A Mean Field Game Approach to Bitcoin Mining

Louis Bertucci

Institut Louis Bachelier

Collège de France, Seminar
Equations aux dérivées partielles et applications

December 10, 2021

Based on work with Pierre-Louis Lions[1], Jean-Michel Lasry[2] and Charles Bertucci[3]

- Mean Field Game Approach to Bitcoin Mining
  Working paper, 2020
- Economic Modelling of the Bitcoin Mining Industry
  Working paper, 2021

[1]College de France
[2]University of Paris-Dauphine
[3]CMAP, Ecole Polytechnique

1 Introduction

Blockchain 101 (in 5')

A Blockchain is a distributed database of which the sequence of recorded events is determined by a distributed consensus protocol

Consensus in Computer Science

- In the distributed systems literature, consensus is hard :
  - Lamport Shostak and Pease (1982) : In synchronous setting, impossibility results if $> \frac{1}{3}$ of Byzantine processes
  - Fischer, Lynch and Paterson (1985) : in asynchronous setting, impossibility result with 1 faulty process

Economic Incentives

- In the distributed system literature, "impossible" = "impossible to guarantee"
- The brilliant idea of Satoshi Nakamoto (Bitcoin) is that when considering economic and rational agents consensus becomes achievable in equilibrium

Creating the Chain of Blocks

Hash Functions - Ex: SHA-256

- Variable length input $\longmapsto$ fixed length output (256 bits)
- $sha256(\text{'hello, world'}) = 0x09ca7e4e...08360d5b$
- $sha256(\text{'hello, world!'}) = 0x68e656b2...f368f728$
- Output distribution is close to uniform

Proof-of-Work - used on Bitcoin

- Miners compete to brute force the solution of a hash-based puzzle
- The winning miner gets to propose the next block of data
- Brute force creates randomness on the selected miner
- But a miner with share $k\%$ of hashrate can expect to find $k\%$ of the blocks
- The difficulty of this puzzle adjusts with the hashrate so that the average number of blocks per unit of time is constant

Motivations

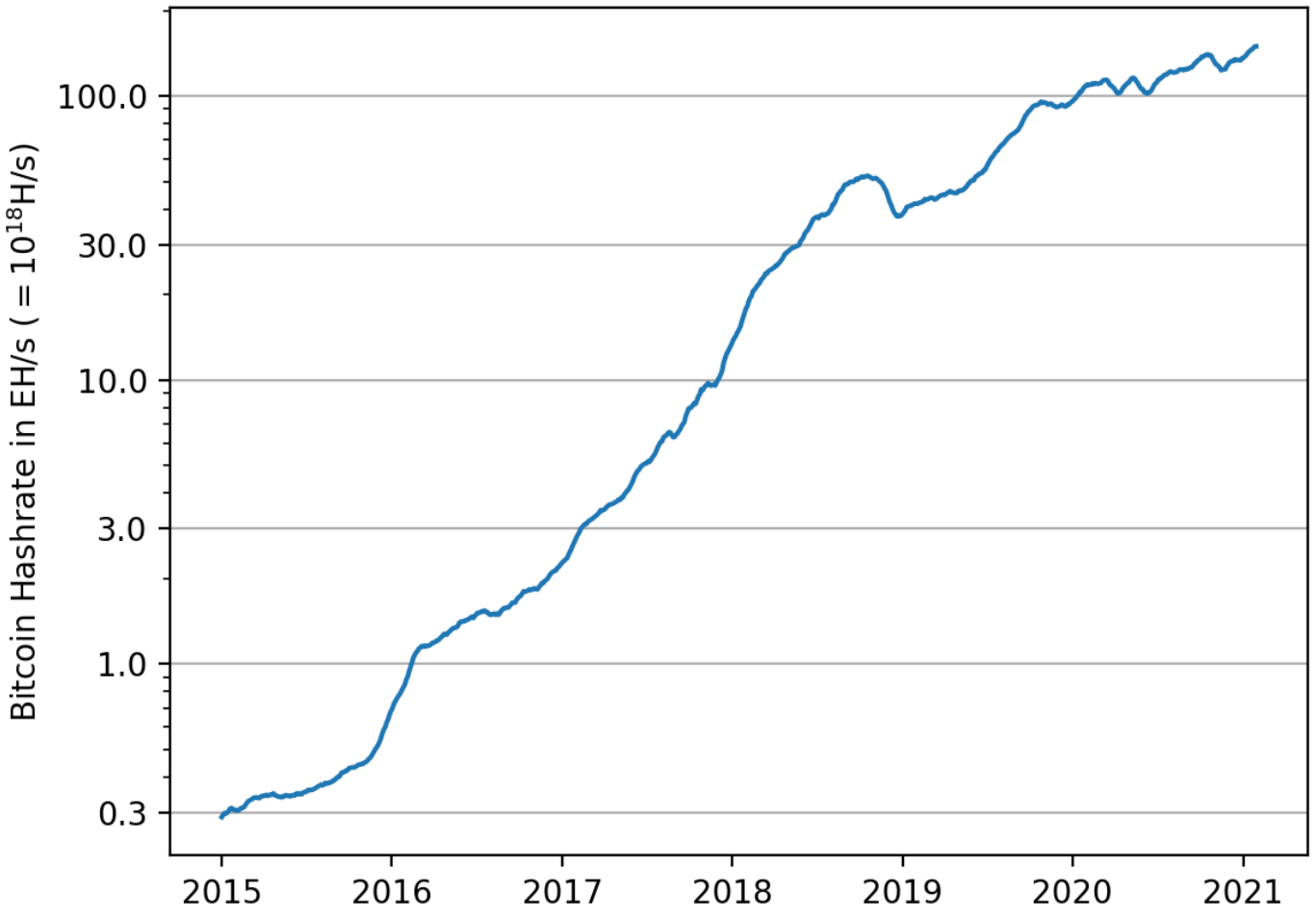


Figure: Total Bitcoin hashrate - log scale

Motivations

- On Proof-of-Work chains, the total hashrate is often said to represent the security of the blockchain
- We build a framework to understand the hashrate dynamics in various situations
- The hashrate is the result of miners interactions through computational power
- To understand the hashrate we need to understand the market for computational power

