A Distributed Game Theoretic Approach for Blockchain-based Offloading Strategy

Weikang Liu[1], Bin Cao[1], Lei Zhang[2], Mugen Peng[1] and Mahmoud Daneshmand[3]
[1]State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2]James Watt School of Engineering, University of Glasgow, G12 8QQ Glasgow, U.K.
[3]School of Business, Stevens Institute of Technology, Hoboken, NJ 07030, USA
Email: {2013211995, caobin}@bupt.edu.cn, lei.zhang@glasgow.ac.uk, pmg@bupt.edu.cn, mdaneshm@stevens.edu

***Abstract*—Keeping patients sensitive information secured and untampered in the e-Health system is of paramount importance. Emerging as a promising technology to build a secure and reliable distributed ledger, blockchain can protect its data from being falsified, which has attracted much attention from both academia and industry. However, with limited computational resources, medical IoT devices do not have enough ability to fulfill the functionalities as a full node in wireless blockchain network (WBN). Facing this dilemma, Mobile Edge Computing (MEC) brings us dawn and hope through offloading the high resource demanding blockchain functionalities at the IoT devices to the MEC. However, aiming to maximize the mining profit, most of existing offloading strategies have ignored that the actual need of wireless devices is instant data writing, which is also the problem faced by blockchain technology. In this paper, according to different needs, blockchain nodes are firstly divided into two categories. One is blockchain users whose needs are faster transaction uploading, the other is blockchain miners whose goals are maximum revenue. Then, to maximize both the utilities of blockchain users and blockchain miners, a Stackelberg game is introduced to formulate the interaction between them. From the simulation results, this game is proved to converge to a unique optimal equilibrium.**

I. Introduction

Internet of Things (IoT) has been identified as one of the most disruptive technologies of this century. It has attracted much attention of society, industry and academia as a promising technology that can enhance day to day activities, the creation of new business models, products and services, and as a broad source of research topics and ideas. However, due to the low cost and low complexity constraints, IoT is also one of the most vulnerable elements in the network to be attached, and thus, facing serious data security issues. In recent years, security and traceability of collected data from IoT devices has attracted great attention from society, especially the health data in the field of e-Health. Initially proposing a solution to this problem in cryptographic domains, blockchain has gradually become the focus in both the financial sector and the society [1]. Besides being an effective means to protect the security and privacy of virtual assets, it also emerges as a promising tool in designing an autonomous and scalable decentralized network which can attract more participants to share their edge resources. To foster distributed edge-centric models for edge-centric IoT by encouraging edge resources sharing, [2] has elucidated the consensus facets from myriad of aspects, such as data structure, scalable consensus ledgers, and so on.

However, constrained by the cost, size and battery life, typical IoT devices can not possess sufficient capability to run a resolute demanding blockchain protocol. MEC, as an emerging technology, allows wireless devices to offload their their computation tasks to edge servers. It has been studied that the computational resource allocation problem of public blockchain network can be solved under MEC environment, where wireless devices rent computational resources from corresponding edge servers to solve the Proof-of-work (PoW) puzzle, and earn mining rewards as well as transaction fees from blockchain [3]. As mobile miners, wireless devices can resort to the nearby edge server to perform the PoW puzzle and content caching in [4], where computation offloading scheduling and caching strategy are jointly considered. Although the topic of blockchain based offloading strategy has been studied extensively, there still exist some overlooked problems.

Most of researches treat wireless devices as miners whose main purposes are to maximize the mining rewards. However, what motivates wireless devices to upload transactions to blockchain is actually the characteristics of a trusted leger, where data can not be tempered and destroyed. In contrast to the faster transaction uploading needs of wireless devices, the throughput of current blockchain project is so small. For example, Bitcoin's throughout is only about 7 transactions per second. How to do the mining process is not the focus of wireless devices, but the concern of edge servers who aim to earn transaction fees. To this end, in this paper, wireless devices are blockchain users who only need to upload transactions to blockchain with requirements for transaction rate, while both normal edge servers and servers with wireless access function are actual blockchain miners who undertake blockchain functionality operations. Besides, it is reasonable to assume that all IoT devices are connected with the servers through wireless channel. It is worth to note that the wireless link between the device and server is secure since every transaction contains the signature [5]. To avoid transactions uploading termination caused by single point failure of the accessed server, wireless devices can broadcast their transactions to all nearby access points they can access.

