Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks

Kang, Jiawen; Xiong, Zehui; Niyato, Dusit; Wang, Ping; Ye, Dongdong; Kim, Dong In

2018

Kang, J., Xiong, Z., Niyato, D., Wang, P., Ye, D. & Kim, D. I. (2018). Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks. IEEE Wireless Communications Letters, 8(1), 157-160. https://dx.doi.org/10.1109/LWC.2018.2864758

https://hdl.handle.net/10356/140139

https://doi.org/10.1109/LWC.2018.2864758

Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks

Jiawen Kang, Zehui Xiong, Dusit Niyato, *Fellow, IEEE*, Ping Wang, *Senior Member, IEEE*, Dongdong Ye, Dong In Kim, *Senior Member, IEEE*

***Abstract*—In proof-of-stake based consortium blockchain networks, pre-selected miners compete to solve a crypto-puzzle with a successfully mining probability proportional to the amount of their stakes. When the puzzle is solved, the miners are encouraged to take part in mined block propagation for verification to win a transaction fee from the blockchain user. The mined block should be propagated over wired or wireless networks, and be verified as quickly as possible to decrease consensus propagation delay. In this work, we study incentivizing the consensus propagation considering the tradeoff between the network delay of block propagation process and offered transaction fee from the blockchain user. A Stackelberg game is then formulated to jointly maximize utility of the blockchain user and individual profit of the miners. The blockchain user acting as the leader sets the transaction fee for block verification. The miners acting as the followers decide on the number of recruited verifiers over wired or wireless networks. We apply the backward induction to analyze the existence and uniqueness of the Stackelberg equilibrium. Performance evaluation validates the feasibility and efficiency of the proposed game model in consensus propagation.**

***Index Terms*—Consensus propagation, proof-of-stake, consortium blockchain, game theory, network delay**

I. Introduction

Recently, blockchain has been emerging as a promising paradigm that enables trustless nodes/users to securely interact with each other without relying on a trusted third party. Blockchain provides immutable ledgers and decentralized platforms for various practical scenarios [1]. Based on diverse characteristics, blockchain networks can be categorized into three main types: public, private and consortium blockchain networks. A public blockchain network has better information transparency and auditability due to no access limitation. However, block mining and blocks synchronization among all nodes incur high cost and long delay, and thus makes public blockchain networks unsuitable for energy-limited and time-sensitive scenarios. Private blockchain networks are only accessed by a specific, limited organization and cannot be widely adopted in diverse trading activities [1].

Compared with the above blockchain networks, recently, consortium blockchain networks have attracted enormous attention due to the advantages of modest cost, good scalability and short delay [2]. The widely adopted consortium blockchains denote the certain blockchains that apply the proof-based consensus algorithms (e.g., proof-of-stake) among a set of pre-selected miners to maintain the distributed ledger, in which the efficient consensus management is achieved [1], [3]. In particular, Proof-of-Stake (PoS) is a popular consensus algorithm requiring only mild cost and computing power on mining competition. The probability of winning a mining competition is determined by a miner's stake, since the difficulty level of the crypto-puzzle for each miner is adjusted according to the amount of their stakes [3].

There are two major steps in consensus management for PoS-based consortium blockchain networks: (i) mining step and (ii) mined block propagation for verification step. The pre-selected miners in PoS-based consortium blockchain networks record new transactions from the blockchian user into a block, and compete to solve a crypto-puzzle with a probability proportional to the amount of their stakes in the mining step. In the blockchain networks, the fastest miner finding a valid nonce that meets the difficulty of the crypto-puzzle propagates its mined block to other miners for verification over a wired or wireless channel. If this mined block is finally added into the blockchain, the miner will receive a mining reward for its effort in the consensus management [3], [4].

However, due to the limited number of pre-selected miners in consortium blockchain, the miners are encouraged to propagate the mined block to more verifiers [2]. Recruiting more verifiers can avoid centralized block verification and decrease impacts of compromised verifiers leading to more reliable and secure blockchain network [1], [5]. Additionally, some light-weight nodes, e.g., nearby mobile devices with blockchain clients [6], reachable quickly through wireless networks, can also be the verifiers in consortium blockchain. These verifiers can form different verifier sets to finish verification. Each miner needs to recruit its own verifiers to verify the mined blocks. The block verification tasks are divided into sub-tasks and assigned to pre-selected miners over the network according to their individual number of recruited verifiers for verification [7], [8]. When the mined block is verified to be valid, the miners share the transaction fee according to their verification contributions.

