A survey on security of Proof-of-Stake (PoS) Ethereum

Seyyed Saeed Safai
sssafais@hotmail.com

***Abstract*—Ethereum, the second largest cryptocurrency market with a market cap of $190 trillion at the time of writing, has recently switched from using Proof-of-Work (PoW) to Proof-of-Stake (PoS) as the consensus mechanism. This transition helps the world to minimize the power consumption of maintaining a secure distributed ledger. As PoS has gained attention in recent years, security analyses of PoS have been less rigorous in comparison to PoW which has been on the market since the beginning of cryptocurrencies. In this paper, after a brief introduction to blockchain structure, PoS Ethereum or Ethereum 2 and its consensus mechanism in detail, we summarize security threats and attacks known to Ethereum 2 and discuss how they can be mitigated or how they are currently mitigated by patches. For each attack, we discuss the requirements for launching it and the impact of doing so. The paper concludes with an analysis of the current state of security of after-the-merge PoS-based Ethereum and the potential for further enhancements.**

***Index Terms*—Blockchain, Proof-of-Stake, Ethereum, Consensus security**

I. Introduction

A distributed ledger is made up of a network of nodes located throughout the world. There is a problem known as the "Byzantine fault" in such a system, which prevents all nodes in the network from reaching consensus regarding the state of the ledger. Bitcoin [1] as a decentralized digital currency was an implementation of BFT[1] which demonstrated the potential of blockchain technology. Following Bitcoin, Ethereum [2] created a brand-new blockchain that is designed to enable programmability over blockchains using Smart Contracts [3].

PoW[2] is the consensus mechanism used by Bitcoin, Ethereum (v1), and other early cryptocurrencies for reaching consensus on their blockchain networks. The consensus mechanism relies on the computational challenge of creating a new block of the blockchain. PoW networks require participants to solve a cryptographically challenging problem in order to create new blocks of transactions. The process is called "Mining". Participants are rewarded with a specific amount of the native currency. But in recent years, there has been an increasing interest in the PoS[3] consensus mechanism. As of today nearly 60% of top 10 cryptocurrencies without considering USD pegged coins are using a variant of the PoS consensus algorithm (Ethereum, BNB [4], Cardano [5], and Polygon [6]). Participants in PoS protocols contribute to the security of the network by depositing a part of their wealth into the network (staking) and placing their wealth at risk if they misbehave. Participants in turn are chosen based on their staked wealth and they are responsible for validating transactions and creating a new block. The first PoS-powered cryptocurrency was Peercoin [7]. Since mining is a computationally intensive activity, reducing energy consumption is one of the main reasons for this transition from PoW to PoS. According to [8] and [9], Bitcoin mining consumes more electricity than 157 countries.

Ethereum, the second most popular cryptocurrency in the world with a market cap of $190 trillion at the time of writing, recently changed its consensus mechanism from PoW to PoS. The upgrade was called "The Merge". There have been a lot of PoW protocols and as a result, lots of security analyses have been done on them, especially on Nakamoto Consensus variants [10]. PoS has gained attention in recent years, and security analyses have been less rigorous than analyses of PoW [11]. In this paper we contribute to this by describing the current after-the-merge security status of Ethereum.

The Section II will provide some preamble information about how the Ethereum 2's PoS consensus mechanism works. In Section III, different attacks on Ethereum 2 are discussed and how they can be countered. We conclude this paper by discussing the security status of Ethereum 2 as a leading PoS-based cryptocurrency.

II. Background

To have a better understanding of potential attacks that threaten Ethereum's new consensus mechanism we should have a basic understanding of how a blockchain works and how Ethereum 2 reaches consensus in its network. During the remainder of this section, a brief explanation of blockchain structure is provided, and then Ethereum 2's PoS-based consensus mechanism is discussed.

A. Blockchain

A blockchain can be imagined as a distributed append-only timestamped data structure. In a peer-to-peer network of anonymous nodes and without the need for any trusted third party, blockchains allow peers to have reliable interaction with each other [12]. In essence, a blockchain is a chain of blocks that contain a list of transactions. Typically, transactions involve an asset exchange between the participants or a transition in the state of the network initiated by a participant (e.g., a change in the value of a variable). They are signed by one of the participants using their private key. Full nodes

[1] Byzantine fault tolerance
[2] Proof-of-Work
[3] Proof-of-Stake

(miners in PoW or block proposers in PoS) are the ones who are responsible for wrapping new transactions into the next blocks. In Figure 1 an abstract structure of a blockchain is shown. The Genesis block is the first block on a blockchain, which is trusted by all nodes by default. Each node in the network can verify all blocks in a branch starting with the Genesis block.

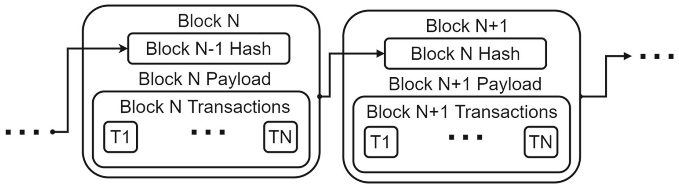

Fig. 1. A simplified blockchain data structure. Each block is securely linked to the previous block by the cryptographic hash [13].