Literature Review

- Mean Field Games :
  - Lasry and Lions (2007)
  - Master equation : Lions (Cours au Collège de France (2008)), Cardaliaguet, Delarue, Lasry and Lions (2019), Bertucci, Lasry and Lions (2020)
  - Multi-populations : Cirant (2015), Achdou, Bardi and Cirant (2017),

- Blockchain mining :
  - Mining pools : Schrijvers, Bonneau, Boneh and Roughgarden (2016), Fisch, Pass and Shelat (2017), Cong, He and Li (2019)
  - Mining concentration : Alsabah and Capponi (2019), Li, Reppen and Sircar (2019)
  - Prat and Walter (2021)

2 The Basic Model

Model Setup - Base case model

A very simple model to understand the underlying mechanisms

Model assumptions

- Continuous-time environment ; time is discounted at rate r
- Perfect mining diversification ; constant reward in cryptocurrency
- Constant cryptocurrency price (relaxed later)

Technological progress - Efficiency

- assume constant technological progress rate : δ
- "real hashrate", K_t, is the "nominal hashrate", P_t, discounted by δ

$$K_t := e^{-\delta t} P_t$$

- the real hashrate is a better measure of the cost and security

$\Longrightarrow$ focus on the value of 1 unit of real hashrate, denoted by U

Market for Mining Devices

- Demand-side :
  - PoW fairly rewards miners, solely based on their computational power
  - So miner's demand, $D(p)$, is of the form

$$D(p) = \begin{cases} +\infty & \text{if } p \leq U \\ 0 & \text{if } p > U \end{cases}$$

- Supply-side :
  - Hardware manufacturers face quadratic costs
  - Their supply, $Q(p)$, is of the form

$$Q(p) = \lambda p$$

with $0 < \lambda < +\infty$ the elasticity of the supply with respect to the price

- Equilibrium :
  - Price is $p^* = U$; manufacturers can anticipate the demand
  - Quantity is constrained and is $Q^* = Q(p^*) = \lambda U$

Real Hashrate Dynamics

$$\frac{dK}{dt} = -\delta K + \lambda U$$

- The real hashrate depreciates at the rate of technological progress
- Miners decisions are continuous
- From the equilibrium of the mining hardware industry we know miners will continuously add $Q^* = \lambda U$ of real hashrate

Value of one unit of real hashrate

- Denote by c the electricity cost associated to running one unit of real hashrate
- Value function :

$$U(K) := \int_0^\infty e^{-(r+\delta)t} \left(\frac{1}{K_t + \epsilon} - c \right) dt$$

where $(K_t)_{0 \leq t}$ is the process satisfying

$$\begin{cases} dK_t = -\delta K_t dt + \lambda U(K_t) dt \\ K_0 = K \end{cases}$$

- If U is smooth, it satisfies the master equation

$$0 = -(r+\delta)U + U'_K(-\delta K + \lambda U) + \frac{1}{K+\epsilon} - c \text{ in } [0, \infty)$$

Master Equation and Solution

$$0 = -(r+\delta)U + U'_K(-\delta K + \lambda U) + \frac{1}{K+\epsilon} - c \text{ in } [0,\infty)$$

Theorem 3.1

There exists a *unique* lipschitz function solution of the master equation, such that $U' < 0$, $U(0) \geq 0$, and $\lim_{K\to\infty} U(K) \leq 0$

Idea of the proof

- Rely extensively on the monotonicity of the problem :
  - The reward $\frac{1}{K+\epsilon}$ is a decreasing function of K
  - The hashrate increments $\partial_t K$ is an increasing function of the value function U

Stationary State

Proposition 3.1

There always exists a unique stationary state for the real hashrate, K_*, and all induced trajectories converge toward it, regardless of K_0.

Explicit formula for K_*

- $\dot{K}(K_*) = 0 \iff \delta K_* = \lambda U(K_*)$
- from the master equation : $U(K_*) = \left(\frac{1}{K_*+\epsilon} - c\right)(r+\delta)^{-1}$
- combining the 2 yields :

$$K_* = \frac{\sqrt{(\delta\epsilon - \frac{c\lambda}{r+\delta})^2 + 4\frac{\delta\lambda}{r+\delta}} - \delta\epsilon - \frac{c\lambda}{r+\delta}}{2\delta}$$

