# IMPACTS OF CONSENSUS ALGORITHMS IN CRYPTOCURRENCY

## *THEORETICAL ANALYSIS OF POW VERSUS POS IN ETHEREUM*

*Dapeng Pan, Harbin Institute of Technology, China*
*J. Leon Zhao*, City University of Hong Kong, China*
*Shaokun Fan, Oregon State University, USA*

***Abstract***

**The plan of switching from PoW to PoS system in the blockchain has been around for a while. However, the impact of this changeover is not clearly defined although discussions on the pros and cons of PoW and PoS consensus algorithms have been ongoing in the cryptocurrency community. In this paper, we examine the bookkeeper behavior and the fairness issues of switching from PoW to PoS from a theoretical perspective. By modeling the utility of PoW versus PoS bookkeepers in the two cryptocurrency systems, respectively, we find that the distribution of bookkeepers tends to polarize in both cases as some real-world data have indicated. Our static comparison shows that in the PoS system, the bookkeepers polarize further and the top bookkeepers turn to grab even more power. That is, the efficiency advantage of PoS must be paid by giving in on market fairness.**

## INTRODUCTION

Most cryptocurrencies, including Bitcoin, use "proof of work" (PoW) as the consensus mechanism. However, the PoW consensus protocol has been challenged for its efficiency because the computation process requires an immense amount of energy [1]. To address this challenge, alternative consensus protocols that can achieve similar security goals are proposed to improve efficiency of cryptocurrency systems. Ethereum, as one of the most famous cryptocurrency systems, is considering transferring to the proof of stake (PoS) consensus mechanism. The PoS protocol that is designed for Ethereum is named as "Casper" [2], [3]. Since the idea about Casper was first put forward in 2015, the implementation date has been delayed for several times. Recently, Ethereum launched the Constantinople and St. Petersburg updates as preparations for the Casper upgrade. However, there are still much doubt about the efficiency, fairness, and incentive issues of switching from PoW to PoS. For example, Vitalik Buterin, the founder of the Ethereum project, expressed four concerns [4]: (1) Lower than expected participation rates in transaction validation; (2) Stake pooling becomes too popular; (3) Sharding turns out more technically complicated than expected; and (4) Operating nodes turns out more expensive than expected.

Researchers have also discussed differences between PoW and PoS on issues related to scalability, security [5], stability, incentive compatibility [6] and so on. So far, it is still not clear what could happen when a cryptocurrency's consensus mechanism switches from PoW to PoS. In this paper, we try to provide insights to this problem based on theoretical analysis of groups of bookkeepers in the system. The consensus mechanism allows participators of blockchain to run for bookkeeper in order to earn rewards. A bookkeeper needs to validate transactions, create new blocks, and verify the validity of newly created blocks [7]. A bookkeeper sometimes is also called miner or validator [8]. By modeling the bookkeepers' utilities in different systems, we first analyze the bookkeepers' behavior characteristics in PoW and PoS systems respectively. Then we make a comparative static analysis to study the impacts of protocol switch on the bookkeepers.

### Bookkeepers in a PoW system

We assume that, in a PoW-based blockchain network, $N$ bookkeepers participate in the consensus process. Let $x_i$ denote the hash rate provided by bookkeeper $i$. It measures the speed at which bookkeeper $i$'s computing power can compute the hash function in a cryptocurrency system. Hash rate is usually calculated at hashes per second. Then the bookkeeper $i$'s relative hash rate [9] can be defined as:

$$h_i = \frac{x_i}{\sum_{j\in N} x_j} = \frac{x_i}{x_i + x_{-i}}. \qquad (1)$$

Wherein, $x_{-i} = \sum_{j\in N, j\neq i} x_j$ represents all hash rate provided by the bookkeepers other than $i$. Therefore, $\sum_{i\in N} h_i = 1$. The reward for bookkeeper $i$ consists of fixed reward $r_f$, i.e. the mining reward and the variable reward $r_v t_i$, i.e., the transaction fee, which is the average

fee per transaction $r_v$, times $t_i$, the total number of trades processed by bookkeeper $i$. Bookkeeper $i$'s expected utility is therefore,