For the blockchain user, if its offered transaction fee is high

This work was supported in part by WASP/NTU M4082187 (4080), Singapore MOE Tier 1 under Grant 2017-T1-002-007 RG122/17, MOE Tier 2 under Grant MOE2014-T2-2-015 ARC4/15, NRF2015-NRF-ISF001-2277, EMA Energy Resilience under Grant NRF2017EWT-EP003-041, and the National Research Foundation of Korea (NRF) Grant funded by the Korean Government under Grant 2017R1A2B2003953.

Jiawen Kang, Zehui Xiong and Dusit Niyato are with School of Computer Science and Engineering, Nanyang Technological University, Singapore. (e-mails: kavinkang@ntu.edu.sg, zxiong002@e.ntu.edu.sg, dniyato@ntu.edu.sg). Dongdong Ye is with School of Automation, Guangdong University of Technology, China. (emails: dongdongye8@163.com). Ping Wang is with Department of Electrical Engineering and Computer Science, York University, Canada. (email:pingw@yorku.ca). Dong In Kim is with the Department of Electrical and Computer Engineering, Sungkyunkwan University, South Korea. (email: dikim@skku.ac.kr). Corresponding author: Dong In Kim.

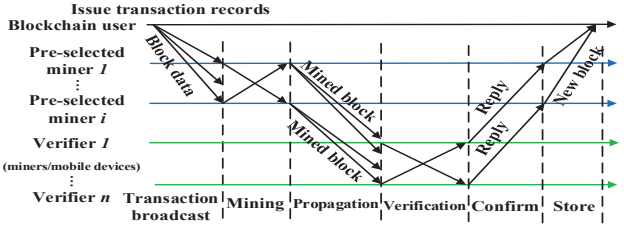


Fig. 1: A system model of consensus management.

enough, the transaction records in mined blocks can be verified by more verifiers [6], [7]. However, the more verifiers lead to a costly and time-consuming consensus process due to the larger block transmission cost and block verification processing and network delay [5]. The blockchain user should strategically set transaction fee to incentivize the miners and save the cost.

In this letter, we study the consensus propagation problem and balance the tradeoff between the delay of propagation process and the offered transaction fee from the blockchain user in PoS-based consortium blockchain networks. We first model the interaction among the blockchain user and miners as a Stackelberg game, in order to jointly maximize the utility of the blockchain user and the individual profit of miners. We obtain the Stackelberg equilibrium and prove its existence and uniqueness. Lastly, we present the numerical results to show the efficiency of the game model.

II. System Model and Problem Formulation

A. System Model

As illustrated in Fig. 1, there are three entities in the PoS-based consortium blockchain network under our consideration: 1) blockchain users, 2) miners, and 3) verifiers. In this paper, both miners in the blockchain network and mobile devices with blockchain clients can be the verifiers [6]. A blockchain user generates transaction records and periodically broadcasts the transaction records to pre-selected miners in the network. The miners put the issued transaction into a data block, and use their own computing power to solve a crypto-puzzle according to given parameters of the blockchain [3].[1] Compared with traditional proof-of-work, the difficulty level of crypto-puzzle of PoS for each miner depends on the amount of their own stakes. The more stake leads to a lower difficulty level [3]. Once a miner successfully solves the puzzle, the miners propagate the puzzle result and the block data to their verifier sets for verification. Each miner has its cooperative verifier set consisted of a certain number of nearby verifiers [9]. The fastest miner to finish the propagation can earn the mining reward R in the consortium blockchain.

Similar to [8], [10], each pre-selected miner in the consortium blockchain is assigned a particular verification task according to their own recruited verifiers. Thus, every miner can share the given transaction fee, denoted as x, from the blockchain user based on their verification contributions, i.e., the number of recruited verifiers. Moreover, there exists the communication cost between the miner and verifiers due to the block verification overhead.

[1]If there are multiple blockchain users submitting transactions at the same time, the mining task for these transactions will be arranged in a queue according to transaction fee, in which the conflict will not happen.

