The Framework of Consensus Equilibria for Gap Games in Blockchain Ecosystems

Lan Di[1], Fan Wang[2], Lijian Wei[2], George Yuan[2,3,4(✉)], Tu Zeng[4], Qianyou Zhang[5(✉)], and Xiaojing Zhang[6]

[1] School of Artificial Intelligence and Computer Science, Jiangnan University, Wuxi 214122, China
[2] Business School, Sun Yat-Sen University, Guangzhou 510275, China
george_yuan99@yahoo.com
[3] School of Fintech, Shanghai Lixin University of Accounting and Finance, Shanghai 201209, China
[4] BBD Technology Co., Ltd. (BBD), No. 966, Tianfu Avenue, Chengdu 610093, China
[5] Business School, Chengdu University, Chengdu 610106, China
zhangqianyou@163.com
[6] Military Science Press, Military Academy of Science, Xianghongqi, Haidian District, Beijing 100091, China

Abstract. The goal of this paper is to establish the general framework of consensus equilibria for Mining Pool Games in Blockchain Ecosystems, and in particular to explain the stable in the sense for the existence of consensus equilibria related to mining gap game's behaviors by using one new concept called "Consensus Games" under the environment of Blockchain Ecosystems, where, the Blockchain Ecosystem mainly means the economic activities by taking into the account of three fundamental factors which are "Expenses, Reward Mechanism and Mining Power" for the work on blockschain by applying the key consensus called "Proof of Work" due to Nakamoto in 2008 and related ones.

Keywords: Consensus equilibrium · Nakamoto consensus · Mining gap game · Blockchain ecosystems

1 Introduction

The goal of this paper is to explain the stable in the sense for the existence of consensus equilibria for mining gap games by using one new concept called consensus games (CG) under the framework of Blockchain Ecosystems which mainly mean the economic activities by taking into the account of three types of different factors which are expenses, reward mechanism and mining power for the work on blockschain by applying consensuses including the Proof of Work due to Nakamoto in 2008 as a special case.

By a fact that both equity and currency tokens are typically two kinds of initial coin offerings (ICOs) like Bitcoin or Ethereum based on the platform of

Z. Zheng et al. (Eds.): BlockSys 2020, CCIS 1267, pp. 45–53, 2020.
https://doi.org/10.1007/978-981-15-9213-3_4

Blochchains to provide a particular product or service, it is very important to study the mechanism of Blockchain Ecosystems. It is well known that in the Bitcoin world, all miners following the so-called Nakamoto's consensus protocol (2008), and work in a number of different groups (pools) to mine for Bitcion. Work on the block in a process called "mining" is successfully and approved due to the majority of miners applying key consensus called "Proof of Work", as each miner or pool may work in different ways, we need to thus deal with the so-called "Pool-Games" of miners (also use the term, "Mining Pool Game") with their working (mining) behaviors as an individual or in a group (pool) by following either cooperative or non-cooperative ways. In order to so do, we will introduce a new notion called "Consensus Games" which will be used to establish the general existence of consensus equilibria for consensus games to describe mining behavior for Blockchain Ecosystems in Fintech. In particular, we will focus on the general discussion for the mechanism of the phenomenon called "Mining Gap Behavior" (in short, "Gap Games") for miners under the framework of general incentives consensus in which miners would avoid mining blocks when the available fees are insufficient (in particular, if incentives come only from fees, then a mining gap behavior would happen, for more in details, see Carlesten et al. [3], Tsabary and Eyal [25] and related references wherein).

The idea to consider the mixture of both Nash and cooperative equilibria together was originally studied by Zhao [29] under the name called "Hybrid Solution", and supported by recently work under Yang and Yuan [27], we are able to establish a new tool by "Consensus Games" in topological vector spaces without ordered preferences from the viewpoint of Blockchain in Fintech (see also Di et al. [9,10])

Briefly, the "Consensus Game" is a new concept which allows us to discuss if there exists an acceptable (may or not be "optimal") collaborative 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, or non-cooperative game strategies by following such as mining "Longest Chain Rules (LCR)" due to Nakamoto [20] consensus (see also Biais et al. [1], Nyumbayire [22] and reference wherein) for the discussion with or without occurring forks for blockchain acting as a platform called the "Blockchain Ecosystems" or "Consensus Economics"). Thus, when comparing with the traditional cooperative and non-cooperative game, the consensus game is a natural extension for a consensus economy, especially under the framework of the Bitcoin ecosystem associated with Nakamoto's consensus protocol. We note that mining pool games were extensively studied by Bonneau et al. [2], Eyal [11], Eyal and Sirer [12], Kroll et al. [18], Sapirstein et al. [23] and references wherein. By applying the new concept called "Consensus Game" discussed by Di et al. [9,10], the aim of this paper is to discuss he following issue which is one of the most fundamental questions for consensus economics in Fintech:

"Is it possible to have a general consensus (for example, the Nakamoto's one) to lead the Mining-Pool Game stable in supporting the Blockchain ecosystem to run (even with existing attacker) in terms of two issues below:

(1) there always exists honest miners maintaining the Mining Longest Chain Rules (LCR) (given the plausibility of mining pool attacking); and

(2) Bitcoin ecosystem always works (or, majorities of miners do not collude to break it; here the term "collusion" means an attempt to violate the LCR and for a high reward block)?"

2 The Meaning for the New Concept "Consensus Games"

By following the consensus protocol due to Nakamoto in year 2008, it is expected that the way to follow a set of rules formulated by the consensus protocol truthfully for each miners (agents) from mining pools should correspond a preference mapping (e.g., see the profit function discussed in next section) under the framework of so-called the abstract economy model (see Yuan [28] and references wherein), it thus is very important to study the existence (and stability) of Blockchain consensus in the perspective of the existence for equilibria of miners (from mining pools) to follow the so-called "LCR" (see the discussion in Sect. 3 below) while with or without occurring of forks for blockchain of Bitcoin ecosystems.

Based on the idea of the consensus mechanism associated with blockchains, a mining pool game can be regarded as a problem to find a (game) strategy under which some group of miners (called, "honest miners") in the mining pools (for Bitcoins) to apply for "LCR" consensus respect to either non-cooperative or cooperative game's behaviors though maybe some miners may take "selfish mining" or "mining pool with attacking" strategies, this situation by the mixing of both cooperative and non-cooperative game behaviors is indeed the concept for so-called a "Consensus Game".

For a given consensus $\mathbf{G}$, by following Di et al. [10], let $N = \{1, 2, \cdots, n_0\}$, the set of players (or say, agents), and $p = \{N_1, \cdots, N_{k_0}\}$, the partition of N. For each $i \in N$, the mapping $u_i : X \rightrightarrows R$ is a payoff function for i associated with the rules of the consensus $\mathbf{G}$, a normal form of a "Consensus Games" is defined by the form: $CG := (\mathbf{G}, N, p, (X_i, u_i)_{i \in N})$. Thus, a consensus game (in short, CG) is defined by

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

where N is the set of players (miners); $p := \{N_r | r \in R\}$, a partition of N; $X(t)$ is the strategy space of player t; and $X := \prod_{t \in N} X(t), X(S) = \prod_{t \in S} X(t), X(-S) = \prod_{t \notin S} X(t), \forall S \in \mathcal{N}$; and $P(t, \cdot) : X \rightrightarrows X$ is its 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 will use the consensus equilibria for consensus games in Sect. 4.

3 The Consensus Equilibria of Mining Gap Games

In order to discuss the general existence and stability problems related the study from a number of literatures for mining pool games of Bitcoins consensus principle introduced by Nakamoto [20] in Year 2008, we first give the description for the Mining Gap Game.

1) The Concept of General Gap Games for Miners

As discussed by Tsabary and Eyal [25], the repeated search for the blocks becomes a series of independent one-shot competitions, in each only one miner gets the reward but all miners pay expenses. The reason to consider the expected revenues, rather than considering the individual iterations we consider a one-shot game played by the miners. A player's strategy is the choice of start times of all of her rigs: when each rig is turned on. The choice of start times are made a-priori by all players. We define the profit function $P_i(t)$ for the miner i (but the corresponding utility of a player to be her/his expected profit), which is her/his expected income minus her/his expected expenses at a given time t.

Here we recalled that a "Gap Game (GP)" indeed is a set of miners $N := \{1, 2, \cdots, n\}$ with a partition $N_1, N_2, \cdots, N_k$ of N which is a system (consisting of n mining rigs controlled by k players), each N_j is a player, where $j \in K = \{1, 2, \cdots, k\}$: The player j controls the set of rigs with indices R_j.

We use "Block-Interval" to denote the expected block time interval achieved by the protocol, let s_j be the start time of each rig j, and using $\hat{s}_j := \frac{s_j}{Block-Interval}$ to represent the normalized start time.

