IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 16, 2019, accepted June 29, 2019, date of publication July 8, 2019, date of current version July 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2927257

Decentralization is Vulnerable Under the Gap Game

YIRAN LIU[1], JUNMING KE[1], QIULIANG XU[2], HAN JIANG[2], AND HAO WANG[3]
[1]School of Computer Science and Technology, Shandong University, Jinan 250100, China
[2]School of Software, Shandong University, Jinan 250100, China
[3]School of Information Science and Engineering, Shandong Normal University, Jinan 250358, China

Corresponding author: Qiuliang Xu (xql@sdu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61572294, 61602287, in part by the State Key Program of National Natural Science of China under Grant 61632020, in part by the Major Innovation Project of Science and Technology of Shandong Province under Grant 2018CXGC0702, in part by the Natural Science Foundation of Shandong Province under Grant ZR2017MF021, in part by the Fundamental Research Funds of Shandong University under Grant 2017JC019, in part by the Primary Research and Development Plan of Shandong Province under Grant 2018GGX101037, and in part by the Development and Construction Funds Project of National Independent Innovation Demonstration Zone in Shandong Peninsula under Grant S190101010001.

ABSTRACT The blockchain is the core mechanism of Bitcoin, which is mainly enabled by a distributed consensus mechanism. Essentially, in Proof-of-Work-based consensus protocol, the miners generate a series of blocks to realize decentralization practical. Miners receive two types of revenue: block rewards and transaction fees, in which the reward of block drops off as time goes on. Carlsten et al. defined a mining gap and then Tsabary et al. analyzed the gap game exploring how mining gaps form. In this paper, we analyze the other implications of the gap game. First, it is well known that the security of Bitcoin decentralized consensus protocol relies on miners behaving correctly. The security of the blockchain system will be threatened in case of the consensus mechanism is breached. Therefore, we also described how the gap game impacts the decentralization of Bitcoin and the stability of blockchain. Second, to confirm the implication, we discuss what aspects of decentralization can be impacted by the gap game; then we defined a new decentralization model and listed its main features. In the end, we analyze the block reward capacity in the blockchain and consider the impact on the existing two common block reward systems when the gap game was formed.

INDEX TERMS Blockchain security, decentralization, reward, gap game, mining.

I. INTRODUCTION

The Bitcoin, proposed by Nakamoto et al. [1], realized a monetary system without relying on any third trusted central authority, has been obtaining increasing popularity and acceptance by a wider community. One reason for Bitcoin far-ranging adoption is that a low-cost, decentralized currency is inherently independent of governments and any central authorities.

The blockchain is the core mechanism for the Bitcoin. It relies, among other things, on a network of computers that synchronous transactions with a process called mining. Miners collect transactions and append them to the blockchain, forming a globally-agreed ledger. Instead of relying on a third trusted central authority, the most famous blockchain-based Bitcoin [1]–[3] relies on incentives to ensure security. It uses Proof-of-Work (PoW) [1], [4], [5], requiring participants to solve a difficult computing problem that is hard to solve but easy to verify. The miners who can work out this problem has the right to create a new block.

Systems that use proof of work rely on the assumption that at least 50% of computational work invested in mining is by honest participants [1]. To stimulate miner's participation, this cryptocurrency system provides them with block rewards. In addition, the miners who created a new block can also get transactions fees, paid from handling transactions. This system is designed to ensure participants to follow the protocol rules, and if they don't obey this rule, their profit will be decreased.

When we talked about the Bitcoin is a decentralized system,we have mentioned that the Bitcoin uses a proof of work scheme as It's block generation strategy to realize the control of the block, and thus renders decentralization practical [6], [7]. The use of proof of work to eliminate the

The associate editor coordinating the review of this manuscript and approving it for publication was Yinghui Zhang.

central party and to decentralize and secure ledger. However, this is not always the case for the Bitcoin System. Some prior works show that the vital operations and decisions that Bitcoin is currently undertaking are not decentralized [8], [9]. On the one hand, mining and block creation is currently largely centralized. On the other hand, other Bitcoin operations, like protocol updates and event handling are controlled by a small number of administrators whose influence depend on their function within the system.

The security of Bitcoin decentralized consensus protocol relies more upon miners behaving correctly. If they obey the rules, they will get mining revenues under the assumption that they are rational. Miners can receive two types of revenue: block rewards and transaction fees. The former rewards for the large majority of miner revenues now, but in the future, it is expected to transition to the latter as the block rewards decreased (it's halved every four years). There has been an implied belief that whether miners are paid by block rewards or transaction fees does not affect the security of the blockchain. In [10], they show that this belief is not correct. They analyzed if without a block reward, immediately after a block is found there is zero expected reward for mining but nonzero electricity cost, making it unprofitable for any miner to mine. This phenomenon is called mining gap. Explicitly, this would have a negative impact on Bitcoin security. This is due to the effective hash power in the network would decline, and it would become easier for a malicious miner to fork.

In [11], they defined and analyzed the gap game exploring how mining gaps form as a function of subsidy and fees, they also use EBRR denote the ratio of the expected base reward and the expected accumulated fees, and show that EBRR $\approx$ 6 is sufficient to avoid mining gaps in presented scenarios, indeed, they show that gaps form well before fees are the only incentive. Then they analyzed the implications on security. Surprisingly, we also discover the formation of gap game reduces the decentralization of Bitcoin.

We consider our main contributions to be the following.

