Securing IoT Transactions Against Double-Spending Attacks based on Signaling Game Approach

Hafsa BENADDI*, Mohammed JOUHARI*, Khalil IBRAHIMI (*IEEE Senio Member*)*, Abderrahim BENSLIMANE†
*Ibn Tofail University, Faculty of Sciences, LaRI Laboratory, Kenitra, Morocco
†University of Avignon, CERI/LIA, France
hafsa.benaddi@uit.ac.ma, jouhari4med@gmail.com, ibrahimi.khalil@uit.ac.ma, abderrahim.benslimane@univ-avignon.fr

GLOBECOM 2021 - 2021 IEEE Global Communications Conference | 978-1-7281-8104-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/GLOBECOM46510.2021.9685598

***Abstract*—With considerable demand for higher throughput, greater capacity, and lower latency for consumers, the Internet of Things (IoT) network is anticipated to meet the desired security and privacy requirements. This study provides high transaction throughput on critical IoT applications, particularly Bitcoin security against double-spending attacks. To this end, we investigated the signaling game approach to model the interaction between two miners while considering players behavior (malicious or honest miners) and the incoming transaction throughput. To the best of our knowledge, this is the first work that exploits the signaling game to cover the incoming transactions randomness waiting for validation, which influences the honest miners behavior. With extensive simulations, we show that our proposed signaling game reduces the impact of double-spending attacks on IoT transactions. The results also illustrate the benefit of using the signaling game to model the interaction between two miners while handling the incomplete information of the incoming transactions and the type of miners.**

***Index Terms*—Bitcoin Blockchain, Internet of Things, Signaling Game, Double-Spending attacks.**

I. Introduction

Currently, the Internet of Things (IoT) has received significant attention from different fields. Despite the Big Data paradigm's opportunities, the existence of such a massive amount of Big Data leads to security challenges. The information exchange and transaction of devices have shown a significant impact on business and safety. Conventionally, integrating the emerging technology Blockchain in IoT applications [1], [2], [3] is crucial to establish a decentralized autonomous trading platform for IoT networks without a third-party entity. Bitcoin is a widely used digital currency employed by the general public in the payment ecosystem [4]. At the heart of how Bitcoin works is a global public ledger called the Blockchain, which is the enabling technology behind a range of digital cryptocurrencies solved by specific participants called **miners**. However, Blockchain is a chain of blocks using a growing directory of the cryptographic hash block [5] that stores information and digital certificates in a distributed, decentralized network [6], [7]. Miners in bitcoin communicate over Transmission Control Protocol (TCP/IP) [8], but with delays. The delay between fellow miners may differ based on geographic location, physical connection, hardware, software, and message size. For simplicity, we assume that the time delay between every two miners is constant at 10 minutes. Furthermore, validating a Blockchain block requires many calculations in generating a block. Solving all of those mathematical computations with delay impact is called Proof of Work (PoW), and it consists of finding the value of the Nonce field to be filled in the block header so that the hash of the block header leads to a result lower than a particular value over time [9]. If the average time is too short, the difficulty is then revised upwards. If it is too long, the difficulty is reduced. While mining blocks compete, miners require a lot of energy for transmitting, receiving transactions, and validating a certain number of Blocks on the simulated network. The miner who succeeds receives a reward called the mining reward. Bitcoin still suffers from the vulnerability of attacks [10] such as double-spending attacks [11] which is the outcome of using some cryptocurrency more than once at the same time. Likewise, this attack aims to interact with miners to extend the maximum number of blocks with the most available transaction fees that follow the longest chain. However, the main reason for the existing fraudulent miners is the network's delay in decreasing the effectiveness of honest mining pools This paper investigates a novel approach based on a signaling game to model the interaction between two miners. We also aim to improve the efficiency of decentralized and distributed systems through the Blockchain against malicious activities by enforcing the honest miner's validation dynamically and by rewarding the honest miner and punishing the malicious ones in a game.

