Decentralized Mining Pool Games in Blockchain

Zhihuai Chen
Institute of Computing Technology
Chinese Academy of Sciences
Beijing, China
chenzhihuai@ict.ac.cn

Xiaoming Sun
Institute of Computing Technology
Chinese Academy of Sciences
Beijing, China
sunxiaoming@ict.ac.cn

Xiaohan Shan
Department of Computer Science and Technology
Tsinghua University
Beijing, China
shanxiaohan@tsinghua.edu.cn

Jialin Zhang
Institute of Computing Technology
Chinese Academy of Sciences
Beijing, China
zhangjialin@ict.ac.cn

***Abstract*—We use cooperative game theory to model mining pools and design reward allocation schemes in this paper. Specifically, we propose a cooperative game model named as "Decentralized Mining Pool Game (DMPG)". The player set of DMPG is the set of all pool managers and the utility function is defined as the sum of block rewards and transaction fees. In our model, we take miners in pools as normal nodes rather than only as computational powers, that is, all miners joining mining pools also participate in the propagation and validation of transactions in the network, this setting can effectively avoid the formation of centralized mining pools. We design two kinds of reward allocation schemes for DMPG and present efficient methods to compute them. One scheme is the stable allocation scheme which focuses on maintaining the rationality of miners (i.e. the core of DMPG) and the security of mining pools (i.e. resistance to pool block withholding attack). The other kind of scheme is the fair allocation scheme which focuses on the fairness of miners (i.e. the Shapley value of DMPG).**

***Index Terms*—cooperative game; blockchain; mining pool; core; Shapley value**

I. Introduction

In the past decade, Bitcoin became the most influential peer-to-peer digit crypto-currency. The key technique in Bitcoin – blockchain is a distributed tamper-proof ledger which prevents altering confirmed transaction records and then provides trustless but secure trade channel for the users in a decentralized network. To be more precise, the blockchain is a chain of block storing the verified transactions, and it grows in an append-only method with new verified block containing new verified transactions. Indeed, such decentralized system is very dependent on transaction propagation to ensure its proper function. But, it becomes an issue that the users in such a decentralized network is a motivational to diffuse the transaction that he receives. One reason is that the informed users can't benefit from delivering such a information, the other reason is that they realize that they have more chance to obtain the transaction fees by keeping those transactions.

The direct incentive of miners is to gain the payoff by mining a block, and their payoff can be divided into two parts: the block reward for their effort that proposing a block and the transaction fees inclused in the this proposed block. The block reward can be seen as a constant number in a short term and the transaction fees is dependent on the volume of trades recorded in this block. If a selfish miner receives a transacton with high transaction fee, he will prefer to reserve it in his own mining block. This motivates us to consider such problem in the perspective of game theory, specially the cooperative game.

A cooperative game $\Gamma = (V, \gamma)$ consists of a player set $V = \{1, 2, \ldots, n\}$ and a profit function $\gamma : 2^V \to \mathbb{R}$ with $\gamma(\emptyset) = 0$. A subset of players $S \subseteq V$ is called a *coalition* and V is called the *grand coalition*. For each coalition S, $\gamma(S)$ represents the profit obtained by S without help of other players. An allocation over the players is denoted by a vector $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ whose components are one-to-one associated with players in V, where $x_i \in \mathbb{R}$ is the value received by player $i \in V$ under allocation x. For any player set $S \subseteq V$, we use the shorthand notation $x(S) = \sum_{i \in S} x_i$. A set of all allocations satisfying some specific requirements is called a *solution concept*.

The *core* [8], [15] is one of the earliest and most attractive solution concepts that directly addresses the issue of stability. The core of a game is the set of allocations ensuring that no coalition would have an

978-1-7281-8156-1/20/$31.00 ©2020 IEEE
DOI 10.1109/ICBK50248.2020.00067

incentive to split from the grand coalition, and do better on its own. More precisely, the core of a game Γ (denoted by $\mathcal{C}(\Gamma)$), is the following set of allocations: $\mathcal{C}(\Gamma)$=$\{x \in \mathbb{R}^n : x(V) = \gamma(V), x(S) \geq \gamma(S),\ \forall\ S \subseteq V\}$. Intuitively, the requirement of $x(S) \geq \gamma(S)$ means that the coalition S receives profit allocation $x(S)$ that is at least their profit contribution $\gamma(S)$, so they would prefer to stay with the grand coalition.

