Smart Contracts and Blockchain Technology

Lecture 2. The mining game

Christian Ewerhart

University of Zurich

Fall 2022

Introduction and overview

Last lecture: Introduction to the topic

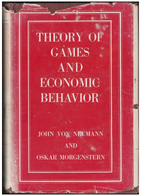
This lecture:

- We plan to have about four lectures on the game-theoretic analysis of
  - mining and
  - consensus formation.
- *Today:* The mining game with homogenous costs

Bitcoin mining as a contest (1)

The game-theoretic approach

Game theory has existed for more than a century by now. Its breakthrough to mainstream economics is often associated with the appearance of the monograph by John von Neumann and Oskar Morgenstern (1945).



Bitcoin mining as a contest (2)

In a **non-cooperative game**, a finite number of players independently and simultaneously choose strategies, which has payoff implications for all of them.

An **equilibrium concept**, such as Nash equilibrium, is applied to make specific predictions.

Examples:

- Cournot model (quantity competition)
- Bertrand model (price competition)

Bitcoin mining as a contest (3)

Non-cooperative games

We will model blockchain mining as a game. As an equilibrium concept, we use the **Cournot-Nash equilibrium**.[1]

This means that each player **correctly anticipates** the strategies chosen by her opponents, and chooses an optimal response.

Optimality means here that each player **maximizes her expected payoffs** given equilibrium expectations.

[1] Nash equilibrium was initially defined for games with finitely many strategies for each player (Nash, 1950, 1951). The Cournot-Nash equilibrium is a generalization in which players may choose strategies from a continuous strategy set (e.g., from an interval).

Bitcoin mining as a contest (4)

Posing a difficult mathematical problem

Suppose that, in regular time intervals, the crypto protocol formulates a new **mathematical problem**, and organizes a competition between anybody interested to participate.

The **reward** for solving the puzzle is denoted by $R > 0$.

In reality, the reward is denominated in crypto (e.g., bitcoin) and may be composed of several components:

- block reward
- transaction fees
- additional rewards (e.g., so-called uncle rewards in Ethereum)

Bitcoin mining as a contest (5)

Miners

Users participating in the competition are called **miners**. Each miner $i \in \{1, 2\}$ decides about her computational power $h_i \geq 0$ (the "hash rate").

The computations are assumed to create a **continuous flow of costs** $C(h_i)$, say within a fixed time interval of length $T > 0$.

We assume that miner i's **cost function** is given by $C(h_i) = c_i \cdot h_i$, where $c_i > 0$ is miner i's constant marginal cost to produce a unit of computational power.

Bitcoin mining as a contest (6)

Discussion of the assumptions on the cost functions

In reality, miners' investment decisions are more complicated for various reasons.

We impose the following **assumptions**:

- Fixed-cost investments (set-up of hardware and software) are depreciated using the straight-line method.
- Costs of computational power stand for operational variable costs (such as energy consumption and maintenance).
- Costs are expressed in bitcoin (rather than in fiat currency).

Bitcoin mining as a contest (7)

The case of homogeneous costs

For simplicity, we start with the case of two **ex-ante identical** miners.

Thus, we assume that:

- $n = 2$, and
- $c_1 = c_2 \equiv c$ (**homogeneous costs**).

Bitcoin mining as a contest (8)

Excursus: Poisson process

The Poisson process is one of the stochastic processes most commonly used in economics (and many other fields).

Key properties:

- Process in continuous time $t \geq 0$
- Counting process (starting at zero, constant almost everywhere, upward jumps by one at random times)
- Memoryless (delay does not make the "discovery" in the next instant more or less likely)

The Poisson process may be considered as the limit of discrete-time search processes as the time interval $\Delta t > 0$ between two consecutive experiments goes to zero, where the probability of a discovery $p \approx \lambda \cdot \Delta t$ is asymptotically linear in Δt.

Bitcoin mining as a contest (9)

The distribution of the time of discovery

Denote by $\widetilde{t}$ the **time of the discovery**. This is a random variable.

