A General Consensus Game Framework Supporting Blockchain Ecosystems in FinTech

Authors: Yuan Xianzhi, Yuan Xianzhi

Date: 2020-03-31T00:00:00+00:00

Abstract

The purpose of this paper is to establish a general framework for consensus equilibrium in mining pool games within blockchain ecosystems, specifically to explicate the stability—in the sense of the existence of consensus equilibrium associated with behavior in Gap Games—by employing a novel concept of 'Consensus Game' , wherein the blockchain ecosystem primarily denotes economic activities that apply the key consensus mechanism of 'Proof of Work' (proposed by Nakamoto in 2008), taking into account three distinct factors: fees for blockchain operations, reward mechanisms, and mining rights. To this end, we first outline how the general existence of consensus equilibrium in mining pool games is formulated, then explain the stability of Bitcoin gap games (Gap Games) through the existence of consensus equilibrium within the blockchain consensus framework, and subsequently establish general existence results for consistent equilibrium in general mining gap games by employing miners' profit functions as payoffs in game theory. As an application, general existence results for consistent equilibrium in gap games (Gap Games) are established, which not only assists in asserting the existence of general stability for gap games (Gap Games) within the general framework of blockchain ecosystems, but also enables us to elucidate certain distinct phenomena observed in mining pool game research that may arise from miners' behavior in Gap Games and scenarios embedded within Bitcoin economics. Our interpretive study on the stability of mining gap games in blockchain ecosystems demonstrates that the concept of consensus equilibrium may play a significant role in the development of foundational theories for consensus economics.

Full Text

Preamble

The Framework of Consensus Equilibria for Blockchain Ecosystems in Fintech

George Xianzhi Yuan
Shanghai Lixin University of Accounting and Finance, Shanghai 201209 China
Business School, Chengdu University, Chengdu 610106 China
Center for Financial Engineering, Soochow University, Suzhou 215008 China, and
Business School, Sun Yat-Sen University, Guangzhou 510275 China
E-mail: george yuan99@yahoo.com

Abstract

This paper establishes a general framework of consensus equilibria for Mining-Pool Games in Blockchain Ecosystems, with particular emphasis on explaining stable mining gap game behaviors through a new concept called "consensus games (CG)" in Blockchain Ecosystems. Here, the Blockchain ecosystem primarily refers to economic activities that account for three distinct factors: expenses, reward mechanisms, and mining power for blockchain work, applying the key consensus mechanism known as "Proof of Work" introduced by Nakamoto in 2008.

We first outline how the general existence of consensus equilibria for Mining-Pool Games is formulated and then apply this framework to explain stability for Bitcoin Gap Games through the existence of consensus equilibria under Blockchain consensus. We establish a general existence result for consensus equilibria of general mining gap games by using miners' profit functions as payoffs in game theory. As applications, we derive general existence results for consensus equilibria of Gap games, which not only demonstrate the general stability of Gap games under the Blockchain ecosystem framework but also illustrate various phenomena in mining-pool games with potential impacts from miners' gap behaviors in Bitcoin economics. Our study shows that the concept of consensus equilibria may play an important role in developing fundamental theory for consensus economics.

Keywords: Consensus equilibrium, Nakamoto consensus, Proof of work, Stability, Blockchain ecosystems, Mining-pool game, Mining gap games, Longest chain rules (LCR), Incentive compatibility, Cooperative and non-cooperative games, Hybrid solution.

JEL: C73, D82, D89, G20, G28, G39, L13, L86, O31.

Introduction

In the Bitcoin world, all miners follow the so-called Nakamoto consensus protocol, introduced in 2008, and work in various groups (pools) to mine Bitcoin. The process of working on blocks, called "mining," is successfully approved when the majority of miners apply the key consensus mechanism known as "Proof of Work." Since each miner or pool may work differently, we must address the so-called "Pool-Games" of miners (also termed "Mining Pool Game") with their mining behaviors as individuals or groups following either cooperative or

non-cooperative strategies.

To this end, we introduce a new notion called "Consensus Games" to establish the general existence of consensus equilibria for describing mining behavior in Blockchain Ecosystems in Fintech. We particularly focus on the mechanism of the phenomenon called "Mining Gap Behavior" (or "Gap Games") for miners under the general incentives consensus framework, where miners avoid mining blocks when available fees are insufficient. If incentives come only from fees, mining gap behavior emerges (see Carlsten et al. (2016), Tsabary and Eyal (2018) and related references for details).

In game theory, Nash equilibrium follows non-cooperative principles, while the Core concept considers cooperative behavior. Generally speaking, Aumann (1961) first introduced a cooperative solution concept (-core). Later, Scarf (1971) proved a nonemptiness result for the -core in normal-form games with continuous quasiconcave payoff functions. Building on Scarf (1971), Kajii (1992) generalized this result to games with nonordered preferences, modifying and developing the proof technique from Border (1984).

Florenzano (1989) defined group preferences for each coalition and provided proofs using the Gale-Mas-Colell fixed point theorem. Following Florenzano' s method, Lefebvre (2001) generalized this to economies with different information. Building on Kajii (1992), Martins-da-Rocha and Yannelis (2011) extended these results to games on (Hausdorff) topological vector spaces. For additional work on the -core, see Askoura (2011), Askoura et al. (2013), Noguchi (2018), Yang and Yuan (2019) and references therein.

The idea of mixing Nash and cooperative equilibria was originally studied by Zhao (1992) under the name "Hybrid Solution." Building on Zhao (1992) and Kajii (1992), and supported by recent work from Yang and Yuan (2019), we establish a new tool through "Consensus Games" in topological vector spaces without ordered preferences from the Blockchain Fintech perspective.

Briefly, the "Consensus Game" is a new concept that allows us to examine whether an acceptable (though not necessarily "Pareto optimal") collaborative strategy exists, combining cooperative and non-cooperative behaviors under a given consensus principle such as the "Longest Chain Rules (LCR)" from Nakamoto (2008) consensus. We define a miner as acting cooperatively under the Bitcoin mining framework if the miner applies the general principle of Nakamoto' s consensus protocol, particularly applying at least the LCR; otherwise, the miner is said to play mining-pool games using non-cooperative strategies. One typical non-cooperative behavior is when a miner acts as a "selfish miner" or "mining-pool attacker" to violate the LCR for a high-reward block, acting against the general principle of a given "consensus" (see Nyumbayire (2017), Biais et al. (2019) and references therein for discussions on forks in blockchain platforms called "Blockchain Ecosystems" or "Consensus Economics").

Thus, compared to traditional cooperative and non-cooperative games, the consensus game is a natural extension for consensus economies, especially under the

Bitcoin ecosystem framework associated with Nakamoto' s consensus protocol. Mining pool games have been extensively studied by Kroll et al. (2013), Eyal et al. (2014), Eyal (2015), Bonneau et al. (2015) (see also Carlsten et al. (2016), Kiayias et al. (2016), Sapirstein et al. (2016) and references therein). Smart contracts were discussed by Cong and He (2019), and blockchain-based accounting and assurance were addressed by Dai and Vasarhelyi (2017) and others. However, one critical issue remains: "Is it possible to have a general consensus that leads the Mining-Pool Game to be stable (see detailed meaning below) in supporting the Blockchain ecosystem?"

Based on the meaning of consensus games (see also Section 2), it appears that the notion of consensus equilibria for consensus games with a partition of the player set through general profit functions as payoff functions (which are nonordered preferences mappings) in game theory would be a useful tool for studying consensus economics under the Blockchain framework. Our goal is to address one of the most fundamental questions for consensus economics in Fintech: "Is it possible to have a general consensus (for example, Nakamoto' s) that leads the Mining-Pool Game to be stable in supporting the Blockchain ecosystem (even with existing attackers) in the sense that (1) there always exist honest miners maintaining the Mining Longest Chain Rules (LCR) (given the plausibility of mining-pool attacking); and (2) the Bitcoin ecosystem always works (or majorities of miners do not collude to break it; here 'collusion' means an attempt to violate the LCR for a high-reward block, see Saleh (2020) for discussion)?"

The structure of this paper is as follows: We first discuss the new concept of "Consensus Game" (CG) motivated by blockchain mechanism design in financial technology under Nakamoto' s (2008) consensus incentives (see also Biais et al. (2019), Cong and He (2019), Narayanan et al. (2016), Nyumbayire (2017) and related references). Building on results from Zhao (1992) to Yang and Yuan (2019), where existence results have been established for general games, our paper captures the blockchain consensus idea in Fintech, with Yang and Yuan (2019) playing an important role in modeling Blockchain in Fintech. After outlining how general existence results for consensus equilibria of consensus games are formulated as the existence of general stability for Mining Pool Games, we establish general existence results for consensus equilibria of general gap games using miners' profit functions directly as payoff functions in game theory. This not only demonstrates general stability for Gap games under the Blockchain ecosystem framework but also illustrates various phenomena in mining pool-games with potential impacts from Mining Gap Games behaviors in Bitcoin economics.

