PoolCoin : Toward a distributed trust model for miners' reputation management in blockchain

Abdellah KACI
Laboratoire des Technologies Innovantes (LTI)
Ecole Nationale Supérieure de Technologie (ENST)
Algiers, Algeria
ab_kaci@esi.dz

Abderrezak RACHEDI
Gaspard Monge Computer Science Laboratory (LIGM UMR8049)
Université Paris-Est
Champs sur Marne, France
rachedi@u-pem.fr

***Abstract*—In blockchain, transactions between parties are regrouped into blocks, in order to be added to the blockchain's distributed ledger. Miners are nodes of the network that generate new blocks that meet the consensus protocol. Thus, when a miner adds a valid block to the distributed ledger, the miner is rewarded. Due to the difficulty of the problem to be solved by the miner in order to find a valid block, it becomes difficult to a single miner to gain rewards. Therefore, miners join mining pools, where the powers of miners are federated to ensure stable revenues for miners. In public blockchains, access to mining pools is not restricted, which makes mining pools vulnerable to considerable threats such as: block withholding (BWH) attacks and distributed denial of service (DDoS) attacks. In the present work, we a new blockchain named PoolCoin that manages reputation in mining pools. In addition, we provide a trust model for PoolCoin, inspired by the job market signaling model. The proposed PoolCoin blockchain allows pool managers to accept trusted miners in their mining pools, while miners are able to evaluate pool managers. The performance evaluation is conducted and the obtained simulation results are presented and discussed. In order to study the efficiency of the proposed trust model, a performance evaluation was provided. Thus, the model parameters' are optimized in order to detect and exclude misbehaving miners, while honest miners are maintained in the mining pool.**

***Index Terms*—Blockchain, distributed trust model, miner reputation, mining pool, signaling games**

I. Introduction

The blockchain was introduced for the first time by the creator(s) of Bitcoin in [1]. Due to the success of Bitcoin, many other blockchains have appeared. A blockchain uses a data structure called distributed ledger, that consists in an ordered list of transactions, regrouped into blocks. The same copy of the distributed ledger should be shared between all the nodes of the system. A blockchain uses a consensus protocol, in order to ensure that all nodes agree replicated updates on the distributed ledger [2].

Different consensus protocols are used in blockchains, such as Proof-Of-Work (PoW), Proof-Of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), etc. The Proof-Of-Work (PoW) is used by common blockchains, such as BitCoin and Ethereum [3]. In order to validate transactions, Proof Of Work (PoW) involves scanning for a value that when hashed, the hash begins with a number of zero bits. The average work required is exponential with the number of zero bits required. However, the verification requires executing only a single hash. [1]

Nodes that verify transactions and participate in the generation of new blocks are called miners. From a single miner's point of view, the interval between mining events exhibits high variance. By consequence, miners organize themselves into mining pools, in order to make the mining revenues more predictable. All members of a pool work together to mine blocks, and share their revenues when one of them successfully mines a block [4].

In the mining pool, miners submit to the pool manager partial proofs of work (also known as textitshares), having a difficulty level less than the difficulty level of the proof of work acceptable by the network. The pool manager, checks the submitted shares, in order to find among them a full proof of work valid according to the consensus protocol. This full proof will be used to claim the mining reward [4].

Mining pools use reward systems based on shares submitted by miners. For instance, in Proportional Payout Schema (PPS), a miner is rewarded proportionally to the number of its shares [5]. One of the commonly used reward mechanism is Pay-Per-Last-N-Shares (PPLNS), which distributes the reward among the miners that reported the N last shares [6].

Mining pools are competing between them to find valid blocks. Therefore, a mining pool may be confronted to a distributed denial-of-service (DDoS) attack from other mining pools [7]. Another attack on mining pools is the block withholding (BWH) attack, where malicious miners submit only partial proofs and withdraw those that represent a full proof of work [4]. The BWH attack uses the fact that miners are rewarded according to their submitted shares.

