Quantified Analysis of Security Issues and Its Mitigation in Blockchain Using Game Theory

Ashis Kumar Samanta[1](✉), Bidyut Biman Sarkar[2], and Nabendu Chaki[3]

[1] Department of Computer Science and Engineering, University of Calcutta, Kolkata, India
aksdba@caluniv.ac.in
[2] MCA Department, Techno International Newtown, Kolkata, India
bidyut.biman.sarkar@tict.edu.in
[3] Department of Computer Science and Engineering, University of Calcutta, Kolkata, India
nabendu@ieee.org

Abstract. Storing data in the Blockchain is indeed one of the good security measures for data. However, blockchain itself could be under different types of security threats. The mining of the block into the longest chain is a constrained task. Typically, the nodes having high investments are selected as potential miners in the blockchain. A miner or a pool of miners is assigned for this mining job. The challenge lies in working with the honest miners against the continuous negative influence of dishonest miners. There have been considerable efforts in the existing literature that tries to overcome such security threats. Game theory is used and incorporated towards this by many researchers. This manuscript aims to analyze different security threats of blockchain mining and the possible approaches that have claimed to overcome these. We also analyzed and correlated some of the selected well-cited solution approaches that uses game theory and presented a comparative performance analysis among those.

Keywords: Block-chain · Smart contract · Data security · Security threat · Game theory

1 Introduction

Security and transparency of data are among the primary aspects behind introducing the blockchain (BC) technology. Using the blockchain technology the distributed, pair to pair ledger is made available to all the authorized users within the network in a secured manner. Blockchain technology is used by blending multiple technologies like pair to pair network, distributed and decentralized network technology, cryptography, etc. [3]. A blockchain may be public or private. The transactions are generated as a block. Subsequently, the blocks are verified before these are appended to the longest chain in the network. Each block contains a block header. The block header contains a hash function. This hash value is the main building key-window of blockchain technology. The hash value of the block itself is one of the main security issues as well as a solution to the network. Transactions done by the users are stored within the blockchain. The writing

P. Dutta et al. (Eds.): CICBA 2021, CCIS 1406, pp. 3–19, 2021.
https://doi.org/10.1007/978-3-030-75529-4_1

responsibility of the block is normally assigned to the selected nodes of the network called miners or set of miner pools. The miners are selected depending upon the various protocols and consensus algorithms. The miners are also interested to write the block into the blockchain for their incentives. The transaction fees paid by the transaction blocks are the main incentives of the miner blocks [12]. The security issues of the blockchain are quite much dependent on the performance of the miners. The question arises that at what extent the miners are trustable. Different protocols and consensus algorithms, used in blockchain, are indeed quite matured to identify any dishonest miner, at the instant of any mining process. However, the major threat to blockchain security could be due to the selection of a dishonest miner pool for the process of mining.

The intensive and the deep study give us a specific idea about the security attack experienced by the blockchain at the time of mining of the block. In this particular paper, we analyzed a different kind of security threats faced by the blockchain and also different approaches to overcome this threat using game theory. We also tried to correlate the result of paper [4] and paper [6] and also analyzed the possible outcomes. The comparative analysis of both the paper is presented at the end.

2 Existing Security Issues in the Blockchain

The prime objectives of blockchain technology are the security, transparency, and trustworthiness of transactions and data. Based on the detailed and intensive study on the blockchain, we infer that blockchain is still suffering from various security issues that are presented below.

2.1 Security Issues

2.1.1 51% Vulnerability Issue

The mining power is assigned to the selected nodes in the blockchain network, based on a consensus mechanism called Proof of Work (PoW). If the strength of a mining pool increases more than 50% of the entire selections, then the said pool becomes the miner controlling pool of the chain. If the dishonest miners achieved a majority of 51%, then the hashing control would be a serious security threat for the chain [6, 9].

2.1.2 Double Spending Issue

The mining process (PoW based) is time-consuming. In case of bitcoin, the average mining time of a transaction block is 10 min or more. The dishonest users of the network generally used the same currency (or cryptocurrency) for multiple transactions. This double-spending attack has a fairly high probability of chances due to the short time interval between the two transactions and a long time interval between the receiving of mining acknowledgment of the transactions [11].

2.1.3 Mining Pool Attack Issue

This kind of attack increases the time interval of assigning mining control to the selected miners. The internal pool is attacked by dishonest miners to collect more rewards. The miner then functions maliciously. In case of an external mining pool, the dishonest miner applies higher hashing power to organize a double attack [7, 8].

2.1.4 Distributed Denial of Service Attacks (DDoS) Issues

In the blockchain, the target of the DDoS attack is to retardate the efficiency and activities of the miner pool so that their operation can be disturbed or made to function at a reduced level [4, 5].

2.1.5 Client-Side Security Threats

The blockchain networks maintain public and private key values to manage user accounts. The loss of private keys is also a threat to client-side security [7].

2.1.6 Forking Issue

The software that supports the blockchain framework usually requires system upgradation from time to time. The upgradations may be in terms of hardware, change in the policy of software, or may change in rules of the blockchain. The existing nodes in the network adopting the new upgraded policy and rules form a new blockchain. The nodes that did not upgrade themselves remain in the old chain. There is a lack of compatibility, mutual agreement, and stability between the old and new versions of the chains. That is also a threat to the entire blockchain system [2].

2.1.7 Private Key Security Issues

The private key of the users is one of the security measures in blockchain technology. It describes the credibility of the user. The loss or theft of private keys is a threat to the user as well as the blockchain, as it is not possible to recover the private key by any alternative measure [2].

