Pitfalls of Bitcoin’s Proof-of-Work: R&D Arms Race and Mining Centralization

Agostino Capponi

Department of Industrial Engineering and Operations Research
Columbia University
ac3827@columbia.edu

Joint with Humoud Alsabah (Columbia)

Fintech and Machine Learning
August 6, 2019
Introduction
• Bitcoin has experienced rapid growth in value since its deployment in January 2009.

• As of July 2019, Bitcoin’s market capitalization exceeds $180 billions.

• The most successful of more than 1,500 cryptocurrencies used today.
Catalini and Gans (2016); Cong and He (2019); Malinova and Park (2017); Yermack (2017); Abadi and Brunnermeier (2018): Blockchain as a general purpose technology, and its use in market design.

Athey et al. (2016); Pagnotta and Buraschi (2018); Biais et al. (2018): Bitcoin valuation and pricing.

Chiu and Koeppel (2017); Saleh (2018); Hinzen et al. (2019): Optimal design of cryptocurrencies and sustainable alternatives.

Huberman et al. (2018); Easley et al. (2019); Biais et al. (2019): Study of Bitcoin operations.
Bitcoin Mechanism

- Works through Blockchain, a decentralized digital ledger in which transactions are publicly recorded.
- Relies on a network of nodes to verify, update and store transactions.
- Nodes are incentivized to undertake these tasks through a process called mining.
- Miners (i.e., nodes) compete to solve a computationally costly problem known as *proof-of-work*.
- The winner of the mining process has the right to update the record.
  - Rewarded with newly minted coins and keeps transaction fees paid by bitcoin holders.
Nakamoto (2008) envisioned a decentralized payment system, where mining can be performed by anybody.

However, the rapid increase in bitcoin price induced firms to invest in mining hardware.

- Probability of successfully mining blocks increase.

Mining operations become increasingly vertically integrated.

- Single firms design mining chips, maintain hardware, and operate data centers.
- Bitmain is opening mining farms in Canada and Switzerland, in addition to currently operated farms in China (Cheng (2018)).
- Bitfury is launching a network of Bitcoin mining operations in Paraguay, in addition to those operated in Canada, Norway, Iceland, and Georgia (Khatri (2019)).
This paper

- Does Bitcoin’s proof-of-work still enable and support a decentralized payment system?
  - Critical to assess Bitcoin’s ability to maintain its dominant position among cryptocurrencies.

- We show that proof-of-work
  - Drives the mining industry towards centralization.
  - Leads to a research and development (R&D) arms race in which all firms are worse off.
Problem formulation

- Industry of \( N \geq 2 \) firms and a two-periods timeline.
- **Period 1:**
  - Each firm \( i \) chooses its level of R&D \( x_i \).
  - R&D cost function is assumed to be quadratic: \( \gamma x_i^2 / 2 \).
- **Period 2:**
  - Each firm \( i \) chooses the hash rate \( h_i \) used for mining.
  - The hash cost function \( C_i(h_i, x_i) \) is given by
    \[
    C_i(h_i, x_i) = (\alpha - x_i) h_i.
    \]
Revenue Function

- Rewards allocated to firms depend on the distribution of hash rates \( h = (h_1, \ldots, h_N) \).
- Firm \( i \)'s share of the reward given by

\[
R_i(h) = \frac{h_i R}{H}
\]

where \( H := \sum_{j=1}^{N} h_j \), and \( R \) is the total reward obtained in the second period.

- Captures the two most critical properties of proof-of-work:
  1. Reward obtained by miners proportional to the fraction of computational power they own.
  2. Total coins mined in a period is independent of computational power exerted by all miners.

- The objective of each firm is to maximize its individual second-stage mining profits net of its first-stage R&D expenditure:

\[
\pi_i(h; x_i) = R_i(h) - C_i(h_i, x_i) - \gamma x_i^2 / 2
\]
Solution Methodology

- Solve for the subgame perfect equilibrium (SPE) using backward induction.
  1. Solve the second-stage game for a given R&D profile $x$.
  2. Solve the first-stage game to find the equilibrium R&D levels.
Results
Mining Stage: Characterizing Equilibrium Hash Profile

- Given a R&D profile $\mathbf{x} = (x_1, \ldots, x_N)$, denote by

  $$c_i(x_i) := \frac{\partial C_i(h_i, x_i)}{\partial h_i} = \alpha - x_i$$

  the per-unit hash cost of firm $i$.

- Without loss of generality, we label firms so that

  $$c_1(x_1) \leq c_2(x_2) \leq \cdots \leq c_N(x_N).$$

**Lemma**

At any equilibrium hash rate profile,

1. There are at least two active firms.

2. The set of active firms is of the form $\{1, 2, \ldots, n\}$ for some integer $n \in \{2, 3, \ldots, N\}$. 
Mining Stage: Characterizing Equilibrium Hash Profile

- Constructive procedure for the equilibrium hash profile:
  - Start with the $n$-firm candidate equilibrium and check whether firm $n + 1$, can join and make positive profits.
  - If so, include firm $n + 1$ and repeat.