We note (see also Tsabary and Eyal (2018)) that a Mining Gap Behavior Game is indeed the game of mining Bitcoin played among all miners, which is a one-shot game on finding blocks: The first to find a block receives rewards, while all suffer expenses. Thus all miners decide when to start their mining rigs, striving to optimize their average revenue by maximizing the difference between income and expense. One Gap Game situation occurs when miners under the general

incentives consensus framework "avoid mining blocks" when available fees are insufficient (this is called Gap behavior in mining-pool games). If incentives come only from fees, mining gap behavior emerges and may impact Bitcoin stability (as without block reward, see Carlsten et al. (2016) and references for detailed discussion). We show how this problem can be addressed using payoff functions under the consensus games framework in Sections 3 and 4.

We also share that the way we outline how stability (in terms of equilibrium existence) for mining pool-games can be formulated as an application of consensus games using the concept of consensus equilibria could serve as a fundamental tool for studying consensus economics under the general Blockchain economy framework in Fintech.

The rest of this paper is organized as follows. Section 1 is the introduction. Section 2 provides general existence results for consensus games used as a tool. Section 3 discusses consensus equilibria for mining-pool games and relates them to stability concerning mining Gap games behaviors in Blockchain ecosystems. Section 4 establishes general existence results for consensus equilibria of Gap games and affirmatively answers the stability problems of Blockchain Ecosystems under possible miners' Gap behaviors in Bitcoin economics.

As applications, we illustrate various phenomena in mining pool-games with potential impacts from miners' gap behaviors in Bitcoin economics. Our study shows that the concept of consensus equilibria may play an important role in developing fundamental theory for consensus economics. Section 5 concludes.

2 The Concept of Consensus Games

Based on hybrid solutions in game theory, we first introduce a new concept called "Consensus Game" (CG), which will be used in consensus economics to describe what kinds of general consensus (through mechanism design realization) will achieve incentive compatibility to combat non-cooperative behaviors (i.e., refusing to follow "Nakamoto' s consensus" but adopting strategies like "selfish mining" or "mining-pool attacking") for coalitions of participants under the Blockchain platform. We then discuss the existence of general consensus game equilibria using hybrid solutions. For references on Blockchain and Nakamoto consensus, see Nakamoto (2008), Kroll et al. (2013), Eyal and Sirer (2014), Eyal (2015), Bonneau et al. (2015) (see also Carlsten et al. (2016)), Kiayias et al. (2016), Sapirstein et al. (2016), Biais et al. (2019), Nyumbayire (2017), Narayanan et al. (2016) and references therein.

Under the Nakamoto consensus protocol introduced in 2008, one key issue is finding a set of consensus rules to encourage agents (miners from mining pools) to follow rules truthfully under the corresponding protocol, which may be formulated as preference mappings under abstract economy models (see Yannelis and Prabhakar (1983), Yuan (1999) and references therein). Thus it is crucial to study Blockchain consensus stability in terms of equilibrium existence for miners (from mining pools) following the so-called "LCR" (see Section 3 discus-

sion) with or without blockchain forks in Bitcoin ecosystems. Other issues to consider include possible collusive equilibria (see Saleh (2020) and references) and behaviors related to smart contracts, dynamic equilibria under blockchain disruption as discussed by Cong and He (2019), and emerging blockchain-based accounting and assurance outlined by Dai and Vasarhelyi (2017), discussed by Narayanan et al. (2016), and other questions (see Saleh (2020) and references).

Using the blockchain framework and associated consensus mechanism, the stability (in terms of equilibrium existence) for the mining pool game can be formulated as the problem of finding a strategy where some group of miners (called "honest miners") in mining-pools follow "LCR behaviors" with respect to either noncooperative or cooperative behaviors, though some miners may adopt "selfish mining" or "mining pool with attacking" strategies. This mixing of cooperative and non-cooperative game behaviors is exactly the notion of "hybrid solution" for games given by Zhao (1992). We thus have the following definition for a Consensus Game (CG):

Given a consensus G (consisting of rules), let N = {1, 2, $\cdots$, n0} be the set of agents and p = {N1, $\cdots$, Nk0} be a partition of N, and N is all subsets of N. For each i N, the mapping ui : X $\to$ R is the payoff function of player i determined by consensus G rules. We say a normal form consensus game (CG) is:

CG := (G, N, p, (Xi, ui)i N)

We say the consensus game CG has a consensus equilibrium if the corresponding formal game (N, p, (Xi, ui)i N) has a hybrid solution (see Zhao (1992) for definition, see also Di et al. (2019)). Basically, the hybrid solution for the finest partition (i.e., k0 = n0, and the partition P = N) is a Nash equilibrium; and in general the hybrid solution is the -core for the coarsest partition consisting of the grand coalition alone.

Hybrid solutions are more general due to the coexistence of competition and cooperation, capturing the omnipresent situation where a group (pool) of miners behaves collectively to compete with other groups (pools) of miners.

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

A consensus game can be defined by CG = (N, p, (X(t))t N, P), where p = {Nr|r R} is a partition of N (the set of all miners in mining-pools for Bitcoin), X(t) is the strategy space (sets) of miner t (i.e., the player' s all mining strategies/behaviors), and X = (cid:81) t S X(t), X(−S) = (cid:81) t S X(t), S N, P(t, $\cdot$) : X X is the preference mapping of player t under a given consensus (e.g., the Nakamoto (2008) consensus protocol). A point x$*$ X is a consensus equilibrium of CG if for any Nr p and any S Nr, there exists no y(S) X(S) such that {y(S)} $\times$ X(Nr − S) $\times$ {x$*$(−Nr)} P(t, x$*$), t S.

Briefly stated, this means there is no better Pareto optimal solution than x∗ when considering both cooperative and non-cooperative strategies together in Bitcoin mining-pool games.

We now list a result used as a tool to discuss the stability of Mining Gap Games under Blockchain Ecosystems (Corollary A.1 from Appendix A).

Theorem 2.1 Suppose a normal-form game with partition G = (N, p, (Xi, ui)i N) satisfies: (i) N is finite; (ii) for each i N, Xi is a nonempty convex compact subset of a Hausdorff topological vector space Ei; (iii) for each i N, ui is continuous and quasiconcave on X.

Then G has at least one hybrid solution (thus the consensus equilibrium of consensus game G).

The consensus game results in this section are mainly based on theoretical game theory models first established by Yang and Yuan (2019) (see also Di et al. (2019)). Theorem 2.1 will be used in Section 4 to discuss general stability problems of mining pool-games for miners under Blockchain consensus, illustrating various scenarios embedded by miners' gap behaviors for consensus economics.

3 The Consensus Equilibria of Mining Gap Games and Applications

This section discusses general stability problems from literature on Bitcoin mining pool-games under Nakamoto' s 2008 consensus principle, then establishes general existence results for consensus equilibria of mining-pool games. Our discussion with illustrations shows that consensus games play a key role in consensus economics studies in Fintech.

Bitcoin' s blockchain protocol provides two incentives for miners: "Block rewards" and "transaction fees," which are key drivers for Bitcoin ecosystems. The former accounts for the vast majority of miner revenues at the system' s beginning but is expected to transition to the latter as block rewards dwindle. There has been implicit belief that whether miners are paid by block rewards or transaction fees does not affect blockchain security. However, Carlsten et al. (2016) (see also Kroll et al. (2015) and references) show this is not the case. Their key insight is that with only transaction fees, block reward variance is very high due to exponentially distributed block arrival times, making it attractive to fork a "wealthy" block to "steal" rewards. This results in an equilibrium with undesirable properties for Bitcoin' s security and performance, and even non-equilibria in some circumstances. They also study selfish mining (see Eyal and Sirer (2014)) and show it can be profitable for miners with arbitrarily low hash power shares, poorly connected within the network, or working alone (i.e., miners' noncooperative behavior). Thus we must consider Bitcoin ecosystem stability in terms of hybrid solution existence (i.e., consensus equilibrium) for mining-pool games with honest and dishonest miners mixing cooperation and

non-cooperation, particularly regarding miners' working behavior and strategy in different pools implementing Nakamoto's "proof of work" mechanism.

We focus on the mechanism of "Mining Gap Behavior" (or "Gap Games") where miners avoid mining blocks when available fees are insufficient. If incentives come only from fees, mining gap behavior emerges, potentially impacting Bitcoin stability (see Carlsten et al. (2016) and references). Based on our results, we affirmatively answer a fundamental question in consensus economics (raised in Section 1): "Can we design a reasonable consensus (e.g., Nakamoto's 2008 Consensus) to lead the mining-pool game to be stable (even with miner gap behaviors) in the sense that (1) honest miners always maintain Mining Longest Chain Rules (LCR) (with or without Gap Behavior or Fork Chain), plus plausible mining-pool attacking; and (2) the Bitcoin ecosystem always works (as majorities of miners do not collude to break it; 'collusion' means attempting to violate LCR and fork a high-reward block; see Saleh (2020) for discussion)?"

Furthermore, our applications illustrate that consensus equilibria serve as a fundamental tool for consensus economics studies under the Blockchain economy framework in Fintech.

3.1 The Meaning of Stability for Bitcoin Ecosystems

Bitcoin is the first widely popular cryptocurrency with a broad user base and rich ecosystem, all hinging on incentives to maintain the critical Bitcoin blockchain. For blockchain as a platform supporting businesses under the Bitcoin ecosystem, participants naturally form pools where members aggregate power and share rewards. Bitcoin experience shows that the largest pools are often open, allowing anyone to join. However, members can sabotage open pools by joining but never sharing proofs of work (called "attackers"). The pool shares revenue with the attacker, reducing earnings for participants (see Kroll et al. (2013), Eyal et al. (2014), Eyal (2015), Bonneau et al. (2015), Carlsten et al. (2016), Kiayias et al. (2016), Sapirstein et al. (2016), Tsabary and Eyal (2018) and references).