The main contributions of this paper are as follows: 1)

Considering the actual needs of wireless devices which are constrained by cost, size and battery life, different from other researches, they are treated as blockchain users in this paper, who only need to upload transactions into blockchain, while the blockchain functionality operations are executed in the edge servers. 2) The Stackelberg game is constructed to model the interaction between blockchain users and blockchain miners. According to the data spread on blockchain network, acting as the leader, all blockchain miners can reach a consensus on the price per block. Then, as followers, blockchain users require their transaction rate based on the price. 3) A distributed algorithm is proposed, which can effective solve the game model.

The system model and problem formulation are given in Section II. In Section III, the optimal solution of the Stackelberg game formulated in previous section is analysed and the distributed algorithm is proposed. Simulation results are discussed in Section IV. In Section V, the conclusion and future work are given.

II. System Model And Problem Formulation

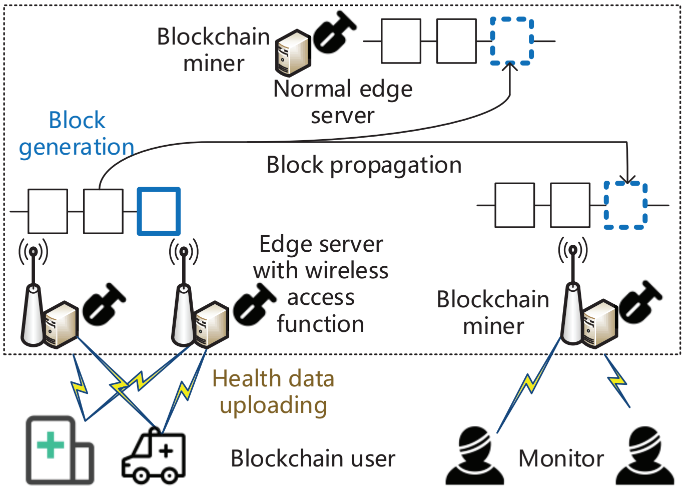


Fig. 1. A typical scenario of blockchain based MEC for e-Health

A. System model

As illustrated in Fig.1, the system model adopted in this paper consists of two entities: 1) blockchain users, 2) blockchain miners. Wireless devices who need to upload transactions to blockchain are blockchain users. Both normal edge servers and edge servers with wireless access function in this system are blockchain miners. With PoW consensus mechanism, each blockchain miner needs to perform hashing operations at a huge rate, resulting in a low block completion probability for its Bernoulli trails, meaning that the block completions at each blockchain miner can be modeled as a Poisson process [6]. Let $\{\lambda_1, ..., \lambda_i\}, i \in \mathbb{K}$ denote the block completion rate of blockchain miners' set (denoted by $\mathbb{K} = \{1, ..., K\}$) measured by the number of blocks per hour. Therefore, the aggregate block completion of blockchain can also be modeled as a Poisson process with rate.

$$\Lambda = \sum_{i=1}^{K} \lambda_i. \tag{1}$$

The main chain is chosen by the Longest-Chain-Rule (LCR) [1] in the model. Due to the fact that a mined block is not immediately synchronized to the entire system because of transmission delay, it will routinely happen that simultaneous blocks may spread in the system and each miner individually chooses which block to accept. Thus, the effective growth rate of the main chain (denoted by Γ) will be less than the aggregate block completion rate Λ. Assuming that each block contains T transactions, the effective transaction rate of whole blockchain can be modeled as a Poisson process with rate $T\Gamma$. To inspire normal operation of this system, it is reasonable for blockchain miners to charge blockchain users a fee with price β per block. Of course, there is no need for blockchain users to pay for orphan blocks. Paying a fee, it is also reasonable for blockchain users to require an appropriate transaction rate $\gamma_j, j \in \mathbb{N}$ ($\mathbb{N} = \{1, ..., N\}$ denote blockchain users' set). Thus, there exists an equation between the overall effective transaction rate $T\Gamma$ and transaction rate γ_j,

$$T\Gamma = \sum_{j=1}^{N} \gamma_j. \tag{2}$$

Focusing on symmetric scenarios, the block completion rate of different blockchain miners can be set to the same value with $\lambda_i \equiv \lambda$, for all $i \in \mathbb{K}$. Therefore, the aggregate block completion rate $\Lambda = K\lambda$. According to [7], the communication intervals between two blockchain miners $k \neq l, \{k, l\} \in \mathbb{K}$ can be assumed as an exponential distribution with parameters $\mu_{k,l}$. Without loss of generality, for all $k \neq l, \{k, l\} \in \mathbb{K}$, the communication intervals can be also set to the same value with $\mu_{k,l} \equiv \mu$. Based on the conclusion of [6], the effective growth rate Γ behaves as

