Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8885179, 12 pages
https://doi.org/10.1155/2020/8885179

Research Article

A Novel Pricing Mechanism for User Coalition in Blockchain

Yi Jiang,[1] **Xu Liu**,[1,2] **and Jun Dai**[1]

[1]*School of Information Engineering, Yangzhou University, Yangzhou Jiangsu 225127, China*
[2]*School of Business, Victoria University, Melbourne VIC 3011, Australia*

Correspondence should be addressed to Xu Liu; 1438239097@qq.com

Received 21 September 2020; Revised 15 October 2020; Accepted 23 October 2020; Published 28 November 2020

Academic Editor: Junwu Zhu

As the blockchain platform is widely used as a new trading way, both participants and transaction volume in the blockchain projects have been growing by leaps and bounds. The generic mechanisms of ranking transaction priorities are heavily dependent on the transaction fees the users append into each transaction; then, all transactions are ranked in the nonincreasing order according to the transaction fee amounts, and the selected transactions will be packed into a new created block in order based on the ranking results. However, more complex influence factors more than transaction fees on transaction priority ranking results are not taken into consideration in the generic transaction priority ranking mechanisms, and a single user is the objective to create transactions in these mechanisms. In order to optimize the generic transaction priority ranking mechanisms and enrich transaction creation modes, a novel user-coalition-based transaction pricing mechanism (UCTPM) is proposed, and the user coalition quality score, user coalition contribution degree, and the transaction type demand degree are formulated and introduced into the UCTPM mechanism. Our research findings indicate that the UCTPM mechanism satisfies the economic attributes of budget balanced, individual rationality, and incentive compatibility when the user coalition contribution degree increases through theoretical proof and experimental analysis. Moreover, the UCTPM mechanism allows all the transactions to be processed more efficiently by experimental analysis.

1. Introduction

In contrast to the traditional financial systems that heavily rely on centralized supervision, digital cryptocurrencies use blockchain as the technical solutions providing a decentralized distributed ledger economic model for the current financial market and enabling participants to freely join this kind of open-market platform without constraints. Due to various excellent characteristics of blockchain technologies such as data immutability, information traceability, and node pseudonyms, more participants have enjoyed such new transaction methods provided by blockchain platforms. [1, 2]

With the emergence and constant improvement of various blockchain projects such as Bitcoin and Ethereum, the digital cryptocurrencies issued by different blockchain projects have attracted a large number of participants to contribute to the computational power in mining activities which is to compete for being the first valid participant solving the proof-of-work-based cryptographic puzzle then to receive a certain amount of lucrative cryptocurrency as a mining reward. In detail, among the blockchain projects where the consensus process is based on proof of work (PoW), new blocks are normally generated by the participants called miners who continuously perform massive hash calculations to obtain the full solution for the hash puzzles, and the miner who firstly gains the full solution is granted the right to add these selected transactions into a new created block; then, he or she can get the transaction fees as extra mining profit in addition to the fixed block reward once the new block is committed as valid to the main chain [3, 4].

During the transaction confirming process, all the participants can create transactions; when a node firstly generates one transaction and broadcasts it to other nodes within the whole blockchain network, a certain amount of transaction fee is needed to append along with the generated transaction (even though the transaction fee is not enforced to append along with the transaction); once the transaction is verified to be valid, then it will be added into the mempool waiting in queue to get processed by the miner who wins the mining competition; then, some transactions are selected to append into the new created block based on certain rules (generally from the highest transaction fee down to the lowest fee). Once the full solution of the cryptographic puzzles is found, the newly mined block is added to the main chain and propagated through the network. The transaction fee, as an economic incentive method of blockchain, is one of the important and effective approaches to guarantee nodes of participation in mining activities and transaction verification during the whole transaction confirming processes. Among the generic methods of transaction selection, miners normally prefer these transactions with higher fees to append into a new block in order to optimize the total profit while mining; as a result, users are stimulated to increase the transaction fees to some extent with the purpose of getting transactions to be confirmed as soon as possible [5]. Moreover, users can perform strategic bidding by observing and analysing the dynamic status of transaction queuing states in the mempool to estimate the transaction threshold fee (that is, the lowest transaction fee among all the transactions is being added into the new block), thus fluctuating the overall profit of miners and affecting the efficiency of blockchain network transaction confirming processing as consequences [6].

As it has been considered about the continuous improvement and widespread use of smart contracts in blockchain, the transaction types have been expanded. In the current PoW-based blockchain projects, the common transaction types can be divided into two main categories as token transfer class and smart contract operation class. In detail, the token transfer class covers transactions with different amounts of token and lock-time settings (that is, the expected time for the transaction to be added into a new block), while the smart contract operation class includes calling, updating, and creating. Beyond these transaction types above, participants also can convert the main chain tokens into the side chain tokens in order to bring more functions for the whole network under the applied advanced smart contracts; therefore, the shifting evolution of smart contracts results in a wider variety of transaction types [7, 8]. With all the nodes involved in the blockchain network are the behaviour subjects who are involved in transaction verification, transaction creation, mining reward competition, and other activities via the blockchain platform, and all the historical activity information is recorded in the relevant code fragment in the blockchain; this makes it possible to use such activity information as a basis to measure the quality and contribution of each node in the network.

In addition, for most mechanisms used in the transaction confirming process in the blockchain, incentive compatibility is of great importance for any participants to behave truthfully when bidding the transaction fees, and the rare resource in the transaction confirming process is the number of transactions which can be packed successfully during each round of mining. In this paper, we strive to study the factors affecting the transaction confirming process, and we declare that the participants who are involved in the blockchain network are user, user coalition, and miners for simplification.

As the fast development and application of blockchain technologies and the widespread usage of the digital economic system with such a technical foundation, a mechanism where participants are encouraged to join more activities and behave honestly is necessary for the blockchain market [9]. Based on the analysis above, we proposed a user-coalition-based transaction pricing mechanism (UCTPM); this mechanism consists of two algorithms: user coalition weighted transaction priority (UCWTP) algorithm and transaction priority rank-based pricing (TPRP) algorithm, and each of the algorithms corresponds to transaction priority determination and pricing for the winning user coalitions, respectively. Although there are several researches that bring the transaction size, historical transaction volume, and user waiting costs to calculate the transaction priority results, the calculation modes of these factors are not given in the general second price auction model. [10] It needs to be emphasized that, in the UCWTP mechanism, the user coalition quality score, coalition contribution degree, and transaction type demand degree are formulated in detail and introduced to optimize the transaction priority algorithms that only focus on the single transaction fee. In addition, we consider that the participants join the user coalitions as the transaction creation mode, which is fairly a novel transaction creation mode, and we believe that the main advantage to consider such a new transaction creation mode is that the efficiency of the transaction confirming process can be improved due to the transactions that are selected by batch instead of by individual, also it is verified via the experiments conducted in this paper.

