A Correlated Equilibrium based Transaction Pricing Mechanism in Blockchain

Qin Hu*, Yash Nigam*, Zhilin Wang†, Yawei Wang‡, Yinhao Xiao (Corresponding Author)§
*Department of Computer and Information Science, Indiana University-Purdue University Indianapolis, Indiana, USA
†School of Economics and Management, Nanchang University, Jiangxi, P.R. China
‡Department of Computer Science, The George Washington University, Washington DC, USA
§School of Information Science, Guangdong University of Finance and Economics, Guangzhou, P.R. China
Email: qinhu@iu.edu, ynigam@iu.edu, hellojerrywong18@gmail.com, yawei@gwu.edu, xyh3984@gmail.com

***Abstract*—Although transaction fees are not obligatory in most of the current blockchain systems, extensive studies confirm their importance in maintaining the security and sustainability of blockchain. To enhance blockchain in the long term, it is crucial to design effective transaction pricing mechanisms. Different from the existing schemes based on auctions with more consideration about the profit of miners, we resort to game theory and propose a correlated equilibrium based transaction pricing mechanism through solving a pricing game among users with transactions, which can achieve both the individual and global optimum. To avoid the computational complexity exponentially increasing with the number of transactions, we further improve the game-theoretic solution with an approximate algorithm, which can derive almost the same results as the original one but costs significantly reduced time. Experimental results demonstrate the effectiveness and efficiency of our proposed mechanism.**

***Index Terms*—Blockchain, transaction pricing, game theory, correlated equilibrium**

I. Introduction

Since Bitcoin was proposed in 2008 as the first representative conceptualization of blockchain, the world witnessed a huge amount of attention being injected into this area from both the academia and industry. The most important contribution of blockchain is that it can achieve distributed trust without any centralized coordination, which further highlights an attractive feature of blockchain that all recorded information, such as transactions and smart contracts, inside blocks on the main chain cannot be arbitrarily modified or repudiated. This delicately designed technology achieving distributed security enables wide applications of blockchain in various directions, such as blockchain-based database [1], blockchain-witnessed trustworthy cloud service [2], blockchain-assisted admission control in cognitive radio network [3], and blockchain-driven internet of things [4], [5].

To maintain the aforementioned attractive feature, a large number of nodes are involved to reach consensus on who should append the newly generated block to the main chain so as to guarantee the stability and security of the whole blockchain network, which might incur massive costs for participated nodes, e.g., computation cost and communication cost, according to specific consensus algorithms. As an incentive for their work, the node who finally wins the accounting right will receive a reward, which usually comes from two sources, including the blockchain system and the information-record owners. The first part is generally predefined when the blockchain system is initially designed, which is relatively stable. While the second part is determined by the record owners as a sort of handling fee. As *transaction* is a representative type of information record in blockchain, we study its pricing problem as an example in this paper[1] and refer to its owner as a *user*. In most prevailing blockchain systems, such as Bitcoin [6] and Ethereum [7], the transaction fee is optional, thus making it unpredictable and seemingly trivial. However, as pointed out in [8]–[10], transaction fees from users have a significant influence on the system security of blockchain, which becomes even more prominent in blockchain systems with decreasing block rewards.

Being aware of this, many researchers analyze specific relationships between transaction fees and various security metrics of blockchain systems with the help of game theory [11]–[14]. Other existing work is devoted to transaction pricing mechanism design based on auctions [10], [15], [16] from the perspective of miners' profit. In contrast, our paper designs a transaction pricing mechanism from the perspective of users, providing price suggestions to realize both global and individual rationality.

However, it is challenging to design such a transaction pricing mechanism due to the following two reasons. First, from the perspective of users, the ultimate goal of everyone is to get his transaction included in a valid block on the main chain by paying the transaction fee as low as possible. This is hard to achieve since they have to compete with each other on price with incomplete information about the offers from other competitors. Second, from the perspective of the blockchain system, if malicious competitions among users enforce an excessive pricing bar or extremely long waiting time, users who cannot afford it will stop using it, which impedes the sustainable development of blockchain.

To address the above challenges, we resort to game theory

[1] Pricing of other sorts of information records can be tackled in a similar way.

978-1-7281-6680-3/20/$31.00 ©2020 IEEE

to model the coexisted competition and collaboration among users and take advantage of the concept of correlated equilibrium [17] to achieve both individual and global optimum. To be specific, we consider a platform for price recommendation with users inputting the sizes and time sensitivities of their transactions, which can efficiently calculate the optimal pricing strategies for all users with the best utilities, thus solving the first challenge. In addition, as the recommended prices are derived according to the real-time parameters of all transactions, the expenses of users will not increase uncontrollably for the cumulative impact of malicious bidding, which therefore overcomes the second challenge.