1) Firstly, to our best knowledge, there are hardly any researches in decentralization model. Therefore, to confirm our implication that the formation of the gap game threatens the decentralization of Bitcoin, we defined a new decentralization model and listed its main features. They represent three levels of the decentralized model: fairness, liveness, and security.
2) Secondly, We depicted the mining model and gap game to describe the possible behaviors of Bitcoin users and miners when the gap game of Bitcoin is formed. That is, as the reward of the entire Bitcoin shift from block rewards to transaction fees, the miners and users in Bitcoin will engage in those behaviors. With the effects of these behaviors on the decentralization system that are also analyzed. Afterward, we discuss what aspects of decentralization can be impacted by the gap game. And then we also analyzed the impact of the formation of gap game on the security of the Bitcoin system and the stability of the blockchain structure.
3) In the end, we analyze the block reward capacity in the blockchain and consider the impact on the existing two common block reward systems when the gap game was formed.

We proceed as follows: after introducing the relevant work (Section 2), we propose our decentralization model and mining model (Section 3 and Section 4). Then, we analyze how the formation of gap game impacted on decentralization model of Bitcoin. In particular, we consider the behavior of miners and users when the gap game is formed. And other influences on Bitcoin security and blockchain stability (Section 5). And blockchain reward capacity (Section 6), mainly considered two reward systems about the mining pool. We then give some evaluations about the formation of gap game (Section 7). In the end, we come to some conclusions (Section 8).

II. RELATED WORK

In recent years, a number of models to issue the block reward have been proposed. At the beginning of white paper [1], the composition of reward is simply explained, and the idea of incentives is presented intuitional. Eyal and Sirer [12] show an abnormal mining strategy named selfish mining, by which an attacker increases her relative reward. Sapirshtein et al. [13] both show more complicated variations of the original selfish mining attack that increase the attacker s reward when applied.

Other work by [14] shows mining pools are incentivized to allocate some of their mining rigs to sneak on other mining pools. It also concludes that an equilibrium exists were two pools steak on one another, in which they both end up losing compared to the situation if they did not attack at the beginning. In [15], they combine selfish mining with infiltration attack. All of the above works we illustrated, they all consider a model that block reward are the main incentives for the miner to mine. However, the expenses are not considered at all. In our work, we take into account not only the reward the miners will receive but also the expenses they spend in mining. We define a different mining model in which the miner's expenses is determined by different mining strategies that miners use.

The work by Babaioff et al. [16] discuss incentives for generation transactions in a cryptocurrency network. They analyze several reward schemes to incentivize participants to distribute transactions in the network. Moser and Bohme [17] review and analyze the history of transaction fees in Bitcoin. In our work, we analyze a reward scheme where participants can get rewards for mining with non-negligible expenses.

In [10], they analyze Bitcoin with no block reward and only incentivized by transactions fees, in a model where the block capacity is limitless. In this model, there are no remainder fees after the new block is generated. Not only that, they improved selfish mining and showed a new version that was more suited to the transaction fee as the main incentives. In their work, they propose a hypothesis called the formation of the mining gap. The mining gap is a period of time when

miners shut down mining rigs to reduce mining expenses. When such mining gap exists, the mining power utilization of the network is sub-optimal.

In [11], they present a model to analyze miners' profits and use it to show that mining gaps do form. Their model holds for both bounded and unbounded blocks, as well as for combinations of subsidy and fees as part of the block reward. They present a model that is in a quasi-static state. That means no miners join or leave, existing miners maintain their behavior and the system reached equilibrium. They also conclude by showing that with sufficient initial block reward, all miners are incentivized to resort to the default mining strategy. However, this work using a quasi-static state to quantify parameters. This is dependable since the parameter of Bitcoin is changing all the time. In our work, we analyze a dynamic state and we also show that rational miners will form coalitions to increase their profits, result in decentralization is being attacked.

Adem et al. [8] analyze decentralization in Bitcoin and Enthereum. They provide new tools and techniques for measuring blockchain-based cryptocurrency networks. What's more, they perform a comparative study of decentralization metrics in Bitcoin and Ethereum. Arthur et al. [9] show that the vital operations and decisions that Bitcoin is currently undertaking are not decentralized. And they explore possible solutions and recommendations to enhance the decentralization in Bitcoin. In our work, we propose a decentralized model that suits our mining model. Then we study the relationship between gap game and decentralization. Meni [18] describe the various reward systems used to calculate rewards of participants in Bitcoin mining pools.

III. DECENTRALIZATION MODEL

In the traditional centralized transaction system, each transaction must be verified by a central trusted institution (e.g., the central bank), which inevitably leads to the cost performance bottleneck of the central server. In a Bitcoin decentralized system, the payment process is completed through Bitcoin transfer Bitcoin coins (BTCs) to generate transactions between each participant.

The Bitcoin block contains several transactions. These transactions are broadcast all over the blockchain network. To prevent double-spending attacks in Bitcoin, Bitcoin uses a proof-of-work mechanism (PoW) [1], [4], [5]to generate new blocks. Specifically, participants must find a value to solve a difficult computing problem [1]. If this problem can be solved, this participant has the right to generate a new block. The new block is then broadcast to the network and other participants can verify the validation of the block as well as those contained transactions. On successfully generating a new block, participants currently receive a certain amount of BTCs and transaction fees included in the block. This motivates participants to keep the Bitcoin running well. The newly created block will be forwarded to all participants in the Bitcoin network, and the remaining participants can check its correctness by verifying the hash computation. If the newly generated block passes validation, the participants attach the new block to the previously generated block.