The *major contributions of this paper* are summarized as follows:

- We proposed a model to reduce the impact of double-spending attacks on IoT transactions;
- We used the signaling game to model the interaction between miners to identify honest miners' best decision policy to win the game against the malicious miner;
- We considered the impact of the transaction throughput on the system's security level, consequently increasing the appearance of more branches, especially when transaction throughput is coming to the network;
- We conducted an extensive simulation to evaluate our proposed model and reach the equilibrium using multiple scenarios.

The remainder of the paper is organized as follows: In section II, we provide a comprehensive background review on the

978-1-7281-8104-2/21/$31.00 ©2021 IEEE

safety of Blockchain, outlining its building blocks, alternative consensus algorithms, and protocols used against intruders. In Section III, a signaling game between two miners is formulated for studying the incoming transaction throughput. In Section IV, performance evaluation is implemented. Lastly, we conclude our investigation, summarize lessons learned, and some possible future research guidelines are presented in Section V.

II. Related Work

Over the past few years, the analytical engine of securing transactions for IoT applications has undergone several learning approaches. This section provides a brief outline of the literature review that uses game theory in the mining competition process in bitcoin to validate new incoming transactions in the network Blockchain. Karame *et al.* [12] presented a new modification of Bitcoin as the first comprehensive study for detecting double-spending attacks for Bitcoin in fast payments where the attacker achieved with an overwhelming probability. In this context, Lewenberg *et al.* [13] suggested a novel modification on the inclusive protocol for behavior changes by nodes, which integrate the contents of off-chain blocks into the Blockchain and lead to higher throughput and payoff of weak miners. The authors recommended including additional analysis on authorization policies of transactions of the protocol under the known attacks. In particular, Altman *et al.* [14] initiated the competition among miners using congestion game to reach a consensus over the public Blockchain and Edge Computing Service Provider (ESP). The authors proved that this study does not account for strategic decisions regarding punishment and cooperation among miners during a repetitive game. Alzahrani *et al.* [15] also proposed a new consensus protocol based on game theory and randomness by using validators at each timestamp a new block is offered to avoid attacks. Moreover, this game aims to reward honest players who join and to penalize dishonest ones. On the contrary, the player with malicious behavior plays in a static way. At the same time, the proposer-leader mapping only guarantees anonymous mapping for a single proposal round. In addition, Singh *et al.* [16] examined dynamic resources in Bitcoin mining using game theory analysis in continuous time. They showed that their results correspond well with the common belief that cooperative mining will be improved over single mining in a non-cooperative game. Motepalli *et al.* [17] described a framework for a reward mechanism that is suitable for many PoS Blockchains. The authors designed the block validation game. Through the use of evolutionary game theory, they discussed how players' behavior could potentially grow with the reward mechanism.

Compared with the existing research on game-theoretical approaches for securing Blockchain [18], our model has the advantage of employing signaling game with incomplete information of players' consideration of the throughput of the network, which decreases the challenge of double-spending attacks on the Bitcoin Blockchain network.

III. Signaling Game Model and Analysis

A. Model Description

Our modeling approach focuses on the incentives of Bitcoin miners to get a payoff by mining blocks into the Blockchain while getting benefits from the time-variance of the incoming transactions waiting for validation and mining. To this end, we proposed using a signaling game to model the interaction between the miners to cover the randomness of incoming transactions, which is defined in this paper as the throughput K. It is known that the signaling game is the most suitable game to handle the stochastic aspect of the mining game. It takes in consideration multiple parameters such as the number of the miners, their hash rate or potential, the number of transactions waiting to be stored/validated, Block size (max number of transactions to be included in a single block), and the mining duration (the time required to mine a single block to the main Blockchain). These constraints make modeling very problematic and are very challenging tasks. Thus we will focus our effort on a particular case of the bitcoin without loss of generality.

