UNIVERSITÉ DE GENÈVE

ADVANCED SECURITY
14X040

Understanding Proof-of-Stake and its Security Implications through the Example of Ethereum 2.0

Author: Dany A. DARGHOUTH

E-mail: dany.al-moghrabi@etu.unige.ch

May 2024

UNIVERSITÉ
DE GENÈVE
FACULTÉ DES SCIENCES
Département d'informatique

Summary

The grammar, spelling and formatting of this report have been reviewed using AI tools such as Quillbot and Grammarly, explaining a possible high detection score when using AI detection tools.

1. Introduction

This report explores the concept of blockchain technology, specifically focusing on the hybrid consensus mechanism utilized by Ethereum as it transitions from Proof of Work (PoW) to Proof of Stake (PoS). The primary goal of this project is to understand the vulnerabilities associated with this hybrid system, which combines elements of both PoW and PoS mechanisms. As blockchain technology continues to evolve, understanding these vulnerabilities is crucial for improving the security and efficiency of future implementations.

To provide a practical perspective on the theoretical vulnerabilities discussed, this report is accompanied by Python-based implementations that simulate potential security breaches within a simplified model of a hybrid blockchain system. These demonstrations are intended to offer insights into how such vulnerabilities can be exploited and, consequently, how they might be mitigated.

This report as well as the latest version of the accompanying code, and presentation slides can be found on the following GitLab repository:
https://gitlab.unige.ch/Dany.Al-Moghrabi/14x040-advanced_sec-semester_project

1.1 Context

The adoption of blockchain technology in various sectors has necessitated the exploration of more efficient consensus mechanisms than the traditionally used Proof of Work (PoW). Proof of Stake (PoS) emerges as a compelling alternative, heralding significant advancements in terms of energy efficiency and scalability. This shift is epitomized by Ethereum's transition from PoW to PoS, marking a pivotal moment in blockchain development. As the second-largest cryptocurrency platform by market capitalization, Ethereum's move to integrate PoS is indicative of a broader industry trend towards more sustainable and scalable blockchain solutions [1].

Proof of Stake is not merely a technical upgrade but a fundamental change in how block validations are performed. Unlike PoW, where the probability of mining a block is dependent on computational power, PoS allocates mining power based on the proportion of coins held by a miner. This method not only reduces the amount of energy required to maintain the network but also mitigates the risk of centralization seen in PoW, where the increasing hardware requirements can limit the ability to mine to a few heavily capitalized actors [2].

The transition to PoS, however, introduces new challenges and vulnerabilities, necessitating thorough investigations into its security implications. This report delves into these vulnerabilities, offering a comprehensive analysis supported by practical demonstrations of potential exploits. By addressing these issues, the research contributes to the ongoing discussion on how blockchain technologies can be secured and optimized. Such insights are crucial for the development of future blockchain frameworks that aim to balance efficiency, security, and decentralization.

1.2 Existing works

A growing body of research has been dedicated to exploring the security implications of the Proof of Stake (PoS) consensus mechanism, particularly as it becomes increasingly prevalent across major blockchain platforms. Notable among these is the study by Pavlov in 2023, which scrutinizes the Ethereum Proof-of-Stake model. Pavlov's analysis provides a comprehensive examination of potential security weaknesses inherent in Ethereum's shift from a purely PoW to a hybrid PoS system [3]. Complementing this, the Ethereum Foundation has ramped up its security efforts with significant bug bounty payouts aimed at identifying and mitigating vulnerabilities during its transition to PoS, indicating a proactive approach to securing the blockchain [4].

Additional insights are provided by Neuder et al., who have detailed specific attack strategies like one-block reorgs that exploit the PoS system's vulnerabilities. Such research underscores the sophisticated nature of threats that PoS systems face and the necessity for advanced defensive measures [5]. Beyond Ethereum-specific studies, broader analyses in the field also discuss various potential attack vectors and mitigation strategies applicable to all PoS-based blockchains, offering a more comprehensive view of the security landscape [6].