The initial design goal of the Bitcoin is to make the transaction generation and confirmation process completely decentralized. However, operations at Bitcoin will only work in practice if the majority of the computing power in the network recognizes the decisions made in the Bitcoin. But in fact, participants with more computing power in the Bitcoin control the currency.

We conclude the factors of the decentralization [8] system. Here we list three features of the decentralization model.

1) **Fairness**

   Mining in a Bitcoin network is a complex process that typically requires strong computing power. Nevertheless, so long as there are many different groups mining in the Bitcoin, the whole system remains decentralized. For a decentralized system, participants should join or leave the system unaffected by external factors. In other words, Participants voluntarily enter or exit the decentralized system. If none of the participants wanted to form a decentralized system, there would be no decentralized system. So the willingness of the participants is very important.

   Therefore, in a decentralized Bitcoin system, participants who would like to start a new mining activity must have enough incentives to participant mining work and join any pools that he likes. And not only that, miners who are already involved in mining pools can also stop at any time if they don't want to continue for some reason.

2) **Liveness**

   We use fairness to describe voluntary action of miners to join or leave the pool. As for decentralized systems, once a participant enters the system, he has the right to vote on the decisions of the system. Not only that, but participants must ensure that their votes are fair and reasonable. Now we consider that when the miners enter the pool, they have the right to vote as part of the pool and they must ensure that the results of the voting are fair and impartial. Only if the miners abide by the rules and correctly use their right to vote can the pools be maintained.

3) **Security**

   In a decentralized system, if some malicious actors want to control the whole system, the system must ensure that the decisions of these malicious actors are not adopted. We call this feature is security. In some scenarios, the developer must take action on issues that may cause conflict. In addition, the process must be completely transparent and subject to strict supervision. So in the Bitcoin, participants must promise to make transparent decisions.

   In other words, if there are some malicious miners who want to change the honest miner's decision, such behavior is unlikely to succeed. Only in this way, the whole Bitcoin will become more secure. As a result,

the situation for malicious miners in the Bitcoin will become tougher, and they can hardly change Bitcoin's decision.

In this section, We summarize three main characteristics of a decentralized system. Fairness describes the freedom of participants to enter and exit a decentralized system. For the Bitcoin system, miners join or leave the pool to follow their own will. Liveness describes the state of a participant after he enters the decentralized system. When he enters the decentralized system, he possesses the right to vote on the events of the system. Moreover, he must guarantee the fairness and impartiality of his voting results. For the Bitcoin system, once a miner comes to the pool, he has the right to vote on decisions made inside the pool, and he has to make sure that his voting result is correct. Security also describes a feature within a decentralized system. In a decentralized system, this is not possible if there are malicious actors who want to try to change the decision of the entire system. As for the Bitcoin system, if a malicious miner wants to change the voting decision of the entire Bitcoin system, the decentralized system must ensure that the idea of the malicious miner cannot be realized. Only when a system satisfies the above three properties can it be called a decentralized system.

For any adversary $\mathcal{A}$ with less than ϵ power, then:

$$1 - Pr\left[\begin{array}{c} L^{\mathcal{A}} \overset{accept}{\longrightarrow} L^{S(i)} : S(i) \leftarrow S \wedge \\ power(L^{S(i)}) > power(L^{\mathcal{A}}) \wedge \\ decision(S) \overset{unchange}{\longleftarrow} \mathcal{A} \end{array}\right] \leq f(\epsilon) \qquad (1)$$

where $f(\epsilon)$ is a function depends on adversary's power and it decreases sharply when ϵ decreases.

Naturally, a decentralization system should be fair, live and secure. The definition of the decentralization system is straightforward: As showed in Fig 1. We use L denotes decentralization, S for the set of all the miners, $S(i)$ for the subset of all the miners, and $\mathcal{A}$ for all the possible adversaries. So the above inequalities (1) says that the probability of all events that do not satisfy the decentralized behavior is not exceeding $f(\epsilon)$. Event 1 means that if a subset $S(i)$ is selected from any set of miners, as long as the subset satisfies the three characteristics mentioned above, then The decentralized system will accept this subset of miners. Event 2 shows that the voting power of the set of any adversaries $L^{\mathcal{A}}$ is less than that the power of subset of miners. Event 3 indicates that any set of adversaries want to change the voting result is impossible. If the probability of all events that affect decentralization is less than $f(\epsilon)$, we can call this system is a decentralized system.

IV. THE MINING MODEL

We introduce a mining model [11] that we use throughout our rest work to describe Bitcoin mining process. Therefore, the model is composed of a number of miners and a number of mining rigs. Every miner have a number of mining rigs and control at least one rig and one rig is only controlled by one miner.

Every rig has two states: off and on. Each miner allocates a start time to each rig, on which the rig is opened. In case of a rig is opened, the time for finding a valid block in proportion to the hashing power rate of the rig, among all mining rigs [1], [12], [13], [19]. As a consequence, the time to find the first block is the smallest time of all different rigs finding time. Since the value of the difficulty parameter and the block time interval is also a constant value determined by the system. The difficulty parameter indicates the difficulty of the hard computing problem. The value of the difficulty parameter is influenced by the miner's open time of specified rig. If the newly generated block founded time is too fast or slow, the agreement will adjust the difficulty parameter to make the block interval time as suitable as before. The block reward of miners is controlled by the rigs which first find a new block. The block reward consists of two parts. The first part that is transaction fees that we showed before. This part of the reward is determined by time. As the number of transactions in the Bitcoin increases, the rewards for this segment will continue to increase. The second part is the block reward. Especially, only the miners controlled rigs that find the block would get the reward, and the rest of the miners are not rewarded.