Signaling game is known by modeling game with incomplete information through considering the nature impact which determines the type of players and their behavior (their preferred strategies) [19], [20]. In our case, nature determines the number of incoming transactions that should be processed by validating and mining while taking into account to minimize the waiting time of each transaction. This pushes the miners to speed up on mining blocks, decreasing the system's security level and allowing the malicious miners to perform their attacks easily. In a high transaction throughput scenario, multiple honest miners will mine their blocks to different branches, which results in multiple chains with low length as shown in Fig.1. Consequently, the malicious miner will publish its private chain to get the benefits of mining and perform the double-spending attack. Throughout this work,

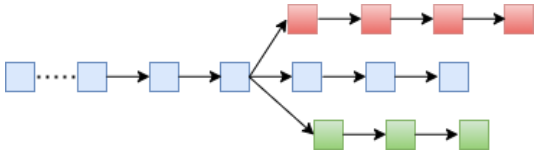

Fig. 1. Double-spending attack scenario: Honest miners mine their blocks to the main chain in case of low transaction throughput aiming to get the payoff of mining (blue blocks). At high transaction throughput honest miners and attacker mine respectively to the fork chain (green blocks) and to their private chain (red blocks).

we present an honest miner as Player I while a malicious miner as Player II, each player has the incentive to win the game by maximizing its payoff. The game depends essentially on the transaction throughput, which is determined by nature. Our game considers two throughput levels, High and Low throughput, determined by the probabilities π_H and π_L following the Poisson distribution such as $\pi_H + \pi_L = 1$. In general, as studied in the literature, miners working in high transaction throughput have a bigger probability of mining

their blocks in a fork other than the main chain, contrarily in low throughput, the miners tend to mine in the main Blockchain. This idea presents the key of our model, which is investigated through its impact on the security level of the system and the behavior of the miners. The probability π_H of high transaction throughput is defined following the Poisson distribution using the parameters μ and K, which are respectively a duration of time and the number of transactions coming during this duration:

$$\pi(K > K_{th}) = \pi_H = \frac{e^{-\mu}\mu^K}{K!} \tag{1}$$

Where K_{th} is the throughput threshold which determines the transactions' type as follows: for $K \leq K_{th}$ and $K > K_{th}$ correspond respectively to low and high transactions throughput levels.

B. Game Analysis

Our game models the interactions between two miners working on validating blocks in the main Blockchain. Each miner can be either an honest or malicious player regarding its strategies and intentions. Some malicious miners work simultaneously with the honest nodes by mining their blocks to the private chain. These attackers wait while the main chain seems shorter to publish their private chain and benefit from mined blocks, knowing that in the case of multiple chains, the longest one is considered the main chain. In addition to the benefit of mining, malicious nodes may change the block information to reuse their Bitcoin, called the double-spending attack. In addition, with high transaction throughput, besides the collision problem where the miners may choose the same subset of transactions to include in the blocks, which causes computation waste and reduces the number of blocks mined in the system, miners may add their blocks to different forks. This reduces the system's security level, wastes the effort of honest miners, and allows weaker attackers to reverse payments.

The strategy of an honest miner (Player I) is defined by its actions depending on the throughput levels. At the same time, the malicious node (Player II) chooses its strategy based on the received signal from Player I and its belief in the received signal. After choosing a strategy from its strategy set S_I Player I send a signal s_x to Player II to inform them about its state without knowing its nature. This signal allows the honest miners to collaborate and mine on the main chain in high throughput transactions. In case of the signal received by the malicious node as Player II, Player I will send a biased signal that can be identified only by honest miners who know the sender's history and the throughput type.

Formally, we write this as follows:

- Player I chooses its strategy from the set of strategies $S_I = \{q_i q_j, ...\}$ and sends a signal s_x to inform Player II of its strategy, where q_i (resp. q_j) corresponds to the action taken by Player I when the transaction throughput is high (resp. low) such as $i, j = 1, 2$. Knowing that Player I can either mine its block to the main chain corresponding q_2 or to the fork corresponding q_1.
- Player II chooses its strategy from the set of strategies $S_{II} = \{p_k p_l, ...\}$ and send a signal r_y to respond to player I, where p_k (resp. q_l) corresponds to the action taken by Player II responding to Player I's action such as $k, l = 1, 2$. Knowing that Player II can either mine its block to the private chain corresponding p_1 or publish its private chain corresponding p_2.

