


Analyzing Blockchain Consensus Mechanisms for Double-Spending Attack Prevention

Jiasong Ye ^a

Engineering Department, Shenzhen MSU-BIT University, Shenzhen, China

Keywords: Blockchain, Consensus Mechanisms, Double-Spending Attacks, Cryptocurrency.


Abstract: With the rapid development of blockchain technology, cryptocurrency transactions face increasing security risks, particularly from double-spending attacks. This paper explores the effectiveness of various blockchain consensus mechanisms in preventing these attacks. It examines the principles and applications of Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) mechanisms, evaluating their advantages and limitations. The paper provides a comprehensive classification and comparison of these consensus methods, focusing on their strategies for countering double-spending threats. Through a blend of theoretical analysis and methodological research, the study identifies the strengths and weaknesses of existing mechanisms. Experimental results show that while PoW offers strong security, it is hindered by high energy consumption and mining power centralization. In contrast, PoS and DPoS reduce energy consumption and improve network flexibility but grapple with issues like power centralization and governance efficiency. This research provides valuable insights for future improvements in blockchain consensus mechanisms and enhances the security of cryptocurrency systems.

1 INTRODUCTION

In the Internet era, electronic payments have become the mainstream method for daily transactions. However, this reliance brings potential privacy risks and data security issues, leading to public scepticism about the ability of third-party institutions to protect data. In the absence of a trust mechanism, there is an urgent need for a new way for parties to conduct transactions to ensure security and privacy (Kim et.al, 2008). Blockchain technology emerges as a solution to these problems. Many institutions regard blockchain as a key breakthrough for future technological development, believing it has the potential to fundamentally transform existing business models. In 2008, a researcher under the pseudonym “Satoshi Nakamoto” first proposed the concept of digital cryptocurrency (Nakamoto, 2008). He then introduced the concept of Bitcoin (Guth and Leymann, 2018), marking the birth of blockchain technology. Unlike the traditional monetary system, where a central bank holds centralized control, the Bitcoin system distributes the responsibility of maintaining the ledger and issuing currency among

all participants. The primary issue that consensus mechanisms in cryptocurrency systems address is determining ownership as the currency circulates (Pass and Shi, 2016).

Cryptocurrency consensus mechanisms can be divided into permissionless and permissioned types (Cryptape, 2016). In permissionless mechanisms, Proof of Work (PoW) is the most representative protocol, where all nodes have equal rights. Permissioned protocols include Proof of Stake (PoS) and Delegated Proof of Stake (DPoS), which are applied in different scenarios based on the authorization levels of nodes. The success of Bitcoin is not only attributed to these consensus mechanisms but also built on the foundation of early decentralized digital currency systems such as b-money (Fujian et.al, 2024) and hashcash (Back, 2002), which first realized a fully decentralized electronic cash system. However, due to the network's decentralized nature, the system is also vulnerable to malicious attacks, such as double-spending and denial-of-service attacks, which could disrupt its normal operation (Mehtar et.al, 2019). Studying Bitcoin's PoW mechanism has played a crucial role in addressing the

^a <https://orcid.org/0009-0008-1157-3396>

issue of double-spending (Miller et.al, 2015). Before the advent of blockchain technology, double-spending could only be prevented through centralized means. Bitcoin, through its decentralized PoW mechanism, provided a novel solution, effectively preventing this issue.

As blockchain technology advances and the value of cryptocurrencies increases, attacks on these systems have become more prevalent. In August 2010, a hacker exploited a vulnerability in Bitcoin's code, creating over 18 billion Bitcoins, leading to Bitcoin's first hard fork. This marked the first major attack on a PoW-based cryptocurrency. Since then, attackers have increasingly targeted blockchain mechanisms and ecosystems. For example, in 2012, the Bitcoinica exchange was hacked, leading to the theft of customers' Bitcoin keys, and in 2016, a smart contract vulnerability on Ethereum caused the failure of The DAO project, prompting another blockchain fork. In 2018, Bitcoin Gold suffered a 51% attack, and other cryptocurrencies like Beauty Chain and Monacoin faced losses due to smart contract vulnerabilities and selfish mining attacks. These incidents underscore the risks in blockchain applications. Researchers, including Satoshi Nakamoto, have long warned of threats like the 51% attack (Karame et.al, 2012). As computational power centralizes, the risk of such attacks grows. To address these vulnerabilities, this paper explores consensus mechanisms in cryptocurrencies, particularly their role in preventing double-spending attacks. By categorizing different consensus models, the study provides theoretical and practical insights to improve cryptocurrency security.