$$\Gamma = K\lambda \left(1 - \frac{\lambda A}{\mu}\right) = \Lambda \left(1 - \frac{\Lambda A}{K\mu}\right) \tag{3}$$

where $A = \sum_{k=1}^{K-1} \frac{1}{k}$ for the sake of presentation. Based on equation (2), Λ can then show as follows,

$$\Lambda = \frac{K\mu(T - \sigma)}{2AT} \tag{4}$$

where

$$0 < \sigma = \sqrt{\frac{T\left(KT\mu - 4A\sum_{j=1}^{N} \gamma_j\right)}{K\mu}} < T. \tag{5}$$

Actually, there is another feasible solution $\Lambda^{'} = \frac{K\mu(T+\sigma)}{2AT} > \frac{K\mu}{2A}$. However, when $\Lambda = \frac{K\mu}{2A}$, Γ gets its extreme value. As a result, when $\Lambda = \Lambda^{'}$, there would be more computational resources consumption. Thus, for a better state, $\Lambda^{'}$ is discarded.

Once a blockchain user generates a transaction, this transaction will be then broadcast to the nearby blockchain miners which are equipped with wireless access function. In order to include transactions in a block and spread this block on blockchain, blockchain miners would compete with each other to solve a PoW puzzle with the given parameters derived by the data of blockchain, at the cost of their own computing power. Let c denote the cost of a blockchain miner to produce a unit of computational power, and then the cost for each block is cr where r is the miner's computing power or hash power [8]. Learning from [9], there exists an relationship $\lambda = {}^{r}/_{D}$ where D is the difficulty of mining a block. Thus, the cost of generating a block in this model is

$$cr = cD\frac{r}{D} = cD\lambda = cD\frac{\Lambda}{K}. \tag{6}$$

Considering a practical constraint that D must be an appropriate value which can avoid generating block too fast [1] and each blockchain miner has finite computation capacity. Therefore, there exists a constraint $\lambda \leq \lambda_{max}$. As a result, there exists

$$\Lambda = K\lambda \leq K\lambda_{max}. \tag{7}$$

Then, in this symmetric scenario, based on the equation (3), there exists an fixed upper bound Γ_{max} for Γ with corresponding value K,

$$\Gamma_{\max} = \begin{cases} K\lambda_{\max}\left(1 - \frac{\lambda_{\max}A}{\mu}\right) & \lambda_{\max} < \frac{\mu}{2A}, \\ \frac{K\mu}{4A} & \lambda_{\max} \geq \frac{\mu}{2A}. \end{cases} \tag{8}$$

Hence, according to equation (2), the constraint on blockchain users' requirements for their transaction rates can show as follows,

$$\sum_{j=1}^{N} \gamma_j = T\Gamma \leq T\Gamma_{max}. \tag{9}$$

B. Stackelberg Game Formulation

In order to encourage blockchain miners to share their computational resources, they have rights to claim for a fee for every transaction which is paid by blockchain users. With different fees, blockchain users could require different transaction rates. As to blockchain user j, defined as f_j, when it has a requirement γ_j for transaction rate, according to equation (3), the fee, that it should pay to each transaction, is ${}^{\beta}/_{T}$, where β is the price of single block. Thus the Stackelberg game can be formulated to model the interaction between the blockchain users and blockchain miners, where the blockchain miners' set is the leader and blockchain users are the followers.

At blockchain users' side, the utility of blockchain user f_j includes the satisfaction degree and incentive cost, i.e., the transaction fee. The objective of them is to maximize the utility by requiring considerable transaction rate γ_j, for given price β per block set by blockchain miners' set. Therefore, the optimization problem for f_j can be expressed as follows

$$\begin{aligned} \max_{\gamma_j} \quad & U_{f_j} = \alpha \log\left(1 + \gamma_j\right) - \frac{\beta}{T}\gamma_j \\ s.t. \quad & \sum_{j=1}^{N} \gamma_j \leq T\Gamma_{max} \end{aligned} \tag{10}$$

where α is the weight factor. Widely used in mobile computing and wireless communication domains [10] [11], the logarithmic function $f = \log(1 + y)$ is adopted to evaluate the satisfaction degree of blockchain users in this paper.

