A Novel GSP Auction Mechanism for Dynamic Confirmation Games on Bitcoin Transactions

Juanjuan Li, *Member, IEEE*, Xiaochun Ni, Yong Yuan, *Senior Member, IEEE*, and Fei-Yue Wang, *Fellow, IEEE*

Abstract—Bitcoin is gaining ground in recent years. In the Bitcoin system, miners provide computing power to confirm transactions in pursuit of transaction fees, while users compete by bidding transaction fees for faster confirmation. This process is in essence analogous to online ad auctions, where advertisers bid for more prominent ad slots. Therefore, inspired by ad auction research, we propose to apply the Generalized Second Price (GSP) auction mechanism in the dynamic confirmation game on Bitcoin transactions. Our model is targeted to deal with the problems caused by instability and low efficiency in the currently-adopted Generalized First Price (GFP) auction model in Bitcoin confirmation games. Besides, we use the "rank-by-cost" rule to replace the "rank-by-fee" rule, where each transaction's cost is calculated by the user-submitted fee and the waiting time. Aiming to probe users' equilibrium strategy, we first discuss the GSP game with complete information under synchronous submissions, and show that it has the Locally Envy-Free equilibrium. Then, we study the GSP game with incomplete information under asynchronous submissions, and define two types of strategies, i.e., the Farsighted Balanced (FB) strategy and the Instant Balanced (IB) strategy. The FB strategy is in line with users' practical needs of determining fees so as to maximize the long-term payoffs; however it cannot generate a stable equilibrium. Alternatively, the IB strategy focuses on the instant payoff maximization, and if all users follow the IB strategy, their equilibrium fees can finally converge to a stable profile. Finally, we design computational experiments to validate our theoretical models and analysis. Our research findings indicate that this novel GSP mechanism is superior to the currently adopted GFP mechanism. Besides, the convergence of the GSP game under the IB strategy has also been illustrated by the computational experiments.

Index Terms—Blockchain, bitcoin transaction confirmation game, generalized second price mechanism, transaction fee

1 Introduction

Owing to the desirable features of peer-to-peer decentralization, trustlessness, tamper-resistance, anonymity and auditability [1], [2], [3], blockchain technology has attracted intensive research interests and witnessed phenomenal development in recent years [4], [5]. The most well-known blockchain system is Bitcoin, which generates an online economy of multi-billions of dollars [6], [7], [8]. Bitcoin uses the Nakamoto consensus protocol to secure and update its underlying ledger of linked blocks [9]. Typically, new blocks are created via miners repeatedly solving puzzles, that is, to find a specific random number utilizing a brute force approach. This process is called mining [10]. The miner (individual or group) winning the mining competition has the right to confirm transactions packaged by him/her and record them into the new block. Then, the block will be appended to the main chain of previously agreed blocks, and the miner will get paid the block reward (i.e., 12.5 bitcoins currently) and transaction fees [11], [12]. In this process, transaction fees play the key role as the economic incentive to stimulate miners contributing their computing power to mine blocks and confirm transactions [13], [14]. As a result, revenue-maximizing miners will preferentially confirm those transactions with higher fees [3], forcing users to increase their transaction fees for faster confirmation, or otherwise queue and wait for a longer time. Since both the Bitcoin block generation rate and the block size are limited, the transaction confirmation rate is also restricted, which causes fierce competitions among users and in turn high required fees, especially in case of transaction surge.

Therefore, there is a critical need in the individual-level for users to optimize their transaction fees, and also in the system-level for Bitcoin blockchain to improve its transaction fee auction mechanism, with the aim of reducing the inflating transaction fees and enhancing the system efficiency. However, the unique features of Bitcoin transaction confirmation game make the Bitcoin transaction fee management very challenging. Different from the traditional dynamic game, currently Bitcoin fees should be decided by users simultaneously with their transaction submissions, to compete for the perishable block space rather than storable objects. Once fees are determined, it is typically impossible for users to make the real-time adjustment. However, the unconfirmed transactions will continue to participate in the following games for each block until they are confirmed finally. This setting endowers the blockchain-powered Bitcoin transaction confirmation game with the unique characteristics of "dynamic environment coupled with static strategies". As such, users are required to be farsighted when determining the optimal fees to maximize the long-term payoffs gained over multiple rounds of games.

• *The authors are with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China, and also with the Qingdao Academy of Intelligent Industries, Qingdao 266109, China. E-mail: {juanjuan.li, xiaochun.ni, yong.yuan, feiyue.wang}@ia.ac.cn.*

Manuscript received 18 July 2019; revised 22 Apr. 2020; accepted 11 May 2020. Date of publication 14 May 2020; date of current version 15 June 2022. (Corresponding author: Yong Yuan.)
Digital Object Identifier no. 10.1109/TSC.2020.2994582

Currently, a large majority of Bitcoin transactions are processed in a pipeline with the ranking rule defined by the "rank-by-fee" mechanism and the pricing rule defined by the "pay-at-bid" mechanism, which is known as "Generalized First Price (GFP)" auction [15], [16], [17]. That is: transactions with higher fees will be confirmed first and users need to pay their submitted fees to miners.

From the perspective of users, the simple rule of GFP mechanism will lead users to pay unnecessarily high fees to maintain a desirable rank of their transactions. Generally, the higher is the required transaction fee, the longer a transaction could reside in the memory pool before being considered dormant [18]. In particular, when the memory pool encounters transaction congestions, users need to pay extra high fees for faster confirmation [19], which will partially weaken the enthusiasm of users to submit fees [20]. Transaction fees usually account for only a small percentage of the bitcoins transferred by transactions; however, it is possible that transaction fees might reach or even exceed the trading bitcoins, especially in micro-payment scenarios [21]. For this consideration, the exorbitant transaction fees resulting from the GFP mechanism will lead to transaction fee inflation and thus harm users' experience [22], [23].

From the perspective of miners, the unstable fee generated by the GFP mechanism cannot guarantee reliable incentives for them to keep mining as well as confirming transactions. The GFP mechanism has been proven to be unstable in dynamic scenarios, because it encourages inefficient investments in gaming the system [24]. Under certain conditions, users will be engaging in cyclical fee adjustments, and equilibrium fees may follow a cyclical pattern with price-escalating phases interrupted by price-collapsing phases [25]. As such, it generates volatile prices that in turn cause allocative inefficiencies. In general, the Bitcoin system should have simple, practical fee mechanism designs to encourage miners to provide suitable security guarantees against cheating [16]. However, the current Bitcoin fee market has failed to yield stable revenues for miners, because the current fee mechanism cannot keep users' rational behaviors aligned with the goal of paying enough fees (i.e., buying enough security) for the entire system [17] and lead to the absence of strategy equilibrium of the GFP mechanism [15].

The market practice in the Bitcoin system has also proven the existence of the above-mentioned problems resulting from the GFP mechanism. First, the GFP mechanism causes Bitcoin users to pay unnecessarily high fees for faster confirmation. For example, in December 2017, the Bitcoin memory pool was stuffed with over 180,000 transactions, which leads to severe transaction congestion. Under that situation, users even need to wait for several days to get their transaction confirmed, and the transaction fee of a typical transaction even costed up to 20 dollars.[1] Besides, the empirical analysis shows that transaction fees collected by each block are distinctly different and the daily transaction fees also have great variance, which causes high volatility of miners' revenues.

To conclude, the GFP mechanism fails to be a well-applicable auction mechanism for the Bitcoin transaction confirmation game. In this paper, we are motivated to deal with the above-mentioned problems resulting from the currently adopted auction mechanism in the Bitcoin system, and propose a mechanism that incentivizes the non-strategic behaviors of users as well as guarantee the allocation efficiency of the Bitcoin system.

Existing online ad auction practices, especially the sponsor search auctions (SSA), have provided us with good reference models. In the SSA market, advertisers bid for more prominent ad slots, which is essentially similar to the Bitcoin transaction fee auction process. The GFP mechanism was the original design for SSA since 1998, but has been replaced by the Generalized Second Price (GSP) mechanism due to the obvious shortcomings revealed by the market practice, which is introduced by Google in 2002. Each year, Google earns over 90 percent of the revenues from the keyword auctions on the GSP basis. Nowadays, almost all the online ad auctions, including SSA, real-time bidding and header bidding, etc., adopt the GSP mechanism, and it has created a considerably large global market of more than 110 billion dollars in 2019. [2] The GSP mechanism has been proved to be much more user-friendly and less susceptible to gaming, and thus is more stable and has higher allocative efficiency [24], [26], [27]. Inspired by the evolvement of the SSA market from the GFP mechanism to the GSP mechanism, we propose to apply the GSP mechanism in the Bitcoin system. Actually, it can be tailored to the unique characteristics of the Bitcoin transaction fee auction. GSP insists that users offer a single fee for each transaction; consequently, even though users participate in the multi-objective game, their valuations can be properly represented by one-dimensional types [24]. Different from online ad auctions, one fee per transaction can be sufficiently expressive to fully convey users' preferences, because they need to independently determine the transaction fee for each transaction.