In 1950s, Shapley [14] proposed another solution-concept of payoff assignment problem, called Shapley value. With such a concept, the payoffs are allocated according to the players' individual marginal contributions to the game. To be more precise, in this solution-concept, a player's individual contribution is defined as the weighted average marginal increase in the payoff of any coalition that he may join. Shapley value is famous and important solution-concept, since it is the unique division scheme such that:

(i) efficiency - the full payoff of the grand coalition is totally divided to the players;
(ii) symmetry - the payoffs to the players don't depend on their identity;
(iii) dummpy player - if a player's contribution to any coalition is exactly the amount he can achieve alone, the payoff he received equals to exactly the amount that he can gain on his own;
(iv) additivity axioms - if the game is summation of two sub-game, then the allocation solution is summation of two sub-allocation as well.

A. Contributions

We formulate mining pools in blockchain as cooperative games in which miners contribute not only computational powers but also unconfirmed transactions. Having the mining pool game model, we study allocation schemes from different perspectives. Specifically, we summarize our main contributions as follows.

(i) We model the mining pool as a cooperative game model named as Decentralized Mining Pool Game (DMPG). The player set of DMPG is defined as miners in blockchain systems and the utility function is defined as the sum of transaction fees and block rewards.
(ii) We propose two kinds of allocation schemes for DMPG: fair allocation and stable allocation. Specifically, the fair allocation scheme is the Shapley value of DMPG and the stable allocation scheme has three properties: efficiency, rationality and pool block withholding attack resistance.
(iii) For the fair allocation scheme (Shapley value), we prove that the Shapley value of DMPG can be computed in polynomial time.
(iv) We present a stable allocation for DMPG.

B. Related Works

Cooperative game theory is a branch of (micro-)economics that studies the behavior of self-interested agents in strategic settings where binding agreements between agents are possible [3]. Numerous classical studies about cooperative game provide rich mathematical framework to solve issues related to cooperation in multi-agent systems [4], [5].

The mining pool is the gathering result of miners, which is a typical game theory scenario. Thus, there are many studies that use game theory to analyse mining pools [11]. In [10], authors proved that there are always some miners that have an incentive to leave their pools and join other pools to increase their utility if the reward allocation of pools is non-linearity. [2] used cooperative game theory to analyse the respective aspect of interactions among the miners and pools. [13] used non-cooperative game theory to analyse the interactions between the miners and the pool manager and show that If a certain condition is satisfied, the strategy that each miner reports the shares immediately is the Nash equilibrium. [7] used a repeated game to study the case that miners report the shares repeatedly, and the pool manager can optimize its reward allocation to maximize its utility.

To the best of our knowledge, most game models defining on mining pools ignore the possibility that miners could join the network and contribute to transaction fees. In this paper, we present a cooperative game model that take miners not only as "computational powers" but also as normal "nodes" in blockchain system.

II. Model

A. Decentralized Mining Pool Games (DMPG)

A decentralized mining pool game is denoted by $\Gamma = (V, \gamma)$, where $V = \{1, 2, \ldots, N\}$ is the player set represents the set of miners for some blockchain systems.

Each miner $i \in V$ associates two parameters, one is his computational power q_i and the other is the set of unconfirmed transactions T_i he holds, we use $q(S) = \sum_{j \in S} q_j$ to denote the total computational power of miners in S and use $T_S = \bigcup_{i \in S} T_i$ to denote all unconfirmed transactions held by the miner set $S \subseteq V$.

For each transaction $t \in T_V$, suppose c_t be the transaction fee of t and c_t will be awarded to the miner who makes it confirmed. We use $c(T)$ to represent the total fee in transaction set T, that is, $c(T) = \sum_{t \in T} c_t$.