Comparative statics

- the stationary state itself

$$K_*$$

- the value of one unit of real hashrate

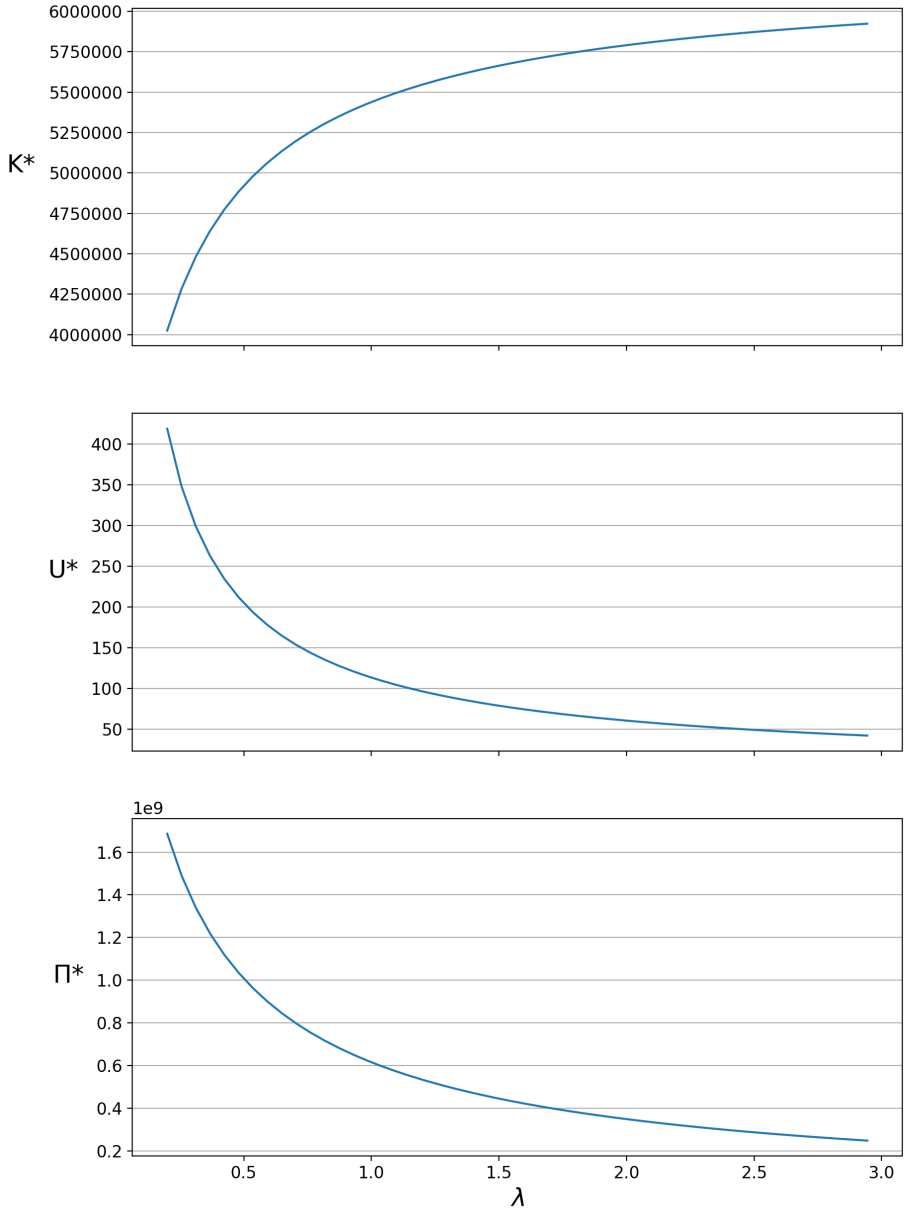
$$U(K_*) = \frac{\delta K_*}{\lambda}$$

- the total value of the real hashrate in place (value generated by miners)

$$\Pi_* = K_* U(K_*) = \frac{\delta K_*^2}{\lambda}$$

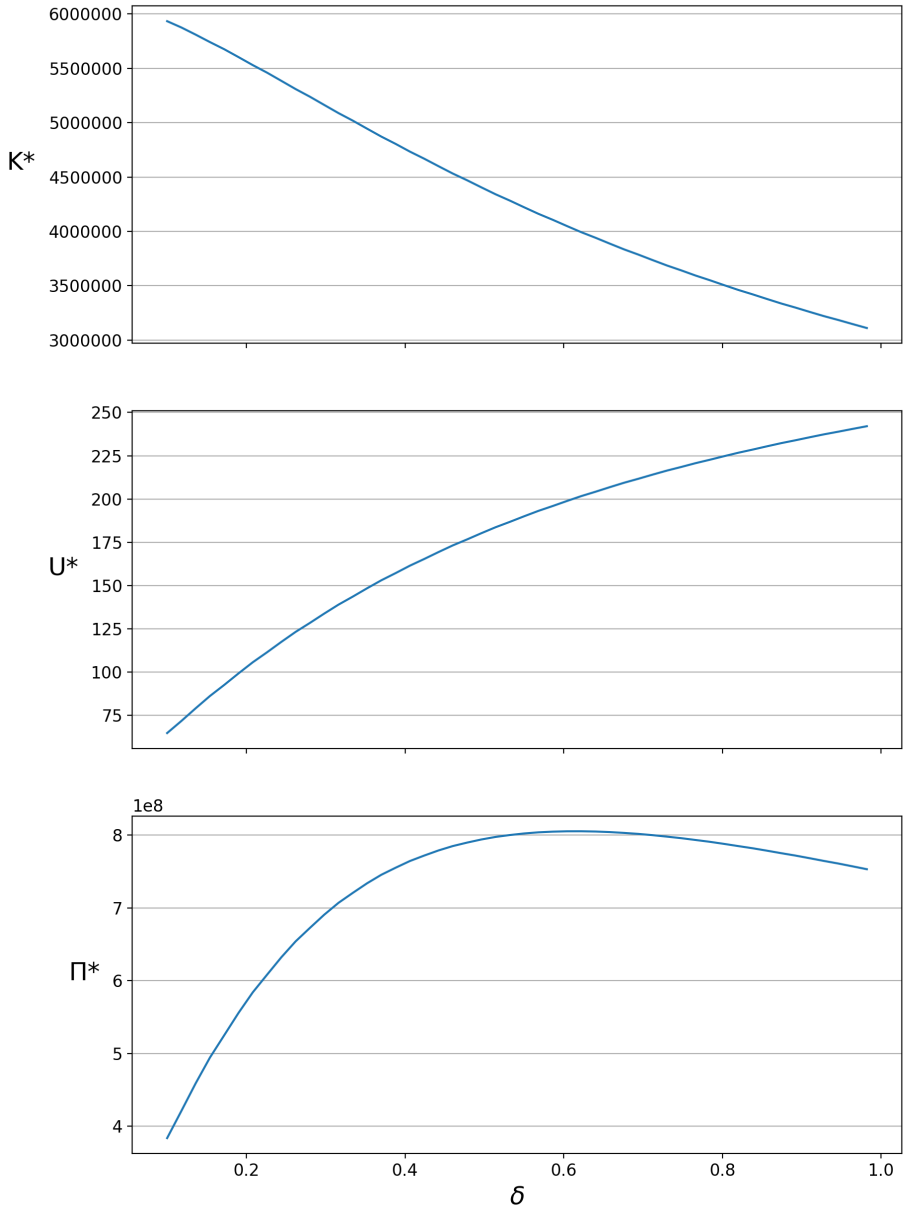
1. with respect to the friction parameter, λ
2. with respect to the technological progress, δ

With respect to market frictions



- The real hashrate can be linked to energy consumption and security
- In equilibrium, less frictions implies a higher real hashrate
- With less frictions, miners extract less rent from mining
- If miners make money, this is because of frictions

With respect to technological progress



- As δ increases, the real hashrate, K_*, depreciates more, because new machines will soon become better so miners buy less machines in equilibrium
- However, less machines imply mining is more profitable
- non-monotonic effect for Π_*
- hardware manufacturers collectively desire technological progress but not too much