2 METHODOLOGY

In the comprehensive examination of the cryptocurrency landscape, addressing security threats, particularly double-spending attacks, is paramount. This paper focuses on analyzing the consensus mechanisms used in cryptocurrencies and explores their vital role in preventing such attacks. To achieve this, an extensive literature review and detailed case studies are conducted to classify and evaluate different consensus mechanisms, such as PoW, PoS, and DPoS. Each mechanism's strengths and vulnerabilities are analyzed in relation to security, revealing how they either mitigate or expose systems to double-spending risks. Lastly, the study compiles a set of targeted preventive strategies and practical recommendations that enhance the resilience of cryptocurrencies against various security

threats. These measures aim to safeguard users' assets and maintain trust in digital transactions. The research process, outlined in Figure 1, follows a structured approach that includes reviewing current practices, analyzing vulnerabilities, and proposing actionable solutions.

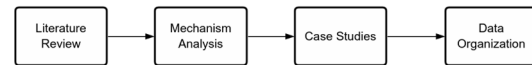


Figure 1: The pipeline of this study (Picture credit: Original).

2.1 Blockchain Technology and Related Background

Blockchain technology originated in the late 1970s when a computer scientist named Ralph Merkle filed a patent for hash trees, also known as Merkle trees (Merkle, 1987). These trees are a computer science structure that links blocks through cryptography. Blockchain is a distributed ledger technology that records transaction information in a decentralized manner, thereby eliminating the reliance on centralized authorities. It forms an immutable data chain by linking blocks in chronological order, where each block contains a series of transactions, timestamps, and the cryptographic hash of the previous block. Each block includes several transaction data and a hash value pointing to the previous block to ensure the integrity and security of the data (Lei and Gang, 2016). The data on the blockchain is consistent over time because it cannot be deleted or modified without network consensus. Thus, blockchain technology can create immutable ledgers to track orders, payments, accounts, and other transactions. The system's built-in mechanisms prevent unauthorized transaction entries and create consistency in the shared view of these transactions (Yidong and Xiaotong, 2012). Other characteristics of blockchain technology include open consensus, where anyone can participate in the blockchain network, and each node has a complete copy of the database, making the network open and transparent. It is trustless, requiring no reliance on a trusted third party, as nodes collaborate according to rules, making the system public and transparent, and difficult to deceive other nodes. Anonymity links users' identities to their public key addresses rather than their real identities, enabling users to trade and use blockchain anonymously. Traceability means that transaction data carries timestamps, allowing each transaction to be traced back to its origin, ensuring data integrity and transparency.

2.2 Consensus Mechanisms and Double-Spending Attacks

2.2.1 PoW Module

This is the most widely used consensus mechanism, initially implemented in Bitcoin. It relies on computational power to solve complex cryptographic puzzles. The first node to solve the puzzle gains the right to add a new block and receives a corresponding reward. This mechanism ensures network security by requiring significant computational resources, making it extremely costly for malicious actors to control the network. The PoW mechanism is based on competition among miners to solve cryptographic puzzles that require substantial computational power. The solution to this puzzle, known as the "proof," needs to be verified by the network before the block can be added to the chain. The security of PoW is reflected in its high computational cost and economic penalties for double-spending attempts. An attacker would need to control more than 51% of the network's computing power to alter the blockchain, which is nearly impossible for a large network like Bitcoin.

