IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 16, 2018, accepted August 24, 2018, date of publication August 29, 2018, date of current version September 21, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2867631

A Novel Bitcoin Mining Scheme Based on the Multi-Leader Multi-Follower Stackelberg Game Model

SUNGWOOK KIM
Department of Computer Science, Sogang University, Seoul 121-742, South Korea
e-mail: swkim01@sogang.ac.kr

This work was supported in part by the Ministry of Science and ICT (MSIT), South Korea, through the Information Technology Research Center (ITRC) Support Program, supervised by the Institute for Information and Communications Technology Promotion (IITP), under Grant IITP-2018-2018-0-01799, and in part by IITP through the Korean Government (MSIT), under the Development of Deidentification Technique-Based on Differential Privacy under Grant 2017-0-00498.

ABSTRACT Since the introduction of Bitcoin in 2009, it has gained a significant popularity around the world. Bitcoin is a peer-to-peer electronic payment system where payment transactions are stored in a data structure named the block-chain. Based on a fully decentralized network, the blockchain is maintained by a community of participants. In Bitcoin system, mining is the fundamental concept. In this paper, we design a new Bitcoin mining scheme based on the multi-leader multi-follower Stackelberg game model. To effectively implement the peer-to-peer relationship of Bitcoin system agents, we assume that mining pool operators are leaders and mining participating users are followers in our Stackelberg game. By using the dynamics of feedback-based repeated process, leaders, and followers can be interacting with one another and make their decisions in a way to reach an efficient system solution. Without the influence of any central authorities and organizations, the proposed method is practically applied to a distributed Bitcoin system. Through system level simulations, we show that our game approach outperforms the existing Bitcoin schemes in providing a better fair-efficient system performance.

INDEX TERMS Bitcoin mining, distributed computation, peer-to-peer networks, multi-leader multi-follower Stackelberg game, bargaining solutions.

I. INTRODUCTION

Recent improvement in computer technology and communication networks has created some alternatives for traditional money exchange. In particular, number of users using financial Internet services have increased and gained a lot of popularity. However, traditional financial services have always been controversial and we will encounter many problems. First, people need to trust some third parties, which are built as centralized systems. There have been many reports about stolen credentials and financial information from the centralized system. Usually, people sensitively concern with their privacy and security. Second, classical monetary system is still analog based on fiat currencies such as US Dollar. This currency is backed by the US government, but it is inflationary. Third, there are some difficulties and inconveniences through traditional financial services. For example, transaction time limitations and extra service fees, etc. [1], [2].

In 2009, Satoshi Nakamoto released a new peer-to-peer distributed and trustless electronic cash, called Bitcoin. As the first decentralized cryptocurrency, Bitcoin has introduced some unique features which has never done before. In particular, Bitcoin replaced the central servers with a consensus mechanism based on the Proof of Work (PoW) protocol. As a decentralized form of currency, Bitcoin offers the opportunity to have nearly anonymous transactions. A transaction is formed when a user digitally signs a hash of the previous transaction where this Bitcoin was last spent. The Bitcoin system verifies transactions which are stored in a data structure called the blockchain which is maintained by a community of participating users. Nowadays, Bitcoin has received a lot of attentions and brought many new opportunities to the next generation financial services [1], [3].

To ensure Bitcoin system integrity, all transactions should be verified through cryptographic proof in the network system. This process is called Bitcoin mining [4].

In particular, Bitcoin mining is a peer-to-peer computing process, which is used to secure and to verify Bitcoin transactions on a decentralized network. During the Bitcoin mining, Bitcoin uses a hash-based PoW mechanism to generate blocks; individual blocks must contain a PoW to be considered valid. This PoW is verified by other Bitcoin users at each time they receive a block while confirming transactions to the rest of the network as having taken place. Therefore, Bitcoin uses a PoW function to distinguish legitimate Bitcoin transactions from attempts to re-spend Bitcoins that have already been spent elsewhere [4].

Any user connected to the Bitcoin network can participate in creating a block by finding a valid PoW. When a block is generated, the chain grows linearly, and participating users get Bitcoins as a reward. For example, if users successfully generate a block, they're granted a fixed amount of Bitcoins. This is an incentive for them to continuously support the Bitcoin system. Therefore, the primary purpose of Bitcoin mining serves the purpose of disseminating new Bitcoins in a decentralized manner as well as participating users to provide security for the system through mining [4].

However, the Bitcoin mining process requires dedicated hardware devices and consumes intense amounts of energy. Therefore, it is infeasible to mine a block using personal computers or individual mining devices. To overcome this difficulty, it is expected in the phenomenon that stresses distributed computation situation [5], [6]. Recently, the new concept, called pool mining, was introduced to make the Bitcoin mining profitable. Pool mining is a mining approach where groups of individual users contribute their computation power to mine a block, and then split the obtained Bitcoin reward according to their processing contributes. To adaptively split the reward into pool members in proportion to their actual contributions, there is a space for algorithmic improvements [4], [7]. Usually, each pool has its own policies for sharing the Bitcoin reward, and the profit that each participating user gets varies. Therefore, each individual user willing to join a pool must decide which pool would be the most profitable to him [8].

In the widely dynamic Bitcoin mining process, individual users and pool operators can be assumed as intelligent decision-makers, and they rationally select a best strategy to maximize their expected profits. This situation is well-suited for the game theory. Game theory is a field of applied mathematics that provides an effective tool to model interactions among independent decision makers. It can describe the reactions of one set of decision makers to another and analyze the situations in terms of conflict and cooperation [9]. During the Bitcoin mining operation, game theory is really useful in analyzing the mutual interactions between users and mining operators, and can be a major control paradigm to retain an effective solution [4].

In 1934, H. V. Stackelberg proposed a hierarchical non-cooperative game model based on two kinds of different decision makers; a leader and followers. In traditional Stackelberg games, a leader makes the first move in the game, and multiple followers would respond to the actions of the leader. Recently, the classical Stackelberg game model has been extended as a multi-leader multi-follower Stackelberg game. In this new game model, multiple leaders first predict the behaviors of all followers while considering the corresponding strategies of other leaders. And then, leaders select their strategies. Followers choose their preferred leaders according to the strategies set by the leaders [9], [10]. Compared with the traditional Stackelberg game, the multi-leader multi-follower Stackelberg game is suitable and adaptable for the practical implementation of Bitcoin mining situation.

Motivated by the above discussion, we propose a novel Bitcoin mining scheme based on the multi-leader multi-follower Stackelberg game model. In the proposed scheme, users are grouped as a mining pool, and multiple mining pools exist in a distributed way. The main focus of our scheme is to develop new algorithms for the reward payment and computation power distribution processes. From the viewpoint of pool operators, the main interest is to maximize their profits by adaptively deciding the pooling fee. From the viewpoint of mining users, how to effectively distribute their computation power is an essential challenge. Based on the repeated interaction, users and pool operators can highlight issues of cooperation and competition in each mining pool and across multiple pools. Under widely different and diversified Bitcoin network situations, the proposed Stackelberg game approach can get a globally desirable system performance.

A. CONTRIBUTION

In this paper, we design a new Bitcoin mining scheme in accordance with the multi-leader multi-follower Stackelberg game. The main novelty of our scheme is the reciprocal combination of the fee decision and power distribution algorithms while paying a serious attention to the adjustable dynamics considering the current Bitcoin system environments. To the best of our knowledge, this is the first work that applies the Stackelberg game model with multiple leaders and multiple followers to study the Bitcoin mining process. The contributions of this study can be summarized as follows:

- **Stackelberg game implementation:** we introduce a novel non-cooperative multi-leader multi-follower Stackelberg game model while capturing dynamic interactions of mining operators and users. Depending on their different viewpoints, our approach is generic and applicable to implement the real-world Bitcoin mining mechanism.
- **Fee decision algorithm in the mining process:** we implement the fee decision algorithm in each mining pool using a specialized learning protocol. To attract enough mining users' participations, the pooling fee in each pool should be adjusted dynamically based on the current system conditions.
- **Bargaining solutions for mining participations:** we employ the basic concept of bargaining solutions to formalize the users' mining strategies. To maximize their profits, users distribute their computational power

among a set of mining pools while participating in multiple mining processes.
- **The synergy of combined algorithms:** we explore the sequential interaction of the fee decision and computational power distribution algorithms, and jointly design an integrated scheme to strike an appropriate performance balance between conflicting requirements. The synergy effect lies in its responsiveness to the reciprocal combination of different control algorithms.
- **Practical implementation:** we investigate the dynamic system environment based on the step-by-step repeated game process. This is a suitable and practical approach for real-world Bitcoin network operations.
- **Performance analysis:** we evaluate the system performance based on the simulation model. Numerical study demonstrates that the overall performance of the proposed scheme can be significantly improved by comparing to the existing [4], [7], [13] schemes.

