The Consensus Games for Consensus Economics Under the Framework of Blockchain in Fintech

Lan Di[1], Zhe Yang[2], and George Xianzhi Yuan[3,4,5,6,7(✉)]

[1] School of Digital Media, Jiangnan University, Wuxi 214122, China
dilan@jiangnan.edu.cn
[2] School of Economics, Shanghai University of Finance and Economics, Shanghai 200433, China
zheyang211@163.com
[3] Business School, Chenngdu University, Chengdu 610106, China
george_yuan@yahoo.com
[4] School of Financial Technology, Shanghai Lixin University of Accounting and Finance, Shanghai 201209, China
[5] Center for Financial Engineering, Soochow University, Suzhou 215008, China
[6] Business School, Sun Yat-Sen University, Guangzhou 510275, China
[7] BBD Technology Co., Ltd. (BBD), No. 966, Tianfu Avenue, Chengdu 610093, China

Abstract. The goal of this paper is to introduce a new notion called "Consensus Game (CG)" with motivation from the mechanism design of blockchain economy under the consensus incentives from Bitcoin ecosystems in financial technology (Fintech), we then establish the general existence results for consensus equilibria of consensus games in terms of corresponding interpretation based on the viewpoint of Blockchain consensus in Fintech by applying the concept of hybrid solutions in game theory. As applications, our discussion in this paper for the illustration of some issues and problems on the stability of mining pool-games for miners by applying consensus games shows that the concept of consensus equilibria could be used as a fundamental tool for the study of consensus economics under the framework of Blockchain economy in Fintech.

Keywords: Hybrid solutions · Consensus equilibrium · Consensus game · Nakamoto consensus · Bitcoin ecosystem · Blockchain Protocol · Blockchain economy · Stability · Longest chain rules (LCR) · Chain Fork · Nonordered preferences · Mining economics · Minier dilemma · Multi-pools game · Fintech

This research is supported by National Natural Science Foundation of China (Nos. 11501349 and U181140002) in Part.

D. Li (Ed.): EAGT 2019, CCIS 1082, pp. 1–26, 2019.
https://doi.org/10.1007/978-981-15-0657-4_1

1 Introduction

In the game theory, Nash equilibrium follows the noncooperatitive idea, while the core is defined by considering the cooperative behavior of players. They concern on the noncooperative and cooperative idea respectively. Generally speaking, a cooperative solution concept (the α–core) was first introduced by Aumann [5]. Later, Scarf [44] proved an nonemptiness result for the α–core in a normal-form game with continuous and quasiconcave payoff functions. Inspired by Scarf [44], Kajii [29] provided a generalization of Scarf [44] to games with nonordered preferences, and Kajii's result and proof technique is also a modification and development of Border [11]. On the other hand, Florenzano [20] provided a new proof technique to obtain an existence theorem of the core in a coalition production economy with nonordered preferences. In [20], Florenzano defined the group preferences of each coalition and gave the proof by using Gale and Mas-Colell fixed point theorem. Following the method of [20], Lefebvre [32] provided a generalization to an economy with different information, and Martins-da-Rocha and Yannelis [33] extended Kajii's result to games on Hausdorff topological vector spaces. For more work on the α–core, we can refer to [1–4, 28, 38, 39, 45, 48, 52–54] and references wherein.

With motivation from Zhao [57] and Kajii [29], as discussed by Yang and Yuan [54] recently, our first goal is to establish consensus games without ordered preferences from the viewpoint of Blockchain in Fintech. In briefly, the consensus game considers whether there exists an acceptable (may or may not be "optimal") collaborating strategy which consists of a partial cooperative strategy and a partial noncooperative strategy under a given consensus rule in which some participants are based on cooperative, and the other part based on noncooperative game strategies to follow "Mining Longest Chain Rules (LCR)" (see also the original idea due to Nakamoto [36], the study by Nyumbayire [40], Biais [9] and reference wherein), while with or without occurring forks for blockchain acting as a platform (in supporting for different types business activities so-called digital economy). Thus, comparing with the traditional cooperative and noncooperative game, the consensus game is a natural extension for consensus economy, especially under the framework of Bitcoin ecosystem associated with consensus incentives in Bitcoin ecosystems (in terms of Nakamoto's consensus protocol as one example). Moreover, by following the study for the stability of the blockchain in supporting Bitcoin ecosystems under general consensus (due to Nakamoto [36]) in terms of mining economics, mining games and pool games extensively studied by Kroll et al. [31], Eyal and Sirer [19], Eyal [18], Bonneau et al. [10] (see also Carlsten et al. [12], Kiayias et al. [30], Sapirstein et al. [43], Biais et al. [9] and references wherein), plus the study on the existence of equilibria for blockchain disruption with or without occurring forks by Biais [9], smart contracts discussed by Cong and He [15], and move toward blockchain-based accounting and assurance given by Dai and Vasarhelyi [17], and following the idea of Zhao [57], it seems that the notion of consensus equilibria for consensus games with a partition of the set of players through the nonordered preferences

mappings and related forms will be a useful tool for the study of consensus economics under the framework of Blockchain as a new kind of data structure in the practice.

Note that the classical results for the α–core concern on games with finitely many players. By considering a strong blocking concept, Weber [50] first proved an nonemptiness result for a core of a nontransferable cooperative game with infinitely many players. Inspired by Weber [50], Askoura [1] proved the existence of the weak core for games with a continuum of players. Later, Askoura [4] improved the result by considering the equi-usc condition of payoffs. Moreover, the work on the weak α–core was studied by Yang [52] and Yang [53]. Recently, Yang and Yuan [54] provided a generalization of Zhao [57] to games with nonordered preferences and proved the existence of weak hybrid solutions with infinitely many players.

In brief, we shall introduce a concept called "Consensus Game" (CG) with motivation from the mechanism design for the blockchain in financial technology under the consensus incentives introduced by Nakamoto [36] (see also Biais [9], Cong and He [15], Narayanan et al. [37], Nyumbayire [40] and related references wherein). Starting from results by Zhao [57] to Yang and Yuan [54] where a number of existence results have been established for a general game, while our paper mainly captures the consensus idea of blockchain consensus in Fintech, and the work of Yang and Yuan [54] plays an important role in modelling the Blockchain in Fintech, e.g., see Yuan et al. [58] and references wherein.

We like to share with readers that in this paper, we give a outline how the issue and problems on the stability of pool-games (e.g., the Bitcoin economy) can be formulated as applications of consensus games by using the concept of consensus equilibria, which could be used as a fundamental tool for the study of consensus economics under general framework of Blockchain economy in Fintech.

The rest of this paper is organized as follows. In Sect. 2, we recall the model and results from Zhao [57]. Section 3 recalls the main results from Yang and Yuan [54]. Section 4 illustrates how our notion of consensus games can be used easily to study the stability for Bitcoin ecosystems as applications of consensus games for two-pool games and multi-pools games, and Sect. 5 is the conclusion.

2 The Concept of Hybrid Solution in Game Theory

In this section, we recall some definitions and results from Zhao [57] (see also Yang and Yuan [54] and recent references wherein). Which were also recalled in Sect. 2 of [54]. For the sake of completeness for reading, we give their statements for results on Hybrid solution in game theory.

Let $N = \{1, \cdots, n_0\}$ be the set of agents and $p = \{N_1, \cdots, N_{k_0}\}$ be a partition of N, i.e.,

$$N_1 \bigcup \cdots \bigcup N_{k_0} = N,\ N_i \bigcap N_j = \emptyset, \forall i \neq j.$$

Denote by $\mathcal{N}$ the set of all nonempty subsets of N and $\mathcal{N}_r$ the set of nonempty subsets of N_r for each $r = 1, \cdots, k_0$.

A normal-form game with a partition can be defined by

$$G = (N, p, (X_i, u_i)_{i \in N}),$$

where X_i is the strategy set of player i, and $X = \prod_{i \in N} X_i$, $X_S = \prod_{i \in S} X_i$, $X_{-S} = \prod_{i \notin S} X_i, \forall S \in \mathcal{N}$; $u_i : X \longrightarrow R$ is the utility function of agent i. A strategy $x^* \in X$ is said to be a hybrid solution of G if for any $N_r \in p$ and any $S \in \mathcal{N}_r$, there exists no $y_S \in X_S$ such that

$$u_i(y_S, z_{N_r - S}, x^*_{-N_r}) > u_i(x^*_{N_r}, x^*_{-N_r}),\ \forall i \in S,\ \forall z_{N_r - S} \in X_{N_r - S}.$$

The following result is a stronger version of Theorem 2 in Zhao [57] (see also Theorem 2.1 of Yang and Yuan [54]).