The miners involved in the Bitcoin will incur some expenses. These expenses can be divided into two forms [11]. One is capital expenses (capex) that miners who are owing rigs must spend whether the rig off or on. The other is operational expenses (opex) which miners are paid for having rigs mining. Particular, these fees will be paid regardless of whether the miners succeed in mining new blocks. In Bitcoin, the process of generating blocks is always going. When a new block is founded, all miners will go to look for the next one. The difference value between a miner's income and his expenditure is his gain. They will make efforts to increase their earnings if the miners are rational.

V. THE GAP GAME AND ANALYSIS

In [11], they formed a game could be formalized before the block reward goes down to 0, that is, the gap game. The strategy of players' is to select the start time of all their rigs. All players can choose the start time first. We define a participant's earning as his expected income, that is, his expected income minus his expected expenses. In this model, the system is composed of k rigs controlled by n players. Note that turning rigs down is irrational behavior. This means that the probability that the rig will find the block at some interval is not affected by how long it has taken the miner to start mining. Thus, the chance of a single rig finding a block does not decrease over time. Not only that, but the block rewards also increase over time.

The parameter values are affected by lots of factors, affected by different resources. The fees are influenced by system participants and market state [17]. The block reward is also affected by market state and system participants. Indeed, it is also affected by mining rate which depends on the protocol in the system. Capex is influenced by factors such as

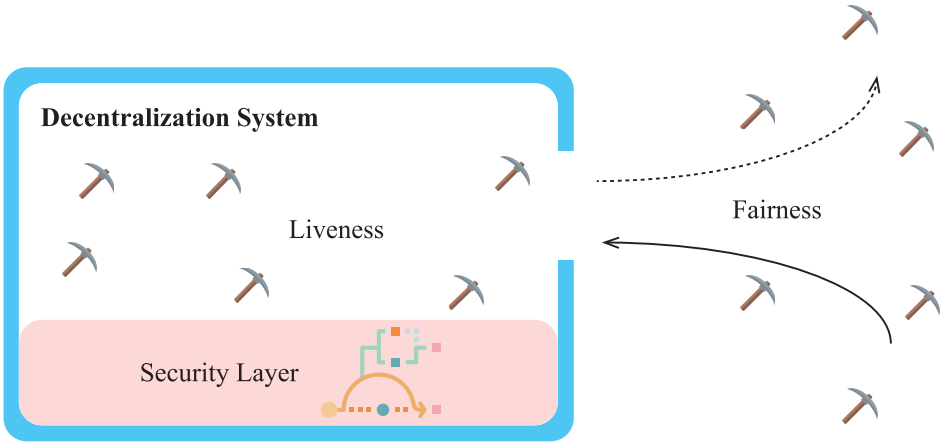

FIGURE 1. Decentralization System: fairness means the freedom of miners join(leave); liveness means the voting power of internal miners and the security means the unalterability of the honest miners' voting result.

mining rigs efficiency, personal salaries, and actual personal cost. Opex is mainly influenced by the electrics cost used by mining rigs. This expenses not only include the cost of solving the hard difficult computing problems but also include the fees that maintain rigs normal operation. As a result, these parameters are not only difficult to estimate, but they are also different for various cryptocurrencies. Moreover, even for the same cryptocurrency, their values change with time. Therefore, when we study these parameters, we focus on the trends that are robust of the parameter range [11]. More specifically, in [11] they use the concrete number to calculate when the gap game could spring up, when $EBRR \approx 6$, that is, the ratio of the expected base reward and the expected accumulated fees closes to 6, the Bitcoin network will emerge the gap game.

However, this research uses the current parameters to calculate this *EBRR*, this is not dependable, because the parameters of the Bitcoin network keep changing all the time, after a long time, it will be another case compared to now. For example, if the Bitcoin only remains 1 rig, that means, the Bitcoin only have one miner to mine the block, and the Bitcoin doesn't need other fees to maintain its tasks. The *EBRR* must be less than 6.

We don't yet know the adjustment of the Bitcoin network in the future, because the Bitcoin changes at every moment. Here we modeled a simplified version of the gap model to simulate the gap game.

There are k rigs in the Blockchain, each rig costs b BTC per time unit in electricity to run, each block contains m rewards, where $m = 0$ is the transaction fees model, that means, only transaction fees could reward miners and no base reward. The transaction fees reward arrive continuously at a rate of r per time unit. When the current difficulty coefficient of mining is determined, the expected time of mining blocks is t.

In the present, the Bitcoin network complies with the following Inequality (2):

$$kbt \leq m_1 + rt_1 \tag{2}$$

where t_1 means the transaction fees have been happening for t_1 time units before the start mining time and m_1 means the block reward at t_1 time units, because $kbt \leq m_1$, the miners do not need to wait, they just start mining when the previous block was mined. The whole process continues t time units.

However, when the gap game appears, the Bitcoin network complies with the following inequality (3):

$$kbt \leq m_2 + rt_2 \tag{3}$$

where t_2 means the transaction fees have been happening for t_2 time units, after t_2 time units, the miners start mining and they will find a block in t time units, the whole process continues $t + t_2$ time units. Because $kbt \geq m_2$ that means current rig cost is larger than the block reward, so the miners have to wait for t_2 time units until $kbt \leq m_2 + rt_2$, this is the reason why the gap game formalized.