All nodes, each with a different view of the network, should reach an agreement called "consensus". They should all agree on which blocks and transactions are valid and should be kept in the chain. As stated before, different types of consensus are available. Two of the most popular mechanisms are PoW and PoS. In PoW, miners try to mine the next valid block faster than others. The first valid block is appended to the chain by participants based on a rule e.g., the "longest chain" rule in Bitcoin. The miner who proposed the block will be rewarded with a specific amount of the native currency (BTC in Bitcoin). On the other hand, in PoS there are some minters or validators. They can participate in the consensus algorithm by staking a portion of the native currency in the network. They can propose or validate blocks based on some rules.

The ledger output by a consensus protocol should have these properties to be called as secure [14]:

1) Safety
The ledgers output by two honest validators at different times are consistent with each other.
2) Liveness
Valid transactions will eventually be confirmed by honest validators.

B. Ethereum 2

In PoS Ethereum, security is provided using its native cryptocurrency, Ether (ETH). Participants or validators who wish to contribute to the security of the chain must deposit 32 ETH into a specific smart contract on Ethereum. When the validator acts dishonestly or lazily, the staked ETH can be destroyed. The validator is responsible for checking the validation of new blocks proposed and sometimes creating and propagating new blocks over the network [15]. The validator could be in one of the following states [16]:

1) Deposited
The validator deposited some Ethers into the contract.
2) Eligible to be activated (Pending)
If the Ethers deposited meet the 32 Ethers limit, the validator is added to a queue to be activated.
3) Activated
It should take some time for the validator to be activated and to participate in the consensus protocol.
4) Slashed
The validator will be punished and slashed for misbehaving. They are forced into the exit queue and cannot withdraw for 36 additional days from when they exit.
5) Exited
The validator has exited.
6) Withdrawable
Validators can withdraw their Ethers following a specific delay after exiting.

Ethereum 2's consensus mechanism consists of two main components: the HLMD-Ghost[4] [17] fork choice algorithm and the Casper FFG[5] [18] as a finality gadget on top. The combination of these two parts is known as "Gasper" and the original version of it was described at [17]. To put it simply, the Ethereum consensus protocol works in two stages and on two different timescales.

Based on [19], time in Ethereum is divided into epochs, each containing 32 slots. Each slot's duration is 12 seconds and consequently each epoch lasts 6 minutes and 24 seconds. Validators are shuffled into 32 committees each containing 64 subnets of validators (at most). An epoch's slots are allocated to committees in order. The first validator of a committee is the block proposer and should wrap new valid transactions into a block. Then other members of the committee should release their vote as an "attestation". Attestations consist of voting for 3 blocks:

1) Source EBB[6]
2) Target EBB
3) The head of the chain

The first block of each epoch is an EBB. In simple terms, source EBB is the most recent ıjustified block in the canonical chain of the validator and target EBB is the first block in the current epoch. HLMD-Ghost vote is the part of the vote that corresponds to the head of the chain, while Casper FFG vote is the part of the vote that corresponds to the EBB blocks. In Casper FFG, an EBB block upgrades to "justified" if a supermajority of validators (2/3 of them) votes for it to be a target EBB. And a justified block converts to a "finalized" block if it is voted a source EBB by a supermajority. A finalized block is considered to be unchangeable because reaching a finalized block requires a two-step supermajority of validators. There is no doubt that these block upgrades occur every epoch. An example of Casper FFG is illustrated in Figure 2. The output of Casper FFG is fed to HLMD-Ghost to determine the head of the chain in each slot. In HLMD-Ghost, the head of the chain is determined by calculating the accumulated staked ether of attestations of a given block and its descendants. Instead of calculating the weight, starting from the genesis block, it is calculated from the most recent justified block (Hybrid part of HLMD). For each validator, just count

[4] Hybrid Latest Message Driven Greedy Heaviest Observed SubTree
[5] Friendly Finality Gadget
[6] Epoch Boundry Block

its latest vote (LMD). A leaf block with the most weight is the head of the chain (Ghost). A proposer using HLMD-Ghost determines the head of the chain and appends a new block to it. Similarly, the calculation is done by the validators too for creating an attestation. An example of HLMD-Ghost is shown in Figure 3.

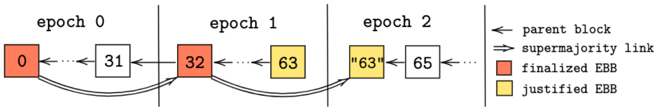

Fig. 2. The process of justification and finalization for the first three epochs. Since the EBB of epoch 2 is not produced, the highest block of the canonical chain with slot < 2 is borrowed as the EBB of epoch 2 [20].

