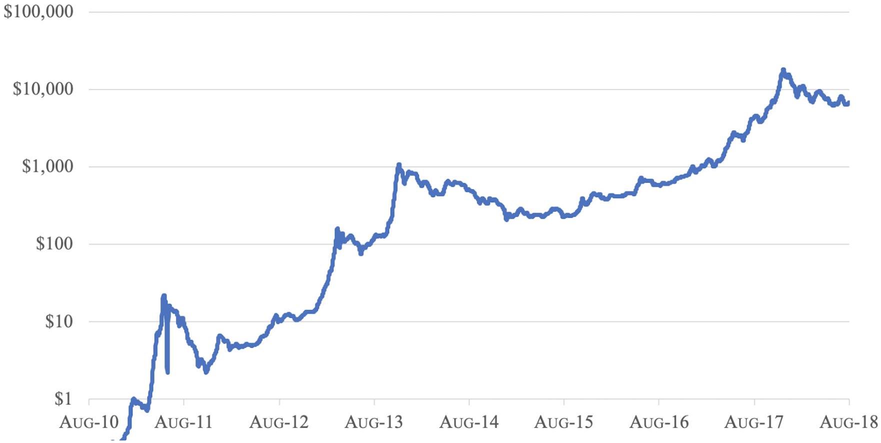
Bitcoin as Decentralized Money: Prices, Mining, and Network Security

Emiliano S. Pagnotta

Imperial College London

AEA. January 3, 2020

FIGURE: Bitcoin Price (log scale): August 2010 to August 2018



Decentralized Networks: Security Models

Definition:

*We say that a token's security (S) is **intrinsic** when $p \neq p'$ implies $S(p) \neq S(p')$. Otherwise, we refer to the token's security as **extrinsic**.*

Figure: Intrinsic and Extrinsic Security Models

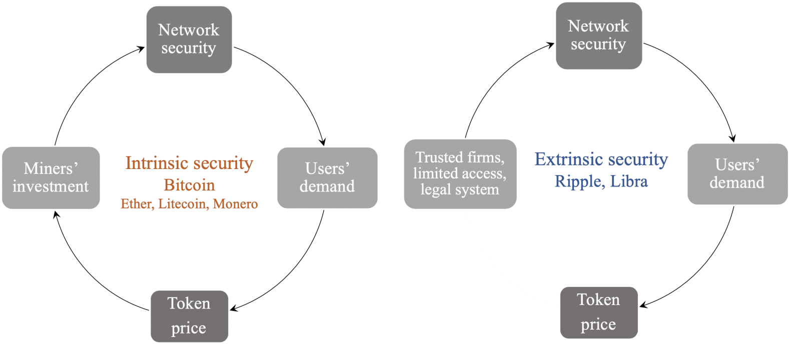
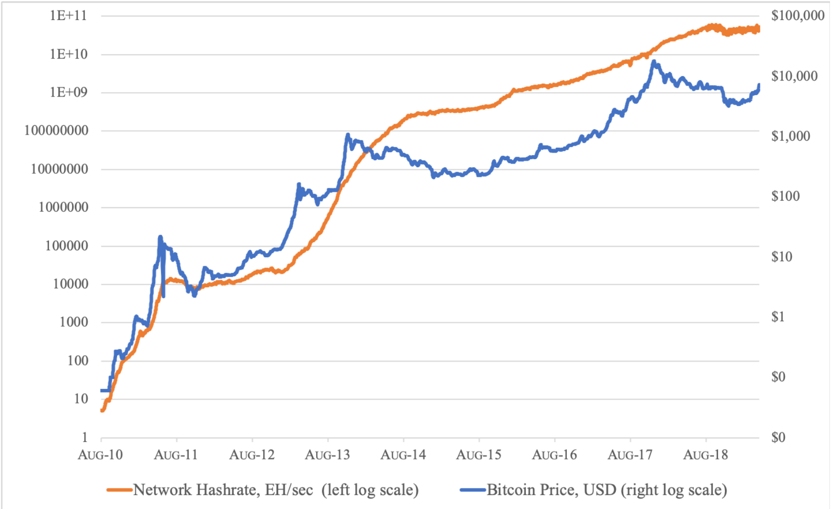


FIGURE: Bitcoin Price and network hashrate: August 2010 to May 2019



- Key mechanism we capture: token simultaneously serves an exchange function for users and incentive device for miners.