For each coalition $S \subseteq V$, the utility of S is the expected benefits obtained by S and the formula is defined as following,

$$\gamma(S) = \frac{q(S)}{m}(g(S) + \alpha), \tag{1}$$

where α is the block reward and $g(S)$ is the transaction reward defined as the sum of the top ℓ transactions in T_S. Specifically, suppose $T_S = \{t_1, t_2, \cdots, t_{T_S}\}$ with $c_{t_1} \geq c_{t_2} \geq \cdots \geq c_{t_{T_S}}$, the top ℓ transactions in T_S is defined as $T_S^\ell = \{t_1, t_2, \cdots, t_\ell\}$ then

$$g(S) = \sum_{t \in T_S^\ell} c_t.$$

Notice that the utility function defined above is super-additive (see Lemma 1), so intuitively, players are prefer to work together.

Lemma 1. *The utility function $\gamma(S)$ is super-additive, that is, $\gamma(A \cup B) \geq \gamma(A) + \gamma(B)$ for any $A, B \subseteq V$ and $A \cap B = \emptyset$.*

Proof. For any $A, B \subseteq V$ and $A \cap B = \emptyset$, we have,

$$\begin{aligned}\gamma(A \cup B) &= \frac{q(A)+q(B)}{m}(g(A \cup B) + \alpha) \\ &\geq \frac{q(A)+q(B)}{m}(\max\{g(A), g(B)\} + \alpha) \\ &\geq \frac{q(A)}{m}(g(A) + \alpha) + \frac{q(B)}{m}(g(B) + \alpha) \\ &= \gamma(A) + \gamma(B).\end{aligned}$$

□

For easy reference, we list the notations as follows:

- $V = \{1, 2, \cdots, N\}$: the grand player set, i.e., the set of all miners.
- q_i: computational power of miner $i \in V$.
- $q(S)$: computational power of miner set S, $q(S) = \sum_{j \in S} q_j$, for any $S \subseteq V$.
- $V_1, V_2, \cdots, V_n$: mining pools.
- $m_1, m_2, \cdots, m_n$: computational powers of pools.
- m: total computational power, $m = \sum_{i \in [n]} m_i = \sum_{j \in [N]} q_j$.
- $g(S)$: transaction fee obtained by miner set S, for any $S \subseteq V$.
- α: system rewards for proposing a block.
- ϕ_{ij}: the rewards pool V_i allocates to miner j.

B. Allocation schemes of DMPG

In this section, we consider allocation schemes of DMPG, i.e., how to allocate the total rewards of a mining pool into its miners.

Given an instance of DMPG $G = (V = V_1 \cup V_2 \cup \cdots \cup V_n, \gamma)$, we use ϕ to denote an allocation scheme and ϕ_{ij} is the rewards that pool V_i allocates to miner j, for any $i \in \{1, 2, \cdots, n\}$ and $j \in V_i$. Let $\phi(S) = \sum_{j \in S} \phi_{ij}$ be the total rewards allocated to coalition S from mining pool V_i, for any $i \in \{1, 2, \cdots, n\}$ and $S \subseteq V_i$. When phi is a random allocation scheme, we use $E[\phi_{ij}]$ to denote the expected rewards that pool i allocates to miner j.

We propose two kinds of allocation schemes of DMPG, *stable allocation* and *fair allocation*. The stable allocation scheme focuses on the stability of players and the security of the system. Specifically, the stability of players corresponds to the core of cooperative game, that is, players are prefer to stay at the current mining pool; the security of the system means that no one would like to launch the block withholding attack. The fair allocation scheme corresponds to the Shapley value in the cooperative game theory.