At blockchain miners' side, the utility function of them is defined as charged transaction fees minus computational resources consumption per hour. The goal of them is to maximize their revenue by helping blockchain users upload transactions to blockchain with price β per effective block. Mathematically, the optimization problem can be expressed as

$$\max_{\beta} \quad U_l = \beta\Gamma - cD\frac{\Lambda}{K} \cdot \Lambda. \tag{11}$$

III. Optimal Solution Analysis

In this section, based on the Karush-Kuhn-Tucker (KKT) conditions [12] and backward induction method, the optimization problem of both leaders and followers are firstly analysed. Then, in the distributed environment, under the help of iterative update function proposed in this paper, the optimal solution can be obtained. Finally, the optimal solution is proved to be a SE in the proposed game.

A. Analysis of Follower's Optimization Problem

For blockchain user f_j, the second order derivation of U_{f_j} with respect to γ_j can be expressed as follows,

$$\frac{\partial^2 U_{f_j}}{\left(\partial\gamma_j\right)^2} = -\frac{\alpha}{\left(\gamma_j + 1\right)^2} < 0. \tag{12}$$

That means U_{f_j} is a concave function of γ_j. Since the constraint (9) is affine, the Lagrangian with the multiplier u can be applied to solve this optimization problem (10) at blockchain user f_j as follows

$$\begin{aligned} L_{f_j}(\gamma_j, u) =& \alpha \log\left(1 + \gamma_j\right) - \frac{\beta}{T}\gamma_j \\ & -u\left(\gamma_j + \sum_{i \neq j} \gamma_i - T\Gamma_{max}\right), \end{aligned} \tag{13}$$

and the KKT conditions can be gotten as follows where $*$ represent the optimal solution.

$$\begin{aligned} u^*\left(\gamma_j^* + \sum_{i \neq j} \gamma_i - T\Gamma_{max}\right) &= 0, \\ \gamma_j^* + \sum_{i \neq j} \gamma_i - T\Gamma_{max} &\leq 0, \\ \gamma_j^* > 0, u^* &\geq 0. \end{aligned} \tag{14}$$

Let $\frac{\partial L_{f_j}(\gamma_j, u)}{\partial \gamma_j} = 0$, the optimal γ_j^* can be obtained

$$\gamma_j^* = \frac{T\alpha}{\beta + Tu^*} - 1. \tag{15}$$

It is easy to see that γ_j^* is a function of β, which means that to obtain γ_j^*, the corresponding β is a necessary information. Besides, the information about the maximum transaction rate $T\Gamma_{max}$ this system can afford and the current transaction

$$\frac{\partial^2 U_l}{(\partial\beta)^2} = -\frac{2\alpha T u}{(\beta+Tu)^3} - \frac{2cD}{K}\left\{\frac{1}{\sigma^2}\frac{T^2\alpha^2}{(\beta+Tu)^4} + \Lambda\left[\frac{2AT}{K\mu\sigma^3}\frac{T^2\alpha^2}{(\beta+Tu)^4} + \frac{1}{\sigma}\frac{2T\alpha}{(\beta+Tu)^3}\right]\right\} < 0. \tag{16}$$

flow $\sum_{i\neq j}\gamma_i$ is also necessary. Based on the above, these information exchange will be considered in the designed blockchain of future work.

B. Analysis of Leader's Optimization Problem

For blockchain miners, based on the backward induction method, the second order derivation of U_l with respect to β can be expressed as follows

$$\begin{aligned}\frac{\partial^2 U_l}{(\partial\beta)^2} =& 2\frac{\partial\Gamma}{\partial\gamma_j}\frac{\partial\gamma_j}{\partial\beta} + \beta\left[\frac{\partial^2\Gamma}{(\partial\gamma_j)^2}\left(\frac{\partial\gamma_j}{\partial\beta}\right)^2 + \frac{\partial\Gamma}{\partial\gamma_j}\frac{\partial^2\gamma_j}{(\partial\beta)^2}\right] \\ & - \frac{2cD}{K}\left\{\left(\frac{\partial\Lambda}{\partial\gamma_j}\frac{\partial\gamma_j}{\partial\beta}\right)^2 + \Lambda\left[\frac{\partial^2\Lambda}{(\partial\gamma_j)^2}\left(\frac{\partial\gamma_j}{\partial\beta}\right)^2 + \frac{\partial\Lambda}{\partial\gamma_j}\frac{\partial^2\gamma_j}{(\partial\beta)^2}\right]\right\}.\end{aligned} \tag{17}$$