B. Problem Formulation

We consider a consortium blockchain network with a group of pre-selected miners (denoted by $\mathbb{J} = \{1, \ldots, y\}$) and large verifier sets cooperating with different miners (denoted by $\mathbb{V} = \{\mathbb{V}_1, \ldots, \mathbb{V}_i\}, i \in \mathbb{J}$). Each miner decides on the ratio of recruited verifiers in its cooperative verifier set for verification. Let $\mathbb{R} = \{r_1, \ldots, r_i\}$ denote the strategy profiles consisting of all miners' strategies. The strategy represents the ratio of recruited verifiers in cooperative verifier sets. So the number of recruited verifiers for each miner $i \in \mathbb{J}$ is $r_i |\mathbb{V}_i|$, wherein $|\mathbb{V}_i|$ is cardinality of set $\mathbb{V}_i$. The probability of winning a mining competition for miner i depends on the mining contribution, which is expressed by $P_{\mathrm{m}} = \varrho e^{-\lambda z T}$ [4], where ϱ is the proportional value between individual stake and total stakes in the consortium blockchain. We use a random variable following a Poisson process with the mean value of $\lambda = 1/600$ to model the occurrence of solving the crypto-puzzle [4]. $z > 0$ is a given delay factor, and T is the number of transactions in the mined block. The profit function of miner i consists of 1) expected revenue obtained from mining and mined block verification, 2) incurred communication cost due to overhead of verification, and 3) a pre-defined electricity and other costs of mining c_i, which is formulated as follows:

$$U_m^i = l_1 R P_{\mathrm{m}} + l_2 x \frac{r_i |\mathbb{V}_i|}{\sum_{j \in \mathbb{J}} r_j |\mathbb{V}_j|} - \alpha_i r_i |\mathbb{V}_i| - c_i. \quad (1)$$

l_1 and l_2 represent the weight factors of expected revenue obtained from mining and verification, respectively, and $l_1 + l_2 = 1$. R denotes the fixed token reward issued by the blockchain system and RP_{m} is the obtained token reward according to the mining contribution of miner i in the consortium blockchain. $x \frac{r_i |\mathbb{V}_i|}{\sum_{j \in \mathbb{J}} r_j |\mathbb{V}_j|}$ represents the obtained transaction fee of miner i according to its verification contribution, i.e., the number of recruited verifiers, $r_i |\mathbb{V}_i|$, for mined block verification. Note that communication between the miner and its recruited verifiers can be through a wired or wireless connection, which incurs a certain communication cost (e.g., bandwidth resource) during mined block propagation [11]. Thus, we use $\alpha_i (r_i |\mathbb{V}_i|)$ to represent the communication cost, where $\alpha_i > 0$ is a given average communication cost coefficient.

The utility of the blockchain user includes expected satisfaction and incentive cost, i.e., the transaction fee, as follows:

$$U_s = f[r_1, r_2, \ldots, r_i; \tau_1(r_1), \tau_2(r_2), \ldots, \tau_i(r_i)] - x, \quad (2)$$

where $\tau_i(r_i)$ is the mined block propagation time for miner $i \in \mathbb{J}$. $f[r_1, r_2, \ldots, r_i; \tau_1(r_1), \tau_2(r_2), \ldots, \tau_i(r_i)]$ is the satisfaction function with respect to the ratio of recruited verifiers in verifier set. Similar to that in [12], we consider a general and realistic assumption that $f[r_1, r_2, \ldots, r_i; \tau_1(r_1), \tau_2(r_2), \ldots, \tau_i(r_i)]$ is a strictly concave function in variables $r_1, r_2, \ldots, r_i$. Moreover, $f[0, 0, \ldots, 0; \tau_1(0), \tau_2(0), \ldots, \tau_i(0)] = 0$. This satisfaction function is also monotonically increasing in each $r_i, i \in \mathbb{J}$.

