Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 18, No. 2, 2025

A Game-Theoretic Defense Mechanism Against Blockchain Denial-of-Service Attacks in Bitcoin

Chunming Zha, Jing Zhang and Qingbin Zhang

College of Software, Henan Polytechnic University, Jiaozuo, 454000, China

Abstract: Bitcoin, the world's first decentralized digital currency, offers a high degree of security and transparency with its distributed network based on blockchain technology. However, with the widespread use of Bitcoin and other blockchain systems, cyberattacks have become one of the major issues threatening their stability and security. Among them, BDoS (Blockchain Denial of Service) attacks and SDoS (Selfish Denial of Service) attacks, as new types of denial-of-service attacks, especially pose a significant threat to the Bitcoin network. Since the Bitcoin network adopts the Proof of Work (PoW) mechanism, BDoS and SDoS attacks force miners to stop mining or waste computing resources by exploiting the blockchain reward mechanism and creating chain forks. In this paper, based on blockchain technology and game theory, we propose an effective defense strategy to avoid denial-of-service attacks on the blockchain, and the scheme does not require modification of the existing blockchain protocol.

Keywords: Blockchain; SDoS; BDoS; Bitcoin; PoW.

1. Introduction

Cryptocurrency, as an emerging digital asset, has rapidly gained widespread attention and application worldwide due to its decentralization, anonymity and global circulation. Bitcoin, as the first cryptocurrency to successfully implement blockchain technology, has not only reshaped the traditional landscape of the financial sector, but also promoted the widespread application of blockchain technology. The Bitcoin network relies on blockchain technology, a distributed ledger-based system that ensures the transparency and immutability of transaction data, providing a solid guarantee of the security of the cryptocurrency.

Bitcoin [1] employs the Proof-of-Work (PoW) consensus mechanism as a way for miners in the blockchain network to reach agreement. Through the PoW mechanism, miners are required to solve complex mathematical puzzles to validate transactions and create new blocks, and those who succeed are rewarded with bitcoins. This mechanism not only guarantees the decentralization and security of the network, but also incentivizes miners to actively participate in mining activities. With the gradual growth of the bitcoin system's arithmetic power and the deepening of related research, mining attacks have become a serious problem for the blockchain system. Current mining attacks are mainly categorized into three types: selfish mining [2][3], block interception attacks [4][5][6], and blockchain denial-of-service attacks [7][8][9].

Blockchain Denial of Service (BDoS) is completely different from the classic Denial of Service (DoS), which implements attacks against flaws in the blockchain protocol: using the reward mechanism of the blockchain system itself to force miners to actively choose to stop mining. Simply put, in a BDoS attack, the attacker mines a block and then hides the full information of the block by throwing out the block header (or some other proof method to prove that he or she has already mined the next legitimate block), forcing honest miners to actively choose to stop mining, thus giving the attacker a higher probability of winning the mining race and obtaining the block reward. Researchers have proposed corresponding defense methods for this attack, for example, the main working principle of the latest scheme [10] is to add a virtual block at the end of the main chain to prevent the attacker from maliciously causing a fork of the blockchain, and who is responsible for the creation of the virtual block is an important issue that has not yet been resolved in the paper. In this paper, we introduce a new “regulator” role, and utilize blockchain and game theory techniques to establish a spontaneous reward and punishment mechanism to solve this problem, and turn the trust problem into an economic problem.

2. Preparatory Knowledge

2.1. Blockchain

Blockchain is a decentralized distributed ledger technology capable of storing data securely, transparently and immutably across multiple nodes. A blockchain can be viewed as a distributed database maintained by all nodes, with its first block called the genesis block, after which blocks are interconnected by a chain structure, each block indexing the hash value of the previous block, and each block storing information about the system's transactions. In reality, the block structure of various blockchains is not exactly the same, but the basic structure of the vast majority of blocks consists of two parts: the block header (Header) and the block body (Body). Among them, the main role of the block header is to link the previous block and verify the integrity of the transaction data recorded in the previous block, which consists of the version number (Version), the hash value of the previous block (Prev_hash), the Merkle Root, the timestamp (Time), the difficulty value (Target_bits), and random number (Nonce) Composition; the main role of the block body is to record all electronic transaction data since the creation of the Genesis block, which are stored in the block body in the form of Merkle trees. The main data structure of the blockchain is shown in Figure 1.