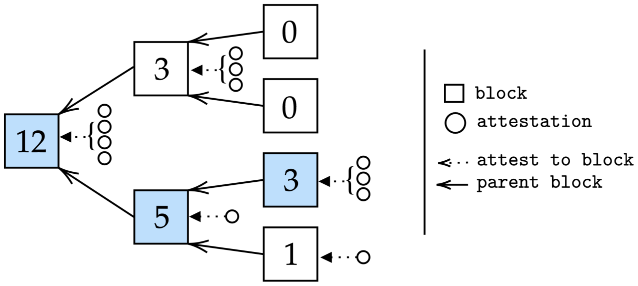

Fig. 3. The result of running HLMD-Ghost to choose one of four conflicting leaf blocks. The blue blocks are the heaviest at each fork [20].

We should mention a few points about Gasper here. A validator should create and broadcast an attestation if one of these two conditions is met:

1) A valid block created by the proposer of the slot is received.
2) 1/3 of the slot (4 seconds) is passed.

During the slot period, blocks received in the first third of their own slot are boosted by 40%. Equivocating validators' attestation is removed from the fork choice algorithm. Any changes to the latest justified EBB are allowed in the first 1/4 slots of an epoch.

One of the most compelling features of Ethereum's PoS mechanism is the incentives and slashing system used to motivate people to participate in consensus, improve security, and penalize misbehaving validators. When an honest validator participates in proposing and validating blocks, they are rewarded and some Ethers are added to their stake. On the other hand, missing Casper FFG votes is punished with the same amount of the potential reward for the same action. In addition to that, misbehaved validators are punished during an action called "slashing". Slashing occurs when one of the actions bellow is done by the validator [15]:

1) Proposing and signing two different blocks for the same slot.
2) Attesting to a block that surrounds another one in a way that effectively changes the history.
3) "Double voting" by attesting to two candidate blocks for the same slot.

If a validator gets slashed, immediately 1/32 of their stake (up to 1 ETH) is burned and they are forcefully exited from the chain with an additional 36 days delay before being able to withdraw. During this period their stake gradually bleeds away. On day 18 an additional penalty named "correlation penalty" is applied whose magnitude is scaled by the total staked Ether of all slashed validators on the same day that the validator was slashed. Last but not least, another penalization mechanism is "inactivity leak". If 1/3 of the validators are offline or vote against the majority, preventing the Beacon Chain from finalizing for more than four epochs, the inactivity leak mechanism is activated. It gradually eliminates the stakes of the minority in order to allow the network to achieve finality. Validators with less than 16 ETHs are forcefully exited.

III. Attacks and Defenses

Security issues associated with PoS have gained increased attention since Ethereum began working on switching from a PoW consensus protocol to a PoS consensus protocol in 2019. As we discussed in Section II, some basic considerations have been taken into account to limit typical attacks like Sybil and long Reorg attacks as much as possible. Based on how attacks target Ethereum 2, we may categorize them as follows:

1) Layer 0-targeted
2) Cryptography-targeted
3) Protocol-targeted

As we continue through this section, we will discuss each type of attack in greater detail and how they can be mitigated.

A. Layer 0-targeted attacks

As Ethereum is a community-based cryptocurrency, the social layer or "Layer 0" is a potential attack surface. An attack of this kind can be performed by a group of people with virtually no knowledge of Ethereum's design. These attacks usually aim to undermine public trust in Ethereum and devalue Ether. If there is a successful protocol attack, a layer 0 attack makes it more challenging for the community to respond quickly to the attack out-of-band. This type of attack could take several forms, including: misinformation or negative deliberate advertisements, intimidation of the developer community, over-zealous regulation, malicious actors among the developer community, bribery of key players, etc [21].

Defending against layer 0 attacks is not straightforward. It requires a comprehensive understanding of the community and social psychology. There are several basic principles that can be considered in order to prevent the occurrence of a large scale layer 0 attack. These include maintaining a high signal to noise ratio for public information about Ethereum in social networks, having a clear governance protocol and mission statement, being open to new members of the community, etc [21].

B. Cryptography-targeted attacks

Two main elements are widely used in blockchains such as Ethereum: Hash functions and Digital signature schemes. The security of transactions is provided by digital signature schemes, and the integrity of blockchains is ensured by the one-way nature of hash functions. Unfortunately, the security of both is threatened by the evolution of quantum computers. The theory of quantum algorithms has grown dramatically in the 20 years since Shor's discovery [22]. Grover's [23] and Shor's [24] algorithms are two well-known quantum algorithms that threaten Ethereum's security.

In the case of digital signature schemes, public-key cryptosystems are used. A transaction is signed by the private key of the sender and is verified by the corresponding public key attached to the transaction. Ethereum 2 uses BLS signature scheme [25] which its security relies on the hardness of ECDLP[7]. Shor's algorithm on a sufficiently powerful quantum computer can solve ECDLP in polynomial time of the input size. The fastest known classical algorithm to solve the same problem takes a sub-exponential time [3]. Based on [26], for breaking an ECDLP with a 384-bit prime, 3484 qubits are required. As of writing, such a powerful quantum computer isn't available: the most powerful quantum computer has only 433 qubits named Osprey created by IBM [27]. But based on the roadmap published by IBM [28], we can expect a 384-bit ECDLP break-capable quantum computer by the end of 2025.