Definition 1 (Stable allocation scheme)**.** *Given an instance of DMPG $G = (V = V_1 \cup V_2 \cup \cdots \cup V_n, \gamma)$, an allocation ϕ is a stability allocation of G if and only if ϕ satisfies the following properties:*

- *Efficiency: The efficiency property demands that a mining pool should distribute all rewards to its miners when this pool proposes a block successfully, that is , $\phi(V_i) = g(V_i) + \alpha$, for any $i \in \{1, 2, \cdots, n\}$.*
- *Rationality: The rationality property demands that there is no miner preferring to deviate from the current mining pool, that is, for any $S \in V_i$ and $i \in \{1, 2, \cdots, n\}$, $E[\phi(S)] \geq \gamma(S)$, where $E[\phi(S)]$ is the expected value of $\phi(S)$.*
- *Pool Block Withholding Attack (PBWA) Resistance: This property means that no pool has the incentive to launch a pool withholding attack.*

Now we introduce the pool block withholding attack. It is shown in [6] that the permissionless mining pools have strong incentives to launch the *pool block withholding attacks (PBWA)* on each other: one strategic pool manager sends some of her miners to other pools and these miners pretend to work on the puzzles but actually do nothing. In Bitcoin or any decentralized system, the pool managers are not able to recognize such malicious miners, thus these miners can still obtain the reward from mining pool proportional to their computing powers.

Eyal [6] modelled the above scenario as *pool block withholding games (PBWG)* and we redefine the definition of PBWG with the notation system in our paper now.

PBWA is also demonstrated in [12] with a different reward function. and showed that with any number of pools, no-pool-attacks is not a Nash equilibrium. When there are two pools, the situation faced by the two managers is similar to prisoner's dilemma, which is called *miner's dilemma*: in an equilibrium, both manages launch the PBW attack and accordingly earn less rewards compared to when they mine honestly. Alkalay-Houlihan and Shah [1] further studied the miner's dilemma between two strategic mining pools and obtained the bound of the social loss due to noncooperation, i.e., price of anarchy. They showed that the pure Nash equilibrium always exists, and the pure price of anarchy is at most 3 in this game. They also conjectured the tight bound

should be 2 and demonstrated this in some special cases.

The players in a PBWG are the managers of n mining pools, denoted by $U = \{U_1, U_2, \cdots U_n\}$. Let $m_i \in \mathbb{R}^+$ be the mining power of manager $U_i \in U$. Assume m is the total mining power in the system and $m \geq \sum_{U_i \in U} m_i$. For any player U_i, U_i's strategy space is all possible $S_i = (S_{ij})_{j \in U \setminus \{U_i\}}$ such that $\sum_{j=1}^{n} w_{ij} \leq m_i$ and $w_{ij} \geq 0$ for all $U_j \in U \setminus \{U_i\}$, where $w_{ij} = q(S_{ij})$. Each S_{ij} with $j \neq i$ represents the miner set that U_i wants to infiltrate pool U_j. Denote by $\mathbf{S} = (S_1, \cdots, S_n)$ a full strategy profile.

Each player U_i's reward $r_i(\mathbf{S})$ in PBWA consists of two parts: *direct reward* and *infiltrating reward*. The direct reward is produced by U_i's mining and the infiltrating reward comes from sharing in other pools.

In the rest of this paper, we propose a stability allocation and a polynomial algorithm to compute fairness allocations of DMPG.

III. Stable Allocation Scheme

In this section, we propose a stability allocation scheme. Given an instance of DMPG $G = (V = V_1 \cup V_2 \cup \cdots \cup V_n, \gamma)$, let ϕ^s be an allocation with the following formula:

$$\phi^s_{ij} = \begin{cases} \alpha + \frac{q_j}{m_i} g(V_i), & \text{if } j \text{ proposes a block successfully} \\ \frac{q_j}{m_i} g(V_i), & \text{if a miner in } V_i \setminus \{j\} \text{ proposes a block successfully} \\ 0, & otherwise \end{cases}$$

Now we prove that the allocation ϕ^s defined above is a stable allocation of G.