2.1.8 Criminal Activity Issues

Blockchain suffers from so many criminal threats like bribing, hacking transactions, and extortion money by incorporating "Ransomware" etc. [2].

2.2 Game Theory

"A game is any situation in which players (the participants) make strategic decisions - i.e., decisions that take into account each other's actions and responses" [1]. All the strategic decisions have connected pay-offs that result in rewards or benefits for the players. The players are the decision-makers of their own and always choose strategies towards optimization of payoffs by utilizing the available sets of strategies. In-game theory, it is also considered that the players are rational and their decisions are also rational. Some of the well-known game types are mentioned below.

1. Non-Cooperative Game
2. Cooperative Game
3. Splitting Game
4. Mean-Payoff game
5. Stochastic Game
6. Cournot Game
7. Stackelberg Game
8. Sequential Game
9. Repeated Game
10. Coordination Game

3 Literature Review

In paper [3], a dynamic Bitcoin (BTC) mining process is proposed. The mining powers (electricity) are invested by respective miners. In this paper, one block is mined by a particular miner. The proposed process is described by incorporating the game theory. The miner writes the block into the chain wins the game among all miners. The co-operative and non-cooperative strategies are used by the miners for the mining process. Three dynamic components of game theoretical models are proposed to find the solutions. These three components are Social optimum, Nash equilibrium, and myopic Nash equilibrium.

a. Social optimum
The co-operation strategy is taken by each miner separately or in the pool to consume the energy to compute. The incentive (pay-off) is distributed equally among each miner in the pool.
b. Nash equilibrium
The non-co-operation (selfish mining) strategy is adopted to maximize the gain of each miner and the pay-off is calculated accordingly.
c. myopic Nash equilibrium
Multiple players (miners) can participate in this dynamic game to maximize one's pay-off with the negligible influence of the present state of the miners.

The consumed electric power is invested jointly by all the miners to participate in the mining process. The wasting of the electrical power by all the miners excluding the miner that owned the game and writes the block into the longest chain. The wastage of electricity (power) consumed is the main problem definition in this paper during mining as the main threat. The proposed solutions claimed that the profit of the miners at an optimum level in case of a cooperative game strategy.

The miner nodes in the mining pool increase their outputs either by cooperating with the mining pool or by investing additional resources and the addressing of the threat of DDoS in the blockchain is done in paper [4]. How the dishonest mining pools stimulate to degrade the efficiency of the actual mining pools to build the confidence of the next PoW has been analyzed. This is done either by increasing the resource of dishonest minor pool or in some other menacing ways. To analyze the fact, non-cooperative game theory has been chosen. Two different sized mining pools are considered as the two players - S (small) and B(big) pool respectively. The strategical pay-off matrix has been calculated and the best strategy is described through Nash Equilibrium. The result of the paper states that the incentive is much more for attacking B-pool by removing one or more miners from the pool than by attacking the S-pool. (Large pool attack = 63%, Small pool attack = 17%), i.e. the S-pool makes a higher gain by attacking the B-pool than the gain B-pool makes by attacking S-pool. This paper describes the primary focus of to reduce the performance and hampered the effectiveness by DDoS attack.

1. The operation of the computing mining pool slower down.
2. Encourage individual miners to associate with the dishonest mining pool.

In the proposed model the baseline cost of failure the attack in blockchain mining has been discussed. The impact of the miners of the choice of different investment has also been analyzed.

In paper [5], a long term mining strategy of blockchain through repeated games has been introduced. The objective is to give incentive to an honest miner and simultaneously penalize a dishonest miner. After each iteration of the game, the "reputation" of the miners are measured. This paper primarily addresses the DDoS attack of the type.

1. *Block withholding attack*: where the dishonest miner provides a partial solution of verifications. The total solution is provided to the entire pool with a partial contribution to each and earns the incentive without effective investment.
2. *Selfish mining or Stubborn mining*: a miner (or group of miners) increases their revenue by strategically withholding and releasing blocks to the network. Typically, we expect a miner to announce a block as soon as they find it. If the block is confirmed, they will get the block reward.
3. *Eclipse attack*: the attack aims to obscure a participant's view of the peer-to-peer network, to cause general disruption or disturbed the performance.

A concept of a miner manager is introduced in this model. The miner manager invites the subset of the miner pool for mining. The Nash equilibrium is reached by eliminating the strictly dominating strategy.

In paper [6], a model of sequential game theory is developed to address the DDoS attack on the mining pool. The model describes the short term as well as the long term attacking effects of mining pools. The threshold value of non-attacking incentives and the passive intensive of partial attacking is calculated. The conditions of no-incentive (attack) and incentive (no-attack) are calculated accordingly. This model is calculating the cost (fixed cost as well as variable cost) of the attack. A defensive mechanism is incorporated to calculate the unit cost of attacking. After each round, the miner can migrate from one pool to another according to its regaining strategies. In each round, the miner can go for the attack to lose its incentive as a short term effect. The miner can go for a long-term migration effect to give consistency for the next round, to reach a steady-state of Nash equilibrium. On violating that when one miner is attacking the other one, the Nash equilibrium deviated.

In paper [7], a punishment mechanism is proposed to the devices of edge networks rather than the miner pool of Blockchain. When a request or DoS attack on the server is encountered by a device of edge network, the server may give the output of the request or punish the device. A model is developed for this punishment mechanism through non-cooperative game theory. Both the device and the server can adapt its strategy depending on the history recorded in the blockchain. This model states that to achieve the maximum gain both the players (edge device and server) will not attack each other, because of the extensive punishment mechanism. This non-attacking response brings the game to the horizon of the Nash equilibrium.