In early stages of Bitcoin, 50 KB out of 1 MB in each block was reserved for the priority transactions without fees, and these priority transactions' ranks are mainly determined by the waiting time.[3] That means the transaction confirmation are conducted in two separate pipelines, where one pipeline is for transactions with fees, and the other pipeline is for priority transactions without fees. However, with the average transaction size growing, the reserved 50 KB turns out to be insufficient to deal with the confirmation of those priority transactions. Besides, since Bitcoin Core v0.12 is launched, the priority rule is no longer performed by default.[4] Then, some of priority transactions deviate to submit fees aiming to compete for better rank in the fee pipeline. If we keep the ranking rule in the fee pipeline regulated uniformly by transaction fees, on the one hand, the priority rule will not work any more, which is not in favor of the priority transactions' benefits; on the other hand, transactions originally with associated fees are faced with more fierce competition, which will lead to those with low fees be ranked lower and thus experience longer delay. Therefore, we consider to deal with these two kinds of transactions through one uniform pipeline, and propose a new ranking mechanism incorporating both transaction fees and the waiting time.

1. According to data released by blockchain.info

2. According to data released by Interactive Advertising Bureau

3. http://en.bitcoin.it/wiki/Transaction fees/

4. https://bitcoin.org/en/release/v0.12.0

Since studying the equilibria of a novel mechanism is often necessary and meaningful, we also try to study fee-determining strategies adopted by users aiming to maximize their payoffs in the GSP auction. We model the Bitcoin transaction confirmation game as the multi-round game, explicitly considering the dynamic nature of the game environment. Our analysis begins with the case of synchronous submissions, then we connect it to the single-round static game described by Edelman *et al.* [24], and prove the existence of Locally Envy-Free equilibrium under the setting of complete information. Further, we proceed to discuss the case of asynchronous submissions, and show that if all users follow the newly-defined Instant Balanced Strategy, the game will eventually converge to a fixed equilibrium fee profile.

To summarize, our major contributions in this paper are to propose a novel GSP mechanism for Bitcoin transaction fee auctions, where transactions are ranked by costs instead of submitted fees; and also to study its equilibrium strategy. The remainder of this paper is organized as follows. Section 2 briefly reviews the related literature. Section 3 establishes the basic GSP auction model for the transaction confirmation game. Then, we discuss users' equilibrium fee strategies under synchronous submissions in Section 4 and asynchronous submissions in Section 5, respectively. Section 6 conducts computational experiments to validate our theoretical models and analysis. Section 7 summarizes this paper and discusses the future work.

2 Literature Review

Currently, the research efforts devoted to understanding the transaction fee auction in the Bitcoin system are still quite limited. In view that the fixed transaction fee is equivalent to setting a maximum block size instead [28], the auction-based mechanism could be a better choice. Lavi *et al.* [17] argued that Bitcoin's current fee market does not extract revenue well for miners when blocks are not congested. Also, according to Houy [28], if transaction fees are totally determined by a decentralized market and the maximum block size is not constrained, transaction fees will eventually go to zero and miners will not have sufficient incentives to keep mining, and hence to keep Bitcoin viable. Huberman *et al.* [11] analyzed the implied congestion queueing game, calculated each user's trade-off between transaction fees and delay costs, and concluded that each user's equilibrium transaction fee equals the externality imposed by his/her transaction. Thus, equilibrium transaction fees coincide with the payments that result from selling the priority of service in a VCG (Vickrey-Clarke-Groves) auction.

For the fee mechanism design in the Bitcoin transaction confirmation game, there are only limited studies. Lavi *et al.* [17] proposed two alternative auction mechanisms: the monopolistic price mechanism, and the random sampling optimal price mechanism. They proved that the monopolistic price mechanism extracts revenue better from users. Yao [16] further proved that the monopolistic price mechanism is nearly incentive compatible for any independently identically distribution as the number of users grows large. Basu *et al.* [15] proposed an alternative fee setting mechanism, and proved that it is free from manipulation as the number of users increases. However, they ignored the dynamic feature of the Bitcoin fee auctions. Our previous work on the GSP auction mechanism in the static full-information Bitcoin transaction confirmation game has proven that it is superior to the currently adopted GFP mechanism in formulating stable fee level and improving transaction confirmation efficiency [29].

In theoretical researches, multiple advantages of the GSP mechanism have already been confirmed and documented. Conceived as a natural extension of the Vickrey-Clarke-Groves (VCG) auction, GSP allows bidders to pay at the minimum price that can maintain the current rank [30], and it is simple and works reasonably well [24]. Moreover, the GSP mechanism is much more user-friendly and less susceptible to gaming compared to the GFP mechanism, and thus is more stable and has higher allocative efficiency [24], [26], [31], [32]. It is well known that user's valuation on each transaction is very critical in the transaction fee auction. However, GSP is not incentive-compatible, and it has no guarantee that users submit their true valuations. As such, under the GSP mechanism, users are forced to undertake the complicated task of choosing a fee strategy. The first economic analysis of GSP is formulated by Edelman *et al.* [24] and Varian [33], and they proposed the Locally Envy-Free Equilibrium and the Symmetric Nash Equilibrium for the GSP auction with complete information, respectively. In both equilibria, the bidder's position and payment are equal to those in the dominant-strategy equilibrium of VCG auctions, respectively. VCG is a more theoretically effective mechanism encouraging bidders to bid on their true valuations. However, it is very hard to apply the VCG mechanism into the practice due to its high computing complexity, especially for the multi-object auction scenarios [34]. As such, GSP surpasses VCG to become the mainstream auction mechanism in practice.

Considering the good applicability of the GSP auction model to the Bitcoin transaction confirmation game, as well as its advantages proven in both the theoretical research and the online auction practice, we believe that employing the GSP auction model to replace the currently adopted GFP auction model is a timely and meaningful research innovation for the Bitcoin system. In the following sections, we will establish the GSP model for Bitcoin transaction fee auctions, and also analyze users' equilibrium decisions on transaction fees.

3 The Basic Model

Typically, the basic process of the transaction confirmation game in the Bitcoin system is described by Fig. 1. At the beginning of each round, new transactions pending for confirmation with associated fees are submitted simultaneously by users, and they will enter the memory pool. Then, miners rank them according to the predetermined rule, and those ranked at top positions will be confirmed and recorded into the new block. Correspondingly, the confirmed transactions should transfer a certain amount of fees to miners. Meanwhile, those transactions failing to be confirmed will stay in the memory pool and continue to participate in the next round of game.

We begin with establishing the basic GSP auction model for the Bitcoin transaction confirmation game. Notations of this paper are listed in Table 1.

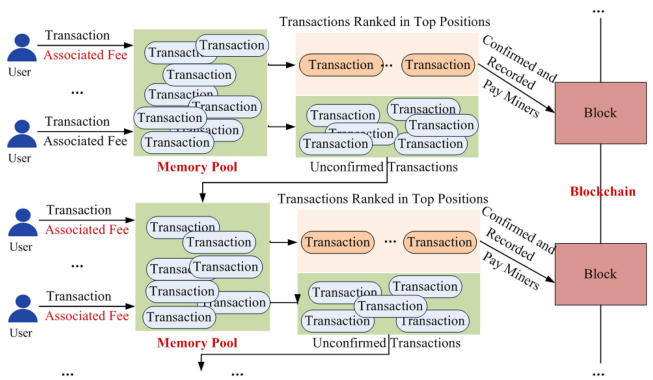


Fig. 1. The basic process of the transaction confirmation game.

Suppose there are n risk-neutral users participating in the dynamic game. The dynamic games are conducted multiple rounds at a fixed time interval following the block generation rate. We consider these games adopting the GSP mechanism. Suppose each user only submits one transaction at each round. For the transaction $i(\underline{t})$ submitted by the user i in the round $\underline{t}$, it is usually accompanied by a fee b_i, aiming to win a desired position in the block with the expectation to get the transaction confirmed. Suppose the valuation of the transaction is v_i. For simplicity, we assume that all transactions have the same fixed size. Accordingly, the number of positions in one block per round is exogenously determined as x.

We propose to rank the unconfirmed transactions with the cost $\tilde{b}_i$, which is calculated by their associated fees and the waiting time. Here, the time cost is incorporated to compensate users waiting until their transactions are confirmed. Due to the rule of rank-by-cost, even the users cannot afford the fee required by the available position at the submission round, they still can resort to the higher costs accumulated from long waiting time and win a position in the future rounds. If several transactions have the same cost, they are ranked randomly. In the round $t \in T = \{1, 2, ...\}$, we calculate the cost by the equation

$$\tilde{b}_i^t = b_i + \beta w_i^t, \tag{1}$$

where β is the weighted factor and w_i^t is the waiting time. Here, $w_i^t = (t - \underline{t}_i)\tau$, and τ is the fixed time interval of each round. Generally, we have $\beta \geq 0$. Without loss of generality, we do not give the detailed formulations of β. However, we can establish different formulations according to the specific design targets without affecting the soundness of our theoretical analysis. For example, we can determine the fixed β to make sure all the retained transactions can be compensated equally according to their waiting time, or we can set that β increases with the waiting time getting longer to avoid over-long retention of unconfirmed transactions.

