Ewerhart, Christian

Working Paper

Finite blockchain games

Working Paper, No. 355

Provided in Cooperation with:
Department of Economics, University of Zurich

Suggested Citation: Ewerhart, Christian (2020) : Finite blockchain games, Working Paper, No. 355, University of Zurich, Department of Economics, Zurich, https://doi.org/10.5167/uzh-188648

This Version is available at:
https://hdl.handle.net/10419/222569

University of Zurich[UZH]

University of Zurich

Department of Economics

Working Paper Series

ISSN 1664-7041 (print)
ISSN 1664-705X (online)

Working Paper No. 355

Finite Blockchain Games

Christian Ewerhart

July 2020

Finite Blockchain Games*

Christian Ewerhart†

July 18, 2020

Abstract This paper studies the dynamic construction of a blockchain by competitive miners. In contrast to the literature, we assume a finite time horizon. It is shown that popular mining strategies such as adherence to conservative mining or to the longest-chain rule constitute pure-strategy Nash equilibria. However, these equilibria are not subgame perfect.

Keywords Blockchain · Proof-of-work · Nash equilibrium · Subgame perfection · Selfish mining

JEL Classification C72 — Noncooperative Games; C73 — Stochastic and Dynamic Games · Evolutionary Games · Repeated Games; D72 — Political Processes: Rent-Seeking, Lobbying, Elections, Legislatures, and Voting Behavior; E42 — Monetary Systems · Standards · Regimes · Government and the Monetary System · Payment Systems

*For useful discussions and comments on the material contained in this paper, I would like to thank participants of the 2020 Summer School "Deep Dive into Blockchain," organized by the UZH Blockchain Center.

†Department of Economics, University of Zurich, Schönberggasse 1, CH-8001 Zurich, Switzerland; phone: +41-79-9384010; e-mail: christian.ewerhart@econ.uzh.ch.

1 Introduction

Since the introduction of the bitcoin consensus protocol by Nakamoto (2009), blockchains have fascinated scholars from a variety of disciplines. The game-theoretic analysis of dynamic consensus protocols has, consequently, gained substantial momentum over the last decade. In an important recent contribution, Biais et al. (2019) proposed modeling the construction of a blockchain as a stochastic game in continuous time with infinite horizon and possibly incomplete information. Their sophisticated framework allows a wealth of interesting conclusions. Here, we will try a related, but more elementary analysis.

Specifically, in this paper, we model the construction of a blockchain as an extensive-form game with finite time horizon T. In each stage, the population of n miners (or mining pools) strives to append the respective next block to the existing blockchain. Thus, starting from the so-called genesis block, the blockchain develops in a stochastic manner. Choosing a parent block at libitum, miners may intentionally try to create forks. A **conservative miner** always appends any new block to the original chain, i.e., to the chain that contains the first child block, thereof the first child block, and so on. We also consider the class of mining strategies that follow the **longest-chain rule**, i.e., that append any new block to one of the longest chains in the blockchain. We confirm that conservative mining and, in fact, any combination of strategies consistent with the longest-chain rule, form Pareto efficient Nash equilibria. However, we also show that, under the assumptions made below, these equilibria are not subgame perfect (Selten,

1965). This contrasts with findings of the recent literature that has found such strategies to be consistent even with the more restrictive concept of Markov perfect equilibrium.

The rest of the paper is organized as follows. Section 2 recalls the formal definition of a blockchain. Section 3 introduces finite blockchain games. We establish the Nash equilibrium property of conservative mining and longest-chain mining in Section 4. Section 5 discusses the lack of subgame perfection. Section 6 concludes.

2 Formal model of the blockchain

Suppose there are $n \geq 2$ miners, collected in a set $N = \{1, ..., n\}$. We will use the following model of a blockchain (cf. Biais et al., 2019).

Definition 1. A **blockchain** $\mathbb{B}$ consists of

(i) a **sequence of blocks** $B = \{b_0, b_1, ..., b_T\}$, where $T \geq 0$;

(ii) a **parent-child relation** $\Leftarrow$ on B;

(iii) an **assignment map** $\iota : B \backslash \{b_0\} \to N$.