$$u_i = (r_f + r_v t_i)P_i - c_i x_i. \quad (2)$$

Where, $P_i$ and $c_i$ denote the probability of success and the mining cost involved, respectively. A complete successful process of validation includes a mining step and a propagation step. The success probability of the mining step is directly determined by its relative computing power $h_i$. This is because only the first node who obtain the right hash value by solving the proof-of-work puzzle could be the bookkeeper of this block. Thus, the more computing power a node has, the more likely the node will become the bookkeeper. In the propagation step, the bookkeeper needs to propagate the mined block, which has a possibility of being discarded by other bookkeepers. This is called orphaning, which is usually caused by long network latency [10]. We use the Poisson distribution with the mean value $\lambda$ to model the process of solving the proof-of-work puzzle [9], [11]. Denote $P_o$ as the probability of orphaning, and then we can get

$$p_0 = 1 - e^{-\lambda\sigma} \text{ and } P_i = h_i(1 - P_o) = h_i e^{-\lambda\sigma}, \quad (3)$$

where $\sigma$ denotes the propagation time. $\sigma$ is positively related with block size which represents the number of transactions in a block but we make a simplification to assume that it is static [9], [11]. Then, Equation 2 is translated into

$$u_i = (r_f + r_v t_i)\frac{x_i}{x_i + x_{-i}} e^{-\lambda\sigma} - c_i x_i. \quad (4)$$

The objective function for bookkeeper $i$ is

$$\begin{aligned} &\text{Max } u_i, \\ &s.t. 0 \le x_i \le \infty. \end{aligned} \quad (5)$$

By taking its first order derivative with respect to $x_i$, we can obtain

$$\frac{\partial u_i}{\partial x_i} = (r_f + r_v t_i)\frac{x_i + x_{-i} - x_i}{(x_i + x_{-i})^2} e^{-\lambda\sigma} - c_i.$$

According to the first order derivative condition, we have $\frac{\partial u_i}{\partial x_i} = 0$. Solve the equation, and we obtain bookkeeper $i$'s optimal strategy in terms of hash rate to provide as

$$x_i^* = \sqrt{(r_f + r_v t_i)e^{-\lambda\sigma}\frac{x_{-i}}{c_i}} - x_{-i}. \quad (6)$$

Substitute $x_i^*$ into equation (4) and we have

$$\begin{aligned} u_i^* &= c_i x_{-i} - 2\sqrt{(r_f + r_v t_i)c_i e^{-\lambda\sigma} x_{-i}} + (r_f + r_v t_i)e^{-\lambda\sigma} \\ &= \left(\sqrt{c_i x_{-i}} - \sqrt{(r_f + r_v t_i)e^{-\lambda\sigma}}\right)^2. \end{aligned} \quad (7)$$

It is obvious that this quadratic equation of $\sqrt{x_{-i}}$ intersects with the $\sqrt{x_{-i}}$ - axis at $\sqrt{\frac{(r_f + r_v t_i)e^{-\lambda\sigma}}{c_i}}$ and $u_i^*$ -axis at $(r_f + r_v t_i)e^{-\lambda\sigma}$. Then we can qualitatively draw the graph of Equation 7 in MATLAB. Figure 1 shows that $u_i^*$ has the maximal value when $x_{-i}$ approaches 0 or $\infty$ (and $h_i$ approaches 1 or 0). This demonstrates that for the bookkeepers whose relative computing power is in the middle range between 1 and 0, they would choose to reduce it to near 0 or raise it close to 1 in order to maximize profit. Bookkeepers who own sufficient financial resources and hold optimistic view about future development of the blockchain certainly would choose to raise their relative computing power to maximize profits by upgrading or purchasing more mining machines. They generally hold a large number of tokens at the same time. Even the bookkeepers who do not have much money would choose to form a collective top bookkeeper i.e. mining pool. However, the bookkeepers who only care for immediate interest but not long-term development would choose to reduce relative computing power to maximize profit, such as selling some mining machines to new bookkeepers. Even the conservative bookkeepers who do not do anything would be passively pushed to bottom bookkeepers. This is because as time goes by, their mining machines gradually lag behind the new ones and top bookkeepers control increasing computing power. Then, the conservative bookkeepers' relative computing power decreases gradually.