Accordingly, the top position is allocated to the transaction with the highest cost, the second position to the transaction with the second highest cost, down to the position $min\{n^t, x\}$, where n^t is the number of unconfirmed transactions participating in the round t.

Generally, the transaction's valuation to the user does not depend on the position in which it is confirmed and then recorded to the blockchain, yet the position does influence

TABLE 1
List of Notations

Notations	Definitions
$i(\underline{t})$	The transaction submitted by user i in round $\underline{t}$, $i \in N = \{1, \ldots, n\}$
b_i	The fee of transaction $i(\underline{t})$
v_i	User's valuation on transaction $i(\underline{t})$
x	Count of positions in one block per round
$\tilde{b}_i^t$	The cost of transaction $i(\underline{t})$ in round t, $t \in T = \{1, 2, ...\}$
β	The weighted factor
w_i^t	Waiting time of transaction $i(\underline{t})$ until round t
n^t	Count of unconfirmed transactions in round t
α^j	"Internal" temporal utility of position j, $j \in X = \{1, \ldots, x\}$
p_i^t	The fee transferred to miners if transaction $i(\underline{t})$ is confirmed in round t
r_i^t	Instant payoff of transaction $i(\underline{t})$ in round t
R_i	User i's long-term payoffs in the multi-round games
δ	The discount factor
b_i^*	Equilibrium fee strategy profile
$\tilde{v}_i^t$	The weighted valuation of user i in round t
n_d^t	Count of new transactions in round t
n_o^t	Count of old submissions in round t
b_{i_d+1}	The fee of the new submission ranked highest among $\{x+1, \ldots, n^t\}$
$b_{-i_o}^t$	Retained old transactions' fees in round t
b_{-i_d}	The predicted new transactions' fees
l^*	The targeted optimal position under Farsighted Balanced Strategy
j^*	The targeted optimal position under Instant Balanced Strategy if there is no old submission can be confirmed in any round
$\hat{j}^*$	The targeted optimal position under Instant Balanced Strategy if there is only one old submission can be confirmed in each round

the confirmation sequence and the user's waiting time of completing the confirmation in each block. In view of this, we consider that being ranked in different positions within a round will result in different "internal" temporal utility, and we denote the "internal" temporal utility of the position $j \in X = \{1, \ldots, x\}$ as α^j. In the Bitcoin transaction confirmation game, positions are lined in descending order, and higher positions correspond to higher "internal" temporal utility. That is: for any j and $j+$ such that $j < j+$, we have $\alpha^j > \alpha^{j+}$. Similarly, we do not give the detailed formulation of the "internal" temporal utility; however, different formulations can be established as long as the above condition is satisfied, and they will not influence the correctness of the following analysis in this paper.

In the round t, if the transaction is allocated to the position j, the fee transferred to miners under the formulated GSP mechanism is

$$p_i^t = p_i^{j,t} = \tilde{b}_i^{j+1,t} - \beta w_i^t, \tag{2}$$

which represents the minimum fee that can maintain the current position. If the transaction does not win a position, there is no need to pay any fee in this round. Besides, the unconfirmed transaction will continue to bid for an available position with the originally submitted fee. For the special case of $x \geq n^t$, the last transaction's payment $p^{x,t}$ equals zero.

In the Bitcoin system, transactions are accomplished independently, so the user needs to optimize the fee individually

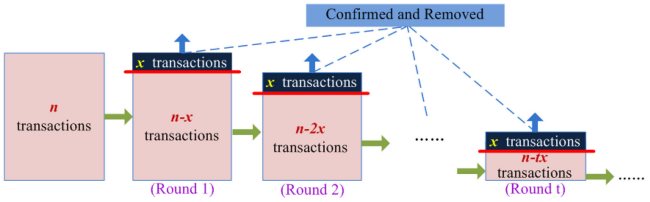


Fig. 2. The case of synchronous submissions.

for each transaction to maximize its payoff. Accordingly, we establish the instant payoff function of the submission $i(\underline{t})$ in the round t as

$$r_i^t = \begin{cases} \alpha^j(v_i - p_i^t), & \text{if } \ \bar{t}_i = t \\ 0, & \text{if } \ \bar{t}_i \neq t \end{cases}. \tag{3}$$

Here, $\bar{t}_i = t$ represents that the transaction is confirmed in the round t.

In practice, Bitcoin transactions will eventually be confirmed. As such, users are committed to maximize their long-term payoffs in the multi-round games, which can be given as follows.

$$R_i = \sum_{t \in [\underline{t}_i, \bar{t}_i]} r_i^t \delta^{w_i^t}, \tag{4}$$

where $0 < \delta \leq 1$ is the discount factor, representing the "external" temporal externality as a result of the delayed transaction confirmation.

In the following sections, we will discuss users' equilibrium strategies in the cases of synchronous submissions and asynchronous submissions.

4 Synchronous Submissions

First, we study the case that all users submit their transactions in a certain round synchronously. The transaction confirmation process under this case is described in Fig. 2. Here, we have $v_1 > ... > v_n$ and $V = \{v_1, .., v_n\}$. Obviously, all transactions' ranks are determined in this round and will not change any more, and they will be confirmed in order at the rate x per round.

As it should be, the temporal utility of a specific position at different round will be unequal. More formally:

$$\begin{aligned} \alpha &= (\alpha^1, .., \alpha^x, \alpha^{x+1}, .., \alpha^{2x}, \ldots, \alpha^{(t-1)x+1}, \ldots, \alpha^{tx}, ...) \\ &= (\alpha^1, .., \alpha^x, \delta\alpha^1, \ldots, \delta\alpha^x, \ldots, \delta^{t-1}\alpha^1, \ldots, \delta^{t-1}\alpha^x, ...), \end{aligned} \tag{5}$$

where, for any t, we have $\delta^t \alpha^x > \delta^{t+1}\alpha^1$.

If the submitted transactions exceed the available positions, i.e., $n^t > x, \forall t \in T$, the multi-round dynamic game with complete information is equivalent to the single-round static game with mx positions described in [24]. It has been proven to have the Locally Envy-Free (LEF) Equilibrium, where no user can improve the payoff through exchanging fees with the one ranked just one position above him/her, that is:

$$\alpha^j(v^j - p^j) \geq \alpha^{j-1}(v^j - p^{j-1}), \forall i \leq tx. \tag{6}$$

Consequently, the equilibrium fee strategy profile can be described by the following recursive function:

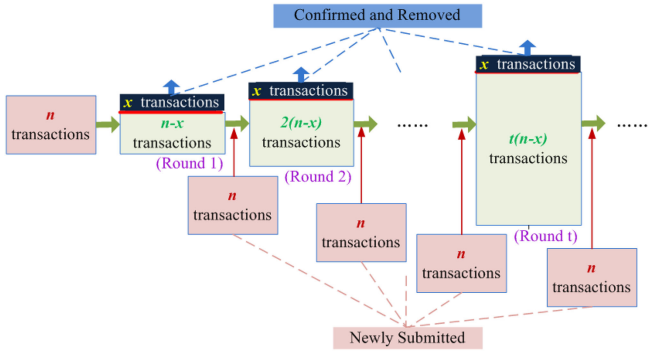


Fig. 3. The case of asynchronous submissions.

$$b_i^* = \begin{cases} \in (b_2, v_1], & \text{if } \ i = 1 \\ v_i - \dfrac{\alpha_i}{\alpha_{i-1}}(v_i - b_{i+1}), & \text{if } \ i \in \{2, \ldots, mx\} \\ v_i, & \text{if } \ i \in \{mx+1, \ldots, n\} \end{cases} \tag{7}$$

In conclusion, under the case of synchronous submissions, our formulated dynamic GSP game with complete information has the LEF Equilibrium, which results in the payments identical to that of the VCG mechanism.

In what follows, we give an example to illustrate the aforementioned case.

Example 1. Let $x = 2$, $\delta = 0.9$, $\alpha^1 = 1$, and $\alpha^2 = 0.95$. We consider the game takes 2 rounds, and 5 users submit transactions pending for confirmation at the very beginning of the game. Suppose these 5 users' valuations are $v_1 = 10$, $v_2 = 9$, $v_3 = 6$, $v_4 = 5$, and $v_5 = 2$, respectively. Then, this case is equivalent to that 5 users compete for 4 positions, which have the temporal utility of $\alpha^1 = 1$, $\alpha^2 = 0.95$, $\alpha^3 = 0.9$, and $\alpha^4 = 0.855$, respectively.