In contrast to digital signature schemes, hash functions are considered to be more resistant to quantum algorithms as they are an NP-hard problem [29]. Grover's search algorithm can provide a quadratic speed-up for brute-forcing a hash. By using Grover's algorithm, an attacker can replace a block on the blockchain without affecting its integrity.

Hash functions can remain as secure as before by doubling their key size. But in the case of digital signature schemes, they should be replaced by quantum-resistant equivalents. Post-quantum cryptography standardization was announced by NIST[8] at 2016. The competition is currently in its round 4 [30] and 4 winners have been announced so far for standardization [31]. The conclusion of NIST's competition can be the first step for the Ethereum community to start its transition to post-quantum algorithms, as discussed in [32]. Despite the fact that we have neared the end of the competition, none of the post-quantum algorithms selected are as good as the classic ones in terms of performance, signature size, or key size.

C. Protocol-targeted attacks

Protocol-targeted attacks can usually have three main effects: reorg, double finality, and finality delay.

Reorg attacks are in a way that create changes in the chain, reordering the blocks or adding/removing blocks to/from it. They can be used to do double spending, providing more time to adversary for front-running and back-running transactions to extract value (MEV[9] [33]), or censoring. Two types of reorgs exist; $expost$ reorgs which target known old blocks and $exante$ reorgs which target unknown future blocks.

Double finality can occur in rare cases when two parallel forks get finalized. Creating a permanent branch in the chain.

Finality delay prevents the chain from advancing the finalized block forward. Reducing the trust on financial operations on the network. These attack usually are aimed to disrupt Ethereum more than profiting.

In following we discuss different attacks proposed until now and how they have been mitigated or can be mitigated.

1) Mitigated attacks: Up to now, different attacks have been reported, and in response, the Ethereum community has patched them. Most of the reorg attacks were a result of under-activity (not proposing/attesting or doing it late) or over-activity (equivocating). The initial reorg attacks were proposed using 30% of the staked Ether [20] and then they were demonstrated to be much easier using only 2% of the stakes [34] or even a single validator [14] instead [21]. Most of the reorg attacks with lower stakes were designed as a balancing attack. A balancing attack produces a split view of the chain for validators. Two blocks are proposed, and the network is managed so that half of the validators attest to one and the other half attest to the other. In order to manage validators' votes in this manner, adversaries should have fine-grained control over the network, or at least a probabilistic one. In balancing attacks finality is not achieved as none of the blocks attract more than 2/3 of the votes (finality delay). This enables the attacker to do relatively long reorg whenever they want to stop the network from being balanced. There was a preconceived notion that having fine-grained control over the network is not practical in real-world scenarios [35], but [14] showed that an adversary with 15% stake in the network can stall Ethereum using probabilistic delays; the adversary can calculate a T_{delay} up to which a message is seen by x fraction of the network. A solution called "proposer boosting" was later suggested in [35] and implemented in [36] to mitigate these balancing attacks [14], [20], [34], [37] by encouraging proposers and validators to get their jobs done in a timely manner, which gives them a boost on the score of the block in its own slot. As the mentioned attacks all relied on under-activity, they became unpractical for low-stake adversaries. However, as explained in [38], being the proposer for multiple slots in a row can help the adversary to bypass the proposer boosting and land their attack successfully. The most recent attack mentioned in [11] showed how the proposer boosting can be exploited by an adversary to create a permanent split view of the chain for validators. This attack was mitigated by [39] being merged into Ethereum, filtering out equivocations in the fork-choice algorithm at all. In general, with more stakes, you have a greater chance of launching a successful attack. In Figures 4 and 5 borrowed from [38], the amount of stake required to land a balancing, ex ante reorg, or ex ante sandwich reorg attack in presence of the proposer boosting is demonstrated.

Another type of attack proposed was the "bouncing attack" mentioned in [40], [41]. Due to the attack mentioned in [41], validators were being switched between two forks because of the newer justified blocks, preventing the network from reaching finality. [42] was first suggested and then implemented in [43] to mitigate this attack, preventing the change in the latest