2.2.2 PoS Module

Unlike PoW, PoS selects validators based on the number of tokens they hold and are willing to stake as collateral. Validators are chosen to propose and verify new blocks based on their staked assets, reducing the need for extensive computational resources. PoS aims to address the energy efficiency issues of PoW and mitigate the "nothing-at-stake" risk through penalty mechanisms. The PoS mechanism allocates block validation rights based on the amount of tokens held by validators. The selection of validators follows a pseudo-random process, considering factors such as the age of the staked tokens and randomness. PoS reduces the computational burden associated with PoW and ensures network security through economic incentives. Validators' staked assets are at risk, and if they are found to behave maliciously, such as attempting a double-spending attack, their staked assets will be forfeited.

2.2.3 DPoS Module

DPoS introduces a voting system where token holders elect a small number of representative nodes to verify transactions and generate new blocks. This mechanism maintains decentralization while improving efficiency and transaction speed. However, DPoS poses a centralization risk when

voting power is concentrated among a few large stakeholders. DPoS builds on PoS by introducing an election mechanism, where token holders vote to elect a small number of witnesses to verify transactions. This reduces the number of nodes involved in the consensus, improving transaction throughput and reducing latency. However, this mechanism also introduces the risk of centralization, as a few large stakeholders may dominate the network through the voting process.

2.3 Double-Spending Attacks

Double-spending is one of the most threatening attack forms in blockchain, referring to the situation in digital currency systems where the same digital asset is improperly used multiple times due to the duplicability of data. In simple terms, it means the same amount of digital currency is spent twice or more.

Reasons for double-spending attacks include: 1. Rapid Successive Transactions: Attackers may quickly submit multiple new transactions before the initial transaction is confirmed, attempting to double-spend and make it difficult for the system to detect and prevent this behavior in time; 2. Use of Multiple Identities: Attackers may use multiple identities to submit transactions, increasing the chances of a successful double-spending attack; 3. Control of Multiple Nodes: Attackers may try to control multiple nodes or participate in multiple mining pools to increase the probability of a successful double-spending attack. For example, conducting a 51% attack to control the entire blockchain network, enabling the attacker to publish fraudulent transactions and thus perform a double-spending attack. Types of double-spending attacks include: 1. Finney Attack: The attacker privately mines a block containing another transaction. Once the initial transaction is confirmed, the attacker publishes this privately mined block, effectively performing a double-spend and successfully stealing funds; 2. Race Attack: The attacker broadcasts another transaction to part of the network while simultaneously mining a block that does not include that transaction. If the alternative transaction is confirmed before the legitimate one, the attacker can successfully double-spend; 3. Vector76 Attack: This attack targets cryptocurrencies that rely on the BIP16 payment protocol variant. By exploiting vulnerabilities in the payment protocol, the attacker can execute a double-spending attack.

2.4 Prevention of Double-Spending from the Perspective of Consensus Mechanisms

In PoW, nodes compete to solve complex mathematical problems, granting them the right to add blocks to the blockchain. Bitcoin's decentralization ensures that transaction legitimacy is collectively verified, and only when the majority agrees is a transaction confirmed. To counter double-spending, PoW relies on dispersing computational power across the network. By making it economically unfeasible for attackers to control over 51% of the network's computing power, PoW deters such attacks. Additional security is achieved by increasing transaction confirmation requirements and total hash rates, which raise the cost of reorganizing the chain. Moreover, random block production mechanisms, such as Bitcoin-NG and Greedy Heaviest Observed Subtree (GHOST), add unpredictability to block creation, making it harder for attackers to exploit the system. PoS introduces stake locking and penalties for malicious behavior, such as attempting double-spending attacks. Validators must lock tokens as collateral, and if caught acting maliciously, they lose their stake, significantly raising the cost of attacks. Validators are also selected randomly, preventing attackers from predicting or controlling the block production order. Additionally, PoS utilizes a committee of validators to approve blocks, further decentralizing control and making it difficult for an attacker to succeed with double-spending. DPoS focuses on node management and supervision. Token holders elect supernodes to verify transactions, and malicious nodes can be replaced via voting if necessary. Real-time monitoring and dynamic penalties ensure that nodes exhibiting harmful

behavior are immediately penalized. Observer nodes provide an additional layer of oversight, reporting any abnormal actions to the community, ensuring a fair and secure blockchain system through collective governance.