Environment: Bitcoins users, miners, and attacker

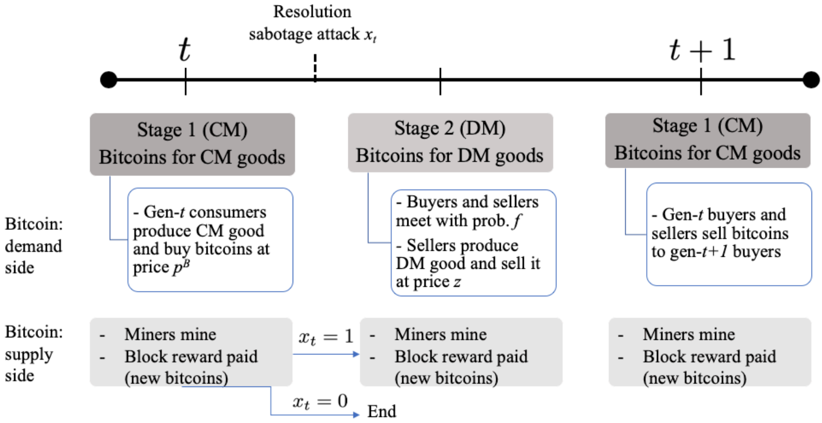
Demand: Markets and Players

- Each period $t \in \{0, 1, ...\}$ has two stages: first stage is frictionless (CM) and second (DM) is subject to a participation friction, similar to Rocheteau and Wright (ECMA 2005)
- **Buyers:** mass n. Wish to consume in the DM, but cannot produce. Lifetime utility:

$$U^B = u(c_t) - l_t + u(q_t) + \delta c_{t+1}$$

- **Sellers:** *Sellers* can produce in the DM, but do not wish to consume. Utility $U^S = -q_t + \delta c_{t+1}$
- Meeting prob. is f. DM price is z (units of CM good)
- **Bitcoin.** Single network token with price p and supply B with deterministic growth $\rho_t = B_t / B_{t-1}$
- **Miners**: $m \geq 2$, homogeneous and risk-neutral
- **Attacker**: Interested in hurting the system

FIGURE: Model Timeline



Resolution
sabotage attack x_t
t
$t+1$
Stage 1 (CM)
Bitcoins for CM goods
Stage 2 (DM)
Bitcoins for DM goods
Stage 1 (CM)
Bitcoins for CM goods
Bitcoin: demand side
- Gen-t consumers produce CM good and buy bitcoins at price p^B
- Buyers and sellers meet with prob. f
- Sellers produce DM good and sell it at price z
- Gen-t buyers and sellers sell bitcoins to gen-$t+1$ buyers
Bitcoin: supply side
- Miners mine
- Block reward paid (new bitcoins)
$x_t = 1$
- Miners mine
- Block reward paid (new bitcoins)
- Miners mine
- Block reward paid (new bitcoins)
$x_t = 0$
End

- **Attack outcome** $x_t \in \{0, 1\}$ (*aggregate risk*)
  - $x_t = 1$ **network survives** within t
  - $x_t = 0$ **successful attack,** network unusable thereafter: $p_{s>t} = 0$

BITCOIN USERS: SECURITY$(S)\to$PRICE(p)

- Let $S_t := \mathbb{P}(x_t = 1)$
- Buyers born in period t solve

$$\max_{B_{it},c_t,l_t} u(c_t) - l_t + S_t \left(f \max_{q_t^d \le \frac{B_{it}p_t}{z_t}} \left\{ u\left(q_t^d\right) + \delta \mathbb{E}_t^1 \left(B_{it} - \frac{z_t q_t^d}{p_t} \right) p_{t+1} \right\} + (1-f)\, \delta \mathbb{E}_t^1 B_{it} p_{t+1} \right),$$

s.t. $B_{it}p_t + c_t \le l_t$. $\mathbb{E}_t^1$ is the expectation of p_{t+1} cond. on $x_t = 1$