Throughout of this paper, for the convenience, we assume that once a rig is turned on, the time the rig requires to find a block following an independent exponentially distributed with parameter $\mu(\hat{s})$), and $\hat{s}$ denotes the vector of increasing order n rigs' start times. By assuming all rigs are identical (i.e., with the computing power), thus each mining rig costs "C_{cap}" per time unit for the ownership explained as the capital cost (for example), and "C_{op}" per time unit if it is turned on explained as operation cost.

Without loss of the generality, we assume that the fees reward accumulation over time to use a linear regression to model (see Tsabary and Eyal [25]). Thus, total block reward is modelled as a linear function and denoted by λ_t as the "fees accumulation rate", and λ_0 as the "base reward", we have following notations by defining "Expected-Total-Fees" being the expected total fees accumulating during the expected time to find a block, namely,

$$\text{Expected-Total-Fees} := \text{Block-Interval} \cdot \lambda_t,$$

and also define $\text{EBRR} := \frac{\lambda_0}{\text{Expected-Total-Fees}}$.

By the fact that we assume any miner has only one option either joining or leaving the system, and for the simplicity, we may suppose the cost of C_{op} and C_{cap} are a fixed amount.

Next we discuss the profit function $P_i(t)$ for each $i = 1, 2, \cdots, k$ at time t, which allow us to establish the general existence of consensus equilibria for Gap Games described in next section.

2) The Miner's Profit Function for Mining Gap Games
For a given miner $i = 1, 2, \cdots, k$, assume a single rig $j \in R_i$ with start time s_j, the random variable in time for this rig to find a block is denoted by B_j, then B_j is drawn from the shifted exponential distribution with parameters s_i and $\mu(\hat{(s)})$. For any time t and any player i, the active sets $\text{active}_i(t)$ and $\text{active}(t)$ are defined by $\text{active}_i(t) := \{j \in R_i : s_j \leq t\}$ and, $\text{active}(t) := \cup_{i=1}^{k} R_i$. By defining $\alpha_i(t) := \frac{|\text{active}_i(t)|}{|\text{active}(t)|}$ as the ratio of player i's active rigs out of all the active rigs at time t, then we know that the ratio $\alpha_i(t)$ is continuous in t, and is also the expected factor of player i's portion of the total reward.

We also recall that players in general have two kind of expenses: The first one may be called "Capex", would be explained for the capital cost such as for "owning a rig"; and the second one called "Open", for example, which would be explained for the operation cost such as for "keeping a rig active". By a fact that the Capex for all rigs is controlled by the player (whether turned on or not), it follows for each rig, the Capex it imposes by time t is the quantity: $C_{\text{cap}} \cdot t$.

Then for each miner i, we have the following profit function (e.g., see Tsbary and Eyal [25]):

$$P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t - C_{\text{op}} \cdot \Sigma_{j \in \text{active}_i(t)}(t - s_j) \qquad (1)$$

4 The Consensus Equilibria of Gap Games

Now for a given mining gap game, where $i \in N = \{1, 2, \cdots, n\}$, without loss of generality we may assume that T_i assigned a big enough value in the real line R for time, and we define $X_i := [0, T_i]$ and $X := \prod_{i=1}^{n} X_i$. Then X_i and X are both compact and convex subsets of the real line R and R^n for $i \in N$. Based on the notations of a gap game introduced above, and incorporating with the profit function $P_i(t)$ for $i \in N$ at time t defined in X_i, then it is easy to see that a gap game indeed is a consensus game $CG := (N, K, (X_i, P_i)_{i \in N})$, where $N = \{1, 2, \cdots, n\}$, $K = \{1, 2, \cdots, k\}$ with the $k's$ partition $N_1, \cdots, N_2, \cdots, N_k$ of N as mentioned above.

We now have the following general existence results for consensus equilibria of Gap Games in supporting the stability for Blochchain Ecosystems as applications of general consensus game model established in Sect. 2 above.

Theorem 4.1 (The Consensus Equilibria for Mining Gap Games). For a given general Mining Gap Game (which is indeed a consensus game (in short, CG) if the profit function P_i (defined above) is concave from $[0, T_i] \mapsto R$ for each $i \in N = \{1, 2, \cdots, n\}$, then the Gap Game CG has at least one consensus equilibrium.

Proof. Note that for each $i \in N$, P_i is continuous in t, plus we assume that P_i is concave, thus P_i is continuous and concave. All assumptions of Theorem 2.2 of Di et al. [10] are satisfied, and the conclusion follows and the proof is complete.