Whereafter, it is also proved through theoretical proof that the UCTPM mechanism proposed in this paper satisfies the economic attributes of budget balanced, individual rationality, and incentive compatibility under the circumstance that the user coalition contribution degree increases. Besides, it shows that the UCWTP algorithm in the proposed UCTPM mechanism can help to reduce the impact of a single transaction fee on transaction priority ranking by an average of 5.17% when compared to the traditional transaction priority algorithm through experimental analysis.

Our contribution can be summarized as the following three:

(1) Design a new UCTPM mechanism to optimize the traditional transaction priority algorithms by introducing the user coalition quality score, coalition contribution degree, and transaction type demand degree

(2) Adopt user coalition transaction creation model instead of an individual transaction creation model to enrich the transaction creation modes for the blockchain

(3) Prove that nodes under the UCTPM mechanism can be effectively stimulated to participants in the activities such as transaction creation, transaction verification, and computing power competition for bookkeeping right, so as to improve the contribution degree and quality score

The rest of the paper is structured as follows: Section 2 gives a brief review of related work. Section 3 defines the basic concepts that are used in the UCTPM mechanism model. Section 4 describes the problem details. Section 5 formally establishes the models of the UCWTP algorithm and the TPRP algorithm that both consisted of the UCTPM mechanism. Section 6 presents the detailed algorithms of UCWTP and TPRP and theoretically verifies that the UCTPM mechanism satisfies the economic attributes of individual rationality, budget balanced, and incentive compatibility as the user coalition contribution degree increases. In Section 7, the proposed UCWTP algorithm can effectively help to reduce the impact of the single transaction fee on transaction priority through the experimental analysis, thus motivating user coalition to actively join the activities in the blockchain platform, and the transaction confirming process time is also reduced under the user coalition transaction creation mode. Finally, this paper is summarized and some future work is discussed in Section 8.

2. Related Work

During the initial stage of the Bitcoin project, users need to provide the default transaction fee, and miners are required to process the transactions according to the system settings even for the zero fee transactions, whereas users prefer to offer a higher transaction fee to attract miners in order to reduce the transaction processing waiting time with the growth of transaction volume and users [11]. As recorded in the official document of Bitcoin, the transaction fees are not required for some certain types of transactions though the zero transaction fees cannot be financially sustainable with the development of Bitcoin [12].

As the emergence of transaction fees has led to the transformation of blockchain from a simple structure of mining to a market-based ecological structure, some researches and methodologies have been studied about the influence factors on transaction fees. The game model is established in Kasahara and Kawahara's research to analyse the impact of factors on transaction fees including the transaction flow-in rate, flow-out rate, and user waiting time [13]. Moreover, several mechanisms such as providing a fixed transaction fee to users and miners and the Vickrey-Clarke-Groves (VCG) auction-based pricing model are compared to analyse the equilibrium transaction fee, due to the fee that essentially depends on the cost of involving in the infrastructure for miners to compete in mining [14]. However, the fixed transaction fee is infeasible in the long run according to the static partial equilibrium model that is designed for the economic analysis of the transaction fee [15].

In addition, the Bitcoin market attribute of incentive compatibility is deeply studied, and the monopoly pricing model and random sampling pricing model are established with the purpose of avoiding user utility improvement by lying the transaction fees, and the results of theoretical verification show that the monopoly pricing mechanism is near incentive compatibility under the condition of enough users and transaction volume [16].

The researches on transaction fees introduced above are more focused on the user perspective, but the transaction fees are crucial to miners as well. Transaction fees as the extra reward are the economical incentive to sustain mining operations [17]. Furthermore, when miners cannot profit from the mining process, they may switch from the current blockchain platform to another one for mining [18]. Since the past few years that Bitcoin was invented, the fixed block reward plays a much more important role in the whole mining revenue system; the average revenue is approximately 14 BTC per block with the fixed block generation reward 12.5 BTC in 2017; however, the situation starts to change somehow with the decreasing fixed block reward per 4 years, and the highest overall revenue is about 19.79 BTC per block; all the changes indicate that the transaction fees start to play a key role in the blockchain market and can affect the miner's revenue to a certain extent [19, 20].

Nevertheless, transaction fees not only are an important part of the blockchain market economy that determines the revenue of both users and miners but also have great influence on transaction priority ranking results which are the key basis for the transaction confirming process. Under different priority rules, the user transaction fee decisions are various [21]. Moreover, users prefer to increase the transaction fees for the higher transaction priority in the transaction confirming process where only transaction fees directly affect priority rank results; meanwhile, users with lower transaction fees are discouraged to create transactions due to prolonged waiting time, thus leading to negative influence on the blockchain development [22, 23].

3. Concept Definition

Definition 1 (user coalition). Any node who creates transactions via the blockchain platform is called a user, and such a node can be a miner as well. User coalition is a group with $n\ (n > 1)$ users to create transactions, and in writing, the user coalition is set as CL_k, $k \in \mathrm{CL}_k = 1, 2, \cdots, k$. In particular, any users in the user coalition create their own transactions severally and form a transaction set as the coalition's transaction set.

Definition 2 (miner). The nodes who contribute to the computational power in the mining process are called miners. And there is only one miner m who will obtain the transaction fees and block rewards during each round of mining competition; moreover, the transactions of winning user coalition are processed by m.

Definition 3 (user coalition utility). Denote that the utility of user coalition $k(\forall k \in \mathrm{CL}_k)$ is $u_{\mathrm{CL}_k} = (V_k - p_k)$; that is, the utility is the difference value between the overall valuation of the transactions and actual payment of any k.

Definition 4 (individual rationality). If there is no loss of profit for any k who participates in the mechanism, that is, $u_{\mathrm{CL}_k} \geq 0\ (\forall k \in \mathrm{CL}_k)$, this demonstrates that the mechanism satisfies the attribute of individual rationality.

Definition 5 (budget balanced). If all the income of the mechanism comes from the total payment of winning user coalition without any external personnel, and the expenditures of the mechanism are all used to pay the miner who processes the transaction without any value transfer, that is, $\sum_{k\in W} p_k = \text{pay}_m$, this illustrates that the mechanism satisfies the attribute of budget balanced, and the attribute of budget balanced ensures that there is no value to be transferred in or out from the mechanism.