To prove that U_l has an extreme value, its convexity should be first analysed. From equation (15), with the corresponding β, γ_j^* can be calculated. Then, its first order derivation and second order derivation to β can be gotten

$$\begin{cases}\frac{\partial\gamma_j}{\partial\beta} = -\frac{T\alpha}{(\beta+Tu)^2}, \\ \frac{\partial^2\gamma_j}{(\partial\beta)^2} = \frac{2T\alpha}{(\beta+Tu)^3}.\end{cases} \tag{18}$$

According to equation (2) and (4), the first and second derivation of Γ and Λ show as follows,

$$\begin{cases}\frac{\partial\Gamma}{\partial\gamma_j} = \frac{1}{T}, \\ \frac{\partial^2\Gamma}{(\partial\gamma_j)^2} = 0.\end{cases} \tag{19}$$

$$\begin{cases}\frac{\partial\Lambda}{\partial\gamma_j} = \frac{1}{\sigma}, \\ \frac{\partial^2\Lambda}{(\partial\gamma_j)^2} = \frac{2AT}{K\mu\sigma^3}.\end{cases} \tag{20}$$

where $\sigma = \sqrt{\frac{T\left(KT\mu - 4A\sum_{j=1}^{N}\gamma_j\right)}{K\mu}}$. As a result, the conclusion exists that $\frac{\partial^2 U_l}{(\partial\beta)^2} < 0$ in equation (16), which indicates that U_l is a concave function of β.

Therefore, the optimal price β^* set by blockchain miners can be gotten when $U_l(\beta^*)$ is the extreme value. Although, in distributed environment, it is hard to get the closed form of β^* from the equation (21), because blockchain miners do not know the utility function of blockchain users. However, with the classic iterative method [10], the optimal solution can be worked out, and this progress will be represented in below.

$$\frac{\partial U_l}{\partial\beta} = \Gamma + \beta\frac{\partial\Gamma}{\partial\gamma_j}\frac{\partial\gamma_j}{\partial\beta} - \frac{2cD}{K}\Lambda\frac{\partial\Lambda}{\partial\gamma_j}\frac{\partial\gamma_j}{\partial\beta} = 0. \tag{21}$$

C. Optimal Solution

Combined with the above analysis, an updating scheme in distributed environment could be designed to achieve the optimal solution. In the proposed Stackelberg game, based on the computing cost c, β firstly is assigned an appropriate value which satisfies $\frac{\partial U_l(\beta)}{\partial\beta} > 0$. Then according to equation (15), after receiving the price β^t (t denote the iteration index) set by blockchain miners, the corresponding γ_j^t can be obtained at blockchain user f_j. Before sending it as game information to blockchain miners for price updating, it is necessary to check whether $u^t = 0$ and $\gamma_j = \gamma_j^t$ meet the KKT conditions. When $\gamma_j^t > T\Gamma_{max} - \sum_{i\neq j}\gamma_i$ which tells that the constraint $\gamma_j + \sum_{i\neq j}\gamma_i \leq T\Gamma_{max}$ is active. Then, in this condition, $\gamma_j^t = T\Gamma_{max} - \sum_{i\neq j}\gamma_i$, and according to equation (22), u^t can be gotten,

$$u^t = \frac{\alpha}{T\Gamma_{\max} + 1 - \sum_{i\neq j}\gamma_i} - \frac{\beta^t}{T}. \tag{22}$$

Next, from information γ_j^t and $\frac{\partial\gamma_j}{\partial\beta}\Big|_{(\beta^t,u^t)}$ sended by the blockchain user f_j, based on equation (18)-(21), blockchain miners can update their price by using the following updating