In paper [8], a decentralized protocol of mining is proposed where the validator does not consider the Proof of Work (PoW). The validator is chosen from a random set and size to overcome Benzamine 1/3 (one-third) fault tolerance to minimize the attack. Game theory has been used to resolve the problem. The validators were not selected previously. The efficiency of the transaction is enhanced by allowing some of the miners to mining work among the group of selected validators. Most of the emphasis has been given on the selection procedure of the miners to a trade-off between the efficiency and security of the chain.

In paper [9], a bribing aspect of a smart contract using the electronic voting system is analyzed. The incentive (gain) is achieved by the mining nodes by mining the transaction of the smart contract of cryptocurrency. The transfer of bitcoin from one user to another user in a smart contract is considered as bribes. The game theory used here is the "Smart contract bribe game". The type of risks are handled through a proposed election voting model in two ways.

1. The identification of honest and dishonest bribers (mining nodes) function as the miner of transactions of the smart contract.
2. The threshold budget value of bribers to achieve more than 50% vote is only possible if the bribers control more than 20% of the Nash equilibrium.

In paper [10], the incorporation of the evolutionary game has been done. This paper has explored the sharing mechanism to maintain an optimum security level in data mining in smart contract applications. The strategy of handling of sharing of data (data mining) using evolutionary game theory. The proposed model handle three situations.

1. Neither of the player sharing the data or not taking part in mining.
2. Both the player taking part in data sharing.
3. One player taking part in data sharing and the other user is not involving in data sharing.

In paper [11], the Game theory is applied to Smart contract security enhancements. This model proposed to make it decentralized under the strict vigil of its validator to combat the challenger of validation. The paper analyzes and validates "Differentiated Services Code Point (DSCP)" using the tool of smart contract "BITHALO'. The tool has been designed by applying traditional mathematical methods and game theory. The double-spending attack is primarily countered in this paper using game theory. This protocol is used to the vigil at the time of deposit. It verifies the pre-requisite payment amount exceeds the value of the goods to counter the double payment threat.

Authors in paper [12], have proposed to analyze the participation of the miner. It analyses where the incentives are high for participating miners and marginally low incentives for non-participants in the mining process. In a real sense that affects the security measures of the blockchain. The analysis mechanism done here aims to find out the gap in the mining process by incorporating "Gap Game". The game contributes to finding out the average time quantum required for a miner to become active for the honest mining process. The average incentive is assigned to the mining block. It assumes a quasi-static system in which no miner can join or can go out of the respective pool to reach the equilibrium system. The fixed set of miners controls an individual rig (the mechanism used for the mining process, requires electrical power for its function). The start of the rig is determined with a timestamp marking the point of time of conversion of the status of the miner from inactive to active. This paper mainly deals with the mining gap of the blockchain. The gap model considers only the operational expenses. The block size in the blockchain is unbounded; the mining process includes all the pending transactions in the process. When a block is generated, there would not be any pending transactions and unclaimed fees. However, there would not be any incentive due to the mining of the previous block, as there is a gap between the generation and mining between the previous and next block of the blockchain. The findings of papers 3 to paper 12 are illustrated in the tabulated format in Table 1 below.

The Proof of Work (PoW) is a complicated consensus algorithm, used for the mining process of blockchain. It is used for data validation of legitimate transactions to avoid security threats like DDoS and double-spending. In the selfish mining process, the complicacy and energy-consuming amount of PoW is for hash generation. The miners are competing with each other for their incentives. The complicacy and energy consumption of the PoW system is much greater. The minimum time required to generate a block in the PoW system is more than 10 min. That causes security threats as well.

4 Open Research Issues on Blockchain Security for Data Mining

The Blockchain uses the successful PoW consensus algorithm to secure the blockchain network. Several new consensus algorithms have already been proposed and developed meanwhile. Every algorithm has its own merits and demerits. The aspects are important to understand which consensus algorithm is to be chosen for a specific case.

The study finds that each proposed model has merits and demerits. Our objective is to propose such a model where the maximum identified disadvantages can be eliminated. The blockchain still has the following open research issues related to its security and data mining concerned:

4.1. The security threats are regulated by honest and dishonest mining. Therefore there is always a tussle between secure and insecure environments. Game is also a competition of winners and losers. There may be a zero-zero status in between. Hence a suitable game form needs to be proposed for suitable solutions. Therefore we can explore avenues to sort out the maximum security issues of blockchain through suitable game forms.

4.2. The model may be considered without PoW. Alternately, the Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) or Proof of Capacity (PoC) or Proof of Authority (PoA) or Proof of Elapsed Time (PoET) or Proof of Importance (PoI) or some other factor may be considered for future research work.

4.3. The blockchain contains multiple nodes in the network. The game form that will be considered to overcome the security threats needs to be a multiplayer (nodes) game.