Definition 6 (incentive compatibility). Denote the truthful bid as b_k, the lying bid as b_k' for $k(\forall k \in \text{CL}_k)$ when k $(\forall k \in \text{CL}_k)$ bids for the transaction set, and the corresponding utilities are u_{CL_k} and u_{CL_k}', respectively. The mechanism is incentive compatible if one of the following two conditions is true: (1) it satisfies $\forall k \in \text{CL}_k, b_k > b_k' \longrightarrow u_{\text{CL}_k} \geq u_{\text{CL}_k}'$ when k lowers the transaction fee bid, or (2) there exists a strategy α_k for k to increase the transaction fee bid and strategy α_k^* for k to increase the quality score, when it satisfies $\forall k \in \text{CL}_k, u(\alpha_k^*, \alpha_{-k}^*) \geq u(\alpha_k, \alpha_{-k}^*)$ under the conditions that k's contribution degree increases. Both of the conditions indicate that any k cannot improve the utility by lying the transaction fee bid. Moreover, the attribute of incentive compatibility indicates that k satisfies the current transaction fee bid under certain conditions, so that the incentive of the lying transaction fee bid is deprived.

4. Problem Description

In this section, we formalize the transaction confirming problem in detail to lay the foundation for the establishment of the UCWTP mechanism, and the basic parameters involved in the problem are listed in Table 1.

Assume there are n nodes in the blockchain network and denote U as the set of nodes, written as $U = \{1, 2, \cdots, n\}$. And there are two types of roles involved in the transaction confirming process, respectively, miner m who wins the mining competition during the current round and user coalition CL_k, and $\text{CL}_k \in U, m \in U$.

According to the real situation of blockchain, there is only one m who is verified to be valid for packing transactions into a new created block to gain the transaction fees during each round of mining competition. Because the user coalition k's actual payment is affected by the discount factor in different priority ranks, in order to ensure the profit of miner m, m can set the unit reserve price c_m for transactions packed into a new block according to the actual mining cost. User coalition transaction volume, estimated ranking discount, and c_m are reported to the mechanism by m.

Assume there are $|\text{CL}_k|$ user coalitions in the whole network and each user coalition is required to submit the transaction report which contains transaction information including transaction fee bid set $B_k = [b_1, b_2, \cdots, b_k]$ and transaction size set $S_k = [s_1, s_2, \cdots, s_k]$. Denote the report submitted by user coalition CL_k as a triple $\text{Req}_k = (V_k, B_k, S_k)$, where $|B_k|$ represents the total volume of transactions in the set due to the arbitrary bid corresponding to a certain transaction, and V_k represents k's valuation on the transactions, and V_k also can represent the maximum price k is willing to pay:

Table 1: Basic parameters used in this paper.

Notation	Explanation
CL	Set of user coalition
α_k	Transaction type demand
B_k	Transaction fee bid from user coalition
φ_k	User coalition quality score
V_k	Transaction valuation from user coalition
con_k	User coalition contribution degree
p_k	User coalition actual payment
u_{CL_k}	User coalition utility
S_k	Transaction set size
θ_k^j	The discount factor of k in rank j

$$V_k = \begin{cases} [v_1, v_2, \cdots, v_n], & S_k \neq 0, \\ 0, & S_k = 0. \end{cases} \tag{1}$$

The blockchain transaction confirming processing is shown in detail in Figure 1; firstly, users join the coalition and report the transaction information to the UCTPM mechanism; miner m who wins the mining competition reports his/her own information as well; then, the transaction priority ranking results are available according to the UCTPM mechanism. The winning user coalition needs to make the payment according to the priority ranking results; thus, the essence of the UCWTP algorithm can be seen as to determine the winner set whose transaction sets are packed into a new block. Lastly, m gains the total transaction fees paid by winning user coalitions and broadcasts the new block to the network.

5. Design of UCTPM Mechanism

Our UCTPM mechanism consists of the UCWTP model and the TPRP model. The UCWTP model determines the winner determination problem, that is, determining whose transaction sets are packed into the new block, while the TPRP model is used for the actual payment of winning user coalitions.

5.1. UCWTP Transaction Priority Model. Assume that the arbitrary user is involved in the blockchain participant in the activities such as transaction creation, transaction verification, and extending the main chain, and these historical activities are recorded, so that such information can be used as a basis for calculating the quality score of the user coalition. Besides, the user coalition contribution degree and valid transaction volume are also considered the influencing factors for the user coalition quality score in our model, and the quality score calculation model is as follows:

$$\varphi_k = \left(\phi_0 + \text{con}_k \sum_{m=1}^{n} (|tx_k m|) \right)^{\mu}. \tag{2}$$

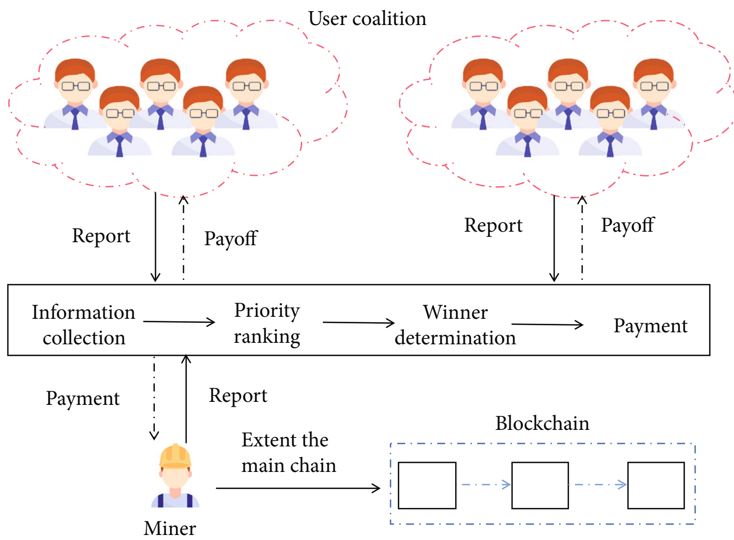

FIGURE 1: Basic transaction process diagram of blockchain.

In equation (2), ϕ_0 is the initial quality score for arbitrary user coalition k and ϕ_0 is a constant value. $|tx_k m|$ represents the valid transaction volume of k during the transaction confirming processing for the current round (for example, the nth round), which can be divided into two parts precisely: firstly, the total volume of transactions that have been recorded into the main chain during the $n-1$ rounds; secondly, the verified transaction volume for current round n. And μ is the constrained parameters where $0 < \mu < 1$. In addition, con_k is k's contribution degree and can be formulated as

$$\mathrm{con}_k = \frac{1}{n}\left(\sum_{m=1}^{n} \Omega_{km} \times (P_{km} + 1)\right). \tag{3}$$

In equation (3), Ω_{km} represents the number of transactions verified by k at the mth round of transaction confirming processing, and denote $P_{km} = \{0, 1\}$ to indicate whether there are users in the coalition who wins the mining competition at the mth round, where $P_{km} = 1$ means there is such a miner, $P_{km} = 0$ otherwise.