Merkel tree is also known as a hash binary tree, which consists of Merkel root, intermediate nodes and leaf nodes, as shown in Figure 1, Hash 1, 2, 3... represents the hash value of all transactions, Merkel tree can be all the transaction hash

value two by two operation to get the new hash value, and ultimately all the transaction operation formation for a Merkel root. Using this storage structure, on the one hand, it can save the storage space of transaction information, on the other hand, it can determine whether there is any malicious behavior such as tampering in the transaction by calculating the Merkel root, which reduces the amount of computation for integrity verification and tampering detection of the transaction.

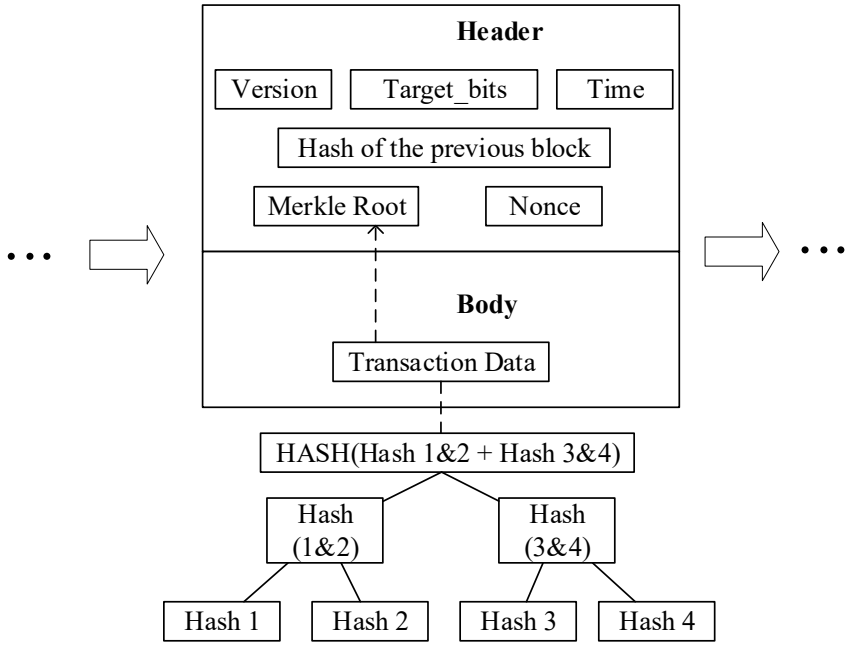

Figure 1. Blockchain structure

2.2. Game theory

Von Neumann introduced the theory of modern game theory in 1928, which itself is the study of how players make optimal decisions in situations with conflict, cooperation or competition. It focuses on how multiple decision makers choose strategies in interdependent environments and aims to find the optimal behavior for each player. The core concepts of game theory include players, strategies, payments, and information structures, and can usually be categorized into two types: static and dynamic games. In a game, players' decisions are not only influenced by their own goals, but also depend on the decisions of other participants. Game theory is widely used in economics, political science, military science and other fields to analyze competitive markets, auctions, contract design and other problems.

Game theory is a discipline based on mathematical modeling to study the decision-making of mutual behavioral activities between rational participants, there are two relationships between the participants, cooperation and conflict, but each relationship is to maximize their own interests, and each decision is based on rationality. The participants are usually two or more people, the participants mainly use game theory to analyze or predict the behavioral strategies of other participants, and then make rational behavioral choices based on the behavior of other participants, and sometimes also provide suggestions for decision makers to achieve their goals.

