Smart Contracts and Blockchain Technology

Lecture 3. Extensions of the basic mining model

Christian Ewerhart

University of Zurich

Fall 2022

Introduction and overview

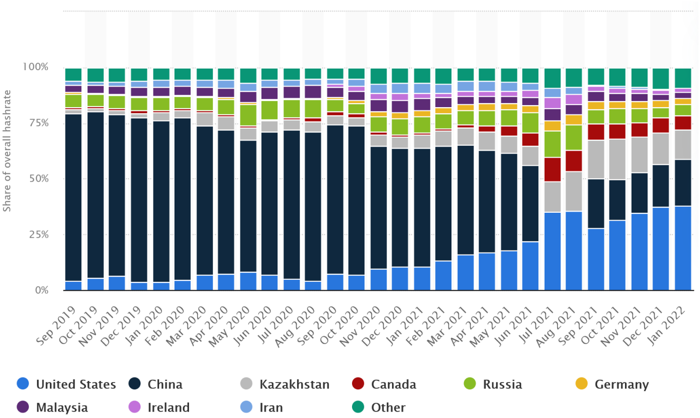
Last lecture: The game played by blockchain miners with homogenous costs.

This lecture: Extensions such as:

- More than two miners and heterogeneous costs
- Intertemporal smoothing (risk aversion)

Extensions of the basic mining model (1)

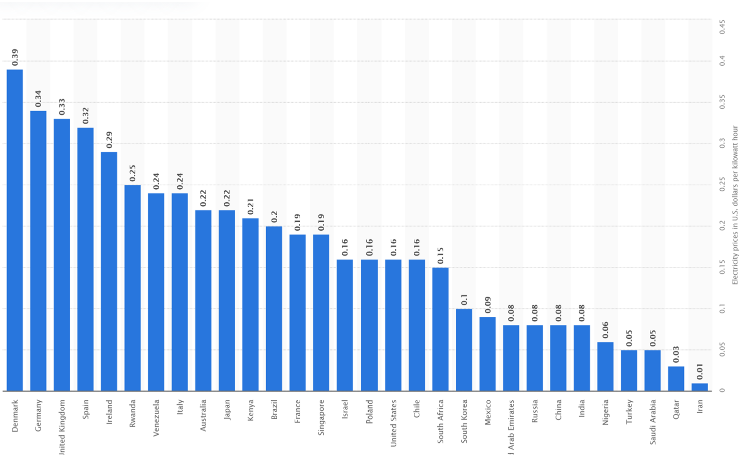
Distribution of Bitcoin mining hashrate 09/2019-01/2022, by country[1]



[1] Source: www.statista.com. In July 2021, a Chinese court ruled that bitcoin mining is harmful to the climate and incompatible with China's carbon neutrality goal (www.climatechangenews.com).

Extensions of the basic mining model (2)

Household electricity prices in 12/2021, by select country[2]



[2] Source: www.statista.com

Extensions of the basic mining model (3)

More than two miners and heterogeneous costs

More than two miners. Rather than just two miners, we allow now for any number $n \geq 2$ of miners. Let $i \in \{1, \ldots, n\}$ denote a generic miner.

Heterogeneous costs. Each miner i chooses a hash rate $h_i \geq 0$, and the computations are assumed to create a continuous flow of costs

$$C_i(h_i) = c_i h_i \tag{1}$$

in a given period of time $T > 0$, where $c_i > 0$ is the constant marginal cost for miner i to produce a unit of computational power.[3]

[3] We assume for simplicity complete information regarding c_i, i.e., miners know each other's marginal costs.

Extensions of the basic mining model (4)

Waiting times for a miner

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

$$\lambda_i = \frac{h_i}{d}. \tag{2}$$

where d is the difficulty of the puzzle.