Haddadou et al. in [8] proposed a distributed trust model named DTM^2, based on the economical job market signaling model. DTM^2 allocates credits to nodes and securely manage them using Trusted Platform Modules (TPMs). DTM^2 applies costs on data reception and sending. In addition, nodes that send useful data, receive rewards.

In order to incite miners to behave honestly, Tang et al. proposed in [9] a reputation based mechanism for mining pools. In this work, the reputation of each miner is evaluated by a miner selected randomly, that will play the role of Pool Manager. However, the reputation system proposed in [9] is

978-1-7281-3893-0/20/$31.00 ©2020 IEEE

vulnerable, due to the fact that the Pool Manager is randomly selected. In fact, if a malicious miner is selected as the Pool Manager, the malicious miner will be able to drive attacks on the mining pool. In addition, in [9], pool managers are able to evaluate miners, while miners are not able to evaluate pool managers.

In this paper, we propose to introduce the distributed trust model, in the miner selection problem. Therefore, we propose the PoolCoin blockchain that manages miners' reputations. The reputation of a miner is stored in the blockchain as a *trust score*. According to the miners' trust scores, a pool manager selects miners that can join its mining pool. The main contributions of this research work are:

- The proposition of PoolCoin, a blockchain that manages reputation of miners and pool managers
- The proposition of a trust model inspired by the job market signaling model
- Optimization of model's parameters, in order to detect malicious miners and differentiate them from honest miners

II. Related works

Rewards provided to miners incite malicious nodes in the blockchain to attack miners. For instance, in Selfish Mining attack, a strong attacker increases its revenue at the expense of others nodes [10]. In fact, in the Selfish Mining strategy a group of miners keeps its discovered blocks private, to intentionally generate forks in the chain. Thus, the group develops a longer branch in the public chain, kept private. The selfish miners reveal their private blockchain, only when the length of public branch approaches the public branch's length [11].

Individual miners tend to join mining pools in order to secure stable benefits [12]. Thus, mining pools represents a valuable target for attackers. In addition to existing attacks on blockchains, mining pools are faced to special attacks such as the DDoS (distributed denial-of-service) attack and the block withholding (BWH) attack.

Johnson et al. [7] studied the motivation behind the DDoS (distributed denial-of-service) attack against Bitcoin mining pools. Their study shown that, there is a greater incentive to attack a larger mining pool than a smaller one. In addition, they observed that mining pools larger than a threshold are subject to economically motivated attacks, while pools smaller than the threshold are not.

In the block withholding (BWH) attack, malicious miners don't submit full proof of work used by the pool manager to add a valid block and claim its reward. Bag and Sakurai proposed in [4] a solution to the BWH (Block Withholding) attack, by introducing a special reward for the miner that shared the full proof of work.

Due to the importance of the miner, the selection of miners is crucial for the security of the blockchain. Yahiatene and Rachedi proposed in [13] a distributed algorithm named DM-CDS (Distributed Miners Connected Dominating Set), where the selection of miners is based on a trust metric and network parameters.

In a recent research work [9], Tang et al. proposed a reputation based mechanism that incites miners to behave honestly. For a blockchain composed of J miners and I mining Pool, a pool manager M_i is selected randomly. The latter will choose a reputation access threshold v_0, such that only miners with reputation value greater than v_0 can join the mining pool. The reputation evaluation of a miner j is based on the Pool Manager's satisfaction.

Nojoumian et al. in [14], proposed a trust model based on the miner's lifetime in order to avoid that a Re-Entry attack, where a miner previously excluded from a mining pool comes-back with a new identity. The proposed trust model relies on the seniority of miners and includes the lifetime of miners in the miners' reputation.

The Distributed Trust Model (DTM^2) proposed by Haddadou et al. [8], provides a reputation based trust model, that incite network's nodes to cooperate honestly. The trust proposed trust model of DTM^2 is inspired by the job market signaling model. To send a message, a node should pay a cost that will be covered by the reward, if the message is considered correct. Furthermore, to receive messages, receivers also pay a reception cost. By consequences, nodes are incited to send correct messages on the network.