Theorem 2.1. *Suppose that a normal-form game with a partition*

$$G = (N, p, (X_i, u_i)_{i \in N})$$

satisfies the following conditions:

(i) for each $i \in N$, X_i is a nonempty convex compact subset of R^{m_i};
(ii) for each $i \in N$, u_i is continuous and quasiconcave on X.

Then there exists at least a hybrid solution of G.

Furthermore, Zhao [57] defined a general cooperative game with a partition

$$G = \{G_r(x_{-N_r}) = (N_r, (X_S, u_S(\cdot, x_{-N_r}))_{S \in \mathcal{N}_r}) | r = 1, \ldots, k_0\},$$

where $u_S(\cdot, x_{-N_r}) : X_S \longrightarrow R^{|S|}$ is a vector-valued utility function of the coalition $S \in \mathcal{N}_r$ for any $x_{-N_r} \in X_{-N_r}$ and any $r = 1, \ldots, k_0$. A point $x^* \in X$ is a hybrid solution of G if for any $r = 1, \ldots, k_0$ and any $S \in N_r$, there exists no $y_S \in X_S$ such that

$$u_S(y_S, x^*_{-N_r}) > (u_N(x^*_{N_r}, x^*_{-N_r}))_S.$$

The following result is Theorem 3 of [57] (see also Theorem 2.2 of Yang and Yuan [54]).

Theorem 2.2 (Zhao [57]). *Suppose that a general cooperative game G with a partition p satisfies the following conditions:*

(i) for any $r = 1, \cdots, k_0$ and any $x_{-N_r} \in X_{-N_r}, G_r(x_{-N_r})$ is balanced;
(ii) for any $i \in N$, X_i is a nonempty convex compact subset of R^{m_i};
(iii) for any $N_r \in p$ and any $S \in \mathcal{N}_r$, u_S is continuous on $X_S \times X_{-N_r}$ and $u_S(\cdot, x_{-N_r})$ is quasiconcave on X_S for any $x_{-N_r} \in X_{-N_r}$.

Then there exists a hybrid solution of G at least.

3 The Concept of Consensus Games and Related Results

In this section, as applications of hybrid solutions, we shall introduce a new concept called "Consensus Game" (in short, "CG"), which is used in consensus economics to describe what kind of general consensus (through the realization of mechanism design) will achieve incentive compatibility to fight noncooperative behaviors and the coalition of participants (agents) under the platform of Blockchain in financial technology. Then we will discuss the existence of general consensus games' equilibria by using the concept of hybrid solutions. For the related reference on Blockchain and related Nakamoto consensus [36], please see Kroll et al. [31], Eyal and Sirer [19], Eyal [18], Bonnean et al. [10] (see also Carlsten et al. [12]), Kiayias et al. [30], Sapirstein et al. [43], Biais et al. [9], Nyumbayire [40], Narayanan [37] and related references wherein).

In the Fintech, in particular under the Nakamoto consensus protocol introduced in Year 2008, one key issue is to find a set of rules (for consensus) to encourage agents (miners from mining pools) to follow rules truthfully under the corresponding (consensus) protocol which may be formulated as preference mappings for abstract economy model (see Yannelis and Prabhakar [51], Yuan [55] and references wherein), thus it is very important to study the stability of Blockchain consensus in terms of equilibria for miners (from ming pools) to follow the so-called "Mining LCR" (also see the discussion in Sect. 4 below) while with or without occurring of forks for blockchain of Bitcoin ecosystems, the some other issues needed to be considered are possible collusive equilibria and their behavior related to smart contracts, or dynamic equilibria under blockchain disruption as initially discussed by Cong and He [15], and some other issues such as emerging blockchain-based accounting and assurance outlined by Dai and Varsarhelyi [17], discussed by Narayanan et al. [37] and so on.

Using the framework of the blockchain and associated consensus mechanism, the stability for Blockchain can be formulated as the question to find a strategy for all miners of pools (for Bitcoins) to follow up "LCR behaviors" respect to either noncooperative or cooperative behaviors (see also the discussion given in Sect. 4.3), which is exactly the notion for the concept of "hybrid solution" for games given by Zhao [57]), we thus come to have the following definition for a Consensus Game (in short, "CG"):

Given a consensus $\mathbf{G}$ (by consisting of a number of rules), let $N = \{1, 2, \cdots, n_0\}$ be the set of agents and $p = \{N_1, \cdots, N_{k_0}\}$ be a partition of N (as defined above). For each $i \in N$, the mapping $u_i : X \longrightarrow R$ is the payoff function of player i determined by the rules of the consensus $\mathbf{G}$, we say that a normal form of consensus game (CG) is just the following form:

$$CG := (\mathbf{G}, N, p, (X_i, u_i)_{i \in N})$$

We say the consensus game CG has a consensus equilibrium if the corresponding formal form of the game $(N, p, (X_i, u_i)_{i \in N})$ has a bybrid solution.

We note that by using the quorum function, Zappala et al. [56] used the term (that is, consensus game) to measure agents' degree of supporting for the

formulation of that coalition to study decision problem, which is different from our motivation above.

Throughout the rest part of this paper, when mentioning the consensus game (CG), we always assume it associated with the consensus **G** and omit it if no confusion. We now have the defining consensus equilibria for the consensus games with nonordered preferences.

A consensus game can be defined by

$$CG = (N, p, (X(t))_{t\in N}, P),$$

where $p = \{N_r | r \in R\}$ is a partition of N, $X(t)$ is the strategy space of player t, and $X = \prod_{t\in N} X(t), X(S) = \prod_{t\in S} X(t), X(-S) = \prod_{t\notin S} X(t), \forall S \in \mathcal{N}$, $P(t,\cdot) : X \rightrightarrows X$ is the preference mapping of player t. A point $x^* \in X$ is a consensus equilibrium of CG if for any $N_r \in p$ and any $S \in \mathcal{N}_r$, there exists no $y(S) \in X(S)$ such that

$$\{y(S)\} \times X(N_r - S) \times \{x^*(-N_r)\} \subset P(t, x^*),\ \forall t \in S.$$

We now recall results from Yang and Yuan [54]. The following result is the consensus game's version due to Theorem 3.1 of Yang and Yuan [54].

Theorem 3.1 (Yang and Yuan [54]). *Suppose that a consensus game*

$$CG = (N, p, (X(t))_{t\in N}, P)$$

satisfies the following conditions:

(i) N is a finite set;
(ii) for each $t \in N$, $X(t)$ is a nonempty convex compact subset of R^{m_t};
(iii) for each $t \in N$, $P(t,\cdot)$ is convex-valued with open graph in $X \times X$, and $x \notin P(t,x)$ for any $x \in X$.

Then there exists at least a consensus equilibrium of CG.

Yang and Yuan [54] next gave an infinite dimensional version of Theorem 3.1, see Theorem 3.2 of [54]. Here we state it by using concept of consensus games.

Theorem 3.2 (Yang and Yuan [54]). *Suppose that a consensus game*

$$CG = (N, p, (X(t))_{t\in N}, P)$$

satisfies the following conditions:

(i) N is a finite set;
(ii) for each $t \in N$, $X(t)$ is a nonempty convex compact subset of a Hausdorff topological vector space $E(t)$;
(iii) for each $t \in N$, $P(t,\cdot)$ is convex-valued with open graph in $X \times X$ and $x \notin P(t,x)$ for any $x \in X$.

Then there exists at least a consensus equilibrium of CG.

As an application of Theorem 3.2, we have the following corollary which is indeed an extension of Theorem 2.1 into topological vector spaces.

Corollary 3.1 *Suppose that a normal-form game with a partition*

$$G = (N, p, (X_i, u_i)_{i \in N})$$

satisfies the following conditions:

(i) for each $i \in N$, X_i is a nonempty convex compact subset of a Hausdorff topological vector space E_i;
(ii) for each $i \in N$, u_i is continuous and quasiconcave on X.

Then there exists at least a hybrid solution of G (thus the consensus equilibrium of consensus game G).

We next recall the result with infinitely many players from Yang and Yuan [54]. Let N be a topological space. We define the set Ω by

$$\Omega = \{(N_r, S) | S \subseteq N_r, N_r \in p\},$$

for a consensus game $CG = (N, p, (X(t))_{t \in N}, P)$.