- The program of a seller at time t is

$$\max_{q_t^s} \left\{ -q_t^s + \delta \mathbb{E}_t^1 \left(z_t q_t^s \frac{p_{t+1}}{p_t} \right) \right\}$$

- **Partial equilibrium**: higher security implies higher price

SUPPLY SIDE: PRICE(p)$\rightarrow$MINING(H)

Nakamoto competition to verify blocks

- Miner j provides h_j at a cost ch_j, $c > 0$, wins with prob $\frac{h_j}{h_j + h_{-j}}$
- If j wins, receives reward next period
- Reward given by newly minted bitcoins
- Supply: $B_{t+1} = B_t + 2 \times \text{reward}_t$
- No user fees: “blocks not full yet,” $nf <$ block size
- Mining difficulty adjusts so block confirmations occur every period
- Look for symmetric Nash equilibrium
- **Partial equilibrium:** $H := \sum h_j \uparrow$ with reward, price , and m

SABOTEUR: MINING(H)→SECURITY(S)

Attacker

- Interested in hurting the system (e.g., regulatory, military, or intelligence agency; multilateral task force; central bank association; competing system; short seller)
- Agency has use-it-or-loose-it budget affords $A > 0$ computer power per period

Subgame interim CM and DM

- Saboteur seeks to create a disruptive fork of $k > 1$. Intuitions: aggregate denial of service, consensus crisis, honest miners leave, retailers stop accepting bitcoins
- Gamblers' ruin: if $H_t > A$, probability of a disruptive fork of $k > 1$ blocks is: $\left(\frac{A}{H_t}\right)^k$
- Security function:

$$S\left(H_t, A\right) = \begin{cases} 1 - \left(\frac{A}{H_t}\right)^k & H > A \\ 0 & \text{else} \end{cases}$$

General Equilibrium

1. Is there an equilibrium where the value of bitcoin is always zero?
2. With a constant and positive real bitcoin balances?
3. If so, is it unique?
4. Is it dynamically stable?

General Equilibrium

1. Is there an equilibrium where the value of bitcoin is always zero?
   Yes
2. With a constant and positive real bitcoin balances?
   Yes, depending on the relation between n and A
3. If so, is it unique?
   No
4. Is it dynamically stable?
   The lowest value always is, regardless of preferences

Decentralized Monetary Equilibrium (DME)

Definition

A sequence $\left\{B_{it}, q_t^d, q_t^s, h_t, z_t, p_t\right\}_{t=0}^{+\infty}$ *of consumption, production, saving, hashrate supply decisions, and prices, such that: (i) buyers and sellers maximize utility, (ii) miners maximize profits, and (iii) markets clear*

Decentralized Monetary Equilibrium (DME)

Definition

A sequence $\left\{B_{it}, q_t^d, q_t^s, h_t, z_t, p_t\right\}_{t=0}^{+\infty}$ of consumption, production, saving, hashrate supply decisions, and prices, such that: (i) buyers and sellers maximize utility, (ii) miners maximize profits, and (iii) markets clear

1. In a DME, bitcoin price and security are *jointly* determined
2. *Absent subsidies, $p = 0$ is always a stationary equilibrium*
3. Focus on stable equilibrium within an 'inflation era': *constant network market cap $b = Bp$*, supply B growing at $\rho > 1$, prices decreasing at same rate

$$b_t = \underbrace{\frac{\delta}{\rho} S\left(H_t, A\right) b_{t+1} \left\{ f\left(u'\left(\frac{\delta}{\rho} \frac{b_{t+1}}{n} \right) - 1 \right) + 1 \right\}}_{D(b_{t+1})},$$

$$\text{s.t.} H(b) = \left(\frac{m-1}{m} \right) \frac{\delta}{\rho} \left(\frac{\rho - 1}{2c} \right) b$$