B. ORGANIZATION

The rest of the paper is structured as follows. In the next section, we review some related Bitcoin mining schemes and their problems. Section III introduces the basics of Bitcoin system and provides an outline of the multi-leader multi-follower Stackelberg game model. In addition, we explain the proposed Bitcoin mining scheme in detail, and show the main steps of the proposed scheme to increase readability. In Section IV, performance evaluation results are presented along with comparisons with the schemes proposed in [4], [7], and [13]. Finally, we end up with some concluding remarks in Section V. In this section, we also discuss the remaining open challenges in this research area along with possible solutions.

II. RELATED WORK

Recently, several Bitcoin mining schemes have been presented for peer-to-peer distributed network systems. In [11], a new game model is defined and analyzed. In this game model, pools use some of their participants to infiltrate other pools and perform such an attack. In addition, a new concept, called miner's dilemma, is introduced. The special cases where either two pools or any number of identical pools play the game are studied. In these cases, there exists an equilibrium that constitutes a tragedy of the commons where the participating pools attack one another and earn less than they would have if none has attacked. For pools, the decision whether or not to attack is the miner's dilemma, an instance of the iterative prisoner's dilemma [11].

Beikverdi and Song [1] introduces a centralization factor in Bitcoin's mining which shows the state of centralization in the network. In order to keep Bitcoin as a distributed and decentralized network, mining process should be clear to users. Moreover, any users with current normal processing power should be able to contribute in the mining process. Centralization phenomenon is something that happens to any disciplined system by nature to make things simpler. Therefore, in case of Bitcoin mining process, centralization is considered as a big concern. In the paper Beikverdi and Song [1] show that Bitcoin is getting centralized, and this issue should be resolved.

Salimitari *et al.* [8] focus on the profit maximization problem. It becomes challenging for a new miner to decide the pool he must join such that the profit is maximized. By using the prospect theory, the profit of a specific miner can be predicted with his hash rate power and electricity costs. A utility value is calculated for each pool based on its recent performance, hash rate power, total number of the pool members, reward distribution policy of the pool, electricity fee in the new miner's region, pool fee, and the current Bitcoin value. Then, based on these parameters during a certain time duration, the most profitable pool is found for each miner. Results reveal that the proposed approach is consistent with what users actually mine [8].

The paper [12] analyzes the pooled mining reward systems, and seems to best capture the principles of pooled mining process. In mining reward systems, payments are calculated based on a division to rounds, where a round is the time between one block found by the pool to the next. At the end of every round, when a block is found and the pool receives a specific reward, the operator keeps a fee, and the rest is distributed among the miners, in direct proportion to the number of shares they submitted during this round [12].

Fang *et al.* [25] employ the coordinated multiple relays communication to improve the physical-layer security of the wireless network. To systematically model the source and the multiple relays' behaviors, a stackelberg game model is proposed based on the single-leader multiple-followers' interactive mechanism. And then, an optimal price allocation algorithm is also developed to achieve the cooperative communication. Numerical studies demonstrate that the proposed scheme in [25] performs much better in defending against the eavesdropping attacks than those existing schemes.

In [26], a novel trust management is established based on fuzzy logic and game theory by considering the uncertainty. First, a multi-criteria fuzzy decision-making model is developed to predict trust in the fuzzy and complex environment. Second, a trust updating process based on game theory and evolutionary learning is designed. Finally, two illustrative examples are provided to verify the proposed model. Compared to the traditional trust measurement method, the simulation results show that the proposed model in [26] has better adaptability and accuracy in fuzzy large-scale networks.

The Distributed Computation based Power Splitting (DCPS) scheme [13] proposes a new computational power splitting game for the Bitcoin mining mechanism. This game model includes multiple supervisors and incentivized users to compete in solving large computation tasks in exchange for financial rewards. Users with computation power play a game of solving computation problems by acting as a supervisor or joining other pools. In particular, the DCPS scheme enables users connect to the Internet to participate in the Bitcoin mining while splitting their computational

powers among a set of competing pools. Based on the game model, users have the choice to contribute their power to one supervisor's pool or anonymously spread it across many pools. Finally, it is shown that the DCPS scheme is a powerful Bitcoin protocol in competitive distributed computation scenarios [13].

The Cooperative Game based Bitcoin Mining (CGBM) scheme in [7] examines the dynamics of pooled mining and reward distribution. Cooperative game theoretic tools are used to analyze how pool members may share the reward. According to the skewed reward mechanism, the CGBM scheme demonstrates the fact that a hard-work pool gains more rewards, in expectation, than its fair share. Due to the non-linear nature of returns, this scheme creates an incentive for some users to leave their pool and join other pools so as to increase their expected reward. Finally, the CGBM scheme illustrates the use of game theoretic tools applied to a real-world Bitcoin network environment [7].

S. Kim designs the Group Bargaining based Bitcoin Mining (GBBM) scheme while developing a novel incentive payment process [4]. To effectively implement an incentive payment mechanism, he adopts the concept of the group bargaining solution by considering a peer-to-peer relationship, and it is practically applied to a distributed computation network system. Based on the desirable features of group bargaining approach, self-regarding users are induced to actively participate in the fair-efficient Bitcoin mining process, and the protocol in [4] explores an effective solution that can maximize Bitcoin users' rewards.

All the earlier work has attracted a lot of attention and introduced unique challenges. However, although some work has been done to improve the performance of Bitcoin mining process, no published research attempts to capture the hierarchical interaction among users and pool operators to get the desirable solution. In this study, we compared the performance of our proposed scheme with that of the DCPS scheme [13], the CGBM scheme [7] and the GBBM scheme [4] to confirm the superiority of our approach in Bitcoin network system operations.

III. PROPOSED FAIR-EFFICIENT BITCOIN MINING ALGORITHMS

In this section, we consider a new Bitcoin mining process powered by the peer-to-peer network system. Due to the technology shift from a regular single-user mining process to the cooperative mining pool mechanism, we focus on the multi-leader multi-follower Stackelberg game model.

A. STACKELBERG GAME MODEL FOR BITCOIN NETWORKS

Recent advances in distributed computation technology have solved large computational problems by harnessing the availability of computers connected to the Internet [13]. By having Internet as a great platform where everyone has an access to, distributing information has become significantly simpler, and can easily benefit from Internet as a distributed and decentralized peer-to-peer platform [1], [14], [15]. Based on this situation, cryptocurrency has emerged as an important financial software system. It is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions while verifying the transfer of assets. To generate and distribute currency units, participants contribute their computational resources in exchange for direct financial gain or monetary compensation. This process requires distributed verifications of transactions without a central authority [16].

Bitcoin, created in 2009 by Satoshi Nakamoto, was the first decentralized cryptocurrency while using a decentralized control mechanism as opposed to centralized electronic money and central banking systems. This decentralized control approach is related to the use of blockchain transaction database in the role of a distributed public ledger. Blockchain consists of a distributed, chronological chain of blocks and it is a continuously growing list of blocks, which are added to it with a new set of records. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. As a distributed ledger, blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. The process of adding a new block is based on a consensus. Therefore, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires the collusion of network majority. Based on this blockchain technology, transactions across Bitcoin systems can be more secure than traditional transaction processes [1], [2], [4], [8], [17].