These studies form a crucial foundation for understanding the challenges and opportunities presented by PoS mechanisms. They highlight the need for ongoing research and adaptation to address security concerns as blockchain technologies continue to evolve and expand.

2. The Proof of Stake Consensus Mechanism

2.1 Reminder: Consensus Mechanisms

Consensus mechanisms are the foundational aspect of a blockchain network, serving as the protocol through which the network nodes agree on the validity and order of transactions that are added to the blockchain. Such mechanisms are critical as they ensure all participants in the decentralized network have a consistent view of the ledger, preventing issues like double spending and ensuring the network operates smoothly without the need for a central authority.

Traditionally, blockchain networks like Bitcoin used a consensus mechanism known as Proof of Work (PoW). PoW required participants, known as miners, to solve complex cryptographic puzzles. The first miner to solve the puzzle would gets the right to add a block of transactions to the blockchain and receives a reward in the form of the blockchain's native cryptocurrency.

2.2 Proof of Stake (PoS)

Proof of Stake (PoS) [7] is a consensus mechanism where the creation of new blocks is handled by validators who are chosen based on the number of coins they hold and are willing to "stake" as collateral, (i.e. "to lock up"). Validators lock up their stake in a special wallet to show their commitment to maintaining the network's integrity. This stake can be lost or slashed if they are found to be acting maliciously, such as validating fraudulent transactions or attempting to alter the network's protocol. The risk of losing their stake deters validators from committing such actions. This staking acts as both a security deposit and a sign of commitment to the network's integrity. The fundamental concept is that the more coins an actor stakes, the higher its chances of being chosen to validate transactions and create new blocks.

The selection of validators in a PoS system typically involves several factors:

- **Stake Size:** The primary factor is the amount of the cryptocurrency that a validator stakes. The larger their stake, the greater their chances of being chosen to validate a block. This is because a larger stake signifies a greater loss if they were to act maliciously, hence a higher degree of trustworthiness
- **Randomization:** Many PoS systems incorporate a degree of randomness in the selection process. This can be achieved through algorithms that use factors like the age of the staked coins and the node's wealth to ensure fairness and reduce the predictability of being chosen.
- **Coin Age:** Some variations of PoS consider the age of the coins staked, where older staked coins could increase a validator's chance of creating a block. This method, however, has fallen out of favor in many newer PoS protocols due to potential security issues.

Once chosen, validators are responsible for block validation (i.e. veryfying the validity of transactions,ensuring no double-spending or other fraudulent activities), block creation, and adding the block to the blockchain. Validators are rewarded for their work in the form of transaction fees or newly minted coins.

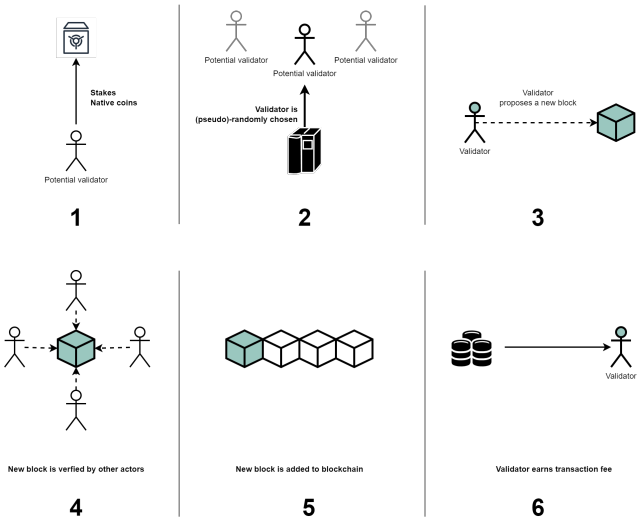

Figure 1: Proof of Stake (PoS) Consensus Mechanism, flowchart of the process.