III. The PoolCoin blockchain

In this section, we will present the proposed blockchain called PoolCoin, used to manage the miners' reputation. Thus, we will begin with a system overview of PoolCoin, followed by the trust model used by PoolCoin for miners' reputation.

A. System Overview

The proposed PoolCoin system is composed of Pool Managers, Miners, Mining Pools, and the PoolCoin's distributed ledger (Fig. 1). A *Pool Manager* receives transactions from the blockchain, then it distributes workload between miners, in order to find a valid block. When a valid block is found, the Pool Manager distributes the corresponding reward among miners that participated in the mining process. *The Miner* performs computations in order to find a valid block and send it back to the Pool Manager. The Miner sends shares (partial proofs of work) to the Pool Manager, in order to proof that it participated to the mining process. These shares will be used by the Pool Manager to determine the Miner's revenue. A *Mining Pool* is formed by the Pool Manager and Miners join it, in order to ensure stable revenues. A Pool Manager uses the reputation of miners to accept them in its Mining Pool. The *PoolCoin's distributed ledger* is stored in a distributed manner among nodes of PoolCoin: Miners and Pool Managers. This distributed ledgers stores information relative to miners' reputation. The Pool Managers affect workload to miners that have sufficient trust score.

B. PoolCoin's Transactions

In PoolCoin, a transaction is composed of six (06) fields:

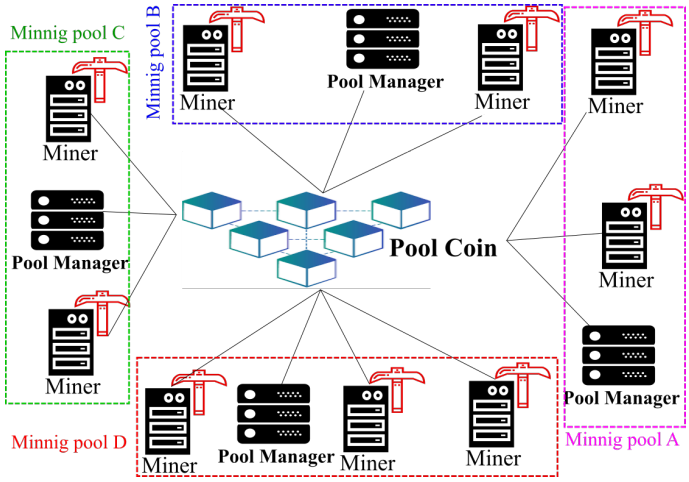

Fig. 1. System overview

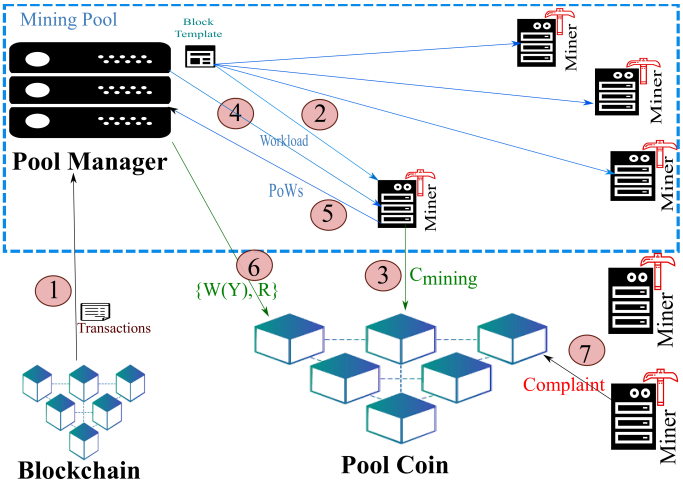

Fig. 2. Trust model of PoolCoin.

- **From**: represents the address of the sender.
- **To**: represents the address of the receiver.
- **Value**: The value of funds received by the miner indicated in the *To field* from the mining pool mentioned in the *From field*.
- **RepValue**: indicates the reputation value transferred from the sender to the receiver.
- **Complaint**: used to store complaints of miners against malicious pool manager
- **ExtraInfo** holds information such as: nonce, signatures, etc.

