Incentivizing Honest Mining in Blockchain Networks: A Reputation Approach

Changbing Tang, *Member, IEEE*, Luya Wu, Guanghui Wen, *Senior Member, IEEE*, and Zhonglong Zheng

***Abstract*—The core security of proof-of-work (PoW)-based blockchain networks, relies on PoW consensus algorithm and requires miners solving a crypto-puzzles of hash computation. However, the mining process in the blockchain is resource-intensive where only the first miner who completes full PoW will be rewarded. Therefore, miners exhibit malicious behaviors which cause a waste of distributed computation resource, even posing a threat on the efficiency of blockchain networks. In this brief, we propose a new reputation-based mechanism for the PoW computation in the blockchain, in which miners are incentivized to conduct honest mining. Based on the game theory, we design a reputation-based algorithm to encourage honest mining of miners, and thereby increase the overall revenue of the pool. In addition, numerical illustrations are also presented to support the performance of our proposed mechanism.**

***Index Terms*—Blockchain, proof-of-work, reputation-based mechanism, game theory.**

I. Introduction

BLOCKCHAIN was first proposed in the white paper of Bitcoin by Nakamoto [1], which is used to verify and store data with the blockchain data structure, to ensure the security of data transmission and access with the cryptography, and to program and manipulate data with the intelligent contracts [2], [3]. As an integrated application of distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm, blockchain has recently generated explosive interest from both academia and industry [4]–[7]. A survey of this topic can be referred to [8].

As one of the most successful applications of the blockchain technology, the security of bitcoin system relies on blockchain technology [9], in which the transactions are written into the open ledger in the form of blocks. To prevent alterations of previous transactions and maintain the integrity of the ledger, the participants (also called miners) contribute their computational power to generate PoW by solving a hash computation crypto-puzzles [10]. The miner solving the problem with the fastest speed will get right to account the block and acquire the bitcoin reward from the system [11]. After the solution is solved by some miner and propagated to the Bitcoin network, the block is generated. Later, a new round starts and all miners begin to solve a new cryptographic puzzle.

However, the mining process of the blockchain is very resource-intensive, which results in intense competitions and malicious behaviors among miners, such as interception attacks, selfish mining, eclipse attacks and stubborn mining [12]–[15]. Take the block withholding (BWH) attack as an example, where the infiltrating miners from other pools only submit partial proof of work (PPoW) to the attacked pool [16], [17]. At last, the revenue of the attacked pool is shared among more miners, which results in the fact that each miner earns less compared to solo mining or honest mining. Such attack makes the pool reward system unfair for malicious miners receiving unearned rewards, which threatens the efficiency of the bitcoin system greatly. Therefore, it is necessary to design an effective and fair mechanism to make miners accountable for any malicious behaviors, and thereby promote the efficient of blockchain networks.

To address the challenge, several literatures have been focused on the study of the malicious behaviors for pool mining. Goodrich [18] investigated a solution to prevent unfair supervisors and lazy miners from cheating, in which the technique can be applied for preventing misbehaving miners in the pool of blockchain networks. Moreover, Kroll *et al.* [19] provided a game theoretic analysis of bitcoin, and argued that the honest strategy constitutes an NE, implying incentive-compatibility. Eyal and Sirer [20] introduced selfish mining, in which the miners of a coalition keep their discovered blocks private and continue to verify more blocks privately until they get a sub-chain. Furthermore, Johnson *et al.* [21] explored the trade-off among DDoS attacks with a series of game-theoretical models of competition between two pools of varying sizes, and found that pools have a greater incentive to attack large pools than small ones.

On the other hand, reputation mechanism and some related distributed mechanisms can provide an incentive to prevent the malicious behaviors [22]–[26]. In addition, Sharples and Domingue [27] proposed a blockchain-based permanent distributed record of intellectual effort which instantiates and democratises educational reputation beyond the academic community. Zhao *et al.* [7] proposed a new blockchain-based

Manuscript received January 30, 2019; accepted February 21, 2019. Date of publication February 26, 2019; date of current version December 26, 2019. This work was supported in part by the National Natural Science Foundation under Grant 61751303, Grant 61672467, Grant 61877055, and Grant 61872323, in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LY16F030002, and in part by the Australian Research Council under Grant DE180101268. This brief was recommended by Associate Editor Y. Xia. *(Corresponding author: Guanghui Wen.)*

C. Tang is with the College of Physics and Electronics Information Engineering, Zhejiang Normal University, Jinhua 321004, China, and also with the School of Engineering, RMIT University, Melbourne, VIC 3001, Australia (e-mail: tangcb@zjnu.edu.cn).