Table 1. The findings of the literature review

Ref no.	Observations
[3]	In reality, the miner has to work under security threat and the pay-off is much less in this proposed model. In dynamic systems, past record PoWs are considered. The model is silent about the present state action of the dishonest miner. The difference between Nash equilibrium and Greedy Nash equilibrium in the non-cooperative method is kept silent.
[4]	In this proposed model, a player will use those strategies which are in binary mode. The player either goes for mining or for DDoS attack to reduce the performance. The model does not discuss the case where any player keeps silent without selecting any strategy and hence does not conclude about how the Nash equilibrium will be affected for the silent players. In case if the value of R is large enough the computational pay-offs for both for the big(B) and small(S) miners ($\frac{\mathrm{B}}{(\mathrm{B+S+R})}$ and $\frac{\mathrm{S}}{(\mathrm{B+S+R})}$ respectively) will be reduced. So another problem is to determine the value of R and how the Nash equilibrium will be maintained in respect to R. In the best response strategies, if S goes for the DDoS attack then B's best strategy also will be the DDoS attack, that contradicts the actual mining interest of the blockchain.
[5]	The introduction of a mining manager is also a good concept for extra vigilance. The introduction of a mining manager will increase mining timing. What strategy will be taken if the mining manager becomes dishonest; how it will affect the Nash equilibrium have not been discussed. The result through any experimental setup or simulation has not been stated for any set of data.
[6]	The concept of the model that the big pool(B) will ways go for mining and the small pool(S) always goes for the attack. This concept contradicts the denial attack of 51% dishonest nodes. Migration from S to B increases the size of the mining pool, B. When the migration happens from B to S the rate of DDoS will increase. In the case of B becomes the dishonest pool then also the security threat will increase. What strategy will be taken in this situation to combat security issues?
[7]	The figures in Theorem-2 and Theorem-4 (fig-a and fig-b) show that the utilities or actions of the server process also diminish along with the diminishing of the performances of the device when the device is punished. In that case, the other read operations of the server for miming will be affected (due to the reduction of performance of the server). How this could be mapped with the security measures of the blockchain? In the case of a multiple payer environment, the Nash equilibrium may be violated.
[8]	The type of risk or the threat that can be combated using the proposed algorithm is also not cleared in the paper. What will be the criteria of a selection of actual miners among the honest mining pools?
[9]	In case of a successful smart contract less than Pj (bribing price), no solution is provided. However, it is not clear how the figure of more than 20% control of the overall budget is reached for a briber to conduct a 51% attack and how Nash equilibrium will be affected.

(*continued*)

Table 1. (*continued*)

Ref no.	Observations
[10]	There may be another case of threat to the system where both the players participate either with one player as honest and the other as dishonest or with both the players as dishonest.
[11]	The mechanism of addressing the double payment issue is silent in this paper.
[12]	The equilibrium point in the quasi-static system cannot be maintained. Joining or leaving cannot be restricted in a real scenario. The inclusion of the time component in the incentives of the miner is a positive contribution to enhancing the security mechanism in mining.

4.4. The introduction of a miner manager or validator leader in a mining process increases the security measures [4, 8]. A suitable alternative also needs to be considered in case of the dishonesty of the miner manager or validity leader.

4.5. Among the honest mining pools, some selected nodes will be allowed for mining work [8] by applying a suitable strategy. This will increase mining efficiency.

4.6. A suitable methodology needs to be adopted so that the honest miners can gain some incentives and the dishonest miner can get the punishment. It also needs to record the silent player who is not taking part in miner voting and consider such a player as a partially dishonest miner.

4.7. To increase the mining efficiency only some miners within the mining pool need to be allowed for mining.

4.8. A strategy needs to be determined that allows threshold limit of the attack and to determine a strategy in case the limit is crossed

4.9. The findings of other mining gaps and the introduction of time constraints can enhance the security features and mining efficiency in blockchain technology. The inclusion of time constraints also strengthens the desired model.

The authors feel that there's a strong need for an efficient security model that addresses, if not all, then most of the issues identified above. In Sect. 5, we have taken two interesting existing models for further study.

5 Analysis of Simulation Result

After a thorough study, we try to analyze the result outputs of the above-mentioned papers with their respective outcomes. In particular, we have considered two models proposed by B. Johnson, A. Laszka and that are described in [4] and [6]. We have analyzed using simulation and tried to present a critical comparison of these two models [4, 6]. A brief definition of these models is included in Annexure 1 for the sake of completeness.

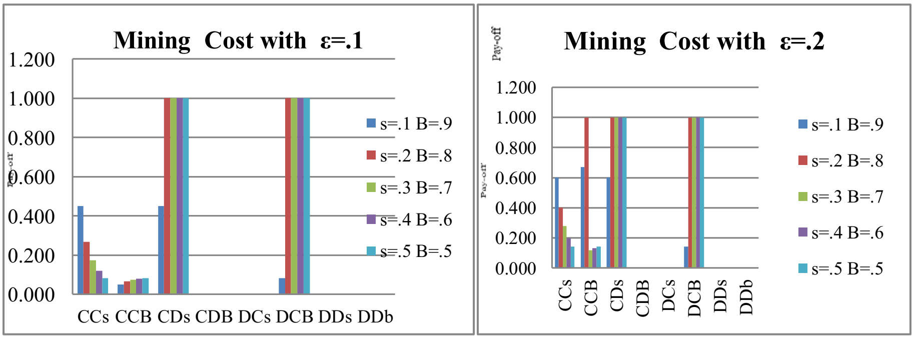
We recapitulate some of the definitions used in the two models [4, 6] for better understanding of the simulation and for proper interpretation of the results. The big and small size mining pools are represented by B and S respectively. R represents the rest of the bitcoin mining market. The rate of increase in computation power is ε. The probability of an attack is σ and γ and λ are two arbitrary constants such that $\lambda < \gamma$. The notations $a_B^{(k)}$, $a_S^{(k)}$ represent the attack pools at any iteration k.

Let, $M \in [0, 1]$ be the rate of migration and $C \in [0, 1]$ is the unit cost of attack. AB and AS are the relative attractiveness of the pool B and S respectively.

Here, $A_B,\ A_S \in [0, 1] \wedge\ A_B + A_S \in [0, 1]$. $S_B^{(k)}$ and $S_S^{(k)}$ are the relative size of the pool at any iteration k, where $S_B^{(k)}, S_S^{(k)} \in [0, 1]$ and $S_B^{(k)} + S_S^{(k)} \in [0, 1]$.