In summary, our contributions in this paper are as follows.

- We propose a *pricing game* to sketch the transaction pricing competition among users in blockchain, where the possibility of each transaction being included is defined to help depict the individual utility of each user.
- To achieve individual rationality with the maximized utility, we leverage *correlated equilibrium* to integrate it to the global optimal objective for securing the interests of all users, which comes into an optimization problem with exponential complexity in the number of transactions.
- To overcome the weakness on computational cost, we propose an approximate algorithm with divided optimum achieved parallelly for speeding up the calculation process, which is numerically evaluated to demonstrate its effectiveness and efficiency.

The rest of this paper is organized as follows. We investigate the most related work on blockchain transaction pricing in Section II. In Section III, we formulate the problem of transaction fee determination as a pricing game, where all users hope to maximize their individual utility. To achieve the goal, we take advantage of the correlated equilibrium to analyze the pricing game from a global perspective in Section IV, which is summarized as an optimization problem and approximately solved with higher efficiency in Section V. We evaluate our proposed solution in Section VI and conclude the whole paper in Section VII.

II. Related Work

Although paying transaction fees is not mandatory in most existing blockchian systems, a large number of studies have indicated that it plays a major role in the security of blockchain. In [8], a financial reasoning was conducted to demonstrate the unsustainability of blockchain with zero or infinitesimal transaction fees. Further, as a counterintuitive conclusion, Carlsten *et al.* [9] proved that whether rewards of miners are coming from blockchain system or transaction fees significantly affects the system security since there exists nearly no equilibrium with favorable security properties.

Besides, game theory is widely adopted to analyze the impact of transaction fees on blockchain. Correlating the issue with simple static partial equilibrium, Houy [11] analyzed that it is equivalent to keep a fixed transaction fee or let the decentralized market to determine the unit price with a fixed block size. Focusing on the owner-less characteristic of blockchain, Huberman *et al.* [12] provided closed form formulas on the relationship between the transaction fees and waiting times through formulating user behavior as a queuing game. Similarly, a queuing game with non-preemptive priority was employed in [13] to depict the dynamics in memory pool of blockchain with transactions flowing in and out, where five types of Nash equilibrium were found. In [14], Easley *et al.* constructed a game-theoretic model to analyze the evolution of transaction fees in Bitcoin from a market perspective.

With knowing the importance of transaction fees, more research work has been conducted to design various pricing schemes in recent. Most of the existing pricing mechanisms take advantage of auction to find the optimal price setting strategy, with a focus on maximizing the profit of miners. In [10], Lavi *et al.* figured out two challenges in Bitcoin related to the decreasing block reward and limited block size, based on which they analyzed the applicability of monopolistic auction in this scenario due to its immunity to untrusted auctioneers. In particular, all transactions included in a block pay the same lowest bid instead of the current pay-your-bid approach in Bitcoin, which can decouple the above two challenges. As a theoretical supplement to the monopolistic auction mechanism in [10], Yao [15] proved its approximate incentive-compatibility and further demonstrated its dominance compared to a traditional auction mechanism named Random Sampling Optimal Price auction (RSOP) [18]. Besides, Basu *et al.* [16] proposed a novel transaction pricing mechanism based on the generalized second price auction, which was demonstrated to be resistant to arbitrary manipulation as the derived bidding satisfied truthfulness.

In summary, the existing work related to transaction fees in blockchain have revealed its importance, most of which utilized game theory to conduct analysis; other closely related work on pricing mechanism design mainly relies on auctions, aiming at improving the efficiency and profit of miners. In contrast, our work leverages game theory to model the competitive and collaborative relationships among users considering the size and time sensitivity of each transaction, which can result in both global and individual optimum, thus maintaining a more sustainable and lively blockchain ecosystem.

III. Problem Formulation

In this paper, we consider the *mempool* of a blockchain system with all transactions from users, where the miners will select a set of transactions to be included in their individual block. Since there will be only one valid block at the end of each round of mining, we focus on the selection of transactions in this single block from a global perspective[2]. As the blockchain network prevails, increasingly large amount of transactions are generated, streaming into the mempool to be included in the valid block. However, the size of a block is limited, yielding the competition among transactions with respected to the transaction fees.