Algorithm 1 Iterative Updating Function

Input: α, c, D, μ, λ_{max}, K, N, T
Output: the converged β and $\gamma_j, j \in \mathbb{N}$ ($\mathbb{N} = \{1, ..., N\}$

```
Get Γ_max using (8)
Let the price β^t = c + Δ where Δ is an extremely small positive number
for each blockchain user f_j, j ∈ ℕ (ℕ = {1, ..., N} do
    Set iteration number index t = 0
    converged ← false
    while not converged do
        For blockchain user f_j:
            Set the Lagrangian multiplier u^t = 0
            Get β^t and Σ_{i≠j} γ_i according to blockchain state,
            update the corresponding transaction rate γ_j^t using (15)
            if γ_j^t > TΓ_max − Σ_{i≠j} γ_i then
                Get the right u^t according to (22)
                γ_j^t = TΓ_max − Σ_{i≠j} γ_i
            end if
        t = t + 1
        For blockchain miners:
            if ∂U_l|_{γ_j=γ_j^t} / ∂β < 0 then
                converged ← true
                β* = β^t and γ_j* = γ_j^t
            end if
            Get γ_j^t and u^t from blockchain user f_j, update
            the block price β^{t+1} according to (23).
    end while
end for
return β* and γ_j*, j ∈ ℕ (ℕ = {1, ..., N}
```

function (23) as follows,

$$\beta^{t+1} = \frac{\mu c D \left(T - \sigma^t\right)}{A \sigma^t} + \frac{{\gamma_j}^t + \sum_{i \neq j} \gamma_i}{T \alpha} \left(\beta^t + T u^t\right)^2, \quad (23)$$

where $\sigma^t = \sqrt{\frac{\left(K T \mu - 4 A \gamma_j^t - 4 A \sum_{i \neq j} \gamma_i\right) T}{K \mu}}$.

After that, it would be sent to blockchain users for the next round updating. Repeating the process until both the β and γ_j converge to a unique fixed value finally, the utility of both the users and miners cannot increase any more. Finally, the optimal solution is achieved. To better elucidate the above, the detail of the process is illustrated in Algorithm 1.

D. Stackelberg Equilibrium Solution

To prove the optimal solution analysed above is also the SE solution in which any participants has no motivation to deviate, the SE in this model can be firstly stated in Definition 1.

Definition 1. *When β is fixed, if γ_j^* satisfies $L_{f_j}\left(\gamma_j^*, u^*\right) \geq L_{f_j}\left(\gamma, u\right)$, and when γ_j if fixed, if β^* satisfied $U_l\left(\beta^*\right) \geq U_l\left(\beta\right)$, the Strategy Profile $\left(\beta^*, \gamma_j^*\right)$ is a SE in the proposed game.*

Then the conclusion that $\left(\beta^*, \gamma_j^*\right)$ is equal to the SE solution $\left(\beta^{SE}, \gamma_j^{SE}\right)$ can be drawn according to Appendix A.

IV. Performance Evaluation

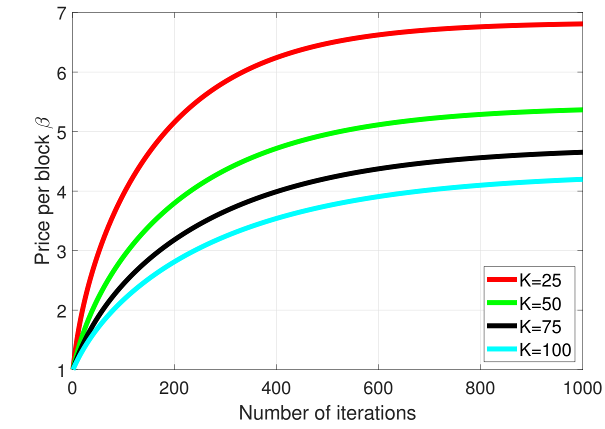
In this section, the performance is numerically evaluated in two aspects. First, the iterative updating process is showed under different numbers of blockchain miners. Second, the tendency of the strategy profile and utility are presented with an increasing number of blockchain miners.

A. Simulation Settings

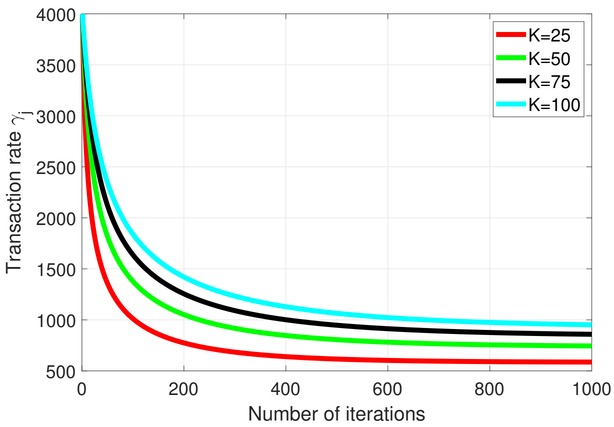
Corresponding to the average communication delay $12.6s$ in Bitcoin which is stated in [13], the communication interval parameter is set $\mu = 285/h$. Bitcoin's block completion rate is $6/h$ which can also be learned in [13], and its throughput is about 7 transactions per second [14]. Thus, every ten minutes, one block is generated and about 4000 transactions are written into blockchain. Hence, the number of transactions in each block T can be set to 4000. Let weight factor $\alpha = 1$ and $cD = 1$ which can also be set to other appropriate positive value. The max block completion rate of single device is fixed $\lambda_{max} = 0.1$, showing that each blockchain miner can generate a maximum of one block every ten hours.