Let

$$F(t) = \text{prob}\{\widetilde{t} \leq t\} \tag{1}$$

be the **cumulative distribution function** of the probability law that is followed by $\widetilde{t}$.

The **instantaneous probability** of a discovery is

$$f(t) = \lim_{\Delta t \to 0} \frac{F(t + \Delta t) - F(t)}{\Delta t} = F'(t). \tag{2}$$

Bitcoin mining as a contest (10)

Relationship to the exponential distribution

As the process is memoryless, the instantaneous probability of a discovery, conditional on not having discovered the solution before, is constant:

$$\frac{f(t)}{1 - F(t)} = \lambda, \tag{3}$$

for some $\lambda > 0$.

Solving the ordinary differential equation (3) leads to

$$\begin{aligned} F(t) &= 1 - \exp(-\lambda t), & (4) \\ f(t) &= \lambda \exp(-\lambda t). & (5) \end{aligned}$$

Thus, $\widetilde{t}$ is **exponentially distributed** with parameter λ.

Bitcoin mining as a contest (11)

Expected waiting time

The expected waiting time is defined as

$$E[\tilde{t}] = \int_0^\infty f(t)tdt. \tag{6}$$

Lemma 1. *The* **expected waiting time** *for the discovery is*

$$E[\tilde{t}] = \frac{1}{\lambda}. \tag{7}$$

Bitcoin mining as a contest (12)

Proof of the lemma

We use the **integration-by-parts** formula

$$\int_a^b u'(t)v(t)dt = u(t)v(t)\big|_a^b - \int_a^b u(t)v'(t)dt, \tag{8}$$

with functions

$$\begin{aligned} u(t) &= -\exp(-\lambda t) \quad (9) \\ v(t) &= t. \quad (10) \end{aligned}$$

Then,

$$\int_0^\infty \lambda \exp(-\lambda t) t dt = \int_0^\infty \exp(-\lambda t) dt = \frac{1}{\lambda}, \tag{11}$$

as has been claimed. $\square$

Bitcoin mining as a contest (13)

Waiting time for an individual miner

We assume that solving the puzzle (by try and error) follows a Poisson process with parameter

$$\lambda_i = \frac{h_i}{d}, \tag{12}$$

where d is the **difficulty of the puzzle**.

Let $\widetilde{t}_i$ be miner i's **waiting time** for solving the puzzle. Then, $\widetilde{t}_i$ is an exponentially distributed random variable with parameter λ_i.

Moreover, the **expected waiting time for miner** i is

$$E[\widetilde{t}_i] = \frac{1}{\lambda_i} = \frac{d}{h_i}. \tag{13}$$

Bitcoin mining as a contest (14)

Waiting time for the market

The time of the first solution in the market is $\widetilde{t} = \min(\widetilde{t}_1, \widetilde{t}_2)$.

Let's assume that individual waiting times $\widetilde{t}_1$ and $\widetilde{t}_2$ are stochastically independent.

Then, $\widetilde{t}$ is likewise exponentially distributed because, for any $t \geq 0$,

$$\begin{aligned} \text{prob}\{\widetilde{t} \leq t\} &= 1 - (1 - F_1(t))(1 - F_2(t)) && (14) \\ &= 1 - \exp(-\lambda_1 t) \exp(-\lambda_2 t) && (15) \\ &= 1 - \exp(-(\lambda_1 + \lambda_2) t). && (16) \end{aligned}$$

Bitcoin mining as a contest (15)

Parameters

For the computation above, the parameter of the exponential distribution underlying $E[\widetilde{t}]$ has the parameter $\lambda = h/d$, where $h = h_1 + h_2$.

Moreover, the **expected waiting time for the market** is

$$E[\widetilde{t}] = \frac{1}{\lambda} = \frac{d}{h}. \quad (17)$$

Note: The parameter d is adjusted by the protocol such that $E[\widetilde{t}] = T$ (e.g., in the case of bitcoin, $T = 10$ minutes).