[2] Transactions included in different blocks owned by different miners might be heterogeneous due to the network transmission delay, which will be considered in our future work.

To describe this competitive system, we denote all transactions in the current mempool as $\{tx_1, tx_2, \cdots, tx_n\}$, where n is the total number of transactions from users. Each transaction has a specific size as s_i, which is fixed once the transaction is appearing in the mempool. The total size of all transactions included in one block cannot exceed the maximum limitation. Considering that transactions can have different time sensitivity, we assume that each transaction tx_i come with a time tag T_i indicating its remaining time to be included in a valid block; otherwise, the user launching this transaction will suffer from a big loss. In our paper, we aim to study how to design a pricing mechanism to provide unit price suggestions for all transactions in the current mempool considering both competitive prices provided by other transactions and their various emergency levels (i.e., time sensitivity).

Given a unit price v_i for tx_i with size s_i, the miner will get the payment of $v_i s_i$ for including tx_i in the valid block. In particular, we characterize the miner's behavior of including transactions in the valid block with a probabilistic model which is inspired by the *Discrete Choice Model* presented in [19]. Formally, we define the transaction inclusion probability as follows.

Definition III.1 (Transaction Inclusion Probability). *With the unit price vector from all transactions in the current mempool, denoted as* $\mathbf{v}$*, the probability of* tx_i *with unit price* v_i *being included in the valid block is*

$$p_i(\mathbf{v}) = \frac{\exp(a_i v_i - b)}{\sum_{j=1}^{n} \exp(a_j v_j - b)}, \tag{1}$$

where $a_i > 0$ *and* $b > 0$ *are parameters related to each* tx_i *and the block, respectively.*

The above definition based on discrete choice model can macroscopically describe the transaction inclusion event from both the perspectives of the miner (block) and the user (transaction). Generally, the probability of a transaction tx_i being included is positively proportional to its provided unit price v_i. In practical, the miner would be more willing to include those transactions with higher unit price as they can bring more profit for a length-limited block; and the transactions eager to be included are inclined to come with higher unit price to attract the miner's attention.

In addition, a_i and b in (1) can reflect the randomness during the process of including transactions in a block, which may come from both the transaction side and the block side. For example, since the size of the block is limited, the miner cannot always select the remaining highest unit price provider in the current mempool especially when the size of the block left cannot cover the length of this transaction with the highest unit price, which can be captured by the parameter a_i dependent on tx_i at this point, denoted by $a_i = \psi(s_i)$; similarly, other factors of the block, such as the generation location, can also impact the transaction inclusion results.

It is worth mentioning that the values of a_i and b could be obtained by querying the transaction and statistically calculating the historical block information.

With the definition of inclusion probability, we can calculate the payoff of the user, which is defined as individual utility in the following.

Definition III.2 (Individual Utility). *The expected individual utility of a user publishing* tx_i *with size* s_i *and unit price* p_i *can be calculated by*

$$U_i(\mathbf{v}) = p_i(\mathbf{v})\big(\phi(T_i) - v_i s_i\big), \tag{2}$$

where T_i *is the time tag of* tx_i *and* $\phi(\cdot)$ *is a non-decreasing function with* T_i*. In particular,* $\phi(\cdot)$ *can be defined as*

$$\phi(T_i) = \frac{\alpha_i}{1 + \exp(-\beta_i T_i)}, \tag{3}$$

where $\alpha_i, \beta_i > 0$ *are scalars for* tx_i*.*

In (2), the individual utility of a user is mainly dependent on two parts, i.e., the profit of the transaction being successfully included before its deadline and the total cost that the user needs to pay for the transaction. The cost part is obvious to be the unit price multiplying the size of the transaction. For the profit part defined in (3), we consider that, generally, the sooner the transaction gets included, the higher profit the user can gain, so the increasing remaining time to be included for a transaction can bring more profit for this user; while this sort of advantage of time length left cannot last forever, which is reflected in the upper limitation of $\phi(T_i)$ as α_i. In addition, the increasing speed of $\phi(T_i)$ with respect to T_i is unique for each transaction tx_i, decided by β_i.

Note that since the range of $\phi(T_i)$ is $[\frac{\alpha_i}{2}, \alpha_i]$, we assume that $\alpha_i \geq 2 v_i s_i$ to guarantee the individual utility defined in (2) is non-negative.

According to the above definition, it can be seen that the individual utility of each transaction is not only related to its own posted unit price but also the unit prices provided by other transactions in the current mempool. In order to depict this interdependent relationship among all transactions, we take advantage of the non-cooperation game to further model this problem as a *Pricing Game*.

