universität innsbruck

A Primer on Economics for Cryptocurrencies

School on Security & Privacy for Blockchains and Distributed Ledger Technologies

Rainer Böhme

Motivation

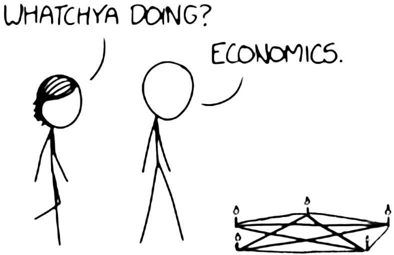
We have tried – quite some time ago – to explain Bitcoin to economists:

- Böhme, R., Christin, N., Edelman, B., and Moore, T. Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29, 2 (2015), 213–238
- **Today I am trying to do the opposite.**

Outline

1. **Rational Agents and Adversaries**
2. Efficient Markets
3. Market Concentration

Economics

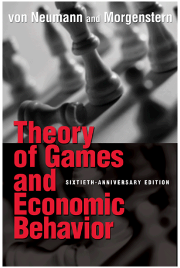


~~predict~~ behavior

model

Illustration: xkcd.com

Game Theory



A mathematical approach to model strategic behavior

Interpretation as generalizations of . . .

a. Probability theory – replace uncertainty with rationality assumption
b. Optimization – objective function anticipates optimal response

Mechanism design (MD)

“Reverse game theory”: define payouts to incentivize intended behavior

The protocol is the mechanism. Users are agents – “players”.

Classification of Security Games

Attacker vs Defender

- for security investment and tactics
- often zero sum

Defender vs Defender

- for security policy
- often non-zero sum
- attackers are “nature”, i. e., stochastic but not strategic

Attacker vs Protocol Designer (less common)

- “rational” protocol design inspired from “rational cryptography”
- defenders are “nature”

Garay, J. et al. *Rational Protocol Design: Cryptography Against Incentive-driven Adversaries*, 2013.

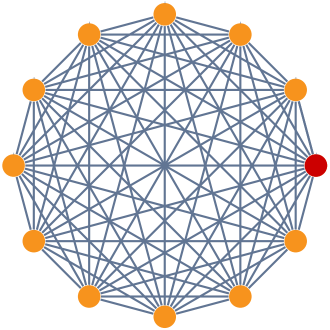
Weak Identities

Games without central identity provider:

Douceur, J. R. The Sybil Attack. In P. Druschel, F. Kaashoek und A. Rowstron (eds.), *Peer-to-peer Systems*. LNCS 2429, Springer, Berlin Heidelberg, 2002, 251–260.

Weak Identities

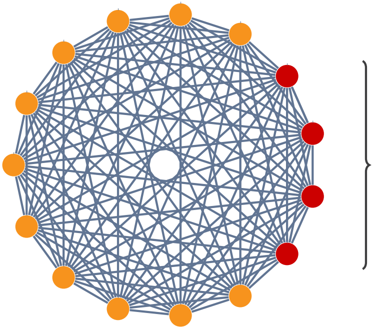
Games without central identity provider:



Douceur, J. R. The Sybil Attack. In P. Druschel, F. Kaashoek und A. Rowstron (eds.), *Peer-to-peer Systems*. LNCS 2429, Springer, Berlin Heidelberg, 2002, 251–260.

Weak Identities

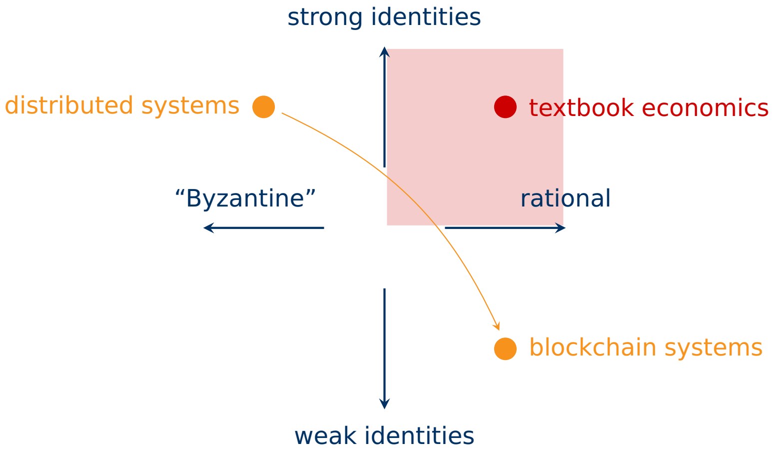
Games without central identity provider:



Douceur, J. R. The Sybil Attack. In P. Druschel, F. Kaashoek und A. Rowstron (eds.), *Peer-to-peer Systems*. LNCS 2429, Springer, Berlin Heidelberg, 2002, 251–260.