5.1 Discussion on Simulation Result

The payoff matrix of Table 3 [4] is converted into the corresponding data value for further analysis. Figure 1a and Fig. 1b shows the graphical representation of the corresponding data (Shown in [13]). It can be stated that in the Nash equilibrium strategy both B and S will attack each other. However, the best strategy obtained whenever the ratio of B and S is 80:20,70:30, 60:40 and even 50:50. The mining cost is best either S involved in computing or B involved in computing. The value of mining incentive is much better for B:S is 90:10 when the value of ε changes from 0.1 to 0.2.

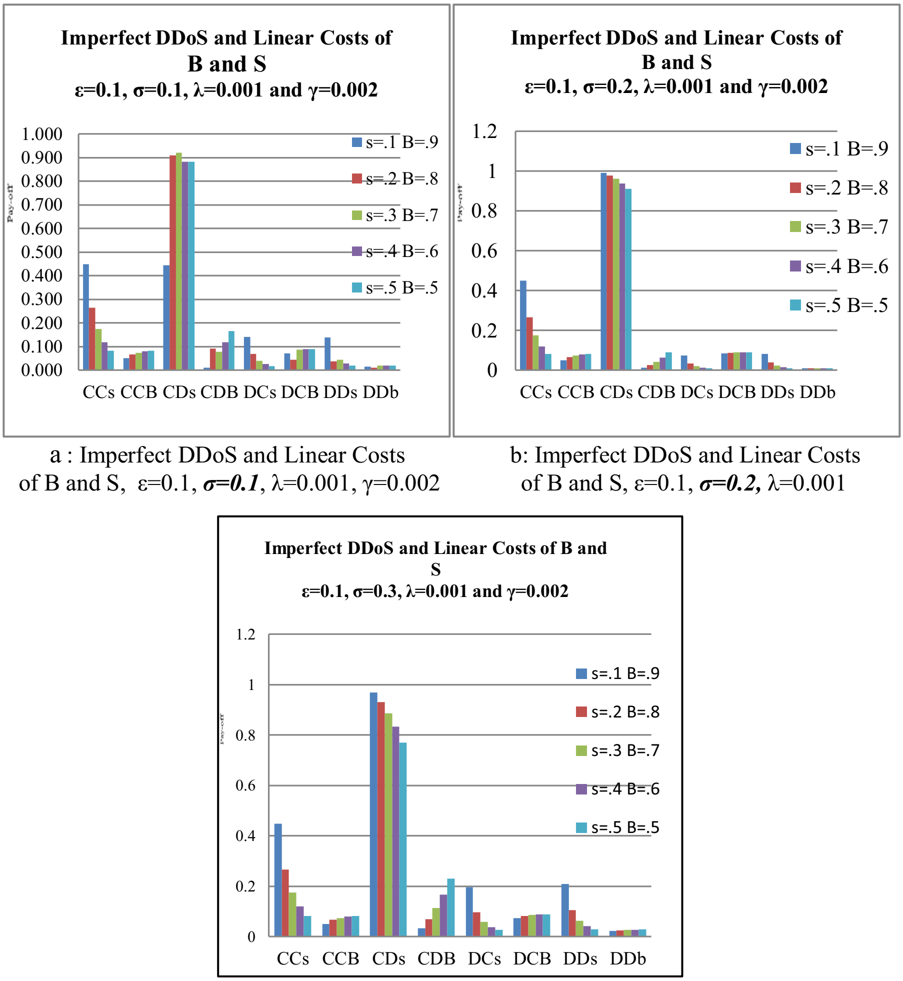


a: Mining cost of B and S with ε=0.1 b: Mining cost of B and S with ε=0.2

Fig. 1. a. Mining cost of B and S with ε = 0.1. **b.** Mining cost of B and S with ε = 0.2

In the enhanced model of [4] as stated in pay-off in Table 4, it is seen that (Fig. 2a, Fig. 2b and Fig. 2c) the highest rate of attack incurred when the S go for computing and B go for the attack. The attack in the enhanced approach is reduced in the CDs component. However, the DCB component of mining of B is get reduced. In general concept, the tendency of attack is increased in the respective areas of DDs and DDB which was nil in the previous case. The computation value of S is decreasing for each size of S with the increasing probability of attack ($\sigma = 0.1, 0.2,$ and 0.3) respectively.

In the peaceful equilibrium in the proposed model [6], the unit cost of attack due to migration has been shown in Fig. 3a (where, As = 0.2, AB = 0.3, $a_s = 0$, $a_B = 0$ and using Eq. 3a). The attacking cost is maximum (near about .6) when the migration rate is 0.1. The rate of the cost of attack reduces with the increased rate of migration until the migration rate is 0.7. After this threshold value (0.7) of the migration rate, the attacking cost remains the same.



a : Imperfect DDoS and Linear Costs of B and S, ε=0.1, ***σ=0.1***, λ=0.001, γ=0.002