Two populations of miners (1)

- Let's now introduce two populations of miners that each face a different electricity cost

$$c_1 \neq c_2$$

- Here we also allow miners to switch off their mining hardware if this is more profitable
- Miners of type 1 / type 2 :
  - Hashrate in place : K / L
  - Hashrate running : $\phi(K, L)$ / $\psi(K, L)$
- With

$$\phi(K,L) = \begin{cases} K & \text{if } \frac{1}{K+\psi(K,L)+\epsilon} \geq c_1 \\ (c_1)^{-1} - \psi(K,L) - \epsilon & \text{if } \frac{1}{K+\psi(K,L)+\epsilon} \leq c_1 \leq \frac{1}{\psi(K,L)+\epsilon} \\ 0 & \text{otherwise} \end{cases}$$

$$\psi(K,L) = \begin{cases} L & \text{if } \frac{1}{\phi(K,L)+L+\epsilon} \geq c_2 \\ (c_2)^{-1} - \phi(K,L) - \epsilon & \text{if } \frac{1}{\phi(K,L)+L+\epsilon} \leq c_2 \leq \frac{1}{\phi(K,L)+\epsilon} \\ 0 & \text{otherwise} \end{cases}$$

Two populations of miners (2)

- The value functions are defined by

$$U(K,L) := \int_0^\infty e^{-(r_1+\delta)t} \max\left(\frac{1}{\phi(K_t,L_t)+\psi(K_t,L_t)+\epsilon} - c_1; 0\right) dt$$

$$V(K,L) := \int_0^\infty e^{-(r_2+\delta)t} \max\left(\frac{1}{\phi(K_t,L_t)+\psi(K_t,L_t)+\epsilon} - c_2; 0\right) dt$$

where $(K_t)_{t\geq 0}$ and $(L_t)_{t\geq 0}$ evolve according to

$$\begin{cases} dK_t = -\delta K_t dt + \lambda_1 U(K_t, L_t) dt, \\ dL_t = -\delta L_t dt + \lambda_2 V(K_t, L_t) dt, \\ K_0 = K, L_0 = L. \end{cases}$$

- The system of master equations followed by U and V is

$$\begin{cases} 0 = -(r_1+\delta)U + (-\delta K + \lambda_1 U)\partial_K U + (-\delta L + \lambda_2 V)\partial_L U + \max\left\{\frac{1}{\phi+\psi+\epsilon} - c_1; 0\right\} \\ 0 = -(r_2+\delta)V + (-\delta K + \lambda_1 U)\partial_K V + (-\delta L + \lambda_2 V)\partial_L V + \max\left\{\frac{1}{\phi+\psi+\epsilon} - c_2; 0\right\} \end{cases}$$

Two populations of miners (3)

Theorem 4.2

There exists a unique lipschitz couple (U, V) solution of the system of master equations, such that $U(0,\cdot) \geq 0$ and $V(\cdot,0) \geq 0$, and both U and V are decreasing to both arguments.

Proposition 4.2

There exists a unique stationary state (x_0, y_0) and all induced trajectories converge toward it.

Remarks :

- At the stationary state, all existing machines are necessarily running
- Say $c_1 < c_2$
  - if c_2 is large enough, only miners of type 1 will mine
  - if c_2 is lower than some (explicit) bound, both populations will mine in equilibrium

3 A Homogenous Model of Bitcoin Mining

Random Price and Homogeneity Assumptions

$\Longrightarrow$ Here let's go back to the one population case

- The reward now follows

$$\frac{dR}{R} = \alpha dt + \sigma dW_t$$

- The Supply function of mining devices is now assumed to be

$$Q(p) = \lambda K(p - \overline{p})$$

- This means that the law of motion of the real hashrate is now

$$\frac{\dot{K}}{K} = -\delta + \lambda(U - \overline{p})$$

The Master Equation

- New master equation with $U = U(K, R)$, with $\nu = \frac{\sigma^2}{2}$

$$0 = -(r-\delta)U + K\partial_K U(-\delta + \lambda(U - \overline{p})) + \alpha R \partial_R U + \nu R^2 \partial_{RR} U + \frac{R}{K} - c$$

- U is an homogenous function, so with $\phi(\frac{R}{K}) = U(K, R)$, and with $x = \frac{R}{K}$, we have :

$$0 = -(r+\delta)\phi - x\phi'(-\delta + \lambda(\phi - \overline{p}) - \alpha) + \nu x^2 \phi'' + x - c$$

- Let's consider $z = ln(\frac{R}{K})$ and $\psi(ln(\frac{R}{K})) = \phi(\frac{R}{K})$

$$0 = -(r+\delta)\psi - \psi'(-\delta - \alpha + \nu + \lambda(\psi - \overline{p})) + \nu\psi'' + e^x - c$$

Social Planer Problem

- Here the problem is equivalent to that of a benevolent planer
- We can integrate this master equation and obtain an HJB equation :

$$0 = -(r+\delta)V(z) + V'(z)(\delta + \alpha - \nu) + \nu V''(z) - \frac{\lambda}{2}\left(V'(z) - \overline{p}\right)^2 + e^z - cz$$

Taking the model to the data

- We solve the HJB equation using standard numerical scheme (Godunov/Newton) with Neumann boundary conditions
- We use a structural approach to calibrate the mining hardware manufacturers supply function

$$Q(U) = \lambda K(U - \overline{p})$$

Data

- We use publicly available data of the Bitcoin Blockchain
- Total miners' revenue : $\{R_t\}_t$
- Nominal Hashrate : $\{P_t\}_t$
- Between January 1st, 2015 and February 1st, 2021

Parameters' Calibration

Exogenous parameters

Description	Parameter	Value
Discount Rate	r	0.2
Drift in reward process	α	0.652
Diffusion in reward process	σ	0.679
Technological rate of progress	δ	0.42
Unitary cost of electricity	c	350
Lag of hashrate growth	τ	3 months
Real hashrate normalization	-	29.23