Thus open pools are susceptible to classical block withholding attacks (see Rosenfeld (2011), Kroll et al. (2013), Eyal et al. (2014), Eyal (2015), Bonneau et al. (2015)), where miners send only partial proof of work to the pool manager and discard full proof of work. By sending partial proof, the attacker is considered a regular pool member, allowing the pool to estimate its power. The attacker shares revenue from other members without contributing, reducing revenue for others and itself.

Following Bonneau et al. (2015), we face two opposing Bitcoin viewpoints: First, "Bitcoin works in practice, but not in theory"; second, "Bitcoin's stability relies on an unknown combination of socioeconomic factors that is hopelessly intractable to model with sufficient precision, failing to yield a convincing argument for the system's soundness."

Combining these viewpoints with Bitcoin's three main technical components—

"Transactions (including scripts)," "Consensus protocol," and "Communication network"—we believe it is critical to study "Stability" for Bitcoin regarding these components as a complex ecosystem.

For comprehensive study on stability aspects of mining-pool games, see Bonneau et al. (2015) and references. Here we focus on the following question regarding equilibrium existence for miners: "Does a consensus (hybrid solution) exist for mining-pool games with honest and dishonest miners mixing cooperative and non-cooperative behaviors, particularly regarding miners' strategies in different pools implementing Nakamoto' s 'proof of work' mechanism?"

Many discussions on stability meanings exist (see Bonneau et al. (2015), Garay et al. (2014), Kroll et al. (2013), Miller and La Viola Jr (2014) and references). We list two aspects below:

1) **Stability with bitcoin-denominated utility:** We may ask if simple majority compliance ensures fairness. Interesting non-compliant mining strategies include temporary block withholding (see Bahackm (2013), Eyal and Sirer (2014), Garay et al. (2014)). We may also ask if majority compliance is an equilibrium with perfect information (see Kroll et al. (2013)), or if majority compliance implies convergence and consensus (see Miller and La Viola Jr (2014), Garay et al. (2014)).

2) **Stability with incentives other than mining income:** At least two strategies have been analyzed that may advantage miners whose utility is not purely derived from mining rewards: Goldfinger attacks (see Kroll et al. (2013)) and Feather-forking proposed by Miller (2013).

A key mining pool issue is "Mining Gap" : without a block reward immediately after a block is found, if there is zero expected reward for mining but nonzero electricity cost, it becomes unprofitable for any miner to mine (see Bahackm (2013), Eyal and Sirer (2014), Tsabary and Eyal (2018) and literature).

Below we discuss how to outline Bitcoin system stability as consensus equilibrium existence under the consensus games framework, focusing on consensus associated with the Bitcoin ecosystem. We first briefly recall basic mining economics associated with "three types of consensuses."

3.2 The Explanation of Stability for Mining Pool Games through Consensus Games

Bitcoin economy success requires stable operation of Bitcoin' s distributed protocols, which relies on at least "three types of consensuses" :

1. **Consensus about Rules:** Players must agree on criteria to determine valid transactions. Only valid transactions are memorialized in the Bitcoin log, requiring agreement on validity determination.

2. **Consensus about State:** Players must agree on which transactions have occurred, i.e., they must agree on Bitcoin economy history to achieve

common understanding of coin ownership at any time.

3. **Consensus that Bitcoins are Valuable:** Players must agree that Bitcoins have value to accept them as payment.

These consensus forms depend mutually on each other. For example, agreeing on history is hard without agreeing on rules, and believing in Bitcoin value is hard if participants cannot agree on ownership.

Consensus about state is a technological problem in distributed systems design. Each player sees part of the state, and players must cooperate in large numbers across potentially unreliable networks to achieve consistent global state understanding. Technological consensus must be achieved despite some players deviating from published rules. In distributed systems literature, devious behavior ("Byzantine failures") can often be tolerated if a sufficient majority is honest and cooperative. However, in Bitcoin we explicitly assume players behave according to incentives (assuming cooperation despite contrary incentives would simplify design but be unrealistic). Game-theoretic issues are crucial for correct blockchain protocol execution. This was realized at inception when creator Nakamoto (2008) analyzed incentives in a simple but insufficient model. Understanding these issues is essential for Bitcoin survival and blockchain protocol development. In practice it helps understand strengths and vulnerabilities, and in economic and algorithmic theory it provides an excellent example for studying how rational ("selfish") players can play games in a distributed way, mapping possibilities and difficulties (e.g., the Miners Dilemma discussed by Eyal (2015)).

Distilling essential game-theoretic properties of blockchain maintenance is nontrivial; some "attacks" and vulnerabilities have been proposed but no systematic discovery method seems to exist. This paper studies two mining pool-game models as consensus game applications where miners (distributed network nodes running the protocol for payment) play a complete-information game. We note that incomplete-information situations, which may or may not fall under stochastic games, are not our focus here, as our goal is showing how consensus games are useful for mining pool games, particularly mining gap games.

Many works have focused on rational system analysis (see Rosenfeld (2011), Carlsten et al. (2016), Eyal and Sirer (2014) and references). These treat Bitcoin as a game between competing rational miners maximizing utilities postulated as natural incentive structures. The goal is investigating whether, or under which incentive/collaboration assumptions, Bitcoin achieves a stable state, i.e., a game-theoretic equilibrium.

As discussed, we interpret "attacker" behavior as miners playing noncooperative games with various attack strategies, and "honest miners" playing cooperative games by following Bitcoin consensus's "default compliant mining rule" applying LCR. Bitcoin ecosystem stability existence is equivalent to (hybrid) equilibrium existence, i.e., the "consensus equilibrium" of the "consensus game" defined above.

Therefore, consensus equilibrium existence under the Bitcoin consensus framework means there always exists a group working on "Longest Chain Rule"(LCR), ensuring proper Blockchain maintenance under Bitcoin consensus (though some miners work on forks, others do not; see Biais et al. (2019) addressing this via Markov perfect equilibrium). Thus studying consensus equilibrium existence provides the fundamental basis for consensus economics. We can establish Bitcoin mining game stability as applications of general consensus game existence results, shown below in Theorems 3.1 to 3.3 and Remarks 3.1 to 3.4.

3.3 The Framework of Mining Gap Games and Related Stability

Blockchain-based cryptocurrencies secure decentralized consensus protocols through incentives. Protocol participants called "Miners" (also "Players" or "Controllers") generate (mine) blocks containing monetary transactions. As participation incentives, miners receive newly minted currency and transaction fees. Blockchain bandwidth limits lead users to pay increasing fees to prioritize transactions. However, as Tsabary and Eyal (2018) note, most work focused on models where fees are negligible, except Carlsten et al. (2016) discussed that if incentives come only from fees, a mining gap forms: miners avoid mining when available fees are insufficient.

Our goal is establishing general existence results for consensus equilibria of general Gap Games using corresponding payoff (profit) functions directly, illustrating specific issues and problems on mining pool-game stability with different miner behaviors, and explaining possible Blockchain Ecosystem scenarios as Tsabary and Eyal (2018) did (using utility functions). Our consensus game application to Gap Game stability shows that consensus equilibria play a key role in explaining different consensus economics scenarios.

3.3.1 The General Framework of Mining-Pool Games In mining-pool games, we consider a system with a fixed set of miners and fixed set of mining rigs, where each miner controls at least one rig and each rig is controlled by exactly one miner, assuming homogeneous cost structures and symmetric information for all miners. For simplicity, we assume mining rigs are identical (as in Carlsten et al. (2016)). Rigs have two states: 1) "off state" (default); and 2) "on state" (running until finding a valid block).

Each miner assigns a start time for each controlled rig when it is turned on; we often refer to a turned-on rig as an "active rig." Once turned on, a rig' s time to find a valid block is exponentially distributed with a fixed rate parameter shared among all rigs (see Eyal and Sirer (2014), Nayak et al. (2015), Sapirstein et al. (2016) and references). Therefore, the time to find the first block by any rig is the minimum of all finding times. The rate parameter value is determined by the cryptocurrency protocol such that expected block time interval is constant. The rate parameter represents cryptographic puzzle difficulty, and we use difficulty and rate interchangeably. Miners' assigned start times affect the rate parameter;

if blocks are found too fast or slow, the protocol changes the difficulty parameter to adjust individual rig rates. In equilibrium, the rate parameter is fixed.

The rig finding the block first awards its controlling miner the block reward, comprising two parts. The first is fees reward from aggregating newly introduced transactions, which is time-dependent as pending transactions increase over time, growing potential fees reward. The second is a fixed subsidy called base reward, comprising new currency minting per block and expected transaction fees from the initial pending transaction set. Note that finding a new block rewards only the finding miner, not others.

Miners expend resources to participate. We differentiate two resource types. First, capital expenses ("Capex") for rig ownership (see Digiconomist.net (2017), Twiner (2017)) apply whether rigs are active or not. Second, operational expenses ("Opex") for active mining (see Digiconomist.net (2018a, 2018b)) apply to active rigs. These expenses apply to all miners, not just successful block miners.