Behavior-regulating Assumptions

Building a bridge between distributed systems and economics:



Principles of Economics

Rational choice

- Autonomous decision makers – agents – take actions to maximize their objective function – utility.

$$u_i(a_i)$$

Externality

- Actions taken by one agent affect the utility of other agents.

$$u_j(\dots, a_i, \dots)$$

Social welfare – protocol objective

- Global outcome from all local decisions.

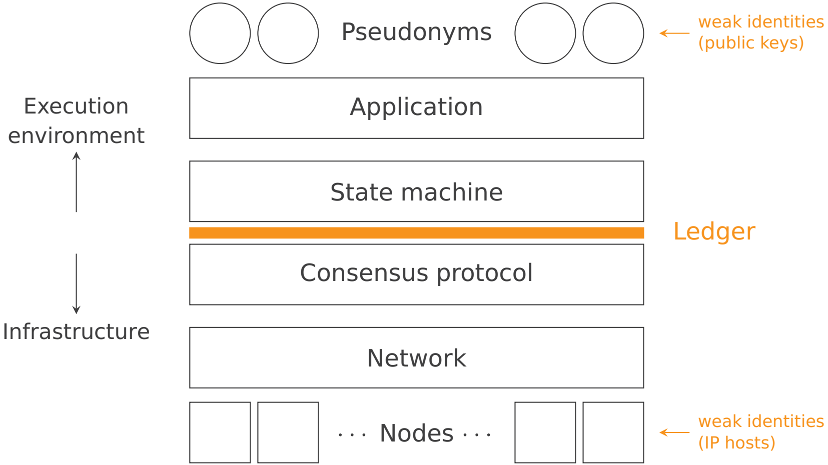
$$\sum_i u_i(\dots, a_i, \dots)$$

Types of Goods

	Excludable (access control)	Non-excludable
Rivalrous (externality)	**Private good**	**Common good**
Non-rivalrous	**Club good**	**Public good**

blockchain read access → Public good

Technology Stack



Public Blockchains Need Cryptocurrencies

A public distributed ledger has characteristics of a **public good**.

- **Cost:** maintenance, in particular proof-of-work, born by nodes
- **Benefit:** depends on application, enjoyed by pseudonyms
- **Mismatch** in value, time, and parties !

Cross-layer incentive mechanism

Blockchain systems need a payment method, so that pseudonyms can pay nodes.

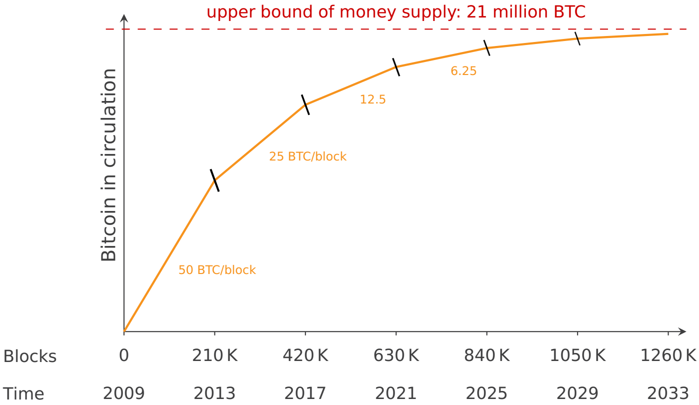
Two common schemes (also in combination):

1. Money creation ("minting") → all accounts pay by devaluation
2. Transaction tax ("fee") → individuals pay for write access

Note: Minting is often prescribed in the protocol, while fees are set (in principle) by market mechanisms at runtime.