Bitcoin mining as a contest (16)

Two-stage game

Stage 1. Miners simultaneously and independently choose hash rates h_1 and h_2.

Stage 2. The protocol endogenously adjusts the difficulty level d such that

$$\frac{d}{h} = 10 \text{ minutes.} \tag{18}$$

Therefore, **miner i's profit** in any time interval of expected length T starting after the discovery of the previous block is

$$\Pi_i(h_1, h_2) = \begin{cases} R - c \cdot h_i & \text{if } i \text{ is first to solve the puzzle} \\ -c \cdot h_i & \text{if } i \text{ is not first to solve the puzzle.} \end{cases} \tag{19}$$

Bitcoin mining as a contest (17)

Property of the Poisson process

The probability for miner 1 to solve the problem is given as

$$\begin{aligned} p_1 &= \int_0^\infty f_1(t)(1 - F_2(t))dt && (20) \\ &= \int_0^\infty \lambda_1 \exp(-\lambda_1 t) \exp(-\lambda_2 t) dt && (21) \\ &= \lambda_1 \int_0^\infty \exp(-(\lambda_1 + \lambda_2)t)dt && (22) \\ &= \frac{\lambda_1}{\lambda_1 + \lambda_2}. && (23) \end{aligned}$$

Lemma 2. *Miner 1's probability of winning equals*

$$p_1 = \frac{\lambda_1}{\lambda_1 + \lambda_2}. \quad (24)$$

Note that

$$\frac{\lambda_1}{\lambda_1 + \lambda_2} = \frac{h_1/d}{h_1/d + h_2/d} = \frac{h_1}{h_1 + h_2}. \tag{25}$$

Therefore, regardless of d, the ratios

$$p_1 = \frac{h_1}{h_1 + h_2} \tag{26}$$

$$p_2 = \frac{h_2}{h_1 + h_2} \tag{27}$$

represent the probabilities that miners 1 and 2, respectively, will be first in solving the puzzle.

Bitcoin mining as a contest (19)

The miner's profit

Therefore, **miner i's expected profit** is

$$E[\Pi_i] = \frac{h_i}{h_1 + h_2} R - c_i h_i \qquad (i \in \{1, 2\}), \qquad (28)$$

where the ratio is interpreted as zero if $h_1 = h_2 = 0$.

Maximization of miner 1's expected profit with respect to h_1 leads to the **first-order condition**

$$\frac{Rh_2}{(h_1 + h_2)^2} = c. \tag{29}$$

We focus on symmetric equilibria. Thus,

$$h_1 = h_2. \tag{30}$$

Then

$$\frac{R}{4h_1} = c \tag{31}$$

$$\Rightarrow \quad h_1^* = h_2^* = \frac{R}{4c}. \tag{32}$$

hi · c = costs

Bitcoin mining as a contest (21)

Nash equilibrium

Proposition 1. *The unique Nash equilibrium of the mining game with homogeneous costs is given by*

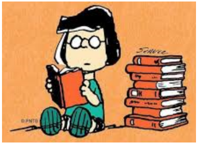
$$h_1^* = h_2^* = \frac{R}{4c}. \tag{33}$$

Comparative statics: The hash power (energy consumption, CO_2 footprint)

- increases strictly in the reward R,
- declines with marginal costs of mining c (i.e., Pigouvian taxation would be desirable).

This lecture is based on the recent **game-theoretic literature on blockchain economics**. This literature studies the **economic incentives and competitive behavior** of blockchain users.

Our model of bitcoin mining follows **Dimitri (2017)**.



Houy (2016) considered a similar model, allowing for endogenous block size.

Bitcoin mining as a contest (23)

References

Dimitri, N. (2017), Bitcoin mining as a contest, *Ledger* **2**, 31-37.

Houy, N. (2016), The Bitcoin mining game, *Ledger* **1**, 53-68.

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

Nash, J. (1951). Non-cooperative games, *Annals of Mathematics* **54**, 286-295.

von Neumann, J., Morgenstern, O. (1945). *Theory of Games and Economic Behavior*.