3 RESULT AND DISCUSSION

3.1 Comparative Analysis of Consensus Mechanisms

Table 1 summarizes the double-spending prevention measures in permissionless and permissioned consensus mechanisms. In permissionless systems like PoW, security is achieved through decentralization and the distribution of computational power. By making it costly for an attacker to control over 51% of the network, PoW reduces the risk of double-spending. Additional measures include multiple block confirmations, increasing the network hash rate, and randomizing block generation through mechanisms like Bitcoin-NG and GHOST. Despite its strengths, PoW faces challenges such as high energy consumption, long confirmation times, and the risk of mining pool centralization, which could increase vulnerability to attacks. Permissioned mechanisms like PoS and DPoS take a different approach. PoS raises the economic cost of attacks by requiring validators to lock tokens as collateral and randomly selecting validators to prevent attack planning. However, PoS risks centralization due to wealth accumulation. DPoS enhances security through elected supernodes and real-time node monitoring, but faces potential issues with vote manipulation and centralization.

Table 1: The double-spending prevention measures.

Mechanism Type	Preventive Measures	Specific Characteristics
PoW	1. Increase transaction confirmation count	Increase the difficulty of reorganizing the chain within a short period of time for attackers
	2. Increase network total computing power	Raise the economic cost of controlling 51% of the computing power
	3. Encourage mining decentralization	Avoid concentration of computing power in a few mining pools, reducing single entity control risk
PoS	1. Staking lock-up and penalty mechanism	Lock up tokens as collateral, punish malicious actors by deducting part or all of the collateral
	2. Random selection of validators	Difficult to predict validators, enhance unpredictability against attackers
DPoS	1. Node election and replacement mechanism	Token holders vote to elect and replace malicious nodes, strengthen network resilience
	2. Node behavior monitoring and dynamic penalty mechanism	Monitor node behavior, revoke eligibility and deduct collateral from malicious actors

Table 2: Advantage and disadvantage of different methods.

Consensus Mechanism	Type	Advantage	Disadvantage
PoW	No authorization	<ol style="list-style-type: none"> 1. Decentralization, any node has the opportunity to participate. 2. The cost of a 51% attack is high, reducing the risk of double-spending attacks. 3. The number of transactions confirmed improves security. 4. Increasing network computing power reduces the risk of being attacked. 5. Randomized block mechanisms increase unpredictability. 	<ol style="list-style-type: none"> 1. High energy consumption issues affect sustainability. 2. Longer transaction confirmation times affect user experience. 3. Mining concentration may lead to centralization of computing power and increased risks.
PoS	Authorization	<ol style="list-style-type: none"> 1. Staking currency as collateral increases the cost of malicious behavior. 2. Randomly selecting validators reduces predictability for attackers. 3. The validator committee mechanism enhances security. 	<ol style="list-style-type: none"> 1. It may lead to a “rich get richer” phenomenon, increasing centralization risks.
DPoS	Authorization	<ol style="list-style-type: none"> 1. Selecting super nodes increases flexibility. 2. Real-time monitoring of node behavior quickly eliminates malicious nodes. 3. Improve network anti-attack capabilities. 	<ol style="list-style-type: none"> 1. Centralization risks, voting manipulation issues. 2. Weakening the efficiency of community governance.

Overall, the PoW mechanism provides robust security against double-spending attacks, but its drawbacks in terms of energy consumption and user experience are evident. In contrast, PoS and DPoS excel in terms of cost-effectiveness and flexibility, but they also face challenges such as power concentration and governance efficiency. Future consensus mechanisms may combine these strengths to form hybrid models that achieve higher security, efficiency, and sustainability, further reducing the risk of double-spending attacks. Table 2 summarizes the strengths and weaknesses of PoW, PoS, and DPoS in preventing double-spending attacks.