Endogenous Parameters

- Real hashrate Dynamics is $\frac{\dot{K}}{K} = -\delta + \lambda(\phi - \overline{p})$
- We minimize the distance

$$(\lambda^*, \overline{p}^*) = \min_{\lambda, \overline{p}} \Gamma(\lambda, \overline{p}) = \sum_t \left(\frac{K_{t+\tau} - K_t}{K_t} - \left(-\delta + \lambda \left(\phi_{\lambda, \overline{p}} \left(\frac{R_t}{K_t} \right) - \overline{p} \right) \right) \right)^2$$

Value Function Calibration

- $\lambda = 7 \times 10^{-4}$ and $\overline{p} = 775$

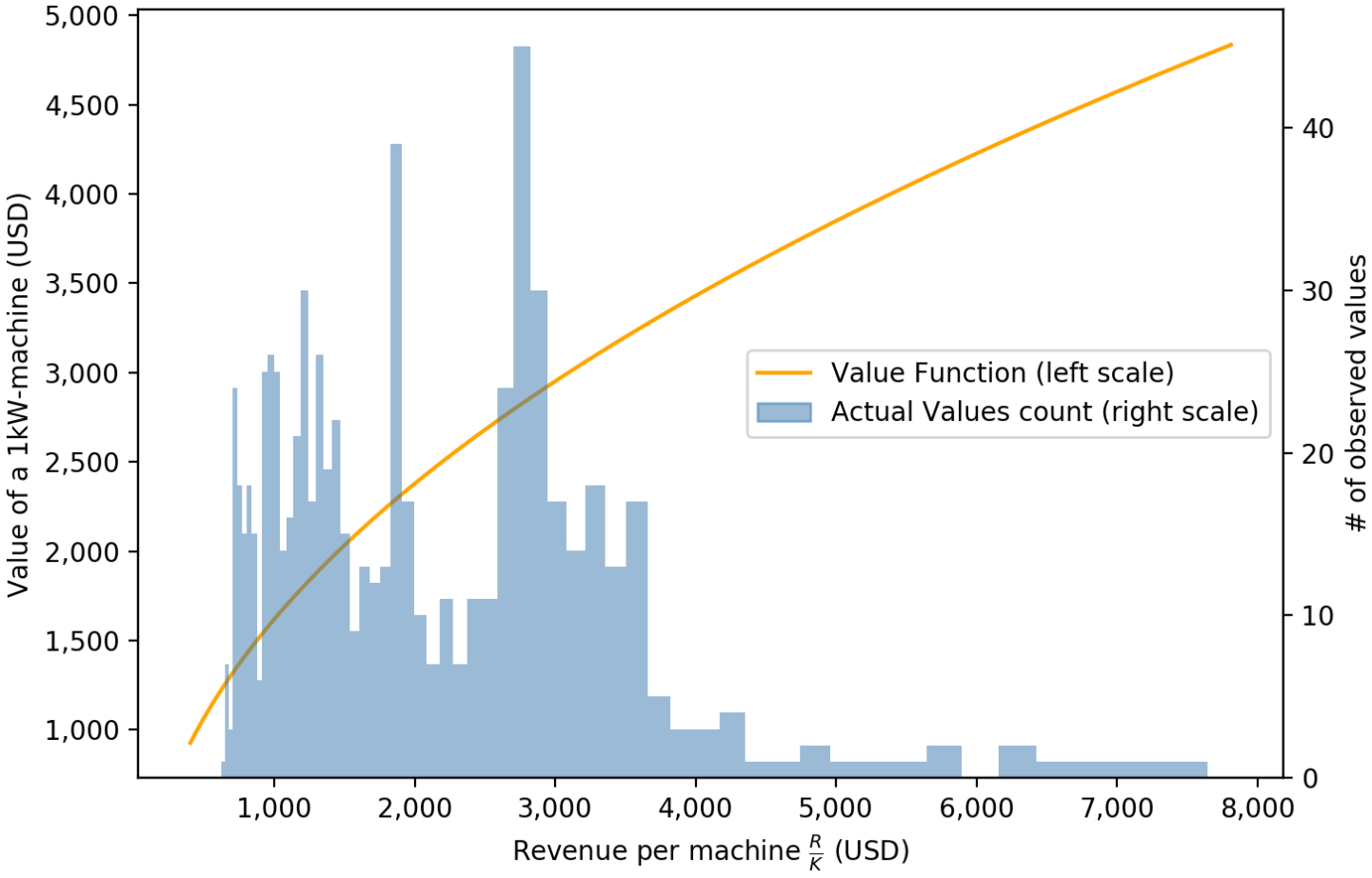


Figure: Value function (orange - left) and values for $x = \frac{R}{K}$ (blue - right)

Hashrate Dynamics

- correlation = 63% (***)