L. Wu is with the College of Physics and Electronics Information Engineering, Zhejiang Normal University, Jinhua 321004, China.

G. Wen is with the School of Mathematics, Southeast University, Nanjing 211189, China, and also with the School of Engineering, RMIT University, Melbourne, VIC 3001, Australia (e-mail: wenguanghui@gmail.com).

Z. Zheng is with the College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua 321004, China (e-mail: zhonglong@zjnu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSII.2019.2901746

fair payment to study the cyber physical system (CPS), in which reputation system is applied such that a subscriber evaluate the published event and mark the publisher based on the reputation.

In this brief, we propose a new reputation-based mechanism to incentivize miners to conduct honest mining, thereby promote the efficient of bitcoin system. Specifically, we first describe the system model in term of PoW-based blockchain network, where miners present some malicious behaviors during the mining process. We then design a reputation mechanism based on the interval estimation and the fluctuation of reputation to incentive the honest mining for miners, in which the reputation depends on the historical evaluation. We find that the pool manager strictly selects high-quality miners based on the reputation mechanism we proposed, which contributes understanding for PoW consensus algorithm and provides a new method to explore the bitcoin system.

II. System Model and Reputation Mechanism

A. System Model

Consider a PoW-based blockchain network with J individual miners, which organize themselves into I mining pools in solving a crypto-puzzle competition to win the reward. According to the Nakamoto Consensus protocol [1], only the pool which accomplishes the PoW firstly will be rewarded. Therefore, we pay our attention to the payoff of miners in the target pool. Define the strategy set of miners as $\mathbb{S} = \{H, D\}$, where H stands for honest mining and D stands for dishonest mining. During the mining process, rational miners will take actions to maximize their own benefits. However, the resource of PoW computation is consumable, which gives rise to the fact that miners present some malicious behaviors during the competition mining process. These malicious behaviors may cause a waste of distributed computation resource, even posing a threat on the efficiency of blockchain networks.

To encourage miners presenting honest mining, we design a reputation approach to constrain the miners' malicious behaviors, in which the history of miners' behavior is evolved. Consider a randomly selected miner in the pool as a pool manager, who will evaluate the satisfaction of each miner involved in mining. Denote the pool manager as M_i, where $1 \leq i \leq I$ is the identity of the pool manager. Denote the general miner as m_j, where $1 \leq j \leq J$ is the identity of the miners. The evaluation of the satisfaction for the manager M_i towards the miner j is recorded as $P_i[j]$, where $-1 \leq P_i[j] \leq 1$. Here, $P_i[j] = 1$ means that the manager is very satisfied with the miner; while $P_i[j] = -1$ means the manager is very dissatisfied with the miner.

After the n-th transaction, the satisfaction of the miner is recorded as X_{jn} ($X_{jn} \in P_i[j]$). We record this history satisfaction of each miner as a reputation set $h_j = \{X_{j1}, X_{j2}, \ldots, X_{jn}\}$. Since the reputation level of a miner is constantly changing within a certain range, we use the probability interval to define the level of reputation. Before starting to mine, the manager sets the reputation access threshold of the open pool, which is denoted as v_0. If the reputation of miner is below the value of v_0, he is not eligible to join the pool. In addition, we use the reputation fluctuation to judge whether a miner is reliable or not based on the probability interval. Denote the fluctuation value of the reputation as σ_j. Similarly, the manager sets the reputation fluctuation threshold of the open pool as σ_0. If the miner's $\sigma_j < \sigma_0$, he will be kicked out of the mining pool.