2.3. Nash equilibrium

The concept of Nash equilibrium was introduced by the American mathematical volume John Forbes Nash in 1950, describing a non-cooperative game in which individual players choose a combination of strategies such that each player has no incentive to unilaterally change his or her own strategy, knowing the strategies of the other players. In other words, a Nash equilibrium is a stable strategy configuration under which no player can obtain a better outcome by changing his or her strategy. A Nash equilibrium can be a pure strategy equilibrium or a mixed strategy equilibrium, the latter meaning that players choose probability distributions to make random decisions in the game. In equilibrium, the strategies of all players match each other to achieve a stable state of interaction.

3. Description of BDoS and SDoS Attacks

3.1. BDoS attack

Blockchain Denial of Service (BDoS) is completely different from the classic Denial of Service (DoS), which implements attacks against flaws in the blockchain protocol: using the reward mechanism of the blockchain system itself to force miners to actively choose to stop mining. Simply put, in a BDoS attack, the attacker mines a block and then hides the block body information by throwing out the block header (or some other method of proving that he or she has already mined the next legitimate block), forcing honest miners to voluntarily choose to stop mining, which in turn gives the attacker a higher probability of winning the mining race and obtaining the block reward.

Initial state and the main chain: In the current state of the blockchain, there is a newest block on the main chain, denoted as Bn . This block is the one mined and confirmed by the miners, and is the “correct” chain of the current blockchain. This is the “correct” chain for the current blockchain, as shown in Figure 2.

Behavior of Attacker A: Attacker A mines a legitimate block Ba after block Bn . However, instead of immediately broadcasting Ba in its entirety to the entire network, the attacker only publishes Ba 's block header information (including key information such as block hash, previous block

hash, timestamps, etc.) and hides the block body information (including transaction records, etc.). The purpose of this behavior is to hide the block body content, making it impossible for other miners to know the complete content of the block. As shown in Figure 3.

Reaction of other miners: Other miners do not know the content of the attacker's Ba block body, so if they find and successfully mine a new legitimate block after block Bn, they will broadcast that block (called Bh) to the network. In this way, there will be two different blocks (Ba and Bh) in the whole network and these two blocks will fork with block Bn and the blockchain will be in a competitive state. As shown in Figure 4.

Attacker broadcasts block body information to cause a fork: Once an honest miner has mined a legitimate block after Bn to post in the blockchain network, the attacker quickly broadcasts the full block body information of Ba. At this point, other miners will see the full contents of Ba. If the block body of the attacker's block Ba contains valid transactions and meets the consensus rules of the blockchain network, other miners may accept Ba as a valid block and continue to mine on it. As more honest miners mine new blocks based on Ba, the blockchain will fork, as shown in Figure 5.

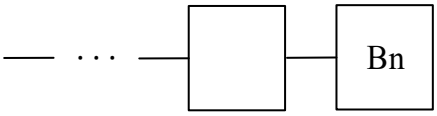

Figure 2. Blockchain Initial state

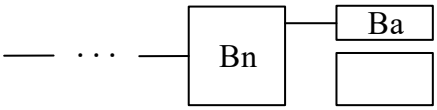

Figure 3. Behavior of Attacker A

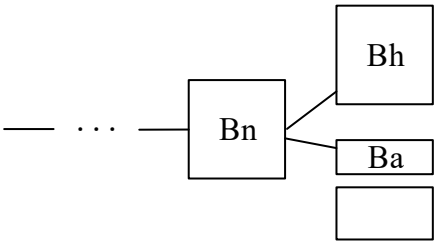

Figure 4. Reaction of other miners

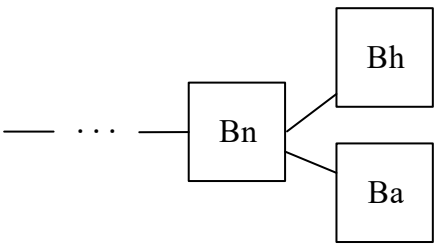

Figure 5. Blockchain fork state

3.2. SDoS attack

SDoS (Selfish Mining-Based Denial-of-Service) attack is a blockchain attack that combines selfish mining and denial-of-service (DoS) attack. The attacker first adopts a selfish mining strategy, not immediately releasing the mined blocks into the blockchain network, but keeping these blocks to form a private chain, waiting for the opportunity to choose a favorable time to release them, which leads to the honest miner's block to become an orphaned block, wasting its computational power to enhance the attacker's own mining revenue.