Definition III.3 (Pricing Game). *All users with transactions*[3] *in the current mempool form a pricing game where any user with* tx_i *is a game player, exerting the strategy to provide a unit price* v_i *and getting the payoff of the individual utility* $U_i(\mathbf{v})$*.*

As the individual utility of any user is collectively decided by all the unit prices, we can specifically express it as $U_i(v_i, \mathbf{v}_{-i})$ where $\mathbf{v}_{-i} = (v_1, \cdots, v_{i-1}, v_{i+1}, \cdots, v_n)$ denotes the unit prices provided by other users for their transactions $\{tx_1, \cdots, tx_{i-1}, tx_{i+1}, \cdots, tx_n\}$. As a rational and utility-driven player, any user wants to maximize the individual utility $U_i(v_i, \mathbf{v}_{-i})$. However, it is not feasible for any user to achieve this goal without knowing the offers from others. Therefore, in this paper, we start from a global

[3] Here we consider each user only has one transaction. For a user with multiple transactions, we treat each transaction individually, regarding there is a corresponding user behind each one.

perspective to help all users make the decision on how to provide reasonable unit prices to their transactions to get them included in the valid block before the deadline and achieve maximum payoffs as well.

IV. Game Theoretic Solution

In the previous section, we propose the pricing game to characterize the unit price decision problem of transactions among all users, which leaves the individual utility maximization as a challenge. In this section, we first derive it as a correlated equilibrium, and then analyze this problem from a macro perspective to achieve the global optimum for all users, followed by the final solution.

Without loss of generality, we assume that the strategy space of users is discrete, denoted by $\mathcal{V}$, and with the size of V. According to the individual utility maximization requirement of each user, we can get the correlated equilibrium of the pricing game as follows.

Definition IV.1 (Correlated Equilibrium)**.** *For our proposed pricing game, there exists a correlated equilibrium $F(\mathbf{v})$, which is a unique probability distribution over the space $\mathcal{V}^n$ denoting all possible combinations of unit prices provided by all users, if and only if for any user with the strategy $v_i \in \mathcal{V}$, it satisfies*

$$\sum_{\mathbf{v}_{-i} \in \mathcal{V}^{n-1}} F(v_i, \mathbf{v}_{-i}) \Big(U_i(v_i, \mathbf{v}_{-i}) - U_i(v_i', \mathbf{v}_{-i}) \Big) \geq 0, \quad (4)$$

where $v_i' \in \mathcal{V}$ is any strategy other than v_i.

According to the above definition, one can see that under the correlated equilibrium $F(\mathbf{v})$, any user has no motivation to deviate from the current strategy v_i when others are fixed to $\mathbf{v}_{-i}$. In other words, any user can thus maximize the individual utility as long as each user sets v_i according to $\mathbf{v}$ sampled from $F(\mathbf{v})$. Since $F(\mathbf{v})$ is a probability distribution, we have the constraints $F(\mathbf{v}) \geq 0$ and $\sum_{\mathbf{v} \in \mathcal{V}^n} F(\mathbf{v}) = 1$. Combined with the above inequality (4), it is easy to calculate a correlated equilibrium through solving a linear programming problem, which could generate a set of results as multiple correlated equilibria. In order to find the best one, we introduce the following global objective of social welfare for the pricing game.

Definition IV.2 (Social Welfare)**.** *For a specific correlated equilibrium of the pricing game $F(\mathbf{v})$, the social welfare is defined as the expected total utilities of all users, i.e., $\sum_{\mathbf{v} \in \mathcal{V}^n} F(\mathbf{v}) \sum_{i=1}^{n} U_i(\mathbf{v})$.*

Therefore, to derive the best pricing strategy for each user, we can solve the best correlated equilibrium for the pricing game from a global perspective, which can be summarized into the following optimization problem.

$$\max : \sum_{\mathbf{v} \in \mathcal{V}^n} F(\mathbf{v}) \sum_{i=1}^{n} U_i(\mathbf{v}) \quad (5)$$

$$\text{s.t.} : F(\mathbf{v}) \geq 0, \quad (6)$$

$$\sum_{\mathbf{v} \in \mathcal{V}^n} F(\mathbf{v}) = 1, \quad (7)$$

$$\sum_{\mathbf{v}_{-i} \in \mathcal{V}^{n-1}} F(v_i, \mathbf{v}_{-i}) \Big(U_i(v_i, \mathbf{v}_{-i}) - U_i(v_i', \mathbf{v}_{-i}) \Big) \geq 0, \quad \forall v_i, v_i' \in \mathcal{V}. \quad (8)$$