From the above analysis, we could know the gap game's time t' could be represented as follows (4):

$$t' = \frac{kbt - m}{r} \tag{4}$$

When t' is negative, it indicates there will not have the gap between the two blocks, which is the current situation.

Now we use Bitcoin capacity to analyze how the gap game will influence the decentralization.

A. BITCOIN USERS

Due to the decline of the block reward, the Bitcoin users have to increase each transaction fees to let the miners choose their transaction. This is because miners prefer to deal with transactions with high transaction fees. And this has led to an increase in transaction fees across the Bitcoin. Meanwhile, because of the very small size of the block, many small transactions can be delayed because miners prefer high-fee transactions. However, larger block sizes will slow down propagation and cause blockchain forks. We can predict that when the transaction fees increase to a point where it exceeds the ability of some Bitcoin miners to pay, they will leave

Bitcoin and stop transactions. In section 3, we discussed the decentralization model of the Bitcoin. And we list some factors about the decentralization model. Bitcoin users are free to participate in the system and free to leave. But in the setting we just described, transaction fees in the system are rising and may exceed the ability of most users to pay. At this time, most users may choose to leave the Bitcoin because they cannot afford the high transaction fees. The decentralization of Bitcoin will be affected.

B. BITCOIN MINERS

What's more, for a large k, every mining rig belongs to Bitcoin miners can get a small share of the reward $n+ft_2$. Few fees reward can break the balance between mining rigs and miners. There are two main problems with this phenomenon. On the one hand, the miners would refuse other rigs to join the Bitcoin network. This is because the fees reward in the network is already very small, if there are other rigs to join, these miners will be their share of the already small reward, so they refused to join these new miners. On the other hand, the other rigs would refuse to join the Bitcoin network due to the limited rewards. For period passes, the miners would gather as one pool and the other rigs would be rejected to join the mining pool. When that happens, it means that most of Bitcoin mining power may be controlled by in a large group. Maybe rational miners are ought to form small groups to increase their gains, leading to a centralized system. Worse still, the miners could monopoly the mining process, which is not good news for the whole Bitcoin.

In summary, we analyze the impact of gap game on Bitcoin decentralization from the perspective of Bitcoin users and miners. For Bitcoin users, the formation of the gap game leads to a reduction in block rewards, and the user must increase the transaction fees in order to make miners to choose his own transactions. Only then will the miners handle their own transactions. However, some users have limited financial resources and do not have enough capacity to pay high transaction fees. When this happens, these users will opt out. Once this happens, the decentralization of the system will be affected by the user's participation or logging out. For miners, if some miners have enough mining rigs to mine, once the gap game is formed, the amount of reward will be reduced, and the reward that each miner can get will be less than before. At this point, the accession of new miners will inevitably reduce the number of rewards for existing miners in the system, so the existing miners in the system do not want new miners to join. For miners who want to join the system, the new accession to the system will not bring them considerable rewards. On the contrary, the cost of maintaining the operation of the mining rigs may far exceed the reward for successful mining. In addition, when the gap game is formed, the miners in the system are more likely to aggregate into a coalition (that means some miners banded together for acquiring more benefit) in order to get more revenues by the hook. If the power of this coalition that is comprised of rational miners is too large, and their incentives are to deviate the honest protocol operation. Ultimately, the decentralization of Bitcoin will be seriously threatened.

Although the formation of gap game has affected miners and users behaviors, the impact of gap game goes far beyond that. Below, we will analyze the impact of this formation on the security of the entire Bitcoin system and the stability of the blockchain.

1) **Potential Attacks**

Most of the reasons why Bitcoin can achieve decentralization are due to the existence of the consensus mechanism. And the security of Bitcoin relies on the distributed consensus mechanism achieved by the mining game. In our analysis thus far, we have assumed, as the Bitcoin miners do, they will form a coalition. Over time, If their overall mining computational power exceeds 50% of the total network, they may develop into a cartel of miners [20]. They naturally showed what a mining cartel could do if one ever comes to exist. A cartel can change any rules which are enforced by consensus and miners who are not in the cartel will likely be obliged to follow. For example, a cartel can choose any strategy in the mining game. Miners who continue to use the old strategy risk having their newly-mined blocks ignored as forks of the consensus branch and thereby risk losing the mining reward payments associated with those blocks. Thus, if the cartel announces its mining strategy, it can shift the equilibrium chosen by the non-cartel miners. Bitcoin has value because people are willing to exchange it for goods and services. If users are unwilling to use Bitcoin for transactions and consumption because they fear their payments will be invalid, the value of Bitcoin will disappear due to users' distrust.

Not only that, but it can also lead to another attack that calls selfish mining [12]. They show that even nodes with less 51% power are still dangerous. Selfish-Mining allows a pool of sufficient size to obtain a revenue larger than its ratio of mining power. This strategy resulted in honest miners following the Bitcoin protocol wasting resources on mining, but ultimately getting nothing in return. So selfish miners tend to get more revenue. Rational miners will be attracted to join the selfish pool and the selfish can exceed 51% power quickly. In [19], they showed that for small miners, there is more to be gained and profitable from some selfish mining strategies than simply selfish mining. Although the gains are very small. Furthermore, it also shows that attackers with less than 25% of the computational power can still gain from selfish mining. At this point, when the gap game was formed, miners are more motivated to launch some attacks by any means to obtain higher revenues. In the end, the Bitcoin system ceases to be a decentralized currency.