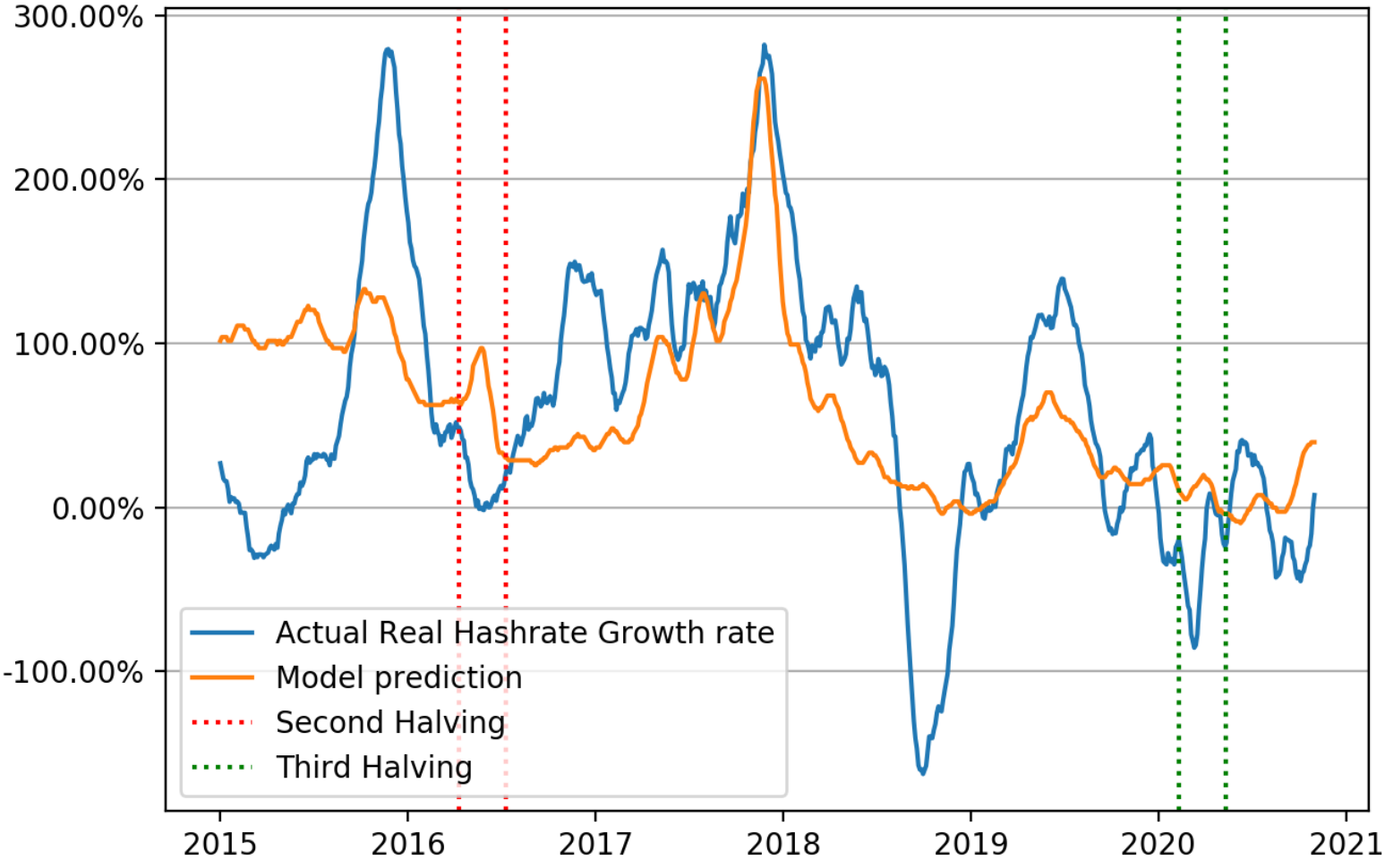


Figure: Actual (blue) and prediction (orange) of real hashrate growth rate

Revenue per Machine (1)

- Model assumes : both miners reward and real hashrate grow at the same constant rate on average

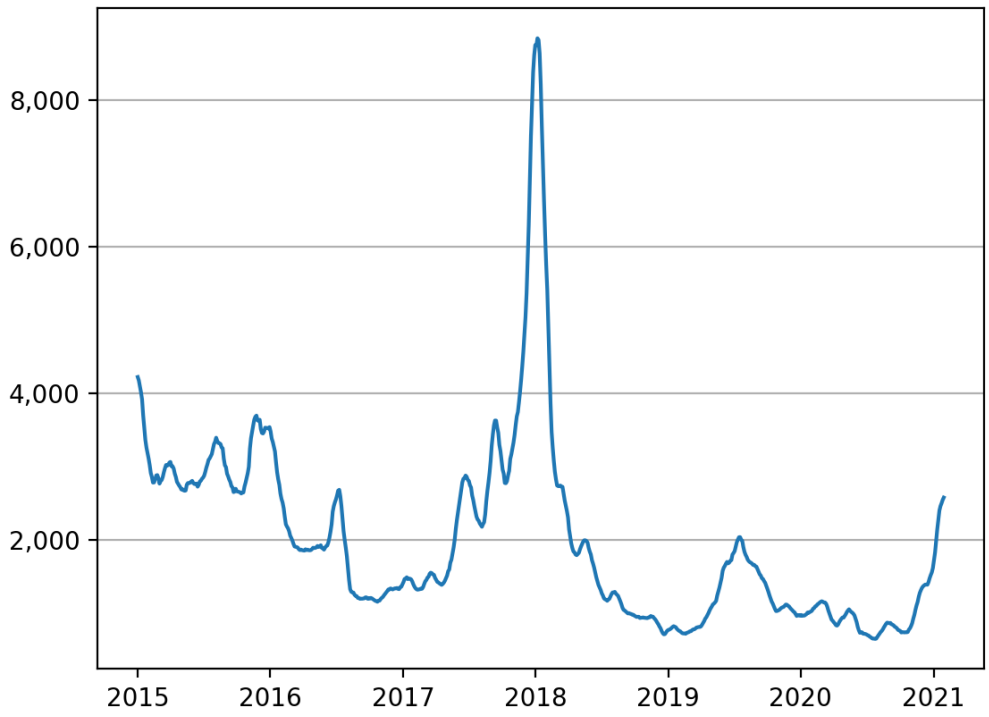


Figure: Revenue per machine that consumes 1kW of energy at current efficiency

- Law of motion of z :

$$dz_t = (\delta - \lambda(\tilde{v}(z) - \overline{p}) + \alpha - \nu)\, dt + \sigma dW_t$$

Revenue per Machine (2)