Thus, a blockchain $\mathbb{B}$ consists of $(T+1)$ blocks, where T is the time horizon. The block b_0 is referred to as the **genesis block**. Any two blocks may be related to each other by a parent-child relationship. Finally, each block except the genesis block has a miner assigned to it. An example of a blockchain is shown in Figure 1. The numbers close to the circles are the respective miner assignments.

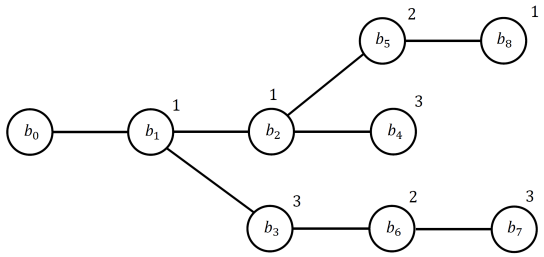

Figure 1. A blockchain

We will impose the following two additional requirements:

(a) each block except the **genesis block** b_0 has precisely one parent, i.e., for any $t' > 0$, there is precisely one t such that $b_t \Leftarrow b_{t'}$

(b) the parent has a lower index than the child, i.e., $b_t \Leftarrow b_{t'}$ implies $t < t'$.

Popular mining strategies are based on the notion of a chain. A **chain** of length $K \geq 1$ in the blockchain $\mathbb{B}$ is a set $C = \{b^{(0)}, \ldots, b^{(K)}\}$ such that $b^{(k-1)} \Leftarrow b^{(k)}$ for $k = 1, \ldots, K$. The **original chain** starts at b_0 and, if there is more than one child to a given parent, continues with the child with the lowest index. E.g., in the example shown in Figure 1, the original chain is $C^{\text{org}} = \{b_0, b_1, b_2, b_4\}$. A **longest chain** is a chain in blockchain $\mathbb{B}$ for which K is maximal. Clearly, any longest chain starts at b_0. If a longest chain is unique, it is referred to as the longest chain in $\mathbb{B}$. In the example shown in Figure 1, there are two longest chains, viz. $C_1 = \{b_0, b_1, b_3, b_6, b_7\}$ and $C_2 = \{b_0, b_1, b_2, b_5, b_8\}$.

3 Finite blockchain games

Suppose the n miners incrementally construct a blockchain $\mathbb{B}$ by interacting over $T \geq 1$ stages. We denote the intermediate blockchains as $\mathbb{B}_0, \mathbb{B}_1, \ldots, \mathbb{B}_T$. At the start of the game, $\mathbb{B}_0$ consists only of the genesis block, so that $B_0 = \{b_0\}$, and both $\Leftarrow_0$ and ι_0 are empty. Next, at any intermediate stage $t \in \{1, 2, \ldots, T\}$, $\mathbb{B}_t$ is constructed from the existing blockchain $\mathbb{B}_{t-1}$ as follows. Each miner $i \in N$ selects a block $\widehat{b}_{t-1}(i) \in B_{t-1}$ from the existing set of blocks B_{t-1}. Then, a fair random draw selects the winning miner $i_t^* \in N$ of stage t.[1] The new block b_t is assigned to i_t^*. Moreover, it is appended as a child to the block $\widehat{b}_{t-1}(i_t^*)$ chosen by the winning miner. Figure 2 illustrates the incremental build-up process of the blockchain.