B. Interval Estimation of Reputation

According to the data $h_j = \{X_{j1}, X_{j2}, \ldots, X_{jn}\}$, we give the calculation method of reputation interval. Denote the expectation and variance of the miners' reputation history as $\mu_j = E(X_j)$ and $\sigma_j = D(X_j)$, respectively. According to central-limit theorem for independent identically, the arithmetic mean of the random variable $\{X_{j1}, X_{j2}, \ldots, X_{jn}\}$ is expressed as $\bar{X}_j = (1/n)\sum_{i=1}^{n} X_{ji}$. When $n \to \infty$, i.e., the number of historical transactions of the miners is sufficiently large, the approximate distribution is expected to obey normal distribution with a variance of μ_j of σ_j^2/n. Through using the interval estimation theory, we get

$$\frac{\bar{X}_j - \mu_j}{\frac{\sigma_j}{\sqrt{n}}} \sim t(n-1), \tag{1}$$

where $\bar{X}_j = \frac{1}{n}\sum_{i=1}^{n} X_{ji}$, $\sigma_j = \frac{1}{n-1}\sum_{P_i[j]\in h_j}(P_i[j] - \bar{X}_j)^2$, and t represents the t-distribution with a degree of freedom $n-1$. By simply calculation, we can get the confidence level interval $(1-a)$ as

$$R_j[a] = (\bar{X}_j - \frac{\sigma_j}{\sqrt{n}} t_{\frac{a}{2}}(n-1), \bar{X}_j + \frac{\sigma_j}{\sqrt{n}} t_{\frac{a}{2}}(n-1)). \tag{2}$$

Here, $R_j[a]$ is the fluctuation range of the reputation we requested. The reputation of miner j is within the interval $(\bar{X}_j - (\sigma_j/\sqrt{n})t_{\frac{a}{2}}(n-1),\ \bar{X}_j + (\sigma_j/\sqrt{n})t_{\frac{a}{2}}(n-1))$ with a probability of $(1-a)$.

C. Measuring the Fluctuation of Reputation

The pool manager judges a miner's reputation fluctuations based on corresponding reputation interval. The higher the fluctuation value is, the more likely to be dishonest the miner is. Thus, the pool manager takes a miner's reputation fluctuation as a measurement to decide whether to allow the miner to join the pool.

Based on the miner's historical behavior record $h_j = \{X_{j1}, X_{j2}, \ldots, X_{jn}\}$, we make the following assumptions:

$$\begin{cases} H_0 : \sigma_j^2 \leq \sigma_0^2, \\ H_1 : \sigma_j^2 > \sigma_0^2. \end{cases} \tag{3}$$

Here, σ_0 is the threshold of the reputation, which is an adjustable parameter. If the actual value is greater than σ_0^2, the historical reputation value of miner j is excessively fluctuating. Thus, it is important to set a suitable threshold. If the threshold is set too high, a large number of miners will not be able to join the pool, which results in the fact that the overall revenue of the system decreases. If the threshold is set too low, it will allow too much attackers to take advantage of the honest mining and share the final reward. Furthermore, we propose a hypothesis test with a significant level of α. The calculated test statistic is

$$\frac{(n-1)\sigma_j^2}{\sigma_0^2} \sim \chi_\alpha^2(n-1). \tag{4}$$

And the rejection interval is

$$\sigma_j^2 \geq \frac{\sigma_0^2 \chi_\alpha^2(n-1)}{n-1}. \tag{5}$$

In terms of the above assumptions and the hypothesis test, we can judge whether a miner is reliable or not. That is, once σ_j^2 fall into the rejection interval, we refuse to believe that the historical reputation value of miner j is reliable.

III. Honest Mining With Reputation Mechanism

In this section, we consider the accumulated benefits of miners, in which miners adjust their strategies according to the reward they received. To restrict dishonest miners in the pool, we introduce a concept of life time L_j which represents a miner's mining age in the pool. Further, we define the miner's attack probability Q as follows:

$$Q = \begin{cases} 0, & \text{if } \bar{X}_j + \frac{\sigma_j}{\sqrt{n}} t_{\frac{\alpha}{2}}(n-1) \le v_0 \\ \frac{\mu_j - (|X_{jn} - \bar{X}_j| + v_0)}{\mu_j}, & \text{if } \bar{X}_j + \frac{\sigma_j}{\sqrt{n}} t_{\frac{\alpha}{2}}(n-1) > v_0. \end{cases} \tag{6}$$

Denote the payoff of miner j with the strategy $\mathbb{S}$ as $s_j(\mathbb{S})$, where $s_j(H) = Q$ and $s_j(D) = 0$. Accordingly, we get the long-term benefits $U_j(\mathbb{S})$ as follows:

$$U_j(\mathbb{S}) = (\bar{X}_j - \mu_j) + s_j(\mathbb{S}) + L_j/\sigma_j^2. \tag{7}$$

According to the Eq. (9), we design a reputation-based algorithm to incentive miners mining honestly. The detailed steps of Algorithm 1 are listed as follows.