The miners may have different block propagation time owing to the different number of recruited verifiers for verification. In the mined block propagation step, the time needed for a block to reach a consensus is determined by both the transmission delay, τ_p^i, and the block verification time, τ_v^i,

among the recruited verifiers. For a mined block of size b, the average time for reaching a consensus, i.e., the block propagation time, is denoted as: $\tau_i(r_i) = \tau_p^i + \tau_v^i = \frac{br_i|\mathbb{V}_i|}{\delta k_1} + k_2 r_i |\mathbb{V}_i| b$ [7]. $k_1 > 0$ and $k_2 > 0$ are coefficients given by the system. δ is the average effective channel link capacity of communication connection between miners and verifiers. Similar to that in [7], $r_i |\mathbb{V}_i| / k_1$ represents the network scale parameter and $k_2 r_i |\mathbb{V}_i|$ represents the parameter determined by both the network scale and the average verification speed of the verifiers. The utility of the blockchain user is affected by both the satisfaction level in terms of block propagation delay and the offered transaction fee. The more verifiers lead to a more secure blockchain network [5]. However, this also results in the larger block propagation time since the miners may need to communication with some verifiers that are not close through multi-hop relays. Thus, in the following, we define a security-delay metric s_i to balance the network scale (i.e., the number of recruited verifiers) and the block propagation time for miner i, which is expressed by

$$s_i = \frac{m_1 (r_i |\mathbb{V}_i|)^q}{m_2 \frac{\tau_i}{T_{\max}}} = \frac{m_1 k_1 \delta T_{\max}}{b m_2 (1 + k_1 k_2 \delta)} \times (r_i |\mathbb{V}_i|)^{q-1}, \quad (3)$$

where $m_1 > 0$ and $m_2 > 0$ are coefficients given by the system. $T_{\max}$ denotes the maximum value of tolerant block propagation time of the blockchain user. $q \geq 2$ is a given factor indicating the network scale. In what follows, we consider $q = 2$ for ease of presentation [5]. We rewrite Eqn. (2) as follows:

$$U_s = f(s_1, s_2, \ldots, s_i) - x. \quad (4)$$

The interaction between the blockchain user and miners can be formulated as a Stackelberg game, where the blockchain user is the leader and the miners are the followers [13]. In Stage I, the blockchain user determines transaction fee to pay to miners, and the miners respond with the best ratio of recruited verifiers in Stage II according to the transaction fee. Note that a rational miner will not take part in the mining process with a negative profit. Therefore, the transaction fee offered by the blockchain user is assumed to be bigger than a minimum value denoted as $x_{\min}$. Specifically, the objective functions for the leader and followers are expressed as follows:

$$\begin{aligned} &\text{Leader}: \max_{\mathrm{x}} \mathrm{U_s(x)}, \\ &\text{s.t. } \mathrm{x} > \mathrm{x_{min}}. \\ &\text{Followers}: \max_{\mathrm{r_i}} \mathrm{U_m^i(r_i)}, \\ &\text{s.t. } 1 \geq \mathrm{r_i} \geq 0. \end{aligned} \quad (5)$$

III. Game Equilibrium Analysis

We employ the backward induction method to analyze the Stackelberg equilibrium of the proposed game [2].[2] Given the transaction fee x decided by the blockchain user, the miners compete to maximize their individual utilities by choosing their ratios of recruited verifiers in verifier sets, which forms a noncooperative Miners' Verification Game (MVG) $\mathbb{G}^m = \{\mathbb{J}, \mathbb{R}, \{U_m^i\}_{i\in\mathbb{J}}\}$, where $\mathbb{J}$ is the set of miners, $\mathbb{R}$ is the strategy set of miners, and U_m^i is the profit function of miner i.

Definition 1: *A set of strategy profiles* $\mathbb{R}^{\mathrm{ne}} = \{r_1^{\mathrm{ne}}, \ldots, r_i^{\mathrm{ne}}\}$ *is the Nash equilibrium of the MVG* $\mathbb{G}^m = \{\mathbb{J}, \mathbb{R}, \{U_m^i\}_{i\in\mathbb{J}}\}$, *if, for* $\forall i \in \mathbb{J}$, $U_m^i(r_i^{\mathrm{ne}}, \mathbb{R}_{-j}^{\mathrm{ne}}, x) \geq U_m^i(r_i, \mathbb{R}_{-j}^{\mathrm{ne}}, x)$ *for* $r_i \geq 0$, *where* $\mathbb{R}_{-j}^{\mathrm{ne}}$ *represents the Nash equilibrium set excluding* r_j.

Theorem 1: A Nash Equilibrium exists in MVG $\mathbb{G}^m = \{\mathbb{J}, \mathbb{R}, \{U_m^i\}_{i\in\mathbb{J}}\}$ [4].