Once a block is found, all miners move to find the next block, repeating indefinitely. A miner' s profit per block is the difference between total expenses and total reward. Rational miners strive to maximize profit, creating a game. The fundamental question is: "Do we have honest miners maintaining Bitcoin ecosystems by applying Mining Longest Chain Rules (in terms of Pareto optimal strategies maximizing profits under mining Gap Games behaviors)?" Below we establish general existence for consensus equilibria of mining-pool games, positively answering this question and confirming stability existence for mining gap games—a fundamental question for consensus economics.

3.3.2 The Concept of General Gap Games for Miners Mining-pool game behavior is critical for Blockchain ecosystems because blockchain-based cryptocurrencies secure decentralized consensus protocols through incentives. Miners generate blocks containing monetary transactions, receiving newly minted currency and transaction fees as incentives. Blockchain bandwidth limits cause users to pay increasing fees to prioritize transactions. However, we face a fundamental question (see Carlsten et al. (2016)): if incentives come only from fees, a mining gap may occur where "miners avoid mining when available fees are insufficient" (see Carlsten et al. (2016), Eyal and Sirer (2014), Tsabary and Eyal (2018) and references).

Following Tsabary and Eyal (2018), repeated block searches become a series of independent one-shot competitions where only one miner gets the reward but all pay expenses. To reason about expected revenues, we consider a one-shot game where a player' s strategy is choosing start times for all rigs. Players make start time choices a-priori. We define profit (and corresponding utility as expected profit) as expected income minus expected expenses at time t.

A "Gap Game (GP)" is a set of miners N := {1, 2, $\cdots$, n} with partition N1, N2, $\cdots$, Nk of N forming a system of n mining rigs controlled by k players,

where each Nj is a player j K = {1, 2, ⋯, k} controlling rig set Rj. For any j, i = 1, 2, ⋯, k, where i j, we have Rj , Ri Rj = and N = _{i=1}^k Ri = {1, 2, ⋯, n}.

Denote the expected block time interval achieved by the protocol as "Block-Interval." Each rig j' s start time is sj, with normalized start time ŝj := sj / Block-Interval. Once turned on, we assume a rig's block-finding time follows "an independent exponential distribution with rate parameter μ(ŝ)."For convenience, denote ŝ as the vector of n rigs' start times in increasing order. We assume all rigs are identical (i.e., with equal computing power). Each mining rig costs "Ccap" per time unit for ownership (capital cost) and "Cop" per time unit when turned on (operation cost).

The strategy space does not include turning rigs off, as this is irrational behavior. Block-finding time for an active rig follows an exponential distribution, which is memoryless. This means the probability of a rig finding a block in some time interval is unaffected by how much time has passed since mining began. Therefore, a single rig' s chances of finding a block do not decrease over time. Since total reward also increases over time, if reward justifies turning a rig on at some point, this justification holds from that time until the block is found.

3.3.3 The Framework of Fees Reward Accumulation and Related Costs Mining-pool parameter costs are affected by wide-ranging factors from different sources. Fees are affected by system users and markets (see Binns (2018), Blockchain.info (2018a, 2018b, 2018c), Earn.com (2018), Khatwani (2018) and Moser and Bohme (2015)). Base reward is also affected by users, markets, and minting rate defined by cryptocurrency protocol. Capital cost ("Capex") is affected by mining rig efficiency technological advancements (see Biais et al. (2019)), personnel wages, and real estate costs (see Digiconomist.net (2017), Malkin (2018), Wang (2017) and references). Operational cost ("Opex") is primarily affected by electricity costs (see Browne (2017), Digiconomist.net (2017, 2018a, 2018b)) for operating mining rigs, including puzzle solving and cooling expenses. These parameters are difficult to estimate, vary between currencies, and change over time for the same currency. Therefore, we analyze the system across parameter ranges to make general observations, focusing on robust trends.

Based on Tsabary and Eyal (2018)' s study of fees reward accumulation over time, it seems reasonable to use linear regression to measure fee reward accumulation. Thus we model total block reward as a linear function where the slope is the expected fees accumulation rate and the intercept is the sum of newly minted currency and expected fees available immediately after a block is found. Repeating measurements at other dates for different periods yields similar results. We denote t as the "fees accumulation rate" and 0 as the "base reward." To compare 0 and t importance, we define:

"Expected-Total-Fees" as the expected total fees accumulating during the ex-

pected time to find a block: Expected-Total-Fees := Block-Interval · t. We define EBRR := Expected-Total-Fees / Base-Reward.

Assuming each miner has only the option to join or leave the system, and for simplicity, we suppose Cop and Ccap are fixed amounts.

Next we build the profit function Pi(t) for each i = 1, 2, · · · , k at time t, allowing us to establish general consensus equilibria existence for Gap Games.

3.3.4 The Profit Function of Mining Gap Games To find the profit (and associated utility) function for each Gap Game player i at time t, we analyze block-finding time' s probability distribution as a payoff function of players' start time selections. We model block-finding time as random variable B with cumulative distribution function (CDF) FB(t; ŝ, μ(ŝ)) and probability density function (PDF) fB(t; ŝ, μ(ŝ)).

For a given miner i = 1, 2, · · · , k, assume a single rig j Ri with start time sj. Denote the time this rig requires to find a block as random variable Bj. Recall a single rig' s rate is μ(ŝ), set by protocol. Bj is drawn from a shifted exponential distribution with shift si and rate μ(ŝ).

Since all rigs compete to find the next block, the rig finding the next block first has the minimal Bj value, so the time to find the next block is the stop time process B defined as:

For any time t and any player i, the active set activei(t) is defined as activei(t) := {j Ri : sj t} and we define active(t) := _{i=1}^k Ri.

The corresponding CDF is (see Appendix B for details):

$$FB(t; \hat{s}, \mu(\hat{s})) = 1 - \Pr(t \quad B) = 1 - \exp(-\mu(\hat{s}) \cdot \Sigma\_\{j \text{ active}(t)\}(t - sj))$$

and the PDF is:

$$fB(t; \hat{s}, \mu(\hat{s})) = \mu(\hat{s}) \cdot |\text{active}(t)| \cdot \exp(-\mu(\hat{s}) \cdot \Sigma\_\{j \text{ active}(t)\}(t - sj))$$

where |active(t)| denotes the absolute value of active(t).

Once a rig is turned on, its block-finding time follows an exponential distribution. The exponential distribution is memoryless, meaning elapsed time does not affect a rig' s chances of finding a block. Since rate parameter μ(ŝ) is shared among all rigs, at any given time all active rigs have equal chance to find a block, regardless of active duration. Given active rig set active(t) at block-finding time, the probability of a specific active rig finding the block is one divided by the total number of active rigs.

Note that since a block is found at time t, there exists j {1, 2, · · · , k} such that sj t and thus |active(t)| > 0. As players may control many rigs, the probability that player i controls the rig finding the block is the number of her controlled active rigs divided by total active rigs. We denote player i' s active rigs ratio at time t as i(t) defined by:

$i(t) := |activei(t)| \ / \ |active(t)|$

The ratio $i(t)$ is continuous in t and represents the expected factor of player i' s portion of total reward. Thus for a block found at time t, player i' s expected income (denoted $E(Incomei|B = t)$) is:

$E(Incomei|B = t) = \ i(t) \ \cdot(\ 0 + \ t \ \cdot t)$

Players have two expense types (see Tsabary and Eyal (2018)): "Capex" for capital costs like "owning a rig," and "Opex" for operation costs like "keeping a rig active." Since Capex applies to all rigs controlled by a player, whether on or off, each rig' s capex by time t is $Ccap \ \cdot t$. As Rj is the set of rig indices player j controls, totaling $|Rj|$ rigs, player j' s total Capex at time t is $Ccap \ \cdot |Rj| \ \cdot t$.

Opex applies only to active rigs. For each active rig, expenses by time t are Cop multiplied by active duration: at time t, active rig j with start time sj has been active for time $t - sj$. Then player i's expected expenses (denoted $E(Expensei|B = t)$) at time t are:

$E(Expensei|B = t) := Ccap \ \cdot |Ri| \ \cdot t + Cop \ \cdot \Sigma\_\{j \ activei(t)\}(t - sj)$

For a given miner (player or controller) i at time t, we define its Profit Function Pi through expected income and expense functions:

$Pi(t) := E(profiti|B = t) = E(Incomei|B = t) - E(Expensei|B = t)$

where $E(Incomei|B = t)$ and $E(Expensei|B = t)$ are expected income and expenses at time t for a given Gap Game. We assume the reward function has the form:

$E(Incomei|B = t) = \ i(t)(\ 0 + \ t \ \cdot t)$

For more general studies on incentive-compatible reward functions for Bitcoin mining pools, see Schrijvers et al. (2017) and references. It follows that for each miner i (see Appendix B for details):

$Pi(t) = \ i(t)(\ 0 + \ t \ \cdot t) - Ccap \ \cdot |Ri| \ \cdot t - Cop \ \cdot \Sigma\_\{j \ activei(t)\}(t - sj)$

We list special cases below for each miner i:

Case I: When $Cop = 0$, $Pi(t) = \ i(t)(\ 0 + \ t \ \cdot t) - Ccap \ \cdot |Ri| \ \cdot t$.