2) **Influence for Blockchain**

Therefore, when the gap game is formed, there will be some serious problems in some cases, which will

seriously threaten the whole Bitcoin system. So when this kind of conflict and threat exists, the developers of Bitcoin will take some measures to maintain the normal operation of the Bitcoin system. A Bitcoin developer is a programmer who maintains the source code for Bitcoin. We can imagine what measures the Bitcoin developers will take to make up for the impact of the formation of the gap game on the Bitcoin system.

If some developers want to increase transaction fees to maintain the normal income of miners, however, some developers do not agree with this practice, because they are afraid that the increase of transaction fees will make small transactions gather together and form a mining pool, threatening the stability and security of Bitcoin. As a result, differences of opinion among developers will lead to a fork in Bitcoin. For example, Bitcoin and Bitcoin cash [21]. At first, Bitcoin and Bitcoin cash were both Bitcoin, but one day, Bitcoin's developers had different opinions. These divergences of developers led to different developers designing two different versions of the mining software. The two versions are incompatible, so miners cannot communicate with each other. So it is impossible for the miners to put an end to the bifurcation. This kind of fork is called a hard fork. A hard fork [22] refers to a permanent split in the blockchain, where an old version does not accept a legal block created by a new version and considers a legal block created by a new version to be illegal. So clearly hard forks are not forward compatible. The other kind of fork is called the soft fork. Soft fork forward compatibility, the old version will accept the block created by the new version, in the soft fork, the miners only need to upgrade to the new version, users can continue to use the old version of the protocol, they will still accept the block created by the new version of the protocol. So the soft fork is not ''real'' fork. The end result of the fork is bound to be some fluctuation in the intrinsic value of the Bitcoin.

If all the developers agree that the gap game will have a huge impact on Bitcoin. They decided to modify the consensus mechanism of the whole system and change the existing proof-of-work (PoW) mechanism into the proof-of-stake (PoS) mechanism. The concept of coinage is introduced into the proof-of-stake (PoS) system [23]–[25] . The coinage of a person is related to the amount of money he has and the time he holds the coin. As a result, the more Bitcoin you have and the longer you keep them, and the more likely you are to generate a new block. Therefore, in the PoS system, there are no mining rigs. It solves the monopoly problem of the large computational power mining pool, and there is no mining gap problem as well. Therefore, the change of consensus mechanism can reduce or even eliminate the influence brought by the formation of a gap game.

To sum up, the formation of gap game has exerted a significant impact on the existing Bitcoin system. On the one hand, it has compromised the decentralized nature of Bitcoin by making it easier for miners to launch attacks on the system. On the other hand, it also has a significant impact on the blockchain. The formation of gap game may lead to the divergence of opinions among Bitcoin developers, which may result in a fork of blockchain or change of system consensus mechanism.

VI. BLOCKCHAIN CAPACITY

At present, Bitcoin is often referred to as the first cryptocurrency and one of the most hotly discussed cryptocurrencies, which has achieved great success. The blockchain is the main mechanism for the Bitcoin. In previous work, when they talked about blockchain capacity, they mostly mentioned block capacity, but the capacity we are going to talk about is the capacity of the reward in the whole Bitcoin. An important aspect of the design of Bitcoin is mining, in which participants expend resources to solve difficult computing problems and get rewards. When this difficult problem is resolved, it allows a valid block to be generated, for which the miner will receive a certain amount of Bitcoin.

Our analysis is based on [18], they describe some Bitcoin mining systems and analyze their advantages and disadvantages. In our work, we will analyze the impact on the two reward systems when the gap game is formed. When a valid block is generated, the miner who finds the block will receive an amount of Bitcoin rewards, which is represented by B. We use D to represent the difficulty coefficient, which is periodically adjusted by the system. In [18], we know that there are many problems with solo individual mining. Therefore, we only consider the pools reward system, where several miners work together to find new blocks and distribute rewards according to the contributions of miners [18]. If the total hashrate of all miners is H, a single miner with hashrate is:

$$h = qH \tag{5}$$

q is the ratio of the pool's total power contributed by the miner. Each pool is managed by a pool operator who may be required to charge a service fee for the service. This is usually a fixed percentage of f of the block reward. Therefore, for each block was found, the operator will charge fB and the remaining $(1-f)B$ will be allocated to the remaining miners.

Now we will consider what happens to two simple reward systems [18] when the gap game is formed. The first is the proportional system, which is the most intuitional system to embody the principles of pools mining. The payment is calculated built on the division of the round in this system, where the round is the time interval between the new block foundation and the previous block. A new block will be generated at the end of each round. As a result, the mining pool can get the reward of B, the operator will retain the cost of ρB, meanwhile, the remaining $(1-\rho)B$ will be distributed among the remaining miners. The amount of reward will be