Hence, in the PoW-based blockchain, the amount of top and bottom bookkeepers would grow over time and the distribution of bookkeepers tends to polarize. Figure 2 shows the computing power of Ethereum bookkeepers denoted by the proportion of blocks mined in a month. We can see that most of the computing power in the system is under the control of several top bookkeepers. In fact, the top 5 bookkeepers control more than 80% of the computing power. Figure 3 shows that the bottom bookkeepers' computing power decreases in the month. Therefore, the theoretical result about bookkeepers' strategy is supported by real world data in Ethereum blockchain.

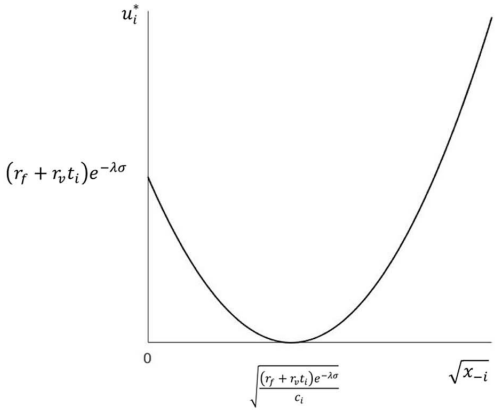



**Fig. 1** Optimal Strategy in PoW based Blockchain

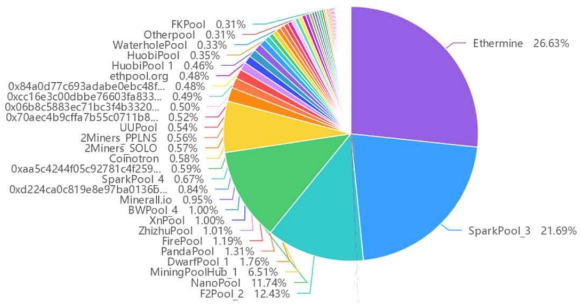



**Fig. 2** Bookkeepers Distribution by Blocks[1]

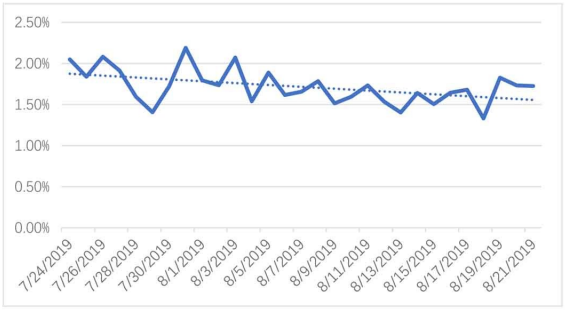



**Fig. 3** Proportion of Blocks Mined by Bottom Bookkeepers[2]

## Bookkeepers in a PoS system

Assume that a blockchain uses the consensus protocol PoS, let $y_i$ denote the number of tokens staked by bookkeeper i for block creation. Then, bookkeeper $i$'s relative stake $s_i$, with respect to the total stake, can be formulated [12] as

$$s_i = \frac{y_i}{\sum_{j\in N} y_j} = \frac{y_i}{y_i + y_{-i}}. \tag{8}$$

Wherein, $y_{-i} = \sum_{j\in N, j\neq i} y_j$ represents all tokens staked collectively by bookkeepers other than $i$. Then, the probability of success $P_i$ can be formulated as

$$P_i = s_i e^{-\lambda\sigma}. \tag{9}$$

Same as Kang et al.'s research about PoS-based consortium blockchain [12], we model bookkeeper $i$'s expected utility in a PoS-based blockchain as followed

$$U_i = r_f P_i + r_v t_i s_i - d_i y_i \tag{10}$$

Bookkeepers do not need to bear the cost of mining in a PoS-based blockchain. But they have to hold tokens required for staking, such that the risk of token price volatility $d_i$ takes the place of mining cost.

Definitions of $r_f$, $r_v$ and $t_i$ are the same as defined in Section 2. By substituting (8) and (9) into (10), we can obtain

$$U_i = r_f e^{-\lambda\sigma} \frac{y_i}{y_i + y_{-i}} + r_v t_i \frac{y_i}{y_i + y_{-i}} - d_i y_i. \tag{11}$$

The objective function for bookkeeper $i$ is therefore,

$$\begin{aligned} &\max\ U_i \\ &s.t. \underline{y_i} \le y_i \le \overline{y_i}. \end{aligned} \tag{12}$$