Case II: When $Ccap(t) = 0$, $Pi(t) = \ i(t)(\ 0 + \ t \ \cdot t) - Cop \ \cdot \Sigma\_\{j \ activei(t)\}(t - sj)$.

Case III: When $Cop = 0$ and $Ccap(t) = 0$, $Pi(t) = \ i(t)(\ 0 + \ t \ \cdot t)$.

These cases will be used below to study consensus equilibria existence for Gap Games.

We note that our approach differs from most existing literature in key ways: (1) Our Blockchain ecosystem stability study is based on the Profit function Pi using consensus equilibria from game theory, allowing us to handle the general Gap games framework and prove existence of honest miners maintaining "Mining

Longest Chain Rules (LCR)"under a given consensus (leading to Profit Functions meeting required conditions). Thus we positively claim: (1) honest miners always maintain LCR (with or without Gap Behavior or Fork Chain), plus plausible mining-pool attacking; and (2) the Bitcoin ecosystem always works (as majorities do not collude to break it). (2) Many scholars (e.g., Tsabary and Eyal (2018), Liu et al. (2019) and references) use utility function Ui for each player i to identify gap behavior impact, where expected Utility is defined as Ui(t) := E(Profiti) for each miner i. This transforms Gap game choices into a multi-objective optimization problem. However, general existence results for such problems are hard to establish, requiring algorithms and numerical simulations as in Tsabary and Eyal (2018), Liu et al. (2019) and others.

4 The Consensus Equilibria of Gap Games and Stability of Blockchain Ecosystems

For a given mining gap game with i N = {1, 2, ⋯, n}, without loss of generality we assume Ti is a sufficiently large value in R for time, and define Xi := [0, Ti] and X := (cid:81)_{i=1}^n Xi. Then Xi and X are compact convex subsets of R and R^n for i N.

Based on Gap game notation and profit function Pi(t) for i N at time t defined on Xi, a gap game is indeed a consensus game CG := (N, K, (Xi, Pi)_{i N}), where N = {1, 2, ⋯, n}, K = {1, 2, ⋯, k} with k' s partition N1, ⋯, N2, ⋯, Nk of N as mentioned above.

We have the following general existence results for consensus equilibria of Gap Games supporting Blockchain Ecosystem stability as applications of the general consensus game model from Section 2.

Theorem 4.1 (Consensus Equilibria for Mining-Gap Games). For a given general Mining Gap Game (which is a consensus game CG), if the profit function Pi (defined above) is concave from [0, Ti] → R for each i N = {1, 2, ⋯, n}, then the Gap Game CG has at least one consensus equilibrium.

Proof. For each i N, Pi is continuous in t, and by assumption concave, thus Pi is continuous and concave. All Theorem 2.1 assumptions are satisfied, so the conclusion follows from Theorem 2.1.

Theorem 4.1 shows that under a given consensus, if miner i' s Profit function Pi is reasonably well-behaved (see special cases below that naturally satisfy this), consensus game theory allows us to handle the general Gap games framework and prove existence of honest miners maintaining "Mining Longest Chain Rules (LCR)" under a given consensus (e.g., Nakamoto (2008)). This affirmatively answers: "Blockchain ecosystem stability exists due to honest miners maintaining LCR under a reasonable consensus," leading to claims: (1) honest miners always maintain LCR, plus plausible mining-pool attacking; and (2) the Bitcoin ecosystem always works.

As Theorem 4.1 applications, we have results assuming zero operational cost for the Gap Game system.

Theorem 4.2 (Gap Games without Operational Cost). For a given general Gap Game with zero operational costs, if the ratio function i(t) is concave in t for each i N = {1, 2, ⋯, n}, then the Gap Game has at least one consensus equilibrium.

Proof. For i N, assuming i is concave in t, the second derivative '' _i of i is nonnegative. With Cop = 0, Pi(t) = i(t)(0 + ⋅t) − Ccap ⋅|Ri| ⋅t. Then the second derivative P'' _i of Pi(t) is nonnegative, so Pi is concave. Since Pi is also continuous for t Xi = [0, Ti], all Theorem 4.1 assumptions are satisfied, and the conclusion follows from Theorem 4.1.

Based on Theorem 4.2, we discuss a "No Gap" phenomenon for Mining-Pool games in practice when the system has no operational cost.

Remark 4.1 (Mining-Pool Game Stability without Operational Cost). By Theorem 4.2, each miner i's Profit function has form Pi(t) = i(t)(0 + ⋅t) − Ccap ⋅|Ri| ⋅t. Since the term "−Ccap ⋅|Ri| ⋅t"plays a large negative role in Pi(t) at time t, one way to reduce system loss (in terms of Pi(t)) is to make ratio i(t) as large as possible at time t. If miner i' s computing power is mi for i N, one possible best strategy is running all rigs, making activei(t) = mi and thus i(t) = mi / Σ_{j=1}^n mj at any time t [0, Ti]. Therefore i(t) is independent of t and thus concave, satisfying concavity assumptions, implying the gap game system without operational cost always has at least one equilibrium with miners starting mining at time zero (thus without operational cost, pool-games generally have no "gap" phenomenon as all miners prefer starting at time zero due to no operational expense).

This result indicates that if a system is designed to mine Bitcoin with only capital cost (zero operational cost), there always exists a subgroup of miners running the system, resulting in Bitcoin ecosystem stability. This affirmatively answers the general stability existence question for mining-pool games regarding following Longest Chain Rules (LCR), a fundamental question from academia to financial industries. This is exactly the "Scenario One: No Mining Gap" case discussed by Tsabary and Eyal (2018), assuming "a system comprised of two miners with no operational expenses," where each miner tries to increase mining power as soon as possible to find blocks without additional cost by starting at time zero (here we also illustrate pool games with more than two miners without gap phenomenon). For two-miner pool games, both players prefer increasing mining power at time zero (if no operational cost), leading ratios 1(t) and 2(t) to be m1/(m1+m2) and m2/(m1+m2) respectively, reaching general equilibrium maintaining system operation without gap phenomenon.

When mining pool game systems have zero capital and operational costs, we have the following general result for mining pool games without gap game behavior.

Theorem 4.3 (Mining Gap Games without Capital and Operational Cost). For a given general Gap Game with both Capital and Operational Costs zero, if the ratio function i(t) is concave in t for each i N = {1, 2, ···, n}, then the mining pool game has at least one consensus equilibrium and no gap game behavior phenomenon.

Proof. Equilibria existence follows from Theorem 4.2, and no gap game behavior follows from Remark 4.1.

Remark 4.2. When Cop = 0 and Ccap(t) = 0, considering Profit function Pi(t) = i(t)(0 + t ·t), the best way to increase Pi(t) is fully running rigs, making i = mi / Σ_{j=1}^n mj where mi is miner i' s mining power for i {1, 2, ···, n}. Here i(t) is constant, satisfying all Theorem 4.3 assumptions, leading to at least one equilibrium.

Based on the Profit function from Theorem 4.1, we can discuss arbitrary mining gap phenomena without assuming zero capital and operational costs.

Remark 4.3 (Scenarios of Arbitrary Mining Gaps Games). In Theorem 4.1, for each miner i N = {1, 2, ···, n}, Profit function Pi(t) = i(t)(0 + t ·t) − Ccap ·|Ri| ·t − Cop ·Σ_{j activei(t)}(t − sj). Generally, with non-zero Capital and Operational costs, the term Ccap ·|Ri| ·t + Cop ·Σ_{j activei(t)}(t − sj) negatively contributes to Pi(t) at time t, while i(t)(0 + t ·t) positively contributes. Thus base reward and fees accumulation rate are important factors for miners deciding mining power for Bitcoin mining in gap games behavior regarding start time decisions.

Two situations show when arbitrary mining gap phenomena may occur based on EBRR values (see EBRR definition in Section 3.3.3):

Case 1: If EBRR is small, i.e., EBRR c for some constant c, then 0 c · t ·Block-Interval, implying i(t)(0 + t ·t) i(t) · t ·(c ·Block-Interval + t). This means base reward and fees accumulation rate contributions to Pi(t) are limited (bounded above). Thus we may conclude "player i has negative utility" because as player i controls more rigs (i.e., has higher relative mining power), her per-mining-rig utility decreases with total mining power by the above inequality. Even though higher mining power increases reward probability, expense increases are more significant, resulting in lower utility. This leads miners to run rigs later (not at the beginning), i.e., start times not at or near zero, causing arbitrary mining gap phenomena.

Case 2: If EBRR is large enough, i.e., EBRR c1 for some constant c1, then 0 c1 · t ·Block-Interval, implying i(t)(0 + t ·t) i(t) · t ·(c1 ·Block-Interval + t). This means base reward and fees accumulation rate contributions to Pi(t) are bounded below, making contributions positive because as player i controls more rigs, her per-rig utility increases with total mining power. The increased reward probability surpasses expense increases, resulting in higher utility. Thus miner i tends to run rigs at the very beginning around time zero (resulting in no mining gap).

These trends for miners in both cases are maintained for all opex and capex ratio settings under high or low EBRR levels.