Except for user coalition quality φ_k which can affect the results of transaction priority ranking, the different transaction types created by k should influence the ranking results as well. User coalition can implement different functions and achieve various purposes by creating various transactions, and we roughly divide the common transaction types into five categories: transactions with or without lock-time, also with the smart contract operation, creation, and other transaction types:

$\mathrm{type}_t \longleftarrow \mathrm{type}_1$, if transaction with lock-time,
$\mathrm{type}_t \longleftarrow \mathrm{type}_2$, if transaction without lock-time,
$\mathrm{type}_t \longleftarrow \mathrm{type}_3$, if creation of smart contract,
$\mathrm{type}_t \longleftarrow \mathrm{type}_4$, if operation of smart contract,
$\mathrm{type}_t \longleftarrow \mathrm{type}_5$, if others.

Considering that the volume of a certain transaction type in the total volume that transactions are recorded on the main chain can reflect the demand degree of this certain type of transaction, thus we formula the transaction type demand degree based on type_t for arbitrary user i from k as

$$\gamma_i = \left(1 + \frac{\sum |\mathrm{type}_t|}{\mathrm{Num}}\right)^{1/\varepsilon}. \tag{4}$$

In equation (4), type_t reflects the total volume of this certain transaction type recorded on the main chain, Num represents the overall transaction volume on the main chain, and parameter $1/\varepsilon$ help to prevent the boost increase of certain transaction types in the blockchain network from severely impacting transaction priority ranking results. Because we consider the scenario that users join the coalition for transaction creation, the transaction type demand degree for k is developed on the average value of equation (4) as shown below:

$$\alpha_k = \frac{\sum_{i \in \mathrm{CL}_k} \gamma_i}{|\mathrm{CL}_k|}. \tag{5}$$

The methods that used to reduce the impact of transaction fee bid B_k on priority ranking results should not only focus on the introduction of user coalition quality score φ_k but also consider the impact of B_k on the transaction priority ranking results which should be gradually decreased when B_k increases under the condition that user coalition contribution degree con_k keep increasing. Therefore, we adopt a new method to calculate the transaction fee bid as the following:

$$b'_k = B_k \times e^{-(\sigma \mathrm{con}_k)}. \tag{6}$$

The parameter $\sigma (0 < \sigma < 1)$ is used to restrain the abrupt attenuation of b'_k when con_k increases. In addition, only the transaction sets that meet the requirement $B_k/|B_k| \geq c_m$ can be processed in order to guarantee the profit of m, where c_m is unit reserve price for m. In consequence, we proposed the UCWTP calculation model based on equations (2), (5), and (6):

$$B_k' = \frac{b_k' \times \varphi_k \times \alpha_k}{S_k}. \tag{7}$$

The new transaction priority ranking results for user coalition can be sorted as $B_1' \geq B_2' \geq \cdots \geq B_k'$ according to equation (7), and the corresponding priority rank is $r_1 \geq r_2 \geq \cdots \geq r_k$. Meanwhile, m is supposed to pack the transaction sets into a new created block by the rank from high to low until the block size cap. And denote $x_{ck} = \{0, 1\}$ to indicate the transaction set packing results, $x_{ck} = 1$ means the transaction set is packed into the new block, and $x_{ck} = 0$ otherwise, so that the winning user coalition set can be denoted as $W = \{\forall k \in CL_k \mid x_{ck} = 1\}$.

5.2. TPRP Pricing Model. The user coalition can obtain different transaction priority ranks by the comprehensive results of transaction fee bid, contribution degree, quality scores, and transaction type demand degree, and the actual payment of the winning user coalition based on various ranks is different, which also should be irrelevant to the user coalition transaction fee bid; otherwise, the user coalition will always have the incentive to lie the transaction fee under the situation of becoming the winner. Thus, we propose the TPRP pricing model that is based on the transaction priority ranks and on the purpose of depriving the correlation between payment and user coalition owning transaction fee bids:

$$p_k = \theta_k^j \times |B_k| \times c_m. \tag{8}$$

In equation (8), $|B_k|$ is the volume of transactions created by user coalition, and θ_k^j is the discount factor of k when k ranks j, and also, $\theta_k^j \leq \theta_k^g$ when $r_j \geq r_g$:

$$\theta_k^j = \beta \times r_k^j \longrightarrow (0, 1]. \tag{9}$$

The transaction set of winning user coalition is processed by m; then, m broadcasts the new block to the whole blockchain network after the selected transaction sets are packed into the new generated block; then, m receives the total transaction fees from winning user coalitions as a reward:

$$\mathrm{pro}_m = -\sum_{k \in W} p_k \tag{10}$$

The winning user coalition will also be profit after the new block is considered to be valid as it appended onto the main chain; therefore, the expected revenue V_k is obtained by k, and the utility of such a user coalition can be formulated as

$$u_{\mathrm{CL}_k} = xc_k(V_k - p_k). \tag{11}$$

6. Algorithm and Attribute Proof

6.1. UCWTP Algorithm and TPRP Algorithm. The UCTPM mechanism proposed in this paper mainly includes two parts: the transaction priority ranking algorithm and the winning user coalition pricing algorithm. The essence of the transaction priority ranking algorithm is used for winner determination so that the specific miner needs to pack the selected transaction sets into the new created block, and the transaction priority ranking algorithm is called the UCWTP algorithm, while the TPRP algorithm is the solution to the winning user coalition payment issue.

Algorithm 1 describes the process of winner determination, and we set each round of priority ranking process as static; that is, once the transaction sets are selected for the transaction priority ranking process, these sets are not affected by any changes due to new transaction sets arriving in the mempool. First of all, Steps 2 to 5 indicate that the transaction priority ranking result of the selected user coalition is calculated based on the coalition quality score, transaction type demand degree, transaction fee, and contribution degree; Step 7 shows that the new transaction sequence is sorted in a nonincreasing order; finally, Steps 8 to 11 determine the winning user coalition sets according to the priority ranking result and the block capacity limitation.

Algorithm 2 describes the pricing process for the winning user coalition; Steps 2 to 6 illustrate that these user coalition needs to make the actual payment according to the transaction priority ranking result and the transaction volume, so that the user coalition actual payment is irrelevant to user coalition own transaction fee bid. In addition, the lower the rank is, the higher the user coalition payment would be due to the discount factor; nevertheless, when the user coalition wants to lower the actual payment by reaching the higher transaction priority rank, the user coalition will prefer to improve the unit quality score instead of the unit transaction fee. As a result, it deprives the motivation for the user coalition to improve utility by lying the transaction fee bid.