The signal sent by Player I to Player II is determined based on the throughput type as follow:

$$s_x = \begin{cases} 0 & \text{if } q_i = q_1 \text{ and } q_j = q_1, \\ 1 & \text{if } q_i = q_1 \text{ and } q_j = q_2, \\ 2 & \text{if } q_i = q_2 \text{ and } q_j = q_1, \\ 3 & \text{if } q_i = q_2 \text{ and } q_j = q_2. \end{cases} \tag{2}$$

Player II responds by choosing a strategy from its set of strategies based on the received signal and on its belief on the Player I following the above formula. Such as the believe of Player I on the Player II is designed as follow:

$$\beta(s_x) = \begin{cases} 0 & \text{if } \beta \leq \beta_{th}, \\ 1 & \text{Otherwise.} \end{cases} \tag{3}$$

Where β_{th} is the belief threshold of Player II, such as $\beta(s_x) = 1$ means that Player II believe in the signal sent by Player I while $\beta(s_x) = 1$ signify that there is no trust between players.

The response of Player II is designed as follow:

$$r_x = \begin{cases} 0 & \text{if } s_x = 0 \text{ and } \beta(s_x) = 1, \\ 1 & \text{if } s_x = 1 \text{ and } \beta(s_x) = 1, \\ 2 & \text{if } s_x = 2 \text{ and } \beta(s_x) = 1, \\ 3 & \text{if } s_x = 3 \text{ and } \beta(s_x) = 1. \end{cases} \tag{4}$$

$$r_y = \begin{cases} 0 & \text{if } s_x = 3 \text{ and } \beta(s_x) = 0, \\ 1 & \text{if } s_x = 2 \text{ and } \beta(s_x) = 0, \\ 2 & \text{if } s_x = 1 \text{ and } \beta(s_x) = 0, \\ 3 & \text{if } s_x = 0 \text{ and } \beta(s_x) = 0. \end{cases} \tag{5}$$

Where $r_x = 0, 1, 2$ *or* 3, (similarly $r_y = 0, 1, 2$ *or* 3) corresponds respectively to p_1p_1, p_1p_2, p_2p_1 *and* p_2p_2. Such as the response r_x is taken by Player II when he believes in the received signal while r_y is taken when he doesn't believe.

In this game, each player has the incentive to maximize its payoff to win the game by following the best strategy that allows a bigger outcome. The payoff that both players try to achieve is the Bitcoin amount paid for mining blocks, while the malicious player will try to reverse its payment by publishing its private chain. To efficiently study the interaction between these two players, we designed a utility function for each player where we defined the utility function of Player I as follows:

$$\begin{aligned} U_I^H(K > K_{th}, q_i q_j, p_k p_l) = q_i.w_h.(1 - p_k.c_I) \\ + q_i.w_m.(1 - p_k.c_I).\gamma(q_i, p_k) \end{aligned} \tag{6}$$

$$U_I^L(K \leq K_{th}, q_i q_j, p_k p_l) = q_j.(1 - p_l.c_I) \tag{7}$$

$$U_I(K, q_i q_j, p_k p_l) = \pi_H.U_I^H + \pi_L.U_I^L \quad (8)$$

Where w_h presents the gain for Player I from a successful game while w_m is the gain of player II from publishing its private chain and reverse the payment. c_I the risk of player To lose the game, $U_I^H(K > K_{th}, q_i q_j, p_k p_l)$ presents the payoff of Player I playing the strategy $q_i q_j$ for high incoming transaction throughput against the strategy $p_k p_l$ of Player II. Similarly, $U_I^L(K \leq K_{th}, q_i q_j, p_k p_l)$ is the payoff of player I for low transaction throughput, knowing that in this case, honest players have the incentive to mine their blocks to the main chain due to low transaction waiting for validation. While $\gamma(q_i, p_k)$ is defined as follow:

$$\gamma(q_i, p_k) = \begin{cases} -1 & \text{if } q_i = 0 \text{ and } p_k = 0, \\ 1 & \text{Otherwise.} \end{cases} \quad (9)$$