A second way to discuss possible mining gap behaviors examines profit function Pi impacts based on capital and operational cost relationships:

Case 3: For any player i' s relative mining power and any EBRR, when Capex dominates (much higher than Operational cost), player i' s choice of start times greater than zero is better (leading to mining gap phenomena). This reduces expected opex as controlled rigs are active for less time. The more rigs controlled, the more impactful this effect. This suggests when opex is at play (middle or higher operational cost levels), taking mining gaps is generally a better option.

Case 4: However, when Capex cost is not much higher than operational cost, miners may not exhibit mining gap behavior in practice because early rig operation may find blocks earlier, thus reducing operational cost (as term Ccap · |Ri| · t may not be large compared to Cop · |Ri| · t) based on inequality:

Cop · |activei(t)| min{(t − sj)} Cop · |activei(t)| · t Cop · |Ri| · t

But mining gap behavior may occur if capital cost is not much less than operational cost.

The discussion in Cases 3 and 4 using miner i' s Profit function Pi shows operational costs are also a major mining gap factor, confirmed by numerical simulations in Tsabary and Eyal (2018).

Together, gap game behaviors are caused by three factors: (1) base reward and fees accumulation rate; (2) operational and capital cost levels; and (3) mining power.

As EBRR level applications, we have the following Bitcoin long-term case study expectation.

Remark 4.4 (Bitcoin Case Study). Following Tsabary and Eyal (2018), we briefly discuss Bitcoin ten years from now based on miner i' s Profit function Pi(t) at time t.

Thinking Bitcoin becomes prone to undesired mining gap effects, many operational cryptocurrency systems vary in minting, fees, market cap, and expenses. Given any cryptocurrency' s parameters, similar estimation can be performed using our model, presenting a Bitcoin case study below with Theorem 4.1 illustration.

Today, Bitcoin has around 7 mining pools (see [9]-[11]) controlling about 85% of mining power, with the rest divided among many smaller pools. Though varying in size, we approximate this with 8 equal-size miners. Assuming long-term from today (e.g., around 10 years), we assume EBRR is around 1, which may be required to maintain a small gap. Currently, minting and fees rewards are B12.5 and about B1 respectively, so EBRR 12.5, making gaps unprofitable. However, in about ten years, minting reward drops may lead to EBRR around

1, meaning factor " t" plays a bigger role representing the time value of the positive term i(t)(0 + t ·t), while maintaining cost term Ccap ·|Ri| ·t + Cop ·Σ_{j activei(t)}(t − sj) reasonably small, making Pi(t) positive when time t is long enough in the future. Bitcoin' s long-term mining gap phenomenon (around ten years from now assuming EBRR 1) is also illustrated by Remark 4.3 analysis.

Before concluding, we note that based on the new "Consensus Game (CG)"notion motivated by blockchain economy mechanism design under Bitcoin ecosystem consensus incentives, we first establish general existence results for consensus equilibria of general gap games using profit functions directly. In applications, we discuss general mining gap phenomena for mining-pools, and assuming ten years from now with EBRR 1, we show that while Bitcoin economics mining-pool gap game behaviors may occur (Remark 4.3 discussion), the blockchain platform for Bitcoin ecosystem remains "stable" in the sense that honest miners still mine blocks following "mining LCR" in practice (by Theorem 4.1).

We emphasize that studying Mining Gap games and related mining-pool game stability via consensus games shows that consensus equilibria play a key role in developing fundamental consensus economics theory. Indeed, consensus games can also establish general fundamental results supporting existence and stability for Bitcoin economics mining-pool games.

5 Conclusion

By incorporating cooperative and noncooperative behaviors in game theory for Bitcoin ecosystem Mining Pool Games under blockchain platform mechanism design following Nakamoto' s (2008) consensus principle, it is natural to introduce the new "consensus game" concept. This notion allows analyzing strategy choices where cooperative and noncooperative behaviors coexist in different situations, explaining mining gap game stability using "Consensus Games (CG)." We outline how general consensus equilibria existence is formulated to explain Bitcoin mining gap game stability, then establish general existence results for consensus equilibria of general mining gap games using profit functions as payoff functions.

As applications, results illustrate specific mining pool-game issues and problems with potential impacts from miners' gap behaviors, explaining different mining gap behavior phenomena in Blockchain Ecosystems. Our study shows consensus equilibria may play an important role in developing fundamental consensus economics theory.

Compared to traditional cooperative and noncooperative games, our consensus game concept is a natural extension for consensus economies, especially under the Bitcoin ecosystem framework with consensus incentives (e.g., Nakamoto' s consensus protocol). Our study shows it may lay the foundation for consensus economics.

We conclude that consensus equilibria existence results for consensus games defined in this paper are useful and should provide the basis for consensus economics studies under the Blockchain fintech framework as discussed above.

Further study on different smart contract situations for various digital business activities under Blockchain with associated consensus incentives ("blockchain economy") should be a priority in the big data era. We note recent fintech topic studies by scholars including dynamic equilibria under blockchain disruption (Cong and He (2019)), blockchain-based accounting and assurance (Dai and Vasarhelyi (2017)), and other related issues (Narayanan et al. (2016), Goldstein et al. (2019), Chiu and Koeppl (2019), Foley et al. (2019), Fuster et al. (2019), Tang (2019), Vallee and Zeng (2019), D' Acunto et al. (2019), Zhu (2019), Chen et al. (2019), Di et al. (2019) and references).

Finally, our goal is showing how the new "Consensus Equilibria" notion for Mining-Pool games can study Blockchain ecosystem stability impacts when mining-pool miners exhibit gap behaviors, assuming Mining-Pool Games have homogeneous cost structures and symmetric information for all miners. Indeed, by incorporating both "consensus equilibria" and "Markov equilibrium" concepts, we can also study stability impacts from miners' Gap behaviors under heterogeneous cost structures and asymmetric information in Mining-Pool games—this is our future work.

6 Acknowledgement

This research is supported in part by NSF of China under Nos. U181140004 and 11501349.

References

[1] Askoura, Y. 2011. The weak-core of a game in normal form with a continuum of players. *Journal of Mathematical Economics* 47(1):43-47.
[2] Askoura, Y., M. Sbihi, and H. Tikobaini. 2013. The ex-ante −core for normal form games with uncertainty. *Journal of Mathematical Economics* 49(2):157-162.
[3] Aumann, R.J. 1961. The core of a cooperative game without sidepayments. *Transactions of the American Mathematical Society* 98:539–552.
[4] Badertscher, C., U. Maurer, D. Tschudi, and V. Zikas. 2017. Bitcoin as a transaction ledger: A composable treatment. In: Katz, F., Shacham, H. (eds.) *CRYPTO 2017*, Part I, LNCS, vol. 10401. pp 324-356. Springer, Heidelberg.
[5] Badertscher, C., J. Garay, U. Maurer, D. Tschudi, and V. Zikas. 2018. But why does it work? A rational protocol design treatment of bitcoin. *Advances in Cryptology–EUROCRYPT 2018*, Part II, Lecture Notes in Comput. Sci., vol. 10821. pp. 34-65. Springer, Cham.
[6] Bahackm L. 2013. Theoretical Bitcoin Attacks with less than Half of the Computational Power. Technical Report abs/1312.7013, CoRR.
[7] Biais, B., C. Bisire, M. Bouvard, and C. Casamatta. 2019. The blockchain

folk theorem. *Review of Financial Studies* 32(5): 1662-1715.
[8] Binns, calculate transaction https://support.earn.com/digital-currency/bitcoin-transactions-and-fees/how-do-i-calculate-my-transaction-fee (2018).
[9] Blockchain.info. 2018a. Bitcoin Market Capitalization. http://blockchain.info/charts/market-cap, retrieved Feb. (2018).
[10] Blockchain.info. 2018b. Bitcoin Mining Pools. https://blockchain.info/pools, retrieved May (2018).
[11] Blockchain.info. 2018c. Transaction Fees. https://blockchain.info/charts/transaction-fees, retrieved Feb. (2018).
[12] Bonneau, J., A. Miller, J. Clark, A. Narayanan, A. Kroll, and E. Felten. 2015. 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).
[13] Border, K.C. 1984. A core existence theorem for games without ordered preferences. *Econometrica* 52(6): 1537-1542.
[14] Browne, R. 2017. The cheapest and most expensive countries to mine bitcoin (2017). https://www.cnbc.com/2018/02/15/the-cheapest-and-most-expensive-countries-to-mine-bitcoin.html.
[15] Carlsten, M., H. Kalodner, S.M. Weinberg, and A. Narayanan. 2016. On the instability of Bitcoin without the block reward. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp. 154-167, Vienna, Austria (October 24-28, 2016).
[16] Chen, M., Q. Wu, and B. Yang. 2019. How valuable is FinTech innovation? *Review of Financial Studies* 32(5):2062-2106.
[17] Chiu, J., and T. Koeppl. 2019. Blockchain-based settlement for asset trading. *Review of Financial Studies* 32(5): 1716-1753.
[18] Cong, L.W., and Z. He. 2019. Blockchain disruption and smart contracts. *Review of Financial Studies* 32(5): 1754-1797.
[19] D' Acunto, F., N. Prabhala, and A.G. Rossi. 2019. The promises and pitfalls of Robo-Advising. *Review of Financial Studies* 32(5): 1983-2020.
[20] Dai, J., and M.A. Vasarhelyi. 2017. Toward blockchain-based accounting and assurance. *J. Information Systems* 31:5-21.
[21] Di, L., Z. Yang, and George X. Yuan. 2019. The consensus games consensus economics under D.F.(eds). *Communications in Computer and Information Science*, Vol. 1082, pp. 1-26. 3rd East Asia Game Theory International Conference (March 7-9, 2019, Fuzhou University, Fujian, China). Springer, Singapore.
[22] Digiconomist.net. 2017. A Deep Dive in a Real-World Bitcoin Mine. https://digiconomist.net/deep-dive-real-world-bitcoin-mine (2017).
[23] Digiconomist.net. 2018a. Bitcoin Energy Consumption Index. https://digiconomist.net/bitcoin-energy-consumption (2018).
[24] Digiconomist.net. 2018b. Ethereum Energy Consumption Index. https://digiconomist.net/ethereum-energy-consumption (2018).
[25] Earn.com. Predicting Bitcoin Transactions. https://bitcoinfees.earn.com/ (2018).
[26] Eyal, I. 2015. The Miners Dilemma. In: *Proceedings of the 36th IEEE*