Theorem 4 says that for a given consensus and a miner i, if its Profit function P_i is reasonable well (see below for each special case), the consensus game theory

allows us to deal with the general framework for Gap games, thus we are able to claim the existence for honest miners to keep "Mining Longest Chain Rules (LCR)" under a reasonable consensus (e.g., such as Nakamoto [20]) which indeed answer the following question in affirmatively:

"The stability for Blockchain ecosystems is there due to the existence of the honest miners keeping "Mining Longest Chain Rules (LCR)" under a given reasonable consensus, and thus we would claim the following statements:

(1): there always exists honest miners keeping "Mining Longest Chain Rules (LCR)" (though maybe with or without either "Occurring Gap Behavior, or Fork Chain" for blockchains), plus the plausibility of mining-pool attacking; and

(2): Bitcoin ecosystem always works (as the majorities of miners do not collude to break it)."

As applications of Theorem 4, we have the following Remark 4 by assuming the operation cost for the Gap Game's system being zero.

Remark 4.1 (The Mining Pool Game is Stable without Operational Cost).
Indeed, for each miner i, by (1) it follows that the Profit function $P_i(t)$ has the following form:

$$P_i(t) = \alpha_i(t)(\lambda_0 + \lambda \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t.$$

By the fact that the term "$-C_{\text{cap}} \cdot |R_i| \cdot t''$ play a huge negative role for player i's income in terms of profit function P_i at time t, thus one way to reduce the loss for the system (in terms of $P_i(t)$) is to make the ratio $\alpha_i(t)$ as bigger as possible at time t. If assume miner i's computing power is m_i for $i \in N$, then one of the possible best options (strategies) for player i is to run all rigs, and thus $\text{active}_i(t) = m_i$ and so we have $\alpha_i(t) = \frac{m_i}{\Sigma_{j=1}^{k} m_j}$ for any time $t \in [0, T_i]$. Thus the ratio $\alpha_i(t)$ is independent of t and thus concave, therefor the concavity assumption is satisfies, which implies that the system for the gap game without operational cost always has at least one equilibrium with the mining's starting time for miners at zero (thus in the situation without operational cost, the pool games in general has no "Gap" phenomenon as all miners like to start mining with starting time zero (due to the fact without any expense of the operational cost).

When the system of mining pool games has no capital and operational cost, then we have the following general result for mining pool game without the phenomenon of the Gap game behavior to occur.

Theorem 4.2 (The Ming Gap Games without Capital and Operational Cost). For a given general Gap Game with both Capital and Operational Costs are zero, if assume the ratio function $\alpha_i(t)$ is concave in t for each $i \in N = \{1, 2, \cdots, n\}$, then the mining pool game has at least one consensus equilibrium, and no phenomenon of gap game behavior.

Remark 4.2. When both $C_{\text{op}} = 0$ and $C_{\text{cap}}(t) = 0$, by considering the Profit function $P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t)$. The best way to increase the value of $P_i(t)$ is to fully run rigs, thus it is best at the beginning to have $\alpha_i = \frac{m_i}{\Sigma_{j=1}^{k} m_j}$, where m_i

is the mining power for miner $i \in \{1, 2, \cdots, n\}$. In this way, $\alpha_i(t)$ is a constat, thus all assumptions of Theorem 4 are satisfied, which leads the system has at least one equilibrium.

5 The Conclusions

We wish to point out that the study on the existence of Mining Gap games and related stability for mining-pools games by applying consensus games show that the concept of consensus equilibria would play a key role for the development of fundamental theory for consensus economics. Indeed, the concept of consensus games can also be used to establish the general fundamental results in supporting existence and related stability for mining pool games of Bitcoin economics, and the study for data trading of IoTs and related consensus management (see Di et al. [10], Kang et al. [16] and references wherein).

We also note that problems related to smart contracts related Blockchains, bigdata and related topics in fintech have been studied by Chen et al. [4], Chiu and Koeppl [5], Cong and He [6], D′Acunto et al. [7], Dai and Vasarhelyi [8], Di et al. [9]–[10], Foley et al. [13], Fuster et al. [14], Goldstein et al. [15], Narayanan et al. [21] Tang [24], Vallee and Zeng [26], Zhu [30] and references wherein.

The Acknowledgements. All authors thank the professional service and hardwork provided by the organization committee for Blocksys'2020. This research was supported in part by the National Natural Science Foundation of China under the grant numbers U1811462 and 11501349.