Existence and Multiplicity

Existence, and Multiplicity: Bitcoin

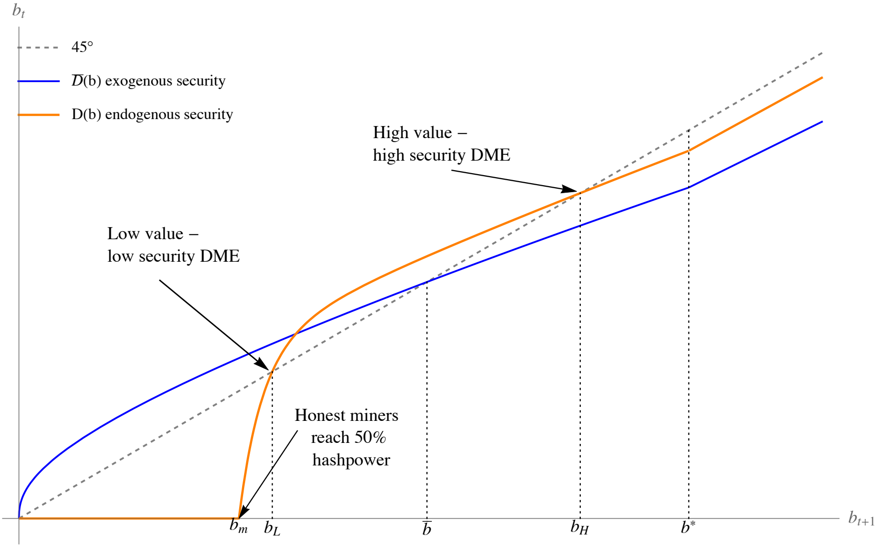
Assume intrinsic security and a saboteur's hash rate $A > 0$

- There is a population level $\hat{n}(A)$ such that if $n > \hat{n}(A)$ a DME must exist
- In general, if a stationary DME exists, there is an even number of them. b_L and b_H lowest and highest

If security is extrinsic a single stationary monetary equilibrium $\overline{b}$ exists

- **Multiplicity intuition**: Directly connected to the intrinsic security model: If the value of bitcoins is low, miners have little incentive to invest, and the security of the network is low. In that case, buyers do not wish to accumulate large real balances, and the resulting valuation is low. The opposite is true when the value of bitcoins is perceived to be high, making it self-fulfilling

FIGURE: Decentralized Monetary Equilibria: Existence and Multiplicity



Implications for Monetary Policy

1. How is bitcoin value affected by changes in ρ?
2. Do quadrennial reward halving always increase the price?
3. How does the socially optimal monetary rule relate to the security model?

Implications for Monetary Policy

1. How is bitcoin value affected by changes in ρ?
   It is nonmonotonic and can lead to deviations of the quantity theory
2. Do quadrennial reward halving always increase the price?
   No. Halving could even decrease it
3. How does the socially optimal monetary rule relate to the security model?
   With extrinsic security, a Friedman-like rule is optimal
   For Bitcoin, a Friedman-like rule is never optimal

Investment-Optimal Monetary Policy

- Extrinsic case: $\uparrow \rho \Rightarrow \downarrow p$ (less scarcity = inflation tax)

Investment-Optimal Monetary Policy

- Extrinsic case: $\uparrow\rho \Rightarrow \downarrow p$ (less scarcity = inflation tax)
- Bitcoin: *two* distinct channels by which ρ affect the price

$$p_t = \frac{n}{B_t}\left(\frac{S\left(H\left(p_t;\rho\right),A\right)\rho^{\sigma}f\delta^{1-\sigma}}{\rho-\delta S\left(H\left(p_t;\rho\right),A\right)\left(1-f\right)}\right)^{\frac{1}{\sigma}}$$