Proof: By differentiating U_m^i defined in Eqn. (1) with respect to r_i, we have $\frac{\partial U_m^i}{\partial r_i} = \frac{|\mathbb{V}_i| l_2 x \sum_{j\in\mathbb{J}_{-i}} r_j |\mathbb{V}_j|}{(r_i|\mathbb{V}_i| + \sum_{j\in\mathbb{J}_{-i}} r_j |\mathbb{V}_j|)^2} - \alpha_i |\mathbb{V}_i|$, and $\frac{\partial^2 U_m^i}{\partial {r_i}^2} < 0$. Where $\mathbb{J}_{-j}$ represents a group of miners excluding j. Noted that U_m^i is a strictly concave function with respect to r_i. Therefore, given any $x > 0$ and any strategy profile $\mathbb{R}_{-j}^{\mathrm{ne}}$ of the other miners, the best response strategy of miner i is unique when $r_i \geq 0$. Accordingly, the Nash equilibrium exists in the noncooperative MVG $\mathbb{G}^m$. ■

Furthermore, we obtain the optimal strategy denoted as r_i^* by solving $\frac{\partial U_m^i}{\partial r_i} = 0$, then we have $r_i^* = \sqrt{\frac{l_2 x \sum_{j\in\mathbb{J}_{-i}} r_j |\mathbb{V}_j|}{\alpha_i |\mathbb{V}_i|^2}} - \frac{\sum_{j\in\mathbb{J}_{-i}} r_j |\mathbb{V}_j|}{|\mathbb{V}_i|}, x > \frac{\alpha_i}{l_2} \sum_{j\in\mathbb{J}_{-i}} r_j |\mathbb{V}_j|$.

When $x \leq \frac{\alpha_i}{l_2} \sum_{j\in\mathbb{J}_{-i}} r_j |\mathbb{V}_j|$, we set $r_i^* = 0$, since miner i does not participate in block verification to avoid a deficit in this case [12]. Thus, the minimum value of transaction fee for the blockchain user is $x_{\min} = \max(\frac{\alpha_i}{l_2} \sum_{j\in\mathbb{J}_{-i}} r_j |\mathbb{V}_j|)$, where $\max(\cdot)$ is the maximum element in the set of $\{\frac{\alpha_i}{l_2} \sum_{j\in\mathbb{J}_{-i}} r_j |\mathbb{V}_j|\}$. By summing up $\frac{\partial U_m^i}{\partial r_i} = 0$, we can obtain $\sum_{i\in\mathbb{J}} r_i |\mathbb{V}_i| = \frac{l_2 x(|\mathbb{J}|-1))}{\sum_{i\in\mathbb{J}} \alpha_i}$, and thus

$$r_i = \frac{l_2(|\mathbb{J}|-1)}{|\mathbb{V}_i| \sum_{i\in\mathbb{J}} \alpha_i} (1 - \frac{(|\mathbb{J}|-1)\alpha_i}{\sum_{i\in\mathbb{J}} \alpha_i}) x, \quad (6)$$

where $|\mathbb{J}|$ is cardinality of set $\mathbb{J}$.

According to the above analysis, the blockchain user knows that the miners can achieve a unique Nash equilibrium for any $x > x_{\min}$ [12]. Therefore, the blockchain user can maximize its utility given in Eqn. (4) by choosing the optimal transaction fee x^*, which is characterized by Theorem 2. In particular, by substituting Eqn. (6) into Eqn. (3), we have

$$\begin{aligned} U_s = f[&\tfrac{k_1\delta m_1 T_{\max}}{m_2 b(1+k_1k_2\delta)} \tfrac{l_2(|\mathbb{J}|-1)}{\sum_{i\in\mathbb{J}}\alpha_i}(1 - \tfrac{(|\mathbb{J}|-1)\alpha_1}{\sum_{i\in\mathbb{J}}\alpha_i})x, \\ &\ldots, \tfrac{k_1\delta m_1 T_{\max}}{b m_2(1+k_1k_2\delta)} \tfrac{l_2(|\mathbb{J}|-1)}{\sum_{i\in\mathbb{J}}\alpha_i}(1 - \tfrac{(|\mathbb{J}|-1)\alpha_i}{\sum_{i\in\mathbb{J}}\alpha_i})x] - x. \end{aligned} \quad (7)$$

Theorem 2: There exists a unique Stackelberg Equilibrium (x^*, r_i^{ne}) in the noncooperative Stackelberg game, i.e., Eqn. (5), where x^* is the unique maximizer of the blockchain user's utility in Eqn. (7) when $x > x_{\min}$, and r_i^{ne} is given by Eqn. (6) with x^*.