Initial state (Figure 2): the main chain of the blockchain is currently forkless, and all miners (both attackers and honest miners) are competing together for the same block (block Bn) and continue mining after block Bn. At this point, the blockchain is in a normal state with no forks.

What happens after an honest miner mines (Figure 2): an honest miner successfully mines the next legitimate block after block Bn (assumed to be block Bh). As an honest miner, they publicly broadcast all information about that block (including the block header and block body) to the network. Other miners (including attackers) will see the block Bh mined by the honest miner and continue mining based on that block. At this point the blockchain state is forkless and all miners continue to extend the same main chain.

The attacker mines after block Bn and hides the information (Figure 3): the attacker successfully mines a legitimate block after block Bn (assumed to be block Ba), but unlike the honest miner, the attacker does not make all the information about the block public, but only publishes the block header (important information such as the block's hash, timestamp, and so on) and hides the block body (i.e., transaction information). In this way, two chains will appear in the blockchain: one is the chain that honest miners continue to mine based on block Bn, and the other is the attacker's private chain that is mined based on block Ba (the chain that hides the block body). At this point, the blockchain system of the entire network starts to fork.

Honest miner's choice (Figure 4): In the case of Figure 3, honest miners need to make a choice: they can choose to continue mining after block Bn, or they can choose to stop mining. If the honest miner chooses to continue mining after block Bn and successfully mines the next block (assuming block Bh), they will publicly broadcast block Bh to the network. An attacker who sees the honest miner's publicized block Bh will quickly broadcast his previously mined block Ba, creating a fork of the blockchain. As shown in Figure 5.

The attacker continues mining (Figure 6): if the honest miner mines block B1 after block B, but the attacker continues mining another block after B1 (assumed to be block Baa), the attacker will add Baa to his private chain. In this way, the attacker's private chain will become longer and more competitive, while the honest miner's block (e.g., B1) will likely be discarded. Blockchain reorganization may occur in the network, and the attacker's private chain will eventually be chosen as the main chain.

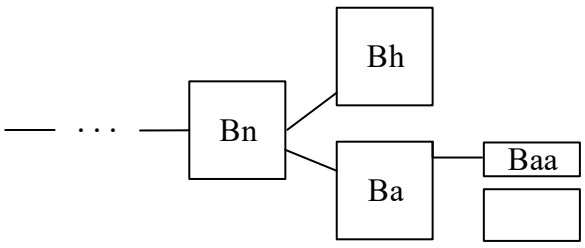

Figure 6. The attacker continues mining

4. Proposed Solutions

This section briefly describes the proposed approach to avoid BDoS attacks and SDoS attacks.

In Section 3, we know that the essence of SDoS attacks is still blockchain denial-of-service attacks, so in the following we mainly discuss the design of blockchain denial-of-service attack defense mechanisms. The main working principle of the latest scheme [10] for defense mechanisms against BDoS attacks is to add a virtual block b_{dummy} at the end of the main chain with an interval of block creation time r plus overhead e, where r denotes the block generation time of the miner in the blockchain network and e denotes some additional time for block propagation. For example, in the Bitcoin blockchain, the value of r is 10 minutes. In a blockchain system where there is a situation where only the block header is published, when the time is greater than $r+e$, the technique will automatically create a virtual block b_{dummy} on the existing public master branch to avoid an attacker from maliciously causing a fork in the blockchain, as shown in the figure 7.

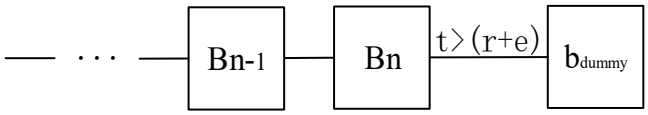

Figure 7. Proposed solution to solve BDoS.