$\underline{y_i}$ denotes the minimum number of tokens required by the system regulations. For example, this number is 32 ETHs according to Casper protocol in Ethereum. And $\overline{y_i}$ denotes the total number of tokens in circulation. Note that no participator would be willing or allowed to hold all the tokens because the system will be controlled by one individual and lose its value as a public blockchain. Differentiate $U_i$ with respect to $y_i$, we have

$$\frac{\partial U_i}{\partial y_i} = (r_f e^{-\lambda\sigma} + r_v t_i) \frac{y_i + y_{-i} - y_i}{(y_i + y_{-i})^2} - d_i.$$

By solving $\frac{\partial U_i}{\partial y_i} = 0$ we can obtain bookkeeper $i$'s optimal strategy formulated as

$$y_i^* = \sqrt{\frac{(r_f e^{-\lambda\sigma} + r_v t_i) y_{-i}}{d_i}} - y_{-i}. \tag{13}$$

Substitute $y_i^*$ into equation (11) and we have

$$\begin{aligned} U_i^* &= r_v t_i + r_f e^{-\lambda\sigma} + d_i y_{-i} - 2\sqrt{(r_f e^{-\lambda\sigma} + r_v t_i) y_{-i} d_i} \\ &= \left(\sqrt{d_i y_{-i}} - \sqrt{(r_f e^{-\lambda\sigma} + r_v t_i)}\right)^2. \end{aligned} \tag{14}$$

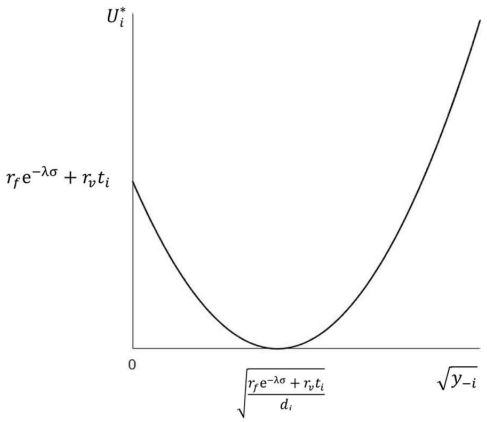



**Fig. 4** Optimal Strategy in PoS based Blockchain

Similar to the results in Section 2, Equation 14 is a quadratic equation of $\sqrt{y_{-i}}$ that intersects with the $\sqrt{y_{-i}}$ -axis at $\sqrt{\frac{r_f e^{-\lambda\sigma} + r_v t_i}{d_i}}$ and $U_i^*$ -axis at $r_f e^{-\lambda\sigma} + r_v t_i$. Then we can also qualitatively draw the graph of Equation 7. As shown in Figure 4, $U_i^*$ achieves the maximal value when $y_{-i}$ close to 0 or ∞, which means $s_i$ is close to 1 or 0. Therefore, the same to the PoW situation, the distribution of bookkeepers still tends to be polarized in a PoS-based blockchain.

In addition, when a blockchain switches from PoW to PoS, in order to participate in transaction validation, bookkeepers have to hold tokens for staking. In the PoW-based blockchain, the bookkeepers who own most of the computing power (top bookkeepers) also hold most of the tokens, while the bookkeepers who own less computing power always sell out the tokens they earn immediately or hold only a few tokens (bottom bookkeepers). Therefore, the coin-holding cost of top bookkeepers is far less than the mining cost in PoW system. Equation 13 indicates that a small $d_i$ results in

[1] https://eth.btc.com/miningstats
[2] https://www.etherchain.org/charts/miner

bigger number of tokens on hold. Therefore, top bookkeepers under PoS would buy more tokens than under PoW. Similarly, for the bottom bookkeepers, holding tokens brings more cost burden as well. Consequently, a large $d_i$ in Equation 13 reduces the bottom bookkeepers' optimal number of tokens on hold. This means that the bottom bookkeepers may wish to hold fewer tokens than the staking minimum so as to drop out of the game.