6.2. Attribute Proof

(1) If the lower bid b_k' results in the failure of the transaction set being packed into the new block, then $xc_k = 0$ according to equation (11); thus, $u_{\mathrm{CL}_k}' = 0$

(2) If the lower bid b_k' results in lower transaction priority rank r_j, then $\theta_k^j \geq \theta_k^g$. And the user coalition actual payment only depends on the transaction priority rank and the transaction volume and is irrelevant with the transaction fee bid; that is, when $\theta_k^j \geq \theta_k^g$, there exists $p_k^j \geq p_k^g$, so that, $u_{\mathrm{CL}_k} - u_{\mathrm{CL}_k}' = V_k - p_k^g - (V_k - p_k^j) = p_k^j - p_k^g \geq 0$

Input: Reports submitted by user coalition: $R_{cl} = \{r_1, r_2, \cdots, r_n\}, r_n = <V_k, B_k, S_k>$
Reports submitted by miner: $R_m = <c_m>$
Output: W: the sets of winning user coalition
initialize $sum \longleftarrow 0, W \longleftarrow N, L \longleftarrow \varnothing C \longleftarrow$ maximum size of a block
for all $k \in W$ **do**
$b_k' = B_k \times e^{-(\sigma con_k)}$
$\varphi_k = (\phi_0 + con_k \sum_{m=1}^{n} (|tx_k m|)^{\mu}$
$B_k' \longleftarrow (b_k' \times \varphi_k \times \alpha_k / S_k)$
end for
sort W in non-increasing order of B_k': $B_1' \geq B_2' \geq \cdots \geq B_k'$
for all $i \in W$ **do**
if $sum \leq C$ **then**
$sum + = S_i$
$W \longleftarrow W \setminus \{i\}, L \longleftarrow L \cup \{i\}$
end if
end for
$W \longleftarrow \varnothing$
$W \longleftarrow L$
return W

Algorithm 1: UCWTP.

Input: Reports submitted by user coalition: $R_{cl} = \{r_1, r_2, \cdots, r_n\}, r_n = <V_k, B_k, S_k>$
Reports submitted by miner: $R_m = <c_m>$
W: the sets of winning user coalition
Output: p the payment sets of winning user coalition
initialize $p \longleftarrow \varnothing$
sort W in non-increasing order of B_k': $B_1' \geq B_2' \geq \cdots \geq B_k'$
for all $i \in W$ **do**
$p_i = \theta_i^j \times |B_i| \times c_m$
$p \longleftarrow p \cup p_i$
$W \longleftarrow W \setminus \{i\}$
end for
return p

Algorithm 2: TPRP.

Theorem 9. *Arbitrary user coalition k cannot improve utility by lowering the transaction fee bid in the UCTPM mechanism.*

Proof. Assume when the user coalition k bids the transaction fee b_k to rank r_g and obtains the utility u_{CL_k}, while the lower bid b_k' to rank r_j and obtains the utility u_{CL_k}'.

Therefore, the conclusion can be reached through the above analysis that arbitrary user coalition k cannot improve utility by lowering the transaction fee bid in the UCTPM mechanism.

Theorem 10. *Arbitrary user coalition k prefers to improve unit quality score instead of unit transaction fee bid to improve utility when con_k increases.*

Proof. The user coalition quality score is calculated according to equation (2): $\varphi_k = \left(\phi_0 + \mathrm{con}_k \sum_{m=1}^{n} (tx_k m)\right)^{\mu}$.

When applied substitution as $TX_k \longleftarrow \sum_{m=1}^{n} (|tx_m k|)$, then we can get $\varphi_k = (\phi_0 + \mathrm{con}_k \times TX_k)^{\mu}$. And deriving φ_k to get $\varphi_k'(\mathrm{con}_k) = \mu TX_k$. As φ_k is the monotone increasing function of con_k due to $|tx_k m| \geq 0$ and $\mu \geq 0$, thus $\mu TX_k \geq 0$, so that $\varphi_k'(\mathrm{con}_k) \geq 0$.

Besides, the effect of user coalition contribution degree con_k on transaction fee bid B_k can be written as $b_k' = B_k \times e^{-(\sigma \mathrm{con}_k)}$ according to equation (6).

Same as above, if $B \longleftarrow b_k'$, then $B = B_k \times e^{-(\sigma \mathrm{con}_k)}$ stands, and deriving B to get $B'(\mathrm{con}_k) = -\sigma B_k e^{-(\sigma \mathrm{con}_k)}$. For arbitrary k's transaction fee bid $B_k > 0$, and $\mathrm{con}_k \geq 0$, $\sigma > 0$, thus $B'(\mathrm{con}_k) \leq 0$, so that, b_k' is the monotone decreasing function of con_k. And the inequation $\varphi_k'(\text{con}_k) \geq B'(\text{con}_k)$ shows that the priority ranking that arbitrary user coalition obtains through improving the unit quality score is higher than improving unit transaction fee bid.

Denote the strategy set of user coalition k as $A_k = \{\alpha, \alpha'\}$, where α means the user coalition's strategy of improving the unit quality score, while α' means the strategy of improving the unit transaction fee bid. We only consider the pure strategy action instead of mixed strategy action for simplification; that is, k only chooses one of specific strategies from strategy set A_k. Denote the utility is u_{CL_k} when k chooses the strategy of α to obtain the priority rank r_g, while utility is u'_{CL_k} when k chooses the strategy of α' to obtain the priority rank r_j, thus $r_g \geq r_j$ based on the analysis above. Considering comprehensively with equation (8), it shows that $p_k^j \geq p_k^g$ when $\theta_k^j \geq \theta_k^g$, so that $u_{\text{CL}_k} - u'_{\text{CL}_k} = V_k - p_k^g - (V_k - p_k^j) = p_k^j - p_k^g \geq 0$, which means arbitrary user coalition will not choose strategy of α' to improve the utility. According to the analysis above, the conclusion can be summed up that arbitrary user coalition k cannot improve utility by improving the transaction fee bid in the UCTPM mechanism.

(1) When $b_k' < b_k$, according to Theorem 9, arbitrary k has the utility $u_{\text{CL}_k} - u'_{\text{CL}_k} \geq 0$, which means k cannot improve the utility through lowering transaction fee bid

(2) When $b_k' > b_k$, according to Theorem 10, for arbitrary k prefers to improve the unit quality score rather than unit transaction fee bid for the higher priority rank to improve utility, which means there is no such a k that chooses the strategy of improving unit transaction fee for extra utility when the coalition contribution degree increases

Theorem 11. *The UCTPM mechanism satisfies the attribute of incentive compatibility when con_k increases.*

Proof. Denote the utility of user coalition k is u_{CL_k} when k bids transaction fee b_k, while u'_{CL_k} when k bids transaction fee b_k'.

