

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>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



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.

16 **1 Introduction**

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

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

40 1965). This contrasts with findings of the recent literature that has found
41 such strategies to be consistent even with the more restrictive concept of
42 Markov perfect equilibrium.

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

48 **2 Formal model of the blockchain**

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

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

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

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

54 (iii) an **assignment map** $\iota : B \setminus \{b_0\} \rightarrow N$.

55 Thus, a blockchain \mathbb{B} consists of $(T + 1)$ blocks, where T is the time horizon.

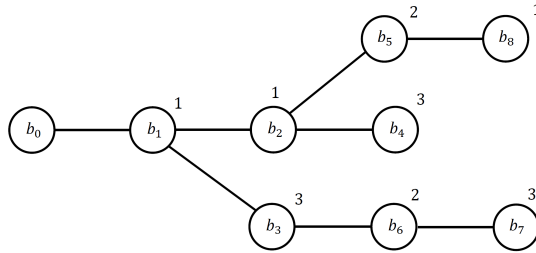
56 The block b_0 is referred to as the **genesis block**. Any two blocks may be

57 related to each other by a parent-child relationship. Finally, each block except

58 the genesis block has a miner assigned to it. An example of a blockchain is

59 shown in Figure 1. The numbers close to the circles are the respective miner

60 assignments.



61

62

Figure 1. A blockchain

63 We will impose the following two additional requirements:

64 (a) each block except the **genesis block** b_0 has precisely one parent, i.e., for

65 any $t' > 0$, there is precisely one t such that $b_t \Leftarrow b_{t'}$

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

67 Popular mining strategies are based on the notion of a chain. A **chain** of

68 length $K \geq 1$ in the blockchain \mathbb{B} is a set $C = \{b^{(0)}, \dots, b^{(K)}\}$ such that

69 $b^{(k-1)} \Leftarrow b^{(k)}$ for $k = 1, \dots, K$. The **original chain** starts at b_0 and, if there

70 is more than one child to a given parent, continues with the child with the

71 lowest index. E.g., in the example shown in Figure 1, the original chain is

72 $C^{\text{org}} = \{b_0, b_1, b_2, b_4\}$. A **longest chain** is a chain in blockchain \mathbb{B} for which

73 K is maximal. Clearly, any longest chain starts at b_0 . If a longest chain is

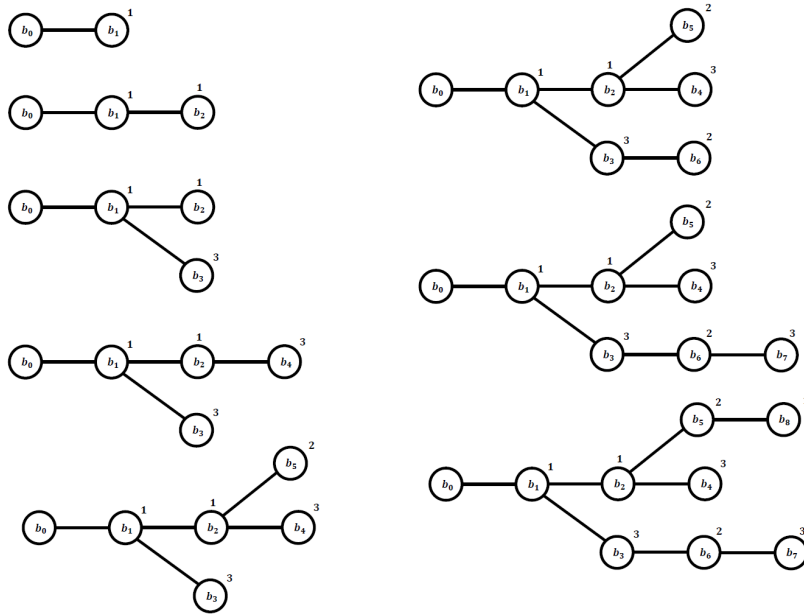
74 unique, it is referred to as the longest chain in \mathbb{B} . In the example shown

75 in Figure 1, there are two longest chains, viz. $C_1 = \{b_0, b_1, b_3, b_6, b_7\}$ and

76 $C_2 = \{b_0, b_1, b_2, b_5, b_8\}$.