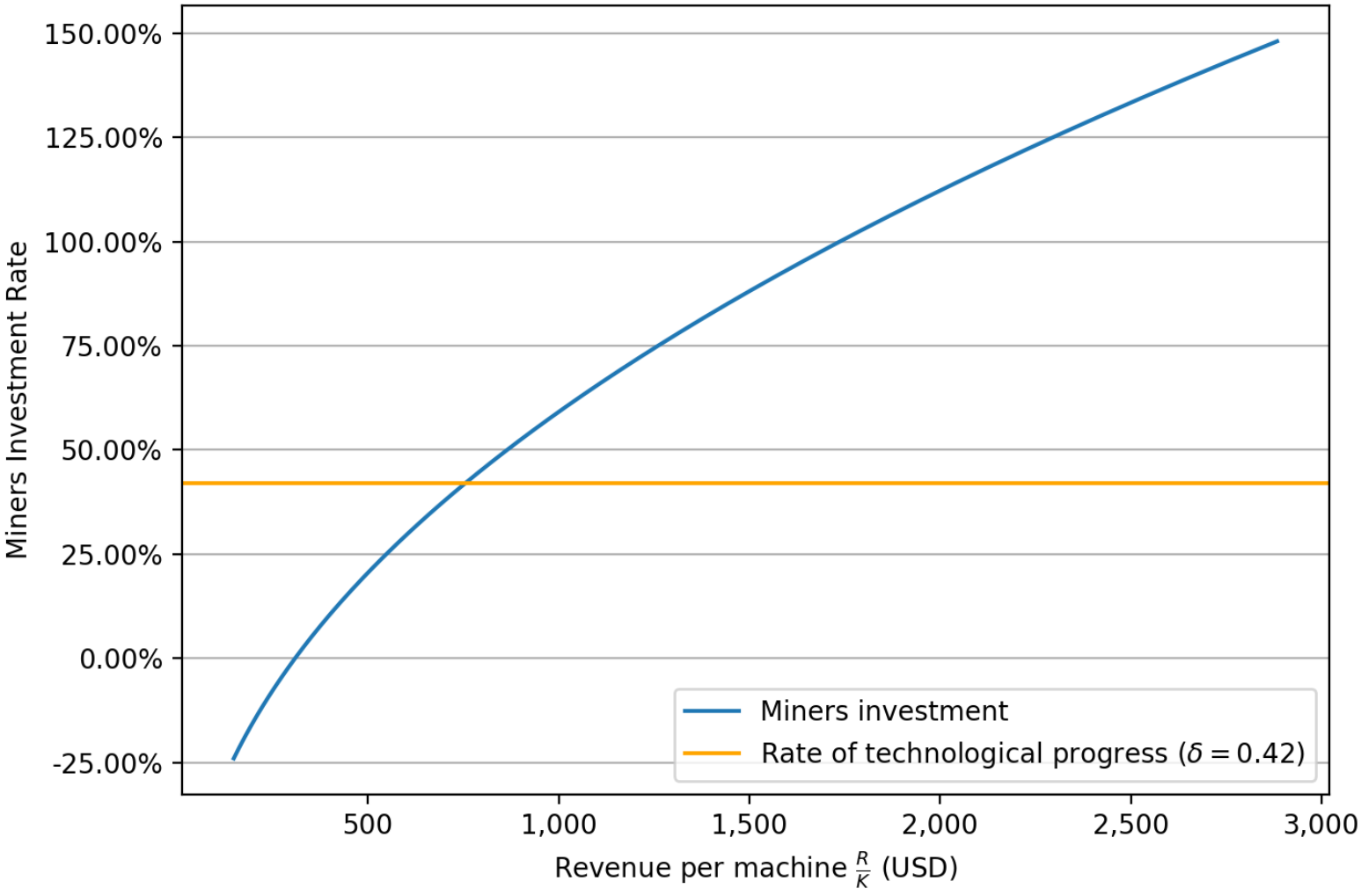


Figure: Miners Investment rate

Revenue per Machine (3)

