Smart Contracts and Blockchain Technology

Lecture 5. Equilibrium in the blockchain game

Christian Ewerhart

University of Zurich

Fall 2022

Introduction and overview

Last lecture: Blockchain game

This lecture:

- Equilibrium in the blockchain game
- Selfish mining

Equilibrium in the blockchain game (1)

Strategies

Definition. *A strategy s_i for miner i selects a block from any given blockchain.*

The formal definition goes as follows:

- Suppose that $\mathbb{B} = (B, \Lleftarrow, \iota)$ is a (state of the) blockchain,...
- ...with $B = \{b_0, b_1, \ldots, b_T\}$ being the ordered set of blocks,...
- ...then $s_i(\mathbb{B}) \in B$.

Equilibrium in the blockchain game (2)

Some canonical mining strategies

Definition

- Miner i is *conservative* if she always chooses the last block of the original chain.
- Miner i follows the *longest-chain rule* if she always chooses the last block of one of the longest chains.
- Miner i adheres to *naïve mining* if she maximizes the expected number of her tokens under the assumption that the current stage is the last one.

Note: Conservative mining is a well-defined strategy, whereas the longest-chain rule and naïve mining each characterizes a set of strategies.

The **set of players** is $N = \{1, \ldots, n\}$.

Denote the **set of strategies** (identical for all miners) by S.

Miner i's **payoff function** (the expected number of tokens) is denoted by $\Pi_i(s_i; s_{-i}) = \Pi_i(s_1, \ldots, s_n)$, where $s_{-i} = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$.

For any given time horizon $T \geq 0$, this defines a **symmetric noncooperative game**.

Equilibrium in the blockchain game (4)

Nash equilibrium

Definition. An n-tuple of strategies $(s_1^*, \ldots, s_n^*) \in S^n$ is a **Nash equilibrium** if $\Pi_i(s_i^*; s_{-i}^*) \geq \Pi_i(s_i; s_{-i}^*)$ for any $s_i \in S$ and $i \in N$.

Thus, each player's strategy maximizes her expected payoff under the assumption that all the other players adhere to their respective equilibrium strategies.

Definition. A Nash equilibrium $(s_1^*, \ldots, s_n^*)$ is **symmetric** if $s_1^* = \ldots = s_n^*$.

Equilibrium in the blockchain game (5)

Conservative mining

Proposition

Conservative mining constitutes a symmetric Nash equilibrium.

Equilibrium in the blockchain game (6)

Proof of the equilibrium property of conservative mining

We assume that all miners $j \in N \backslash \{i\}$ are conservative.

We have to show that, then, miner i likewise weakly prefers to be conservative.

Equilibrium in the blockchain game (7)

Proof of the equilibrium property of conservative mining (continued)

Suppose first that i is conservative, like all other miners.

Then, the blockchain develops into a single chain consisting of $T + 1$ blocks, and miner i receives one token for each block that she mines.

Equilibrium in the blockchain game (8)

Proof of the equilibrium property of conservative mining (continued)

Suppose, instead, that miner i deviates and works on a block that is not the last block of the original chain.

Then, miner i creates a fork with positive probability.

As a result, she does not necessarily receive one token for each block that she mines.

Equilibrium in the blockchain game (9)

Proof of the equilibrium property of conservative mining (continued)

Thus, by deviating from conservative mining, miner i potentially lowers, but never raises the expected number of tokens.

Therefore, a deviation from conservative mining can never lead to a strictly higher expected payoff for miner i! $\square$

Equilibrium in the blockchain game (10)

Miners using different strategies

Proposition. *Any combination of mining strategies consistent with conservative mining, the longest-chain rule, or naïve mining forms a (not necessarily symmetric) Nash equilibrium.*

Proof. Analogous to the previous proof![1] $\square$

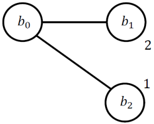
[1] See the problem sets.

Equilibrium in the blockchain game (11)

Subgame perfection

Conservative mining need not constitute a subgame perfect equilibrium.