A member (N_r, S) of Ω consensus-blocks a strategy $x \in X$ if there exists $y(S) \in X(S)$ such that

$$\{y(S)\} \times X(N_r - S) \times \{x(-N_r)\} \subset P(t, x), \ \forall t \in S.$$

A member (N_r, S) of Ω strongly consensus-blocks a strategy $x \in X$ if there exist $y(S) \in X(S)$ and an open set V in $N \times X \times X$ such that

$$S \times \{x\} \times \{y(S)\} \times X(N_r - S) \times \{x(-N_r)\} \subset V \subset clV \subset Graph(P).$$

A strategy $x^* \in X$ is a (weak) consensus equilibrium of CG if every member of Ω cannot (strongly) consensus-block x^*.

The proofs of the following result can be found in Lemmas 3.1–3.3 and Theorem 3.4 of Yang and Yuan [54], and we state it as an existence result for weak consensus equilibria of consensus games in a general form.

Theorem 3.3 (Yang and Yuan [54]). *Suppose that a consensus game $G = (N, p, (X(t))_{t \in N}, P)$ satisfies:*

(1) N is a nonempty compact Hausdorff topological space.
(2) For each $t \in N$, $X(t)$ is a nonempty convex compact subset of a Hausdorff topological vector space $E(t)$.
(3) The correspondence P is convex-valued with open graph in $N \times X \times X$ and $x \notin P(t, x)$ for all $(t, x) \in N \times X$.

Then there exists at least a weak consensus equilibrium.

In this section, the consensus games' results are mainly based on the existence results of theoretical models in game theory first established by Yang and Yuan [54], we omit their proof in details by saving spaces here (for proof details, we refer to Yang and Yuan [54]).

Next as applications, we will discuss the general stability problems of mining pool-games for miners under the framework of Blockchain consensus for Bitcoin economics through the illustration of the general mining pool games related miners for Bitcoins as examples to show that the concept of consensus equilibria could be used as a fundamental tool for the study of consensus economics in Fintech.

4 The Consensus Games for Bitcoin Ecosystems

In this section, we first discuss the general stability problems related study from a number of literatures for mining pool-games of miners for Bitcoins consensus principle (due to Nakamoto introduced in year 2008) under the framework of Blockchain consensus for Bitcoin economics. Then as applications of the existence of consensus equilibria (mainly Corollary 3.1) as an example, we will see how general mining pool games related miners for Bitcoins can be easily illustrated by the concept of consensus equilibria, which could be used as a fundamental tool for the study of consensus economics in Fintech.

Bitcoin is by far the most successful decentralized digital currency after the presentation of white paper by Nakamoto [36]. Its backbone is the blockchain protocol which attempts to keep a consisted list of transactions in a peer-to-peer network. The goal of blockchain protocol is to solve the real distributed problem of agreement, and has the potential to support innovation and applications which require distributed computing across a network, and proving new forms of assets such as "Digital Assets" and others associated business activities with the "Blockchain" (a kind of new data structure) which can also be interpreted acting as a "platform" in supporting digital assets' trading, financing, and many other kinds of business activities. All of these new forms of digital business, digital services with the complex relationship that exists between them under the environment of Bitcoin and blockchain are called "Bitcoin Ecosystems" in general.

Bitcoin implements its incentive systems with a data structure called the *Blockchain* as mentioned above by following "*Blockchain Protocol.*" The key idea of Blockchain Protocol is a serialization of all Bitcoin transactions. It is a single global ledger maintained by an open distributed system. Since anyone can join the open system and participate in maintaining the blockchain, Bitcoin uses a *proof of work* mechanism to deter attacks: participation requires exerting significant compute resources. A participant that proves she or he has exerted enough resources with a proof of work is allowed to take a step in the protocol by generating a block. Participants are compensated for their efforts with newly minted Bitcoins. The process of creating a block is called mining, and the participants, *miners*.

In order to win the reward, many miners try to generate blocks. The system automatically adjusts the *difficulty* of block generation, such that one block is added every 10 min to the blockchain. This means that each miner seldom generates a block. Although its revenue may be positive in expectation, a miner may have to wait for an extended period to create a block and earn the actual Bitcoins. Therefore, miners form *mining pools*, where all members mine concurrently and they share their revenue whenever one of them creates a block.

Pools are typically implemented as a *pool manager* and a cohort of miners. The pool manager joins the Bitcoin system as a single miner. Instead of generating proof of work, it outsources the work to the miners. In order to evaluate the miners efforts, the pool manager accepts partial proof of work and estimates each miner's *power* according to the rate with which it submits such partial proof of work. When a miner generates a full proof of work, it is sent to the pool manager which publishes this proof of work to the Bitcoin system. The pool manager thus receives the full revenue of the block and distributes it fairly according to its members' power. Many of the pools are open by allowing any miner to join them using a public Internet interface.

In fact Bitcoin's blockchain protocol provides two incentives for miners: "*Block rewards*" and "*ransaction fees*," which are key drivers for Bitcoin ecosystems. The former accounts for the vast majority of miner revenues at the beginning of the system, but it is expected to transition to the latter as the block rewards dwindle. There has been an implicit belief that whether miners are paid by block rewards or transaction fees does not affect the security of the block chain. But Carlsten et al. [12] (see also Kroll et al. [31], Eyal and Sirer [19], Eyal [18], Bonneau et al. [10] and a number of related references wherein) show that this is not the case, their key insight is that with only transaction fees, the variance of the block reward is very high due to the exponentially distributed block arrival time, and it becomes attractive to fork a "*wealthy*" block to "*steal*" the rewards therein. They show that this results in an equilibrium with undesirable properties for Bitcoin's security and performance, and even non-equilibria in some circumstances. Moreover, They also study selfish mining and show that it can be profitable for a miner with an arbitrarily low hash power share, who is arbitrarily poorly connected within the network, or working by themselves (i.e., miners' behavior in noncooperation game's way, or saying "noncooperative mining behavior"). Thus we need to consider the stability of Bitcoin ecosystems, in particular, for the miners' working behavior and strategy (also called "*mining for Bitcoin*") in different pools for the implementation of the most important parts due to Nakamoto's consensus being so-called the "*proof of work*" mechanism in Bitcoin economics.

4.1 The Stability of Bitcoin Ecosystems

We know that Bitcoin is the first widely popular cryptocurrency with a broad user base and a rich ecosystem, all hinging on the incentives in place to maintain the critical Bitcoin blockchain. For blockchain which acts as a platform (or saying, a new kind of data structures, or a tool) in supporting businesses under the

Bitcoin ecosystem, a natural process leads participants of such systems to form pools where members aggregate their power and share the rewards. Experience with Bitcoin shows that the largest pools are often open, allowing anyone to join. On the other hand, it has long been known that a member can sabotage an open pool by joining but never sharing proofs of work. The pool shares its revenue with the attacker, and each of its participants earns less.

Thus open pools are susceptible to the classical block withholding attack (e.g., see Rosenfeld [42]), where a miner sends only partial proof of work to the pool manager and discards full proof of work. Due to the partial proof of work sent to the pool by the miner, the miner is considered a regular pool member and the pool can estimate its power. Therefore, the attacker shares the revenue obtained by the other pool members, but does not contribute. It reduces the revenue of the other members, but also its own.

By thinking of another case is that a game where pools use some of their participants to infiltrate other pools and perform such an attack, one of the special cases is where either two pools or any number of identical pools play the game and the rest of the participants are uninvolved. In both of these cases, one natural question to ask is: does there exist an situation (equilibrium) that constitutes a tragedy of the commons where the participating pools attack one another and earn less than they would have if none had attacked?

Moreover, by following Bonneau et al. [10], we face two opposing viewpoints on Bitcoin in strawman form. The first is that "*Bitcoin works in practice, but not in theory.*" A second viewpoint is that "*Bitcoin's stability relies on an unknown combination of socioeconomic factors which is hopelessly intractable to model with sufficient precision, failing to yield a convincing argument for the system's soundness.*"

By putting above two opposing viewpoints on Bitcoin together, and incorporating Bitcoin's three main (technical) components: "*Transactions (including scripts),*" "*Consensus protocol,*" and "*Communication network*" as a whole, we do think it is critical to study the **Stability** (with more details below) for Bitcoin respect to its three main components in terms of complex ecosystem.