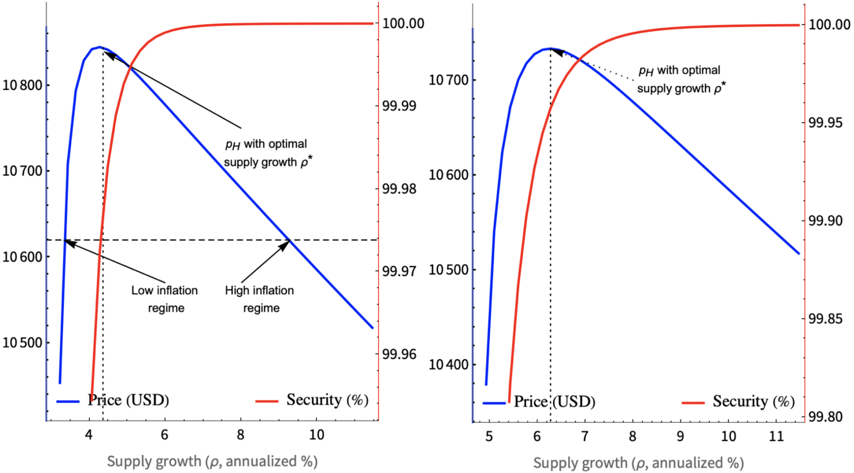
scarcity and security channels

.

- *Scarcity channel*: negative value effect
- *Security channel*: positive value effect

Value-optimal Monetary Policy

For the high DME there is a value ρ^* such that, if $\rho < \rho^*$, bitcoin price increases with ρ, and decreases with it if $\rho > \rho^*$



(a) High DME (baseline)

(b) High DME (high A)

FIGURE: Prices around reward halving: Beginning of 2nd era (2012)

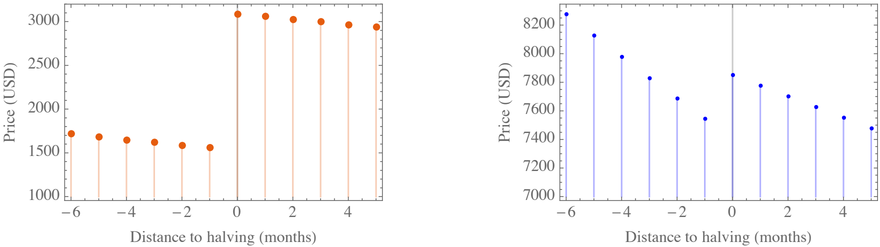


FIGURE: Prices around reward halving: Beginning of 4th era (2020)

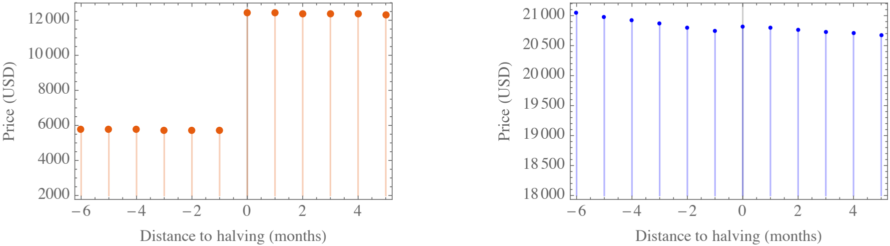
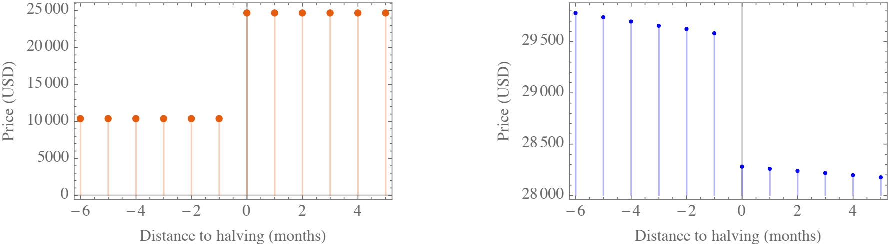


FIGURE: Prices around reward halving: Beginning of 5th era (2024)



Socially–Optimal Monetary Policy

What is the monetary policy that maximizes social welfare, ρ_W?

Optimal Monetary Policy

- For a token with extrinsic security $\overline{S}$, the socially optimal monetary policy is $\overline{\rho}_W = \overline{S}\delta < 1$, a version of the Friedman rule

Socially–Optimal Monetary Policy

What is the monetary policy that maximizes social welfare, ρ_W?