2.3 Main Differences Between PoW and PoS

- **Energy Efficiency:** PoS is far more energy-efficient than PoW since it does not require miners to solve complex mathematical problems using powerful and energy-intensive computer hardware.
- **Reduced Risk of Centralization:** PoW can lead to centralization because individuals or companies with the financial resources to invest in advanced mining equipment can dominate the mining process. In contrast, PoS reduces this risk as the ability to create blocks isn't based on hardware but on the amount of cryptocurrency a validator is willing to stake.
- **Security:** While PoW security is based on the amount of work done by miners, PoS security is based on the amount of stake validators are willing to risk. Some argue this makes PoS less secure, as it might be cheaper to acquire 51% of the stake than to control 51% of the mining power in PoW.

3. Proof of Stake in Ethereum 2.0

3.1 The Beacon Chain

The Beacon Chain, introduced as the initial phase of Ethereum 2.0, is foundational to Ethereum's shift towards a fully PoS-based system. It operates independently of the Ethereum mainnet (which continues to use PoW during the transition) and is responsible for managing the PoS protocol. Key features include:

- **Validator Management:** The Beacon Chain manages a registry of validators and their stakes. Validators are required to stake 32 ETH, a substantial commitment meant to deter malicious behavior.
- **Random Selection for Block Proposal:** The Beacon Chain uses a sophisticated randomness mechanism called the "Randomness Beacon" to select validators for proposing new blocks. This process helps ensure security and fairness in block creation.
- **Epochs and Committees:** Time on the Beacon Chain is divided into epochs, which consist of multiple slots (time periods when new blocks can be created). During each epoch, committees of validators are assigned to vote on proposed blocks, adding an additional layer of consensus and security.

3.2 Shard Chains

Shard chains are an upcoming feature in Ethereum 2.0, designed to enhance the network's scalability by distributing the data processing load across multiple new chains. Each shard chain processes its own set of transactions and interactions, but remains connected to the main chain through the Beacon Chain.

Key features of shard chains include:

- **Increased Throughput:** By dividing the network into multiple shards, Ethereum can process many transactions in parallel, significantly increasing the network's capacity.
- **Crosslinks:** Shard chains will periodically submit summaries of their state to the Beacon Chain, known as "crosslinks". These crosslinks serve as checkpoints that link shard states back to the main Ethereum blockchain, ensuring all parts of the network remain synchronized.

3.3 From PoW to PoS

The transition of Ethereum from Proof of Work (PoW) to Proof of Stake (PoS), as part of the Ethereum 2.0 upgrade, is a complex and multi-phased integration over several stages :

1. **Beacon Chain Launch**
2. **Shard Chains implementations**
3. **Docking the Mainnet to Beacon Chain:** This critical phase will see the existing Ethereum mainnet, still running on PoW, being "docked" or merged with the PoS Beacon Chain. This merger is colloquially known as "The Merge" and represents the point where the current Ethereum mainnet transitions fully to a PoS system. At this stage, PoW will be completely phased out, and the Beacon Chain will become the primary consensus mechanism for all network activities, including transaction processing and smart contracts.
4. **Fully Functional Shards:**The final stage of the transition involves enabling shard chains to handle transactions and smart contracts. This will allow the network to fully utilize the scalability improvements introduced by sharding.

4. Security Implications and risks of PoS

The Proof of Stake consensus mechanism all though presenting a more energy efficient and scalable alternative to Proof of Work, introduces a new set of security risks and challenges. Some being linked to the inherent nature of PoS, while others are specific to the implementation of PoS in Ethereum 2.0. The following will explore the main (i.e. most documented) security implications and risks associated with PoS:

4.1 The nothing-at-stake problem

The "nothing at stake" problem arises because validators in a PoS system do not incur significant costs to support multiple forks of the blockchain, unlike in PoW, where substantial computational resources are needed for mining each fork. This issue can occur during decision points where the blockchain may fork due to normal operations or malicious activities.