As shown from the comprehensive study on the stability discussed by Bonneau et al. [10], the *"stability of the consensus protocol"* should be one of the most important concepts respect to following five issues (see also Garay et al. [24], Kroll et al. [31], Miller and LaViola [35] and references wherein):

1 Eventual consensus: At any time, all compliant nodes will agree upon a prefix of what will become the eventual valid blockchain. We cannot require that the longest chain at any moment is entirely a prefix of the eventual blockchain, as blocks may be discarded (become stale) due to temporary forks.

2 Exponential convergence: The probability of a fork of depth n is $O(2^{-n})$. This gives users high confidence that a simple "k confirmations" rule will ensure their transactions are permanently included with high confidence.

3 Liveness: New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time.

4 Correctness: All blocks in the longest chain will only include valid transactions.

5 Fairness: On expectation, a miner with a proportion α (the computing power) of the total computational power will mine a proportion $\propto \alpha$ of blocks (assuming they choose valid blocks).

If all of these properties hold we can say that the system is "**stable**," but it isn't clear that all are necessarily required as asked by Bonneau et al. [10]. However, Nakamoto [36] originally argued that Bitcoin will remain stable as long as all miners follow their own economic incentives (see also Nakamoto [36] again), a property called "*Incentive Compatibility*." But the concept "*Incentive Compatibility*" has never been formally defined in the context of Bitcoin or cryptocurrencies; its prevalence as a term likely stems from its intuitive appeal and marketing value. We consider "*Compliant Miners*" whose strategies are the so-called "*default mining longest chain rules*" (LCR) (see also discussion by Biais et al. [9] and related references wherein). In game-theoretic terms, if universal compliance were shown to be a Nash equilibrium, this would imply incentive compatibility for Bitcoin as no miner would have any incentive to unilaterally change strategy. This would imply a notion of (weak) stability if other equilibria exist and strong stability if universal compliance were the sole equilibrium.

On the other hand non-compliant strategies dominate compliance, we must ask whether the resulting strategy equilibrium leads to stability for the consensus protocol, thus there are many issues and problems for which we are facing as recalled below in three categories based on the existing literatures (e.g., see mainly from Bonneau et al. [10]):

(1) Stability with bitcoin-denominated utility: We need to ask *if simple majority compliance may not ensure fairness?* by an interesting non-compliant mining strategy which is temporary block withholding as discussed by Bahackm [8], Eyal and Sirer [19], Garay et al. [24]; *if majority compliance is an equilibrium with perfect information* as shown by Kroll et al. [31]; *if majority compliance may imply convergence and consensus* as discussed by Miller and LaViola [35] and Garay et al. [24].

Secondly, one of the most important situations is that *with a majority miner, if stability is not guaranteed*: indeed, it is well known that a single non-compliant miner who controls a majority of computational power could undermine fairness by collecting all of the mining rewards simply by ignoring blocks found by others and building their own chain which by assumption would grow to become the longest chain. The majority miner could separately choose to undermine liveness by arbitrarily censoring transactions by refusing to include them and forking if they appear in any other block. Finally, the majority miner could undermine both convergence and eventual consensus by introducing arbitrarily long forks in the block chain, potentially to reverse and double-spend transactions for profit. All of these strategies would result in nominal profits, but since these behaviors are detectable, they may not be in a rational miner's long-term interest.

We like to mention that for the stability in terms of issue "*if mining longest chain rules*" (LCR) was also discussed by Biais et al. [9] through the Markov

chain method under the situation with, or without mining a fork at the same time (i.e., the weak stability). Thus it is very important to discuss if it is possible among miners (in terms of either coordination (cooperation) or noncooperation behavior) for Bitcoin blockchain on mining LCR (while, with, or without occurring forking) as indeed a fork can also occur even when some miners adopt a new version of the mining software that is incompatible with the current version (if miners fail to coordinate on the same software, this triggers a fork).

Furthermore, in line with Nakamoto [36], it is said that the Bitcoin blockchain protocols are prone to multiple equilibria with forks due to the strategic complementarities of miner's actions, is it true? We would ask, *is the stability there if miners collude?*, and the question, *is stability there if mining rewards decline?*

(2) Stability with externally-denominated utility: Results in the bitcoin-denominated utility model do not provide convincing justification of Bitcoin's observed stability in practice as we may face the issues such as (a) **Liquidity limits**: Currently, exchanges which trade Bitcoin for external currencies typically have low liquidity. Thus, an attacker may obtain a large number of bitcoins but be unable to convert them all into external value, or can only do so at a greatly reduced exchange rate; (b) **Exchange rates in the face of attack**: Some non-compliant strategies, particularly those that would affect stability in a visible way, might undermine public confidence and hence weaken demand for bitcoins in the short run; (c) **Long-term stake in bitcoin-denominated mining rewards**: Most large miners have an additional interest in maintaining Bitcoin's exchange rate over time because they have significant capital tied up in non-liquid mining hard ware which will lose value if the exchange rate declines. If miners expect they will maintain their share of mining power far into the future with low marginal costs, then they may avoid strategies which earn them more bitcoins but decrease the expected value of their future mining rewards.

(3) Stability with incentives other than mining income: At least two strategies have been analyzed which may be advantageous for a miner whose utility is not purely derived from mining rewards, they are *Goldfinger attacks* (see also Kroll et al. [31]); *Feather-forking* proposed by Miller [34].

One of the key issues for the miners in the ming pool needs to consider is *what could go wrong* for the situation called "*Mining Gap*" which means if without a block reward immediately after a block is found if there is zero expected reward for mining but nonzero electricity cost, then it would be unprofitable for any miner to mine?

Indeed as discussed by Carlsteb et al. [12], we know that effects of a mining gap lead to miners mining for a smaller and smaller fraction of the time between the arrival of blocks (with the difficulty dropping to compensate). Clearly, this would have a negative impact for Bitcoin security, as the effective hash power in the network would drop, and it would become easier for a malicious miner to fork. Of course, turning a rig on and off every ten minutes may be practically infeasible. Nevertheless, this analysis illustrates that strategic miners might look for ways to deviate when the default protocol would have them wasting electricity to mine a near-valueless block.

The goal of this part is to establish an outline of the question on the stability of Bitcoin system on Blockchain can be formulated as the existence problem of consensus equilibria under the framework of consensus games with focus on the consensus associated with Bitcoin ecosystem, we give a brief recalling for the description of basic mining economics by following "**three types of consensuses**" below.

4.2 The Basic Mining Economics

Success of the Bitcoin economy requires that Bitcoin's distributed protocols operate and remain stable. In this section we consider the stability of these protocols, under the assumption that players behave according to their incentives. The success of Bitcoin relies on "**three types of consensuses**":

1 Consensus about Rules: Players must agree on criteria to determine which transactions are valid. Only valid transactions will be memorialized in the Bitcoin log, but this requires agreement on how to determine validity.

2 Consensus about State: Players must agree on which transactions have actually occurred, that is, they must agree on the history of the Bitcoin economy, so that there is a common understanding of who owns which coin at any given time.

3 Consensus that Bitcoins are Valuable: Players must agree that Bitcoins have value so that players will be willing to accept Bitcoins in payment.

Each of these forms of consensus depends mutually on the other two. For example, it is hard to agree on the history without agreeing on the rules, and it is hard to believe in the value of a Bitcoin if participants cannot even agree on who owns which Bitcoin.

Consensus about the rules is a social process. Participants must come to a common understanding of what is allowed, so that the rules can be encoded into the software that each participant uses. In Bitcoin, small groups and individuals can exert outsized power.

Consensus about state is a technological problem in distributed systems design. Each player can see part of the state and the players need to cooperate, in large numbers and across a potentially unreliable network, to achieve a consistent understanding of the global state. Technological consensus must be achieved despite the possibility that some players will deviate from the published rules. In the distributed systems literature, devious behavior ("**Byzantine failures**") can often be tolerated if a sufficient majority of players are honest and cooperate. However, in Bitcoin, we explicitly assume that players will behave according to their incentives (assuming cooperation despite incentives to the contrary would make the design much simpler, though unrealistic.)

Game-theoretic issues are very important for the correct execution of the blockchain protocol. This was realized at its inception when its creator, Nakamoto [36] analyzed incentives in a simple, albeit insufficient, model. Understanding these issues is essential for the survival of bitcoin and the development of the blockchain protocol. In practice it can help understand their strengths

and vulnerabilities and, in economic and algorithmic theory, it can provide an excellent example for studying how rational ("*selfish miners*") players can play games in a distributed way and map out their possibilities and difficulties.