Optimal Monetary Policy

- For a token with extrinsic security $\overline{S}$, the socially optimal monetary policy is $\overline{\rho}_W = \overline{S}\delta < 1$, a version of the Friedman rule
- For Bitcoin, $\rho_W > 1$, the Friedman rule is both unfeasible and suboptimal
- ρ_W is implicitly defined by $\frac{dW}{d\rho}(\rho_W) = 0$,

$$W = \underbrace{S(b_{ss}, A) f\left(u\left(q\left(b_{ss}\right)\right) n - \frac{\delta}{\rho} b_{ss}\right)}_{\text{DM surplus}} - \underbrace{\left(1 - S(b_{ss}, A)\frac{\delta}{\rho}\right) b_{ss}}_{\text{cost of carrying balances}}$$

$$- \underbrace{\left(\frac{m-1}{m}\right)(\rho - 1)\frac{\delta}{\rho} b_{ss}}_{\text{aggregate mining investment}}$$

Implications for Price Volatility

1. Monetary policy is rigid. But does the security model matter?
2. Is the direction of prices change a sufficient statistic for changes in security?

Implications for Price Volatility

1. Monetary policy is rigid. But does the security model matter?
   You bet it does
   1) Fundamental channel: it amplifies demand shocks
   2) Nonfundamental channel: it allows for boom-bust equilibria where expectations about future bitcoin prices depend on sentiment

2. Is the direction of prices change a sufficient statistic for changes in security?
   No. Exception can be found when attack resources change over time

Fundamentals: Amplification of Demand Shocks

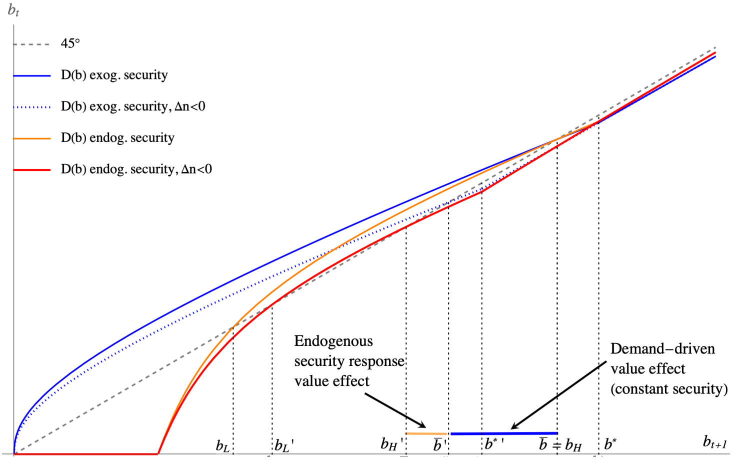


FIGURE: Changes in Demand Fundamentals

NonFundamentals: Sunspot-driven Booms and Busts

- Two-state Markov chain $s \in \{1, 2\}$, persistence $\phi_s := \mathbb{P}(s_{t+1} = s | s_t = s)$. Realization of sunspot beginning of DM

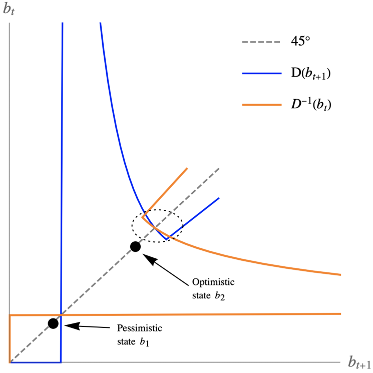


Figure: Nonfundamental volatility

Volatility, Life Exp., and Attackers' Budget

$b_t\,/\,b_{t+1}$	0	b_1	b_2
0	1	0	0
b_1	$1 - S\left(\mathbb{E}_1 b, A\right)$	$S\left(\mathbb{E}_1, A\right)\phi_1$	$S\left(\mathbb{E}_1, A\right)\left(1 - \phi_1\right)$
b_2	$1 - S\left(\mathbb{E}_2 b, A\right)$	$S\left(\mathbb{E}_2 b, A\right)\left(1 - \phi_2\right)$	$S\left(\mathbb{E}_2 b, A\right)\phi_2$