The *RepValue* field is used for the management of the miners' reputation. In addition, the *Complaint* field allows miners to report misbehaving pool managers. The *Complaint* field is composed of: *Level*, *FundLosses*, and *ReputationLosses*. *Level* measures the critically of the complaint. *FundLosses* and *ReputationLosses* represent the losses caused by a pool manager. The pool manager is specified in the "*TO*" field of the transaction. Likewise, the miner that complained is specified in the "*FROM*" field of the la transaction.

C. The Mining process in PoolCoin

In PoolCoin, the Pool Manager receives transactions from the Blockchain. Then, once it selects transactions to be included in the block, it broadcast the block's template to the miners usbscribed to its mining pool. To participate in the mining process, miners should pay a mining cost $C_{minining}$, using their trust score. Only miners that paid their mining cost are able to participate in the mining pool. By consequence, miners that their trust score is low, cannot participate to the mining pool.

The allowed miners will receive workload according to the paid mining cost. To proof that miners are honestly participating to the mining process, miners send Proof-Of-Works (PoWs) to the Pool Manager. We distinct two kinds of PoWs: Full PoWs and Partial PoWs. Full PoWs allows to the Pool Manager to claim the block reward, while the Partial PoWs, allows the Pool Manager to check that miners are honestly participating to the mining process. The number of partial PoWs should be proportional to the received workload. At each Round, the Pool managers provides to miners a reward W(Y) according to their participation in the mining process. The Pool manager provides a financial reward R according to its reward system. The financial reward R can be transferred to any blockchain using the pegged sidechains technology [15]. If the miner is not satisfied by the obtained rewards, PoolCoin allow it to store a Complaint in the blockchain, using the data field of the transactions. Thus, PoolCoins provides protection mechanisms against malicious Pool Managers. Fig. 2 shows the mining process using PoolCoin.

D. The trust model of PoolCoin

In this section, we will present the trust model used by PoolCoin to manage the reputation of miners. When a Miner wants to join a mining pool, he should be able to pay the mining cost C_{mining} from its trust score. According to his hash rate, the miner use a signal Y corresponding to its computing capacity (in terms of gigahash per second). The mining cost C_{mining} to be paid to the Pool Manager is proportional to the signal Y. However, the mining cost C_{mining} decreases when the miner's trust score θ increases. In fact, the mining cost C_{mining} that the Miner pays the Pool Manager is calculated as follows:

$$C_{mining} = \frac{Y}{\theta^{\frac{1}{Y+\alpha}}} \quad (1)$$

The Pool Manager affects workload to a miner according to the used signal Y. If the miner doesn't provide any share to the Pool Manager, the latter will not update its trust score θ. However, if the miner behaves honestly, the Pool Manager will reward it according to the number of shares and the used signal Y. More precisely, the number of partial shares (npPoWs) is divided by the signal Y to incite the miner to use its real capacity in the signal Y. In addition, to reward miners

those find and provide full shares. Thus, the pool manager will provide to the miner the reward W(Y) calculated as described in the formula below. The parameter β is used to incite to share the solution with the Pool Manager when found.

$$W(Y) = \frac{npPoWs^{\frac{1}{\delta}}}{Y} + \beta.nfPoWs \quad (2)$$

The trust score θ of a miner determines the reputation of the mining among different Mining Pool. This will allow a miner to transfer his trust score when it moves from one mining pool to another. When a miner joins the system, it obtains an initial score θ_{init}. The value of the initial score should as small as possible; in order to limit dishonest miners that uses several identities in mining.

E. Mining pools formation

To reward miners, Pool Managers should have sufficient reputation score. In fact, unlike [9] where Pool Managers are randomly selected among miners, Pool Coins requires that only miners with sufficient reputation are able to become Pool Managers. In fact, in PoolCoin Pool Managers should have sufficient funds to reward the miners. By consequence, miners before joining a mining pool, they should check that its Pool Manager has a reputation score sufficient to reward its miners.