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

$$E\left[\widetilde{t}_i\right] = \frac{d}{h_i}. \tag{3}$$

Extensions of the basic mining model (5)

Waiting time for the market

The **time at which the new block is mined** and added to the blockchain is

$$\widetilde{t} = \min\{\widetilde{t}_i\}_{i=1,\dots,n}. \tag{4}$$

Let's assume that **individual waiting times** $\{\widetilde{t}_i\}_{i=1}^{n}$ are independent. Then, $\widetilde{t}$ is exponentially distributed with parameter

$$\lambda = \frac{h}{d}, \tag{5}$$

where

$$h = \sum_{i=1}^{n} h_i \tag{6}$$

is the **total hash rate** of the market.

Extensions of the basic mining model (6)

Expected payoffs

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

$$E[\widetilde{t}] = \frac{d}{h}. \tag{7}$$

As before, d is determined endogenously so that $E[\widetilde{t}] = T$.

Miner i's **expected payoff** is given by

$$E[\Pi_i] = \frac{h_i}{\sum_{j=1}^{n} h_j} R - c_i h_i, \tag{8}$$

where the ratio is interpreted as zero if the denominator vanishes.

Extensions of the basic mining model (7)

First-order conditions

Derivation of the expected profit with respect to h_i leads to the **first-order condition**

$$\frac{R(h-h_i)}{h^2} = c_i. \tag{9}$$

Summing over all miners $i = 1, ..., n$, we obtain

$$\begin{aligned} \textstyle\sum_{i=1}^{n} \frac{R(h-h_i)}{h^2} &= C \qquad &(10)\\ &\Rightarrow \frac{R(n-1)}{h} = C &(11)\\ &\Rightarrow h^* = \frac{R(n-1)}{C}, &(12) \end{aligned}$$

where $C = \sum_{i=1}^{n} c_i$.

Extensions of the basic mining model (8)

Nash equilibrium with heterogenous costs

In view of Eq. (9), it follows that **miner *i*'s optimal has rate** is

$$h_i^* = R(n-1)\frac{C-(n-1)c_i}{C^2}. \tag{13}$$

Thus, if miners are ordered such that $c_1 \leq c_2 \leq ... \leq c_n$, then $h_1 \geq h_2 \geq ... \geq h_n$.

Proposition. *Suppose that $C > (n-1)c_n$. Then, the unique Nash equilibrium of the bitcoin mining game, with complete information about the contestants' marginal costs, is the profile of hash rates $(h_1^*, \ldots, h_n^*)$, where h_i^* is given by Eq. (13).*

Extensions of the basic mining model (9)

Arbitrarily many players with homogeneous costs

Suppose that **all miners are ex-ante identical**, i.e.,

$$c_1 = \ldots = c_n \equiv c. \tag{14}$$

Then, $C = nc > (n-1)c$, and miner i's hash rate is given by

$$h_i^* = R(n-1)\frac{C-(n-1)c}{C^2} = \frac{(n-1)R}{n^2 c}. \tag{15}$$

The **total hash rate** in the market is

$$h^* = \frac{(n-1)R}{nc}. \tag{16}$$

In particular, **rent dissipation** $h^* c/R$ goes to 100 percent as $n \to \infty$.

Extensions of the basic mining model (10)

Numerical example

Suppose that $R = 1$, $n = 3$, and

$$\begin{aligned} c_1 &= 0.08 && \text{(e.g., India)} && (17) \\ c_2 &= 0.19 && \text{(e.g., Singapore)} && (18) \\ c_3 &= 0.25 && \text{(e.g., Switzerland)} && (19) \end{aligned}$$

Then, $C = 0.08 + 0.19 + 0.25 = 0.52 > (n-1)0.08$, and

$$\begin{aligned} h_1 &= R(n-1)\frac{C-(n-1)c_1}{C^2} && (20) \\ &= 2 \cdot \frac{0.52 - 2 \cdot 0.08}{0.52^2} && (21) \\ &\simeq 2.663, && (22) \\ h_2 &\simeq 1.036, && (23) \\ h_3 &\simeq 0.148. && (24) \end{aligned}$$

Extensions of the basic mining model (11)

Activity analysis

Definition. We say that miner i is *active* if $h_i > 0$.