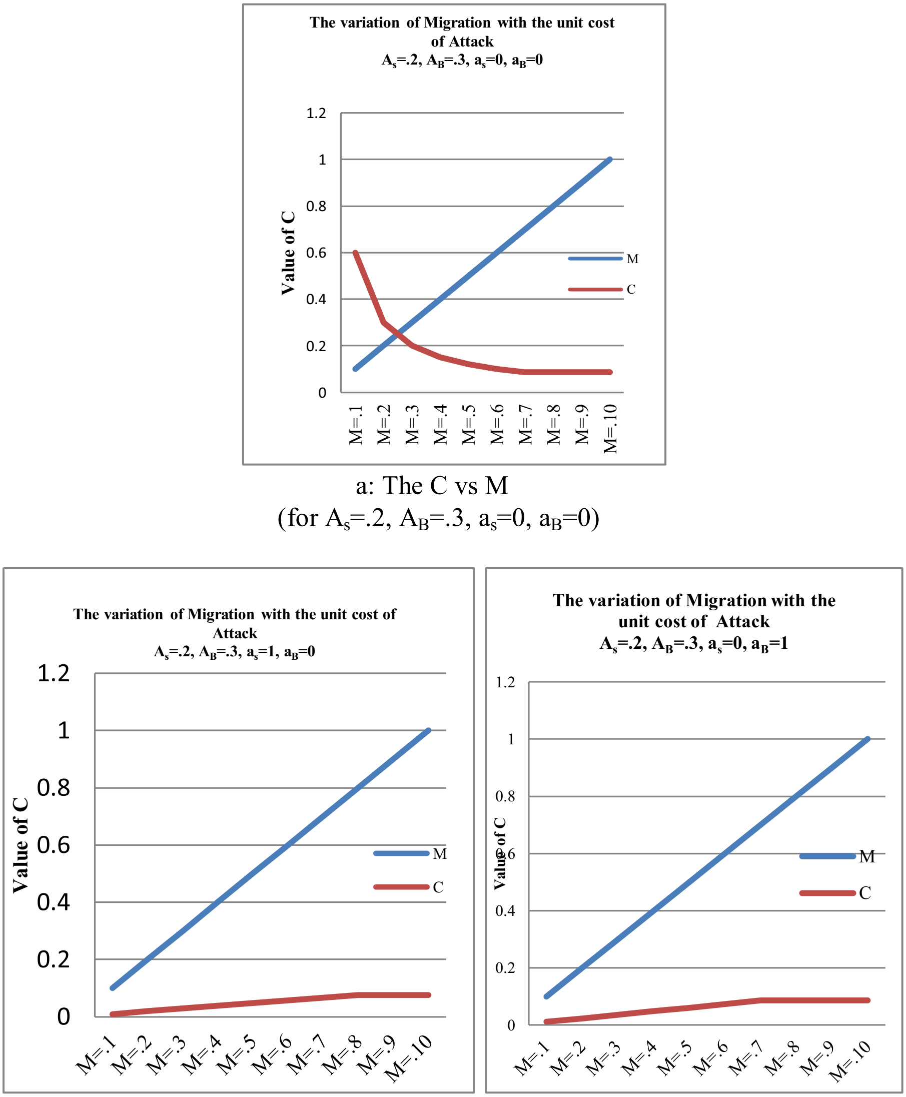
b: Imperfect DDoS and Linear Costs of B and S, ε=0.1, ***σ=0.2,*** λ=0.001

c: Imperfect DDoS and Linear Costs of B and S ε=0.1, σ=0.3, λ=0.001 and γ=0.002

Fig. 2. **a.** Imperfect DDoS and Linear Costs of B and S, $\varepsilon = 0.1$, $\boldsymbol{\sigma = 0.1}$, $\lambda = 0.001$, $\gamma = 0.002$. **b.** Imperfect DDoS and Linear Costs of B and S, $\varepsilon = 0.1$, $\sigma = 0.2$, $\lambda = 0.001$. **c.** Imperfect DDoS and Linear Costs of B and S $\varepsilon = 0.1$, $\sigma = 0.3$, $\lambda = 0.001$ and $\gamma = 0.002$.

In the case of one side attack equilibrium, the unit cost of attack slightly increases with both the cases whether the attacker size as = 1(where $A_s = 0.2$, $A_B = 0.3$, $a_B = 0$ and using Eq. 3b) or the attacker size $a_B = 1$ (where $A_s = 0.2$, $A_B = 0.3$, $a_s = 0$ and using Eq. 3c) shown in Fig. 3b and Fig. 3c respectively.

The value of C is remained equal in Fig. 3a and Fig. 3c after the migration rate is 0.7. The value of C is slightly higher in Fig. 3c ($a_B = 1$) than that of Fig. 3b ($a_S = 1$) for the same set of values of $A_s = 0.2$, $A_B = 0.3$, and M (i.e., migration rate is same in both the figure).



a: The C vs M
(for A_s=.2, A_B=.3, a_s=0, a_B=0)

b: The C vs M
(for A_s=.2, A_B=.3, a_s=1, a_B=0)

c: The C vs M
(for A_s=.2, A_B=.3, a_s=0, a_B=1)

Fig. 3. **a.** The C vs M (for $A_S = .2$, $A_B = .3$, $a_S = 0$, $a_B = 0$). **b.** The C vs M (for $A_S = .2$, $A_B = .3$, $a_S = 1$, $a_B = 0$). **c.** The C vs M (for $A_S = .2$, $A_B = .3$, $a_S = 0$, $a_B = 1$)

5.2 Comparative Analysis of Model

(See Table 2).

Table 2. Critical comparison of models proposed in [4] and [6]