The miners joins a mining pool based on the pool's rank, calculated based on the reputation of its pool manager and the complaints stored in the PoolCoin's transactions. To rank mining pools, for each transaction of PoolCoin containing complaints, the ranking algorithm (Algorithm 1) calculates the complaint score *cs*, based on the complaint's information. The algorithm updates the ranking of the Pool Manager based on θ_m(the trust level of the miner) and cs (the calculated complaint score).

IV. Performance evaluation

In this section we will study the performance of the proposed trust model. Thus, we considered several miners' behaviors and studied the performance of the proposed model. We also extracted optimal parameters of the model.

Algorithm 1: RankingPoolManagers

```
for each b in PoolCoin.getBlocks() do
    for each tx in b.getTransactions() do
        lv = tx.complaint.Level
        fl = tx.complaint.FundLosses
        rl = tx.complaint.ReputationLosses
        cs = complainteScore(lv, fl, rl)
        adrPM = tx.getTo()
        adrMiner = tx.getFrom()
        θ_m = getTrustScore(adrMiner)
        updateRanking(adrPM, θ_miner, cs)
    end for
end for
```

A. Experimental setup

We developed a program in Python that simulates the PoolCoin blockchain, in order to evaluate the trust model. Thus, we considered the trust model presented section III-D. To study the reactivity of our system, we considered exclusion time of miners, expressed in terms of number of mining pool required to exclude the miner from the mining process. Likewise to optimize the model's parameters (section IV-C), we considered the exclusion time of miners. In order to study the reliability of the proposed model (section IV-D), we considered the evolution of the miners' trust score.

To study reactivity of our system, we observed the exclusion time according to the variation of the initial trust score θ_{init}. The model's parameter α is equal to 0, the other parameters β and δ are assigned to 1. We considered different scenarios of Miners behaviors and for each scenario, we observed the evolution of miners' trust score during ten (10) mining rounds. We observed the score of each miner after each mining Round R_i, while R_0 corresponds to the initial state before mining.

The first scenario **Honest Miner** corresponds to a honest miner.

The second Scenario **BWH Malicious Miner** corresponds to a malicious miner that didn't share the solution of the puzzle (the proof of work accepted by the network). In other terms, it corresponds to a malicious miner that performs a BWH (Block Withholding) attack.

The third scenario **Absolute Malicious Miner** corresponds to a malicious miner that didn't contribute to solve the computational puzzle.

The other scenarios **Alternate n% Malicious Miners** alternate between honest and malicious behaviours, where n represents the percentage of the malicious behavior. We considered three such scenarios: **Alternate 80% Malicious Miners**, **Alternate 50% Malicious Miners**, and **Alternate 20% Malicious Miners**

B. Results analysis

In order to study the impact of the choice on the efficiency of the reputation system of PoolCoin, we varied the initial score in order to get optimized value for the initial score $\theta_{initial}$. The results shown in Fig. 3, shows the evolution of the exclusion time (in terms of number of rounds) according to the variation of the initial trust score.

As shown in Fig. 3, $\theta_{initial} < 1$, all miners are excluded in the first round. For other values of $\theta_{initial}$, Absolute Malicious Miners are rejected, while other miners are not detected. We observe that $\theta_{initial}$ values between 1 and 2, provide optimized exclusion time (2 mining rounds). In order to keep the initial trust score as small as possible, we choose 1 as optimal value of $\theta_{initial}$.However, the considered model parameters should be optimized in order to detect: Alternate Malicious Miners and BWH Malicious Miner.

C. Parameters optimization

In order to enhance the accuracy of our model, we will optimize the value of the model's parameters. By consequence,

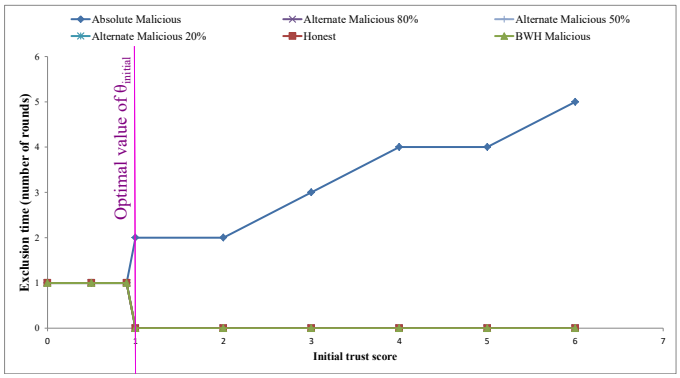

Fig. 3. Impact of initial trust score.