Theorem 1. *ϕ^s is a stability allocation.*

In the rest of this section, we prove Theorem 1 by proving Lemma 2 to Lemma 4

Lemma 2 (Efficiency of ϕ^s)**.** *ϕ^s satisfies the efficiency property in Definition 1, that is, $\phi^s(V_i) = g(V_i) + \alpha$ if a miner in poo V_i propose a block successfully.*

Proof. Suppose miner u in pool V_i proposes a block successfully, then we only need to prove that $\phi^s(V_i) = g(V_i) + \alpha$.

$$\begin{aligned} \phi^s(V_i) &= \sum_{j \in V_i} \phi^s_{ij} \\ &= \phi^s_{iu} + \sum_{j \in V_i \setminus \{u\}} \phi^s_{ij} \\ &= \alpha + \frac{q_u}{m_i} g(V_i) + \sum_{j \in V_i \setminus \{u\}} \frac{q_j}{m_i} g(V_i) \\ &= \alpha + \sum_{j \in V_i} \frac{q_j}{m_i} g(V_i) \\ &= \alpha + g(V_i). \end{aligned}$$

□

Lemma 3 (Rationality)**.** *Given an instance of DMPG $G = (V = V_1 \cup V_2 \cup \cdots \cup V_n, \gamma)$ and any mining pool $V_i \subseteq V$, $E[\phi^s(S)] \geq \gamma(S)$ for any miner set $S \subseteq V_i$.*

Proof.

$$\begin{aligned} &E[\phi^s(S)] = \sum_{j \in S} E[\phi^s_{ij}] \\ =&\sum_{j \in S} [\frac{q_j}{m} (\frac{q_j}{m_i} (g(V_i) + \alpha)) + \frac{m_i - q_j}{m} (\frac{q_j}{m_i} g(V_i))] \\ =&\sum_{j \in S} [\frac{q_j}{m} (g(V_i) + \alpha) \\ \geq&\frac{q(S)}{m} (g(S) + \alpha) = \gamma(S). \end{aligned}$$

□

In the rest of this section, we prove that allocation ϕ^s satisfies the pool withholding attack resistance property.

Given an instance of DMPG $G = (V = V_1 \cup V_2 \cup \cdots \cup V_n, \gamma)$ with allocation scheme ϕ^s, we define an instance of PBWG $G_P$as follows. The player set of G_P is $U = \{U_1, U_2, \cdots, U_n\}$ and U_i represents the manager of mining pool i, the utility function of G_P is denoted by r and r is defined as the sum of directed reward and infiltrating reward under ϕ^s.

Lemma 4 (Pool Block Withholding Attack Resistance)**.** *Suppose $m \geq 2m_i$ and $\alpha \geq 2g(V)$, then no pool launches pool withholding attack is a Nash equilibrium of G_P.*

Proof. When there is no pool launching withholding attack, for any $i \in \{1, 2 \cdots, n\}$, the utility of pool V_i is

$$r_i(0, 0, \cdots, 0) = \frac{m_i}{m} (g(V_i) + \alpha)$$

To simplify notations, we only prove that pool V_1 has no incentive to launch a block withholding attack. Suppose pool V_1 sending miner set S_1 to other pools to launch withholding attacks. Suppose $S_1 = S_{12} \cup S_{13} \cdots \cup S_{1n}$ and $q(S_1) = x_1 = \sum_{i \in \{2, \cdots, n\}} w_{1i}$, where S_{1i} is the miner set attacking pool V_i from pool V_1 and the corresponding computational power is $q(S_{1i}) = w_{1i}$, for any $i \in \{2, \cdots, n\}$. In this case,

$$
\begin{aligned}
& r_1(w_1, 0, \cdots, 0) \\
=& \frac{m_1 - w_1}{m - x_1}(g(V_i \setminus \{S\}) + \alpha) \\
& + \frac{m_2}{m - x_1} \cdot \frac{w_{12}}{m_2 + w_{12}} g(V_2 \cup S_{12}) \\
& + \cdots + \frac{m_n}{m - w_1} \cdot \frac{w_{1n}}{m_n + w_{1n}} g(V_n \cup S_{1n}) \\
=& \frac{m_1 - w_1}{m - w_1}(g(V_i \setminus \{S\}) + \alpha) \\
& + \frac{1}{m - w_1} \sum_{i=2}^{n} \frac{m_i w_{1i}}{m_i + w_{1i}} g(V_i \cup S_{1i}).
\end{aligned}
$$