**Proposition**

For any R&D profile $\mathbf{x}$, there exists a unique equilibrium hash profile $\mathbf{h}(\mathbf{x}) := (h^*_1, h^*_2, \ldots, h^*_N)$.

- If $n$ firms are active in the unique equilibrium, then the equilibrium hash rate is given by

$$h^*_i = \frac{R(n - 1)(c^{(n)} - (n - 1)c_i)}{(c^{(n)})^2}, \quad i = 1, \ldots, n.$$  

where $c^{(n)} := \sum_{j=1}^{n} c_j$ is the sum of the active firms’ hash costs.
Hash rate proportional to Bitcoin price?

**Figure:** Plot of actual aggregate hash rate (left axis) and bitcoin exchange prices (right axis) vs. time.

- **Time period:** July 19 2018-July 18 2019.
Corollary

Let $n$ be the number of active miners, a firm will not actively compete in mining if and only if its per-unit hash rate cost is larger than the average per-unit cost of active miners by at least $\frac{100}{n-1}$%.

- For example,
  - When $n = 10$, firms with per-unit hash cost greater than the average by 11.1% will not be able to compete.
  - When $n = 20$, firms with per-unit hash cost greater than the average by 5.3% will not be able to compete.

→ Investing in R&D supports competitiveness in mining.

- Supports statements released by Tai, the chairman of Hut 8 Mining Corporation,
  - “Smaller miners will drop out, and only five to ten of the largest will survive and be profitable.”
  - Major mining companies such as Bitmain and Bitfury design and make their own mining chips, and hence have lower hashing cost.
Proposition

Suppose $\gamma \geq \gamma^*$. Then there exists a unique symmetric SPE. It satisfies:

- An increase in the mining reward $R$ increases the equilibrium R&D level and hash rate of any firm.
- All firms invest a strictly positive amount in R&D.

Consistent with empirical evidence:

- Mining equipment technological advancements in response to rise in Bitcoin price.
- CPU $\rightarrow$ GPU $\rightarrow$ FPGA $\rightarrow$ ASIC.
Cooperation between Firms

- Does investing in research benefit firms?
  - Investment is costly, but reduces second period mining costs.
- **Benchmark:** firms cooperate on R&D in Period 1, but compete over exerted hash rate in Period 2.
  - In Period 1, firms choose the R&D profile $\mathbf{x}$ to maximize the total profits $\Pi(\mathbf{x}) := \sum_{j}^{N} \pi_j(\mathbf{x})$.
- Unique symmetric outcome for cooperative R&D:
  \[ \mathbf{x}^C = 0 \]
- Firms exert an excessive amount of R&D in the non-cooperative case.
  - *Arms race* ensues.
Combined-profits Externality

- The cooperative solution implies that the optimal level of R&D by each firm maximizes the aggregate profit, i.e. each firm $i$ solves

$$\max_{x_i} \Pi(x).$$

- Note:

$$\frac{\partial \Pi}{\partial x_i} = \frac{\partial \pi_i}{\partial x_i} + \sum_{j \neq i} \frac{\partial \pi_j}{\partial x_i}.$$  

where the sum $\sum_{j \neq i} \frac{\partial \pi_j}{\partial x_i}$ is the *combined-profits externality* conferred by firm $i$’s R&D expenditure on profits of all other firms.

- This negative externality dominates firm $i$’s gains from its research expenditure.
Spillovers

- How does R&D spillovers impact outcome?
- R&D spillovers occur when firms have difficulties protecting their intellectual property.
- Channels for technology to spread:
  - Movement of personnel from one firm to the next.
  - Informal communication networks among engineers.
  - Input supplier.
- To account for spillovers, we use the generalized cost function given by
  \[ C_i(h_i, x; \beta) = (\alpha - x_i - \beta \sum_{j \neq i} x_j) h_i, \]
- \(0 \leq \beta \leq 1\) is the spillover parameter.
Impact of Spillovers

Proposition

(i) An increase in $\beta$ decreases the R&D level of any firm and improves their profit.

(ii) The total hash rate $H^{NC} := \sum_i^N h_i(x^{NC})$ is increasing in $\beta$ when $\beta < \bar{\beta} = \frac{N-2}{2(N-1)}$ and decreasing otherwise.

- Absence of spillovers induces the highest R&D.
- But, does it result in the maximal level of hash rate $H^{NC}$ deployed? **NO!**
- Aggregate hash rate proportional to the effective R&D

$$X^{NC} := x^{NC}(1 + \beta(N - 1)).$$

- Spillovers have a nonlinear impact on the effective R&D.
  - Firms benefit from rivals’ R&D besides their own.
  - Free-riding disincentivizes firms from investing in R&D.
Recall that the cost function $C_i(h_i, x_i)$ is given by

$$C_i(h_i, x_i) = (\alpha - x_i) h_i,$$

where $\alpha$ is the marginal hash cost prior to any R&D.