If all users follow the LEF strategy, their equilibrium fees will be $b_1^* \in (2.685, 10], b_2^* = 2.685, b_3^* = 2.353, b_4^* = 2.15, b_5^* = 2$, and the corresponding payoffs will be $R_1^* = 7.315, R_2^* = 6.315, R_3^* = 3.465, R_4^* = 2.565, R_5^* = 0$. Accordingly, transactions of the user 1 and 2 will be confirmed at the first round and transactions of the user 3 and 4 will be confirmed at the second round; while the user 5 cannot get his/her transaction confirmed in this two-round game. Under the LEF strategy, no user can improve payoffs by deviating from his/her equilibrium fee.

In addition, it is easy to prove all users' paid fees equal the counterpart under the VCG mechanism.

5 Asynchronous Submissions

In this section, we discuss the transaction confirmation game under the case of asynchronous submissions, and its process is shown in Fig. 3. We suppose a set of n users keep participating in the multi-round games, and each user submits one new transaction in each round. Identical to the former case, transactions will be confirmed in order at the rate x per round. Assume that each user has the identical valuation of all submitted transactions, i.e., $v_i^t = v_i$. With the knowledge of their own private valuations, users independently determine the associated fee for each transaction. At the end of each round, users' fees, costs as well as the position allocative

results will be made public. Denote the weighted valuation as $\tilde{v}_i^t = v_i + \beta(t - \underline{t}_i)$, and $\tilde{v}_1^t > ... > \tilde{v}_{n^t}^t$.

Under this case, the number of engaged transactions in the round t is

$$n^t = n + (t-1)(n-x), \tag{8}$$

among which, the number of new submissions and old submissions are $n_d^t = n$ and $n_o^t = (t-1)(n-x)$, respectively. Notice that for any t, we have $n^t > x$.

Generally, the old users with $\underline{t} < t$ and $\overline{t} \geq t$ cannot adjust the fee any more, but their costs $\tilde{b}^t$ keep increasing due to the prolonged waiting time. For the modeling purpose, we suppose at most one old submission can be confirmed in each round. Under this setting, if a new submission wins the last available position x while the position $x+1$ is taken by an old submission at a certain round, it is possible to have $b_i^x < \hat{b}^{x+1}$. If we keep following the rule of paying at the second highest fee, the user will need to pay higher than his/her submitted fee. To avoid this situation, we alternatively let $p_i^x = b_{i_d+1}$, where b_{i_d+1} is the submitted fee of the new submission ranked just second to it.

In this paper, we are motivated to make the aforementioned assumptions for the following reasons: 1) In our game-theoretical research, we need to assume a fixed set of participants to theoretically simplify the equilibrium analysis. This kind of assumption is common in other game-theoretical analysis. Also, the equilibrium analysis of the multi-player game is inherently complex, especially in the multi-round dynamic games. These motivate us to formulate the assumptions, including the fixed number of arriving and confirmed transactions as well as the repeated valuations in each round, to simplify the theoretical analysis. 2) As mentioned above, Bitcoin users should submit the deterministic fees and be unable to make further adjustments on submitted fees any more. In view of this, we focus on the strategy analysis of new submissions, and set the assumption of "at most one old submission can be confirmed at each round" for simplicity. Actually, if we relax these assumptions, the theoretical equilibrium analysis will be much more complex and intractable. 3) The analysis on real-world data generated by the Bitcoin system also indicates that the number of arriving and confirmed transactions can be relatively stable during a certain period. Especially, each Bitcoin block has the upper-limit, which restricts the number of transactions that can be recorded into one block; as the average block size keeps stable during a certain period, it is reasonable for us to consider a fixed confirmation rate. 4) As Bitcoin transactions are basically transfer transactions, it is natural to use the transaction amount to represent the transaction's value to the user [29]. In practice, excluding those outliers with large transaction amount, the distribution of transaction amounts for each block can be very similar over a period of time. The real-world transaction data on December 21, 2017 are good examples of these observations.

5.1 Farsighted Strategy

As mentioned in Section 3, users usually view high of the long-run payoffs. The difficulty lies in the prediction of the new submissions' fees not only of the next round but also multiple later rounds. It is the most simple but a natural way for them to consider competitive users' fee decisions will be same with that at the immediate previous round. Based on these considerations, we give the following definition.

Definition 1 (Farsighted Best-Response (FBR) Strategy). *A farsighted best-response strategy is to determine a fee for the transaction newly submitted in the round t by the user i, with the purpose to maximize its total payoff over the following rounds, on the basis of retained old transactions' fixed fees $b_{-i_o}^t$ as well as the predicted new competitive fees b_{-i_d}.*

Formally, given the competitive fees $b_{-i}^t = (b_{-i_o}^t, b_{-i_d})$, the farsighted best-response strategy is $b_i^{t*} \in \arg\max_{b_i} R_i(b_i, b_{-i}^t)$.

The FBR strategy is applicable to the situation that there is one old transaction getting confirmed in each round. First, users in the round t utilize the FBR strategy to target the optimal position for their new submissions. With consideration of the payoff over the following multiple rounds, the optimal position will no longer necessarily within the round t. Given b_{-i}^t, the new submission has the targeted optimal position l^{t^*}, representing the l^*th position in the round t^*.

If $t^* > t$, it means that the user chooses to rank lower than the position x in the rounds $[t, t^*-1]$. Since there is only one old submission getting confirmed in each round, we can deduce that $l^{t^*-1} = x+1$. However, the backward recurrence is not feasible for the former rounds $[t, t^*-2]$. Getting the position $l^* = x+2$ in the round t^*-2 cannot guarantee a position l^* in the round t^*, because the newly coming submissions in the next round t^*-1 may take up his/her desired position $x+1$. In conclusion, it is very hard for the user to target a long-dated optimal position by the FBR strategy. As such, we consider users only target their optimal positions among those in the round t and $t+1$. Accordingly, the payoff function will be

$$R_i = r_i^t + \delta r_i^{t+1}. \tag{9}$$

Under this setting, the user having $t^* = t+1$ should target the position $l^* = x+1$ in the round t.

After targeting the optimal position, then the user needs to determine a proper fee $b_i^{'t} \in (p_i^{l^*,t}, p_i^{l^*-1,t})$ for it. In order to figure out which specific fee the user should choose, we learn from [31] to further propose the following strategy.

Definition 2 (Farsighted Balanced Strategy). *The farsighted balanced (FB) strategy first targets the optimal position*

$$l^* = \underset{j_i^{t-1} \leq j \leq x+1}{\arg\max}\ R_i, \tag{10}$$

and then chooses a proper fee $b_i^{'t}$ so as to satisfy the following conditions:

If $l^* \leq x$, we choose $b_i^{'t}$ through

$$\alpha^{l^*}(v_i - p_i^{l^*}) = \alpha^{l^*-1}(v_i - b_i^{'t}); \tag{11}$$

and if $l^* = x+1$, we determine $b_i^{'t}$ through

$$\begin{aligned} b_i^{'t} &= b_i^{'t+1} - \beta w, \\ \alpha^{l,t+1}(\tilde{v}_i^{t+1} - p_i^{l,t+1}) &= \alpha^{l-1,t+1}(\tilde{v}_i^{t+1} - b_i^{'t+1}). \end{aligned} \tag{12}$$

As for the special case of $l^* = 1$, we pre-define that $\alpha^0 = 2\alpha^1$, and then the user will choose $b_i^{'t} = (v_i + p_i^1)/2$.

Then, we analyze the property of the FB strategy.

Theorem 1. *The FB strategy cannot lead to a stable assignment for our formulated dynamic GSP auctions of transaction fees.*

Proof. If the user i targets the position $x+1$ as the optimal position, the submitted fee $b_i^{'t}$ can be figured out following the definition of the FB strategy. Under the above assumptions, once the original fee $b_i^{'t}$ is determined, the cost in the round $t+1$ is also fixed as $b_i^{'t}+\beta w$. Then, the user can predict its position l^{t+1} in the round $t+1$. Accordingly, we obtain the following conditions:

$$\begin{gathered}\alpha^j v_i - b^{j+1} < \delta(\alpha^{l,t+1}v_i - b^{l+1,t+1} + \beta w), \forall j \in X \\ \Downarrow \\ \delta\beta w > \alpha^j v_i - b^{j+1} - \delta(\alpha^{l,t+1}v_i - b^{l+1,t+1}), \forall j \in X \\ \Downarrow \\ \delta\beta w > \max_{j\in X}(\alpha^j v_i - b^{j+1}) - \delta(\alpha^{l,t+1}v_i - b^{l+1,t+1}).\end{gathered} \tag{13}$$

If there exists the competitive transactions $-i$ also satisfying the above condition described in Equation (13), they will also target the position $x+1$ as the optimal one and submit a fee as $b_{-i}^{'t}$. If $b_i^{'t} < b_{-i}^{'t}$, the user i will win the position, however, this assignment is not stable, because the competitive users have incentives to submit the fee slightly under $b_i^{'t}$ to swap the position with $-i$, which will further push the user i to reduce the fee. The adjustment of fees will be conducted alternately between these competitors until it reaches the following threshold $\dot{b}$.

$$\dot{b} = \min_{i\in N^t}(b_i^{'t} \mid \max_{j\in X}(\alpha^j v_i - b^{j+1}) \le \delta(\alpha^{l,t+1}v_i - b^{l+1,t+1} + \beta w)). \tag{14}$$

As per the predetermined setting of the dynamic games, with the game continuing, there will be more retained old submissions and their costs will increase as well. Then, it is possible to have $\dot{b} \le \tilde{b}^{x+2}$. If $\dot{b} < \tilde{b}^{x+2}$, these users cannot successfully get the targeted position $x+1$ and have incentives to re-target a new optimal position; and if $\dot{b} = \tilde{b}^{x+2}$, a slightly higher fee is required for the position $x+1$, but it will trigger new round of alternate adjustment of their strategies. □

The following example will provide a more illustrative explanation of the property of the FB strategy.