Given any constant $k_1, k_2 \geq 2$, suppose $\alpha \geq k_1 g(V)$ and $m \geq k_2 m_i$, for any $i \in [n]$, we have,

$$
\begin{aligned}
& r_1(0, 0, \cdots, 0) - r_1(w_1, 0, \cdots, 0) \\
=& \frac{m_1}{m}(g(V_1) + \alpha) - \frac{m_1 - w_1}{m - w_1}(g(V_i \setminus \{S\}) + \alpha) \\
& - \frac{1}{m - w_1} \sum_{i=2}^{n} \frac{m_i w_{1i}}{m_i + w_{1i}} g(V_i \cup S_{1i}) \\
=& \frac{m_1 - w_1}{m - w_1}(g(V_1) - g(V_i \setminus \{S\})) \\
& + \frac{w_1(m - m_1)}{m(m - w_1)}(g(V_1) + \alpha) \\
& - \frac{1}{m - w_1} \sum_{i=2}^{n} \frac{m_i w_{1i}}{m_i + w_{1i}} g(V_i \cup S_{1i}) \\
\geq& \frac{w_1(m - m_1)}{m(m - w_1)}\alpha - \frac{1}{m - w_1} \sum_{i=2}^{n} \frac{m_i w_{1i}}{m_i + w_{1i}} \cdot \frac{1}{k_1}\alpha \\
=& \frac{\alpha}{m - w_1} \sum_{i=2}^{n} \frac{w_{1i}(m - m_1)}{m} \\
& - \frac{1}{m - w_1} \sum_{i=2}^{n} \frac{m_i w_{1i}}{m_i + w_{1i}} \cdot \frac{1}{k_1}\alpha \\
\geq& \frac{\alpha}{m - w_1} \sum_{i=2}^{n} \frac{w_{1i}(m - m_1)}{m} \\
& - \frac{1}{m - w_1} \sum_{i=2}^{n} \frac{m_i w_{1i}}{m_i + 0} \cdot \frac{1}{k_1}\alpha \\
=& \frac{\alpha}{m - w_1} \sum_{i=2}^{n} w_{1i}(1 - \frac{m_1}{m} - \frac{1}{k_1}) \\
\geq& \frac{\alpha}{m - w_1} \sum_{i=2}^{n} w_{1i}(1 - \frac{1}{k_2} - \frac{1}{k_1}) \\
\geq& 0.
\end{aligned}
$$

□

IV. Fair Allocation Scheme (Shapley Value)

A widely used solution-concept in cooperative game theory is Shapley value [14], which reassigned the payoff according the relative importance of a individual player in the game. Comparing with the core, Shapley value is motivated by the fairness of a game but it maybe not stable. Fairness is more important than stable from the perspective of incentiving the miner to share all his transactions and solve the puzzle. For example, if two miners with same computational power but one has lots of transactions while the other has a few. They still got the same reward according to the solution $x_i = \frac{q_i}{m}(g(V) + \alpha)$. Therefore, finding a fair solution is necessary. Fortunately, Shapley value always exists for any coalitional game.

Theorem 2. *Given a coalitional game $G = (N, v)$, there is a unique payoff division $x(v) = \phi(N, v)$ that divides the full payoff of the grand coalition and that satisfies the Symmetry, Dummy player and Additivity axioms.*

Such a unique value is called Shapley value and is defined as following

Definition 2 (Shapley value)**.** *Let $G = (N, f)$ be a cooperative game, the Shapley value is*

$$
\phi_i(N, f) = \frac{1}{n} \sum_{S \subseteq N \setminus i} \binom{n-1}{|S|}^{-1} \Delta_i r(S)
$$

However, computing Shapley value is difficult when the number of players grows rapidly. To be more precise, the computation of Shapley value is NP-hard in general, e.g., weighted voting game [9]. But by exploring the structure of our game, we figure out a brief method to compute Shapley value efficiently.