Example 1. Let $n = 2$ and $T = 3$, and consider the blockchain $\mathbb{B}_2$:



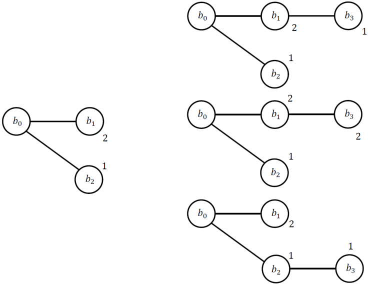
Thus, miner 1 worked on b_2, not following the conservative strategy.

Equilibrium in the blockchain game (12)

Subgame perfection (continued)

At the beginning 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 her, with probability $1/2$, to realize a token for the block b_2.



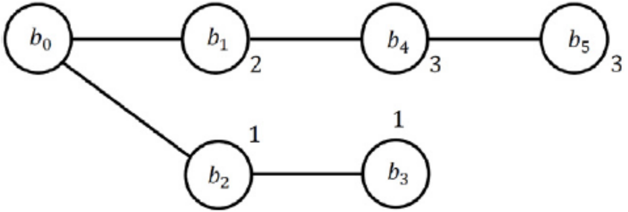
Thus, conservative mining is **not subgame perfect**.

Equilibrium in the blockchain game (13)

Subgame perfection (continued)

Longest-chain mining need not constitute a subgame perfect equilibrium either.

Example 2. Let $n = 3$ and $T = 6$, and consider the blockchain $\mathbb{B}_5$:



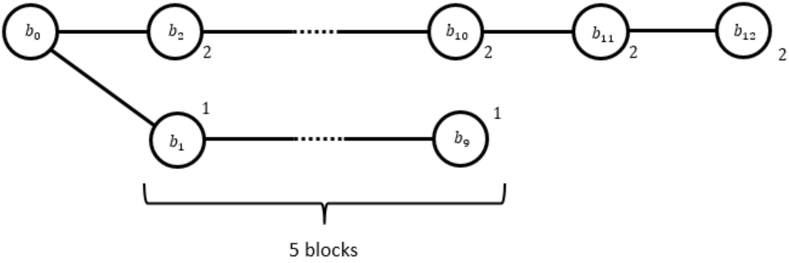
Equilibrium in the blockchain game (14)

Discussion

The model captures the **interplay between two forces**:

- Coordination problem between players
- Problem of vested interests

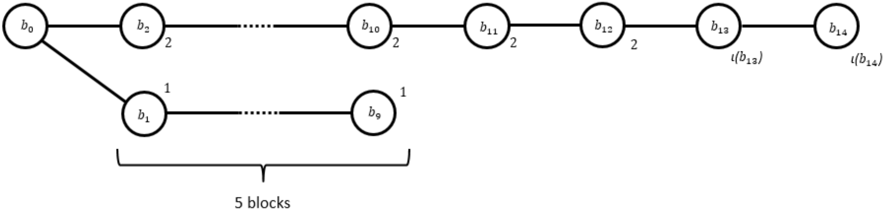
Example 3. Let $n = 2$ and $T = 14$, and consider the following blockchain $\mathbb{B}_{12}$:



Equilibrium in the blockchain game (16)

Naïve mining is not subgame perfect (continued)

If naïve, both miners work on the longest chain in stages $t \in \{13, 14\}$.



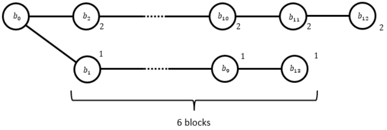
The expected payoff for miner 1 is

$$E[\Pi_1] = \frac{1}{4} \cdot 0 + \frac{1}{2} \cdot 1 + \frac{1}{4} \cdot 2 = 1. \tag{1}$$

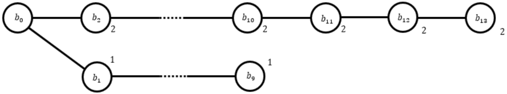
Suppose that miner 1 deviates and decides to work on b_9 in stage $t = 13$, while miner 2 continues to follow the naïve strategy.

Then, there are two scenarios.