Example 2. Let $x=2$, $\delta=1$, $\alpha^1=1$, and $\alpha^2=0.95$. We consider there are 4 users submitting transactions pending for confirmation at each round, and their valuations are $V=\{10,7,5,2\}$. Suppose the time interval of each round is 600 seconds, and we set $\beta=0.002$.

Set fees of old submissions at the immediate previous round as $b=\{10,7,5,2\}$, then the two transactions with fees equal to 5 and 2 will continue participating in the game, and their costs at the current round will be $\tilde{b}_{3o}=6.2$ and $\tilde{b}_{4o}=3.2$.

Consider all new submissions with fees determined by the FB strategy, users first target the optimal position and then determine the proper fees.

If users prefer their transactions to be confirmed at the current round, their equilibrium fees will be $b_{1d}^*=8.5, b_{2d}^*=6.24, b_{3d}^*=5, b_{4d}^*=2$, and the corresponding payoffs will be $r_{1d}^*=3.76, r_{2d}^*=0.76, r_{3d}^*=0, r_{4d}^*=0$.

If they are farsighted to maximize the long-term payoffs, the user 1 and 2 will target the position 3 at the current round as their optimal position, aiming to win the top 2 positions at the next round. Following the FB strategy, their fees will be $b_{1d}=6.01, b_{2d}=5.86, b_{3d}=5, b_{4d}=2$, and the corresponding payoffs will be $R_{1d}=3.933, R_{2d}=1.14, R_{3d}=0, R_{4d}=0$.

However, this equilibrium is not stable, because the user 1 has incentives to adjust his/her fee to $5.8 < b_{1d} < 5.86$, aiming to get a higher payoff generated from the next round, which will further leads to the user 2's adjustment. It is easy to find that their alternate adjustment of fees cannot converge in the interval $(5.8, 5.86)$. The threshold $\dot{b}$ is 5, however this fee cannot guarantee a successful confirmation in the next round.

5.2 Instant Strategy

In view of the shortcomings of the FB strategy, we then propose an alternative strategy which deals with users' instant payoff in their submission round. Because most users can get transactions confirmed in the submission round in practice and they view high of instant payoff. Similarly, we first introduce the instant best-response (IBR) strategy, and its definition is given as follows.

Definition 3 (Instant Best-Response Strategy). *An instant best-response (IBR) strategy is to determine a fee for the transaction newly submitted in the round t by the user i, so as to maximize its instant payoff in this round, on the basis of retained old submissions' fixed fees $b_{-i_o}^t$ as well as the predicted new competitors' fees $b_{-i_d}^t$.*

Formally, given $b_{-i}^t = (b_{-i_o}^t, b_{-i_d}^t)$, the IBR strategy is $b_i^{*t} \in \arg\max_{b_i} r_i^t(b_i, b_{-i}^t)$.

Since the farsighted decision is very challenging for users, it is reasonable for them to alternatively determine the fee so as to maximize the instant payoffs in the submission round. The basic idea behind the IBR strategy matches well with this consideration. Owing to the tremendous difficulty to make fee predictions, it is natural for users to use public outcomes of the immediate previous round to serve as the predictor of newly submitted competitive fees. Accordingly, there is $b_{-i_d}^t = (b_{1_d}^{t-1}, \ldots, b_{i-1_d}^{t-1}, b_{i+1_d}^{t-1}, \ldots b_{n_d}^{t-1})$.

Given b_{-i}^t, if the user i utilizes the IBR strategy to target the position j^*, the submitted fee will be $b^{'t} \in (p_i^{j^*,t}, p_i^{j^*-1,t})$. Similarly, with the purpose to determine the specific fee for the user, we further propose the following strategy.

Definition 4 (Instant Balanced Strategy). *The instant balanced (IB) strategy first targets the optimal position*

$$j^* = \arg\max_{j\ge j_i^{t-1}} r_i^t. \tag{15}$$

Then it chooses a proper fee $b_i^{'t}$ by solving the following equation.

$$\alpha^{j^*}(v_i - p_i^{j^*}) = \alpha^{j^*-1}(v_i - b_i^{'t}). \tag{16}$$

For the special case of $j^*=1$, we assume that $\alpha^0 = 2\alpha^1$, and the user will then determine $b^{'t} = (v_i + p_i^1)/2$.

First, we study the case that there is no old submission can be confirmed at any round. Then, the competitive

submissions will only include the newly submitted ones, that is $b^t_{-i} = b^t_{-i_d}$. Under this case, the multi-round dynamic games described in this section will be equivalent to the repeated game with a fixed set of users formulated by Cary *et al*. [31]. Accordingly, we have the following remark:

Remark 1. When there is no old submission can be confirmed in any round, if the dynamic GSP games have all new submissions with fees determined by the IB strategy, it will reach a fixed point, where miners allocate x positions in order of decreasing values. Moreover, the equilibrium fee profile is

$$b^*_i = \begin{cases} 2b_2, & \text{if } \ i = 1 \\ v_i - \dfrac{\alpha_i}{\alpha_{i-1}}(v_i - b_{i+1}), & \text{if } \ i \in \{2, \ldots, x\} \\ v_i, & \text{if } \ i \in \{x+1, ...\}. \end{cases} \tag{17}$$

Then, we consider that there is one old submission confirmed in the position $\gamma \leq x$ in the round t. Under this case, users need to re-target the optimal position $\hat{j}^*$ for each new submission, on the basis of the original optimal position j^* in the case of $b^t_{-i} = b^t_{-i_d}$.

Lemma 1. *Users will re-target the optimal positions for new submissions according to the following equation*

$$\hat{j}^* = \begin{cases} j^*, & \text{if } \ 1 \leq j^* < \gamma - 1 \\ j^*, & \text{if } \ j^* = \gamma - 1, v_i \geq \dfrac{\alpha^{j^*}\tilde{b}^{\gamma,t} - \alpha^\gamma b^{\gamma+1,t}}{\alpha^{j^*} - \alpha^\gamma} \\ \gamma, & \text{if } \ j^* = \gamma - 1, v_i < \dfrac{\alpha^{j^*}\tilde{b}^{\gamma,t} - \alpha^\gamma b^{\gamma+1,t}}{\alpha^{j^*} - \alpha^\gamma} \\ j^* + 1, & \text{if } \ \gamma \leq j^* \leq x \end{cases}. \tag{18}$$

Proof. The newly submitted transaction with $j^* = x$ will be squeezed out of the position x and lose the game. Consequently, the user will submit a fee equal to its valuation.

For the new submission with $j^* = \gamma$, sticking to the original optimal position will lead to a zero payoff; and for the new submission with $\gamma < j^*_i \leq x - 1$, the original optimal position will be taken up by the one just ranked higher than it. As such, the user should re-target a new optimal position $\hat{j}^*$ lower than j^* for the new submission with $\gamma \leq j^* \leq x - 1$. In what follows, we prove that $\hat{j}^* = j^* + 1$.

$$\begin{gathered} \alpha^{j^*}(v_i - b^{j^*+1,t}) > \alpha^{j^*+1}(v_i - b^{j^*+2,t}) \\ \alpha^{j^*}(v_i - b^{j^*+1,t}) > \alpha^{j^*+2}(v_i - b^{j^*+3,t}) \\ \Downarrow \\ \alpha^{j^*}(v_i - b^{j^*+1,t}) + \xi > \alpha^{j^*+1}(v_i - b^{j^*+2,t}) + \xi \\ \alpha^{j^*}(v_i - b^{j^*+1,t}) + \xi > \alpha^{j^*v+2}(v_i - b^{j^*+3,t}) + \xi \\ \xi = (\alpha^{j^*+1} - \alpha^{j^*})v_i \\ \Downarrow \\ 2(\alpha^{j^*+1}v_i - \alpha^{j^*}b^{j^*+1,t}) \\ \vee \\ (3\alpha^{j^*+1} - 2\alpha^{j^*} + \alpha^{j^*+2})v_i - (\alpha^{j^*+1}b^{j^*+2,t} + \alpha^{j^*+2}b^{j^*+3,t}) \\ \Downarrow \\ \alpha^{j^*+1}(v_i - b^{j^*+1,t}) > \alpha^{j^*+2}(v_i - b^{j^*+2,t}). \end{gathered} \tag{19}$$