From the analysis of (1) and (2), it can be proved that the UCTPM mechanism satisfies the attribute of incentive compatibility when con_k increases.

(1) When $xc_k = 1$, which means the transaction set for this user coalition is added into the new block, thus $u_{\text{CL}_k} = V_k - p_k$. And user coalition k's actual payment p_k is not higher than B_k based on equations (8) and (9), so that $p_k \leq B_k$. In addition, $V_k \geq B_k$ holds for users who use blockchain as the transaction platform; otherwise, they prefer the off-chain methods. Therefore, the utility of k is $u_{\text{CL}_k} = xc_k(V_k - p_k) = V_k - p_k \geq 0$

(2) When $xc_k = 0$, which means the transaction set of k is not appended onto the main chain, and also, there is no need for such a k to pay, so that $u_{\text{CL}_k} = 0$

Theorem 12. *The UCTPM mechanism satisfies the attribute of individual rationality.*

Proof. The user coalition k's utility is written as $u_{\text{CL}_k} = xc_k (V_k - p_k)$ according to equation (11).

The conclusion can be summarized from the analysis above that the UCTPM mechanism is individual rational according to analyses (1) and (2).

Theorem 13. *The UCTPM mechanism satisfies the attribute of budget balanced.*

Proof. According to the payment function defined by the UCTPM mechanism for winning user coalition and miner, the sum of all participants in the mechanism is zero; that is, $\text{pro}_m + \sum_{k \in W} p_k = 0$; thus, the UCTPM mechanism satisfies the attribute of budget balanced.

7. Experiment

The simulation experiment codes are implemented in Python language, and the test hardware is Intel® Core™ i5-4200U CPU+4 GB memory, and Windows 10+Python 3.7+Pycharm 2019 are used for the test software. We conduct the simulation experiments to mainly explore two contents based on the researches in this paper: Firstly, the transaction priority ranking results influenced by the UWCTP algorithm are explored. Secondly, the influences of the UCTPM mechanism on transaction processing time are explored. The experimental results show the feasibility and effectiveness of the UWCTP mechanism, and the detailed experimental contents are as follows:

(1) Exploring the influence of the increasing transaction fee and valid transaction volume on transaction priority scores as user coalition contribution degree increases

(2) Observing the influence differences of the UCWTP algorithm and traditional transaction priority algorithm on transaction priority ranking results

(3) Exploring the transaction processing time differences caused by different transaction creation modes (transactions created by a single user and user coalition) under different transaction volumes in the mempool

In order to explore the influence of the increasing transaction fee bid and valid transaction volume on priority results, we generate the transaction fee within the range of

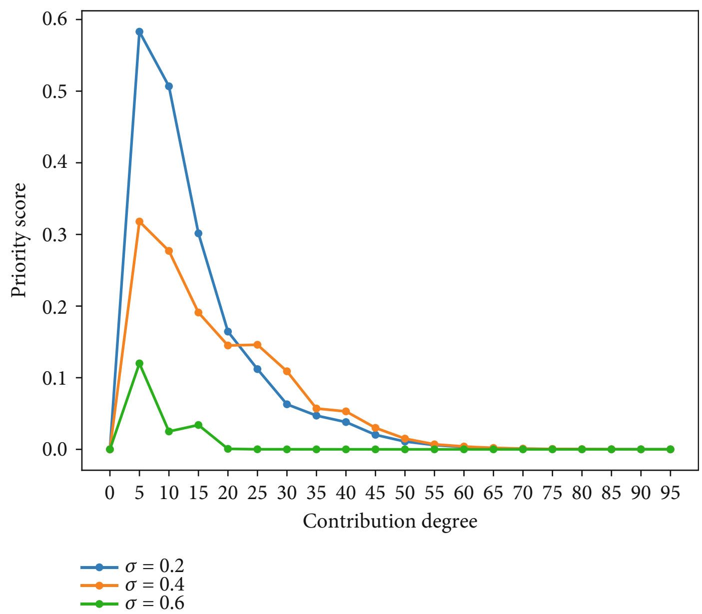

Figure 2: Influence of transaction fee on priority score.

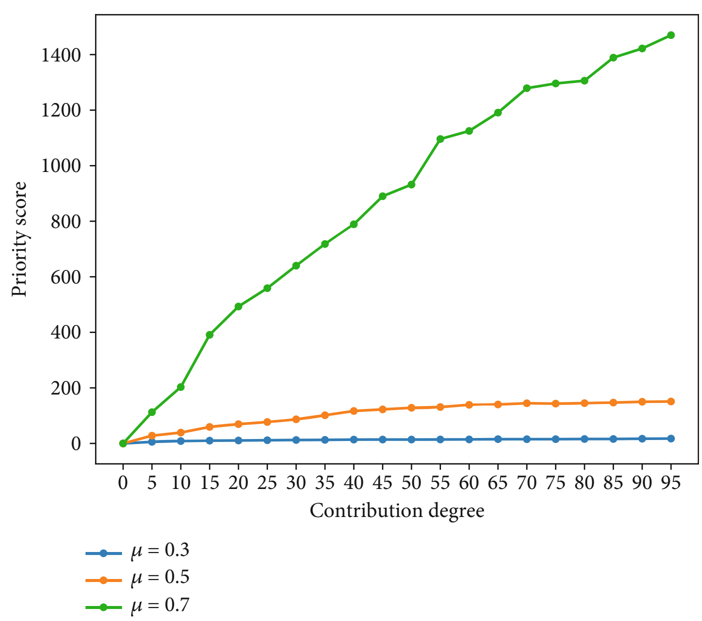

Figure 3: Influence of valid transaction volume on priority score.

[0, 3]/BTC based on the real Bitcoin situation [24] and generate the valid transaction volume within the range of [1, 1000] on the basis of assuming that the maximum valid transaction volume is 1000 in the experimental situation. In all the experiments, the random number generator of Python is used to generate the experimental data, and the average number is applied after the experimental data are generated 500 times with the purpose of reducing the influence of randomness on experimental results. From Figure 2, it can be observed that the priority score corresponds to the increasing transaction fee bid which goes up first, then drops down and tends to 0 as the contribution degree increases with the step of 5, and the results about the transaction fee influence on priority score under different sets of σ share the same tendency. Meanwhile, we conduct the other experiment about the influence of increasing valid transaction volume on the priority score. As the result shows in Figure 3, the overall priority score goes up as the contribution degree increases; besides, the upward trend becomes faster when μ is higher. Moreover, as the value range of the transaction fee is much smaller than the valid transaction volume, there is a huge difference in the score result value, but the result comparison will not be affected; instead, the result value difference indicates that when user coalition increases transaction volume rather than transaction fee bid, the significant higher priority score will be obtained.