For simplicity, we refer this optimization problem as *social welfare maximization problem* as the objective function in (5) is to maximize the social welfare of the pricing game. It is worth mentioning that the first two constraints (6) and (7) are coming from the definition of probability distribution, and the last constraint (8) is to guarantee the individual utility maximization presented in Definition IV.1. As mentioned above, this optimization problem is exactly a linear programming problem, where the variable is the probability distribution over all possible combinations of unit prices, i.e., $F(\mathbf{v})$. Thus we can employ existing algorithms to solve it in an efficient manner, such as dual-simplex and interior-point, which will cost polynomial time in the numbers of variables and constraints. However, it is not realistic to directly adopt the existing algorpaithms to solve our aforementioned optimization problem because the computational cost in our case is non-polynomial, which can be demonstrated by the following Theorem.

Theorem IV.1. *Directly using the existing algorithms to solve the social welfare maximization problem has computational cost exponentially increasing with the number of transactions n.*

Proof. Given the number of transactions n and the size of strategy space V, the number of variables in the social welfare maximization problem, i.e., $F(\mathbf{v}), \mathbf{v} \in \mathcal{V}^n$, is V^n since the probability distribution is over all possible combinations of unit prices. For the number of constraints, it is clear that (7) is a single constraint, while constraint (6) is held for every variable $F(\mathbf{v})$, so its total number is also V^n; and the number of constraints according to (8) is nV. Therefore, both the numbers of variables and constraints are $O(V^n)$.

In this case, even though the computational cost of the existing algorithms for solving the linear programming problem is polynomial time in the numbers of variables and constraints, directly applying them on our social welfare maximization problem will lead to exponential computational complexity in the number of transactions because the numbers of variables and constraints are exponentially increasing with n as mentioned above. □

As shown in the above Theorem, as the increase of the number of transactions n, the number of variables will increase significantly, offsetting the efficiency of employing existing algorithms with polynomial computational complexity. To overcome this challenge, we propose an approximate algorithm to maximize the social welfare of the pricing game based on the existing linear programming algorithms, which is introduced in the following section.

V. An Approximate Algorithm

To decrease the computational cost of directly employing classical linear programming algorithms for solving our problem, we need to eliminate the impact of exponential relationship between the numbers of variables and constraints and the number of transactions. In this section, we achieve this goal through proposing an approximate algorithm which controls the exponentially increasing numbers of variables and constraints to an acceptable level.

In general, our main idea is to divide all the current transactions into small sets where the social welfare is maximized locally in a smaller pricing game to approximate the global optimization objective. Considering that transactions coming with the same time tag will compete with each other more severely as they have the same remaining time to be included in the valid block, we divide all transactions in the current mempool into τ sets, where τ is the number of different time tags of transactions. By this means, the original social welfare maximization problem in (5)-(8) can be divided into τ sub-problems achieving local social welfare maximization for transactions with the same time tag, where the number of transactions in each sub-problem is defined as n_t depending on the time tag. Formally, we can express the t-th sub-problem as follows,

$$\max: \sum_{\mathbf{v}_t \in \mathcal{V}^{n_t}} F_t(\mathbf{v}_t) \sum_{i=1}^{n_t} U_{t,i}(\mathbf{v}_t) \tag{9}$$

$$\text{s.t.}: F_t(\mathbf{v}_t) \geq 0, \tag{10}$$

$$\sum_{\mathbf{v}_t \in \mathcal{V}^{n_t}} F_t(\mathbf{v}_t) = 1, \tag{11}$$

$$\sum_{\mathbf{v}_{t,-i} \in \mathcal{V}^{n_t-1}} F_t(v_{t,i}, \mathbf{v}_{t,-i}) \Big(U_{t,i}(v_{t,i}, \mathbf{v}_{t,-i}) - U_{t,i}(v'_{t,i}, \mathbf{v}_{t,-i}) \Big) \geq 0, \forall v_{t,i}, v'_{t,i} \in \mathcal{V}, \tag{12}$$

where $\mathbf{v}_t$ is the unit price vector of n_t transactions; $F_t(\mathbf{v}_t)$ is a correlated equilibrium of the small pricing game among them; $U_{t,i}$ and $v_{t,i}$ are respectively the utility and unit price of the i-th transaction while $\mathbf{v}_{t,-i}$ is the unit price vector except $v_{t,i}$.