Since the bigger computing power a bookkeeper has, the more tokens he holds, we assume this correlation is linear and can be formulated as $y_i = ax_i$, where $a$ is unknown parameter. Then, Equation 14 can be translated into

$$U_i^* = \left(\sqrt{d_i a x_{-i}} - \sqrt{(r_f e^{-\lambda\sigma} + r_v t_i)}\right)^2. \quad (15)$$

We can see that Equation 15 intersects with the $\sqrt{x_{-i}}$ -axis at $\sqrt{\frac{r_f e^{-\lambda\sigma} + r_v t_i}{d_i a}}$ and $U_i^*$-axis at $r_f e^{-\lambda\sigma} + r_v t_i$. By comparing Equations 7 and 15, we can obtain three cases as shown in Figure 5, where the vertical axis represents "bookkeeper utility". In this figure, we use the solid curve to indicate the utility function of bookkeeper $i$ in a PoS system and the dotted curve to indicate the utility function of bookkeeper $i$ in a PoW system. When $\sqrt{\frac{r_f e^{-\lambda\sigma} + r_v t_i}{a d_i}} > \sqrt{\frac{(r_f + r_v t_i) e^{-\lambda\sigma}}{c_i}}$, we have case 1. In this case, the top bookkeepers, whose $h_i$ approaches 1 ($\sqrt{x_{-i}}$ approaches 0), would obtain more utility in the PoS system $(U_i^* > u_i^*)$ as shown in Figure 5a, where the solid curve is above the dotted curve. However, the bottom bookkeepers whose $h_i$ approaches 0 ($\sqrt{x_{-i}}$ approaches ∞) would obtain less utility in the PoS system $(U_i^* < u_i^*)$, where the solid curve is under the dotted curve. Therefore, when system switches from PoW to PoS, the top bookkeepers have more incentive to mass more power. But the bottom bookkeepers would stay the same. This is because even though the bottom bookkeepers' utility decreases, they still obtain more utility to stay in the bottom group than in middle range. When $\sqrt{\frac{r_f e^{-\lambda\sigma} + r_v t_i}{a d_i}} = \sqrt{\frac{(r_f + r_v t_i) e^{-\lambda\sigma}}{c_i}}$ or $\sqrt{\frac{r_f e^{-\lambda\sigma} + r_v t_i}{a d_i}} < \sqrt{\frac{(r_f + r_v t_i) e^{-\lambda\sigma}}{c_i}}$, we have cases 2 and 3. Similar to case 1, both the top and bottom bookkeepers would obtain more utility in PoS system as shown in Figure 5b and 5c. That is to say, both the top and bottom bookkeepers have more incentive to aggregate toward to the opposite sides under PoS than PoW.

In summary, when a blockchain switches to the PoS consensus protocol from PoW, top bookkeepers tend to mass even more influence. For bottom bookkeepers, they would be weakened further or maintain the status quo. Because some bottom bookkeepers turn to quit the game due to the requirement of minimum staking tokens, the relative power of top bookkeepers under PoS would be even higher than under PoW. Of course, this theoretical result still requires validation in practice.