Distilling the essential game-theoretic properties of blockchain maintenance is far from trivial; some "*attacks*" and vulnerabilities have been proposed but there seems to exist no systematic way to discover them. In this work, we will study two models' stutaions of mining pool-games as applications of our consensus games below in which the miners (the nodes of the distributed network that run the protocol and are paid for it) play a complete-information (may or may not be "*stochastic*") games. Although the miners in the actual blockchain game do not have complete information, our games aim to capture two important questions that selfish miners ask (see also Kiayias et al. [30], Carlsten et al. [12], Badertscher etal. [7] and related references wherein):

(a) What to compute next (more precisely, which block to mine);
(b) When to release the results of computation (more precisely, when to release a mined block).

Ideally, the blockchain would be a simple chain of blocks implying precedence between the corresponding transactions, i.e., a serialization of valid transactions between the clients of the Bitcoin protocol. This would be the case if miners always started mining at the last announced block and propagated each block creation immediately to the network of the remaining miners. However, the selfish nature of the miners who try to receive the rewards of as many blocks as possible (or even the inherent delay of block propagation in the distributed network) can result in temporary forks in the blockchain. The protocol suggests to the miners to always start mining at the end of the branch which needed the largest amount of computational effort so far, i.e., the end of the longest fork. This strategy is called "*frontier*" and we will call the miners that follow it "*honest miners.*"

The reward structure of the protocol guarantees that the honest miners revenue is proportional to their computational power. However, understanding when it is profitable for the miners to deviate from the honest strategy is a central question and has attracted a lot of attention. The original assumption was that no miner has an incentive to deviate from the honest strategy if the majority of the miners are honest. However, this is not true as shown by Eyal and Sirer [19]. They gave a specific strategy which, when followed by a miner with computational power at least 33% of the total power, provides rewards strictly better than the honest strategy (assuming that every other miner is honest). This was extended computationally by Sapirstein et al. [43].

Bitcoin is the first widely popular cryptocurrency with a broad user base and a rich ecosystem, all hinging on the incentives in place to maintain the critical Bitcoin blockchain. But Eyal and Sirer [19] show that Bitcoin's mining protocol is not "*incentive-compatible*": which means there exist a "*selfish-miner*", a mining strategy that enables pools of colluding miners that adopt it to earn revenues in excess of their mining power. As a result, higher revenues can lead new miners to join a selfish miner pool, a dangerous dynamic that enables the

selfish mining pool to grow towards a majority. The Bitcoin system would be much more robust if it were to adopt an automated mechanism that can thwart selfish miners. Eyal and Sirer [19] suggest a backwards-compatible modification to Bitcoin that ensures that pools smaller than $\frac{1}{4}$ of the total mining power cannot profitably engage selfish mining, and they also show that at least $\frac{2}{3}$ of the network needs to be honest to thwart selfish mining, which concludes that "*a simple majority is not enough*", thus we need to study in which way the existence of equilibria for mining economics in "Mining LCR", while, with or without occurring "*mining fork*" from miners of the mining-pools.

4.3 The Stability of Mining Pool Games Under the Framework by Concepts of Consensus Games

Recently, there are a number of informal and/or ad hoc attempts to address the security of Bitcoin, an exciting recent line of work has focused on devising a rigorous cryptographic analysis of the system [e.g., see Garay et al. [23], Garay et al. [26], Pass et al. [41], Badertscher et al. [6]). At a high level, these works start by describing an appropriate model of execution, and, within it, an abstraction of the original Bitcoin protocol of Nakamoto (2008) along with a specification of its security goals in terms of a set of intuitive desirable properties (see Garay [25], Garay [26], Pass [41]), or in terms of a functionality in a simulation-based composable framework (see Badertscher [6]). They then prove that the Bitcoin protocol meets the proposed specification under the assumption that the majority of the computing power invested in mining bitcoins is by devices which mine according to the Bitcoin protocol, i.e., honestly. This assumption of honest majority of computing power which had been a folklore within the Bitcoin community for years underlying the system's security is captured by considering the parties who are not mining honestly as controlled by a central adversary who coordinates them trying to disrupt the protocol's outcome.

Meanwhile, a number of works have focused on a rational analysis of the system (see Rosenfeld [42], Carlsten [12], Eyal and Sirer [19] and references wherein). In a nutshell, these works treat Bitcoin as a game between the (competing) rational miners, trying to maximize a set of utilities that are postulated as a natural incentive structure for the system. The goal of such an analysis is to investigate whether or not, or under which assumptions on the incentives and/or the level of collaboration of the parties, Bitcoin achieves a stable state, i.e., a game-theoretic equilibrium. However, despite several enlightening conclusions, more often than not the prediction of such analyses is rather pessimistic. Indeed, these results typically conclude that, unless assumptions on the amount of honest computing powersometimes even stronger than just majority-are made, the induced incentives result in plausibility of an attack to the Bitcoin mining protocol, which yields undesired outcomes such as forks on the blockchain, or a considerable slowdown.

To our knowledge, no fork or substantial slowdown that is attributed to rational attacks has been observed to date, and the Bitcoin network keeps performing according to its specification, even though mining pools would, in principle, be

able to launch collaborative attacks given the power they control. In the game-theoretic setting, this mismatch between the predicted and observed behavior would be typically interpreted as an indication that the underlying assumptions about the utility of miners in existing analysis do not accurately capture the miners rationale. With motivation of Badertscher et al. [7], we concern the following two situations with focus on the so-called "*Consensus Economics*" (which means the ecosystems based on the framework of Bitcoin consensuses in general):

Q1 Is Bitcoin possibly broken under different kinds of attacks (or, saying differently, why does Bitcoin ecosystem work and why do majorities not collude to break it)?
Q2 Why do honest miners keep mining given the plausibility of such attacks?

Indeed we may interpret the "attackers" as miners playing noncooperative games by taking different kinds of attack strategies, and "honest miners" playing cooperative games by following the "default compliant mining rule" of Bitcoin consensus. By putting Q1 and Q2 together, the existence of the Bitcoin ecosystem is equivalent to the existence of (hybrid) equilibrium which is the so-called "consensus equilibrium" of the "consensus game" defined above in this paper.

Therefore the existence of consensus equilibrium for consensus games under the general framework of Bitcoin consensus means there always exists a group of people working on the "Longest Chain Rule" (LCR) which assures the Blockchain under the Bitcoin consensus is properly maintained (though some miners working on forks, other miners do not, e.g., see also Biais et al. [9] from a different way to address the issue in terms of Markov perfect equilibrium). Thus the study for the existence of consensus equilibrium for consensus games provide the fundamental base for consensus economics in general. In this way, we can study the stability of mining games for Bitcoin as applications of the general existence results established for consensus games above in this paper as shown below.

4.4 The Miner's Dilemma and General Pool Game

By using the concept of consensus games established in this paper, we will discuss Miner's Dilemma for Two Pools Game and the general existence of stability for Multi-Pools Games which was first discussed by Eyal [18] in a different way. As applications of our new concept called "*Consensus Games*", we wish our discussion for the illustration of "Miner's Dilemma and General Pool Game" on the stability of mining pool-games for miners by applying consensus games provide an example that the concept of consensus equilibria could be used as a fundamental tool for the study of consensus economics under the framework of Blockchain economy in Fintech, e.g., see Yuan et al. [50] for the work on the existence of conesnsus equilibria for data trading under the framework of Internet of Things (IoT) with Blockchain Ecosystems as applications of our new notion of Consensus Games.

An open distributed system can be secured by requiring participants to present proof of work and rewarding them for participation. The Bitcoin digital currency introduced this mechanism, which has been adopted by almost all contemporary digital currencies and related services. A natural process leads participants of such systems to form pools, where members aggregate their power and share the rewards. Experience with Bitcoin shows that the largest pools are often open, allowing anyone to join. It has long been known that a member can sabotage an open pool by seemingly joining it but never sharing proofs of work. The pool shares its revenue with the attacker, and so each of its participants earns less.

As discussed by Eyal [18], we define and analyze a game where pools use some of their participants to infiltrate other pools and perform such an attack. With any number of pools, no-pool-attacks is not a Nash equilibrium. We study the special cases where either two pools or any number of identical pools play the game and the rest of the participants are uninvolved. In both of 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 had attacked.