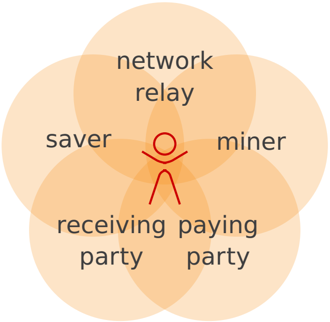
Bitcoin Minting Rewards

Nodes pay pseudonyms for the provision of a public good



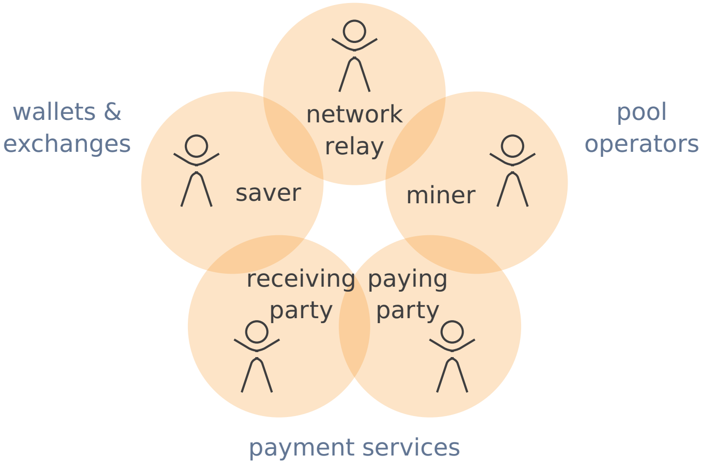
Different Roles of Network Participants

Satoshi's likely working assumption

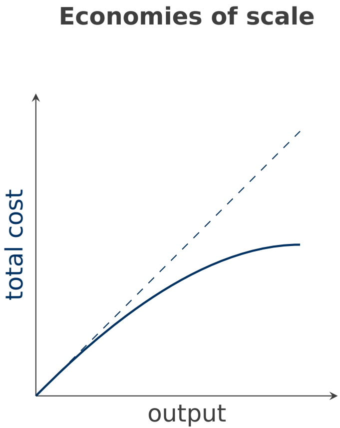


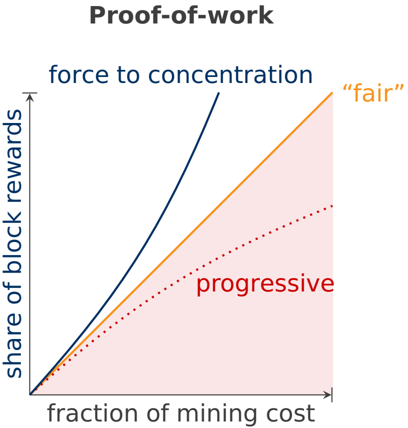
Different Roles of Network Participants

Specialization in the real world



The Enemy of Decentralization





The area under the diagonal (progressive) is not achievable with **weak identities**.

Incentive Compatibility

$$w(P) > w(\overline{P}) + s(\overline{P}) \quad (1)$$

$$\sum_{t=t_0}^{\infty} E\left[w_t(P)\right] \delta^{t-t_0} > \sum_{t=t_0}^{\infty} E\left[w_t(\overline{P})\right] \delta^{t-t_0} \quad (2)$$

$$u_P(w(P)) - c(P) > u_{\overline{P}}(w(\overline{P})) - c(\overline{P}) + s(\overline{P}) \quad (3)$$

P	follow protocol	w	wealth in protocol coins
$\overline{P}$	worst of all other actions (attacks)	u	utility, reflecting real-world preferences
		c	cost in units of utility
δ	discount factor < 1, e.g., $\delta = .97$	s	side-payment (“bribe”, in varying units)

The Fallacy’s Origin

“The incentive may help encourage nodes to stay honest.

If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people [. . .], or using it to generate new coins.

He ought to find it more profitable to play by the rules, [. . .] than to undermine the system and the validity of his own wealth.”

Satoshi Nakamoto 2008, p. 4

Fallacy Continued

“[I]n in our PoS based protocol, malicious slot leaders [. . .] not only risk to forego any potential profit they would earn from behaving honestly but may also risk to lose equity.