References

1. Biais, B., Bisire, C., Bouvard, M., Casamatta, C.: The blockchain folk theorem. Review Finan. Stud. **32**(5), 1662–1715 (2019)
2. 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, 18–20 May 2015
3. 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. 154–167, Vienna, Austria, 24–28 October 2016
4. Chen, M., Wu, Q., Yang, B.: How valuable is FinTech innovation? Rev. Financial Stud. **32**(5), 2062–2106 (2019)
5. Chiu, J., Koeppl, T.: Blockchain-based settlement for asset trading. Rev. Financial Stud. **32**(5), 1716–1753 (2019)
6. Cong, L.W., He, Z.: Blockchain disruption and smart contracts. Rev. Financial Stud. **32**(5), 1754–1797 (2019)
7. D'Acunto, F., Prabhala, N., Rossi, A.G.: The promises and pitfalls of Robo-Advising. Rev. Financial Stud. **32**(5), 1983–2020 (2019)
8. Dai, J., Vasarhelyi, M.A.: Toward blockchain-based accounting and assurance. J. Inf. Syst. **31**, 5–21 (2017)

9. Di, L., Yang, Z., Yuan, G.X.: The consensus games for consensus economics under the framework of blockchain in Fintech. In: Li, D.-F. (ed.) EAGT 2019. CCIS, vol. 1082, pp. 1–26. Springer, Singapore (2019). https://doi.org/10.1007/978-981-15-0657-4_1
10. Di, L., Yuan, G.X., Tu, Z., Zhang, Q., Zhang, X.: The existence of consensus equilibria for data trading under the framework of Internet of Things (IoT) with Blockchain ecosystems. In: Bie, R. Sun, Y. Yu, J. (eds.) 2019 International Conference on Identification, Information and Knowledge in the Internet of Things, Procedia Computer Science, vol. 174, pp. 55–65. Springer, Heidelberg (2020)
11. Eyal, I.: The Miners Dilemma. In: Proceedings of the 36th IEEE Symposium on Security and Privacy, San Jose, California, USA, 18–20 May 2015
12. Eyal, I., Sirer, E.: 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, Heidelberg (2014)
13. Foley, S., Karlsen, J.R., Putnins, T.: Sex, drugs, and Bitcoin: how much illegal activity is financed through Cryptocurrencies? Rev. Financial Stud. **32**(5), 1798–1853 (2019)
14. Fuster, A., Plosser, M., Schnabl, S., Vickery, J.: The role of technology in mortgage lending. Rev. Financial Stud. **32**(5), 1854–1899 (2019)
15. Goldstein, I., Jiang, W., Karolyi, G.: To FinTech and beyond. Rev. Financial Stud. **32**(5), 1647–1661 (2019)
16. Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D.I., Zhao, J.: Toward secure blockchain-enabled internet of vehicles: optimizing consensus management using reputation and contract theory. IEEE Trans. Veh. Technol. **68**(3), 2906–2920 (2019)
17. 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
18. 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)
19. Kwon, Y., Kim, D., Son, Y., Vasserman, E., Kim, Y.: Be selfish and avoid Dilemmas: fork after withholding (FAW) attacks on Bitcoin. In: 2017 ACM CCS 2017, Oct. 30–Nov. 3, 2017, Dallas, TX, USA. 2017 ACM. ISBN 978-1-4503-4946-8/17/10 https://doi.org/10.1145/3133956.3134019
20. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf (2008)
21. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, Princeton (2016)
22. Nyumbayire, C.: The Nakamoto Consensus (https://www.interlogica.it/en/insight-en/nakamoto-consensus). Insight, Interlogica, February 2017
23. 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
24. Tang, H.: Peer-to-Peer lenders versus banks: substitutes or complements? Rev. Financial Stud. **32**(5), 1900–1938 (2019)
25. Tsabary, I., Eyal, I.: The gap game. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security (CCS 2018), pp. 713–728 (2018)

26. Vallee, B., Zeng, Y.: Marketplace lending: a new banking paradigm? Revi. Financial Stud. **32**(5), 1939–1982 (2019)
27. Yang, Z., Yuan, G.X.: Some generalizations of Zhao's theorem: hybrid solutions and weak hybrid solutions for games with nonordered preferences. J. Math. Econ. **84**, 94–100 (2019)
28. Yuan, G.X.: The study of equilibria for abstract economies in topological vector spaces-a unified approach. Nonlinear Anal. TMA **37**, 409–430 (1999)
29. Zhao, J.: The hybrid solutions of an N-person game. Games Econ. Behav. **4**, 145–160 (1992)
30. Zhu, C.: Big data as a governance mechanism. Rev. Financial Stud. **32**(5), 2021–2061 (2019)