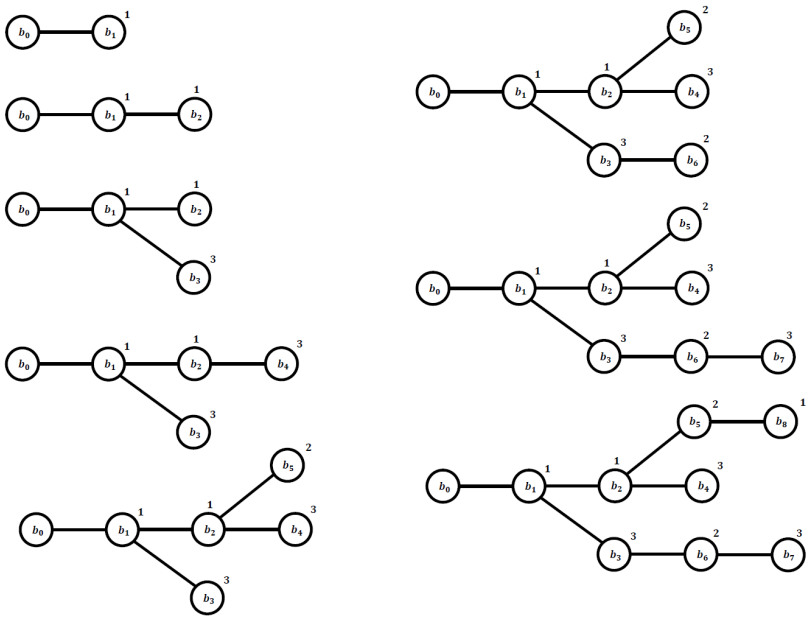

Figure 2. Blockchain construction

[1] The random draw may be understood as a reduced form of the equilibrium in a static model of mining competition such as Dimitri (2017).

Miners' payoffs are determined as follows. After stage T, one of the longest chains C in the blockchain $\mathbb{B}_T$ is drawn with equal probability. Each miner $i \in N$ receives one **token** for each block $b \in C \backslash \{b_0\}$ assigned to him. Miners are risk-neutral and maximize the expected number of tokens they receive.

The stochastic game introduced above will be referred to as a **finite n-miner blockchain game**. Note that, given the possibility of forking and orphan blocks, the game is not constant-sum, i.e., there are gains from coordination.

4 Mining strategies

As the action space of the miners is expanding over time, there is an abundance of pure strategies in the extensive form. Two popular mining strategies, however, are easy to describe. We say that miner i is **conservative** if she always chooses the last block of the original chain. Further, we say that miner i follows the **longest-chain rule** if she always chooses the last block of one of the longest chains. Note that the longest-chain rule is a class of strategies, rather than a single strategy.

We start by studying Nash equilibrium (Nash, 1950). The following result says that conservative mining, and likewise following the longest-chain rule, constitute Nash equilibria in pure strategies.

Proposition 1. *Conservative mining constitutes a symmetric Nash equilibrium. Similarly, any profile of strategies consistent with the longest chain rule constitutes a Nash equilibrium.*

Proof. (Conservative mining) Suppose that all miners $j \in N\backslash\{i\}$ are conservative. We have to show that miner i has no strict incentive to deviate from conservative mining. Assume first that i adheres to the candidate equilibrium strategy. Then, the blockchain develops into a single chain consisting of $(T+1)$ blocks, and miner i receives one token for each block he mined. Assume, instead, that miner i deviates and works, at some stage t, on a block that is not the last block of the original chain. Then, miner i creates a fork when he wins that stage, i.e., with positive probability. As a result, he does not necessarily receive one token for each block that he mined. Thus, miner i potentially lowers, but never raises her payoff. Therefore, a deviation from conservative mining can never lead to a strictly higher expected payoff for miner i. (Longest-chain mining) The proof is entirely analogous and, hence, omitted. □

5 Lack of subgame perfection

In this section, it will be shown using two examples that the considered Nash equilibria need not constitute a subgame-perfect equilibrium (Selten, 1965). We begin with the conservative mining equilibrium.

Example 1. (Conservative mining) Consider a blockchain game with $n = 2$ miners and $T = 3$ stages. Figure 3 shows a possible state of the blockchain $\mathbb{B}_2$, i.e., at the end of stage 2.

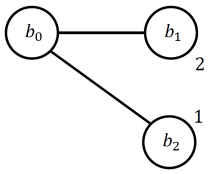

Figure 3. Conservative mining is not subgame-perfect

In this example, miner 1 deviated from the conservative mining strategy in stage 2, mining on b_0 rather than b_1. Thus, we are at a subgame that cannot be reached if all miners followed their candidate equilibrium strategy. Now, at the outset of stage $T = 3$, the last block of the original chain is b_1. However, it is optimal here for miner 1 to work on b_2 because this allows him, with probability $1/2$, to realize a token for the block b_2.

Thus, conservative mining is not subgame-perfect. But neither is the longest-chain rule, as the next example shows.