For a two-pools game, the decision whether or not to attack is called the "*Miner's Dilemma*", an instance of the iterative prisoner's dilemma. The game is played daily by the active Bitcoin pools, which apparently choose not to attack. If this balance breaks, the revenue of open pools might diminish, making them unattractive to participants.

The General Model

By following Eyal [18], we assume the Bitcoin system is comprised of the Bitcoin network and nodes with unique IDs, and progresses in steps. A node i generates tasks which are associated with its ID i. Denote the number of pools with p, the total number of mining power in the system with m and the miners participating in pool i, where $1 \leq i, j \leq p$ with m_i, and $m = \cup_{i=1}^{p} m_i$, and $m_i \cap m_j = \emptyset$ for each $i \neq j$.

A node can work on a task for the duration of a step. The result of this work is a set of partial proofs of work and a set of full proofs of work. The number of proofs in each set has a Poisson distribution, partial proofs with a large mean and full proofs with a small mean. Nodes that work on tasks are called a miners, miners have identical power, and hence identical probabilities to generate proofs of work.

The Bitcoin network pays for full proofs of work. To acquire this payoff an entity publishes a task and its corresponding proof of work to the network. The payoff goes to the ID associated with task. The Bitcoin protocol normalizes revenue such that the average total revenue distributed in each step is a constant throughout the execution of the system. Any node can transact Bitcoins to another node by issuing a Bitcoin transaction. Nodes that generate tasks but outsource the work are called pools. Pools send tasks to miners over the network, the miners receive the tasks, perform the work, and send the partial and full proofs of work to the pool.

We follow the same assumption used by Eyal [18], apart from working on tasks, we assume that all local operations, payments, message sending, propagation, and receipt are instantaneous, and we also assume that the number of miners is large enough such that mining power can be split arbitrarily without resolution constraints. We now recall two definitions as follows.

Definition 1 (A solo miner). A solo miner is a node that generates its own tasks. In every step it generates a task, works on it for the duration of the step and if it finds a full proof of work, it publishes this proof of work to earn the payoff.

Definition 2 (Revenue density). The revenue density of a pool is the ratio between the average revenue a pool member earns and the average revenue it would have earned as a solo miner.

We note that for a solo miner, its revenue density, and that of a miner working with an unattacked pool are one. If a pool is attacked with block withholding, its revenue density decreases.

The Pool Block Withholding Attack

Just as a miner can perform block withholding on a pool j, a pool i can use some of its mining power to infiltrate a pool j and perform a block withholding attack on j. Denote the amount of such infiltrating mining power at step t by $x_{i,j}(t)$. Miners working for pool i, either mining honestly or used for infiltrating pool j, are loyal to pool i. At the end of a round, pool i aggregates its revenue from mining in the current round and from its infiltration in the previous round. It distributes the revenue evenly among all its loyal miners according to their partial proofs of work. The pool's miners are oblivious to their role and they operate as regular honest miners, working on tasks.

The Pool Game

In the pool game, pools try to optimize their infiltration rates of other pools to maximize their revenue. The overall number of miners and the number of miners loyal to each pool remain constant throughout the game.

The Revenue Density Analysis of the Pool Game

Recall that m_i is the number of miners loyal to pool i. and $\mathrm{x}_{i,j}(t)$ is the number of miners used by pool i to infiltrate pool j at step t. The mining rate of pool i is therefore the number of its loyal miners minus the miners it uses for infiltration. This effective mining rate is divided by the total mining rate in the system, namely the number of all miners that do not engage in block withholding. Denote the direct mining rate R_i of pool i at step t by

$$R_i = \frac{m_i - \Sigma_{j=1}^{p} x_{i,j}}{m - \Sigma_{j=1}^{p} \Sigma_{k=1}^{p} x_{j,k}}.$$

The revenue density $r_i(t)$ of pool i at the end of step t is its revenue from direct mining together with its revenue from infiltrated pools, divided by the

number of its loyal miners together with block-withholding infiltrators that attack it:

$$r_i(t) = \frac{R_i(t) + \Sigma_{j=1}^{p} x_{i,j}(t) r_j(t)}{m_i + \Sigma_{j=1}^{p} x_{j,i}(t)}.$$

Hereinafter we move to a static state analysis and omit the t argument in the expressions.

It is clear that if no pool engages in block withholding, for any $i \in m_i$ and $j \in m_j$, we have

$$x_{i,j} = 0 \text{ and we also have that } r_i = \frac{1}{m}$$

that is, each miner's revenue is proportional to its power, be it in a pool or working solo.

The Case for One Attacker

Now by considering a simplified game of two pools, 1 and 2, where pool 1 can infiltrate pool 2, but pool 2 cannot infiltrates pool 1. The $m - m_1 = m_2$ miners outside both pools mine solo (or with closed pools that do not attack and cannot be attacked). The dashed red arrow indicates that $x_{1,2}$ of pool 1s mining power infiltrates pool 2 with a block withholding attack.

Since Pool 2 does not engage in block withholding, all of its m_2 loyal miners work on its behalf. Pool 1, on the other hand does not employ $x_{1,2}$ of its loyal miners, and its direct mining power is only $m_1 - x_{1,2}$ The Bitcoin system normalizes these rates by the total number of miners that publish full proofs, namely all miners but $x_{1,2}$. The pools direct revenues are therefore

$$R_1 = \frac{m_1 - x_{1,2}}{m - x_{1,2}}$$

$$R_2 = \frac{m_2}{m - x_{1,2}}.$$

The revenue density r_2 of pool 2 is

$$r_2 = \frac{R_2}{m_2 + x_{1,2}}$$

and the revenue r_1 of loyal Pool 1 miner is

$$r_1 = \frac{R_1 + x_{1,2} r_2}{m_1}$$

thus we have that

$$r_1 = \frac{m_1(m_2 + x_{1,2}) - x_{1,2}^2}{m_1(m - x_{1,2})(m_2 + x_{1,2})}.$$

The Case for Two Pools Game

We proceed to analyze the case where two pools may attack each other and the other miners mine solo. Again we have pool 1 of size m_1 and pool 2 of

size m_2; pool 1 controls its infiltration rate $x_{1,2}$ of pool 2, but now pool 2 also controls its infiltration rate $x_{2,1}$ of pool 1. Thus total mining power in the system is $m - x_{1,2} - x_{2,1}$. The direct revenues R_1 and R_2 of the pools from mining are their effective mining rates, without infiltrating mining power, divided by the total mining rate:

$$R_1 = \frac{m_1 - x_{1,2}}{m - x_{1,2} - x_{2,1}}$$

$$R_2 = \frac{m_1 - x_{2,1}}{m - x_{1,2} - x_{2,1}}.$$

Then we have the revenues r_1 and r_2 in terms of $x_{1,2}$ and $x_{2,1}$ by the following formula:

$$r_1(x_{1,2}, x_{2,1}) = \frac{m_2 R_1 + x_{1,2}(R_1 + R_2)}{m_1 m_2 + m_1 x_{1,2} + m_2 x_{2,1}}$$

$$r_2(x_{2,1}, x_{1,2}) = \frac{m_1 R_2 + x_{2,1}(R_1 + R_2)}{m_1 m_2 + m_1 x_{1,2} + m_2 x_{2,1}}.$$

Now we have the following general existence result for Two-Pools games as an application of Theorem 3.1 by applying consensus games, this result was first given by Eyal [18].

Theorem 4.1 (Eyal [18]). *For a two-pools game, an equilibrium exists where neither pool 1 nor pool 2 can improve its revenue by changing its infiltration rate.*

Proof. For $i = 1, 2$, by the definition of r_i, we can verify that it is concave respect to $x_{1,2}$ and $x_{2,1}$. Then by Corollary 3.1, it follows that there exists a consensus equilibrium point for Two Pools game. The proof is complete.

For the Two Pools game, we remak that like what said by Eyal [18], no-attack is not an equilibrium point for the Two Pools game as each pool can increase its revenue by choosing a strictly positive infiltration rate. Thus $x_{1,2} = x_{2,1} = 0$ is not a solution for a Two Pools game. Secondly, it is easy to see that a pool improves its revenue compared to the no-pool-attacks scenario only when it controls a strict majority of the total mining power. This fact is also confirmed by the numerical results given by Eyal [18], and the corresponding numerical results show that in extreme cases a pool does not attack its counterpart, which means at equilibrium a pool will refrain from attacking only if the other pool is larger than about 80% of the total mining power.