S1) *Initialization:* Before pool i's n-th transaction, the system initialize every miner m_j's latest record $L_j, \bar{X}_j, R_j[a], \sigma_j$ automatically. At the same time, the pool manager M_i of the target pool i is selected randomly.

S2) *Standard Setting:* The pool manager M_i sets the reputation access threshold v_0 and the reputation fluctuation threshold σ_0.

S3) *Access Conditions:* Every miner m_j sends application to their target pool i. The pool manager decides whether to allow them to join the pool based on pre-set criteria v_0 and σ_0. If $\bar{X}_j + (\sigma_j/\sqrt{n}) t_{\frac{\alpha}{2}}(n-1) \le v_0$ and $\sigma_j^2 \le (\sigma_0^2 \chi_\alpha^2(n-1))/(n-1)$, then $L_j = L_j + 1$. This means miner enter the pool successfully. Otherwise $L_j = L_j - 1$, which means the miner is failed to enter the pool and the miner have to mine independently. Specially, if a miner's $L_j = 0$, then the identity of the miner will be automatically destroyed after leaving the pool, which means that his accumulated benefits are empty. Consequently, he has to apply a new account with initialized data. It is pointed out that the miner is eligible to enter the pool until the reputation value and reputation fluctuation value come up to the threshold together.

S4) *Strategy Updating:* Rational miners have two strategies to choose, which accounts for different payoffs. One is $U_j(H) = (\bar{X}_j - \mu_j) + [\mu_j - (|X_{jn} - \bar{X}_j| + v_0)]/\mu_j + L_j/\sigma_j^2$, the other is $U_j(D) = (\bar{X}_j - \mu_j) + 0 + L_j/\sigma_j^2$. The miners decide to choose the strategies according to their accumulated benefits.

S5) *Reputation Updating:* After this mining competition, the pool manager will evaluate the satisfaction $P_i[j]$ to each miner according to their contribution. And every miner's satisfaction record is updated as $h_j = \{X_{j1}, X_{j2}, \ldots, X_{jn}\}$. Then we can get reputation fluctuation $\sigma_j = (1/(n-1)) \sum_{P_i[j] \in h_j} (P_i[j] - \bar{X}_j)^2$. Finally, miner m_j's newest reputation interval is updated as $R_j[a] = (\bar{X}_j - (\sigma_j/\sqrt{n}) t_{\frac{\alpha}{2}}(n-1),\ \bar{X}_j + (\sigma_j/\sqrt{n}) t_{\frac{\alpha}{2}}(n-1))$.

Algorithm 1: Reputation-Based Mechanism for Mining Pool in the n-th Transaction

```
Initialization: considered a blockchain network with $I$ mining pools and $J$ miners. Then, choose pool $i$ as our target pool. (a)Initialize every miner $m_j$'s latest record $L_j, \bar{X}_j, R_j[a], \sigma_j$; (b) The pool manager $M_i$ of the target pool $i$ is randomly selected;
For convenience: we pay our attention to pool $i$'s $n$-th transaction. Denote the number of honest miners as $N$.
while $N < J$ do
    The pool manager $M_i$ sets the reputation access standard $v_0$ and the reputation fluctuation standard $\sigma_0$;
    Every miner $m_j$ sends application to target pool $i$;
    if $\bar{X}_j + \frac{\sigma_j}{\sqrt{n}} t_{\frac{\alpha}{2}}(n-1) \le v_0$ and $\sigma_j^2 \le \frac{\sigma_0^2 \chi_\alpha^2(n-1)}{n-1}$ then
        $L_j = L_j + 1$;
        else
            $L_j = L_j - 1$;
        end
    end
    if $L_j = 0$ then
        kick $m_j$ out of the mining pool. Initialize miner $m_j$'s record $L_j, \bar{X}_j, R_j[a], \sigma_j$;
        else
            $U_j(H) = (\bar{X}_j - \mu_j) + Q + \frac{L_j}{\sigma_j^2}$;
            $U_j(D) = (\bar{X}_j - \mu_j) + 0 + \frac{L_j}{\sigma_j^2}$;
            if $U_j(H) > U_j(D)$ then
                $\mathbb{S} = H$;
                else if $U_j(H) < U_j(D)$ then
                    $\mathbb{S} = D$;
                end
                else if $U_j(H) = U_j(D)$ then
                    $\mathbb{S} = H$ or $D$;
                end
            end
            for $j = 1; j \le J; J++$ do
                $X_{jn} = P_i[j]$;
                $h_j = \{X_{j1}, X_{j2}, \cdots, X_{jn}\}$;
                $\sigma_j = \frac{1}{n-1} \sum_{P_i[j] \in h_j} (P_i[j] - \bar{X}_j)^2$;
                $R_j[a] = (\bar{X}_j - \frac{\sigma_j}{\sqrt{n}} t_{\frac{\alpha}{2}}(n-1),$
                $\bar{X}_j + \frac{\sigma_j}{\sqrt{n}} t_{\frac{\alpha}{2}}(n-1))$;
            end
        end
    end
end
```