Consider a marginally active miner n (with highest cost), and suppose that $n \geq 3$. Then,

$$\begin{aligned}
h_n &= R(n-1)\frac{C-(n-1)c_n}{C^2} = 0 && (25)\\
&\Leftrightarrow \quad C-(n-1)c_n = 0 && (26)\\
&\Leftrightarrow \quad c_n = \frac{C}{n-1} \qquad \Bigg| -\frac{c_n}{n-1} && (27)\\
&\Leftrightarrow \quad c_n \cdot \frac{n-2}{n-1} = \frac{c_1+\ldots+c_{n-1}}{n-1} && (28)\\
&\Leftrightarrow \quad c_n = \left(1+\frac{1}{n-2}\right)\frac{c_1+\ldots+c_{n-1}}{n-1}. && (29)
\end{aligned}$$

Extensions of the basic mining model (12)

Activity analysis (continued)

Observations:

- For miner n to be active, it is necessary and sufficient that her marginal cost c_n is low enough compared to cost average of all more efficient miners, i.e., that

$$c_i \leq c_i^* \equiv \left(1 + \frac{1}{n-2}\right) \frac{c_1 + \ldots + c_{n-1}}{n-1}. \qquad (30)$$

- c_i^* converges to the average cost as $n \to \infty$ (perfect competition).
- However, the block reward R, provided it is positive, does not matter for the decision regarding activity. Instead, R matters for the decision about the optimal hash rate.

Extensions of the basic mining model (13)

In the maturing market, solo miners have entered pools...[4]

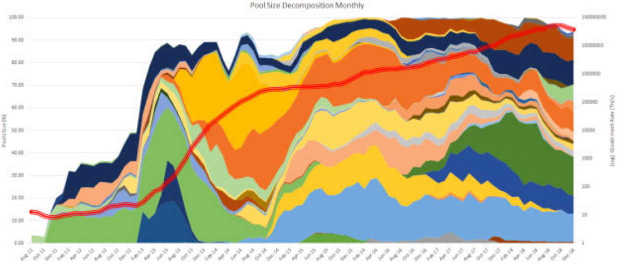


Figure 1
The evolution of Bitcoin mining
This graph plots (1) the growth of aggregate hash rates (right-hand-side vertical axis, in log scale) starting from June 2011 to December 2018 and (2) the size evolution of all Bitcoin mining pools (left-hand-side vertical axis) over this period, with pool size measured by each pool's hash rates as a fraction of global hash rates. Colors represent different pools, and white spaces represent solo mining. Over time, mining pools have increasingly taken over Bitcoin mining, but no pool ever seems to dominate the mining industry for long. The pool hash rates data come from https://data.bitcoinity.org/bitcoin/hashrate/6m?c=m&g=15&t=a and https://btc.com/, with details given in Section 4.

[4] Source: Cong, He, and Li (2021).

Extensions of the basic mining model (14)

Heuristics of solo mining

Within 30 days, the bitcoin blockchain with $T = 10$ min produces a total number of

$$\frac{60 \text{ min}}{T} \times 24 \times 30 = 4320 \tag{31}$$

new blocks.

Let

$$p_i = \frac{h_i}{\sum_{j=1}^{n} h_j} \tag{32}$$

denote miner i's probability of winning a new block within T.

Extensions of the basic mining model (15)

Heuristics of solo mining (continued)

Then, miner *i*'s probability of winning at least one block in 30 days is

$$\widehat{p}_i = 1 - (1 - p_i)^{4320}. \tag{33}$$

E.g., if miner *i* is one of 100000 ex-ante identical miners, then

$$p_i = 0.001\% \tag{34}$$

$$\Rightarrow \widehat{p}_i \simeq 4.2\%. \tag{35}$$

Thus as the market grows, the probability of successfully mining a block within a whole month becomes too small to be the basis of a regular business, i.e., **solo mining** becomes a prohibitively risky strategy for small miners.

Extensions of the basic mining model (16)

The impact of risk aversion

Suppose that miner i exhibits **constant absolute risk aversion (CARA)**, i.e., her utility function is given as

$$u_i(x) = -\exp(-\alpha x),$$

for some $\alpha > 0$. The parameter α is known as the Arrow-Pratt coefficient of absolute risk aversion.