Obviously, the above sub-problem has the same components as the original one, which will output the best correlated equilibrium $F_t(\mathbf{v}_t)$ for maximizing the local social welfare in each small set of transactions. Thus, after solving all sub-problems with the existing linear programming algorithms, we can derive an approximate solution through combining all the solutions of sub-problems, which means $F(\mathbf{v}) = (F_1(\mathbf{v}_1), F_2(\mathbf{v}_2), \cdots, F_\tau(\mathbf{v}_\tau))$. By this means, the computational cost of solving the social welfare maximization problem come into an acceptable level, which is demonstrated in the following theorem.

Theorem V.1. *Assuming that the number of transactions with the same time tag has a maximum limitation as $\bar{n}$, which is much less than n since the time tags of transactions could be much diverse; and that the number of different time tags τ is polynomially increasing with n. Then our proposed approximate solution can solve the social welfare maximization problem in polynomial time.*

Proof. Using the existing algorithms, we can solve the above sub-problem with the computational cost of $O(V^{n_t})$ according to Theorem IV.1. As we assume that $n_t \leq \bar{n} \ll n$, we have $O(V^{n_t}) \leq O(V^{\bar{n}})$ where the latter item can be regarded as constant with respect to n. In addition, since τ increases with n in a polynomial manner, the overall computational cost of our proposed approximate solution is $\tau O(V^{\bar{n}})$ which is polynomial in n. □

VI. Experimental Evaluation

In this section, we evaluate our proposed pricing mechanism through simulation experiments. We implement our experiments using MATLAB R2019a in Windows 10 running on Intel i7 processor with 16 GB RAM and 512 GB SSD. For parameters related to transactions, we randomly choose $s_i \in [100, 300]$ KB and $T_i \in [10, 30]$ min. Other parameters are set as $n = 500$, $\alpha_i = 3000$, $\beta_i = 0.01$, $a_i = \frac{s_i}{100}$, $\tau = 200$, and $n_t \in \{1, 2, 3\}$ unless otherwise specified. Note that all our experiments are repeated 20 times to have the average results.

A. Numerical Comparison

In order to demonstrate that our proposed approximate solution in Section V can bring similar results for the optimization problem in a more efficient manner, we compare the experimental results returned by traditional solution with the interior-point method and our proposed one. In detail, we set the number of transactions $n \in \{5, 6, \cdots, 16\}$ and run both the traditional and approximate algorithms to obtain the computational efficiency and the results of optimization problem, i.e., maximized social welfare and the unit price vector with the highest probability as the correlated equilibrium.

As shown in Fig. 1, the computational cost of the traditional algorithm solving the linear programming problem increases exponentially with the number of transactions n, while that of our proposed approximate solution is linearly changing with n, which is consistent with the analysis results presented in Theorems IV.1 and V.1. Besides, we present the optimization results in Tables I and II, where only the results of $n = 5$ to 8 are reported to avoid redundancy and the results in other cases have the similar trend. As can be seen from Table I, even though our proposed approximate solution cannot obtain the exact same maximized social welfare compared to the traditional one with the accurate constraints, we can have approximate values fluctuating around the accurate ones with lower computational cost in the long run. Since the optimal correlated equilibrium for social welfare maximization is a

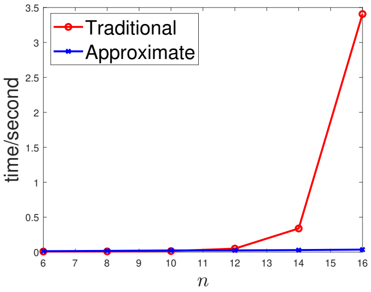

Fig. 1. Computational cost comparison changing with n.

TABLE I
MAXIMIZED SOCIAL WELFARE.

Solution	n=5	n=6	n=7	n=8
Traditional	709.25	1293.53	876.43	712.17
Approximate	713.57	1284.19	916.59	692.05

probability distribution over all possible combinations of unit price vector, we regard that the combination with the highest probability is the most appropriate one, which is presented in Table II. One can see that all cases we examined come with the same results.

From the above analysis on our numerical comparison results, we can have the conclusion that our proposed approximate solution can solve the social welfare maximization problem efficiently and obtain similar results to the traditional one.

B. Performance Evaluation

In this subsection, we evaluate the performance of our proposed approximate solution with respect to the maximized social welfare when $n = 500$ under different parameter settings of a_i, α_i, β_i, and τ.