IV. Numerical Simulations

In the experimental environment, we set $J = 100$ and the confidence level of each round as 0.95. Each mining pool selects the miner with the highest reputation as the pool manager. The satisfaction rating of pool manager towards each miner is calculated according to the contribution of the miners. Repeat the operation 30 times without adding reputation rule to form an initial database. After a period of time, the incentive functions of our reputation mechanism are activated.

The fluctuations for the credibility of miners with different number of mining rounds are shown in Fig. 1. Compared

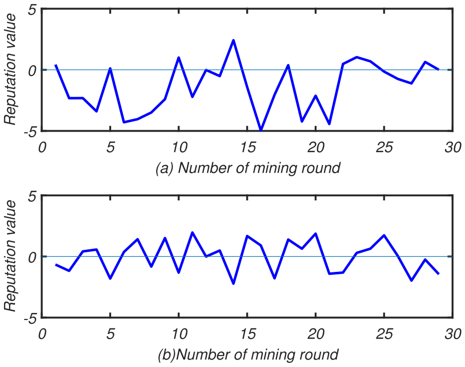

Fig. 1. The reputation fluctuations for miners with different number of mining rounds.

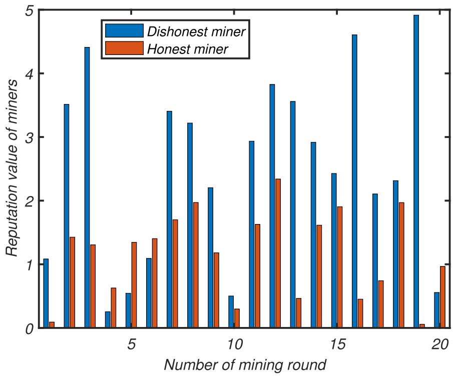

Fig. 2. The variation of reputation interval for honest miners and dishonest miners.

with Fig. 1(a), we see that the level of reputation fluctuations in Fig. 1(b) is relatively stable, which reflects that miners contribute relatively stable computing power. This provides a clue for the manager to evaluate the reputation of miners, which shows that only miners with a stable reputation and high credibility (exceeds the threshold) are eligible to participate in the mining pool. As the satisfaction evaluations of miner for each mining changing, their reputation intervals also change accordingly. In Fig. 2, we plot the variation of honest miners and dishonest miners in the width of the reputation interval. We find that the reputation interval of miners with more fluctuations is greater than that of miners with less fluctuations. Therefore, the width of the reputation interval can also be used as an indicator for the manager to judge the reputation of miners.

Set the threshold of the miners' reputation fluctuations be $v_0 = \{0.2, 0.25, 0.3, 0.35\}$ and $\sigma_0 = \{0.1, 0.2, 0.3, 0.4\}$. It is shown in Fig. 3 that the number of miners who choose the honest mining strategy in different pools presents an increasing trend. When the entry threshold v_0 is too low, it is impossible to judge the probability of miner taking the attack strategy in early stage, which means that the detection function of reputation mechanism does not work well. As the entry threshold v_0 is increased, it is better to distinguish the dishonest miners. With the decision of miners during each round of mining, the rational mining union tends to choose honest mining. The similar result is found with parameter σ_0, which is shown in Fig. 4. When the threshold σ_0 is small, the abnormality of node detecting with the fluctuation is too sensitive, which leads to misjudgment of the normal behavior of some honest miners. When the threshold σ_0 is too large, it is not easy to detect some miners with abnormal behavior. Thus, it is important to choose appropriate reputation access threshold v_0 and fluctuation threshold σ_0.