The utility of Player II is based essentially on the received signal and on its belief in the sender. For simplicity, the utility function is described as follow:

$$U_{II}^1(K > K_{th}, \beta > \beta_{th}, s_i, r_x) = \bar{s_i}.\bar{r_x}.w_m + s_i.r_x.c_I.w_m \quad (10)$$

$$U_{II}^2(K > K_{th}, \beta \leq \beta_{th}, s_i, r_y) = \bar{s_i}.r_y.c_I.w_m - s_i.\bar{r_y}.w_m \quad (11)$$

$$U_{II}^3(K \leq K_{th}, \beta > \beta_{th}, s_i, r_x) = s_i.r_x.c_I.w_m - s_i.\bar{r_x}.w_m \quad (12)$$

$$U_{II}^4(K \leq K_{th}, \beta \leq \beta_{th}, s_i, r_y) = \bar{s_i}.r_y.c_I.w_m - \bar{s_i}.r_y.c_I.w_m \quad (13)$$

$$U_{II}(K, \beta, s_i, r_x, r_y) = \pi_H.(\beta.U_{II}^1 + (1-\beta).U_{II}^2) + \pi_L.(\beta.U_{II}^3 + (1-\beta).U_{II}^4) \quad (14)$$

Where $\bar{s_i}$, $\bar{r_x}$, and $\bar{r_y}$ are respectively the complements of the variables s_i , r_x, and r_y. The payoff of Player II is decomposed into fourth parts based on the transaction throughput (K), its belief on the received signal (β), the signal sent by Player I (s_i), and on its strategy r_x, r_y corresponding respectively to the case where it believes on the received signal and when it doesn't. The utility function of Player II was designed based on the parameters mentioned above as follows: **1.** Equation (10) describes the payoff of Player II playing the strategy r_x and believes on the received signal s_i in high transaction throughput. **2.** Equation (11) presents the payoff in high transaction throughout when Player II plays the strategy r_y without believing in the received signal s_i. **3.** Equation (12) depicts the payoff when Player II chooses to play the strategy r_y and believes on the received signal in low transaction throughput. **4.** The formula (13) determines the payoff when Player II uses the strategy r_y and does not believe in the signal s_i with low transaction throughput. Finally, the formula (14) summarizes the total payoff of Player II considering all the cases. In the next section, we get the Nash equilibrium of the game numerically with different scenarios. We recall that each player aims to maximize its payoff.

IV. Numerical Results and Discussions

This section presents the numerical results to study the interactions between miners based on our proposed signaling game. To this end, we built a simulator on Python considering the behavior of players where two types of players are investigated. Wherein the honest player working to mine blocks into the main chain while under the impact of the incoming transaction throughput. The malicious player tries to reverse payment by mining blocks in its private chain and publish it whenever he can get benefits and win the game. We take transaction threshold $K_{th} = 10\,t/h$ that determines the type of the throughput as the average number of transactions per hour. The gain of both players ranges from 0.1 Bitcoin to 5 Bitcoins such as $w_h \leq w_m$ due to the attacker getting the payoff of mining blocks and double-spending attacks benefits. The risk of Player I to lose the game $c_I = 0.1$ if $K \leq K_{th}$ and $c_I = 0.9$ otherwise. Fig.2, presents the expected utility of Player I at the

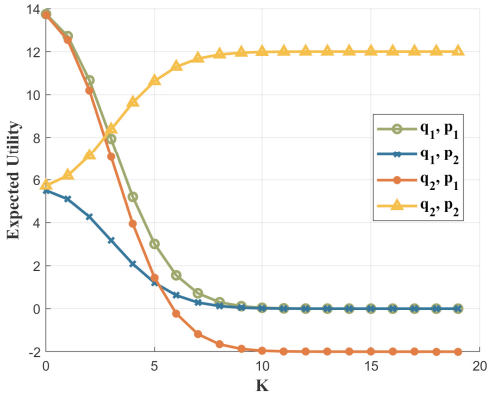

Fig. 2. Pure strategies of Player I versus the incoming transaction waiting to be included in a block.