> *"When a Proof of Stake blockchain forks[$\cdots$], the scarce resource for block production is not hash power but token stake, and, in a fork, an equivalent amount of stake is created on the new network. This means a Block Producer can start creating blocks on both networks immediately, and they do not have to choose (the computation cost of creating a block in a PoS system is generally trivial because miners are not competing with each other based on computation)."* - Smith & Crown [8]

- **Consequences:** If validators decide to validate blocks on multiple chains, it can lead to security breaches such as double spending. This happens because validators might validate a transaction on one fork and then the same or conflicting transaction on another fork, leading to inconsistencies across the network.
- **Technical Explanation:** In PoW, committing resources to a fork is a risk as miners must choose which fork they believe will survive to recoup their computational investments. In PoS, since the cost is minimal, validators might be tempted to maximize their rewards by supporting several forks, reducing the reliability and security of the network.

4.2 Long-range attacks

Long-range attacks involve attackers taking control of private keys for old stakes or finding ways to buy old keys that are no longer actively used but still have associated stakes. These attacks can potentially allow attackers to rewrite a blockchain's history from a point where they can create an alternative longest chain, challenging the network's legitimacy.

- **Execution:** Attackers use these old keys to start building an alternative blockchain from a point back in time, proposing it as the real chain. If they can convince other nodes in the network to accept this rewritten history, it could replace the actual legitimate chain.
- **Implications:** Such attacks can lead to loss of trust in the blockchain's integrity and could devalue the associated cryptocurrency as transaction history may be reversed or altered.

4.3 Bribe Attacks

Bribe attacks exploit the PoS mechanism by providing financial incentives to validators to act maliciously. This could include voting for particular transactions or forks, or creating blocks that include fraudulent transactions.

- **Mechanism:** Attackers can directly offer validators rewards outside the system (off-chain payments), making it lucrative for validators to deviate from honest behavior. Since stakes are public, it is relatively straightforward for an attacker to target wealthy validators or those with significant control over the blockchain state.
- **Risks:** Bribe attacks risk centralizing power in the hands of wealthy validators or external entities who can afford to pay bribes, undermining the decentralized nature of the blockchain and potentially leading to fraudulent states being accepted as valid.

4.4 Other Risks

The vulnerabilities and concerns posed by PoS are not limited to the above-mentioned risks. Other potential security implications include, Stake Centralization, where a small number of validators control a significant portion of the network, leading to centralization risks similar to PoW, Validator Collusion where validators conspire to manipulate the blockchain, etc...in addition to Software specific risks such as bugs, vulnerabilities, and exploits in the PoS implementation.

5. Mitigating Security Risks in PoS

Addressing the vulnerabilities inherent in Proof of Stake (PoS) systems requires a multifaceted approach, focusing on technological, community, and procedural enhancements to strengthen the network.

This section does not aim at giving a comprehensive list of all possible mitigation strategies, but rather to provide a few examples of how the risks associated with PoS can be addressed.

5.1 Mitigating the Nothing-at-Stake Problem

The "nothing-at-stake" problem can be mitigated by introducing penalties for validators who show harmful behavior. Implementing slashing conditions where validators lose a portion of their stakes for behaviors that harm the consensus process, such as validating multiple conflicting blocks, can deter the "nothing at stake" issue. By penalizing validators who act maliciously or irresponsibly, the network can maintain security and integrity.

An other approach to mitigate this issue is to use a checkpoint system, where validators are required to commit to a specific chain, reducing the likelihood of supporting multiple forks. This system can help prevent validators from exploiting the "nothing-at-stake" problem by forcing them to choose a single chain to validate, enhancing network security and consistency.

5.2 Addressing Long-Range Attacks

Mitigating long range-attacks can be achived by implementing mechanisms such as Key Evolving Cryptography (KEC), involving changing the private keys used for signing transactions over time, making it difficult for attackers to use old keys to rewrite the blockchain's history. By regularly updating private keys, the network can prevent long-range attacks and maintain the integrity of the blockchain.

An other common approach to prevent long-range attacks would be to introduce a weak subjectivity mechanism, where nodes rely on trusted sources to determine the correct blockchain history. By establishing trusted checkpoints or validators, the network can prevent attackers from rewriting history beyond a certain point, ensuring the security and reliability of the blockchain. This approach however introduces a level of centralization and reliance on external sources, which may conflict with the decentralized nature of blockchain technology.