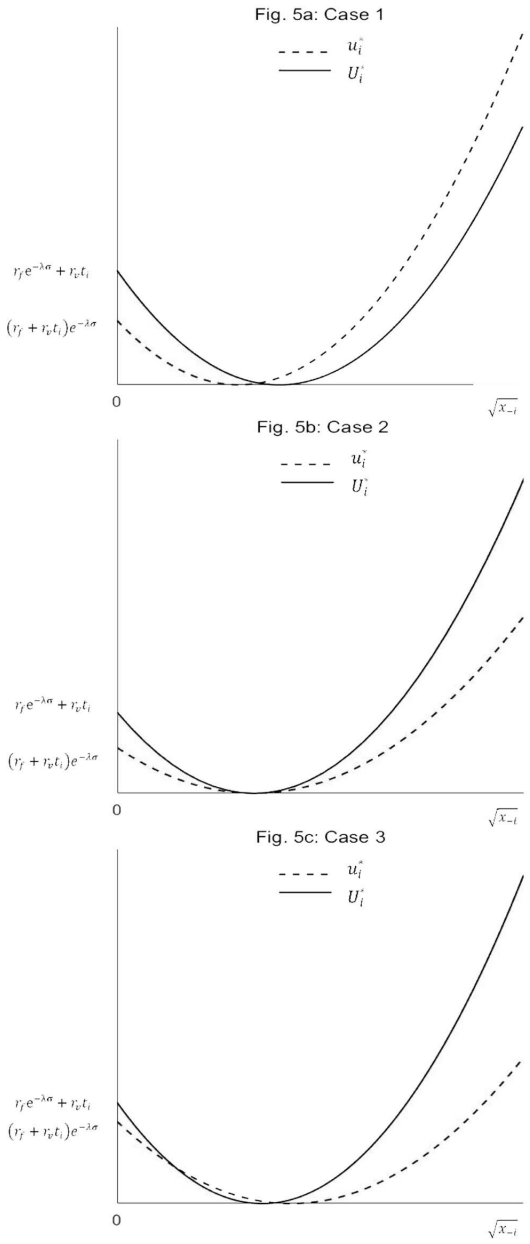



**Fig. 5** Comparison of Optimal Strategies in PoW and PoS

## CONCLUSION

In this paper, we develop economic models to analyze bookkeeper behavior in PoW and PoS systems and study how their behavior changes when switching from PoW to PoS by means of comparative static analysis. This theoretical research method helps us understand reasons and principles of phenomenon theoretically and generates useful insights about future development. First, we find that the distribution of bookkeepers tends to polarize in PoW systems. The validity and accuracy of result is verified by the descriptive statistical analysis in Section 2. Then we draw attention to the PoS system that Ethereum might implement in the near future. By the same method, we find that the distribution of bookkeepers tends to polarize further. Furthermore, the

degree of polarization becomes higher and both the staking power and tokens aggregate more towards to the top bookkeepers. Therefore, our findings show that although the PoS consensus protocol could solve the efficiency problem to a great degree by removing mining cost, it would make the fairness issue even more serious.

The insights of this paper are important for managers and developers of public blockchains. Decentralization as one of the most significant features of public blockchain cannot be guaranteed. The bookkeeping opportunities are always controlled by the top bookkeepers. If a blockchain such as Ethereum pays more attention to decentralization or fairness, it should be aware of this issue. When a blockchain values higher efficiency and lower energy consumption, it may switch to the PoS system. But, this comes at the expense of less fairness. In order to alleviate this negative effect, managers should reduce the minimum staking number to retain more bottom bookkeepers or encourage pooling of bookkeepers with lower staking power.

An interesting phenomenon we realized while working on this short paper is that starting with PoW and then switch to PoS once the blockchain system stabilizes is necessary because the system requires the bookkeepers to be settled down with sufficient tokens for staking. That is to say, a PoS system may be difficult to start by itself, and an initial PoW system is the necessary evil as the foundation of its PoS successor.

This study can be extended in a few directions. First, we only conducted a static analysis at the moment when the consensus protocol is switched from PoW to PoS. Future work could study the dynamics and long-term evolution of bookkeeper behavior and consider the volatility of token price. Second, with the implementation of the Casper protocol in Ethereum, empirical research could be done to validate our theoretical findings in the future. ■

## REFERENCES

[1] M. Swan, *Blockchain: Blueprint for a New Economy.* 2015.

[2] V. Buterin and V. Griffith, "Casper the Friendly Finality Gadget," 2017. [Online]. Available: https://github.com/ethereum/research/blob/master/papers/casper-basics/casper_basics.pdf.

[3] V. Buterin and E. Foundation, "Incentives in Casper the Friendly Finality Gadget Recap : The Casper Protocol," 2017. [Online]. Available: https://github.com/ethereum/research/blob/master/papers/casper- economics/casper_economics_basic.pdf.

[4] G. Machado, "Vitalik Buterin's Four Major Points of Emphasis Regarding the Transition to Proof of Stake Mining," 2019. [Online]. Available: https://bitcoinexchangeguide.com/vitalik-buterins-four-major-points-of-emphasis-regarding-the-transition-to-proof-of-stake-mining/.

[5] L. M. Bach, M. Branko, and M. Zagar, "Comparative Analysis of Blockchain Consensus Algorithms," *2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. (MIPRO). IEEE*, pp. 1545–1550, 2018.

[6] W. Wang *et al.*, "A survey on consensus mechanisms and mining management in blockchain networks," *arXiv Prepr. arXiv1805.02707*, pp. 1–33, 2018.

[7] H. Arslanian and F. Fabrice, *The Future of Finance.* 2019.