equilibrium using its pure strategy against Player II's actions in the function of the transaction throughput K. The yellow line depicts the expected payoff of Player I playing the strategy q_2 corresponding to mining in the main chain against Player II publishing its private chain. This payoff increases when the throughput is below the threshold due to the increase of incoming transactions and the safe strategy taken by Player I. The green and the red lines present the best results for low transaction throughput, although the red line decreases more than the green when K increases. This is due to the dispersed effort of the honest miner while the attacker adds more blocks to its private chain. Fig.3 shows the results of the expected payoff of Player I for the mixed equilibrium strategy; such action is assigned for each transaction throughput type ($q_i q_j$). The payoff is calculated in function of the probability π_H regardless of Player II's actions. We can see from this figure that when Player I chooses to mine their block in the main

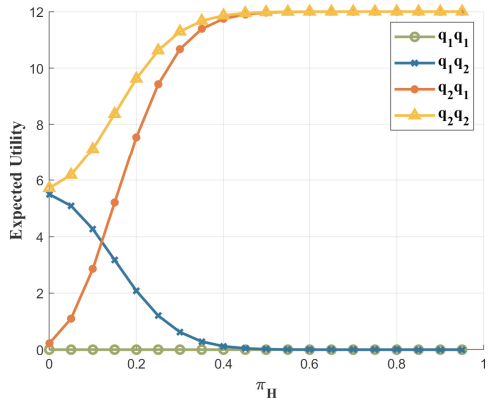

Fig. 3. Mixed equilibrium of Player I in function of the probability of high throughput of incoming transaction.

chain (Yellow line), his payoff increases with the increase of the probability π_h. This is due to the high probability that more transactions are waiting for validation which gives miners more chance to benefit from mining blocks regarding the maximum transaction allowed for each block. For high probability, Player I gets a similar payoff as the yellow line by playing the strategy q_2q_1 but with a low payoff for $\pi_H \leq 0.5$. This means that it will gain an advantage from the private chain by starting mining blocks to the main chain. The attacker will need more computation capability to surpass the main chain either for high transaction throughput. Otherwise, when starting mining blocks in the fork chain for low transaction throughput Player I will always lose the game against the attacker. In Fig.4, we plot the expected utility of Player II

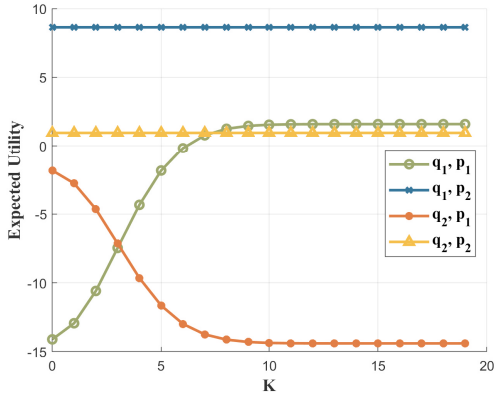

Fig. 4. Pure strategies of Player II versus the incoming transaction waiting to be included in a block.

in the function of the transaction throughput. We can easily see that the attacker can get a stable payoff when playing p_2 against q_2. While its payoff increases with K until reaching some benefits when mining in its private chain against Player I, who is mining in the fork chain. This gain is due to the risk of Player I losing since the attacker is gaining advantages against the main chain. Player II will lose when publishing his private chain as Player I is mining in the main chain. Player II wins the game when publishing his private chain as Player I mines in the fork chain. We present in Fig.5 the expected