Notice that slot leaders must have money invested in the system in order to be able to generate blocks and if an attack against the system is observed it might bring currency value down. [. . .]

Currently our rationality model does not formally encompass this attack strategy [. . .].”

A. Kiayias et al. CRYPTO 2017 (Ouroboros), p. 47

Behavior-regulating Assumptions

Building a bridge between distributed systems and economics:

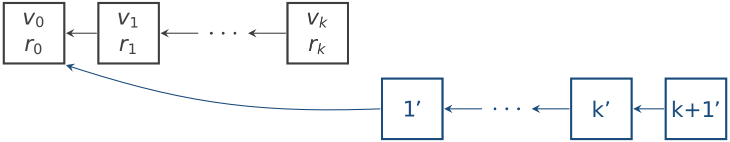
Secure Capacity Under the Longest Chain Rule

(against one type of economic attack $\Rightarrow$ lower bound)

λ bribe loading > 1

r block reward to miner

v double-spendable value



Security condition:

$$\sum_{i=1}^{k-6} v_k \quad < \quad \lambda \left(1 + k^{-1}\right) \sum_{i=1}^{k} r_i$$

Bonneau, J. *Why Buy When You Can Rent?* FC Workshops, 2016; Gervais, A. et al. *On the Security and Performance of Proof of Work Blockchains*. ACM CCS, 2016; Budish, E. *The Economic Limits of Bitcoin and the Blockchain*. 2018; Auer, R. *Beyond the Doomsday Economics of “Proof-of- Work” in Cryptocurrencies*. BIS, 2019. (and others)

Types of Goods

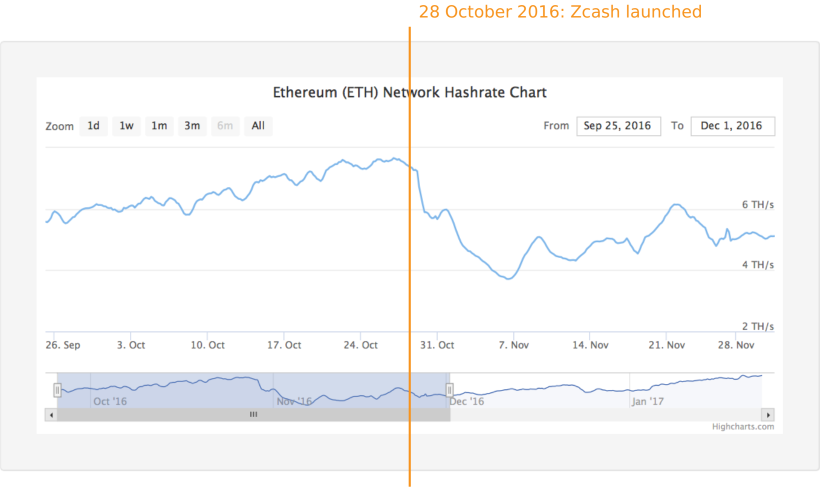
	Excludable (access control)	Non-excludable
Rivalrous (externality)	**Private good**	**Common good**
Non-rivalrous	**Club good**	**Public good**

blockchain secure capacity

Outline

1. Rational Agents and Adversaries
2. **Efficient Markets**
3. Market Concentration

Motivation

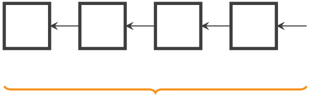


Source: coinwarz.com, accessed on 23 January 2017

Mining Resource Allocation as a Game

Two chains with compatible proof-of-work puzzles and fixed solving capacity:

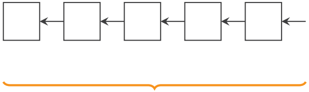
Chain A



expected utility 1 per period

Player i allocates mining power $a_i \in [0, 1]$.

Chain B



expected utility $\delta < 1$ per period

Player i allocates mining power $1 - a_i$.