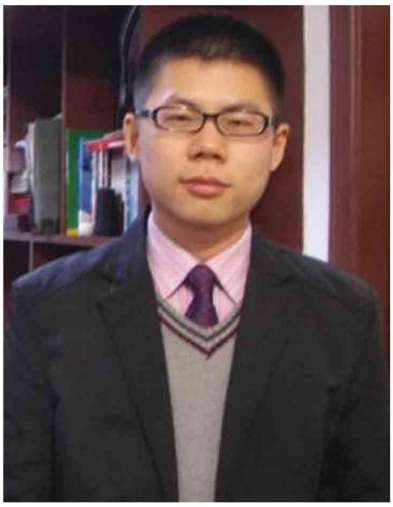
[8] G. Massarotto, "Massarotto G. From Digital to Blockchain Markets: What Role for Antitrust and Regulation," *Available SSRN 3323420*, pp. 1–22, 2019.

[9] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Edge Computing Resource Management and Pricing for Mobile Blockchain," *arXiv Prepr. arXiv1710.01567*, 2017.

[10] N. Houy, "The Bitcoin Mining Game," *Ledger*, vol. 1, pp. 53–68, 2016.

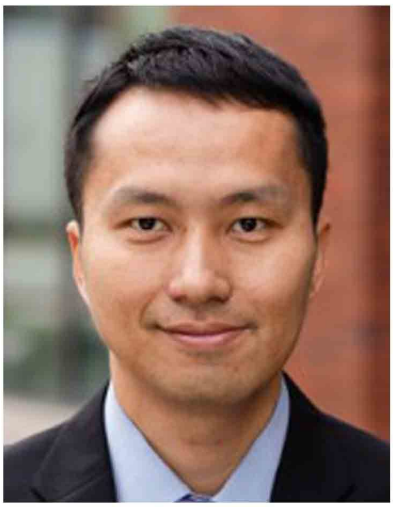
[11] R. Peter, "BLOCK SIZE LIMIT DEBATE WORKING PAPER A Transaction Fee Market Exists Without a Block Size Limit," *Work. Pap.*, pp. 1–16, 2015.

[12] J. Kang, Z. Xiong, D. Niyato, and P. Wang, "Incentivizing Consensus Propagation in Proof-of- Stake Based Consortium Blockchain Networks," *IEEE Wirel. Commun. Lett.*, no. August, 2018.



Dapeng Pan

Dapeng Pan received the B.S. degree from the School of Science, China University of Mining & Technology, Beijing, and the M.S. degree from the School of Science, Heilongjiang University. He is currently a Ph.D. student in the School of management, Harbin Institute of Technology. His research interests include consensus mechanism and incentive mechanism in blockchain network.



Shaokun Fan

Shaokun Fan is an assistant professor in Business Information Systems at Oregon State University. He received his Ph.D. in Management Information Systems from the University of Arizona. His research interests involve fintech, big data analytics, and business process management. He has taught courses on data/text mining, database, programing and system analysis and design. He has published research articles in journals such as Informs Journal on Computing, Decision Support Systems, and Information & Management.

J. Leon Zhao

J. Leon Zhao is currently Chair Professor in Information Systems, City University of Hong Kong (CityU), where he was Head of Information Systems from 2009 to 2015. Before joining CityU, He was Interim Head and Eller Professor in MIS, University of Arizona. He holds Ph.D. in Information Systems from Haas School of Business, UC Berkeley. He is currently director of the CityU Center on Global Internet Finance (since 2015), the CityUSRI Lab on Enterprise Process Innovation and Computing (since 2007), and CityUCRI Center on Blockchain-centric Business Innovation (since 2017). His research has been funded by CityU, NSF, NSFC, RGC, SAP, IBM, Shenzhen Government among others; as PI, he has received over 20 million HKD in total research funding (including two recent grants on blockchain). He received IBM Faculty Award at the University of Arizona in 2005 and Chang Jiang Scholar Chair Professorship at Tsinghua University in 2009. His research is in information technology and applications, with a special focus on FinTech and Blockchain. He has been co-editor of Springer journal on Financial Innovation, Senior Editor of Decision Support Systems, and Associate Editor of IEEE Transactions on Service Computing, ACM Transactions on MIS, and Electronic Commerce Research and Applications among others. Since 2003, He has co-edited over 20 special issues in various academic journals; most recently, he is co-editor of Big Data Special Issue for MIS Quarterly (published in December 2016) and co-editor of FinTech for Information Systems Research (to be completed in 2020). He has chaired numerous conferences and is the lead founder of several academic conferences including China Summer Workshop on Information Management (since 2007) and International Conference on Smart Finance (since 2016).