To begin with, we examine the impact of transaction inclusion probability defined in Definition III.1 on the maximized social welfare, especially the impact of a_i. As mentioned in Section III, here we assume that a_i is a function of s_i, i.e., the size of tx_i, which is set as $a_i = \psi(s_i) = \frac{si}{X}$ with $X = s_i/a_i$ being a parameter changing from 100 to 1000 with an interval of 100. As shown in Fig. 2, we can obtain that the maximized social welfare changes with s_i/a_i in a relatively complicated manner which seems like a combination of the exponential and stable trend. This is reasonable since (1) indicates that the relationship between probability and a_i is exponent divided by the sum of exponents, which could present this sort of complicated curve and further affect the social welfare through the individual utility as defined in (2). It is worth noting that the impact of b has also been checked but brings subtle influence on the maximized social welfare, which is because this parameter is block-related with an equivalent impact on all users, thus finally resulting in an offsetting of its impact.

TABLE II
UNIT PRICE VECTOR WITH THE HIGHEST PROBABILITY.

Solution	Traditional	Approximate
n=5	(10, 5, 10, 10, 10)	(10, 5, 10, 10, 10)
n=6	(10, 5, 5, 10, 10, 5)	(10, 5, 5, 10, 10, 5)
n=7	(10, 10, 5, 10, 5, 5, 10)	(10, 10, 5, 10, 5, 5, 10)
n=8	(10, 5, 5, 5, 10, 10, 5, 10)	(10, 5, 5, 5, 10, 10, 5, 10)

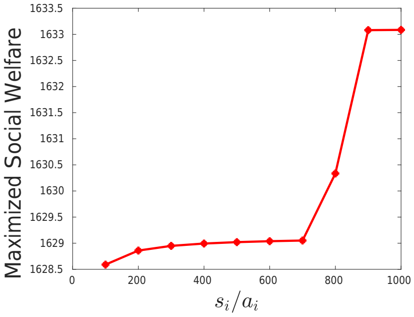

Fig. 2. Maximized social welfare changing with s_i/a_i.

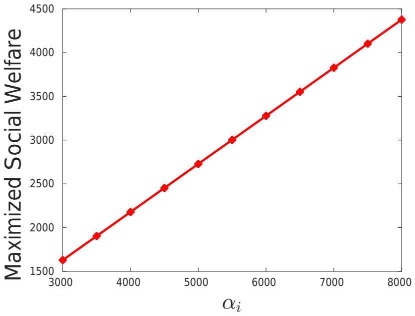

Fig. 3. Maximized social welfare changing with α_i.

Next, we explore the impact of individual utility on the maximized social welfare. In particular, we inspect the influences of α_i and $beta_i$ and report the corresponding experimental results in Figs. 3 and 4, respectively.

For α_i, we change it from 3000 to 8000 with an interval of 500. As can be seen from Fig. 3, the maximized social welfare increases linearly with α_i. This is because individual utility in Definition III.2 is linearly related to α_i when other parameters are fixed. Thus, the maximized social welfare denoting the total utilities of all users has a linear relationship with α_i.

And for β_i, we set it as 0.01 to 0.1 with an interval of 0.01. According to Fig. 4, one can see that the maximized social welfare increases with β_i in a non-linear manner. In fact, it is a part of the "S"-shape curve. As shown in definition III.2, we define that the individual utility is linear to the profit function $\phi(\cdot)$ which is a sigmoid function with respect to β_i as shown in (3). So the maximized social welfare also presents this trend with β_i.

From the above two figures, we can get the conclusion that the maximized social welfare will be affected by α_i and β_i in a similar way that the individual utility U_i gets influenced.

Finally, we study whether changing the number of transactions in subsets will affect the optimization result or not. To be specific, we achieve this by adjusting the number of

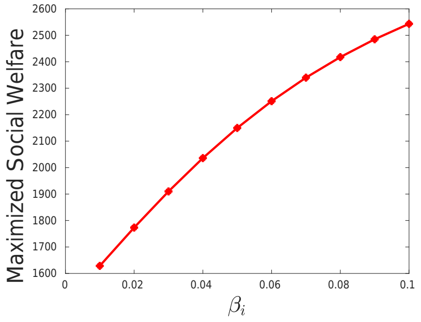

Fig. 4. Maximized social welfare changing with β_i.