77 3 Finite blockchain games

78 Suppose the n miners incrementally construct a blockchain \mathbb{B} by interacting
 79 over $T \geq 1$ stages. We denote the intermediate blockchains as $\mathbb{B}_0, \mathbb{B}_1, \dots, \mathbb{B}_T$.
 80 At the start of the game, \mathbb{B}_0 consists only of the genesis block, so that
 81 $B_0 = \{b_0\}$, and both \Leftarrow_0 and ι_0 are empty. Next, at any intermediate stage
 82 $t \in \{1, 2, \dots, T\}$, \mathbb{B}_t is constructed from the existing blockchain \mathbb{B}_{t-1} as
 83 follows. Each miner $i \in N$ selects a block $\widehat{b}_{t-1}(i) \in B_{t-1}$ from the existing
 84 set of blocks B_{t-1} . Then, a fair random draw selects the winning miner $i_t^* \in N$
 85 of stage t .¹ The new block b_t is assigned to i_t^* . Moreover, it is appended as a
 86 child to the block $\widehat{b}_{t-1}(i_t^*)$ chosen by the winning miner. Figure 2 illustrates
 87 the incremental build-up process of the blockchain.



88

89

Figure 2. Blockchain construction

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

90 Miners' payoffs are determined as follows. After stage T , one of the longest
91 chains C in the blockchain \mathbb{B}_T is drawn with equal probability. Each miner
92 $i \in N$ receives one **token** for each block $b \in C \setminus \{b_0\}$ assigned to him. Miners
93 are risk-neutral and maximize the expected number of tokens they receive.

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

98 4 Mining strategies

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

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

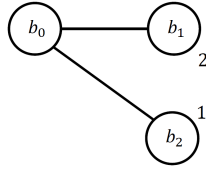
109 **Proposition 1.** *Conservative mining constitutes a symmetric Nash equi-*
110 *librium. Similarly, any profile of strategies consistent with the longest chain*
111 *rule constitutes a Nash equilibrium.*

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

125 **5 Lack of subgame perfection**

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

129 **Example 1. (Conservative mining)** Consider a blockchain game with
 130 $n = 2$ miners and $T = 3$ stages. Figure 3 shows a possible state of the
 131 blockchain \mathbb{B}_2 , i.e., at the end of stage 2.



132

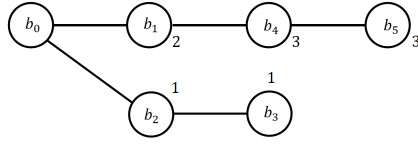
133

Figure 3. Conservative mining is not subgame-perfect

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

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

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



152

153

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

154

155

156

157

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.

158

159

160

161

162

163

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.

164

6 Concluding remarks

165

166

167

168

169

170

171

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

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

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

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

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

197 **References**

- 198 [1] Biais, B., Bisiere, C., Bouvard, M., Casamatta, C., 2019. The blockchain
199 folk theorem. *Review of Financial Studies* 32(5), 1662–1715.
- 200 [2] Dimitri, N., 2017. Bitcoin mining as a contest. *Ledger* 2. 31–37.
- 201 [3] Eyal, I., Sirer, E.G., 2018. Majority is not enough: bitcoin mining is
202 vulnerable. *Communications of the ACM* 61.7, 95–102.
- 203 [4] Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system.
204 <https://Bitcoin.org/Bitcoin.pdf>.
- 205 [5] Nash, J.F., 1950. Equilibrium points in n -person games. *Proceedings of*
206 *the National Academy of Sciences* 36(1), 48–49.
- 207 [6] Selten, R., 1965. Spieltheoretische Behandlung eines Oligopolmodells
208 mit Nachfragerträgeit: Teil I: Bestimmung des Dynamischen Preis-
209 gleichgewichts. *Journal of Institutional and Theoretical Economics* H.2,
210 301–324.