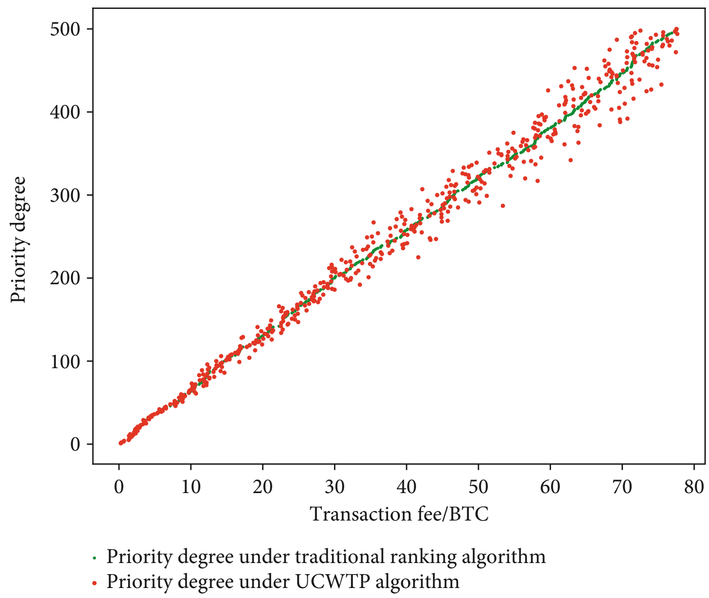

FIGURE 4: Impact of valid transaction volume and transaction fees on priority degree.

In order to make further impact comparisons of the UCWTP algorithm and traditional transaction priority algorithm on the priority ranking results, we conduct the second experiment as the result shows in Figure 4, and we randomly generate 500 transaction fees in the range of [0, 80]/BTC as the user coalitions' transaction fee bid to imitate the actual Bitcoin transaction situation as possible. As it shows in Figure 4, the transaction fee bid is linearly related to the transaction priority degree under the traditional transaction priority algorithm; as a result, user coalition can obtain a higher transaction priority rank through improving transaction fee bid directly. However, with the UCWTP algorithm, the user coalition quality score increases with the growth of valid transaction volume of the user coalition, and the influence of single transaction fee on the transaction priority degree is reduced by an average of 2.34%, and it can be reduced by up to 12.2%; this is mainly because the ranking deviation obtained by the UCWTP algorithm will be reduced when the transaction fee of user coalition is low. However, it is interesting to notice that the impact of a single transaction fee on the priority degree is reduced by an average of 5.17% when referring to the annual ratio of approximately 21.66% for Bitcoin transaction packing (that is, the annual average ratio of the confirmed transactions to the total number of transactions in the blockchain platform from April 2019 to April 2020 [19]).

The experiment results above are consistent with the conclusion of Theorem 10; it is further proved that the arbitrary user coalition can obtain a higher transaction priority rank through improving the quality score when the coalition contribution degree increases; thus, the user coalition prefers to improve the quality score rather than lying to improve the transaction fees on the purpose of optimizing the utility. Besides, the experiment results reflect that the UCTPM mechanism can effectively incentivize users in coalitions to actively participate the blockchain's activities including transaction creation, transaction verification, competition for bookkeeping right, and other activities that help to improve coalition quality scores and contribution degree; sequentially, we believe that the development of the blockchain can be helped to promote in the long run by adopting the UCTPM mechanism.

In addition to the two experiments we conducted for exploring the impacts of the UCWTP algorithm on transaction priority ranking results, we also implement the experiment on transaction confirming process time with the different transaction creation modes. In detail, we set up two different transaction creation modes to conduct the contrast experiments based on the researches in this paper, which are transactions created by a single user and by user coalitions, respectively. Also, the increment step of transaction volumes is set up as 5000 and end up by 60000 in this experiment. Although when compared with the transaction volume in the real Bitcoin situation, the experimental transaction volume is smaller, the experimental results as shown in Figure 5 can still reflect that the overall transaction confirming process time for the transactions created by user coalition is much faster than transactions created by a single user. Under the condition of the increased transaction volume, the transaction processing time of transactions created by a single user grows faster than that of transactions created by user coalition, and the maximum difference in transaction processing time between these two transaction creation modes is up to 6.9347 s when transaction volume reaches 60000. From the transaction processing time growth trend of Figure 5, we predict that if the UCTPM mechanism would be operated in the real blockchain project such as Bitcoin, the overall transaction confirming process time could be significantly reduced with the help of the UCTPM mechanism, because the user coalition transaction creation mode helps to effectively reduce the total time it takes miners to decide which transaction should be packed into a new block under the condition that no other factors affecting transaction confirming process time should be taken into consideration.

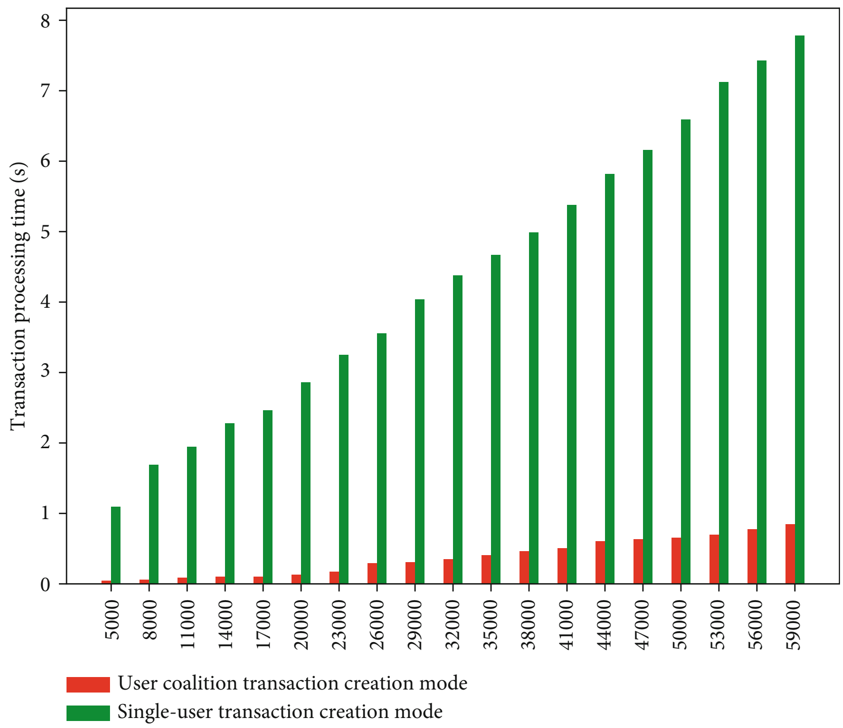

FIGURE 5: Transaction processing time differences between different transaction creation modes.