As a consequence of Theorem 4.1, we have the following result called "Miner's Dilemma of Two Pools Game" (see also discussion by Eyal [18]).

Theorem 4.2 (Miner's Dilemma of Two Pools Game). *For Two Pools game, it exists "Miner's Dilemma" which means the revenue density of each pool is determined by the decision of both pools whether to attack or not. The dominant strategy of each player is to attack, however the payoff of both would be larger if they both refrain from attacking.*

Proof. Indeed by the fact that for the Two Pools game and $i = 1, 2$, when $x_{1,2} = x_{2,1} = 0$, the revenue densities are $r_1 = r_2 = 1$, but this is not an equilibrium point as shown by Theorem 4.1 (or by a simply fact that each pool can increase its revenue r_i by choosing a strictly positive infiltration rate $x_{1,2}$ or $x_{2,1}$).

By following the same argument by Eyal [18], without loss of generality by considering pool 1, as we know that if pool 2 does not attack, pool 1 can increase its revenue above 1 (i.e., $r_1 > 1$) by attacking. If pool 2 does attack but pool 1 does not, we denote the revenue of pool 1 by $\hat{r_1}$. The exact value of $\hat{r_1}$ depends on the values of m_1 and m_2, but it is always smaller than one. As we have seen above, if pool 1 does choose to attack, its revenue increases, but does not surpass one. This completes our claim.

Miner's Dilemma for two pools tell us that the revenue density of each pool is determined by the decision of both pools whether to attack or not. The dominant strategy of each player is to attack, however the payoff of both would be larger if they both refrain from attacking. We also have that in a Two Pools (scenario) game, the revenue at the symmetric equilibrium is inferior to the no-one-attacks non-equilibrium strategy.

Next we can establish the general existence in terms of consensus games for the general case of multi-pools games (which was called "*q Indentical Pool Games*" by Eyal [18]).

The General Multi-Pools Games

Let there be q pools of (identical) size m_i (for $i.j = 1, 2, \cdots q$, $m = \cup_{i=1}^{q} m_i$) (and $m_i \cap m_j = \emptyset$ for each $i \neq j$) that engage in block withholding strategies against one another. Other miners neither attack nor are being attacked, this is the general multi-pools game.

For a general multi-pools game, we would expect that there exists a symmetric equilibrium. Now by considering without loss of generality, a step of pool 1. It controls its attack rates each of the other pools, and due to symmetry they are all the same. We denote by $x_{1,-1}$, the attack rate of pool 1 against any other pool. Each of the other pools can attack its peers as well. Due to symmetry, all attack rates by all attackers are identical. Denote by $x_{-1,*}$ the attack rate of any pool other than 1 against any other pool, including pool 1.

We denote by R_1 the direct revenue (from mining) of pool 1 and by R_{-1} the direct revenue of each of the other pools. Similarly we denote by r_1 and r_{-1} the revenue densities of pool 1 and other pools, respectively. Then by following the similar ide used abovem we have the following

$$R_1 = \frac{m_i - (q-1)x_{1,-1}}{m - (q-1)(q-1)x_{-1,*} - (q-1)x_{1,-1}}$$

$$R_{-1} = \frac{m_i - (q-1)x_{-1,*}}{m - (q-1)(q-1)x_{-1,*} - (q-1)x_{1,-1}}$$

and

$$r_1 = \frac{R_1 + (q-1)x_{1,-1}r_{-1}}{m_i + (q-1)x_{-1,1}}$$

$$r_{-1} = \frac{R_{-1} + (q-2)x_{-1,*}r_{-1} + x_{-1,*}r_1}{m_i + (q-2)x_{-1,*} + x_{1,-1}}.$$

We note that in the symmetric case for general multi-pool game, it follows that $r_1 = r_{-1}$, and indeed like the two-pool game scenario, the revenue at the symmetric equilibrium is inferior to the no-one-attacks non-equilibrium strategy.

Now we have the following general existence consensus games for multi-pools games below.

Theorem 4.3. (General Multi-Pools Games). *For a given general multi-pools game, its consensus equilibrium always exists.*

Proof. For a given multi-pools games (assuming q pools with total number (of miners) being $m = \cup_{i=1}^{q} m_i$, and $m_i \cap m_j = \emptyset$ for each $i \neq j$, while $i, j = 1, 2, \cdots, q$), then by the definition of r_i and its formula above, it follows that r_i is continuous (differentiable) and concave in $x_{1,-1}$. Thus by an application of Corollary 3.1, it follows that exists at least one consensus equilibrium for the general multi-pools games. This completes the proof.

Before we close this part, what we like to share with readers is that the concept of consensus games introduced in this paper is very useful for the study of Bitcoin ecosystem for its stability in terms of the existence for the consensus equilibria. By the fact that the success of the Bitcoin economy requires that Bitcoins distributed protocols operate and remain stable under the stability of these protocols associated with behaviors of players (miners) through pools relying on the incentives derived by the consensuses in general, thus we do think the theory of consensus games should provide the base for consensus Economics under the framework of the Blockchain ecosystems in Fintech (in particular for Bitcoin economics).

Finally, we like to mention that the stability of gap games formulated by Tsabary and Eyal [47] can also be studied under the framework of our consensus games in a natural way by using the partition of miners from different mining pools, and we plan to conduct this research in our next project soon.

5 The Concluding Remarks

Inspired by the hybrid solution concept of Zhao [57] and the mechanism design for the blockchain in financial technology, we introduce the model of the consensus game. Although Zappala et al. [56] used the term "consensus game" for the study of multiagent systems on autonomous agents, which is different from the outlined model and related concepts we introduced and discussed here in this paper. The key point of our model is to analyze the choice of strategies in which there exist cooperative and noncooperative behaviors at the same time and the preference of each agent is nonordered. Finally, we shall end this paper with the following remarks.

Our consensus game and consensus equilibrium can be regarded as an application of hybrid solutions introduced by Zhao [57]. The main model and result of

consensus games have been given by Yang and Yuan [54]. In [54], the consensus equilibrium was called by hybrid solution since the viewpoint of [54] bases the game theory and the purpose of [54] is to study the existence of hybrid solutions with nonordered preferences and infinitely many players. In this paper, our purpose is to analyze the consensus economy under the framework of blockchain in Fintech. The result of Yang and Yuan [54] becomes a good technique to model the framework of blockchain in Fintech. Thus, in Sect. 3, we recall the work of [54] and call the concepts of [54] by consensus games and consensus equilibria.

Finally, we conclude that the existence results of consensus equilibria for consensus games defined in this paper are useful and should provide the base for the study of consensus economics under the framework of Blockchain in fintech as shown by the discussion above. Furthering the study on different situations related to smart contracts for different kinds of digital business activities under the Blackchain with associated consensus' incentives (called "blackchain economy") should be one of the most important things in era of big data. We also note that recently some issue and problems related to topics in fintech have been studied by a number of scholars, for example, the dynamic equilibria under blockchain disruption was initially discussed by Cong and He [15], topics surrounding blockchain-based accounting and assurance was outlined by Dai and Varsarhelyi [17], and other related areas of interest issues were discussed by Narayanan et al. [37]. Moreover a number of issues and problems in Finteh have been recently addressed by Goldstein et al. [27], Chiu and Koeppl [14]. Foley et al. [21], Fuster et al. [22], Tang [46], Vallée and Zeng [49], D'Acunto et al. [16], Zhu [59], Chen et al. [13] and references wherein. By using the new consensus games, Yuan et al. [50] recently conducted some work on the existence of consensus equilibria for data trading under the framework of Internet of Things (IoT) with Blockchain Ecosystems.

Finally, our thinks also go to Miss Susan Bin for her editing service which led to the present version of the paper.