Payoff function for two homogeneous and risk neutral miners i and $\neg i$

$$y_i = \frac{a_i}{a_i + a_{\neg i}} + \frac{\delta \cdot (1 - a_i)}{(1 - a_i) + (1 - a_{\neg i})}$$

utility $=$ return in fiat currency; expectations over realizations of r. v. and in anticipation of difficulty adjustments

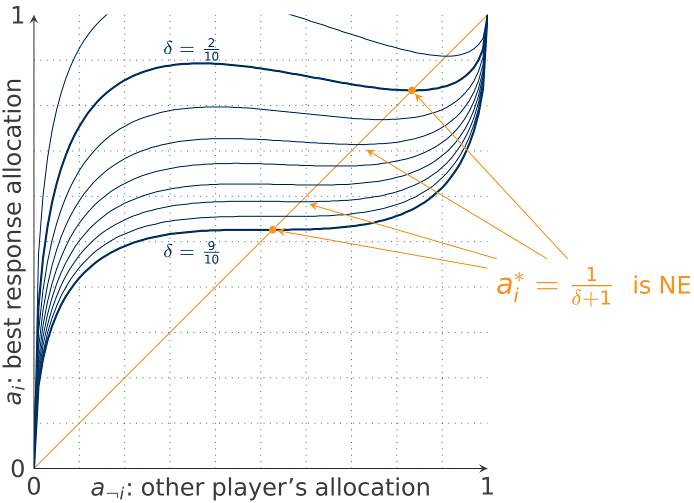
Step 1: Pure Allocations

Payoffs $(y_i, y_{\neg i})$ in normal form representation:

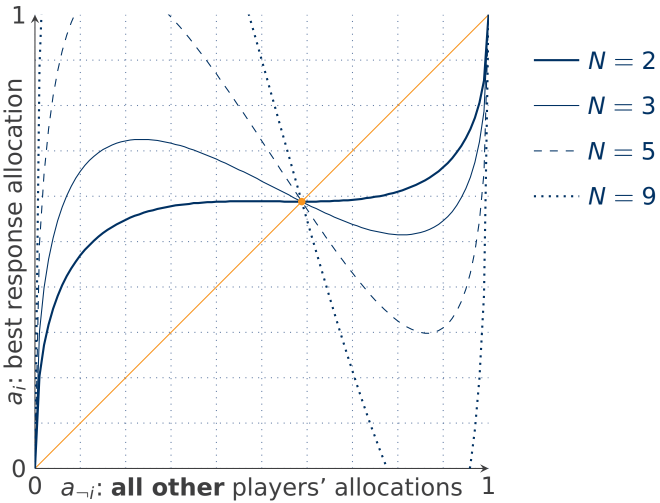
	Player $\neg i$	
	Chain A	Chain B
Player i	$a_{\neg i} = 1$	$a_{\neg i} = 0$
Chain A: $a_i = 1$	$\left(\frac{1}{2}, \frac{1}{2}\right)$	$(1, \delta)$
Chain B: $a_i = 0$	$(\delta, 1)$	$\left(\frac{\delta}{2}, \frac{\delta}{2}\right)$

1. "Greedy" is not a Nash equilibrium if $\delta > \frac{1}{2}$.
2. "Anti-greedy" is never an equilibrium.
3. Coordination on different chains are welfare-maximizing equilibria, but . . .

Step 2: Best Response for Mixed Allocations



Confirmation for $N \geq 2$ Symmetric Players

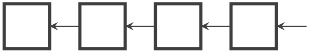


$\delta = \frac{7}{10}$

Mining Resource Allocation as a Game

Two chains with compatible proof-of-work puzzles and fixed solving capacity:

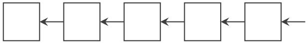
Chain A



expected utility 1 per period

Player i allocates mining power $a_i \in [0, 1]$.

Chain B



expected utility $\delta < 1$ per period

Player i allocates mining power $1 - a_i$.