With fiat money in traditional central banking system, a government decides when to print and distribute money. Bitcoin doesn't have a central authority. Instead, Bitcoins are generated at a predictable rate such that the eventual total number will be 21 million. To issue Bitcoins, we use a special software to solve math problems, which are related to hash-cash PoW. It means that in order to add a block to the blockchain, user should find a specific nonce value for each block in a way that the SHA-256 hash value of the block information and the nonce value will be less than a specific target value [8]. The process of new Bitcoin generation is called mining and users who create and verify blocks are called miners. Miners keep altering the value of nonce, which results in entirely changing the block's header hash, until a valid hash is found. Therefore, the higher the number of random values a miner can generate per second, the higher the chances to meet the target in less time [4].

As a peer-to-peer computing process, bitcoin mining involves adding bitcoin transaction data to Bitcoin's global public ledger of past transactions. To maintain this process, there must be an incentive to contribute verifying transactions within the blockchain. Without miners, new transactions cannot be added to the public ledger, and Bitcoin will not function. However, Bitcoin mining is mathematically hard and time consuming because it can be done only by brute force search and the miners have to try different nonce values randomly to search the answer. To overcome this difficulty,

Bitcoin miners pool their computational resources together and share their hashing power while splitting the reward according to the amount of shares they contributed to solving a block [8], [18].

Bitcoin mining pool is a way to encourage miners to work together as a team while sharing miners' hashing powers to generate a block. During the last several years, several mining pool protocols have been developed to implement the cooperative mining process. Main differences among protocols are pooling fee and payment system strategies. Pooling fees vary according to the payment distribution models, which determine which party is assuming the risk - the miners or the mining pool operator. If the mining pool operator is assuming the risk, then the fee is higher, and if the miners assume the risk then the fee is lower [1], [2], [4], [7], [8].

Over the time, many different payment systems for the Bitcoin mining process have been developed. Usually, payment systems are categorized using the concept of share. As a scorekeeping in each mining software, share describes how much work a miner's computer is contributing to the mining pool, and is awarded to miners who present a valid PoW. It means a miner's shares are counting substantially towards discovering new Bitcoins. The more shares a miner contribute, the more payout for each coin block that is found. According to the amount of shares, the Bitcoin reward is split into miners who contribute to solving a block. Therefore, different payment systems have been invented using the shares of each miner. In an ongoing effort to come up with the fair-efficient methods, most popular payment systems are PPS, Prop, PPLNS and Score [19].

- Pay Per Share (PPS): This model offers a guaranteed payout for each share of miners, who can withdraw their payout immediately. The PPS model allows for the least possible variance in payment for miners while transferring much of the risk to the pool operator. Therefore, the fee is high for the risky pool operator.
- Proportional (Prop): This model offers a proportional distribution of the reward among all miners. It is a round-based method; one round is the time between the first share after the last found block and the share which solves a block. When a block is found, the reward is distributed proportionally based on the number of shares.
- Pay Per Last N Shares (PPLNS): This model looks at the last N shares, regardless of round boundaries, and distributes the reward like as the Prop model. It means that the PPLNS model does not considers valid shares of one round, but considers a number N of shares, no matter if they're apart of the round or not.
- Score: This model uses a method that a proportional reward is distributed and weighed by the time the work was submitted. For each share score is updated based on the timing rule; later shares are worth more than earlier shares. The reward is calculated in proportion to the scores and not shares submitted.

When a miner is deciding to join a mining pool, there are quite a few considerations to take into account; i) payment systems, which are the methods of distributing the block reward, ii) pooling fees, which are charged to miners for the pool management, and iii) each miner's propensity. In this study, the main contribution is the up-to-date presentation of the mutual-interaction relationship between mining pool operators and miners. The dynamics of this relationship can cause cascade interactions of them, and they dynamically make their decisions to maximize their profits. For pool operators, pooling fee adjustments are their major decisions, and for miners, distributions of their computing power are their main concerns. To model the autonomous interacting mechanism between pool operators and miners, we develop a new multi-leader multi-follower Stackelberg game to get an effective solution. Our game model ($\mathbb{G}$) can be represented by a tuple $\mathbb{G} = \left(\{\boldsymbol{\mathcal{L}}, \boldsymbol{\mathcal{F}}\}, \left(\boldsymbol{\mathcal{S}}^{\boldsymbol{\mathcal{L}}}_{L_i \in \boldsymbol{\mathcal{L}}}, \boldsymbol{\mathcal{S}}^{\boldsymbol{\mathcal{F}}}_{F_j \in \boldsymbol{\mathcal{F}}}\right), \left(U^{\boldsymbol{\mathcal{L}}}_{L_i \in \boldsymbol{\mathcal{L}}}, U^{\boldsymbol{\mathcal{F}}}_{F_j \in \boldsymbol{\mathcal{F}}}\right), T\right)$ at each time period of gameplay.

- $\{\boldsymbol{\mathcal{L}}, \boldsymbol{\mathcal{F}}\}$ is the finite superset of game players where $\boldsymbol{\mathcal{L}} = \{L_1, \ldots L_l\}$ represents the set of leaders and $\boldsymbol{\mathcal{F}} = \{F_1, \ldots F_f\}$ is a set of followers. In the $\mathbb{G}$, leaders are pool operators and followers are miners in the Bitcoin mining process.
- $\boldsymbol{\mathcal{S}}^{\boldsymbol{\mathcal{L}}}_{L_i \in \boldsymbol{\mathcal{L}}}$ is the strategy set of the player $L_{1 \le i \le l}$ and $\boldsymbol{\mathcal{S}}^{\boldsymbol{\mathcal{F}}}_{F_j \in \boldsymbol{\mathcal{F}}}$ is the strategy set of the player $F_{1 \le j \le f}$. Commonsensically, payment system of each pool is initially chosen and remains constant eternally. Therefore, $\mathcal{S}^{\boldsymbol{\mathcal{L}}}_{L_i}$ is defined as the pooling fee levels. Through a specific partition function, the F_j distributes his computational power across multiple pools to maximize the profit. Therefore, $\boldsymbol{\mathcal{S}}^{\boldsymbol{\mathcal{F}}}_{F_j}$ represents the F_j's participating level for each individual pool.
- $U^{\boldsymbol{\mathcal{L}}}_{L_i \in \boldsymbol{\mathcal{L}}}$ is the payoff received by the player L_i; it is determined as the sum of obtained fees. $U^{\boldsymbol{\mathcal{F}}}_{F_j \in \boldsymbol{\mathcal{F}}}$ is the payoff received by the player F_j; it is determined as the sum of rewards from mining participations.
- T is a time period. In order to implement the Bitcoin mining process, we partition the time-axis into equal intervals of length unit_time. The $\mathbb{G}$ is repeated at each unit_time with competitive and cooperative manner.

B. UTILITY FUNCTIONS IN THE PROPOSED STACKELBERG GAME MODEL

In this subsection, we formulate utility functions for game players. In our multi-leader multi-follower Stackelberg game model, multiple pool operators and miners compete with each other for their profit maximization while solving computationally large problems. Pool operators adaptively decide their pooling fees to induce selfish miners to participate in their mining pools. With the computational power, miners play a game to maximize their payoffs by joining multiple pools. Based on the step-by-step interactive feedback approach, the proposed game model is designed as a repeated game.

To quantify players' satisfaction, their utility functions are derived based on the outcome of the game. From the point of view of miners, the main goal is to maximize

their profits through the mining process. Basically, the main factors of a miner's utility function are Bitcoin generation probability ($\mathfrak{T}^B$), share generation probability ($\mathfrak{A}^S$), pooling fee (F), transaction incentive (I_F) and a miner's allocated computation power ($\mathfrak{T}_F$). When a block is discovered, the discovering miners may award themselves a certain number of Bitcoins, which is agreed-upon by everyone in the Bitcoin network. Currently this bounty is 12.5 Bitcoins; this value will halve every 210,000 blocks. Additionally, the miner is incentivized by Bitcoin transactions, which will be included in the new block. In the future, as the number of new bitcoins dwindles, this transaction incentive (I_F) will make up a much more important percentage of mining income [1], [2], [4], [7], [8], [19].