Extension: Assume firms have heterogeneous initial marginal hash costs $\alpha_i$

Arrange marginal costs according to increasing $\alpha_i$, that is,

$$\alpha_1 < \alpha_2 < \cdots < \alpha_N$$

How would this heterogeneity influence R&D investments?
Tendency towards Centralization

Figure: The figure plots firms’ individual R&D levels when \( N = 10, \ p = $6,500 \).
- Firms with lower marginal hash costs have a greater incentive to invest in research.
  - The marginal benefits of R&D are higher for firms with lower marginal hash costs
- Matthew Effect → tendency towards centralization.
Firms fail to capture the surplus created by their research (i.e., arms race ensues)
- More R&D leads to a more aggressive second stage mining game.

A remedy to R&D arms race is promoting spillovers: not only reduces wasteful R&D duplication and improves firms’ profits, but may also increases hash rate.
- Higher aggregate hash rate benefits Bitcoin users.
- Implications for policies governing patents and non-compete agreements.

Proof-of-work leads Bitcoin mining towards centralization.
- Against the fundamental reason behind cryptocurrencies.
Thanks for your attention!
Deriving the Revenue Function

- When a hashing power $h_i$ is exerted, the waiting time of miner $i$ to solve the computational task $\tau_i$ is exponentially distributed with parameter $\frac{h_i}{D}$ where $D$ is the difficulty level.
  - The waiting time until the first miner solves the computational task $\tau = \min(\tau_1, \ldots, \tau_N)$ is exponentially distributed with parameter $\frac{H}{D}$.
  - The probability that miner $i$ is the first to solve the computational problem is $\frac{h_i}{H}$.

- The parameter $D$ is adjusted by the Bitcoin system to keep the expected time between the solutions of the computational problem fixed.
  - Total bitcoin rewards in the second stage game does not depend on miners’ total computational power.
  - After accounting for the bitcoin exchange rate, the total reward is denoted by $R$.

- Thus, if miner $i$ exerts a hash rate $h_i$, he is expected to update a fraction $\frac{h_i}{H}$ of the blocks in the second stage mining game, giving him an expected revenue $R_i(h) = \frac{h_i R}{H}$. 
Collusion

- **Alternative benchmark:** Firms cooperate in both stages of the game.
- Optimal to set $h_i = \epsilon > 0$ to the minimum amount required to mine successfully, and $x_i = \frac{\epsilon}{N\gamma} \approx 0$.
- Firms capture all the reward from Bitcoin, while incurring negligible mining costs.
- However, this does not reflect reality, because it removes any barrier to entry.
  - Miners with high electricity costs and inefficient hardware would still want to participate.
Collusion

Assumption

There exists an infinite number of miners with a marginal cost $c^e \geq \frac{N\alpha}{N-1}$.

- Ensures small miners are not able to compete when mining firms do not cooperate.
- Firms agree to exert the minimum hash rate $H^M$ to keep small miners out.
- In the first stage, when $x_i = x^M$ for $i = 1, 2, \ldots, N$, the profit maximizing monopolistic R&D level is given by

$$x^M = \frac{H^M}{N\gamma} > 0.$$  

- In the absence of PoW protocol, firms invest in R&D.
  - i.e. aggressive competition induced by proof-of-work protocol prevents firms from capturing their research surplus.
Comparing Outcomes

Proposition

When firms do not cooperate (NC), cooperate only on R&D (C) and cooperate both on R&D and hash rate (M),

(i) The total hash rate satisfy $H^{NC} \geq H^C \geq H^M$.
(ii) The R&D levels satisfy $x^{NC} > x^M > x^C$.

→ When firms fully cooperate, less competition in the mining stage allows them to capture a higher share of the surplus created by their research, hence incentivizing more R&D expenditures.
Recent trends in Bitcoin: Rise of Aggregate Hash Rate Deployed

**Figure:** Plot of actual aggregate hash rate (left axis) and bitcoin exchange prices (right axis) vs. time.

- Hash rate does not seem proportional to Bitcoin price.
- Apr-Oct 2018: Total hash rate deployed by miners continued to rise despite decrease in Bitcoin price.
- Contradicts model prediction?
Recent trends in Bitcoin: Rise of Aggregate Hash Rate Deployed

Figure: Equilibrium aggregate hash rate as a function of bitcoin’s price.

- **Conservative model prediction:**
  - Five firms.
  - Mining equipment energy efficiency is 10.2 GH/J (Antminer S9).
  - Miscellaneous variable costs are 25% of hashing costs.

- Bitcoin mining was at a transient state till Dec. 2018.
References