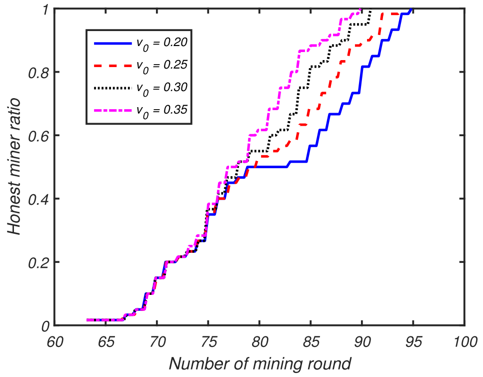

Fig. 3. The honest miner ratio with different entry thresholds v_0.

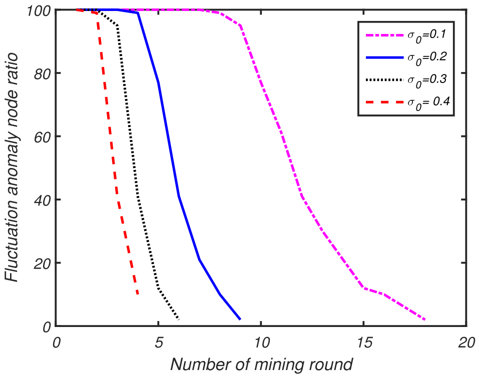

Fig. 4. The fluctuation anomaly of honest miners detection with different thresholds σ_0.

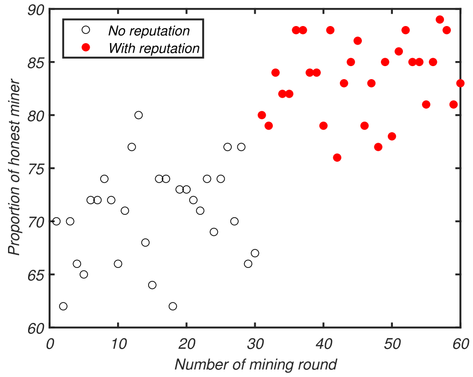

Fig. 5. The proportion of honest miner with no-reputation and reputation mechanism.

To describe the performance of the reputation mechanism, we plot the proportion of honest miner with no-reputation and reputation in Fig. 5. It is shown that the proportion of honest miners with reputation mechanism has a notable improvement compared the situation with no-reputation. Furthermore, we explore the accumulated benefits for miners. It is show in Fig. 6 that when miners tend to mine more honestly, the accumulated benefits becomes higher. For the pool manager, setting

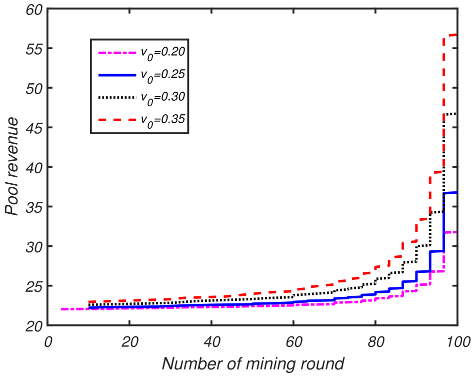

Fig. 6. The overall revenue of all pools with different entry thresholds v_0.

the threshold of the access reputation in the pool is beneficial to protect his mining pool from any malicious attacks, thus maximizing the income of the mine pool. Under our reputation-based mechanism, as the number of miners who have been mining honestly increased, the overall income of pools begins to show an upward trend (See Fig. 6). It is also shown that the rationality of the reputation admission parameters set by the pool manager affects the overall revenue of mining pools. The more reasonable the reputation access criterion is, the higher the revenue receives.