5.3 Protecting Against Bribe Attacks

Bribe attacks can be mitigated by enhancing the transparency and accountability of validators, making it more difficult for attackers to bribe them without detection. By implementing mechanisms to monitor validator behavior and detect suspicious activities, the network can identify and penalize validators who engage in malicious behavior, reducing the risk of bribe attacks.

Decentralizing staking pools and validator selection processes can also help prevent bribe attacks by distributing power and influence across a broader set of participants. By reducing the concentration of stakes and control in the hands of a few validators, the network can enhance security and resilience against external manipulation and bribery.

5.4 Mitigating other Risks

Other concerns such as stake centralization, validator collusion, and software-specific risks can be addressed through a combination of technical enhancements, community engagement, and procedural changes. Implementing mechanisms to prevent stake centralization, such as capping the maximum stake a validator can hold, can help distribute power more evenly across the network, reducing the risk of centralization.

6. Conclusion

Proof of Stake is distinguished by its energy efficiency and scalability, which could make it an attractive alternative to the computationally intensive and environmentally taxing PoW model. Ethereum 2.0 embodies this shift in its hybrid consensus approach, where the Beacon Chain introduces PoS to Ethereum's ecosystem, and the phased integration of shard chains aims to improve transaction processing capabilities significantly.

However, the transition to PoS is not without its challenges. As several vulnerabilities unique to PoS systems are introduced. These issues underscore the critical need for robust mitigation strategies that ensure the security and integrity of PoS-based blockchain networks. Implementing measures like slashing for misbehavior, employing cryptographic techniques for validator selection, and ensuring transparency in validator activities are essential to safeguard the system against vulnerabilities.

In-depth case studies on the real-world application of Ethereum 2.0 and other PoS systems could yield important insights into practical challenges and opportunities, guiding future innovations in blockchain technology. As the blockchain community continues to innovate and adapt, it is imperative to foster a deeper understanding of these mechanisms to harness their full potential effectively.

In conclusion, while PoS offers promising improvements over PoW, realizing its full potential requires addressing its inherent challenges through continuous research, innovation, and community collaboration. The journey towards a more scalable, secure, and sustainable blockchain ecosystem continues, with the developments in PoS at the forefront of this transformative technology.

References

[1] X. Li, Y. Jiang, H. Chen, X. Luo, and C. V. Shen, "The blockchain revolution: From pow to pos," in *Proceedings of the IEEE Symposium on Computers and Communications*, 2019.

[2] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, https://bitcoin.org/bitcoin.pdf, 2008.

[3] U. Pavloff, Y. Amoussou-Guenou, and S. Tucci-Piergiovanni, "Ethereum proof-of-stake under scrutiny," in *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, Tallinn Estonia: ACM, Mar. 27, 2023, pp. 212–221, ISBN: 978-1-4503-9517-5. DOI: 10.1145/3555776.3577655. [Online]. Available: https://dl.acm.org/doi/10.1145/3555776.3577655 (visited on 02/27/2024).

[4] A. Bannister, *Ethereum foundation offers $1m bug bounty payouts with proof-of-stake migration multiplier*, https://portswigger.net/daily-swig/ethereum-foundation-offers-1m-bug-bounty-payouts-with-proof-of-stake-migration-multiplier, Accessed: 2024-04-18, 2022.

[5] Ethereum Foundation, *Ethereum proof-of-stake attack and defense*, https://ethereum.org/en/security/, Accessed: 2024-04-18, 2023.

[6] "Blockchain vulnerabilities and recent security challenges," *Journal of Blockchain Security*, 2023.

[7] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proceedings of the Annual International Cryptology Conference*, Springer, 2017, pp. 357–388.

[8] "Smith and crown." (2024), [Online]. Available: https://www.smithandcrown.com/glossary/nothing-at-stake-problem#:~:text=The%20Nothing%2Dat%2DStake%20Problem,of%20Proof%20of%20Stake%20mechanisms. (visited on 05/12/2024).