Following the same way, we can finally prove that

$$\alpha^{j^*+1}(v_i - b^{j^*+1,t}) > \alpha^j(v_i - b^{j,t}), \forall j \in \{j^* + 2, \ldots, x + 1\}. \tag{20}$$

The new submission with $j^* = \gamma - 1$ is forced by $i^{\gamma,t}_o$ to pay more for j^*. Then, the re-targeted optimal position should be $\hat{j}^* \in \{j^*, \gamma\}$, because the lower position $\gamma + 1 \leq j \leq x$ needs to be won with the payment higher than the case described in Remark 1. Since the fee of $i^{\gamma,t}_o$ has been determined in the previous rounds, the position allocation in the round t will be determined by the new submission. The user prefers the position j^* to γ if and only if

$$\begin{gathered} \alpha^{j^*}(v_i - \tilde{b}^{\gamma,t}) \geq \alpha^\gamma(v_i - b^{\gamma+1,t}) \\ \Downarrow \\ (\alpha^{j^*} - \alpha^\gamma)v_i \geq \alpha^{j^*}\tilde{b}^{\gamma,t} - \alpha^\gamma b^{\gamma+1,t} \\ \Downarrow \\ v_i \geq \frac{\alpha^{j^*}\tilde{b}^{\gamma,t} - \alpha^\gamma b^{\gamma+1,t}}{\alpha^{j^*} - \alpha^\gamma}. \end{gathered} \tag{21}$$

The new submission with $1 \leq j^* < \gamma - 1$ has no incentive to deviate from j^*, because the required payment for the position $\gamma - 1 \leq j \leq x$ has been raised by the cost of $i^{\gamma,t}_o$. As such, its associated fee keeps identical to that calculated by the Equation (17). □

Theorem 2. *When there is one old submission getting confirmed from a certain round, if the GSP games have all new submissions with fees determined by the IB strategy, it will converge to a fixed point, where the equilibrium fee profile is as follows.*

$$b^*_i = \begin{cases} v_i, & \text{if } \ i = 1 \\ v_i - \dfrac{\alpha_i}{\alpha_{i-1}}(v_i - b_{i+1}), & \text{if } \ i \in \{2, \ldots, x\} \\ v_i, & \text{if } \ i \in \{x+1, ...\} \end{cases} \tag{22}$$

Proof. Since the number of retained old submissions grows with the rate $n - x$ while the number of confirmed old submissions keeps to be 1 from a certain round, the highest cost and weighted valuations of these retained old submissions necessarily get higher as the game continues. Eventually, this will finally lead to the improvement of γ to the first position.

According to Lemma 1, if $\gamma = 1$, we have $\hat{j}^* = j^* + 1$. As such, the game will reach a fixed point that these users winning all positions in the set X form a stable set, where the first position belongs to the old submission, and the positions $\{2, \ldots, x\}$ are allocated in order of decreasing valuations of newly submitted transactions in that round.

Moreover, since the old submission fails to be confirmed in the round $\underline{t}_o$, the equilibrium fee will be equal to its valuation. As for new submissions winning positions in the set X, their equilibrium fees can be calculated according to the Equation (17). □

Corollary 1. *When there is one old submission getting confirmed from a certain round, users' equilibrium payment profile in our proposed dynamic GSP games can be described as follows*

$$p_i^* = \begin{cases} \max\{0, b_2^* - \beta w_1^t\}, & \text{if } i = 1 \\ b_{i+1}^*, & \text{if } i \in \{2, \ldots, x-1\} \\ b_{i_d+1}^*, & \text{if } i = x \\ 0, & \text{if } i \in \{x+1, ...\} \end{cases}. \tag{23}$$

Proof. According to the equation (2), we can simply calculate the equilibrium payment of users getting positions $\{2, \ldots, x-1\}$ as b_{i+1}^*.

Besides, the user obtaining the position x will pay at $b_{i_d+1}^*$ according to the setting in Section 5.

Since we propose to rank transactions by their costs, and the equilibrium payment of the old submission getting the first position is $b_2^* - \beta w_1^t$. However, because the old submission is mainly beneficial from the cumulative waiting time to get the highest cost of this round, it is possible that there is $b_2^* - \beta w_1^t < 0$. If it happens, then the user does not need to pay. □

Through the following examples, we illustrate the properties of the IB strategy.

Example 3. Let $x = 2$, $\delta = 0.9$, $\alpha^1 = 1$, and $\alpha^2 = 0.95$. We consider there are 4 users submitting transactions pending for confirmation in each round, and their valuation set is $V = \{10, 7, 5, 2\}$. The time interval of each round is 600 seconds.

Suppose old submissions in the immediate previous round $t-1$ have fees as $b^{t-1} = \{10, 7, 5, 2\}$, then the two transactions with fees equal to 5 and 2 will continue to participate in the game.

- First, we set $\beta = 0$.

In the round t, the transaction fee auction will go on in the group including not only the newly submitted transactions but also the retained old submissions from the round $t-1$, and their weighted valuations are

$$\tilde{V}^t = (\underbrace{10, 7, 5, 2}_{V_d^t}, \underbrace{5, 2}_{\tilde{V}_o^t}).$$

Under this case, no old submissions can be ranked in top 2, consequently will not be confirmed. Consider all users adopt the IB strategy, their equilibrium fees in the round t will be $b_d^{*t} = (5.25, 5.1, 5, 2)$, and the transaction $1(t)$ will win the first position, and the transaction $2(t)$ will win the second position, and they will be confirmed in this round.

In the round $t+1$, we have

$$\tilde{V}^{t+1} = (\underbrace{10, 7, 5, 2}_{V_d^{t+1}}, \underbrace{5, 5, 2, 2}_{\tilde{V}_o^{t+1}}).$$

Similarly, we can figure out the equilibrium fees for the new submissions with fees following the IB strategy as $b_d^{*t+1} = (5.25, 5.1, 5, 2)$.

It is easy to prove that the equilibrium fees for users adopting the IB strategy will converge to $b_d^* = (5.25, 5.1, 5, 2)$ in the dynamic transaction confirmation games.

- Then, we set $\beta = 0.002$.

In the round t, not only the newly submitted transactions but also the retained old transactions from the round $t-1$ will participate in the game, and their weighted valuations are

$$\tilde{V}^t = (\underbrace{10, 7, 5, 2}_{V_d^t}, \underbrace{6.2, 3.2}_{\tilde{V}_o^t}).$$

Under this case, no old submissions can be ranked in top 2, consequently will not be confirmed. Consider all users adopt the IB strategy, their equilibrium fees in the round t will be $b_d^{*t} = (5.25, 5.1, 5, 2)$, and the new submission $1(t)$ and $2(t)$ will win these 2 positions, respectively.

In the round $t+1$, the participants include not only the new submissions but also the old submissions from previous rounds $3(t-1)$, $4(t-1)$, $3(t)$, and $4(t)$. Their weighted valuations are

$$\tilde{V}^{t+1} = (\underbrace{10, 7, 5, 2}_{V_d^{t+1}}, \underbrace{7.4, 6.2, 4.4, 3.2}_{\tilde{V}_o^{t+1}}).$$

Under the case that there is one old submission getting confirmed in this round, if all users utilize the IB strategy, their equilibrium fees in this round will be $b_d^{*t+1} = (8.7, 7, 5, 2)$. Accordingly, the new submission $1(t+1)$ will win the first position, and the old submission $3(t-1)$ will win the second position.

Similarly, transactions participating in the $t+2$th round are $1(t+2)$, $2(t+2)$, $3(t+2)$, $4(t+2)$, $4(t-1)$, $3(t)$, $4(t)$, $2(t+1)$, $3(t+1)$, and $4(t+1)$. Their weighted valuations are

$$\tilde{V}^{t+2} = (\underbrace{10, 7, 5, 2}_{V_d^{t+2}}, \underbrace{8.2, 7.4, 6.2, 5.6, 4.4, 3.2}_{\tilde{V}_o^{t+2}}).$$

Considering there is one old submission getting confirmed in this round, if all users utilize the IB strategy, their equilibrium fees in this round will be $b_d^{*t+2} = (7.15, 7, 5, 2)$. Accordingly, the old submission $2(t+1)$ will win the first position, and the new submission $1(t+2)$ will win the second position.

In the round $t+3$, the participating transactions include $1(t+3)$, $2(t+3)$, $3(t+3)$, $4(t+3)$, $4(t-1)$, $3(t)$, $4(t)$, $3(t+1)$, $4(t+1)$, $2(t+2)$, $3(t+2)$, and $4(t+2)$. Their weighted valuations are

$$\tilde{V}^{t+3} = (\underbrace{10, 7, 5, 2}_{V_d^{t+3}}, \underbrace{8.6, 8.2, 7.4, 6.8, 6.2, 5.6, 4.4, 3.2}_{\tilde{V}_o^{t+3}}).$$

Under the case that one old submission gets confirmed, if all users utilize the IB strategy, their equilibrium fees in this round will be $b_d^{*t+3} = (7.15, 7, 5, 2)$. Then, the old submission $2(t+2)$ will win the first position, and the new submission $1(t+3)$ will win the second position.