V. Conclusion

The reputation interval designed in this brief is a preventive mechanism, which can discriminate potential attackers at the source and prevent attackers from joining the mining pool. The reputation fluctuation is a detection mechanism to determine whether the miners in the mining pool have dishonest aggressive behavior. By applying the reputation-based mechanism we designed, miners tend to mine honestly for higher accumulated benefits and ultimately achieve a consensus on stable state. In this brief, we propose a reputation-based mechanism that encourages rational miners to mine honestly. Through two evaluation of reputation with interval estimation and fluctuation measuring, the judgment of the identity of dishonest miners is basically realized. According to the reputation-based mechanism we proposed, the pool manager strictly selects high-quality miners, which is very beneficial to the development of the bitcoin system.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Washington, DC, USA, Bitcoin, White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] T. McConaghy *et al.* (2016). *BigchainDB: A Scalable Blockchain Database*. [Online]. Available: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

[3] Y. Yuan and F. Wang, "Blockchain: The state of the art and future trends," *Acta Automatica Sinica Chin.*, vol. 42, no. 4, pp. 481–494, 2016.

[4] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[5] Y. Zhang, R. Deng, J. Shu, K. Yang, and D. Zheng, "TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain," *IEEE Access*, vol. 6, pp. 31077–31087, 2018.

[6] A. Lei *et al.*, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[7] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, 2018.

[8] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data*, Honolulu, HI, USA, Jun. 2017, pp. 557–564.

[9] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[10] C.-B. Tang, Z. Yang, Z.-L. Zheng, Z.-Y. Chen, and X. Li, "Analysis and optimization of game dilemma in PoW consensus algorithm," *Acta Automatica Sinica Chin.*, vol. 43, no. 9, pp. 1520–1531, 2017.

[11] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," *ACM SIGMETRICS*, vol. 42, no. 3, pp. 34–37, 2014.

[12] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (FAW) attacks on bitcoin," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, Dallas, TX, USA, Oct./Nov. 2017, pp. 195–209.

[13] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *Proc. IEEE Eur. Symp. Security Privacy*, Saarbrucken, Germany, Mar. 2016, pp. 305–320.

[14] Y. Xia and D. Hill, "Attack vulnerability of complex communication networks," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 55, no. 1, pp. 65–69, Jan. 2008.

[15] I. Eyal, "The Miner's dilemma," in *Proc. IEEE Symp. Security Privacy*, San Jose, CA, USA, May 2015, pp. 89–103.

[16] S. Bag, S. Ruj, and K. Sakurai, "Bitcoin block withholding attack: Analysis and mitigation," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1967–1978, Aug. 2017.

[17] D. K. Tosh *et al.*, "Security implications of blockchain cloud with analysis of block withholding attack," in *Proc. 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput.*, Madrid, Spain, May 2017, pp. 458–467.

[18] M. T. Goodrich, "Pipelined algorithms to detect cheating in long-term grid computations," *Theor. Comput. Sci.*, vol. 408, nos. 2–3, pp. 199–207, 2008.

[19] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining or, bitcoin in the presence of adversaries," in *Proc. 12th Workshop Econ. Inf. Security (WEIS)*, Washington, DC, USA, Jun. 2013, pp. 1–21. [Online]. Available: https://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf

[20] I. Eyal and E. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, 2018.

[21] 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 FC* (LNCS 8438), R. Böhme, M. Brenner, T. Moore, and M. Smith, Eds. Heidelberg, Germany: Springer, Oct. 2014, pp. 72–86.

[22] Z. Wang, L. Wang, Z.-Y. Yin, and C.-Y. Xia, "Inferring reputation promotes the evolution of cooperation in spatial social dilemma games," *PLoS ONE*, vol. 7, no. 7, 2012, Art. no. e40218.

[23] Y. Xia and D. J. Hill, "A dynamic Braess's paradox in complex communication networks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 60, no. 3, pp. 172–176, Mar. 2013.

[24] H.-X. Hu, W. Yu, G. Wen, Q. Xuan, and J. Cao, "Reverse group consensus of multi-agent systems in the cooperation-competition network," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 11, pp. 2036–2047, Nov. 2016.

[25] G. Geetha and C. Jayakumar, "Implementation of trust and reputation management for free-roaming mobile agent security," *IEEE Syst. J.*, vol. 9, no. 2, pp. 556–566, Jun. 2015.

[26] H. Shen, Y. Lin, K. Sapra, and Z. Li, "Enhancing collusion resilience in reputation systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 8, pp. 2274–2287, Aug. 2016.

[27] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *Adaptive and Adaptable Learning EC-TEL* (LNCS 9891), K. Verbert, M. Sharples, and T. Klobučar, Eds. Cham, Switzerland: Springer, Sep. 2016, pp. 490–496.