Symposium on Security and Privacy, San Jose, California, USA (May 18-20, 2015).
[27] Eyal, I., E. G. Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In: *Proceedings of the 18th International Conference on Financial Cryptography and Data Security*, FC' 14, pp. 436-454. Springer, Berlin Heidelberg.
[28] Florenzano, M. 1989. On the nonemptiness of the core of a coalitional production economy without ordered preferences. *Journal of Mathematical Analysis and Applications* 141:484-490.
[29] Foley, S., J.R. Karlsen, and T. Putnins. 2019. Sex, Drugs, and Bitcoin: How much illegal activity is financed through Cryptocurrencies? *Review of Financial Studies* 32(5): 1798-1853.
[30] Fuster, A., M. Plosser, S. Schnabl, and J. Vickery. 2019. The Role of Technology in Mortgage Lending. *Review of Financial Studies* 32(5): 1854-1899.
[31] Garay, J.A., J. Katz, B. Tackmann, and V. Zikas. 2015. 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).
[32] Garay, J.A., A. Kiayias, and N. Leonardos. 2014. The Bitcoin Backbone Protocol: Analysis and Applications. Cryptology ePrint Archive, Report 2014/765.
[33] Garay, J.A., A. Kiayias, and N. Leonardos. 2015. The bitcoin backbone protocol: Analysis and applications. In: Oswald, E., Fischlin, M. (eds). *EUROCRYPT 2015*, Part II, LNCS, vol. 9057, pp. 281-310. Springer, Heidelberg (April 2015).
[34] Garay, J.A., A. Kiayias, and N. Leonardos. 2017. The bitcoin backbone protocol with chains of variable difficulty. In: Katz, J., Shacham, H (eds). *CRYPTO 2017*, Part I, LNCS, vol. 10401. pp. 291-323. Springer, Heidelberg (August 2017).
[35] Goldstein, I., W. Jiang, and G. Karolyi. 2019. To FinTech and beyond. *Review of Financial Studies* 32(5): 1647-1661.
[36] Ichiishi, T. 1981. A social coalitional equilibrium existence lemma. *Econometrica* 49: 369-377.
[37] Kajii, A. 1992. A generalization of Scarf' s theorem: an −core existence theorem without transitivity or completeness. *Journal of Economic Theory* 56:194-205.
[38] Khatwani, S. 2018. Ethereum: Ether, Ether Gas, Gas Limit, Gas Price and Fees. https://coinsutra.com/ethereum-gas-limit-gas-price-fees/ (2018).
[39] Kiayias, A., E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis. 2016. Blockchain mining games. In: *2016 ACM Conference on Economics and Computation*, Maastricht, The Netherlands (July 24-28, 2016).
[40] Kroll, J., I. Davey, and E. Felten. 2013. 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 (June 11-12, 2013).
[41] Kwon, Y., D. Kim, Y. Son, E. Vasserman, and Y. Kim. 2017. Be selfish

and avoid Dilemmas: Fork after withholding (FAW) attacks on Bitcoin. In *2017 ACM CCS' 17*, Oct. 30 - Nov. 3, 2017, Dallas, TX, USA.
[42] Lefebvre, I. 2001. An alternative proof of the nonemptiness of the private core. *Economic Theory* 18(2): 275–291.
[43] Liu, Y., J. Ke, Q. Xu, H. Jiang, and H. Wang. 2019. Decentralization is vulnerable under the Gap game. *IEEE Access* 7: 90999-91008.
[44] Malkin, Bitcoin. Cheapest Mining Places. https://cryptocurrencynews.com/daily-news/cryptocurrency-mining/cheapest-places-mining-bitcoin/ (2018).
[45] Martins-da-Rocha, V.F., and N. Yannelis. 2011. Nonemptiness of the alpha core. Working paper. Manchester School of Social Sciences, University of Manchester.
[46] Miller, A. 2013. Feather-forks: enforcing a blacklist with sub-50% hash power. bitcointalk.org (October 2013).
[47] Miller, A., and J.J. LaViola Jr. 2014. Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin.
[48] Moser, M., and R. Bohme. 2015. Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees. In *Financial Cryptography and Data Security*, Michael Brenner, Nicolas Christin, Benjamin Johnson, and Kurt Rohloff (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 19-33.
[49] Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf.
[50] Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.
[51] Nayak, K., S. Kumar, A. Miller, and E. Shi. 2015. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. IACR Cryptology ePrint Archive 2015: 796. http://eprint.iacr.org/2015/796.
[52] Noguchi, M. 2018. Alpha cores of games with nonatomic asymmetric information. *Journal of Mathematical Economics* 75: 1-12.
[53] Nyumbayire, A. Nakamoto Consensus Insight, Interlogica. https://www.interlogica.it/en/insight-en/nakamoto-consensus.
[54] Pass, R., L. Seeman, and A. Shelat. 2017. Analysis of the blockchain protocol in asynchronous networks. In: Coron, J., Nielsen, J.B. (eds). *EUROCRYPT 2017*, Part II, LNCS, vol. 10211. pp. 643-673. Springer, Heidelberg.
[55] Rosenfeld, M. 2011. Analysis of Bitcoin pooled mining reward systems. arXiv preprint arXiv: 1112.4980.
[56] Saleh, F. 2020. Blockchain Without Waste: Proof-of-Stake. http://dx.doi.org/10.2139/ssrn.3183935 (January 2020). Available at SSRN: https://ssrn.com/abstract=3183935.
[57] Sapirstein, A., Y. Sompolinsky, and A. Zohar. 2016. Optimal selfish mining strategies in bitcoin. In: Grossklags, J., Preneel, B. (Eds.) *Financial Cryptography 2017*, LNCS, vol. 9603. pp. 515-532. The 20th International Conference (FC 2016, Christ Church, Barbados, February 22-26, 2016).
[58] Scarf, H.E. 1971. On the existence of a cooperative solution for a general class of n-person games. *Journal of Economic Theory* 3: 169-181.
[59] Schrijvers, O., J. Bonneau, D. Boneh, and T. Roughgarden. 2016. Incentive compatibility of Bitcoin mining pool reward functions. In: Grossklags, J.,

Preneel, B. (Eds.) *Financial Cryptography 2017*, LNCS, vol. 9603. pp. 477-498. The 20th International Conference (FC 2016, Christ Church, Barbados, February 22-26, 2016).
[60] Shafer, W., and H. Sonnenschein. 1975. Equilibrium in abstract economies without ordered preferences. *Journal of Mathematical Economics* 2: 345-348.
[61] Tang, H. 2019. Peer-to-Peer lenders versus banks: substitutes or complements? *Review of Financial Studies* 32(5): 1900-1938.
[62] Tsabary, I., and I. Eyal. 2018. The gap game. In: *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security (CCS' 18)*, 713-728.
[63] Tuwiner, Bitcoin Mining Hardware. https://www.buybitcoinworldwide.com/mining/hardware/ (2017).
[64] Uyanik, M. 2015. On the nonemptiness of the −core of discontinuous games: Transferable and nontransferable utilities. *Journal of Economic Theory* 158: 213-231.
[65] Vallee, B., and Y. Zeng. 2019. Marketplace Lending: A New Banking Paradigm? *Review of Financial Studies* 32(5): 1939-1982.
[66] Wang, C. 2017. A Visit to a Bitcoin Mining Farm in Sichuan, China Reveals Troubles Beyond Regulation. https://news.bitcoin.com/a-visit-to-a-bitcoin-mining-farm-in-sichuan-china-reveals-troubles-beyond-regulation/ (2017).
[67] Weber, S. 1981. Some results on the weak core of a non-side-payment game with infinitely many players. *Journal of Mathematical Economics* 8: 101-111.
[68] Yannelis, N.C., and N.D. Prabhakar. 1983. Existence of maximal elements and equilibria in linear topological spaces. *Journal of Mathematical Economics* 12: 233-245.
[69] Yang, Z., and X.Z. Yuan. 2019. Some generalizations of Zhao' s theorem: hybrid solutions and weak hybrid solutions for games with nonordered preferences. *Journal of Mathematical Economics* 84: 94-100.
[70] Yuan, X.Z. 1999. The study of equilibria for abstract economies in topological vector spaces—a unified approach. *Nonlinear Analysis* 37: 409-430.
[71] Zhao, J. 1992. The hybrid solutions of an N-person game. *Games and Economic Behavior* 4: 145-160.
[72] Zhao, J. 1996. The hybrid equilibria and core selection in exchange economies with externalities. *Journal of Mathematical Economics* 26(4): 387-407.
[73] Zhu, C. 2019. Big data as a governance mechanism. *Review of Financial Studies* 32(5): 2021-2061.