B. Simulation Analysis

Fig.2 shows the iterative process of the pricing per block set by blockchain miners and the blockchain users' changing requirements of transaction rate under different number of blockchain miners. From Fig.2 (a), it is easy to see that as the number of iteration goes up, the price increases and finally converges to a stable value. Moreover, for more blockchain miners, the converged value of β will become smaller. Because of the increasing ability to generate blocks, although the price is smaller, the total revenue of blockchain miners can still be guaranteed. Similarly, in Fig.2 (b), the transaction rate requirement γ_j of blockchain user f_j will reach a stable value at last. It is also not difficult to understand why it moves inversely. Due to the reduction of price with increased blockchain miners, f_j can have faster requirement of transaction rate.



(a) Updates of price per block β



(b) Updates of transaction rate γ_j

Fig. 2. Price per block vs. block completion rate per device

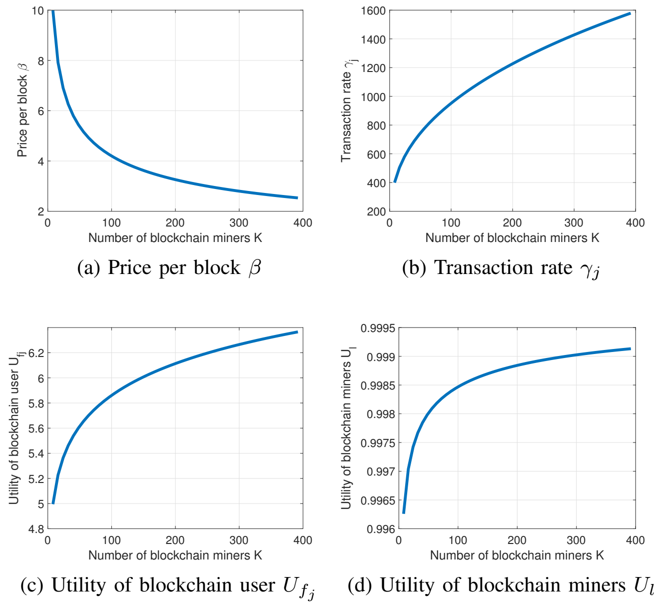
The evolution of utilities of both blockchain users and miners, the price set by the blockchain miners and the transaction rate needed by blockchain users are shown in Fig.3. First, it can be clearly seen in Figs.3 (a) and (b) that the price β increases and transaction rate γ_j decreases with the increasing number of blockchain miners, which is also consistent with the analysis from Fig.2. Second, based on Figs.3 (c) and (d), as the number of blockchain miners increases, the utilities of blockchain users and miners raise as well, though the transaction rate of f_j increases correspondingly. This is also the purpose of this algorithm, while meeting the requirements of blockchain users, it will guarantee the benefits of both parties. Finally, it shows a slowing trend as the number of blockchain miners increases. Because when the number reach a fixed value, the overall effective growth rate of blockchain will not increase, with more orphan blocks.

of definition 1, $L_{f_j}(\gamma_j, u)$ can get its maximum when $\gamma_j = \gamma_j^*$. Thus, it is also the SE solution γ_j^{SE}

$$\frac{\partial^2 L_{f_j}(\gamma_j, u)}{(\partial \gamma_j)^2} = \frac{\partial^2 U_{f_j}}{(\partial \gamma_j)^2} + \frac{\partial^2 g(\gamma_j)}{(\partial \gamma_j)^2} < 0. \tag{24}$$

Property 2. *For blockchain miners, the required transaction rate γ_j of f_j decreases as the price β increases according to equation (18). This makes sense because when blockchain miners increase their price, blockchain users will have lower requirements for the transaction rate.*