8. Conclusion and Future Work

Considering the issues of single-user transaction creation modes and limited influence factors on transaction priority algorithms in the current blockchain research fields, we propose a novel pricing mechanism called the UCTPM mechanism to optimize the traditional transaction priority algorithm and enrich the transaction creation modes. In addition, the user coalition quality score, user coalition contribution degree, and transaction type demand degree are introduced into the UCTPM mechanism to reduce the impact of the transaction fee on transaction priority ranking results.

In our proposed UCTPM mechanism, it is proved through theoretical proof and experimental analysis that the UCTPM mechanism can deprive the motivation of user coalition lying the transaction fees for extra utility as the user coalition contribution increases. From the aspect of the UCWTP algorithm, it demonstrates that the UCWTP algorithm can help to reduce the impacts of transaction fees on the transaction priority ranking results by an average of 5.17%, and the impacts can be reduced by up to 12.2% when compared to the traditional transaction priority ranking algorithm. While in terms of the performance of the UCTPM mechanism, the transaction confirming process time is greatly shorter when the transactions are created by user coalition instead of individual users from our related experiment results; it is also confirmed from the theoretical proof that the UCTPM mechanism satisfies the attributes of incentive compatibility, individual rationality, and budget balanced.

Although the outcomes of the researches conducted by this paper provide a new approach for the transaction priority ranking in blockchain, also enriching the modes of user transaction creation, the calculation models of unit reserve price for the miner who is granted the bookkeeping right, and the discount factor when the user coalition reaches certain ranks is not formalized in detail; thus, our future work will focus on the dynamic unit reserve price and discount factor formalization based on the actual blockchain transaction situation.

Data Availability

The (experimental data) data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 61872313, in part by the Key Research Projects in Education Informatization in Jiangsu Province under Grant 20180012, in part by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant KYCX18_2366, in part by the Yangzhou Science and Technology Bureau under Grants YZ2018209 and YZ2019133, in part by the Yangzhou University Jiangdu High-End Equipment Engineering Technology Research Institute Open Project under Grant YDJD201707, and in part by the Open Project in the State

Key Laboratory of Ocean Engineering, Shanghai Jiao Tong University, under Grant 1907.

References

[1] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: a systematic review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.

[2] A. Al Shehabi, *Bitcoin transaction fee estimation using mempool state and linear perceptron machine learning algorithm, [M.S. thesis]*, San José State University Library, 2018.

[3] Y. Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, Yale University Press, 2006.

[4] K. Chung, H. Yoo, D. Choe, and H. Jung, "Blockchain network based topic mining process for cognitive manufacturing," *Wireless Personal Communications*, vol. 105, no. 2, pp. 583–597, 2019.

[5] J. Derks, J. Gordijn, and A. Siegmann, "From chaining blocks to breaking even: a study on the profitability of bitcoin mining from 2012 to 2016," *Electronic Markets*, vol. 28, no. 3, pp. 321–338, 2018.

[6] D. Easley, M. O'Hara, and S. Basu, "From mining to markets: the evolution of bitcoin transaction fees," *Journal of Financial Economics*, vol. 134, no. 1, pp. 91–109, 2019.

[7] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: a systematic mapping study," *Telematics and Informatics*, vol. 35, no. 8, pp. 2337–2354, 2018.

[8] D. Vujičić, D. Jagodić, and S. Ranđić, "Blockchain technology, bitcoin, and ethereum: a brief overview," in *2018 17th international symposium infoteh-jahorina (infoteh)*, pp. 1–6, East Sarajevo, Bosnia-Herzegovina, March 2018.

[9] N. Houy, *The economics of Bitcoin transaction fees*, Gate WP, 1407, 2014.

[10] J. Li, Y. Yuan, and F. Wang, "A novel GSP auction mechanism for ranking bitcoin transactions in blockchain mining," *Decision Support Systems*, vol. 124, p. 113094, 2019.

[11] G. Huberman, J. Leshno, and C. C. Moallemi, *An economic analysis of the bitcoin payment system*, Columbia Business School Research Paper No. 17-92, 2019.

[12] K. Kerem, "Near zero bitcoin transaction fees cannot last forever," in *Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014)*, pp. 91–99, Ostrava, Czech Republic, June 2014.

[13] S. Kasahara and J. Kawahara, "Effect of bitcoin fee on transaction confirmation process," 2016, http://arxiv.org/abs/1604.0103.

[14] S. O. Lavi Ron and Z. Aviv, "Redesigning bitcoin's fee market," in *The World Wide Web Conference*, pp. 2950–2956, New York, NY, USA, May 2019.

[15] M. Malte and B. Rainer, "Trends, tips, tolls: a longitudinal study of bitcoin transaction fees," in *In International Conference on Financial Cryptography and Data Security*, pp. 19–33, Springer, Berlin, Heidelberg, September 2015.

[16] G. Huberman, J. Leshno, and C. C. Moallemi, "Monopoly without a monopolist: an economic analysis of the bitcoin payment system," in *Bank of Finland Research Discussion Paper*, p. 27, Bank of Finland (Suomen Pankki), 2017.

[17] D. Azzolini, F. Riguzzi, and E. Lamma, "Studying transaction fees in the bitcoin blockchain with probabilistic logic programming," *Information*, vol. 10, no. 11, p. 335, 2019.

[18] E. Erdin, M. Cebe, K. Akkaya, S. Solak, E. Bulut, and S. Uluagac, "A Bitcoin payment network with reduced transaction fees and confirmation times," *Computer Networks*, vol. 172, p. 107098, 2020.

[19] BlockchainApril 2020, https://www.blockchain.com/charts/n-transactions.

[20] A. Richard and R. Hitchens, "Efficient power markets," in *Transforming Climate Finance and Green Investment with Blockchains*, pp. 93–98, Elsevier, 2018.

[21] J. Li, Y. Yuan, and F. Wang, "Bitcoin fee decisions in transaction confirmation queueing games under limited multi priority rule," in *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, pp. 134–139, Zhengzhou, China, China, Nov. 2019.

[22] H. Nicolas, *From mining to markets: the economics of bitcoin transaction fees*, GATE WP, 2014.

[23] Y. Yuan and F. Wang, "Blockchain and cryptocurrencies: model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, 2018.

[24] *Bitcoin transaction fees soar 550% in a month, BCH, dash transactions much cheaper*, 2020, October 2020, https://news.bitcoin.com/.