Sl. No	Descriptions	Proposed model [4]	Proposed model [6]
1	Addressing issue(s)	DDoS (by slowing down the performance or motivating the minor to be dishonest).	DDoS attack on the mining pool is addressed.
2	Type of Game Theory incorporated	A non-cooperative game is used.	A sequential Game is used.
3	Mining Strategy	PoW (increases either by cooperating with other miner or investing extra power).	The computation utility value $U_B^{(k)}$ and $U_S^{(k)}$ are used after each round of k by B and S respectively shown in Eqs. 1a and 1b.
4	Pool Size of mines	Arbitrarily chosen Big honest pool (B) and small dishonest pool (S). The variation of size is not reflected in the proposed model.	The relative size of the honest pool ($S_B^{(k)}$) and dishonest pool ($S_S^{(k)}$) is considered after each iteration(k).
5	Cost incurred	It is assumed that the cost to invest or cost to attack is negligible with respect to the revenue of bitcoin. The pay-off cost of B and S is shown in Table 3.	The unit cost of the attack is calculated. The cost of an attack, non-attack and partial attack are also calculated.
6	Migration of B to S or S to B pool	The migration or the attraction of migration is not considered distinctly.	After each round, the miner can migrate from one pool to another pool. At a particular round k, the size of the miner B and S are defined by Eqs. 2a, 2b, 2c, and 2d after migration.
7	Attacking cost or other evaluations	The attack is assumed to be negligible concerning the revenue of bitcoin.	The unit cost of an attack is calculated in terms of fixed and variable costs
8	Nash Equilibrium (NE)	NE is both B and S will attack each other.	NE is expressed through Eq. 3b and 3c.
9	Efficiency	The enhanced proposed model reducing the overall mining efficiency by introducing DDoS attacks in a different stage of mining.	The efficiency can be achieved through a peaceful equilibrium where there is no size of the miner in attacking strategy.

(*continued*)

Table 2. (*continued*)

Sl. No	Descriptions	Proposed model [4]	Proposed model [6]
10	Comparative issues	1. Assumption of no cost of attack or investment. 2. The theoretical background of the assumption value of R, ε, σ, λ, and γ. 3. The attraction of incentives of migration the miner from one pool to another pool.	1. The basis of the assumption of A_S and A_B. 2. The calculation of the unit cost of incentive and also the threshold value of the incentive to get initiated the mining process. 3. The silent miners are also taken into consideration.

6 Conclusions

In this paper, we have analyzed some of the security solutions for blockchain mining that have used different game theory approaches. We have presented graphical results for simulation. We have also changed the values for the rate of increase in computation power, ε from 0.1 to 0.2 (in case of the model represented in [4]) and the probability of attack σ from 0.1 to 0.2 and 0.3 (in case of the model represented in [6]) to find out the change in the behavioral response of the said models. The results are evident in Sect. 5. With the increase of investment of mining resources, the profit increases up to a certain limit before it saturates In a process of the non-cooperative game theory approach, we have seen that the cost of computation is high when B goes for computing and S go for attack for all combinations of B and S (80:20,70:30, 60:40, 50:50) excepting 90:10. With the introduction of the probability of attack the mining value decreases. The introduction of the pool manager and its invitation to the set of potential miners provide the extra vigil to the mining security. It is shown that the unit cost of an attack decreases with the increasing rate of migration to the attacking pools. In fact, after crossing a threshold value of migration, the cost of attack does not change. In case of increasing the punishment rate to the dishonest miner, the utility rate does not change. In future, we plan to focus on the policy of selection of miners using game theory and also shall put an effort to find out the threshold mining and attacking cost to eliminate the security threat of blockchain mining in an improved way.

Annexure 1

Formalism in the Model Proposed by B. Johnson, A. Laszka et al. [4]

The payoff is defined for B and S of DDoS attack and computation is

Table 3. The pay-off matrix of mining of B and S

		Player B	
		Computation	*DDoS*
Player S	*Computation*	$\frac{\mathrm{B}}{\mathrm{B+S+R}}, \frac{\mathrm{S}}{\mathrm{B+S+R}}$	$\frac{\mathrm{B}}{\mathrm{B+R(1+\varepsilon)}}, 0$
	DDoS	$0, \frac{\mathrm{S}}{\mathrm{S+R(1+\varepsilon)}}$	0, 0

Table 4. Payoff Matrix for B and S with Imperfect DDoS and Linear Costs

		Player B	
		Computation	*DDoS*
Player S	*Computation*	$\frac{\mathrm{B}}{\mathrm{B+S+R}} - \gamma\mathrm{B},$ $\frac{\mathrm{S}}{\mathrm{B+S+R}} - \gamma\mathrm{S}$	$\frac{\mathrm{B}}{\mathrm{B+(\sigma S+R)(1+\varepsilon)}} - \lambda\mathrm{S},$ $\frac{\sigma\mathrm{S}(1+\varepsilon)}{\mathrm{B+(\sigma S+R)(1+\varepsilon)}} - \gamma\mathrm{S}$
	DDoS	$\frac{\sigma\mathrm{B}(1+\varepsilon)}{\mathrm{S+(\sigma B+R)(1+\varepsilon)}} - \gamma\mathrm{B},$ $\frac{S}{\mathrm{S+(\sigma B+R)(1+\varepsilon)}} - \lambda\mathrm{B}$	$\frac{\sigma\mathrm{B}}{\sigma\mathrm{(B+S)+R(1+\varepsilon)}} - \lambda\mathrm{S},$ $\frac{\sigma\mathrm{S}}{\sigma\mathrm{(B+S)\ R(1+\varepsilon)}} - \lambda\mathrm{B}$

Formalism in the Model Proposed by B. Johnson, A. Laszka et al. [6]

The ***Short term policy*** The calculated utility function of B and S are $U_B^{(k)}$ and $U_S^{(k)}$ respectively in kth iteration are given by the equn

$$U_B^{(k)} = \frac{S_B^{(k)} \cdot \left(1 - a_S^{(k)}\right)}{1 - S_B^{(k)} \cdot a_S^{(k)} - S_S^{(k)} \cdot a_B^{(k)}} - \mathrm{C} \cdot a_B^{(k)} \tag{1a}$$

$$U_S^{(k)} = \frac{S_S^{(k)} \cdot \left(1 - a_B^{(k)}\right)}{1 - S_S^{(k)} \cdot a_B^{(k)} - S_B^{(k)} \cdot a_S^{(k)}} - \mathrm{C} \cdot a_S^{(k)} \tag{1b}$$