3.2 Future Development Directions

The future of blockchain consensus mechanisms may evolve towards hybrid models that combine the advantages of PoW, PoS, and DPoS to enhance the security, efficiency, and sustainability of blockchain networks. Initially, the decentralized computing power of the PoW mechanism can be used to ensure network security and resistance to attacks, preventing double-spending in the early stages. Then, the PoS staking mechanism can be adopted, allowing token holders to lock their tokens as collateral to reduce energy consumption and resource usage. Finally, by introducing DPoS's fast election and voting mechanisms, the transaction validation speed and network efficiency can be improved.

To mitigate the high energy consumption of PoW and the centralization issues of PoS and DPoS, new mechanisms may incorporate randomness in validation and dynamic node adjustment strategies, such as randomly selecting validators and using multi-layer consensus structures to decentralize validation power. These strategies aim to ensure decentralization and flexibility, enhancing the system's security and resistance to attacks. The development of the blockchain ecosystem will be a significant trend in the future. As blockchain technology integrates with existing financial systems, compliance and regulation will become key factors. This will drive developers to consider legal and regulatory requirements when designing consensus mechanisms, thereby reducing the risk of double-spending attacks and increasing user trust. Finally, community participation and governance models will gradually evolve. Future consensus mechanisms will place greater emphasis on community governance by designing fair and transparent election mechanisms and governance structures to enhance user engagement and trust in the network. This shift will foster a more secure, efficient, and fair blockchain network, making malicious behaviors such as double-spending more difficult to execute. In conclusion, the future development of blockchain will rely on technological advancements, community governance, and ecosystem refinement to achieve higher levels of security and sustainability.

4 CONCLUSIONS

This paper has analyzed the effectiveness of different blockchain consensus mechanisms—PoW, PoS, and DPoS—in preventing double-spending attacks. Through detailed examination of their strategies and application scenarios, it is evident that each mechanism offers distinct advantages and drawbacks. PoW provides robust security but suffers from high energy consumption and risks related to the concentration of computational power. PoS and DPoS, while improving network efficiency and reducing energy usage, face issues of centralization and governance inefficiencies. Future research will explore hybrid consensus mechanisms that blend the strengths of PoW, PoS, and other emerging methods to enhance blockchain security and scalability. Further investigation will focus on optimizing these mechanisms for specific applications, improving transaction speed while minimizing risks of double-spending. Additionally, enhancing governance structures within the blockchain ecosystem will be essential in creating a more secure, efficient, and sustainable digital currency network. This approach aims to strengthen the foundation for future blockchain systems and their security protocols.

REFERENCES

- Back, A., 2002. Hashcash-a denial of service counter-measure.
- Cryptape, 2016. Consensus calculation. The engine of blockchain.
- Fujuan, L., Zhuo, M., Qun, W., 2024. Overview of identity management mechanism of blockchain system. *Journal of Computer Engineering & Applications*, 60(1).
- Guth, J., & Leymann, F., 2018. Towards pattern-based rewrite and refinement of application architectures. *Advanced summer school on service-oriented computing*. IBM Research Division, 90-100.
- Karame, G.O., Androulaki, E., & Capkun, S. 2012. Double-spending fast payments in bitcoin. In *Proceedings of the ACM conference on Computer and communications security*, 906-917.
- Kim, D.J., Ferrin, D.L., & Rao, H.R., 2008. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems*, 44(2), 544-564.
- Lei, T., Gang, C., 2016. Blockchain 2.0. *Chinese informatization*, 8.
- Mehar, M.I., Shier, C.L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., & Laskowski, M. 2019. Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack. *Journal of Cases on Information Technology*, 21(1), 19-32.
- Merkle, R.C. 1987. A digital signature based on a conventional encryption function. In *Conference on the theory and application of cryptographic techniques*, 369-378.
- Miller, A., Kosba, A., Katz, J., & Shi, E. 2015. Nonoutsourcable scratch-off puzzles to discourage bitcoin mining coalitions. In *Proceedings of the acm sigsac conference on computer and communications security*, 680-691.
- Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto.
- Pass, R., & Shi, E., 2016. Hybrid consensus: Scalable permissionless consensus.
- Yidong, C., Xiaotong, Z., 2012. An economic analysis of the new currency Bitcoin. *Modern economic information*, 16, 8-8.