And who is responsible for creating virtual blocks is an important issue that has not been addressed in the paper [10]. We use game theory to create a spontaneous reward and punishment mechanism to solve the problem, transforming the trust problem into an economic one. As follows:

To determine whether a virtual block needs to be added and to create that block, we try to introduce another new role among the miners called the regulator S. The regulator S is chosen from the normal participants of the blockchain. $S_{set}=\{s_1,s_2,s_3,...,s_n\}$ is the set of n regulators. The regulator has two actions $a_k^{(y)}$ and $a_k^{(n)}$. $a_k^{(y)}$ means that regulator $k\left(k=1,2,3,...,n\right)$ reports that a virtual block needs to be added (there is no full block published in time $r+e$). $a_k^{(n)}$ means that regulator $k\left(k=1,2,3,...,n\right)$ reports that a virtual block does not need to be added (there is a full block published in time $r+e$). We are hoping that the n regulators are honest, so we are going to prove this by introducing game theory and Nash equilibrium, with the aim of mathematically predicting and capturing behaviour in a strategy scenario where the rewards for each regulator depend on their own and others' strategies.

Definition of the reward function: when no full block is announced in $r+e$ time, it is necessary to add a virtual fast. At this time:

$$Pay(x)=\begin{cases}10, x=a_k^{(y)}\\ 0, x=a_k^{(n)}\end{cases}$$

When a full block is published in $r+e$ time, there is no need to add a virtual fast. At this time:

$$pay(x)=\begin{cases}-1, x=a_k^{(y)}\\ 1, x=a_k^{(n)}\end{cases}$$

Where 1 represents one award, 10 represents ten awards, and -1 represents the loss of one award.

Here we analyse the three regulator (s_1,s_2,s_3) games as an example. Table 1 shows how much the regulators gain under various combinations according to the defined reward function.

Table 1. Reward Function for a three- regulator Game

s_1	s_3			
	$a_3^{(y)}$		$a_3^{(n)}$	
	s_2		s_2	
	$a_2^{(y)}$	$a_2^{(n)}$	$a_2^{(y)}$	$a_2^{(n)}$
$a_1^{(y)}$	$(10,10,10)$	$(10,0,10)$	$(10,10,0)$	$(-1,1,1)$
$a_1^{(n)}$	$(0,10,10)$	$(1,1,-1)$	$(1,-1,1)$	$(1,1,1)$

where $(1,-1,1)$ denotes: regulator s_1 receives 1 reward under action $a_1^{(n)}$, regulator s_2 loses 1 reward under action $a_2^{(y)}$, and regulator s_3 receives 1 reward under action $a_3^{(n)}$.

If a violation occurs, the regulator knows that most other regulators are more likely to report the event for higher revenue. Thus, higher revenue motivates the regulator to report the event. Conversely, if there is no violation, the regulator knows that most other regulators are more likely to remain silent. While the regulator wants the highest revenue, it must take a significant risk in paying the penalty for its fraudulent behavior. From a global perspective, all regulators tend to remain silent when there is no violation, so to maximize revenue, the regulator must be honest.

5. Solution Analysis

The proposed solution successfully avoids BDoS attacks and prevents the selfish mining problem. However, the solution has some limitations. The analysis of the proposed solution is described below.

The way in which the regulator is selected is crucial, as it is directly related to the decentralization and fairness of the system. If there are loopholes in the regulator selection mechanism, it may lead to problems of centralization, which in turn affects the fairness and security of the network. For example, if the regulator is selected through some centralization, or if the selection mechanism lacks sufficient randomness and transparency, it may lead to certain mining pools or groups of miners controlling the allocation of regulator roles by controlling more arithmetic power or resources. In this way, these mining pools or small groups are able to manipulate the decision-making of virtual block generation at critical moments, and thus influence the consensus process of the network. This centralization phenomenon may not only undermine the decentralized spirit of blockchain, but also lead to the regulator's decisions being biased in favor of certain specific interests, thus harming the interests of participants across the network. In order to avoid such problems, it is necessary to ensure the fairness and transparency of the regulator selection mechanism, and fully consider the principle of decentralization to avoid the control of the regulator role by a single entity. How to ensure the fairness of the regulator role and avoid certain large mining pools or malicious actors manipulating the selection of the regulator in some way?