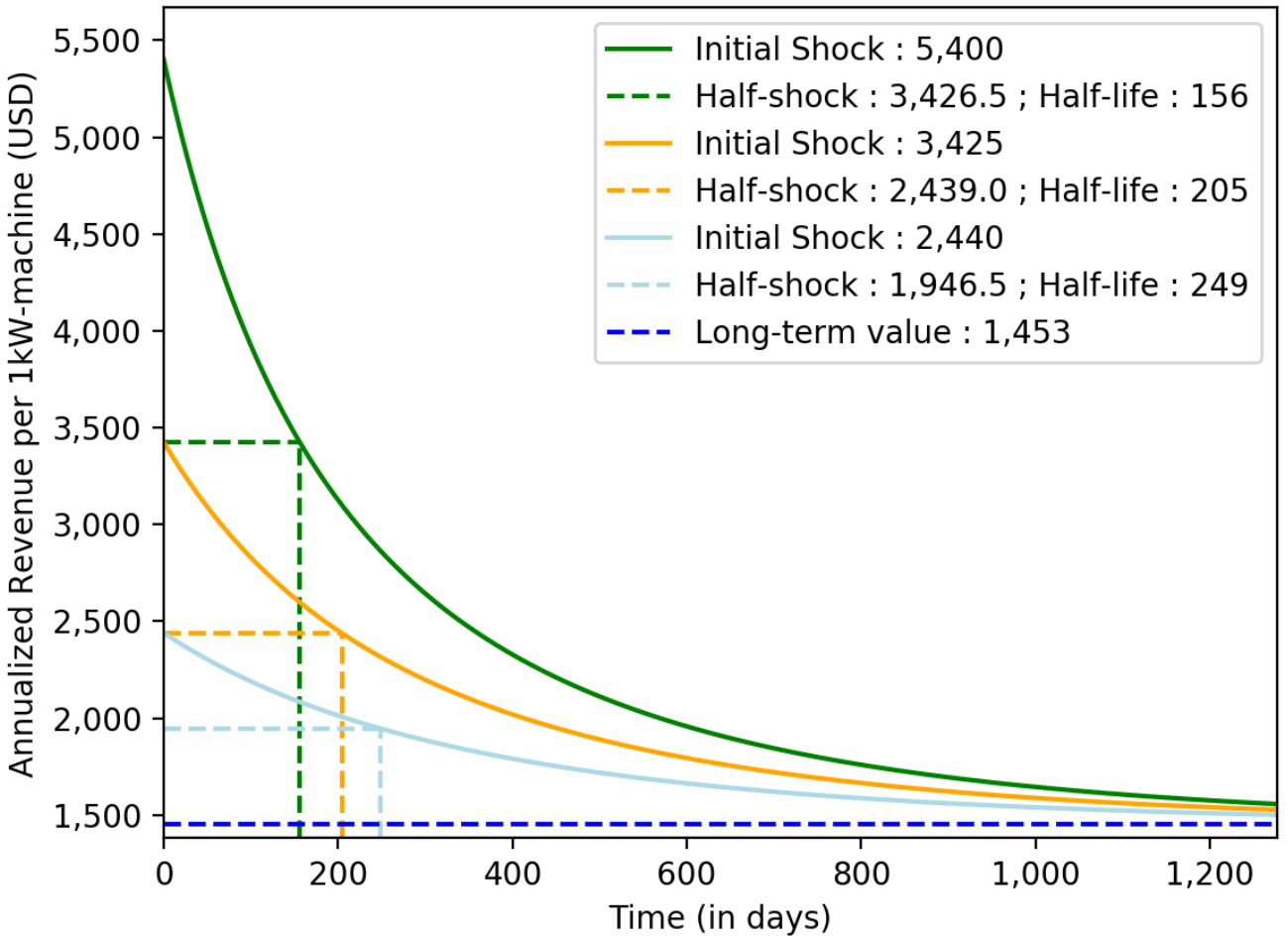


Figure: Response to a shock on the miners' revenue

4 Implications and Conclusion

Implications

- We study implications of the homogenous model on
  1. Blockchain security
  2. Energy consumption
  3. R&D investment
- All analysis is based on the fact that the revenue per machine has a long run target value : x^*

Implication for the Blockchain Security

- Security (Λ) : Resistance to external 51% attacks
- By definition we have

$$\Lambda_t = K_t v\left(\frac{R_t}{K_t}\right)$$

- Therefore, on the long run we have

$$\Lambda = \Lambda(R_t) = \frac{v(x^*)}{x} R_t$$

$\Longrightarrow$ The security grows with the miners reward linearly

Implication for the Energy Consumption

- Energy consumption is directly proportional to the real hashrate K
- And we know that on the long run, K grows with miners reward, as does therefore energy consumption

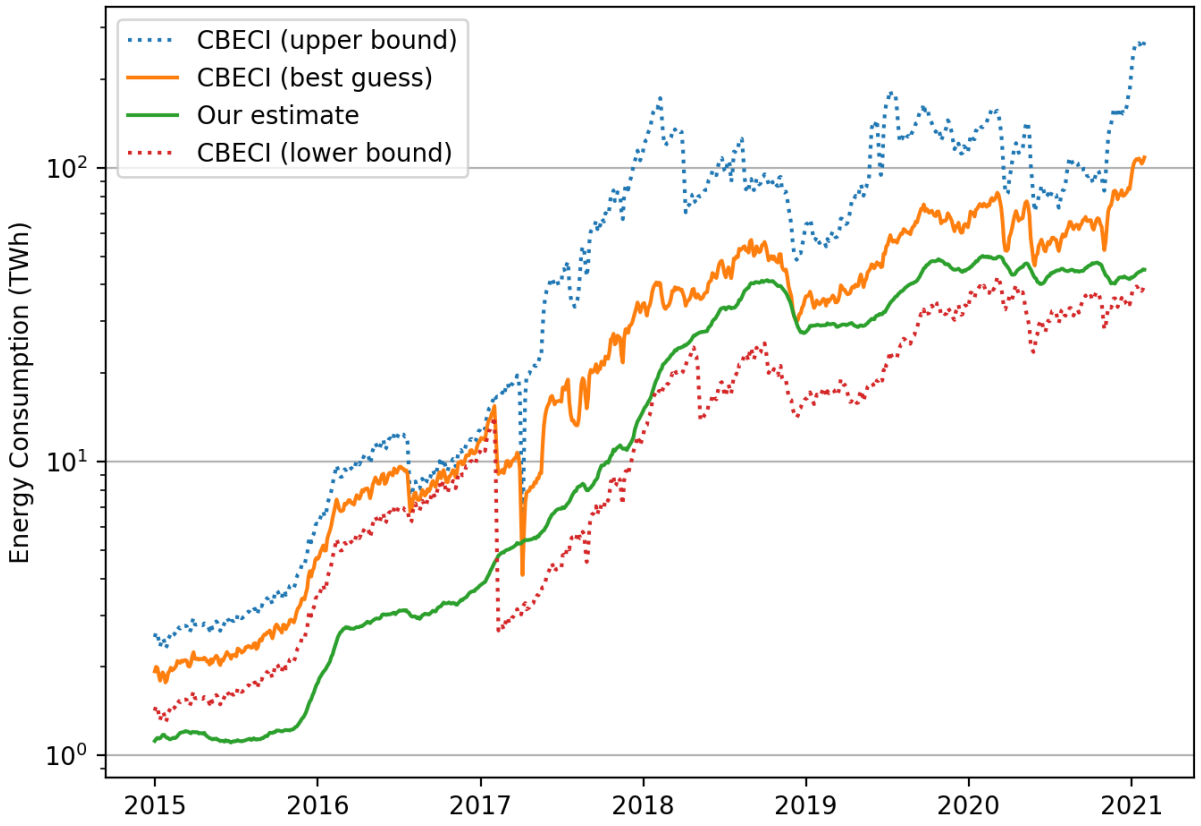


Figure: Bitcoin Energy Consumption

Implication for R&D Investment

- By buying machines from hardware manufacturers, miners contribute to technological progress
- Miners contribute to the real hashrate at rate

$$I_t = \lambda[u(R_t/K_t) - \overline{p}]$$

- Once again, based on the revenue per machine dynamics, we know that, on the long run,

$$I^* = \delta + \alpha - \frac{1}{2}\sigma^2$$

- Therefore, the revenue generated by the whole mining chips manufacturers industry is, on the long run,

$$\Pi^* = I^* K^* v(x^*) = \frac{I^*}{x^*} v(x^*) R_t$$

$\Longrightarrow$ The R&D investment grows with the miners reward linearly

Concluding Remark on the Economics of Bitcoin

- Hopefully you're convinced that PoW is inherently a MFG

- We introduce a class of models that can fit many different situations (other variations in our papers)
- Our different models show that the PoW consensus algorithm produces an extremely stable equilibrium
- The Nash (MFG) equilibrium is fully at play here
  - No outside intervention
  - Individual miners can join or quit, they do not affect the long term value of the equilibrium (see recent chinese ban)
  - Equilibrium very resilient to perturbations

$\Longrightarrow$ the transactional system (i.e. the blockchain) is very solid

A Mean Field Game Approach to Bitcoin Mining

Louis Bertucci

Institut Louis Bachelier

Collège de France, Seminar
Equations aux dérivées partielles et applications

December 10, 2021