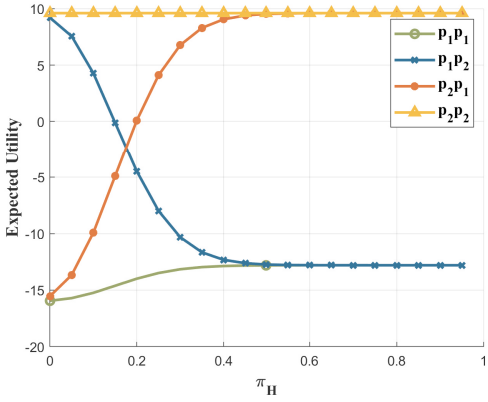

Fig. 5. Mixed equilibrium of Player II in function of the probability of high throughput of incoming transaction.

utility of Player II for mixed equilibrium in the function of the probability π_H. The best strategy for Player II is p_2p_2 when taking the risk to publish its private chain regardless of the type of the transaction throughput; this prevents the main chain from taking advantage of the attacker chain. While the other attacker starting by mining in his chain (p_1, blue line) for low transaction throughput followed by p_2 will lose its payoff while π_H increases. The inverse of this strategy allows the attacker to increase his payoff by the probability π_H. Fig.6,

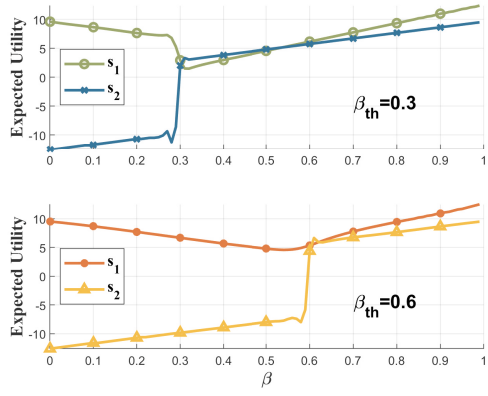

Fig. 6. Utility of Player II in function of its belief on received signal.

shows the expected utility of Player II as a function of its belief in the received signals for low transaction throughput such as s_1 and s_2, which correspond respectively to when Player I informs Player II that it played the strategies q_1 and q_2. Player II determines its belief on the received signal based on the threshold $_{th}$, which results in a change of behavior as shown

in the upper or lower sub-figure. The utility of both players

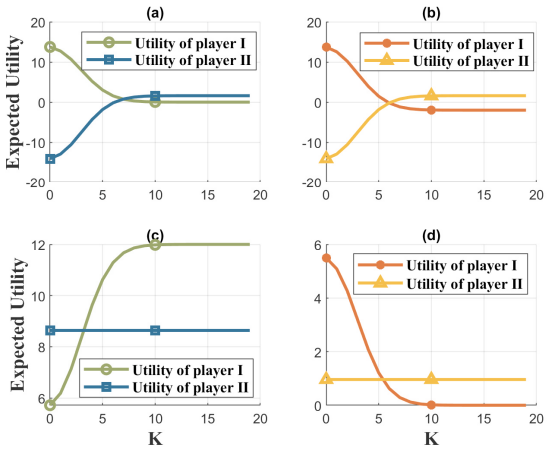

Fig. 7. Utility of players based on their behavior in function of the throughput.

following different scenarios is shown in Fig.7, depending on the nature of the signal sent by Player I (true or biased) and on the belief of Player II on the received signal (believe or not). Fig.7 (a) shows results of Player I playing q_1 and sends a true signal while Player II believes the signal received. We can see that the payoff of Player I decreases by telling the truth about its strategy while it increases for Player II due to its beliefs on the received signal. Fig.7 (b) shows results of Player I playing q_2 and sends a biased signal while Player II does not believe in the received signal. In this case, the payoff of Player I decreases to become negative in the function of K when cheating to Player II. While the outcomes of this later increase by the transaction throughput since it does not believe in the received signal. In Fig.7 (c), both players got positive utilities when Player I playing q_2 and sending a biased signal, and Player II believed in the received signal. In the last case shown in Fig.7 (d), the payoff of Player I decreases when he mines in a fork and sends a biased signal, and Player II believes in the received signal.