Scenario 1 (50%). Miner 1 successfuly mines block b_{13}:



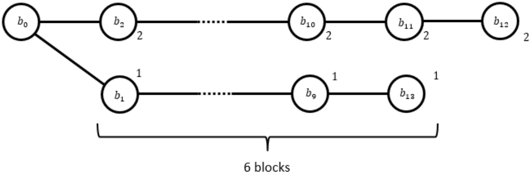
Scenario 2 (50%). Miner 2 successfuly mines block b_{13}:



Equilibrium in the blockchain game (18)

Scenario 1

Suppose that miner 1 wins b_{13}.



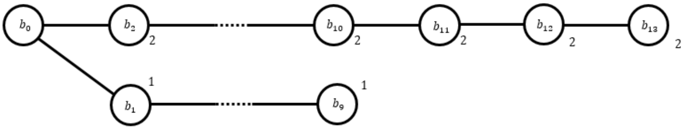
Then, miner 1 works next on b_{13}, while miner 2 works on b_{12}. Miner 1's final payoff is...

- $\Pi_1 = 7$ with probability 25% (if 1 wins and the lower chain is selected),
- $\Pi_1 = 0$ with probability 25% (if 1 wins yet the upper chain is selected), and
- $\Pi_1 = 0$ with probability 50% (if 2 wins).

Equilibrium in the blockchain game (19)

Scenario 2

Suppose that miner 2 wins b_{13}.



Then, there is another stage $t = 14$, and miner 1's payoff is

- $\Pi_1 = 1$ with probability 50% (if 1 wins), and
- $\Pi_1 = 0$ with probability 50% (if 2 wins).

The expected payoff for miner 1 from the deviation is, consequently,

$$E[\Pi_1] = \frac{1}{2} \cdot \frac{1}{4} \cdot 7 + \frac{1}{2} \cdot \frac{1}{2} \cdot 1 = 1.125 > 1. \tag{2}$$

Therefore, naïve mining is not subgame perfect! $\square$

Remark: As of today, a subgame perfect equilibrium is not known for the blockchain game...

Equilibrium in the blockchain game (21)

Selfish mining

It is often argued that the Bitcoin mining protocol is stable provided that **more than half** of the hash power lies with honest miners.

This position ignores the possibility of **selfish mining**:

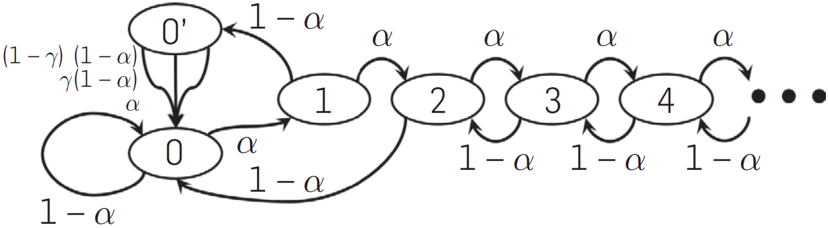
- A pool may strategically delay the broadcast of a successfully mined block.
- The benefit for the pool is that honest miners waste their hash power on side chains that become orphaned soon after.

Relative hash power of selfish pool: $\alpha \in (0, 1)$

Share of honest miners that work on the pool's block $\gamma \in (0, 1)$

State 0': Fork where honest miners and pool each have mined a block

State $a \in \{0, 1, 2, \ldots\}$: The pool's inventory of secret blocks



Equilibrium in the blockchain game (23)

Selfish mining

Nash equilibrium was introduced by Nash (1950). Subgame-perfect equilibrium was conceptualized by Selten (1965).

Eyal and Sirer (2018) show with the help of a Markov chain model that selfish mining can be profitable.

Formal model of the blockchain (24)

References

Eyal, I., Sirer, E.G. (2018), Majority is not enough: Bitcoin mining is vulnerable, *Communications of the ACM* **61**, 95-102.

Nash Jr., John F. (1950), Equilibrium points in *n*-person games, *Proceedings of the National Academy of Sciences* **36**, 48-49.

Selten, R. (1965), Spieltheoretische Behandlung eines Oligopolmodells mit Nachfrageträgheit: Teil I: Bestimmung des dynamischen Preisgleichgewichts, *Zeitschrift für die gesamte Staatswissenschaft/Journal of Institutional and Theoretical Economics*, (Heft 2), 301-324.