TABLE: Transition Probability Matrix

- Informal intuition: More resourceful attacker makes price more unstable and shortens Bitcoin's life expectancy

Volatility, Life Exp., and Attackers' Budget

$b_t\,/\,b_{t+1}$	0	b_1	b_2
0	1	0	0
b_1	$1 - S\left(\mathbb{E}_1 b, A\right)$	$S\left(\mathbb{E}_1, A\right)\phi_1$	$S\left(\mathbb{E}_1, A\right)\left(1 - \phi_1\right)$
b_2	$1 - S\left(\mathbb{E}_2 b, A\right)$	$S\left(\mathbb{E}_2 b, A\right)\left(1 - \phi_2\right)$	$S\left(\mathbb{E}_2 b, A\right)\phi_2$

TABLE: Transition Probability Matrix

- Informal intuition: More resourceful attacker makes price more unstable and shortens Bitcoin's life expectancy

	Sunspot Equilibrium						No-Sunspot Equilibria			
A	p_1	p_2	ϕ_1	ϕ_2	s.d.	MTA	p_L	MTA	p_H	MTA
80	4,878	8,152	0.905	0.883	969.5	14.96	5,419	10.29	10,884	9,51
90	5,561	8,555	0.883	0.898	910.3	17.97	6,244	12.73	10,867	3,07
100	6,281	8,979	0.858	0.921	807.0	23.32	7,140	16.59	10,817	993.4
110	7,068	9,422	0.832	0.954	635.5	33.23	8,173	24.31	10.671	332.4
120	8,069	9,839	0.828	0.999	179.6	59.30	9,687	60.02	9,990	80.21

TABLE: Quantitative Model Outcomes

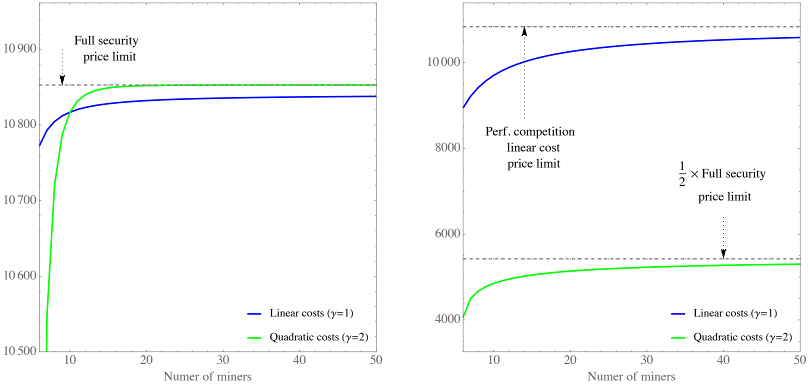
Implications for Industrial Organization of Bitcoin Mining

1. Miner entry: Can we expect Cournot outcomes?
2. How do mining costs relate to minting costs?

Implications for Industrial Origanization of Bitcoin Mining

1. Miner entry: Can we expect Cournot outcomes?
   No
   1) Although total capacity increases with m, the price can increase as well
   2) For miners, bitcoin's security model buffers profit volatility of entry shocks
2. How do mining costs relate to minting costs?
   Perfect competition limit
   1) With linear costs, minting cost equals bitcoin price
   2) With convex power costs (curvature γ), the minting cost is lower, and equals a fraction $\frac{1}{\gamma}$ of the price

FIGURE: High DME Price and Minting costs



Concluding Takeaways

1. The security of open blockchains should be seen as an economic outcome, not as a feature of its technology: The same fundamentals and technology are consistent with equilibria displaying sharply different security levels
2. Bitcoin monetary policy structurally linked to security budget. Leads to surprising results regarding reward halving and socially optimal rules
3. Model rationalizes observed cointegrated relation between price and hash power
4. Model helps rationalizing observed huge price volatility, since the security model amplifies shocks and can lead to unpredictable but rational booms and busts

Thanks