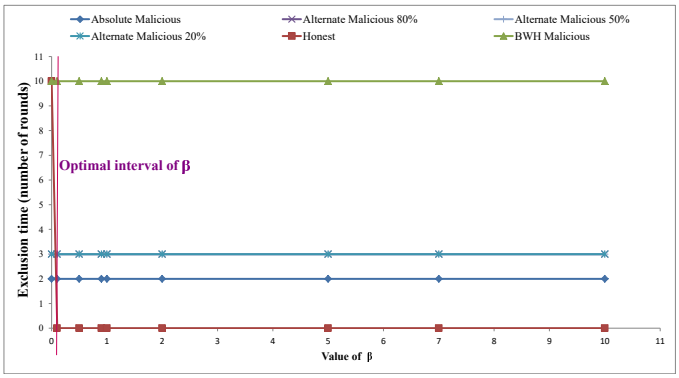

Fig. 5. Impact of parameter β on the execution time.

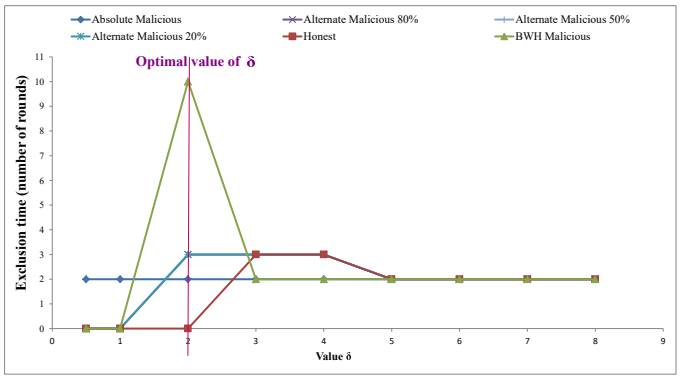

Fig. 4. Impact of parameter δ on the execution time.

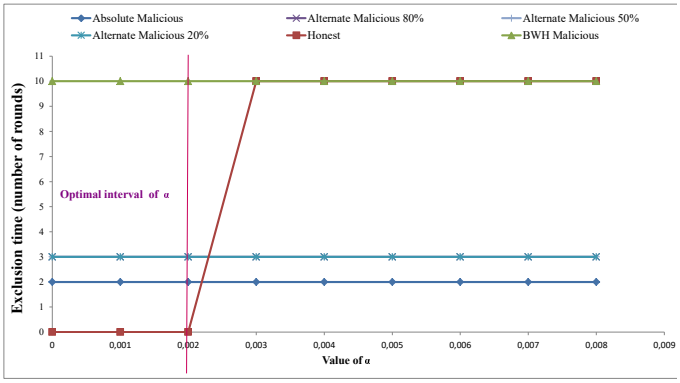

Fig. 6. Impact of parameter α on the execution time.

we will consider the optimal value of the initial trust (1), and extract optimal values of the model's parameters: α, β, and δ.

1) Optimized value of the parameter δ: To extract the optimized value of the parameter δ, we considered the optimized value of the initial score (1). In addition, the other model's parameters α and β are assigned to 0 and 1, respectively. The evolution of the miner's exclusion time according to the value of the parameter δ, is shown in Fig. 4. We note that for values greater than 2, the Honest Miner is excluded from the mining pool. In addition, other values of the parameter δ, don't detect some dishonest miners, namely: BWH Malicious Miner and Alternate 20% Miner. By consequence, we conclude that the optimal value of the parameter δ is 2.

2) Optimized value of the parameter β: Using the optimal values of $\theta_{initial} = 1$ and the parameter $\delta = 2$, we will extract the optimal value of the parameter β. Fig. 5 shows the behavior of the model according to the variation of the parameter β. We remark that, for values of the parameter β less than 0.1, the Honest Miner is excluded from the mining pool. However, for values of the parameter β greater than 0.1, the exclusion time is constant. Thus, we choose the value 0.1 as the optimal value for the parameter β.