[7] Elliptic Curve Discrete Logarithm Problem

[8] National Institute of Standards and Technology

[9] Maximal Extractable Value

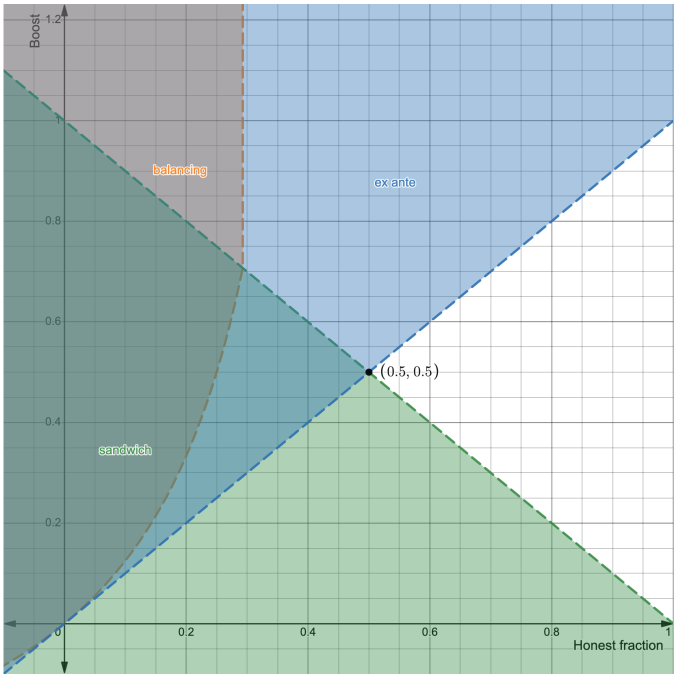

Fig. 4. The proposer boosting resistance to attacks when the adversary controls only one block.

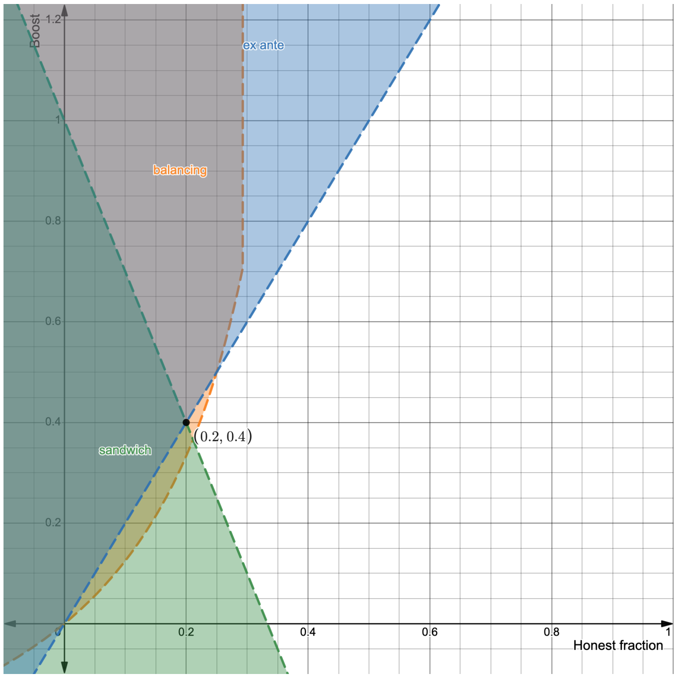

Fig. 5. The proposer boosting resistance to attacks when the adversary controls two blocks in a row.

justified block after the first 1/4 slots of an epoch. The attack in [40] less severe by the merge of [44] and got fully mitigated by the proposer boosting.

2) Low-cost finality delay attack: There is a finality delay attack presented in [20] which is not mitigated yet. In this attack, the adversary needs to control the first few blocks of an epoch to unleash their attack. Consider the situation where the adversary holds 30% of the total stake. We can calculate that such an attacker just needs 2 first slots of an epoch to delay finality. Attestations and the first two blocks will be withheld. Honest members select the latest block of the previous epoch as their target EBB. At the end of the second slot, the adversary releases their hidden blocks. As a result, honest members now recognize the first block of the adversary as the target EBB. If the adversary controls enough initial slots of the epoch (2 for 30% stakes) they can create a situation that results in no EBB blocks being chosen as justified as none of them have 2/3 of the votes. This attack is illustrated in Figure 6.

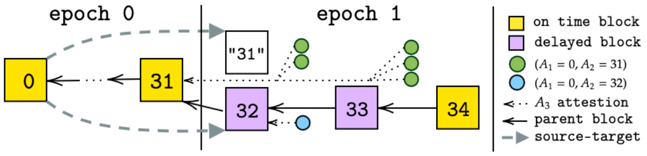

Fig. 6. An attacker who uses the delayed release of blocks 32 and 33 to prevent epoch 1 from being justified. At first, honest validators chose block 31 as their target in their Casper FFG vote. But after the release of block 32 and 33 with an additional attestation, they will choose block 32 as the EBB of epoch 1. By the adversary withholding its remaining attestations, no supermajority link between 0 and 31 or 0 and 32 will be formed and epoch 1 is never justified [20].

An adversary with 30% of the total stake has 0.09 probability of being picked in the 2 first slots of an epoch. They can launch this attack every 1 hour, each time delaying the finality for 2 epochs at a cost of only $100.

The open pull request [45] is for solving this specific attack. It changes the hierarchy of the chain in a way that attestations are attached to "nodes" instead of "blocks". It results in a new node for the EBB referencing the previous block but having newly created attestations on it. This prevents the attack by requiring it to reorg the node to change the EBB. Figure 7 demonstrated the enhanced structure used to mitigate this attack.