When the game goes to the round $t+6$, the old transaction with highest weighted valuations will be ranked at the first place among all transactions. Then the multi-round transaction confirmation game will converge to a fixed point, where all users following the IB strategy will have the equilibrium fees as $b_d^* = (7.15, 7, 5, 2)$.

6 Experimental Analysis

In this section, we conduct computational experiments to validate the aforementioned theoretical analysis. Computational experiments are the applicable method for the case

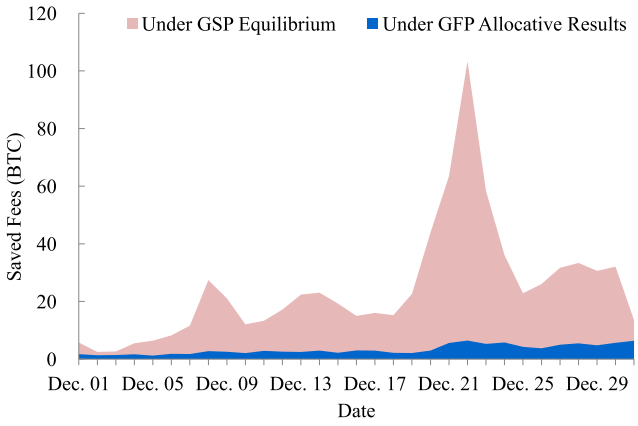


Fig. 4. Saved fees by the GSP mechanism.

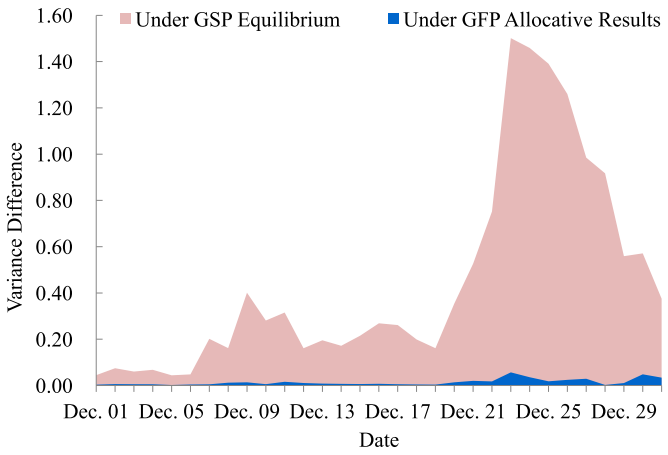


Fig. 5. Variance of paid fees under GFP and GSP mechanism.

without perfect real-world data [14], [35]. It has been proven that the work using synthetic data usually has no significant difference when compared with real-data-based work by data scientists [29]. We use the Bitcoin transaction data during December 2017 as our experimental database, because the amount of submitted transactions are of high demand, and almost all the mined blocks are full during this period.

First, we investigate whether our formulated GSP mechanism is more user-friendly and more stable compared to the currently adopted GFP mechanism. We rank all transactions in each block according to their costs $\tilde{b}$. Because the size s is different for each real transaction, we take it into consideration to define $\tilde{b} = b/s + \beta w$. However, we calculate the total fee transferred by each transaction instead of the unit fee to serve as the basis of comparative analysis on the GFP and GSP mechanisms.

Since the difference of fees paid by users under the GSP mechanism and GFP mechanism does not follow the normal distribution, we use the Wilcoxon test to confirm whether the difference of fees under these two mechanisms is significant. We first assume that there is no difference between the daily fees paid by users in the current GFP game and under the GSP equilibrium, and the Wilcoxon test results show that $Z = -4.860$ and the progressive significance (bilateral) $p = 0.000$, which confirms the significance of difference of fees under these two mechanisms. The Wilcoxon test also confirms the significant difference between the daily fees in the current GFP game and under the GFP allocative results in the GSP game.

During December 2017, the daily saved fees by the GSP mechanism under the GFP allocative results and GSP equilibrium are shown in Fig. 4. In practice, the average daily transaction fee under the GFP mechanism is 616.7604 bitcoins (BTC). Keeping the user-submitted fees and the existing allocative results in the GFP game unchanged, the GSP mechanism can lead to an average saving of 3.3251 BTC per day for all winning users. If the dynamic transaction confirmation game under the GSP mechanism can reach the equilibrium described in Theorem 2, the daily saved fees for users will be much higher, and it is up to 24.5985 BTC on average and can even exceed 103 BTC (e.g., on December 22, 2017). The experimental results confirm that the proposed GSP mechanism is more user-friendly and can help Bitcoin users save fees.

Fig. 5 illustrates the daily difference on variance of paid fees under GFP and GSP mechanism during December 2017. From it, we can see that the variance of paid transaction fees in the GFP game is 1.9464 on average, which is significantly reduced by the GSP mechanism, especially when the GSP game can reach the equilibrium by the IB strategy. Under the GFP allocative results, the variance of transaction fees collected in each block is reduced by 0.0144 BTC^2 per day on average; while the counterpart under the GSP equilibrium is much higher and equal to 0.4511 BTC^2 (i.e., 23.18 percent). Besides, the reduced variance can even exceed 1.0000 on some days, e.g., December 23-26. The experimental results show that transaction fees are more averaged over multiple blocks in the GSP game, which means the GSP game can decrease the variability and increase the stability of miners' revenues generated from different blocks.

Second, we endeavour to validate the theoretical conclusion that the proposed GSP mechanism can achieve stable equilibrium in the dynamic transaction fee auctions. With this purpose, we design the following computational experiments. In these experiments, we consider that 100 users participate in transaction fee auctions under the case of asynchronous submissions. Their valuations, initial fees, as well as waiting time are randomly generated. Here, we relax the assumptions in the computational experiments, including variable valuation sets and unfixed number of old transaction confirmation at each round. To ensure the reliability of experiments, we run 1000 independent experiments with randomly generated parameters.

Fig. 6 shows convergence of user-submitted fee by the IB strategy in one set of computational experiments. This outcome is a typical result of our computational experiments. In this set, after 308 rounds of games, the associated fees of all new submissions have reached the equilibrium profile described in Theorem 2 in this paper.

7 Conclusion and Future Work

Considering the unique features of transaction fee auctions in the Bitcoin system, we propose a novel GSP auction mechanism to tailor to its practical requirements of dealing with the problems caused by the currently-used GFP mechanism, including unnecessarily high fees and instable equilibrium fees.

In the proposed GSP mechanism, we incorporate the user-submitted fee and the waiting time to formulate the cost as

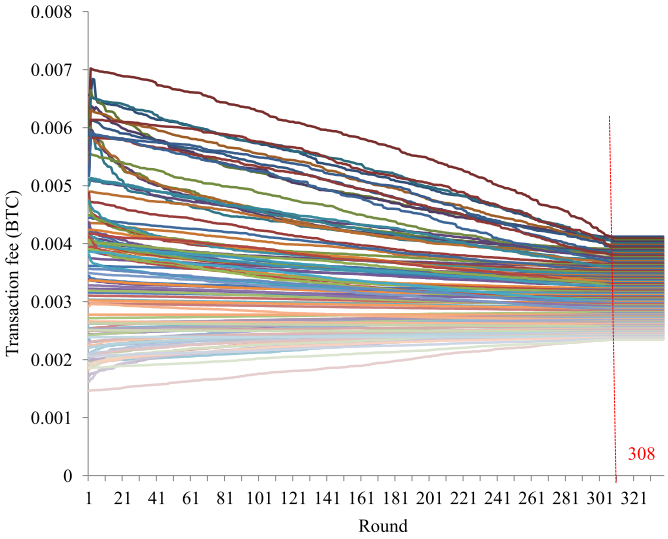


Fig. 6. Convergence profile of the IB strategy under GSP mechanism.

the transaction rank basis. We first discuss the case of synchronous submissions, and find that the dynamic GSP game with complete information has the LEF Equilibrium. Then, we study the case of asynchronous submissions, and define two kinds of strategies to help users determine their optimal fees, which are the FB strategy and the IB strategy. We then show that although the FB strategy meets the requirements of users in the Bitcoin system to make farsighted fee strategies, it cannot lead to a stable equilibrium. Aiming to deal with the shortcomings of the FB strategy, we further alternatively define the IB strategy, and show that if all users utilize the IB strategy, the dynamic transaction confirmation games will converge to a fixed point and thus have the stable equilibrium. Finally, our designed computational experiments have proven that the formulated dynamic GSP game is more user-friendly and stable, and can achieve the convergence following the IB strategy.