To develop a miner's utility function, we should consider the distinctive features of each payment system. The profit of a miner is strongly dependent on the payment system of mining pool, which is selected by the miner. Therefore, a miner's utility function should be defined differently based on each payment system. At each unit_time period, each miner monitors periodically his payoff value and change their strategies dynamically in an online distributed manner. The miner F_j's utility function for the PPS payment system $\left(U_{F_j}^{PPS}\left(\mathfrak{T}_{F_j}^{PPS}\right)\right)$ is given by.

$$U_{F_j}^{PPS}\left(\mathfrak{T}_{F_j}^{PPS}\right) = \mathbb{O}_{F_j}^{PPS} - F_{F_j}^{PPS}, \quad \text{s.t., } \mathbb{O}_{F_j}^{PPS} = \left(\mathfrak{A}_{F_j}^{S}\left(\mathfrak{T}_{F_j}^{PPS}\right) \times \frac{\partial}{(\mu_{PPS} \times \psi)}\right) \quad (1)$$

where $\mathfrak{T}_{F_j}^{PPS}$ is the F_j's allocated computational power to the PPS and ∂ is the mining award. $\mathfrak{A}_{F_j}^{S}\left(\mathfrak{T}_{F_j}^{PPS}\right)$ is the share generation probability in the PPS with $\mathfrak{T}_{F_j}^{PPS}$. The expected value of $\mathfrak{A}_{F_j}^{S}\left(\mathfrak{T}_{F_j}^{PPS}\right)$ has a linear proportional relation with rate $\mathfrak{T}_{F_j}^{PPS}$. μ_{PPS} and ψ are the difficult control factor and discount parameter of the PPS pool, respectively. $F_{F_j}^{PPS}$ is the PPS's pooling fee for the F_j; it is included in the PPS pool operator's payoff. $\mathfrak{A}_{F_j}^{S}\left(\mathfrak{T}_{F_j}^{PPS}\right)$ and $F_{F_j}^{PPS}$ are estimated periodically at each unit_time. The F_j's utility function for the Prop payment system $\left(U_{F_j}^{Prop}\left(\mathfrak{T}_{F_j}^{Prop}\right)\right)$ is defined as follows;

$$U_{F_j}^{Prop}\left(\mathfrak{T}_{F_j}^{Prop}\right) = \left(\frac{\mathfrak{A}_{F_j}^{S}\left(\mathfrak{T}_{F_j}^{Prop}\right)}{\sum_{F_i \in \mathfrak{Z}_{Prop}} \mathfrak{A}_{F_i}^{S}\left(\mathfrak{T}_{F_i}^{Prop}\right)} \times \left(\frac{\partial}{\mu_{Prop}} + I_F^{Prop}\right) \times \mathfrak{T}_{Prop}^{B}\left(\mathcal{M}^{Prop}\right)\right) - F_{F_j}^{Prop}$$
$$\text{s.t., } \mathcal{M}^{Prop} = \sum_{F_i \in \mathfrak{Z}_{Prop}} \mathfrak{T}_{F_i}^{Prop} \quad (2)$$

where $\mathfrak{Z}_{Prop}$ is the set of miners, who participate in the Prop's mining pool. $\mathfrak{T}_{Prop}^{B}\left(\mathcal{M}^{Prop}\right)$ and $\mathfrak{A}_{F_j}^{S}\left(\mathfrak{T}_{F_j}^{Prop}\right)$ are related linearly with the rates $\mathcal{M}^{Prop}$ and $\mathfrak{T}_{F_j}^{Prop}$, respectively. $F_{F_j}^{Prop}$ is the Prop's pooling fee for the F_j where $F_{F_j}^{Prop} = U_{L_{i=Prop}}\left(\mathfrak{T}_{F_j}^{Prop}\right)$. μ_{Prop} and I_F^{Prop} are the difficult control factor and transaction incentive of the Prop pool, respectively. $\mathfrak{T}_{Prop}^{B}(\cdot), \mathfrak{A}_{F_j}^{S}(\cdot), I_F^{Prop}$ and $F_{F_j}^{Prop}$ are estimated periodically at each unit_time. The F_j's utility function for the PPLNS payment system $\left(U_{F_j}^{PPLNS}\left(\mathfrak{T}_{F_j}^{PPLNS}\right)\right)$ is formulated as follows;

$$U_{F_j}^{PPLNS}\left(\mathfrak{T}_{F_j}^{PPLNS}\right) = \left(\frac{1}{\Delta t_{F_j}^{PPLNS}} \times \mathbb{Q}[\Upsilon]\right) - F_{F_j}^{PPLNS}$$
$$\text{s.t., } \Upsilon = N \times \left(\frac{\mathfrak{A}_{F_j}^{S}\left(\mathfrak{T}_{F_j}^{PPLNS}\right)}{\sum_{F_i \in \mathfrak{Z}_{PPLNS}} \mathfrak{A}_{F_i}^{S}\left(\mathfrak{T}_{F_i}^{PPLNS}\right)} \times \left(\frac{\partial}{\mu_{PPLNS}} + I_F^{PPLNS}\right) \times \mathfrak{T}_{PPLNS}^{B}\left(\mathcal{M}^{PPLNS}\right)\right)$$
$$\text{and } \mathcal{M}^{PPLNS} = \sum_{F_i \in \mathfrak{Z}_{PPLNS}} \mathfrak{T}_{F_i}^{PPLNS} \quad (3)$$

where N is the pre-fixed number of shares in the PPLNS pool, and $\Delta t_{F_j}^{PPLNS}$ is the number of unit_times that the PPLNS pool generates N shares. $F_{F_j}^{PPLNS}$ is the PPLNS's pooling fee for the F_j where $F_{F_j}^{PPLNS} = U_{L_{i=PPLNS}}\left(\mathfrak{T}_{F_j}^{PPLNS}\right)$. $\mathbb{Q}[\Upsilon]$ is an outcome function based on the PPLNS condition. When the number of generated shares reaches N, $\mathbb{Q}[\Upsilon]$ returns Υ value. Otherwise, it returns 0. The F_j's utility function for the Score payment system $\left(U_{F_j}^{Score}\left(\mathfrak{T}_{F_j}^{Score}\right)\right)$ is given by;

$$U_{F_j}^{Score}\left(\mathfrak{T}_{F_j}^{Score}\right) = \left(\frac{|T_B - t_{F_j}|}{\sum_{F_i \in \mathfrak{Z}_{Score}} |T_B - t_{F_i}|} \times \Upsilon\right) - F_{F_j}^{Score}$$
$$\text{s.t., } \Upsilon = \left(\frac{\mathfrak{A}_{F_j}^{S}\left(\mathfrak{T}_{F_j}^{Score}\right)}{\sum_{F_i \in \mathfrak{Z}_{Score}} \mathfrak{A}_{F_i}^{S}\left(\mathfrak{T}_{F_i}^{Score}\right)} \times \left(\frac{\partial}{\mu_{Score}} + I_F^{Score}\right) \times \mathfrak{T}_{Score}^{B}\left(\mathcal{M}^{Score}\right)\right)$$
$$\text{and } \mathcal{M}^{Score} = \sum_{F_i \in \mathfrak{Z}_{Score}} \mathfrak{T}_{F_i}^{Score} \quad (4)$$

where T_B, t_{F_j} are the just previous Bitcoin generation time, and the share generation time by the F_j, respectively. $F_{F_j}^{Score}$ is the Score model's pooling fee for the F_j where $F_{F_j}^{Score} = U_{L_{i=Score}}\left(\mathfrak{T}_{F_j}^{Score}\right)$.

Sum up the utility functions for each payment systems, $U_{F_j}^{PPS}$ provides instantly a payout for each share regardless of Bitcoin generation, and $U_{F_j}^{Prop}$ offers a payout proportionally based on the number of shares when a block is found. In this study, the PPLNS pool's payoff is normalized per unit_time to fairly compare each payoff. In the Score payment system, each payout is calculated in proportion to the scores and

preference of latest submitted time according to the timing rule [19].