3) DoS attack: In Ethereum 2 the proposer of each slot is determined by a public function. It is possible for an adversary to determine beforehand which validator is the proposer of a future block by using this function. They can launch a DoS[10] attack at that point in time in order to prevent the proposer from communicating with other nodes. In other nodes' view, the proposer is offline and no block is being proposed for the slot. This could be a form of censoring against a specific validator [21]. Some tricks on the client side can be done to escape these types of attacks, like separating the block proposition from communication and having multiple nodes

[10] Denial of Service

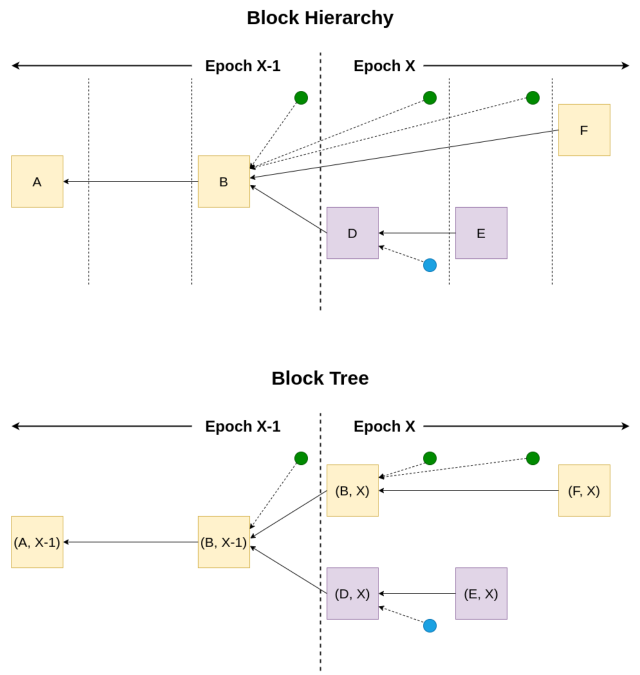

Fig. 7. The newly proposed structure to mitigate the finality delay attack mentioned in [20] [45].

with different purposes. On the protocol side, suggestions like SSLE[11] [46], [47] or NSSLE[12] [48] are being discussed which keep the proposer/proposers hidden from other members of the network. We can expect a similar solution to be implemented in the future.

4) *Attacks using > 33% of the total stake:* 33% can be a milestone for an attacker in their pursuit of success. According to [49], reaching this level requires about $8.4 billion or 5,503,970 ETH. After reaching 33% of the total stake, in addition to the previous attacks, the attacker can easily stall Casper FFG by being inactive. However after 4 epochs, the inactivity leak will be enabled to penalize the attacker. Based on the chart in [50], for an attacker to stall Ethereum for 100 epochs, costs $(32 - 31.987) * 172,000 = 2236ETH = \$3.4million$ which can't be considered a low cost. By having more than 50% of the total stake, an attacker can freely censor specific blocks and extract maximum MEV by doing ex ante reorgs. At the level of more than 66%, an attacker gains the power to do ex post reorgs and finalize any blocks they want.

5) *Shorting attack:* In [51], Vitalik Buterin has described PoS design philosophy as bellow:

> *The one-sentence philosophy of proof of stake is thus not security comes from burning energy, but rather security comes from putting up economic value-at-loss.*

However having an economic layer of defense is a smart way to prevent lots of large scale attacks, but in [52] is shown that it is not enough; an attacker can still benefit from a sabotage attack on Ethereum despite the fact that Ethereum itself gets destroyed.

Consider an attacker who opens a leveraged short position before launching the attack, then launches a sabotage attack on the protocol. An attacker purchases shorted cryptocurrencies for the purpose of returning borrowed assets when the price of the cryptocurrency drops sufficiently. The change is the profit the attacker has gained from the short position. The attacker has succeeded if the gain from the short position is greater than the loss from slashing and depreciation. This attack is named "shorting attack" in [52].

For Ethereum, we assume that the attacker has 1/3 of the total stake to be confident of success. [53] ran a simulation for different stake fractions, depreciation rate, and slashing rate. They showed that in some conditions this attack can be profitable for the attacker. This is especially true when they are using a small fraction of the total stake to launch the attack or the depreciation rate is high. As discussed in III-C4, at least $8.4 billion is required to reach 1/3 of the total stake.

In the papers mentioned, it is assumed that the attacker is using cryptocurrency exchanges to create a leveraged short position. This assumption is not necessarily correct, since most exchanges limit the contract size of positions to the order of millions. This is far away from the order of billions the attacker should be using. However, if rumors about the recent attack on UST, Terra's USD-pegged token [54], were true, the attacker had loaned 100 thousand BTCs (roughly $4 billion at that time) and opened a short position, which resulted in a $1 billion profit for them. Based on these rumors it seems that there are some ways to pull off this huge leveraged short position.

Different attacks have had different effects on the native token of the cryptocurrency system. The attack on Terra resulted in a 99% depreciation of Luna, the native coin of Terra, in just 5 days. On the other hand, the 2022 attack launched on Ethereum Classic [55] resulted in a 38% drop in a month [52].

6) *People: the last line of defense:* As discussed earlier, Ethereum is still vulnerable to some attacks, despite their difficulty and complexity. In severe cases where an attack is successful on Ethereum, the community is the last line of defense. The community should coordinate its way out of the crisis and prepare an emergency response. What is the most appropriate way to penalize the attacker? What should be the next step after an attack? Should we roll back the transaction after the attack? Or should we continue to use the dishonest fork? These are the questions that should be answered by the community in the event of a successful attack. In the Ethereum community, there has been steady discussion about how to recover from an attack [56]–[58]. Discussing solutions helps the community develop a coordinated mitigation plan quickly.