Appendix A: The Consensus Games

Using Section 2 notation, we recall results from Yang and Yuan (2019). The following is the consensus game version of Theorem 3.1 from Yang and Yuan (2019) (see also Theorem 3.1 of Di et al. (2019)).

Theorem A.1. Suppose a consensus game CG = (N, p, (X(t))_{t N}, P)

satisfies: (i) N is finite; (ii) for each t N, X(t) is a nonempty convex compact subset of R^{mt}; (iii) for each t N, P(t, ·) is convex-valued with open graph in X × X, and x P(t, x) for any x X.

Then CG has at least one consensus equilibrium.

Yang and Yuan (2019) gave an infinite-dimensional version of Theorem A.1 (Theorem 3.2 of Yang and Yuan (2019)), stated here using consensus games:

Theorem A.2. Suppose a consensus game CG = (N, p, (X(t))_{t N}, P) satisfies: (i) N is finite; (ii) for each t N, X(t) is a nonempty convex compact subset of a Hausdorff topological vector space E(t); (iii) for each t N, P(t, ·) is convex-valued with open graph in X × X and x P(t, x) for any x X.

Then CG has at least one consensus equilibrium.

As a Theorem A.2 application, we have the following corollary extending Theorem A.1 to topological vector spaces.

Corollary A.1. Suppose a normal-form game with partition G = (N, p, (Xi, ui)_{i N}) satisfies: (i) N is finite; (ii) for each i N, Xi is a nonempty convex compact subset of a Hausdorff topological vector space Ei; (iii) for each i N, ui is continuous and quasiconcave on X.

Then G has at least one hybrid solution (thus the consensus equilibrium of consensus game G).

Appendix B: The Profit Function of Mining Gap Games

For a given miner i = 1, 2, ⋯, k, assume a single rig j Ri with start time sj. Denote the time this rig requires to find a block as random variable Bj. Recall a single rig' s rate is μ(ŝ), set by protocol. Bj is drawn from a shifted exponential distribution with shift si and rate μ(ŝ).

To find the profit (and associated utility) function for each Gap Game player i at time t, we analyze block-finding time' s probability distribution as a function of players' start time selections. We model block-finding time as random variable B with CDF FB(t; ŝ, μ(ŝ)) and PDF fB(t; ŝ, μ(ŝ)). The PDF of Bi is:

f_{Bj} = { 0, t sj; μ(ŝ) · exp(−μ(ŝ)(t − sj)), t > sj }

and its CDF is:

F_{Bj} = { 0, t sj; 1 − exp(−μ(ŝ)(t − sj)), t > sj }

Since F_{Bj}(t; sj, μ(ŝ)) = Pr(t Bj) = 1 − Pr(t Bj), it follows that:

Pr(t Bj) = { 0, t sj; exp(−μ(ŝ)(t − sj)), t > sj }

As all rigs compete to find the next block, the rig finding the next block first has the minimal Bj value, so the time to find the next block is the stop time process B defined as:

B := min_{j {1,2, ⋯ ,k}} Bj

For any time t and any player i, the active set activei(t) is defined as activei(t) := {j Ri : sj t} and we define active(t) := _{i=1}^k Ri.

The probability that none of the rigs have found a block by time t is Pr(t B), which is the product of Pr(t Bj) (as all rigs are independent):

Pr(t B) = *{j {1,2, ⋯ ,n}} Pr(t Bj)* = {j {1,2, ⋯ ,n}} Pr(t Bj) = exp(−μ(ŝ) · Σ_{j active(t)}(t − sj))

The corresponding CDF is:

FB(t; ŝ, μ(ŝ)) = 1 − Pr(t B) = 1 − exp(−μ(ŝ) · Σ_{j active(t)}(t − sj))

and the PDF is:

fB(t; ŝ, μ(ŝ)) = μ(ŝ) · |active(t)| · exp(−μ(ŝ) · Σ_{j active(t)}(t − sj))

Once a rig is turned on, its block-finding time follows an exponential distribution. The exponential distribution is memoryless, meaning elapsed time does not affect a rig's chances of finding a block. Since rate parameter μ(ŝ) is shared among all rigs, at any given time all active rigs have equal chance to find the block, regardless of active duration. Given active rig set active(t) at block-finding time, the probability of a specific active rig finding the block is one divided by the total number of active rigs.

Since a block is found at time t, there exists j {1, 2, ⋯ , k} such that sj t and thus |active(t)| > 0. As players may control many rigs, the probability that player i controls the rig finding the block is the number of her controlled active rigs divided by total active rigs. We denote player i's active rigs ratio at time t as i(t) defined by:

i(t) := |activei(t)| / |active(t)|

The ratio i(t) is continuous in t and represents the expected factor of player i's portion of total reward. Thus for a block found at time t, player i's expected income (denoted E(Incomei|B = t)) is:

E(Incomei|B = t) = i(t) · (0 + t · t)

Players have two expense types (see Tsabary and Eyal (2018)): "Capex" for capital costs like "owning a rig," and "Opex" for operation costs like "keeping a rig active." Since Capex applies to all rigs controlled by a player, whether on or off, each rig's capex by time t is Ccap · t. As Rj is the set of rig indices player j controls, totaling |Rj| rigs, player j's total Capex at time t is Ccap · |Rj| · t.

Opex applies only to active rigs. For each active rig, expenses by time t are Cop multiplied by active duration: at time t, active rig j with start time sj has been active for time t − sj. Then player i's expected expenses (denoted E(Expensei|B = t)) at time t are:

E(Expensei|B = t) := Ccap · |Ri| · t + Cop · Σ_{j activei(t)}(t − sj)

For a given miner (player or controller) i at time t, we define its Profit Function Pi through expected income and expense functions:

Pi(t) := E(profiti|B = t) = E(Incomei|B = t) − E(Expensei|B = t)

where E(Incomei|B = t) and E(Expensei|B = t) are expected income and expenses at time t for a given Gap Game. Generally we assume the reward function has form:

E(Incomei|B = t) = i(t)(0 + t ⋅t)
E(Expensei|B = t) = Ccap ⋅|Ri| ⋅t + Cop ⋅Σ_{s activei(t)}(t − s)

Thus:

Pi(t) = i(t)(0 + t ⋅t) − Ccap ⋅|Ri| ⋅t − Cop ⋅Σ_{j activei(t)}(t − sj)

As in Tsabary and Eyal (2018), we can also define utility function Ui (the expectation of Pi(t)) as:

Ui := E(Pi(t)) = E(E(Profiti|B = t)) = _0^∞ (E(Profiti|B = t) ⋅fB(t; ŝ, μ(ŝ))) dt

Then player (controller) i' s utility function is:

Ui(t) = E(Profiti) = E(E(profiti|B = t)) = *0^∞ { i(t)(0 + t ⋅t) − Ccap ⋅ /Ri/ ⋅t − Cop ⋅Σ*{j activei(t)}(t − sj)} ⋅fB(t, ŝ, μ(ŝ)) dt
= *0^∞ { i(t)(0 + t ⋅t) − Ccap ⋅ /Ri/ ⋅t − Cop ⋅Σ*{j activei(t)}(t − sj)} ⋅ {μ(ŝ) ⋅|active(t)| ⋅exp(−μ(ŝ) ⋅Σ_{j active(t)}(t − sj))} dt

Case I: When Cop = 0, Pi(t) = i(t)(0 + t ⋅t) − Ccap ⋅|Ri| ⋅t, and:

Ui(t) = *0^∞ { i(t)(0 + t ⋅t) − Ccap ⋅ /Ri/ ⋅t} ⋅ {μ(ŝ) ⋅ /active(t)/ ⋅ exp(−μ(ŝ) ⋅ Σ*{j active(t)}(t − sj))} dt

Case II: When Ccap(t) = 0, Pi(t) = i(t)(0 + t ⋅t) − Cop ⋅Σ_{j activei(t)}(t − sj), and:

Ui(t) = *0^∞ { i(t)(0 + t ⋅t) − Cop ⋅Σ*{j activei(t)}(t − sj)} ⋅{μ(ŝ) ⋅|active(t)| ⋅exp(−μ(ŝ) ⋅Σ_{j active(t)}(t − sj))} dt

Case III: When Cop = 0 and Ccap(t) = 0, Pi(t) = i(t)(0 + t ⋅t), and:

Ui(t) = *0^∞ i(t)(0 + t ⋅t) ⋅ {μ(ŝ) ⋅ /active(t)/ ⋅ exp(−μ(ŝ) ⋅ Σ*{j active(t)}(t − sj))} dt

Note: Figure translations are in progress. See original paper for figures.