Proof: Note that $f[r_1, r_2, \ldots, r_i; \tau_1(r_1), \tau_2(r_2), \ldots, \tau_i(r_i)]$ is a strictly concave function in variables $r_1, r_2, \ldots, r_i$, $f(s_1, s_2, \ldots, s_i)$ is also a strictly concave function. Hence, the utility U_s in Eqn. (7) is a strictly concave function of x for $x \in (x_{\min}, \infty)$. The value of U_s given in Eqn. (7) is $-\max(\frac{\alpha_i}{l_2} \sum_{j\in\mathbb{J}_{-i}} r_j |\mathbb{V}_j|) < 0$ when $x = x_{\min}$, and ap-

[2]We can utilize a Bayesian game to analyze the game behavior among miners with incomplete information. According to the Bayesian game theory, an incomplete game can be divided into different complete games corresponding to various miner type combinations, which are subjected to the joint probability distribution. Each miner maximizes its expected profit function by scheduling ratio of recruited verifiers with the consideration of other miners' recruited strategies. An iterative algorithm can be designed to obtain the equilibrium according to Ref. [4], when the miners do not know others' strategies. Due to the limited space, we only discuss the complete information case and provide the closed-form expression of Nash equilibrium in this paper.

TABLE I: Parameter Setting in the Simulation

Parameter	Setting
Fixed reward R	1000 [4]
Electricity cost of mining c_i	0.1
A mined block of size b	100 KB [5]
Tolerant block propagation time (T_{max})	500 seconds
Pre-defined parameter θ	100000
Average channel link capacity δ	100 bps
l_1, l_2, m_1, m_2, k_1, k_2	0.5, 0.5, 0.5, 0.5, 0.5, 0.5

proaches $-\infty$ when x goes to ∞. There exists a unique maximum value of U_s when $x = x^*$ in Eqn. (7), which can be calculated through bisection method [12]. Therefore, the unique Stackelberg Equilibrium $(x^*, r_i^{\rm ne})$ in the noncooperative Stackelberg game can be achieved. ■

IV. Performance Evaluation

For utility function of the blockchain user, we set that $U_s = \theta \log(1+\sum_{i\in\mathbb{J}} s_i) - x = \theta \log[1+\frac{k_1\delta m_1 T_{\max}}{m_2 b(1+k_1k_2\delta)} \frac{l_2(|\mathbb{J}|-1)}{\sum_{i\in\mathbb{J}}\alpha_i} x] - x$ [12]. It is easy to show that $\frac{\partial^2 U_s}{\partial x^2} < 0$, so it is a concave function that satisfies the assumptions in Section II and analytical result in Section III. We evaluate performance of the proposed game with varied number of verifiers and different variation ranges of communication cost. We consider a blockchain network with verifiers in the range of [100, 800] [4]. The communication cost between miners and verifiers varies from 300 to 335 [5], and follows a uniform distribution. More parameter settings are shown in Table I mostly adopted from [4], [7].

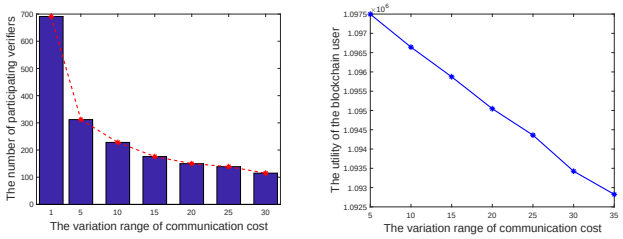
As shown in Fig. 2(a), we compare the total number of participating verifiers, i.e., $|\mathbb{J}|$. The total number of participating verifiers is decreasing when the communication cost has bigger variation range. Here, the variation range is the difference between the maximum and minimum of communication cost for miners. Fig. 2(b) shows that bigger variation range of communication cost brings lower utility of the blockchain user when there are 800 verifiers in the blockchain network.