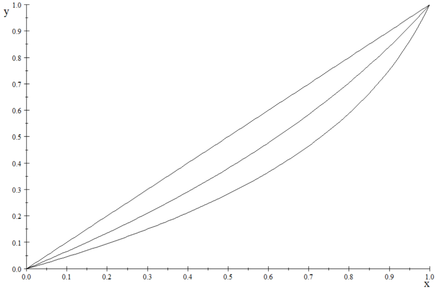
Then, the **certainty equivalent** of the uncertain revenue is given as

$$\begin{aligned} \mathrm{CE}(p_i, R, \alpha) &= u_i^{-1}(p_i u_i(R) + (1-p_i)u_i(0)) && (36) \\ &= -\frac{1}{\alpha} \ln\left(\frac{p_i}{\exp(\alpha R)} + 1 - p_i\right) && (37) \end{aligned}$$

Extensions of the basic mining model (17)

Certainty equivalent

The figure below illustrates the function $\mathrm{CE}(p_i, R, \alpha)$ for $\alpha \in \{0, 1, 2\}$ and $R = 1$.[5]



Observation: Risk aversion strictly lowers the incentive for all miners (with less than half of the market's hash power).

[5] The x-axis shows p_i, the y-axis shows $\mathrm{CE}(p_i, R, \alpha)$.

Extensions of the basic mining model (18)

Proof of the observation

$$\frac{\partial \mathrm{CE}(p_i, R, \alpha)}{\partial p_i} = \frac{\partial}{\partial p_i}\left(-\frac{1}{\alpha}\ln\left(\frac{p_i}{\exp(\alpha R)} + 1 - p_i\right)\right) \quad (38)$$

$$= \frac{e^{\alpha R} - 1}{\alpha\left(p_i + e^{\alpha R} - p_i e^{\alpha R}\right)}. \quad (39)$$

Now,

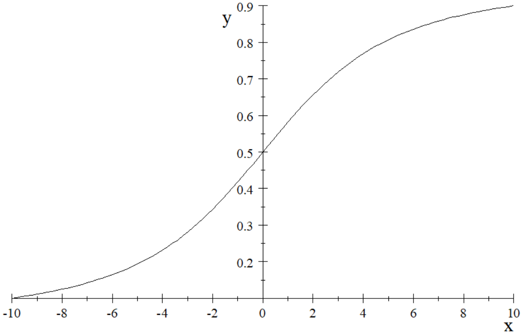
$$\frac{e^{\alpha R} - 1}{\alpha\left(e^{\alpha R} - p_i(e^{\alpha R} - 1)\right)} \gtreqless R \quad (40)$$

$$\Leftrightarrow \quad p_i \lesseqgtr p_i^*(\alpha) = \underbrace{\frac{1}{1 - \exp(-\alpha R)} - \frac{1}{\alpha R}}_{>\frac{1}{2}} \quad (41)$$

Extensions of the basic mining model (19)

Illustration

$$x > 0 \Rightarrow \frac{1}{1 - \exp(-x)} - \frac{1}{x} > \frac{1}{2}$$



Extensions of the basic mining model (20)

Equilibrium analysis

With risk aversion, miner *i*'s **expected payoff** is given by

$$E[u_i(\Pi_i)] = \mathrm{CE}(p_i, R, \alpha) - ch_i, \tag{42}$$

where $p_i = h_i / \sum_{j=1}^{n} h_j$.

Extensions of the basic mining model (21)

Equilibrium analysis (continued)

The first-order conditions reads

$$\frac{h - h_i}{h^2} \cdot \frac{\partial \mathrm{CE}(p_i, R, \alpha)}{\partial p_i} = c. \tag{43}$$

In a symmetric equilibrium, $h = nh_i$ and $p_i = 1/n$. Therefore, the market hash rate is

$$h^* = \frac{n-1}{nc} \cdot \underbrace{\frac{\partial \mathrm{CE}(1/n, R, \alpha)}{\partial p_i}}_{<R}. \tag{44}$$

Thus, compared to the symmetric reference model with $n \geq 2$ risk-neutral miners, the introduction of risk aversion strictly lowers the equilibrium market hash rate.