Parameter δ contains information on the **exchange rate ratio**

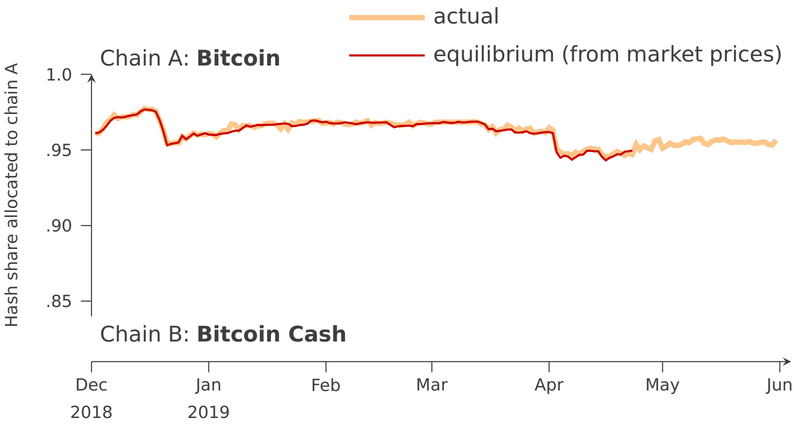
$$\delta = \frac{r_B}{r_A} \cdot \frac{p_B}{p_A} \cdot \frac{\Delta t_A}{\Delta t_B}$$

block rewards in units of cryptocurrency → r_B / r_A

target block times → $\Delta t_A / \Delta t_B$

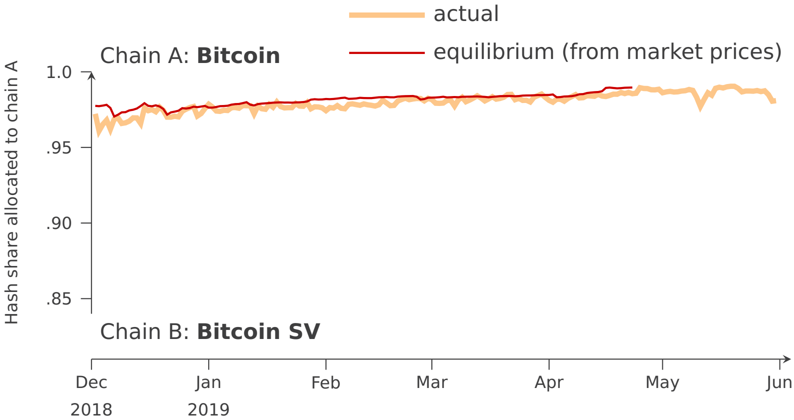
utility = **return in fiat currency**; expectations over realizations of r. v. and in anticipation of difficulty adjustments

Empirical Validation



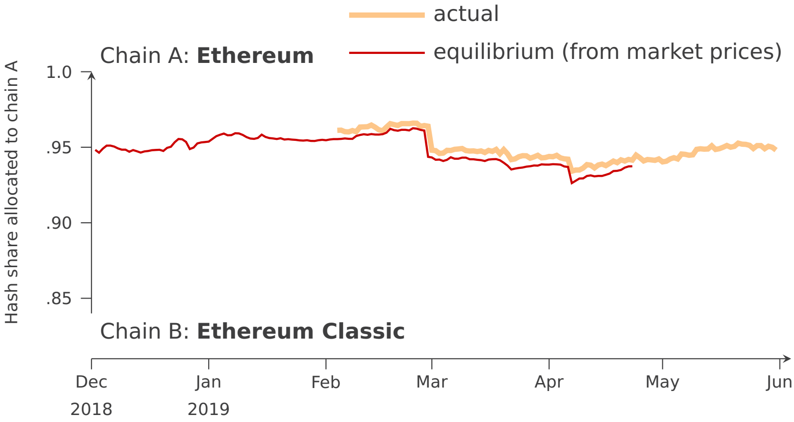
Bissias, G., Levine, B. N., and Thibodeau, D. *Greedy but Cautious: Conditions for Miner Convergence to Resource Allocation Equilibrium*. 2019. Data reused for own visualization with friendly permission.

Empirical Validation



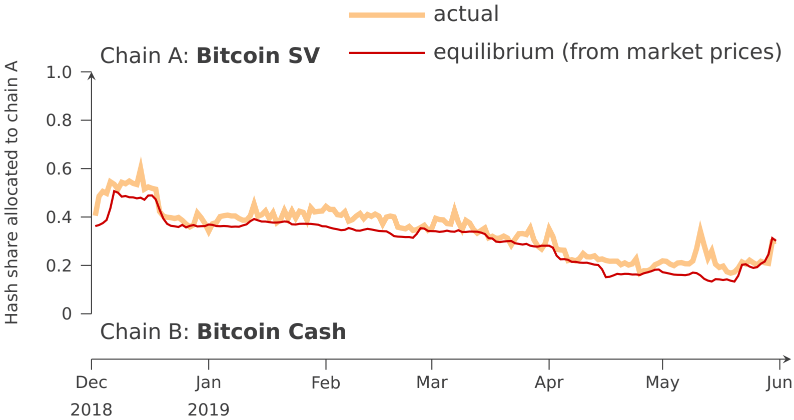
Bissias, G., Levine, B. N., and Thibodeau, D. *Greedy but Cautious: Conditions for Miner Convergence to Resource Allocation Equilibrium*. 2019. Data reused for own visualization with friendly permission.