References

1. Askoura, Y.: The weak-core of a game in normal form with a continuum of players. J. Math. Econ. **47**(1), 43–47 (2011)
2. Askoura, Y., Sbihi, M., Tikobaini, H.: The exante $\alpha-$core for normal form games with uncertainty. J. Math. Econ. **49**(2), 157–162 (2013)
3. Askoura, Y.: An interim core for normal form games and exchange economies with incomplete information. J. Math. Econ. **58**, 38–45 (2015)
4. Askoura, Y.: On the core of normal form games with a continuum of players. Math. Soc. Sci. **89**, 32–42 (2017)
5. Aumann, R.J.: The core of a cooperative game without sidepayments. Trans. Am. Math. Soc. **98**, 539–552 (1961)
6. Badertscher, C., Maurer, U., Tschudi, D., Zikas, V.: Bitcoin as a transaction ledger: a composable treatment. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 324–356. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_11

7. Badertscher, C., Garay, J., Maurer, U., Tschudi, D., Zikas, V.: But why does it work? A rational protocol design treatment of bitcoin. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10821, pp. 34–65. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78375-8_2
8. Bahackm, L.: Theoretical Bitcoin Attacks with less than Half of the Computational Power. Technical Report abs/1312.7013, CoRR (2013)
9. Biais, B., Bisire, C., Bouvard, M., Casamatta, C.: The blockchain folk theorem. Rev. Financ. Stud. **32**(5), 1662–1715 (2019)
10. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, A., Felten, E.: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In: Proceedings of the 36th IEEE Symposium on Security and Privacy, San Jose, California, USA, May 18–20, 2015
11. Border, K.C.: A core existence theorem for games without ordered preferences. Econometrica **52**(6), 1537–1542 (1984)
12. Carlsten, M., Kalodner, H., Weinberg, S.M., Narayanan, A.: On the instability of Bitcoin without the block reward. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, pp. 154C67, Vienna, Austria, October 24–28, 2016
13. Chen, M., Wu, Q., Yang, B.: How valuable is FinTech innovation? Revi. Financ. Stud. **32**(5), 2062–2106 (2019)
14. Chiu, J., Koeppl, T.: Blockchain-based settlement for asset trading. Rev. Financ. Stud. **32**(5), 1716–1753 (2019)
15. Cong, L.W., He, Z.: Blockchain disruption and smart contracts. Rev. Financ. Stud. **32**(5), 1754–1797 (2019)
16. D'Acunto, F., Prabhala, N., Rossi, A.G.: The promises and pitfalls of Robo-Advising. Rev. Financ. Stud. **32**(5), 1983–2020 (2019)
17. Dai, J., Vasarhelyi, M.A.: Toward blockchain-based accounting and assurance. J. Inf. Syst. **31**, 5–21 (2017)
18. Eyal, I.: The miners dilemma. In: Proceedings of the 36th IEEE Symposium on Security and Privacy, San Jose, California, USA, May 18–20, 2015
19. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 436–454. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45472-5_28
20. Florenzano, M.: On the nonemptiness of the core of a coalitional production economy without ordered preferences. J. Math. Anal. Appl. **141**, 484–490 (1989)
21. Foley, S., Karlsen, J.R., Putnins, T.: Sex, Drugs, and Bitcoin: how much illegal activity is financed through Cryptocurrencies? Rev. Financ. Stud. **32**(5), 1798–1853 (2019)
22. Fuster, A., Plosser, M., Schnabl, P., Vickery, J.: The role of technology in mortgage lending. Rev. Financ. Stud. **32**(5), 1854–1899 (2019)
23. Garay, J.A., Katz, J., Tackmann, B., Zikas, V.: How fair is your protocol? A utility-based approach to protocol optimality. In: Georgiou, G., Spirakis, P.G. (eds.) The 34th ACM PODC, ACM. pp. 281–290, July 2015
24. Garay, J.A., Kiayias, A., Leonardos, N.: The Bitcoin Backbone Protocol: Analysis and Applications. Cryptology ePrint Archive, Report 2014/765 (2014)
25. Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol: analysis and applications. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 281–310. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_10

26. Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol with chains of variable difficulty. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 291–323. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_10
27. Goldstein, I., Jiang, W., Karolyi, G.: To FinTech and beyond. Rev. Financ. Stud. **32**(5), 1647–1661 (2019)
28. Ichiishi, T.: A social coalitional equilibrium existence lemma. Econometrica **49**, 369–377 (1981)
29. Kajii, A.: A generalization of Scarf's theorem: an $\alpha-$core existence theorem without transitivity or completeness. J. Econ. Theory **56**, 194–205 (1992)
30. Kiayias, A., Koutsoupias, E, Kyropoulou, M, Tselekounis, Y.: Blockchain mining games. In: 2016 ACM Conference on Economics and Computation, Maastricht, The Netherlands, 24–28 July 2016
31. Kroll, J., Davey, I., Felten, E.: The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In: Proceedings of The Twelfth Workshop on the Economics of Information Security (WEIS 2013), Georgetown University, Washington DC, USA, 11–12 June 2013
32. Lefebvre, I.: An alternative proof of the nonemptiness of the private core. Econ. Theor. **18**(2), 275–291 (2001)
33. Martins-da-Rocha, V.F., Yannelis, N.: Nonemptiness of the alpha core. Working paper. Manchester School of Social Sciences, University of Manchester (2011)
34. Miller, A.: Feather-forks: enforcing a blacklist with sub-50% hash power. bitcointalk.org, October 2013
35. Miller, A., LaViola Jr., J.J.: Anonymous byzantine consensus from moderately-hard puzzles: a model for Bitcoin (2014)
36. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). http://bitcoin.org/bitcoin.pdf
37. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction Hardcover. Princeton University Press, Princeton (2016)
38. Noguchi, M.: Cooperative equilibria of finite games with incomplete information. J. Math. Econ. **55**, 4–10 (2018)
39. Noguchi, M.: Alpha cores of games with nonatomic asymmetric information. J. Math. Econ. **75**, 1–12 (2018)
40. Nyumbayire, C.: The Nakamoto Consensus. https://www.interlogica.it/en/insight-en/nakamoto-consensus. Insight, Interlogica, February 2017
41. Pass, R., Seeman, L., Shelat, A.: Analysis of the blockchain protocol in asynchronous networks. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10211, pp. 643–673. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56614-6_22
42. Rosenfeld, M.: Analysis of Bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980 (2011)
43. Sapirshtein, A., Sompolinsky, Y., Zohar, A.: Optimal selfish mining strategies in Bitcoin. In: Grossklags, J., Preneel, B. (eds.) FC 2016. LNCS, vol. 9603, pp. 515–532. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54970-4_30
44. Scarf, H.E.: On the existence of a cooperative solution for a general class of n-person games. J. Econ. Theor. **3**, 169–181 (1971)
45. Shafer, W., Sonnenschein, H.: Equilibrium in abstract economies without ordered preferences. J. Math. Econ. **2**, 345–348 (1975)
46. Tang, H.: Peer-to-Peer lenders versus banks: substitutes or complements? Rev. Financ. Stud. **32**(5), 1900–1938 (2019)

47. Tsabary, I., Eyal, I.: The gap game. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS 18) (2018)
48. Uyanik, M.: On the nonemptiness of the $\alpha-$core of discontinuous games: transferable and nontransferable utilities. J. Econ. Theor. **158**, 213–231 (2015)
49. Vallée, B., Zeng, Y.: Marketplace lending: a new banking paradigm? Rev. Financ. Stud. **32**(5), 1939–1982 (2019)
50. Weber, S.: Some results on the weak core of a non-side-payment game with infinitely many players. J. Math. Econ. **8**, 101–111 (1981)
51. Yannelis, N.C., Prabhakar, N.D.: Existence of maximal elements and equilibria in linear topological spaces. J. Math. Econ. **12**, 233–245 (1983)
52. Yang, Z.: Some infinite-player generalizations of Scarf's theorem: finite-coalition $\alpha-$cores and weak $\alpha-$cores. J. Math. Econ. **73**, 81–85 (2017)
53. Yang, Z.: Some generalizations of Kajii's theorem to games with infinitely many players. J. Math. Econ. **76**, 131–135 (2018)
54. Yang, Z., Yuan, X.Z.: Some generalizations of Zhao's theorem: bybrid solutions and weak hybrid solutions for games with nonordered preferences. J. Math. Econ. **84**, 94–100 (2019)
55. Yuan, X.Z.: The study of equilibria for abstract economies in topological vector spaces-a unified approach. Nonlinear Anal. **37**, 409–430 (1999)
56. Zappala, J., Alechina, N., Logan, B.: Consensus games. In: Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2012), pp. 1309–1310 (2012)
57. Zhao, J.: The hybrid solutions of an N-person game. Games Econ. Behav. **4**, 145–160 (1992)
58. Yuan, X.Z, Di, L., Zeng, T.: The Existence of consensus games for data trading under the framework of Internet of Things (IoT) with blockchain ecosystems. Working Paper. School of FinTech, Shanghai Lixin University of Accounting and Finance (2019)
59. Zhu, C.: Big data as a governance mechanism. Rev. Financ. Stud. **32**(5), 2021–2061 (2019)