3) Optimized value of the parameter α: In order to optimize α, we considered: $\theta_{initial} = 1$, $\delta = 2$, and $\beta = 0.1$. As shown in Fig. 6, the values of the parameter α greater than 0.02 exclude the Honest Miner. In addition, for values less than 0.02, the exclusion times of misbehaving miners are constants. By consequence, any value of the parameter α less than 0.02 is optimal. Thus, we consider the value 0.02 as the optimal value of the parameter α.

D. Reliability of the model

To study the reliability of our proposed model we studied the evolution of the trust score of the different scenarios through the mining rounds. We considered the optimal values of model parameters': $\alpha = 0.02$, $\beta = 0.1$, $\delta = 2$, and $\theta_{initial} = 1$. Fig. 7 shows the evolution of the miners' trust score during the ten mining rounds.

As shown by Fig. 7, the trust model of PoolCoin allows the Honest Miner to maintain a trust score allowing it to stay in the mining pool as long as it behaves honestly. When a miner alternate between honest and dishonest behaviors (Alternate Malicious n% Scenario), the trust score decreases in order to achieve a trust score that excludes the miner from the mining pool. The exclusion time is three mining rounds regardless of the percentage of the misbehaving. In addition, the trust model of PoolCoin is able to detect the BWH (Block With Holding) attacks at the 10^{th} mining round (R_{10}), when the trust score of the BWH Malicious Miner achieves the score of 2.76.

V. Security Analysis

The proposed trust model of PoolCoin detects five profiles of misbehaving miners: BWH Malicous, Absolute Malicous,

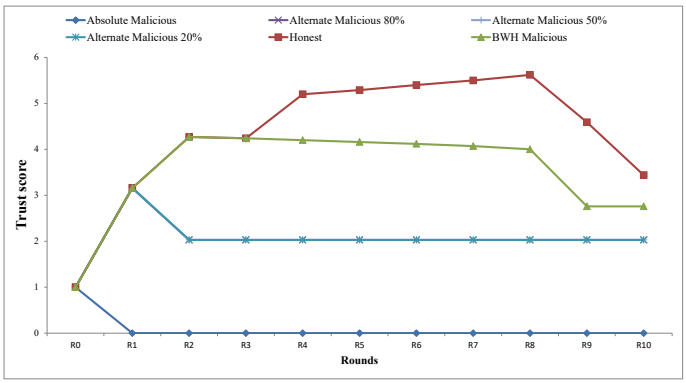

Fig. 7. The trust score evolution according to different rounds.

Alternate Malicious 80%, Alternate Malicious 50%, and Alternate Malicious 50%.

The proposed trust model of PoolCoin protects Pool Managers against malicious miners that try to perform a distributed denial of service (DDoS) attacks. In fact, if all the miners that coordinate their efforts in order to perform a DDoS attack, behave as Absolute Malicious Miner, the trust model of PoolCoin will detect them and exclude them from the mining pool. Likewise, if the miners alternate between honest and dishonest behaviours, they will be also detected and excluded from the mining pool. Furthermore, the detected miners will be denied from all the mining pools using PoolCoin.

The trust model of PoolCoin detect and exclude from the mining pools, miners that fellow the BWH Malicious Miner's behavior. By consequence, mining pools are protected against the well know BWH attack. Compared to the solution proposed in [4], the proposed solution doesn't require the affectation of a special financial reward to the miner that share the full PoW. In addition, as the contrary to the solution of [4], the trust model is able to detect the miner's that performed the BWH attack and exclude it from the mining pool.

The proposed trust model of PoolCoin is able to detect malicious miners, in order to exclude them from the mining pool. Furthermore, miners that perform malicious attacks are excluded from all the mining pools of the blockchain. By consequence, miners are dissuaded from attacking mining pools. However, the trust model of PoolCoin requires that miners uses Trust Platform Modules (TPMs), in order to avoid Re-entry attacks, where malicious miner use a new identity to be accepted in the system.