Empirical Validation



Bissias, G., Levine, B. N., and Thibodeau, D. *Greedy but Cautious: Conditions for Miner Convergence to Resource Allocation Equilibrium*. 2019. Data reused for own visualization with friendly permission.

Empirical Validation



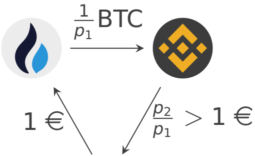
Bissias, G., Levine, B. N., and Thibodeau, D. *Greedy but Cautious: Conditions for Miner Convergence to Resource Allocation Equilibrium*. 2019. Data reused for own visualization with friendly permission.

Arbitrage

Definition Simultaneous purchase and sale of the same or a similar asset in two different markets for an almost risk-free profit

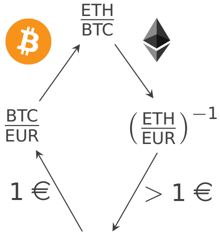
Between locations

(two-point arbitrage)

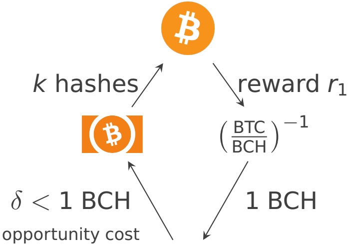


Between assets

(three-point arbitrage)



NEW: between chains



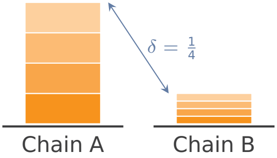
More important than arbitrage: **absence of arbitrage** $\Leftarrow$ economic equilibrium

Harrison, J. M. and Kreps, D. M. Martingales and Arbitrage in Multiperiod Security Markets. *Journal of Economic Theory*, 1979.

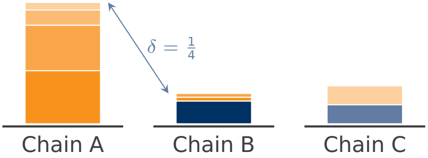
Efficient Markets

The **no-arbitrage condition** gives us the same equilibrium with fewer assumptions.

Our model



The real world



Rational pricing: every “irrational” behavior of some miner creates an arbitrage opportunity which is exploited for profit by at least one other miner.

Law of one price (blockchain version): the marginal miner can expect the same fiat return per hash on every chain.

Outline

1. Rational Agents and Adversaries
2. Efficient Markets
3. **Market Concentration**

How to Make Money

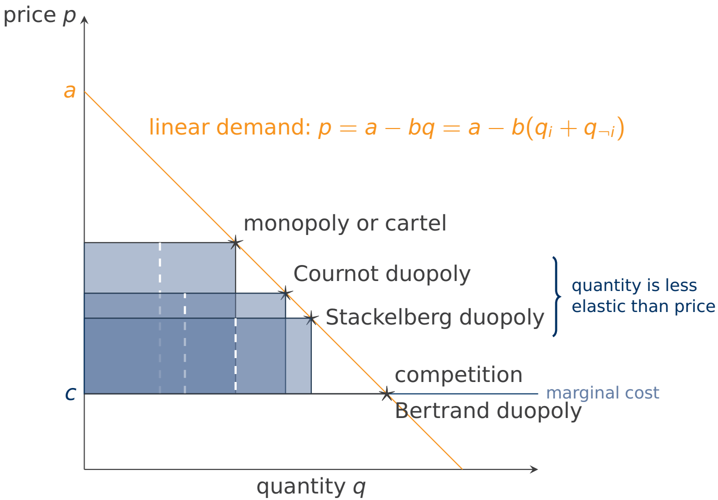
How Silicon Valley transformed investor mindsets:

Profit	**Revenue**	**"Eyeballs"**
1985	2000	2015

"bargain-then-ripoff"

The eyeballs metaphor is borrowed from Zuboff's 2015 essay on "surveillance capitalism".