V. Conclusion

In this paper, we have investigated the impact of high transaction throughput on the security level of IoT transactions based on Bitcoin Blockchain. We proposed a signaling game approach to model the interaction between miners while considering their behaviors depending on the randomness of the incoming transactions. Thanks to the capability of the signaling game to handle non-complete information of the throughput type, we reached the best policy to prevent attackers from performing a double-spending attack. We performed an extensive simulation study to identify the equilibrium of our system depending on the behavior of players. Such as every player works on maximizing its payoff by choosing its best strategy regarding the opponent's strategies. Consequently, we obtained an equilibrium of our game through the simulation where the risk of a transaction being spent twice is low. As future work, we plan to extend our study to cover mining pool characteristics, enhance our model for more crypto-currency systems, and compare it with existing approaches in terms of security strength.

References

[1] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the internet of things: A tutorial," *IEEE Internet of Things Journal*, 2021.

[2] C. Gandhi, N. Shukla, G. Kaur, and K. Yadav, "Blockchain technology: Concept, applications, challenges, and security threats," in *Blockchain Applications in IoT Ecosystem*, pp. 77–104, Springer, 2021.

[3] H. Benaddi, K. Ibrahimi, H. Dahri, and A. Benslimane, "A framework to secure cluster-header decision in wireless sensor network using blockchain," in *International Conference on Advanced Communication Systems and Information Security*, pp. 205–218, Springer, 2019.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," tech. rep., Manubot, 2019.

[5] S. Haber and W. S. Stornetta, "Secure names for bit-strings," in *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pp. 28–35, 1997.

[6] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives," *Journal of Food Quality*, vol. 2021, 2021.

[7] H. Benaddi and K. Ibrahimi, "A review: Collaborative intrusion detection for iot integrating the blockchain technologies," in *2020 8th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 1–6, IEEE, 2020.

[8] Y. Liu, K. Qian, K. Wang, and L. He, "Effective scaling of blockchain beyond consensus innovations and moores law: Challenges and opportunities," *IEEE Systems Journal*, 2021.

[9] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Expert Systems with Applications*, vol. 168, p. 114384, 2021.

[10] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *International Conference on Financial Cryptography and Data Security*, pp. 507–527, Springer, 2015.

[11] G. Karame, E. Androulaki, and S. Capkun, "Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin.," *IACR Cryptol. ePrint Arch.*, vol. 2012, no. 248, pp. 1–17, 2012.

[12] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 906–917, 2012.

[13] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *International Conference on Financial Cryptography and Data Security*, pp. 528–547, Springer, 2015.

[14] E. Altman, D. Menasché, A. Reiffers-Masson, M. Datar, S. Dhamal, C. Touati, and R. El-Azouzi, "Blockchain competition between miners: a game theoretic perspective," *Frontiers in Blockchain*, vol. 2, p. 26, 2020.

[15] N. Alzahrani and N. Bulusu, "Towards true decentralization: A blockchain consensus protocol based on game theory and randomness," in *International Conference on Decision and Game Theory for Security*, pp. 465–485, Springer, 2018.

[16] R. Singh, A. D. Dwivedi, G. Srivastava, A. Wiszniewska-Matyszkiel, and X. Cheng, "A game theoretic analysis of resource mining in blockchain," *Cluster Computing*, vol. 23, no. 3, pp. 2035–2046, 2020.

[17] S. Motepalli and H.-A. Jacobsen, "Reward mechanism for blockchains using evolutionary game theory," *arXiv preprint arXiv:2104.05849*, 2021.

[18] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "A survey on applications of game theory in blockchain," *arXiv preprint arXiv:1902.10865*, 2019.

[19] M. Jouhari, K. Ibrahimi, H. Tembine, M. Benattou, and J. Ben Othman, "Signaling game approach to improve the mac protocol in the underwater wireless sensor networks," *International Journal of Communication Systems*, vol. 32, no. 13, p. e3971, 2019.

[20] C. Boudagdigue, A. Benslimane, and A. Kobbane, "Cluster-based certificate revocation in industrial iot networks using signaling game," in *GLOBECOM 2020 IEEE Global Communications Conference*, pp. 1–6, IEEE, 2020.