Our research can not only provide good support for the mechanism design of the Bitcoin transaction fee auction, and help understand users' transaction fee decisions, but also support the transaction management in other blockchain-powered systems.

One limitation of our theoretical analysis is the simplified assumptions, which is the theoretical abstraction to real-world auctions on Bitcoin transaction fees. Due to the assumptions, our theoretical model can be applied to characterize and explain the dynamic transaction fee auction problem under specific stable environments, e.g., in a setting with relatively stable set of users with fixed values. In the practical Bitcoin system, however, the auction sessions are intrinsically complex. As such, we conduct computational experiments in this research aiming at validating our model and analysis via relaxing the assumptions, and we also plan to extend our theoretical model in our future work to analyze the auction game and its equilibrium in more complicated dynamic environments.

Acknowledgements

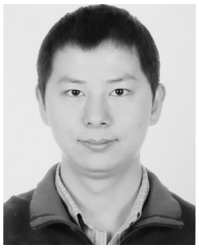
The authors would like to acknowledge the funding supports from the National Key R&D Program of China (#2018AAA0101401) and the National Natural Science Foundation of China (#61533019, #71702182).

References

[1] M. Vasek, "The age of cryptocurrency," *Science*, vol. 348, no. 6241, pp. 1308–1309, 2015.
[2] P. Cska and P. J. Herings, "Decentralized clearing in financial networks," *Manage. Sci.*, vol. 64, no. 10, pp. 4471–4965, 2017.
[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
[4] K. Toyoda *et al.*, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.
[5] S. Wang *et al.*, "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 4, pp. 942–950, Dec. 2018.
[6] A. Extance, "The future of cryptocurrencies: Bitcoin and beyond," *Nature*, vol. 526, no. 7571, pp. 21–23, 2015.
[7] R. Qin, Y. Yuan, and F. Y. Wang, "Research on the selection strategies of blockchain mining pools," *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 5, pp. 748–757, Sep. 2018.
[8] F.-Y. Wang, Y. Yuan, C. Rong, J. Zhang, R. Qin, and M. H. Smith, "Blockchainized internet of minds: A new opportunity for cyber-physical-social systems," *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 4, pp. 897–906, Dec. 2018.
[9] S. Nakomoto, "A Peer-to-Peer electronic cash system," White Paper, 2018. [Online]. Available: https://bitcoin.org/bitcoin
[10] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," 2017. [Online]. Available: https://ssrn.com/abstract=2985764
[11] G. Huberman, J. Leshno, and C. Moallemi, "Monopoly without a monopolist: An economic analysis of the bitcoin payment system," Bank of Finland Research Discussion Paper, 2017. [Online]. Available: https://ssrn.com/abstract=3032375
[12] M. Pisa and M. Juden, "Blockchain and economic development: Hype versus reality," *Center Global Develop. Policy Paper*, 2017. [Online]. Available: https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality
[13] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, architecture and applications," *IEEE Trans. Syst. Man Cybern., Syst.*, vol. 48, no. 9, pp. 1421–1428, Sep. 2018.
[14] F.-Y. Wang, Y. Yuan, C. Rong, and J. Zhang, "Parallel blockchain: An architecture for CPSS-based smart societies," *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 2, pp. 303–310, Jun. 2018.
[15] S. Basu *et al.*, "Towards a functional fee market for cryptocurrencies," 2019. [Online]. Available: https://ssrn.com/abstract=3318327
[16] A. C.-C. Yao, "An incentive analysis of some bitcoin fee design," 2018, *arXiv: 1811.02351*.
[17] R. Lavi, O. Sattath, and A. Zohar, "Redesigning bitcoin's fee market," in *Proc. World Wide Web Conf.*, 2019, pp. 2950–2956.
[18] K. Chalkias and I. Dionysiou, "Going beyond the coinbase transaction fee: Alternative reward schemes for miners in blockchain systems," in *Proc. 20th Pan-Hellenic Conf. Inform.*, 2016, pp. 1–4.
[19] M. Moser and R. Bohme, "Trends, tips, tolls: A longitudinal study of bitcoin transaction fees," in *Proc. Int. Conf. Financial Cryptography Data Secur.*, 2015, pp. 19–33.
[20] D. Easley, M. O'Hara, and S. Basu, "From mining to markets: The evolution of bitcoin transaction fees," *J. Financ. Econ.*, vol. 134, no. 1, pp. 91–109, 2019.
[21] T. Lundqvist, A. de Blanche, and H. R. H. Andersson, "Thing-to-thing electricity micro payments using blockchain technology," *Global Internet Things Summit*, 2017, pp. 1–6.
[22] K. Kaskaloglu, "Near zero bitcoin transaction fees cannot last forever," in *Proc. Int. Conf. Digit. Secur. Forensics*, 2014, pp. 91–99.
[23] J. I Wong, "New study: Low bitcoin transaction fees unsustainable," Oct. 13, 2014. [Online]. Available: http://www.coindesk.com/new-study-low-Bitcoin-transaction-fees-unsustainable
[24] B. Edelman, M. Ostrovsky, and M. Schwarz, "Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords," *Amer. Econ. Rev.*, vol. 97, no. 1, pp. 242–259, 2007.
[25] X. Zhang and J. Feng, "Cyclical bid adjustments in search-engine advertising," *Manage. Sci.*, vol. 57, no. 9, pp. 1703–1719, 2011.
[26] T. Borgers *et al.*, "Equilibrium bids in sponsored search auctions: Theory and evidence," *Am. Econ. J. Microecon.*, vol. 5, no. 4, pp. 163–187, 2013.

[27] Y. Yuan, F.-Y. Wang, and D. Zeng, "Competitive analysis of bidding behavior on sponsored search advertising markets," *IEEE Trans. Comput. Social Syst.*, vol. 4, no. 3, pp. 179–190, Sep. 2017.
[28] N. Houy, "The economics of bitcoin transaction fees," 2014. [Online]. Available: https://ssrn.com/abstract=2400519
[29] J. Li, Y. Yuan, and F.-Y. Wang, "A novel GSP auction mechanism for ranking bitcoin transactions in blockchain mining," *Decis. Support Syst.*, vol. 124, 2019, Art. no. 113094, doi: 10.1016/j.dss.2019.113094.
[30] Y. Kamijo, "Bidding behaviors for a keyword auction in a sealed-bid environment," *Decis. Support Syst.*, vol. 56, no. 1, pp. 371–378, 2013.
[31] M. Cary *et al.*, "On best-response bidding in GSP auctions," Harvard Business School NOM Working Paper, 2008. [Online]. Available: https://ssrn.com/abstract=1087990
[32] V. Krishna, *Auction Theory*. Cambridge, MA, USA: Academic Press, 2009.
[33] H. R. Varian, "Position auctions," *Int. J. Ind. Org.*," vol. 25, no. 6, pp. 1163–1178, 2007.
[34] L. Ausubel and P. Milgrom, "The lovely but lonely vickrey auction," in *Combinatorial Auctions*, Cambridge, MA, USA: MIT Press, 2005.
[35] F.-Y. Wang and S. Tang, "A framework for artificial transportation systems: From computer simulations to computational experiments," *Proc. IEEE Int. Transp. Syst.*, 2005, Art. no. 1130–1134.

Juanjuan Li (Member, IEEE) received the BS and MS degrees in economics from the Renmin University of China, in 2008 and 2010, respectively. She is working toward the PhD degree in the Beijing Institute of Technology. She is currently an assistant professor with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. Her research interests include blockchain, digital currency, computational advertising, and business intelligence.



Xiaochun Ni received the BS and MS degrees in management science and engineering from Dalian Maritime University, in 2006 and 2008, respectively. Currently, he is an engineer with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. His research interests include blockchain, social computing and knowledge automation.

Yong Yuan (Senior Member, IEEE) received the BS, MS, and PhD degrees in computer software from the Shandong University of Science and Technology, Shandong, China, in 2001, 2004, and 2008, respectively. He is currently an associate professor with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. His research interests include blockchain, cryptocurrency, smart contract, and business intelligence.

Fei-Yue Wang (Fellow, IEEE) received the PhD degree in computer and systems engineering from Rensselaer Polytechnic Institute, Troy, NY, in 1990. He joined the University of Arizona, Tucson, AZ, in 1990, and became a professor and the director of the Robotics and Automation Laboratory and the Program in Advanced Research for Complex Systems. In 1999, he founded the Intelligent Control and Systems Engineering Center, Institute of Automation, Chinese Academy of Sciences (CAS), Beijing, China. In 2002, he joined the Lab of Complex Systems and Intelligence Science, CAS, as the director, where he was the vice president for Research, Education, and Academic Exchanges with the Institute of Automation from 2006 to 2010. In 2011, he was named as the State Specially Appointed Expert and director of the State Key Laboratory for Management and Control of Complex Systems, Beijing, China. He was elected as a fellow of INCOSE, IFAC, ASME, and AAAS. His research interests include blockchain, parallel systems, social computing, parallel intelligence, and knowledge automation.