Example 2. (Longest-chain rule) Consider a blockchain game with $n = 3$ miners and horizon $T = 6$. Figure 4 shows a state of the blockchain $\mathbb{B}_5$, i.e., at the end of stage 5. The fork implies that we are, again, off the equilibrium path. In the final stage $T = 6$, miner $i = 1$ would work on b_3, because this allows him to win three tokens with probability $1/2$ (in case he wins the last stage). In contrast, working on b_5 and thereby following the longest-chain rule would allow him to win one token with probability one (in case he wins the last stage), which is strictly less in expectation. Thus, in the considered subgame, miner 1 has a strict incentive to deviate from the longest-chain rule.

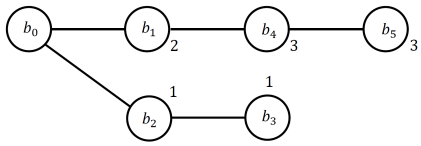

Figure 4. The longest-chain rule is not subgame-perfect.

It should be clear that these examples are not exceptional, but represent a more general problem. In particular, it is not difficult to construct, in both cases, similar examples with an arbitrarily long (but not shorter) time horizon.

Usually, the lack of subgame perfection is associated with the concept of a non-credible threat. This lack of credibility is particularly evident in the case of conservative mining. Indeed, there is intuitively little value in following the original chain once a fork has developed into a much longer chain. As our analysis has shown, the same lack of credibility is also present, but less evident, in the case of the longest-chain rule.

6 Concluding remarks

The framework introduced above may be understood as a finite-horizon version of the infinite-horizon model used by Biais et al. (2019). Our analysis of Examples 1 and 2 above contrasts with their observation that, in a game with infinite horizon, conservative mining constitutes a Markov perfect equilibrium in which players follow the longest-chain rule on the equilibrium path. As any Markov perfect equilibrium is, by definition, subgame-perfect, this is reminiscent of a similar discontinuity in the theory of repeated games. For

instance, the collusive subgame-perfect equilibrium in the infinitely repeated prisoner's dilemma game does not have a counterpart in the finitely repeated version of the model.

However, our finite-horizon model differs also in terms of the assumption on payoffs. Specifically, Biais et al. (2019) assumed that a block's value for a miner increases in the number of miners working on a chain that includes this block. Intuitively, even far off the equilibrium path, a miner with equilibrium beliefs in Biais at al. (2019) will never doubt that all other miners continue to work on the original chain. In contrast, we have assumed that a block's value depends on whether it is contained in one of the longest chains at the end of the game. This clearly makes a difference for the analysis of profitable deviations when the original chain appears orphaned in view to the longest chain.

It may be instructive to compare our findings with Eyal and Sirer's (2018) decision-theoretic analysis of a rational miner interacting with a population of naïve miners. They pointed out that **selfish mining**, i.e., withholding one or several blocks, may dominate naïve mining because it allows the rational miner to bias the mining contest for later blocks in his favor. In our model, all miners are rational, and there is no possibility for mining in secrecy, so the models differ in two important dimensions. Intuitively, however, the lack of subgame perfection of popular mining strategies seems related to the observation that selfish mining strategies may be profitable.

Finally, the analysis raises the question how subgame-perfect equilibria might look like in the class of finite blockchain games. As this question has no straightforward solution, however, it will be left for future work.

References

[1] Biais, B., Bisiere, C., Bouvard, M., Casamatta, C., 2019. The blockchain folk theorem. Review of Financial Studies 32(5), 1662–1715.

[2] Dimitri, N., 2017. Bitcoin mining as a contest. Ledger 2. 31–37.

[3] Eyal, I., Sirer, E.G., 2018. Majority is not enough: bitcoin mining is vulnerable. Communications of the ACM 61.7, 95–102.

[4] Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. https://Bitcoin.org/Bitcoin.pdf.

[5] Nash, J.F., 1950. Equilibrium points in n-person games. Proceedings of the National Academy of Sciences 36(1), 48–49.

[6] Selten, R., 1965. Spieltheoretische Behandlung eines Oligopolmodells mit Nachfrageträgheit: Teil I: Bestimmung des Dynamischen Preisgleichgewichts. Journal of Institutional and Theoretical Economics H.2, 301–324.