Theorem 3. *The Shapley value of this game can be computed in polynomial time.*

Proof. Let T_i be the transactions held by miner i and $T_S = \bigcup_{i \in S} T_i$.

$$
\begin{aligned}
& \Delta_i r(S) = \frac{q(S) + q(i)}{m}(\alpha + g(S \cup i)) \\
=& \frac{q(S)}{m} c(T_i \backslash T_S) + \frac{q(i)}{m}(c(T_S \cup T_i)) + \frac{\alpha q(i)}{m} \\
=& \frac{q(S)}{m} c(T_i \backslash T_S) + \frac{q(i)}{m} c(T_i \backslash T_S) + \frac{q_i}{m} c(T_S) + \frac{\alpha q(i)}{m}
\end{aligned}
$$

In order to simplify Shapley value, we divide it into four parts. For the summation on the first term,

$$
\begin{aligned}
& \frac{1}{n} \sum_{S \subseteq N \setminus i} \binom{n-1}{|S|}^{-1} \frac{q(S)}{m} c(T_i \backslash T_S) \\
=& \frac{1}{n} \sum_{t \in T_i} c_t \sum_{S \subseteq N \setminus i} \binom{n-1}{|S|}^{-1} \frac{q(S)}{m} \mathbb{1}_{x \notin T_S}
\end{aligned}
$$

Let $B(t)$ be the set of miners who don't hold transaction t and c_t be the transaction fee of t. Then

$$
\begin{aligned}
&\frac{1}{n}\sum_{S\subseteq N\setminus i}\binom{n-1}{|S|}^{-1}\frac{q(S)}{m}c(T_i\backslash T_S)\\
=&\frac{1}{n}\sum_{t\in T_i}c_t\sum_{S\subseteq B(t)}\binom{n-1}{|S|}^{-1}\frac{q(S)}{m}\\
=&\frac{1}{mn}\sum_{t\in T_i}c_t\sum_{s=0}^{|B(t)|}\binom{n-1}{s}^{-1}\sum_{j\in B(t)}q(j)\sum_{\substack{S\subseteq B(t)\\|S|=s}}\mathbb{1}_{j\in S}\\
=&\frac{1}{mn}\sum_{t\in T_i}c_t\sum_{s=1}^{|B(t)|}\binom{|B(t)|-1}{s-1}\binom{n-1}{s}^{-1}q(B(t))\\
=&\frac{1}{m}\sum_{t\in T_i}\frac{c_tq(B(t))}{(n-|B(t)|+1)(n-|B(t)|)}
\end{aligned}
$$

With similar caculation, we give a simple form for summation on the second term

$$
\frac{1}{n}\sum_{S\subseteq N\setminus i}\binom{n-1}{|S|}^{-1}\frac{q(i)}{m}c(T_i\backslash T_S)=\sum_{t\in T_i}\frac{c_tq(i)}{m(n-|B(t)|)}
$$

For the third part, we have

$$
\begin{aligned}
&\frac{1}{n}\sum_{S\subseteq N\setminus i}\binom{n-1}{|S|}^{-1}\frac{q(i)}{m}c(T_S)\\
=&\frac{q(i)}{mn}\sum_{S\subseteq N\setminus i}\binom{n-1}{|S|}^{-1}\sum_t c_t\mathbb{1}_{t\in T_S}\\
=&\frac{q(i)}{mn}\sum_t c_t\sum_{s=0}^{n-1}\binom{n-1}{|S|}^{-1}\sum_{\substack{S\subseteq N\setminus i\\|S|=s}}\mathbb{1}_{t\in T_S}
\end{aligned}
$$

Notice that the last summation counts the number of subset that don't hold transation t, thus

$$
\begin{aligned}
&\frac{1}{n}\sum_{S\subseteq N\setminus i}\binom{n-1}{|S|}^{-1}\frac{q(i)}{m}c(T_S)\\
=&\frac{q(i)}{mn}\sum_t\sum_{s=0}^{n-1}\frac{\binom{n-1}{s}-\binom{|B(t)\setminus i|}{s}}{\binom{n-1}{s}}\\
=&\frac{q(i)}{mn}\sum_t(n-\frac{n}{n-|B(t)\backslash i|})
\end{aligned}
$$

