk [12]. However, this attack is highly unrealistic as it assumes that the attacker has enough ether to hold a 51% stake in the system along with holding enough Ether to short such that the profit made on the short from the price depreciation post-attack would be larger than the amount lost to slashing.

VI. Conclusion

In conclusion, the successful merge of the Beacon Chain and the Ethereum mainnet demonstrated the potential for a smooth transition from PoW to PoS. The transition has significantly changed the Ethereum environment, as there are no longer miners proposing or attesting to blocks as validators. According to some, staking could significantly increase Ethereum's security. Our results also show that the switch to PoS has significantly reduced energy consumption, making Ethereum more sustainable and appealing to investors who were previously concerned about the high energy demands of PoW. Additionally, the merge has paved the way for Ethereum scalability, as future phases promise to increase transaction throughput and bring Ethereum closer to traditional financial systems like Visa. Our paper also shows that the decrease in block rewards, due to the lower cost of running a node, has made the network more decentralized, as the financial overhead of operating specialized mining equipment is no longer a barrier to participation. We have further analyzed the stakes of major entities and found that even if one entity were to hold 51% of the stake, a 51% attack is highly unlikely and would be self-destructive. This further strengthens the argument for PoS over PoW and encourages more blockchains to shift to PoS. The influence of Ethereum PoS is not purely hypothetical, as Dogecoin, the 8th largest cryptocurrency in the world [13], has announced plans to shift from PoW to PoS, and we hope that many more will follow suit. [14]

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] "The merge." [Online]. Available: https://ethereum.org/en/upgrades/merge/what-is-the-merge

[3] "Ethereum energy consumption index," Dec 2022. [Online]. Available: https://digiconomist.net/ethereum-energy-consumption

[4] "statistics - validators — mainnet beacon chain (phase 0) ethereum 2.0." [Online]. Available: https://beaconscan.com/stat/validator

[5] "Ethereum price history - table, charts amp; csv," Feb 2020. [Online]. Available: https://ethereumprice.org/history/?start=2020-12-01amp;end=2022-11-26¤cy=USD

[6] "mining reward - ethereum (eth) mainnet chart." [Online]. Available: https://www.etherchain.org/charts/miningReward

[7] R. Rana, "Degree of centralisation," Dec 2022. [Online]. Available: https://dune.com/queries/1723718

[8] M. J. Iqbal, "Sum of top 11 stakes," Dec 2022. [Online]. Available: https://dune.com/queries/1773943

[9] "How the merge impacted eth supply." [Online]. Available: https://ethereum.org/en/upgrades/merge/issuance/

[10] "Is proof of stake a rich get richer scheme?" [Online]. Available: shorturl.at/krAH6

[11] J. Mapperson, "Vitalik buterin reveals why a 51% attack on eth 2.0 'would not be fatal'," Sep 2020. [Online]. Available: https://cointelegraph.com/news/vitalik-buterin-reveals-why-a-51-attack-on-eth-2-0-would-not-be-fatal

[12] S. Lee and S. Kim, "Short selling attack: A self-destructive but profitable 51% attack on pos blockchains," Cryptology ePrint Archive, Paper 2020/019, 2020, https://eprint.iacr.org/2020/019. [Online]. Available: https://eprint.iacr.org/2020/019

[13] "Cryptocurrency prices, charts and market capitalizations." [Online]. Available: https://coinmarketcap.com/

[14] "Dogecoin transition from proof-of-work to proof-of-stake: Why is it important?" [Online]. Available: https://cointelegraph.com/dogecoin-for-beginners/dogecoin-transition-from-proof-of-work-to-proof-of-stake-why-is-it-important