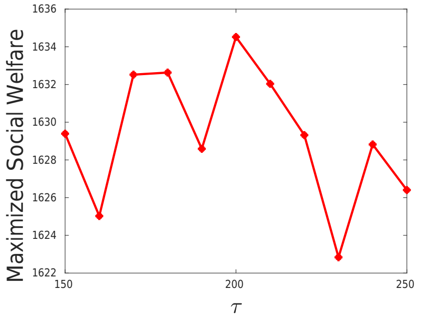

Fig. 5. Maximized social welfare changing with τ.

different T_i of transactions, i.e., τ. As presented in Fig. 5, the maximized social welfare has no obvious changing trend with respect to τ, which helps demonstrate the stability and robustness of our proposed approximate solution.

VII. Conclusion

In this paper, we study the transaction pricing issue in blockchain with the help of game theory from the perspective of users and propose a correlated equilibrium based pricing mechanism for transactions. To be specific, we first model the transaction inclusion competition among users as a pricing game, and then utilize the concept of correlated equilibrium to maximize the individual utility of each user through unifying it with achieving the global optimum. To overcome the weakness of exponential complexity in the original solution, we propose an approximate algorithm to yield polynomial time cost. Finally, we conduct extensive simulations to evaluate our proposed mechanism.

References

[1] Muhammad El-Hindi, Carsten Binnig, Arvind Arasu, Donald Kossmann, and Ravi Ramamurthy. Blockchaindb: a shared database on blockchains. *Proceedings of the VLDB Endowment*, 12(11):1597–1609, 2019.

[2] Huan Zhou, Xue Ouyang, Zhijie Ren, Jinshu Su, Cees de Laat, and Zhiming Zhao. A blockchain based witness model for trustworthy cloud service level agreement enforcement. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pages 1567–1575. IEEE, 2019.

[3] Wenlong Ni, Yuhong Zhang, and Wei Li. Optimal admission control for secondary users using blockchain technology in cognitive radio networks. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pages 1518–1526. IEEE, 2019.

[4] Junqin Huang, Linghe Kong, Guihai Chen, Long Cheng, Kaishun Wu, and Xue Liu. B-iot: Blockchain driven internet of things with credit-based consensus mechanism. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pages 1348–1357. IEEE, 2019.

[5] Chunchi Liu, Yinhao Xiao, Vishesh Javangula, Qin Hu, Shengling Wang, and Xiuzhen Cheng. Normachain: A blockchain-based normalized autonomous transaction settlement system for iot-based e-commerce. *IEEE Internet of Things Journal*, 2018.

[6] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[7] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

[8] Kerem Kaskaloglu. Near zero bitcoin transaction fees cannot last forever. 2014.

[9] Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. On the instability of bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 154–167. ACM, 2016.

[10] Ron Lavi, Or Sattath, and Aviv Zohar. Redesigning bitcoin's fee market. In *The World Wide Web Conference*, pages 2950–2956. ACM, 2019.

[11] Nicolas Houy. The economics of bitcoin transaction fees. *GATE WP*, 1407, 2014.

[12] Gur Huberman, Jacob Leshno, and Ciamac C Moallemi. An economic analysis of the bitcoin payment system. *Columbia Business School Research Paper*, (17-92), 2019.

[13] Juanjuan Li, Yong Yuan, Shuai Wang, and Fei-Yue Wang. Transaction queuing game in bitcoin blockchain. In *2018 IEEE Intelligent Vehicles Symposium (IV)*, pages 114–119. IEEE, 2018.

[14] David Easley, Maureen O'Hara, and Soumya Basu. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, 2019.

[15] Andrew Chi-Chih Yao. An incentive analysis of some bitcoin fee design. *arXiv preprint arXiv:1811.02351*, 2018.

[16] Soumya Basu, David Easley, Maureen O'Hara, and Emin Sirer. Towards a functional fee market for cryptocurrencies. *Available at SSRN 3318327*, 2019.

[17] Haiming Jin, Hongpeng Guo, Lu Su, Klara Nahrstedt, and Xinbing Wang. Dynamic task pricing in multi-requester mobile crowd sensing with markov correlated equilibrium. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pages 1063–1071. IEEE, 2019.

[18] Andrew V Goldberg, Jason D Hartline, Anna R Karlin, Michael Saks, and Andrew Wright. Competitive auctions. *Games and Economic Behavior*, 55(2):242–269, 2006.

[19] Yihan Gao and Aditya Parameswaran. Finish them!: Pricing algorithms for human computation. *Proceedings of the VLDB Endowment*, 7(14):1965–1976, 2014.