From the point of view of pool operators, the major concern is to recruit miners; the larger participating miners, the higher revenue according to the income of pooling fees. Simply, we assume that $\boldsymbol{\mathcal{S}}^{\boldsymbol{\mathcal{L}}}$ is the discreet set of pooling fees where $\boldsymbol{\mathcal{S}}^{\boldsymbol{\mathcal{L}}}_{L_i} = \left(s^1_{L_i} \ldots s^k_{L_i}\right)$. The pool operator L_i's utility function with the strategy $s^{1\le h\le k}_{L_i}\left(U_{L_i}\left(s^h_{L_i}\right)\right)$ is defined as follows;

$$U_{L_i}\left(s^h_{L_i}\right) = \begin{cases} \left(\left(\frac{\partial}{\mu_{L_i}} + I^{L_i}_F\right) \times \mathfrak{T}^B_{L_i}\left(\mathcal{M}^{L_i}\right)\right) \\ \quad - \sum\limits_{F_j \in \mathfrak{Z}_{PPS}} \left(\left(1 - s^h_{L_i}\right) \times \mathbb{O}^{PPS}_{F_j}\right), & \text{if } L_i \text{ is } PPS \\ s^h_{L_i} \times \left(\left(\frac{\partial}{\mu_{L_i}} + I^{L_i}_F\right) \times \mathfrak{T}^B_{L_i}\left(\mathcal{M}^{L_i}\right)\right) \\ \quad = \sum\limits_{F_j \in \mathfrak{Z}_{L_i}} F^{L_i}_{F_j}, & \text{otherwise} \end{cases} \tag{5}$$

where $F^{L_i}_{F_j}$ is the F_j's pooling fee for the L_i. Just the same as miners' utility functions, the values of $\mathfrak{Z}_{L_i}$, $\mathfrak{T}^{L_i}_{F_j}$, $\mathcal{M}^{L_i}$, $\mathfrak{T}^B_{L_i}\left(\mathcal{M}^{L_i}\right)$ and $\mathbb{O}^{PPS}_{F_j}$ are estimated periodically at each unit_time. By considering the reciprocal relationship between the $\mathcal{M}^{L_i}$ and its pooling fee, the L_i adaptively selects his strategy.

C. BITCOIN MINING PROCESS WITH BARGAINING SOLUTIONS

Generally, all miners have unique, complex personalities shaped by socioeconomic background, personal experience, and current status. These diverse factors make it possible to broadly categorize miners into three types; risk-averse, risk-neutral and risk-seeking. When exposed to uncertainty, risk-averse miners attempt to lower that uncertainty; they hesitate to agree to a situation with an unknown payoff rather than another situation with a more predictable payoff but possibly lower expected payoff. On the contrary to this, risk-seeking miners have a preference for risk; they prefer an investment with an uncertain but higher expected outcome. Risk-neutral miners are indifferent to risk when making an investment decision; they place themselves in the middle of the risk spectrum, represented by risk-seeking miners at one end and risk-averse miners at the other [20].

In this study, miners distribute their computation powers to multiple pools, differentially. Therefore, how much computation power would be allotted to a specific pool is an important issue. To allocate the computation power fairly and optimally, we adopt the basic concept of bargaining solutions. Bargaining solution predicts an outcome of game play based only on information about each player's preferences. It is formulated by an expected utility function over the set of feasible agreements and the outcome which would result in case of disagreement. Over the past few decades, various bargaining solutions have been proposed based on slightly different assumptions about what properties are desired for the final agreement point. For bargaining solutions, there are desirable properties [9];

i) Individual rationality: No player is worse off than if the bargaining agreement fails.
ii) Pareto optimality: Bargaining solution gives the maximum payoff to the players.
iii) Invariance with respect to utility transformations: Bargaining solution is invariant if affinely scaled. This axiom is also called Independence of Linear Transformations or scale covariance.
iv) Independence of irrelevant alternatives: Bargaining solution should be independent of irrelevant alternatives. In other words, a reasonable outcome will be feasible after some payoff sets have been removed.
v) Symmetry: If the players' utilities are exactly the same, they should get symmetric payoffs. Therefore, payoff should not discriminate between the identities of the players, but only depend on utility functions.
vi) Individual monotonicity: The increasing of bargaining set size in a direction favorable to a specific player always benefits that player.
vii) Stronger monotonicity: Bargaining solution attempts to grant equal gain to players. In other words, it is the point which maximizes the minimum payoff among players.

Most well-known bargaining solutions are Nash Bargaining Solution (NBS) developed by J. Nash at 1950, Kalai-Smorodinsky Bargaining Solution (KSBS) developed by E. Kalai and M. Smorodinsky at 1975, and Egalitarian Bargaining Solution (EBS) developed by E. Kalai and R. Myerson. These bargaining solutions have some attractive features to model the interactions among independent decision-makers, and achieve a mutually desirable solution between efficiency and fairness. NBS, KSBS and EBS are formulated as follows [9], [21];

- NBS: To provide a fair-efficient bargaining solution, NBS satisfies the i), ii), iii), iv) and v) axioms. By adaptively distribute a miner's computation power $\left(\mathfrak{T}^u_{F_j}\right)$, the NBS is obtained as follows.

$$\begin{aligned} NBS = \arg \max_{\mathfrak{T}^u_{F_j} = \left\{\mathfrak{T}^1_{F_j}\mathfrak{T}^2_{F_j}\mathfrak{T}^3_{F_j}\mathfrak{T}^4_{F_j}\right\}} & \prod_{1\le i\le 4} \left(U^i_{F_j}\left(\mathfrak{T}^i_{F_j}\right) - U^d_{F_j}\left(\mathfrak{T}^i_{F_j}\right)\right) \\ \text{s.t., } U_{F^1_j}\left(\mathfrak{T}^1_{F_j}\right) &= U^{PPS}_{F_j}\left(\mathfrak{T}^{PPS}_{F_j}\right), \\ U^2_{F_j}\left(\mathfrak{T}^2_{F_j}\right) &= U^{Prop}_{F_j}\left(\mathfrak{T}^{Prop}_{F_j}\right), \\ U^3_{F_j}\left(\mathfrak{T}^3_{F_j}\right) &= U^{PPLNS}_{F_j}\left(\mathfrak{T}^{PPLNS}_{F_j}\right), \\ U^4_{F_j}\left(\mathfrak{T}^4_{F_j}\right) &= U^{Score}_{F_j}\left(\mathfrak{T}^{Score}_{F_j}\right) \\ \text{and} \quad \mathfrak{T}^u_{F_j} &= \sum_{i=1}^{4} \mathfrak{T}^i_{F_j} \end{aligned} \tag{6}$$

where $U^d_{F_j}(\cdot)$ is a disagreement payoff, which is the game without bargaining, e.g., 0 in the system;

it guarantees that miners obtain nothing in case of bargaining disagreement.

- KSBS: To achieve a mutually desirable solution with a good balance between efficiency and fairness, KSBS satisfies the i), ii), iii), v) and vi) axioms. Therefore, KSBS is obtained as a weighted max-min solution.

$$
\begin{aligned}
KSBS = \arg \max_{\mathcal{T}^u_{F_j}=\left\{\mathcal{T}^1_{F_j}\mathcal{T}^2_{F_j}\mathcal{T}^3_{F_j}\mathcal{T}^4_{F_j}\right\}} & \times \left\{ \min_{\mathcal{T}^{1\le i\le 4}_{F_j}} \left(\frac{\left(U^i_{F_j}\left(\mathcal{T}^i_{F_j}\right) - U^d_{F_j}\left(\mathcal{T}^i_{F_j}\right)\right)}{\left(\max_{\mathcal{T}^*_{F_j}\le\mathcal{T}^u_{F_j}} \left(U^i_{F_j}\left(\mathcal{T}^*_{F_j}\right)\right) - U^d_{F_j}\left(\mathcal{T}^i_{F_j}\right)\right)} \right) \right\} \\
& \text{s.t., } U^1_{F_j}\left(\mathcal{T}^1_{F_j}\right) = U^{PPS}_{F_j}\left(\mathcal{T}^{PPS}_{F_j}\right), \\
& \quad U^2_{F_j}\left(\mathcal{T}^2_{F_j}\right) = U^{Prop}_{F_j}\left(\mathcal{T}^{Prop}_{F_j}\right), \\
& \quad U^3_{F_j}\left(\mathcal{T}^3_{F_j}\right) = U^{PPLNS}_{F_j}\left(\mathcal{T}^{PPLNS}_{F_j}\right), \\
& \quad U^4_{F_j}\left(\mathcal{T}^4_{F_j}\right) = U^{Score}_{F_j}\left(\mathcal{T}^{Score}_{F_j}\right) \\
& \quad \text{and } \mathcal{T}^u_{F_j} = \sum_{i=1}^{4} \mathcal{T}^i_{F_j} \qquad (7)
\end{aligned}
$$

where $\mathcal{T}^*_{F_j}$ is a computation power to optimize the $U^i_{F_j}(\cdot)$. Therefore, the ideal payoff $\max_{\mathcal{T}^*_{F_j}\le\mathcal{T}^u_{F_j}}\left(U^i_{F_j}\left(\mathcal{T}^*_{F_j}\right)\right)$ for each pool is the maximum effectiveness in the ideal situation in KSBS.