[11] Single Secret Leader Elections
[12] Non-Single Secret Leader Elections

IV. Conclusion

As the leading PoS-based cryptocurrency, Ethereum 2 has been under review by the community for the last few years. There have been so many attacks that have been suggested and patched so far. We have discussed the design structure of Ethereum 2 and it is clear that the design is complex in order to be immune to a wide range of attacks. Ethereum 2 is not unbreakable and is vulnerable to a handful of attacks, as shown earlier. A number of them are complex and require a number of conditions to be met, while others require a large amount of collateral to be put at risk. Currently, no method exists for attacking Ethereum with a small fraction of the stake, and the methods that have been suggested have been mitigated. But with a higher stake, it is still possible to unleash an attack with a high probability of success. However, the minimum collateral needed for such an attack is in the order of billions, which is not something everyone could handle. Both economic and technical defensive measures are preventive elements that make a successful attack more challenging. However, in the event of a successful attack, the community should step in and prepare a quick emergency response.

Due to the high degree of complexity Ethereum 2 has achieved right now and the fundamental problems that can be addressed to it [11], some researchers have proposed a new, simpler protocol to be used instead of the Gasper-based protocol Ethereum 2 currently uses. The proposed protocol is called "Goldfish" [59] and can be considered a viable alternative that may gain more attention in the near future.

References

[1] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008.

[2] V. Buterin *et al.*, *A next-generation smart contract and decentralized application platform*, 2014.

[3] A. M. Khalifa, A. M. Bahaa-Eldin, and M. A. Sobh, “Quantum attacks and defenses for proof-of-stake,” in *2019 14th international conference on computer engineering and systems (ICCES)*. IEEE, 2019, pp. 112–117.

[4] B. team, *BNB chain whitepaper*, 2020.

[5] C. Hoskinson, *Why we are building Cardano*, 2020.

[6] J. Kanani, S. Nailwal, and A. Arjun, *Matic whitepaper*, 2021.

[7] S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” *self-published paper, August*, vol. 19, no. 1, 2012.

[8] (2023, 1) Bitcoin energy consumption index. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption

[9] (2023, 1) How many countries are there in the world? [Online]. Available: https://www.worldometers.info/geography/how-many-countries-are-there-in-the-world/

[10] R. Zhang and B. Preneel, “Lay down the common metrics: Evaluating proof-of-work consensus protocols’ security,” in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 175–192.

[11] J. Neu, E. N. Tas, and D. Tse, “Two more attacks on proof-of-stake ghost/ethereum,” in *Proceedings of the 2022 ACM Workshop on Developments in Consensus*, 2022, pp. 43–52.

[12] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, “A survey on long-range attacks for proof of stake protocols,” *IEEE Access*, vol. 7, pp. 28 712–28 725, 2019.

[13] G. A. F. Rebello, G. F. Camilo, L. C. Guimaraes, L. A. C. de Souza, G. A. Thomaz, and O. C. M. Duarte, “A security and performance analysis of proof-based consensus protocols,” *Annals of Telecommunications*, pp. 1–21, 2021.

[14] C. Schwarz-Schilling, J. Neu, B. Monnot, A. Asgaonkar, E. N. Tas, and D. Tse, “Three attacks on proof-of-stake ethereum,” in *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*. Springer, 2022, pp. 560–576.

[15] (2023, 1) Pos ethereum documentations. [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[16] (2023, 1) Pos ethereum validators lifecycle. [Online]. Available: https://notes.ethereum.org/7CFxjwMgQSWOHIxLgJP2Bw

[17] V. Buterin, D. Hernandez, T. Kamphefner, K. Pham, Z. Qiao, D. Ryan, J. Sin, Y. Wang, and Y. X. Zhang, “Combining ghost and casper,” *arXiv preprint arXiv:2003.03052*, 2020.

[18] V. Buterin and V. Griffith, “Casper the friendly finality gadget,” *arXiv preprint arXiv:1710.09437*, 2017.

[19] (2023, 1) Ethereum specifications. [Online]. Available: https://github.com/ethereum/consensus-specs/tree/v1.2.0

[20] M. Neuder, D. J. Moroz, R. Rao, and D. C. Parkes, “Low-cost attacks on ethereum 2.0 by sub-1/3 stakeholders,” *arXiv preprint arXiv:2102.02247*, 2021.

[21] (2023, 1) Ethereum pos attack and defense. [Online]. Available: https://mirror.xyz/jmcook.eth/YqHargbVWVNRQqQpVpzrqEQ8IqwNUJDIpwRP7SS5FXs

[22] Z. M. Khalid, S. Askar *et al.*, “Resistant blockchain cryptography to quantum computing attacks,” *International Journal of Science and Business*, vol. 5, no. 3, pp. 116–125, 2021.