Property 3. *For blockchain miners, when blockchain users get the desired transaction rate γ_j, β^* is the optimal price which can maximize $U_l(\beta)$ under the condition that $\frac{\partial^2 U_l}{(\partial \beta)^2} < 0$ according to equation (16).*



(a) Price per block β (b) Transaction rate γ_j

(c) Utility of blockchain user U_{f_j} (d) Utility of blockchain miners U_l

Fig. 3. Utility and metrics versus the number of blockchain miners

V. Conclusion And Future Work

In this paper, a Stackelberg game is proposed to coordinate the needs of both the blockchain users and the blockchain miners where as blockchain users, paying fees, E-Health monitors can upload health data to blockchain with the aid of blockchain miners. Through the game between them, the revenue of the overall blockchain miners can be guaranteed, and at the same time, the performance of the transaction rate required by the blockchain users is also ensured. Besides validating the correctness of this model, the numerical results also shows that it behaves better when there are more blockchain miners, though it will not grow obviously after the number of them has reached a certain value.

For future work, simulation of single blockchain user will be extended to multiple blockchain users. Moreover, based on the distributed algorithm designed in this paper, the detailed interaction process between blockchain users and blockchain miners will be further discussed. Considering the existences of malicious blockchain users or blockchain miners, the security performance will be further analysed in future work.

Appendix A

Based on the following properties, the optimal solution can be proved to be equal to the SE solution.

Property 1. *For blockchain user f_j, when β is fixed, γ_j^* is the global optimum which can maximize $L_{f_j}(\gamma_j, u)$.*

According to equation (24), where $\frac{\partial^2 U_f}{(\partial \lambda)^2} < 0$ as analysed in equation (12) and $g(\gamma_j) = -u(\sum_{j=1}^{N} \gamma_j - T\Gamma_{max})$, $L_{f_j}(\gamma_j, u)$ is a concave function of γ_j. Satisfying the condition

References

[1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," White paper, 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues and K. Ko, "Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues," in IEEE Access, vol. 6, pp. 1513-1524, 2018.

[3] N. Zhao, H. Wu and Y. Chen, "Coalition Game-Based Computation Resource Allocation for Wireless Blockchain Networks," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8507-8518, Oct. 2019.

[4] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung and M. Song, "Computation Offloading and Content Caching in Wireless Blockchain Networks With Mobile Edge Computing," in IEEE Transactions on Vehicular Technology, vol. 67, no. 11, pp. 11008-11021, Nov. 2018.

[5] Sun, Y., Zhang, L., Feng, G., Yang, B., Cao, B. and Imran, M. A. (2019) Blockchain-enabled wireless internet of things: performance analysis and optimal communication node deployment. IEEE Internet of Things Journal, 6(3), pp. 5791-5802.

[6] N. Papadis, S. Borst, A. Walid, M. Grissa and L. Tassiulas, "Stochastic Models and Wide-Area Network Measurements for Blockchain Design and Analysis," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, Honolulu, HI, 2018, pp. 2546-2554.

[7] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," IEEE P2P 2013 Proceedings, Trento, 2013, pp. 1-10.

[8] Dimitri, N, 2017, "Bitcoin Mining as a Contest", Ledger, 2, http://doi.org/10.5195/ledger.2017.96.

[9] Bruno Biais, Christophe Bisière, Matthieu Bouvard and Catherine Casamatta, 2018, "The blockchain folk theorem", working paper.

[10] B. Cao, S. Xia, J. Han and Y. Li, "A Distributed Game Methodology for Crowdsensing in Uncertain Wireless Scenario," in IEEE Transactions on Mobile Computing, Early Access.

[11] C. Xu, M. Sheng, V. S. Varma, T. Q. S. Quek and J. Li, "Wireless Service Provider Selection and Bandwidth Resource Allocation in Multi-Tier HCNs," in IEEE Transactions on Communications, vol. 64, no. 12, pp. 5108-5124, Dec. 2016.

[12] H. Hindi, "A Tutorial on Convex Optimization," American Control Conference, 2004, Boston, pp. 3252-3262, Jun-Jul. 2004.

[13] J. Göbel, H.P. Keeler, A.E. Krzesinski, P.G. Taylor (2016). Bitcoin Blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Perf. Eval. 104, 23–41.

[14] B. Cao, Y. Li, L. Zhang et al., "When Internet of Things Meets Blockchain: Challenges in Distributed Consensus," in IEEE Network, Early Access.