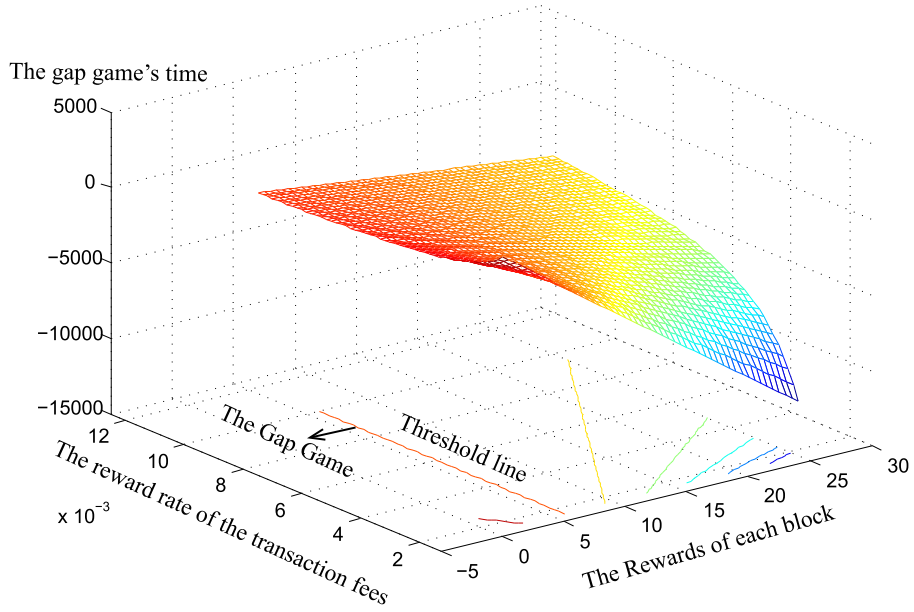

FIGURE 2. The simplified version of the gap game. The block reward from 0 to 25, and the rate of the transaction fees from 1/600 to 1/100, the block reward equal to 6 is sufficient to avoid the gap game.

proportional to the shares submitted by the miners during this round. If a miner submits n shares in this round and the total amount of shares submitted in this round is N, then the miner's reward during this round could be denoted as $Re(\frac{n}{N})$:

$$Re(\frac{n}{N}) = \frac{n}{N}(1-\rho)B \tag{6}$$

In case that the list of miners and the hashrate of each miner are fixed, then the number of shares the miner submits in each *round* will be proportional to his hashrate. Therefore, the expected reward on the number of shares submitted per share is:

$$(1-\rho)pB \tag{7}$$

Each share has a probability of $p = \frac{1}{D}$ to be a valid block. Thus the average rewards per share are $(1-\rho)pB$.

In the case of a fixed number of miners in the mining pool, when the gap game is formed, according to our previous analysis, we can know that the reward of the whole mining pool is reduced, which will reduce the average reward of each share. For the miners internal the pool, their expected reward will be reduced, and even these rewards cannot support the expenses (including Capex and Opex) of their rigs. For external miners who want to join the pool, the average reward from the pool is reduced, making the pool less attractive to outside miners. As time goes on, the pool becomes less attractive, and even some of the internal miners have done everything possible to increase their rewards, reducing the due reward for the rest of the honest miners. Still not only such, but the fact that the internal miners want to leave and the external miners don't want to join will undermine the points of the decentralization model that we proposed earlier.

Another type of reward system is called pay-per-share (PPS) [18]. In the PPS system, the operator works with participants to reduce personal variance. Either way, many blocks are finally found, when a miner submits a share, he is immediately rewarded with $(1-\rho)pB$, amount to the expected value of this share's reward minus fees. However, this system has several advantages for miners. And this is the most dangerous reward system for the pool operator because the operator can offer zero variance to the miners, but he must balance all the variance by his own revenue. So in order to compensate risk, the operator will charge more fees than the other methods, which is the disadvantage of the PPS. But if the operator does not properly balance the pool fees with his financial revenues, the pool is likely to go bankrupt. As derived in [18], with the bankruptcy probability below δ, the operator should keep a reserve of at least:

$$R = \frac{Bln\frac{1}{\delta}}{2\rho} \tag{8}$$

For PPS reward system, when the gap game is formed, the block rewards B in the pool keep decreasing. More than that, with certain bankruptcy probability δ, the operator's reserve R is also decreased. In this case, the operator revenues are reduced, the formation of the mining pool is easier than before. Nevertheless, when the gap game is formed, the formation of a mining pool is effortless. Combined with these changes in the PPS system, the formation of the large pool is accelerated than at any time. And the formation of the large mining pool will pose a fatal threat to the decentralization system.

VII. EVALUATION

From the above analysis, we could learn that the gap game is detrimental to the decentralization system. Meanwhile, the gap game also damages to the other aspects of the decentralized system. What's more, the original features of the decentralized system may also be harmed due to the gap game. Now we refer the parameters from [11], to simulate the gap game in our proposed simplified version of the gap game.

We use the result: EBRR = 6 is sufficient to avoid mining gaps in the presented scenario. And we put into the block reward from 0 to 25, and the rate of the transaction fees from 1/600 to 1/100.

We illustrate the result as Fig 2. The vertical axis is the expected time of mining blocks, due to the lower block rewards, the time of mining blocks is increasing, which means, the miner is waiting for the sufficient transaction fees to support the expenses of the mining process. The Threshold line is when the reward of each block equals to 6, all of the blocks with the reward greater than 6 does not have the worries about the gap game. Conversely, the gap game will be formalized if the reward of each block is less than 6, especially when the reward rate of the transaction fees is less.

We could summarize the findings from the simplified version of the gap game, the Bitcoin system has to increase the transaction fees or inspire the users open up the new transaction for the sake of mitigation of the gap game, however, we have discussed this before, this will let the Bitcoin users out of the system, which is harmful to the decentralization of the Bitcoin system. Another way to make the gap game retarded is that the Bitcoin miners should leave the Bitcoin system to let the expense of the mining process get lower, which is not a good situation for a decentralization system. From the above analysis, we could learn that the gap game is detrimental to the decentralization system.