We randomly choose miner i with a mining probability $P_{\rm m} = 1/800$ and the maximum of random communication cost in the range of [300, 310], i.e., $\alpha_i = 309.8632$, and thus evaluate its profit with respect to the total number of participating verifiers in Fig. 3(a). The profit of miner i decreases when the total number of participating verifiers increases due to more intensive competitions among the verifiers. Moreover, the profit of miner i in our proposed game is significantly higher than that in the baseline scheme that each miner has the same number of recruited verifiers. The reason is that all miners can maximize their profits through calculating individual optimal number of recruited verifiers.

Fig. 3(b) shows the computation time of our proposed game. The running time is linear-like increasing when the number of verifiers increases. The optimal strategies of participating verifiers for miners can be efficiently calculated according to Eqn. (6). In summary, according to the results, our proposed Stackelberg game is effective and efficient for consensus propagation in blockchain networks.

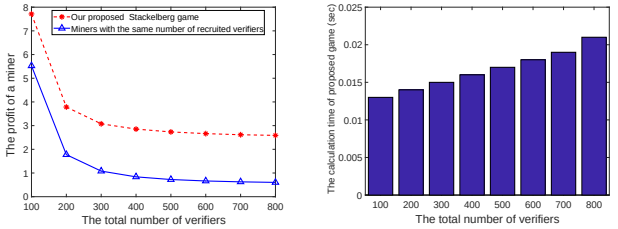
V. Conclusion

In this letter, we have focused on the consensus propagation problem in PoS based consortium blockchain networks. We



(a) (b)

Fig. 2: Impact of variation of communication cost on (a) $|\mathbb{J}|$ and (b) the utility of the blockchain user.



(a) (b)

Fig. 3: Impact of the total number of participating verifiers on (a) the profit of a miner and (b) calculation time.

have addressed this problem considering the tradeoff between delay of block propagation process and offered transaction fee from a blockchain user. A Stackelberg game has been developed to jointly maximize the profit of the miners and the utility of the blockchain user. Thereafter, the existence and uniqueness of the Stackelberg equilibrium have been validated. Performance evaluation demonstrates that the proposed game is feasible and efficient for consensus propagation. In future work, we will investigate the wireless communication cost affected by channel quality and fading, and network congestion.

References

[1] W. Wang, *et al*, "A survey on consensus mechanisms and mining management in blockchain networks," *arXiv preprint arXiv:1805.02707*, 2018.

[2] Z. Li, *et al*, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Trans. on Ind. Inform.*, 2017.

[3] W. Li, *et al*, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pp. 297–315, Springer, 2017.

[4] Z. Xiong, *et al*, "Edge computing resource management and pricing for mobile blockchain," *arXiv preprint arXiv:1710.01567*, 2017.

[5] C. Decker, *et al*, "Information propagation in the bitcoin network," in *IEEE Conf. on P2P*, pp. 1–10, IEEE, 2013.

[6] A. Tomescu, *et al*, "Catena: Efficient non-equivocation via bitcoin," in *IEEE Symposium on S&P*, pp. 393–409, 2017.

[7] X. Liu, *et al*, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communications Letters*, 2018.

[8] A. Miller, *et al*, "Discovering bitcoins public topology and influential nodes," *http://cs.umd.edu/projects/coinscope/coinscope.pdf*, May 2015.

[9] S. Micali, "Algorand: The efficient and democratic ledger," *arXiv preprint arXiv:1607.01341*, 2016.

[10] C.-W. Hsueh and C.-T. Chin, "Epow: Solving blockchain problems economically," *http://rswiki.csie.org/dokuwiki/_media/wikilist:courses:ieee-atc-r-13.pdf*, 2017.

[11] L. Li, *et al*, "Sustainable cnn for robotic: An offloading game in the 3d vision computation," *IEEE Trans. on Sustainable Computing*, 2018.

[12] D. Yang, *et al*, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," *IEEE/ACM Trans. on Netw.*, vol. 24, no. 3, pp. 1732–1744, 2016.

[13] Z. Zhou, *et al*, "Game-theoretic approach to energy-efficient resource allocation in device-to-device underlay communications," *IET Communications*, vol. 9, no. 3, pp. 375–385, 2015.