As described in section III-E, in PoolCoin only miners with high reputation are able to become Pool Managers. Thereby, unlike [9], a malicious miner is not able to become a Pool Manager. Furthermore, miners are able to report misbehaving Pool Managers, thanks to the complaint transactions stored in the distributed ledger of PoolCoin.

VI. Conclusion and Future Works

Mining pools are mainly faced to two kinds of attacks: block withholding (BWH) attacks and distributed denial of service (DDoS) attacks. In the present paper, we proposed PoolCoin a blockchain that deals with reputations of miners. The PoolCoin blockchain provides a trust model that protects mining pool against misbehaving miners. The trust model of PoolCoin is inspired by the job market signaling model. The parameters of the trust model were optimized in order to exclude only misbehaving miners. The optimized parameters of the trust model efficiently protect mining pools from attacks such as DDoS and BWH attacks. Furthermore, PoolCoin allows also to evaluate the Pool Managers' reputation, based on the complaints stored by miners in the blockchain. As future work, we aim to integrate PoolCoin and its turst model in BitCoin Blockchain.

In order to detect *Re-Entry* attacks, where malicious miner attack the mining pool using different identities, PoolCoin relies on Trusted Platform Modules (TPMs). As a future work, we will integrate the miner's lifetime in our trust model, in order to incite miners to use unique identity.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" 2008.
[2] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," IEEE Trans. Knowl. Data Eng., vol. 30, no. 7, pp. 1366–1385, Jul. 2018.
[3] X. Wang et al., "Survey on blockchain for Internet of Things," Comput. Commun., vol. 136, pp. 10–29, Feb. 2019.
[4] S. Bag and K. Sakurai, "Yet Another Note on Block Withholding Attack on Bitcoin Mining Pools," in Information Security, 2016, pp. 167–180.
[5] S. M. Werner, P. J. Pritz, A. Zamyatin, and W. J. Knottenbelt, "Uncle Traps: Harvesting Rewards in a Queue-based Ethereum Mining Pool," 070, 2019.
[6] R. Qin, Y. Yuan, and F.-Y. Wang, "A novel hybrid share reporting strategy for blockchain miners in PPLNS pools," Decis. Support Syst., vol. 118, pp. 91–101, Mar. 2019.
[7] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools," in Financial Cryptography and Data Security, 2014, pp. 72–86.
[8] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks," IEEE Trans. Veh. Technol., vol. 64, no. 8, pp. 3657–3674, Aug. 2015.
[9] C. Tang, L. Wu, G. Wen, and Z. Zheng, "Incentivizing Honest Mining in Blockchain Networks: A Reputation Approach," IEEE Trans. Circuits Syst. II Express Briefs, pp. 1–1, 2019.
[10] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal Selfish Mining Strategies in Bitcoin," in Financial Cryptography and Data Security, 2017, pp. 515–532.
[11] I. Eyal and E. G. Sirer, "Majority is Not Enough: Bitcoin Mining is Vulnerable," Commun ACM, vol. 61, no. 7, pp. 95–102, Jun. 2018.
[12] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary Game for Mining Pool Selection in Blockchain Networks," IEEE Wirel. Commun. Lett., vol. 7, no. 5, pp. 760–763, Oct. 2018.
[13] Y. Yahiatene and A. Rachedi, "Towards a Blockchain and Software-Defined Vehicular Networks Approaches to Secure Vehicular Social Network," in 2018 IEEE Conference on Standards for Communications and Networking (CSCN), 2018, pp. 1–7.
[14] NOJOUMIAN, Mehrdad, GOLCHUBIAN, Arash, NJILLA, Laurent, et al. Incentivizing blockchain miners to avoid dishonest mining strategies by a reputation-based paradigm. In : Science and Information Conference. Springer, Cham, 2018. p. 1118-1134.
[15] BACK, Adam, CORALLO, Matt, DASHJR, Luke, et al. Enabling blockchain innovations with pegged sidechains. URL: http://www.opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, 2014, p. 72.