And the summation on the fouth term is simply $\frac{q_i\alpha}{m}$. Finally, we conclude that the Shapley value for $G=(V,f)$ is

$$
\begin{aligned}
&\phi_i(V,f)\\
=&\frac{1}{m}\sum_{t\in T_i}\frac{c_tq(B(t))}{(n-|B(t)|+1)(n-|B(t)|)}\\
+&\sum_{t\in T_i}c_t\frac{q(i)}{m(n-|B(t)|)}\\
+&\frac{q(i)}{mn}\sum_t(n-\frac{n}{n-|B(t)\backslash i|})\\
+&\frac{q_i\alpha}{m}
\end{aligned}
$$

which can be computed in time linear in number miners times number of transactions. □

V. Conclusions

In this paper, we model the process of propogation and mining as a cooperative game. And in this game, the total reward of the grand coalition consist of the block reward and the transaction fees that shared by all miners. In order to make such a coaltition solid, we consider the allocation solutions in the perspective of stability and the fairness. In the term of stability, we show a simple distribution in the core which make sure not smaller group will escape and form a new coalition. We also prove that withholding attack will not happen with such an allocation. And for the fairness, we simplify the Shapley value into a brief form and therefore make it computable in polynomial time.

VI. Acknowledgment

This work was supported in part by the 973 Program of China Grant No. 2016YFB1000201, the National Natural Science Foundation of China Grants No. 61832003, 61761136014, 61872334, K.C.Wong Education Foundation.

References

[1] C. Alkalay-Houlihan and N. Shah. The pure price of anarchy of pool block withholding attacks in bitcoin mining. In *AAAI 2019*, 2019.

[2] L. Brünjes, A. Kiayias, E. Koutsoupias, and A. Stouka. Reward sharing schemes for stake pools. *CoRR*, abs/1807.11218, 2018.

[3] G. Chalkiadakis, E. Elkind, and M. Wooldridge. Computational aspects of cooperative game theory. *Synthesis Lectures on Artificial Intelligence and Machine Learning*, 5(6):1–168, 2011.

[4] V. Conitzer and T. Sandholm. Complexity of constructing solutions in the core based on synergies among coalitions. *Artificial Intelligence*, 170(6-7):607–619, 2006.

[5] X. Deng and C. H. Papadimitriou. On the complexity of cooperative solution concepts. *Mathematics of Operations Research*, 19(2):257–266, 1994.

[6] I. Eyal. The miner's dilemma. In *2015 IEEE Symposium on Security and Privacy*, pages 89–103, May 2015.

[7] B. Fisch, R. Pass, and A. Shelat. Socially optimal mining pools. In *Web and Internet Economics*, pages 205–218, Cham, 2017. Springer International Publishing.

[8] D. Gillies. *Some Theorems on n-Person Games*. PhD thesis, Princeton University, 1953.

[9] S. Kurz. Computing the power distribution in the imf. *Available at SSRN 2742118*, 2016.
[10] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein. Bitcoin mining pools: A cooperative game theoretic analysis. In *AAMAS*, May 2015.
[11] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y. Liang, and D. I. Kim. A survey on blockchain: A game theoretical perspective. *IEEE Access*, 7:47615–47643, 2019.
[12] 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 *2015 IEEE 28th Computer Security Foundations Symposium*, pages 397–411. IEEE, 2015.
[13] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden. Incentive compatibility of bitcoin mining pool reward functions. In *Financial Cryptography and Data Security - 20th International Conference, FC 2016, Revised Selected Papers*, pages 477–498. Springer Verlag, Jan. 2017. 20th International Conference on Financial Cryptography and Data Security, FC 2016 ; Conference date: 22-02-2016 Through 26-02-2016.
[14] L. S. Shapley. A value for n-person games. *Contributions to the Theory of Games*, 2(28):307–317, 1953.
[15] L. S. Shapley. Markets as cooperative games. In *IJCAIRand Corporation Memorandum*, 1955.