[23] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[24] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[25] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the weil pairing,” *Journal of cryptology*, vol. 17, pp. 297–319, 2004.

[26] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, “Quantum resource estimates for computing elliptic curve discrete logarithms,” in *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II 23*. Springer, 2017, pp. 241–270.

[27] (2023, 1) List of quantum processors. [Online]. Available: https://en.wikipedia.org/wiki/List_of_quantum_processors

[28] (2023, 1) The ibm quantum development roadmap. [Online]. Available: https://www.ibm.com/quantum/roadmap

[29] T. M. Fernandez-Carames and P. Fraga-Lamas, “Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks,” *IEEE access*, vol. 8, pp. 21 091–21 116, 2020.

[30] (2023, 1) Round 4 submissions. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions

[31] (2023, 1) Selected algorithms 2022. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

[32] (2023, 1) Nist post-quantum-cryptography standardization process and what it means for ethereum. [Online]. Available: https://crypto.ethereum.org/blog/nist-pqc-standard

[33] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, “Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability,” in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 910–927.

[34] J. Neu, E. N. Tas, and D. Tse, “Ebb-and-flow protocols: A resolution of the availability-finality dilemma,” in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 446–465.

[35] (2023, 1) Proposal for mitigation against balancing attacks to lmd ghost. [Online]. Available: https://notes.ethereum.org/@vbuterin/lmd_ghost_mitigation

[36] (2023, 1) Proposer lmd score boosting. [Online]. Available: https://github.com/ethereum/consensus-specs/pull/2730

[37] J. Neu, E. N. Tas, and D. Tse, “The availability-accountability dilemma and its resolution via accountability gadgets,” in *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*. Springer, 2022, pp. 541–559.

[38] (2023, 1) Proposer boost considerations. [Online]. Available: https://notes.ethereum.org/@casparschwa/H1T0k7b85

[39] (2023, 1) Remove equivocating validators from fork choice consideration. [Online]. Available: https://github.com/ethereum/consensus-specs/pull/2845

[40] K. Otsuki, R. Nakamura, and K. Shudo, "Impact of saving attacks on blockchain consensus," *IEEE Access*, vol. 9, pp. 133 011–133 022, 2021.

[41] (2023, 1) Analysis of bouncing attack on ffg. [Online]. Available: https://ethresear.ch/t/analysis-of-bouncing-attack-on-ffg/6113

[42] (2023, 1) Prevention of bouncing attack on ffg. [Online]. Available: https://ethresear.ch/t/prevention-of-bouncing-attack-on-ffg/6114

[43] (2023, 1) Bounce attack resistance. [Online]. Available: https://github.com/ethereum/consensus-specs/pull/1465

[44] (2023, 1) Decoy flip flop resistance. [Online]. Available: https://github.com/ethereum/consensus-specs/pull/1466

[45] (2023, 1) (block, epoch)-fork choice. [Online]. Available: https://github.com/ethereum/consensus-specs/pull/2292

[46] D. Boneh, S. Eskandarian, L. Hanzlik, and N. Greco, "Single secret leader election," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020, pp. 12–24.

[47] (2023, 1) Whisk: A practical shuffle-based ssle protocol for ethereum. [Online]. Available: https://ethresear.ch/t/whisk-a-practical-shuffle-based-ssle-protocol-for-ethereum/11763

[48] (2023, 1) Secret non-single leader election. [Online]. Available: https://ethresear.ch/t/secret-non-single-leader-election/11789

[49] (2023, 1) Open source ethereum explorer. [Online]. Available: https://beaconcha.in/

[50] (2023, 1) Upgrading ethereum: A technical handbook on ethereum's move to proof of stake and beyond. [Online]. Available: https://eth2book.info/bellatrix/part2/incentives/inactivity/

[51] (2023, 1) A proof of stake design philosophy. [Online]. Available: https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

[52] S. Lee and S. Kim, "Proof-of-stake at stake: predatory, destructive attack on pos cryptocurrencies," in *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 2020, pp. 7–11.

[53] ——, "Shorting attack: Predatory, destructive short selling on proof-of-stake cryptocurrencies," *Concurrency and Computation: Practice and Experience*, p. e6585, 2021.

[54] (2023, 1) Terra money: Stability and adoption. [Online]. Available: https://terra.money/Terra_White_paper.pdf

[55] (2023, 1) The ethereum classic foundation. [Online]. Available: https://ethereumclassic.org/knowledge/foundation

[56] (2023, 1) Timeliness detectors and 51[Online]. Available: https://ethresear.ch/t/timeliness-detectors-and-51-attack-recovery-in-blockchains/6925

[57] (2023, 1) Responding to 51https://ethresear.ch/t/responding-to-51-attacks-in-casper-ffg/6363

[58] (2023, 1) The pow vs. pos debate | lyn alden & justin drake. [Online]. Available: https://youtu.be/1m12zgJ42dI?t=1712

[59] F. D'Amato, J. Neu, E. N. Tas, and D. Tse, "No more attacks on proof-of-stake ethereum?" *arXiv preprint arXiv:2209.03255*, 2022.