The ***Long term policy*** The calculated size of B and S are $S_B^{(k+1)}$ and $S_S^{(k+1)}$ respectively in k_{th} iteration are given by the equ$^{\mathrm{n}}$

a) Migration of miner into B pool

$$S_B^{(k+1)} = S_B^{(k)} + A_B \cdot [\left(1 - S_B^{(k)}\right) \cdot \ \mathrm{M} \ + S_S^{(k)} \cdot a_B^{(k)} (1 - \mathrm{M}) \tag{2a}$$

b) Migration of miner out of B pool

$$S_B^{(k+1)} = S_B^{(k)} - S_B^{(k)} \cdot (1 - A_B) \cdot \left[\ \mathrm{M} \ + \cdot a_S^{(k)} (1 - \mathrm{M})\right] \tag{2b}$$

c) Migration of miner into S pool

$$S_S^{(k+1)} = S_S^{(k)} + A_S \cdot [\left(1 - S_S^{(k)}\right) \cdot \ \mathrm{M} \ + S_B^{(k)} \cdot a_S^{(k)}(1 - \mathrm{M}) \tag{2c}$$

d) Migration of miner out of S pool

$$S_S^{(k+1)} = S_S^{(k)} - S_S^{(k)} \cdot (1 - A_S) \cdot \left[\mathrm{M} \ + \cdot a_B^{(k)}(1 - \mathrm{M})\right] \tag{2d}$$

In case of peaceful equilibrium where $(a_{S,}\ a_B) = (0{,}0)$

$$\mathrm{C} \ \geq \frac{A_B A_S}{\mathrm{Min}(\mathrm{M}, 1 - A_S, 1 - A_B)}. \tag{3a}$$

In case of one side attack equilibrium where $(a_{S,}\ a_B) = (0{,}1)$

$$\mathrm{C} \leq \frac{A_B A_S}{(1 - A_S)^2} \cdot \ \mathrm{Min}(\mathrm{M}, 1 - A_S) \tag{3b}$$

$$\mathrm{C} \leq \frac{A_B A_S}{(1 - A_B)^2} \cdot \ \mathrm{Min}(\mathrm{M}, 1 - A_B) \tag{3c}$$

References

1. Pindyck, R.S., Rubinfeld, D.L.: Microeconomics, 8th edn. The Pearson Series in Economics (2013). ISBN-13: 978-0-13-285712-3
2. Gupta, N.: Security and privacy issues of blockchain technology. In: Kim, S., Deka, G.C. (eds.) Advanced Applications of Blockchain Technology, pp. 207–226. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-8775-3_10
3. Singh, R., Dwivedi, A., Srivastava, G., et al.: A game theoretic analysis of resource mining in blockchain. Cluster Comput. **23**(3), 2035–2046 (2020). https://doi.org/10.1007/s10586-020-03046-w
4. Johnson, B., Laszka, A., Grossklags, J., Vasek, M., Moore, T.: Game-theoretic analysis of DDoS attacks against bitcoin mining pools. In: Böhme, R., Brenner, M., Moore, T., Smith, M. (eds.) FC 2014. LNCS, vol. 8438, pp. 72–86. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44774-1_6
5. Nojoumian, M., Golchubian, A., Njilla, L., Kwiat, K., Kamhoua, C.: Incentivizing blockchain miners to avoid dishonest mining strategies by a reputation-based paradigm. In: Arai, K., Kapoor, S., Bhatia, R. (eds.) Intelligent Computing: Proceedings of the 2018 Computing Conference, Volume 2, pp. 1118–1134. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-01177-2_81
6. Laszka, A., Johnson, B., Grossklags, J.: When bitcoin mining pools run dry. In: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (eds.) Financial Cryptography and Data Security, pp. 63–77. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48051-9_5
7. Xu, D., Xiao, L., Sun, L., Lei, M.: Game theoretic study on blockchain based secure edge networks. In: IEEE/CIC International Conference on Communications in China (ICCC), Qingdao, pp. 1–5. IEEE (2017). https://doi.org/10.1109/ICCChina.2017.8330529

8. Alzahrani, N., Bulusu, N.: Towards True decentralization: a blockchain consensus protocol based on game theory and randomness. In: Bushnell, L., Poovendran, R., Başar, T. (eds.) Decision and Game Theory for Security: 9th International Conference, GameSec 2018, Seattle, WA, USA, October 29–31, 2018, Proceedings, pp. 465–485. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01554-1_27
9. Chen, L., et al.: The game among bribers in a smart contract system. In: Zohar, A., et al. (eds.) FC 2018. LNCS, vol. 10958, pp. 294–307. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-662-58820-8_20
10. Xuan, S., Zheng, L., Chung, I., Wang, W., Man, D., Du, X., et al.: An incentive mechanism for data sharing based on blockchain with smart contracts. Comput. Electr. Eng. **83**, 106587 (2020). https://doi.org/10.1016/j.compeleceng.2020.106587,Elsevier
11. Bigi, G., Bracciali, A., Meacci, G., Tuosto, E.: Validation of decentralised smart contracts through game theory and formal methods. In: Bodei, C., Ferrari, G., Priami, C. (eds.) Programming Languages with Applications to Biology and Security, pp. 142–161. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-25527-9_11
12. Tsabary, I., Eyal, I.: The gap game. In: 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, USA, Canada (2018). https://doi.org/10.1145/3243734.3243737
13. https://drive.google.com/drive/folders/1aLM7MmyEwEmx_NzCfAMIn4trd0Bl62fp?usp=sharing