VIII. CONCLUSION

In this work, we defined the decentralization model and the mining model based on [11]. For the decentralization model, we summarize the three main characteristics; And for the mining model, we analyze some possible behaviors of mining pool miners and users in the Bitcoin during the gap game. In addition, we analyze the impact of these behaviors on our decentralization model. Not only that, but we also analyzed the potential attacks on Bitcoin by malicious miners due to the reduction of block rewards after the formation of the gap game. And this formation may also lead to the instability of the blockchain structure and changes in the consensus mechanism. In the end, we talk about blockchain reward capacity, also analyzes the impact of the formation of gap game on two common reward systems in Bitcoin, namely, proportional reward system and pay-per-share(PPS) system.

Hence, we can come to some conclusions. First of all, the block reward (the same meaning as the base reward) is critical for Bitcoin security, especially for the decentralization of Bitcoin. The formation of the gap game will decrease the block rewards in Bitcoin, thus undermining the freedom of miners and users to participate in the Bitcoin, and ultimately undermining the decentralization nature of the whole system. Secondly, With the continuous formation of the gap game, the Bitcoin reward system will change from block reward to transaction fees. The existing Bitcoin reward system will be seriously affected, and the transaction fee system seems harder to analyze equilibrium than a block reward system. Therefore, it is urgent to take certain measures for the formation of the gap game.

ACKNOWLEDGMENT

The authors would like to thank Xiangfu Song for comments and suggestions.

REFERENCES

[1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://bitcoin.org

[2] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, 2014. [Online]. Available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[3] C. Lee. (2011). *Litecoin-Open Source P2P Digital Currency*. [Online]. Available: https://litecoin.com/en/

[4] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Advances in Cryptology—CRYPTO*, E. F. Brickell, Ed. Berlin, Germany: Springer, 1993, pp. 139–147.

[5] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols," in *Proc. IFIP TC6/TC11 Joint Work. Conf. Secure Inf. Netw., Commun. Multimedia Secur. (CMS)*. Deventer, The Netherlands: Kluwer, 1999, pp. 258–272. [Online]. Available: http://dl.acm.org/citation.cfm?id=647800.757199

[6] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 104–121.

[7] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[8] A. E. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. G. Sirer, "Decentralization in bitcoin and ethereum networks," in *Proc. Financial Cryptogr. Data Secur. Conf.*, May 2018.

[9] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is bitcoin a decentralized currency?" *IEEE Security Privacy*, vol. 12, no. 3, pp. 54–60, May/Jun. 2014.

[10] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the instability of bitcoin without the block reward," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2016, pp. 154–167. doi: 10.1145/2976749.2978408.

[11] I. Tsabary and I. Eyal, "The gap game," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2018, pp. 713–728. doi: 10.1145/3243734.3243737.

[12] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, 2018. doi: 10.1145/3212998.

[13] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS P)*, Mar. 2016, pp. 305–320.

[14] I. Eyal, "The miner's dilemma," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 89–103.

[15] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (FAW) attacks on bitcoin," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2017, pp. 195–209. doi: 10.1145/3133956.3134019.

[16] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, "On bitcoin and red balloons," in *Proc. 13th ACM Conf. Electron. Commerce (EC)*, New York, NY, USA, 2012, pp. 56–73. doi: 10.1145/2229012.2229022.

[17] M. Möser and R. Böhme, "Trends, tips, tolls: A longitudinal study of bitcoin transaction fees," in *Financial Cryptography Data Security*, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds. Berlin, Germany: Springer, 2015, pp. 19–33.

[18] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," *CoRR*, 2011, *arXiv:1112.4980*, [Online]. Available: https://arxiv.org/abs/1112.4980
[19] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Financial Cryptography Data Security*, J. Grossklags and B. Preneel, Eds. Berlin, Germany: Springer, 2017, pp. 515–532.
[20] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proc. WEIS*, 2013, p. 11.
[21] M. A. Javarone and C. S. Wright, "From bitcoin to bitcoin cash: A network analysis," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst. (CryBlock)*, New York, NY, USA, 2018, pp. 77–81. doi: 10.1145/3211933.3211947.
[22] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.
[23] S. King and S. Nadal. (2012). *PPcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. [Online]. Available: https://peercoin.net/
[24] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Advances in Cryptology—CRYPTO*, J. Katz and H. Shacham, Eds. Cham, Switzerland: Springer, 2017, pp. 357–388.
[25] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y," *ACM Sigmetrics Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014. doi: 10.1145/2695533.2695545.

YIRAN LIU was born in 1996. She is currently pursuing the master's degree with the School of Computer Science and Technology, Shandong University. Her main research interests include blockchain and cryptocurrencies.

JUNMING KE received the master's degree from the School of Computer Science and Technology, Shandong University, Jinan, China, in 2019. His research interests include information security and cryptography, especially blockchain and cryptocurrencies.

QIULIANG XU received the master's and Ph.D. degrees from Shandong University, Jinan, China, in 1985 and 1999, respectively, where he is currently a Professor and a Ph.D. supervisor. He has been with the university, since 1985. His main interests include public key cryptography and multi-party secure computation. He is also a syndic of the Chinese Association for Cryptologic Research. He holds several science foundations and key program of China.

HAN JIANG received the master's and Ph.D. degrees with the School of Computer Science and Technology, Shandong University, Jinan, China, in 2005 and 2008, respectively, where he is currently a Lecturer. His main interests include cryptography and information security, especially secure multi-party computation. He is a member of the CACR.

HAO WANG received the Ph.D. degree in computer science from Shandong University, China, in 2012. He is currently an Associate Professor with Shandong Normal University. His primary interests include public key cryptography, in particular, designing cryptographic primitives and provable security. At present, he is focusing on attribute-based cryptography, secure multi-party computation, and blockchain.