Extensions of the basic mining model (22)

A simple model of mining pools

Suppose that there are **two pool managers** that offer (almost) perfect risk diversification for a large population of small miners.

Each pool $m \in \{1, 2\}$ charges a proportional fee of $f_m \in [0, 1]$. Solo mining is assumed to be prohibitively risky.

Denote by H_m the hash power attracted by pool m.[6] We assume that miners can freely allocate their hash power across mining pools.

[6] Thus, we assume (for simplicity) that pool managers does not do any mining themselves.

Extensions of the basic mining model (23)

Endogenously attracted hash power

Then, the marginal payoff of a miner by allocating a small amount of additional hash power to pool *m* is

$$\begin{aligned} \frac{H_2}{(H_1 + H_2)^2}(1 - f_1)R &= c && (45) \\ \frac{H_1}{(H_1 + H_2)^2}(1 - f_2)R &= c. && (46) \end{aligned}$$

Thus

$$H_2(1 - f_1) = H_1(1 - f_2). \tag{47}$$

Extensions of the basic mining model (24)

The pool's problem

Pool 1 has the following problem

$$\begin{aligned} &\max_{f_1 \in [0,1]} && \tfrac{H_1}{H_1+H_2} f_1 R \\ &\text{s.t.} && \\ &H_2(1-f_1) = H_1(1-f_2) && \end{aligned} \tag{48}$$

Note that

$$\frac{H_1}{H_1+H_2} = \frac{1}{1+H_2/H_1} \tag{49}$$

$$= \frac{1}{1+\frac{1-f_2}{1-f_1}} \tag{50}$$

$$= \frac{1-f_1}{2-f_1-f_2}. \tag{51}$$

Extensions of the basic mining model (25)

The pool's problem (continued)

Pool 1's problem reduces to has the following problem

$$\begin{aligned} & \max_{f_1 \in [0,1]} \quad \tfrac{(1-f_1)}{2-f_1-f_2} f_1 R && (52) \\ = \quad & \max_{e_1 \in [0,1]} \quad \tfrac{e_1}{e_1+e_2}(1-e_1)R && (53) \end{aligned}$$

The first-order condition reads

$$\frac{e_2}{(e_1+e_2)^2}(1-e_1) - \frac{e_1}{e_1+e_2} = 0. \qquad (54)$$

Extensions of the basic mining model (26)

Equilibrium derivation

Hence,

$$\frac{e_2(1-e_1)}{e_1+e_2} = e_1. \tag{55}$$

In a symmetric equilibrium, $e_1 = e_2 \equiv e$, so that

$$\begin{aligned} e &= \frac{1}{3} && (56) \\ &\Rightarrow \quad f_1^* = f_2^* = \frac{2}{3}. && (57) \end{aligned}$$

Extensions of the basic mining model (27)

Equilibrium has rate

Thus,

$$\begin{aligned} H^* &= H_1^* + H_2^* && (58) \\ &= \frac{R}{6c}. && (59) \end{aligned}$$

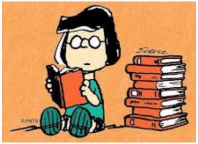
The purely **mining-related rent dissipation** is $\frac{1}{6} = 16.6$ percent, which is surprisingly low (because it is often claimed that pooling leads to excessive rent dissipation).

Extensions of the basic mining model (28)

Bibiographic notes

Cong et al. (2020) argue that pools escalate the arms race between bitcoin miners, leading to even more energy consumption.

Assuming exogenous difficulty, Ma et al. (2018) show that, under free entry, energy consumption is independent of the difficulty of the miner's puzzle.



Extensions of the basic mining model (29)

References

Cong, L.W., He, Z., Li, J. (2021), Decentralized mining in centralized pools, *Review of Financial Studies* **34**, 1191–1235.

Ma, J., Gans, J.S., Tourky, R. (2018), Market structure in bitcoin mining, *NBER Working Paper* 24242.