How to design reasonable incentive and penalty mechanisms is key to realizing this option. If the incentives are insufficient, regulators may be reluctant to take responsibility, resulting in a failure to implement the mechanism, while too high an incentive may trigger moral hazard, with regulators potentially abusing their roles for personal gain. Similarly the implementation of penalties is more complex and it is a challenge to ensure that they are fair and effective. If penalties are unfair or unenforceable, regulators may circumvent them, affecting the normal operation of the system. Therefore, incentive and penalty mechanisms need to be precisely balanced to ensure that incentives and penalties are both fair and enforceable.

6. Conclusion

Bitcoin, the world's first decentralized digital currency, provides a high degree of security and transparency with its distributed network based on blockchain technology. However, with the widespread use of Bitcoin and other blockchain systems, cyber-attacks have become a major issue threatening their stability and security. Among them, BDoS (Blockchain Denial of Service) and SDoS (Selfish Denial of Service) attacks, in particular, pose a threat to the Bitcoin network. Since Bitcoin adopts the Proof of Work (PoW) mechanism, attackers force miners to stop mining or waste computational resources by means of manipulating block rewards and creating chain forks, which affects the normal operation of the network.

To deal with this problem, this paper proposes a defense strategy based on blockchain technology and game theory, which adopts the role of “regulator” and reward and punishment mechanism to reduce block forks and improve the stability of the Bitcoin network. The scheme analyzes the behavior of the regulator through game theory to incentivize him/her to perform his/her duties honestly and prevent selfish mining and misuse of virtual blocks. Unlike traditional methods, this scheme does not need to modify the existing protocol and enhances the protection capability without changing the PoW mechanism by optimizing the regulator selection and reward and punishment mechanisms.

Despite its feasibility, the scheme still faces challenges. First, how to select the regulator in a fair way to avoid manipulation by mining pools or small groups is the key issue. Second, the balance of incentives and penalties needs to be carefully designed to avoid low incentives leading to non-performance of the regulator or high incentives triggering moral hazards. In addition, the fairness and effective implementation of the punishment mechanism are also difficult. Although the scheme effectively improves the defensive capability, further optimization is needed to ensure long-term stable operation.

References

[1] S. Nakamoto and A. Bitcoin. A Peer-to-Peer Electronic Cash System.[Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] I. Eyal and E.G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in Proc. Int Conf. Financial Cryptography Data Secur. Chanm, Switzerland: Springer, 2014, pp. 436-454.

[3] K. Nayak, S. Kumar, A. Miller, E. Shi, “Stubborn mining: Generalizing selfish mining and combining with an eclipse attack,” in Proc. IEEE Eur. Symp. Secur. Privacy, Mar. 2016, pp. 601-619.

[4] Wang W, Hoang D T, Hu P, et al. A survey on consensus mechanisms and mining strategy management in blockchain networks[J]. IEEE Access, 2019, 7: 22328-22370.

[5] Rosenfeld M. Analysis of bitcoin pooled mining reward systems[J]. arXiv preprint arXiv:1112.4980, 2011.

[6] Eyal I. The miner's dilemma[C]//2015 IEEE Symposium on Security and Privacy. IEEE, 2015: 89-103.

[7] M. Mirkin, Y. Ji, J. Pang, et al., “BDoS: Blockchain denial-of-service,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur.,Oct.2020,pp. 601-619.

[8] Q. Wang, T. Xia, D. Wang, Y. Ren, G. Miao, and K. R. Choo, “SDoS: Selfish mining-based denial-of-service attack,” IEEE Trans. InfForensics Security, vol. 17, pp. 3335–3349, 2022.

[9] J. Zhang, C. Zha, Q. Zhang and S. Ma, "A Denial-of-Service Attack Based on Selfish Mining and Sybil Attack in Blockchain Systems," in *IEEE Access*, vol. 12, pp. 170309-170320, 2024.

[10] Habib, M. A., & Manik, M. M. H. (2023, October). A technique to avoid Blockchain Denial of Service (BDoS) and Selfish Mining Attack. In 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA) (pp. 585-590). IEEE.