- EBS: This bargaining solution attempts to grant equal gain, and satisfies the i), ii), iv), v) and vii) axioms. In other words, the EBS is the solution which maximizes the minimum payoff while following the max-min effectiveness concept.

$$
\begin{aligned}
EBS = \arg \max_{\mathcal{T}^u_{F_j}=\left\{\mathcal{T}^1_{F_j}\mathcal{T}^2_{F_j}\mathcal{T}^3_{F_j}\mathcal{T}^4_{F_j}\right\}} & \left\{ \min_{\mathcal{T}^{1\le i\le 4}_{F_j}} \left(U^i_{F_j}\left(\mathcal{T}^i_{F_j}\right) - U^d_{F_j}\left(\mathcal{T}^i_{F_j}\right)\right) \right\} \\
& \text{s.t., } U^1_{F_j}\left(\mathcal{T}^1_{F_j}\right) = U^{PPS}_{F_j}\left(\mathcal{T}^{PPS}_{F_j}\right), \\
& \quad U^2_{F_j}\left(\mathcal{T}^2_{F_j}\right) = U^{Prop}_{F_j}\left(\mathcal{T}^{Prop}_{F_j}\right), \\
& \quad U^3_{F_j}\left(\mathcal{T}^3_{F_j}\right) = U^{PPLNS}_{F_j}\left(\mathcal{T}^{PPLNS}_{F_j}\right), \\
& \quad U^4_{F_j}\left(\mathcal{T}^4_{F_j}\right) = U^{Score}_{F_j}\left(\mathcal{T}^{Score}_{F_j}\right) \\
& \quad \text{and } \mathcal{T}^u_{F_j} = \sum_{i=1}^{4} \mathcal{T}^i_{F_j} \qquad (8)
\end{aligned}
$$

To effectively spread its computation power across four different pools, each individual miner selects one bargaining solution, which can be an effective tool to maximize miners' payoffs. For the bargaining selection, recent research has shown that different bargaining solutions have a relation to the issue of risk [22]. Usually, the NBS predicts that Risk-averse is a disadvantage in bargaining, and the EBS is in accord with Risk-neutral. In this study, we concern bargaining solutions which may consider risky outcomes based on the share generation. Therefore, in the Bitcoin mining situation, we characterize each bargaining solution as advantageous, disadvantageous, or irrelevant from the point of view of uncertainty. In our game model, the risk-averse, risk-neutral and risk-seeking type miners select the KSBS, EBS and NBS, respectively, to distribute their computation power across multiple mining pools.

D. THE MAIN STEPS OF PROPOSED ALGORITHM

In this work, each pool operator is independently interested in the sole goal of maximizing his utility function. Initially, the payment method of each pool is decided. Therefore, the main control issue of pool operators is to select adaptively their pooling fees while maximizing their payoffs. In the proposed scheme, the pooling fee decision mechanism is developed based on the iterative learning process. In a distributed self-regarding fashion, pool operators learn the uncertain Bitcoin system situation and make decisions by taking into account the online feedback mechanism.

For simplicity, we assume that pooling fees are defined as discrete price levels where $\boldsymbol{\mathcal{S}}^{\mathcal{L}}_L = \left\{s^1_L \ldots s^k_L\right\}$. In a distributed manner, each operator periodically re-evaluates the currently selected strategy and iteratively updates its own the probability distribution $\boldsymbol{P}\left[P\left(s^1_L\right)\ldots P\left(s^k_L\right)\right]$ for $\boldsymbol{\mathcal{S}}^{\mathcal{L}}_L$. When a pool operator selects a pooling fee with his respective $\boldsymbol{P}[\cdot]$, his payoff $U_L(\cdot)$ is obtained according to the equation (1). Therefore, the $\boldsymbol{P}[\cdot]$ should be adjusted adaptively in order to cope with the payoff fluctuation. At every unit_time, each individual pooling operator updates his probability distribution based on the modified Roth-Erev learning method [23]. If the pooling operator L_i selects $s^{1\le l\le k}_{L_i}$ in $\boldsymbol{\mathcal{S}}^{\mathcal{L}}_{L_i}$ at the t^{th} unit_time, the L_i updates the $s^l_{L_i}$'s propensity $\phi^{L_i}_{s^l}(t+1)$ like as;

$$
\begin{aligned}
& \phi^{L_i}_{s^l}(t+1) = \left((1-\rho)\times\phi^{L_i}_{s^l}(t)\right) + \mathcal{H}\left(\mathcal{W}^{L_i}_{s^l}(t), \theta, s^h_{L_i}, k\right) \\
& \text{s.t., } \mathcal{H}\left(\mathcal{W}^{L_i}_{s^l}(t), \theta, k\right) \\
& \qquad = \begin{cases} \left(\mathcal{W}^{L_i}_{s^h}(t)\times[1-\theta]\right), & \text{if } s^l_{L_i} = s^h_{L_i} \\ \left(\mathcal{W}^{L_i}_{s^h}(t)\times\dfrac{\theta}{k-1}\right), & \text{otherwise} \end{cases} \\
& \text{and} \quad \mathcal{W}^{L_i}_{s^h}(t) = \frac{U^t_{L_i}\left(s^h_{L_i}\right) - U^{t-1}_{L_i}\left(s^h_{L_i}\right)}{U^{t-1}_{L_i}\left(s^h_{L_i}\right)} \qquad (9)
\end{aligned}
$$

where ρ is a recency parameter and θ is an experimentation parameter to control the learning rate. $s^h_{L_i}$ and $U^{t-1}_{L_i}\left(s^h_{L_i}\right)$ are the selected strategy and the obtained utility at the

$(t-1)^{th}$ unit_time. According to the equation (8), $P_t\left(s^l_{L_i}\right)$ in $\boldsymbol{P}[\cdot]$ for the L_i at the t^{th} unit_time is defined based on the proportion to each strategy's propensity:

$$P_t\left(s^l_{L_i}\right) = \phi^{L_i}_{s^l}(t) \Big/ \sum_{y=1}^{k} \phi^{L_i}_{s^y}(t) \tag{10}$$

In this study, we formulate a novel multi-leader multi-follower Stackelberg game model for the Bitcoin mining process. Based on the step-by-step interactive feedback approach, pool operators and miners adapt their strategies to achieve the better benefit. As leaders, pool operators select their pooling fees. As followers, miners decide their bargaining solutions how to distribute their computational powers. At each unit_time, their decisions are examined and adjusted periodically. It is a realistic and appropriate Bitcoin mining process among selfish and rational game players. Usually, the traditional optimal algorithms have exponential time complexity. However, the proposed approach has only polynomial time complexity. The proposed algorithm is described by the following flowchart.