Profit and Market Structure



Types of Goods

	Excludable (access control)	Non-excludable
Rivalrous (externality)	**Private good**	**Common good**
Non-rivalrous	**Club good**	**Public good**

blockchain write access

Quantity Decisions in Blockchain Space

- Mining power — unconventional economics: “contest”
- Permissionless blockchain space — competitive-then-price discriminating
- Permissioned blockchain space — cartel? Cournot?
- Differentiated virtual assets (tokens) — Bertrand?
- Off-chain payment channel capacity — Stackelberg? Cournot?
- Investment in gas options (storage space, gas tokens) — Stackelberg?
- . . .

$\rightarrow$ It requires some creativity to apply models of oligopoly from economics textbooks to markets governed by distributed ledgers. **Investors, beware.**

Dimitri, N. Bitcoin Mining as a Contest. *Ledger*, 2017.

Two Opposing Views

LINK TO PRIVACY !

Competition and the blockchain

optimistic | critical

"Monopoly without monopolist"

- Benefits of a single platform (mainly network effects)
- Decentralized operation avoids the dead-weight loss of monopolies.

"Tension between decentralized consensus and information distribution"

- Risk pooling gives power to specialized parties ($\rightarrow$ oligopoly of mining pools).
- Transparency encourages monitoring and punishment of deviant behavior ($\rightarrow$ cartel).
- Is coordination on the same protocol anti-competitive in the first place?

Huberman, G., Leshno, J. D. and Moallemi, C. *Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System*, 2017; Cong, L. W. and He, Z. Blockchain Disruption and Smart Contracts. *Review of Financial Studies* 32 (5), 2019. Malik, N. Aseri, M., Singh P. V. and Srinivasan, K. *Why Bitcoin will Fail to Scale*, WEIS 2019.

Summary

1. **Rational Agents and Adversaries**

   Bad news: rational attackers are (almost) as strong as Byzantine ones

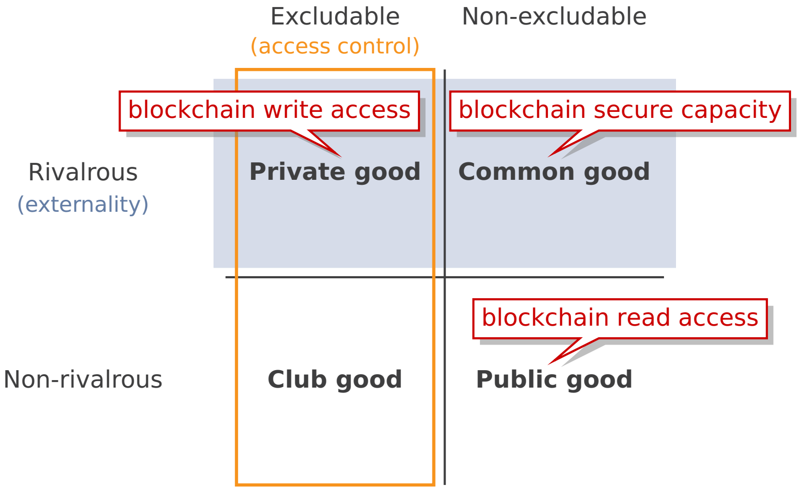
2. **Efficient Markets**

   Good news: efficient markets is where economic theory works (best)

3. **Market Concentration**

   Good news: blockchain (security) economics are sufficiently distinct to merit many exciting and interdisciplinary PhD theses . . .

Lesson Learned



What's Missing ?

Concepts omitted in this primer

- Time and repeated games
- Risk and uncertainty
- Information asymmetries
- Bounded rationality
- Econometrics

Other relevant **topics**

- Monetary economics
- Network economics & adoption
- Market mechanisms
- Economics of crime
- Economics of privacy

universität innsbruck

Thank you for your attention.

A Primer on Economics for Cryptocurrencies

rainer.boehme@uibk.ac.at