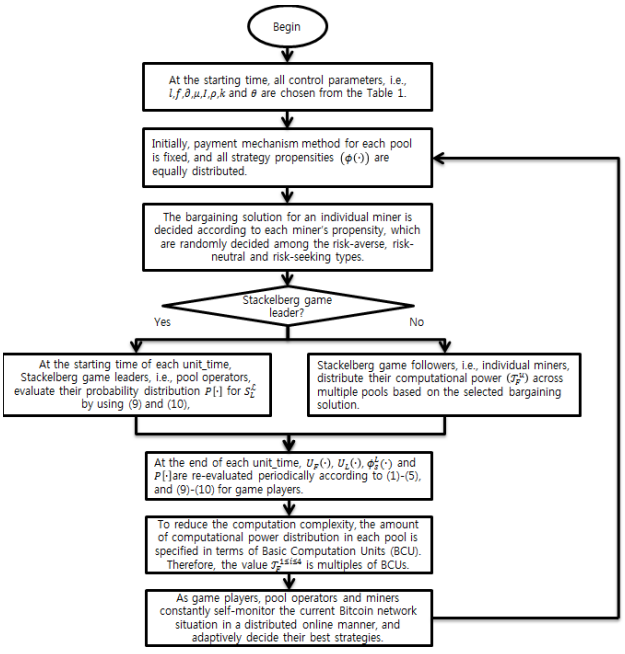


FIGURE 1. Flowchart of the proposed algorithm.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed scheme using a simulation model. In order to ensure that the model is sufficiently generic to be valid in the real-world, the assumptions used in our simulation model were as follows:

- The simulated system consists of four mining pools and 10∼100 miners for the Bitcoin mining process. Therefore, there are four pool operators.
- In the Bitcoin network, the information of each pool is publicly available; miners easily access that information during the mining process.
- In the Bitcoin mining process, miners use a hash-based PoW mechanism to generate blocks. It is a random process with low probability so that a lot of trial and error is required on average before a valid block is generated. In this simulation, the Hash-cash PoW system is used.
- We assume that game players' strategies are not changed in one game round, e.g., unit_time in our system.
- $\mathcal{S}^{\mathcal{L}}$ consists of five strategies where $\mathcal{S}^{\mathcal{L}} = \left\{s^1_L = 1\%, s^2_L = 2\%, s^3_L = 3\%, s^4_L = 4\%, s^5_L = 5\%\right\}$ for the Prop, PPLNS and Score payment system pools and $\mathcal{S}^{\mathcal{L}} = \{s^1_L = 10\%, s^2_L = 20\%, s^3_L = 30\%, s^4_L = 40\%, s^5_L = 50\%\}$ for the PPS payment system pool; s_L represents the percentage of individual miner's outcome.
- $\mathcal{S}^{\mathcal{F}}$ consists of three strategies where $\mathcal{S}^{\mathcal{F}} = \{\text{NBS,KSBS,EBS}\}$.
- Floating point operations per second (FLOPS) is a measure of computation power.
- Each miner's total computational power ($\mathcal{T}^u_F$) is 100 teraFLOPS. One BCU is the minimum amount, e.g., 10 teraFLOPS in our system, of computational power distribution.
- The share generation process is Poisson with the rate, i.e., one Bitcoin/1 petaFLOPS/ unit_time.
- The Bitcoin generation process is Poisson with the rate, i.e., one Bitcoin/10 petaFLOPS/ unit_time.
- System performance measures obtained based on 100 simulation runs were plotted as a function of the offered number of users.
- The performance criteria obtained through simulation are the normalized miner's outcome, the relative ratio of Bitcoin generation, and the miner's payoff fairness under the different number of miners.

In this study, we compare the performance of the proposed scheme with the existing DCPS [13], CGBM [7], and GBBM [4] schemes, and confirm the performance superiority of the proposed approach. As mentioned in the related work section, the DCPS scheme introduces a new distributed computation model which includes multiple supervisors competing with each other to solve computationally large problems [13]. The CGBM considers how the existence of mining pools affects the reward allocation in the Bitcoin network while analyzing the effect of skewed rewards [7]. The GBBM scheme adopts the dual-level cooperative game approach to provide a suitable trade-off between efficiency and fairness [4]. Table 1 shows the system parameters used in the simulation. To emulate the Bitcoin mining system and ensure a fair comparison, we used the system parameters given in Table 1.

In this paper, we compared the performance of the proposed scheme with existing schemes: the DCPS scheme [13], the CGBM scheme [7], and the GBBM scheme [4]. These existing schemes were recently developed as effective Bitcoin mining schemes based on the game theory.

Fig.2 presents the performance comparison of each scheme in terms of normalized miner's outcome in the Bitcoin network systems. In this study, the miner's outcome is defined as the reward for the Bitcoin mining participation. In general,

TABLE 1. System parameters used in the simulation experiment.

Parameter	Value	Description
l	4	the number of pool operators
f	10~100	the number of miners
∂	12.5 Bitcoins	the Bitcoin mining award
μ_{PPS}	0.6	the difficult control factor of the PPS
I_F^{PPS}	1 Bitcoin	the transaction incentive of the PPS
ψ	10^3	the discount parameter of the PPS
μ_{Prop}	0.6	the difficult control factor of the Prop
I_F^{Prop}	1 Bitcoin	the transaction incentive of the Prop
N	10	the prefixed share number in the PPLNS
μ_{PPLNS}	0.6	the difficult control factor of the PPLNS
I_F^{PPLNS}	1 Bitcoin	the transaction incentive of the PPLNS
μ_{Score}	0.6	the difficult control factor of the Score
I_F^{Score}	1 Bitcoin	the transaction incentive of the Score
ρ	0.2	a recency parameter
k	5	the number of pooling fee levels for operator
θ	0.7	an parameter to control the learning rate
$\mathcal{T}_F^u$	100 FLOPS	each miner's total computational power

how to use effectively the individual computation power is strongly relayed to this performance criterion. During the Bitcoin system operations, all the schemes have similar trends. However, to find a valid PoW, miners in our proposed scheme adaptively distribute their computation powers based on the different bargaining solutions. Therefore, we can get a higher miner's reward than the other schemes from low to heavy miners' intensities.

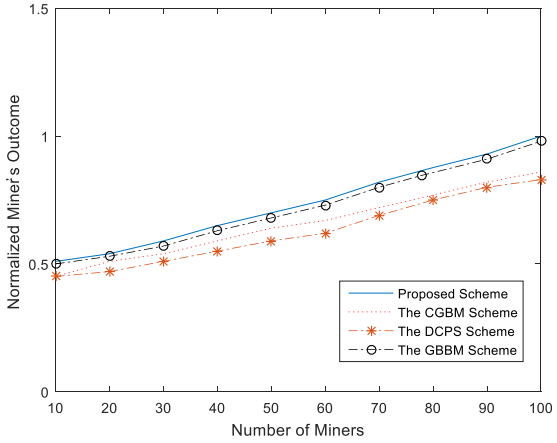


FIGURE 2. Normalized miner's outcome.

Fig.3 shows the relative ratio of Bitcoin generation in the Bitcoin mining process. From the simulation results obtained, the ratio of Bitcoin generation increases proportionally to the number of participating miners; it is intuitively correct. In the real-world Bitcoin mining operation, the higher Bitcoin generation is the most important and desirable property. Based on the multi-leader multi-follower Stackelberg game approach, we can capture the hierarchical interactions among game players, and find an effective power distribution to reach an effective solution. Under different numbers of miners,

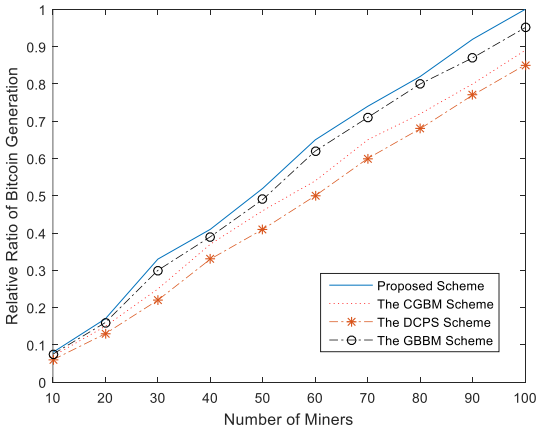


FIGURE 3. Relative ratio of bitcoin generation.

the proposed scheme can get more Bitcoins than the other existing schemes.

The curves in Fig.4 illustrate the miner's payoff fairness for all the schemes. In this study, the miner's fairness is defined as the Jain's index of miner's payoff difference per computation contribution [24]. According to each miner's preference, the computation power is dynamically allocated while ensuring reciprocal fairness. Therefore, the proposed scheme can maintain the excellent payoff fairness among miners than the other schemes.

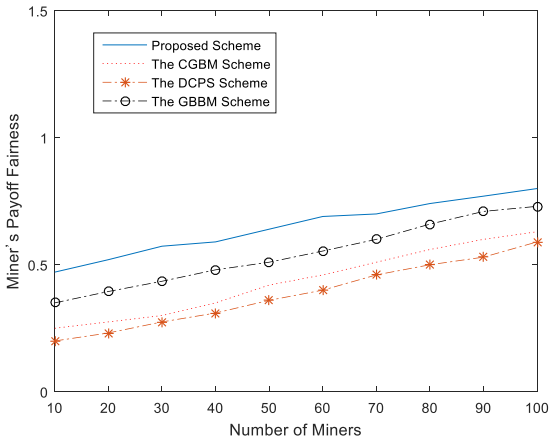


FIGURE 4. Miner's payoff fairness.

The simulation results presented in Figs. 2-4 show that the proposed scheme generally exhibits a well-balanced Bitcoin system performance compared with the other existing schemes [4], [7], [13] under different miner numbers. The proposed scheme can monitor constantly the current Bitcoin system condition to adapt highly dynamic environments. In particular, each individual operator and miner in our multi-leader multi-follower Stackelberg game model acquire information from the system environment, gain knowledge, and make intelligent decisions in a self-adapting manner. Therefore, we can get an attractive system performance, while the DCPS scheme [13], the CGBM scheme [7], and the GBBM scheme [4] cannot offer such an appropriate Bitcoin system performance.

V. SUMMARY AND CONCLUSIONS

In the traditional finance transaction system, all transaction information is managed centrally, and users are not authorized to freely access or to publicly review their transaction information. Therefore, the classical centralized systems have some problems that need to be overcome. To address this challenge, Bitcoin has caught the attention of researchers as a peer-to-peer electronic payment system and digital currency. However, few work has been done to develop an effective mining pool mechanism. In this study, we use game theory to model the interactions among independent decision-makers, i.e., pool operators and miners, and enforce collaborative behaviors. To gain a fair-efficient Bitcoin mining solution, we design a novel multi-leader multi-follower Stackelberg game. In our game model, both leaders and followers can benefit from the multiple mining pool mechanism, and a win-win situation can be achieved. Based on the desirable features of different bargaining solutions, self-regarding miners are induced to actively participate in the fair-efficient Bitcoin mining process. To demonstrate the validity of our scheme, we compare our proposed approach with existing schemes, and demonstrate that our approach outperforms the existing schemes in a simulation environment.

Although we have achieved our goals in the Bitcoin mining process, we believe there is further scope for improving the efficiency of the Bitcoin system. Issues for further research include the design and validation of differential privacy. In addition, our work could be extended to investigate the cryptography algorithm in decentralized Bitcoin network environments. Based on the game theory, cryptography issues in Bitcoin operations are still needed to be studied and improved.

COMPETING OF INTERESTS

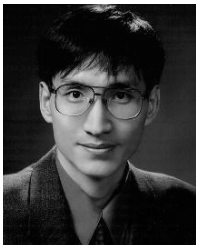
The author, Sungwook Kim, declares that there is no competing interests regarding the publication of this paper.

AUTHOR' CONTRIBUTION

Sungwook Kim is a sole author of this work and ES (i.e., participated in the design of the study and performed the statistical analysis).

REFERENCES

[1] A. Beikverdi and J. Song, "Trend of centralization in Bitcoin's distributed network," in *Proc. IEEE/ACIS SNPD*, Jun. 2015, pp. 1–6.
[2] P.-W. Chen, B.-S. Jiang, and C.-H. Wang, "Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet," in *Proc. IEEE WiMob*, Oct. 2017, pp. 139–146.
[3] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, p. e0163477, 2016, doi: 10.1371/journal.pone.0163477.
[4] S. Kim, "Group bargaining based bitcoin mining scheme using incentive payment process," *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 11, pp. 1486–1495, 2016.
[5] H. Kopetz, "On the design of distributed time-triggered embedded systems," *J. Comput. Sci. Eng.*, vol. 2, no. 4, pp. 340–356, 2008.
[6] K.-H. K. Kim and J. A. Colmenares, "Maximizing concurrency and analyzable timing behavior in component-oriented real-time distributed computing application systems," *J. Comput. Sci. Eng.*, vol. 1, no. 1, pp. 56–73, 2007.
[7] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proc. Int. Conf. Auton. Agents Multiagent Syst.*, 2015, pp. 919–927.
[8] M. Salimitari, M. Chatterjee, M. Yuksel, and E. Pasiliao, "Profit maximization for Bitcoin pool mining: A prospect theoretic approach," in *Proc. IEEE CIC*, Oct. 2017, pp. 267–274.
[9] S. Kim, *Game Theory Applications in Network Design*. Hershey, PA, USA: IGI Global, 2014.
[10] H. Zhang, M. Bennis, L. A. DaSilva, and Z. Han, "Multi-leader multi-follower stackelberg game among Wi-Fi, small cell and macrocell networks," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 4520–4524.
[11] I. Eyal, "The miner's dilemma," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 89–103.
[12] M. Rosenfeld. (2011). "Analysis of Bitcoin pooled mining reward systems." [Online]. Available: https://arxiv.org/abs/1112.4980
[13] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, "On power splitting games in distributed computation: The case of Bitcoin pooled mining," in *Proc. IEEE CSF*, Jul. 2015, pp. 397–411.
[14] J.-H. Kim, K.-J. Lee, T.-H. Kim, and S.-B. Yang, "Effective routing schemes for double-layered peer-to-peer systems in MANET," *J. Comput. Sci. Eng.*, vol. 5, no. 1, pp. 19–31, 2011.
[15] B.-D. Kim, C. Rosales-Fernandez, and S. Kim, "Computational methods for on-node performance optimization and inter-node scalability of HPC applications," *J. Comput. Sci. Eng.*, vol. 6, no. 4, pp. 294–309, 2012.
[16] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, "A brief survey of cryptocurrency systems," in *Proc. IEEE PST*, Dec. 2016, pp. 745–752.
[17] W. Jung and S. Park, "Preventing DDoS attack in blockchain system using dynamic transaction limit volume," *Int. J. Control Automat.*, vol. 10, no. 12, pp. 131–138, 2017.
[18] S. Cho, S. Y. Park, and S. R. Lee, "Blockchain consensus rule based dynamic blind voting for non-dependency transaction," *Int. J. Grid Distrib. Comput.*, vol. 10, no. 12, pp. 93–106, 2017.
[19] M. Rosenfeld. (2011). "Analysis of Bitcoin pooled mining reward systems." [Online]. Available: https://arxiv.org/abs/1112.4980
[20] A. Gosavi, S. Agarwal, and C. H. Dagli, "Predicting response of risk-seeking systems during project negotiations in a system of systems," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1557–1566, Sep. 2017.
[21] S. Kim, "Intervenient stackelberg game based bandwidth allocation scheme for hierarchical wireless networks," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 12, pp. 4293–4304, 2014.
[22] A. E. Roth and U. G. Rothblum, "Risk aversion and Nash's solution for bargaining games with risky outcomes," *Econometrica*, vol. 50, no. 3, pp. 639–647, 1982.
[23] G. Alnwaimi, S. Vahid, and K. Moessner, "Dynamic heterogeneous learning games for opportunistic access in LTE-based macro/femtocell deployments," *IEEE Trans. Wireless Commun.*, vol. 14, no. 4, pp. 2294–2308, Apr. 2015.
[24] M. Dianati, X. Shen, and S. Naik, "A new fairness index for radio resource allocation in wireless networks," in *Proc. IEEE WCNC*, vol. 2, Mar. 2005, pp. 712–715.
[25] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers Stackelberg game scheme," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 197–209, Jan. 2018.
[26] H. Fang, L. Xu, and X. Huang, "Self-adaptive trust management based on game theory in fuzzy large-scale networks," *Soft Comput.*, vol. 21, no. 4, pp. 907–921, 2017.



SUNGWOOK KIM received the B.S. and M.S. degrees in computer science from Sogang University, Seoul, South Korea, in 1993 and 1995, respectively, and the Ph.D. degree in computer science from Syracuse University, Syracuse, NY, USA, in 2003, under the supervision of Prof. P. K. Varshney. He has held faculty positions at the Department of Computer Science, Chung-Ang University, Seoul. In 2006, he returned to Sogang University, where he is currently a Professor with the Department of Computer Science and Engineering, and the Research Director of the Network Research Laboratory. His research interests include resource management, online algorithms, adaptive quality of service control, and game theory for network design.