Rainer Böhme

universität innsbruck

The Bitcoin Economic Ecosystem

IACR Summer School on Blockchain Technologies
Corfu, Greece

Bitcoin and Economics

Motivating questions

- What does it take to engineer money ?
- How successful is Bitcoin and why ?
- How does Bitcoin change the world ?
- Can Bitcoin serve as a social science laboratory ?

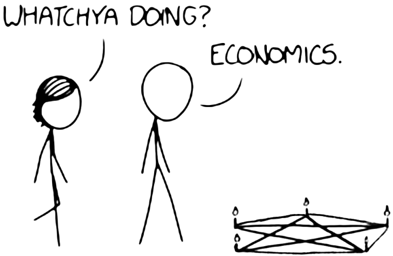
- Does my Bitcoin client act in my best interest ?
- Can we enforce the protocol rules ?
- Can we preserve decentralization ?

Functions of Money

Economists define money by its functions, not its form.

1. Medium of exchange
   → engineering task: enable secure and cheap transfer of digital property
2. Unit of account
   → technical divisibility, social conventions, individual behavior
3. Store of value
   → long-term expectations, future behavior

Economics

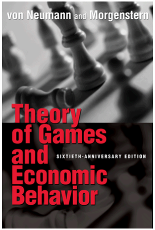


~~predict~~ behavior

model

Illustration: xkcd.com

Game Theory



A mathematical approach to modeling strategic behavior

Interpretation as generalization of . . .

a. **Probability theory** – replace randomness 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. Nodes are agents – "players".

Bitcoin and Economics

Motivating questions

- What does it take to engineer money ?
- How successful is Bitcoin and why ?
- How does Bitcoin change the world ?
- Can Bitcoin serve as a social science laboratory ?

- Does my Bitcoin client act in my best interest ?
- Can we enforce the protocol rules ?
- Can we preserve decentralization ?

Principles of Network Economics

Economics

- 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.

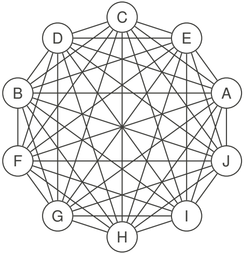
$$u_j(\ldots, a_i, \ldots)$$

Network externality – special case

- Binary actions: join or not to join. Each agent's benefit of joining a network grows with the fraction of agents who join, $q \in [0, 1]$.

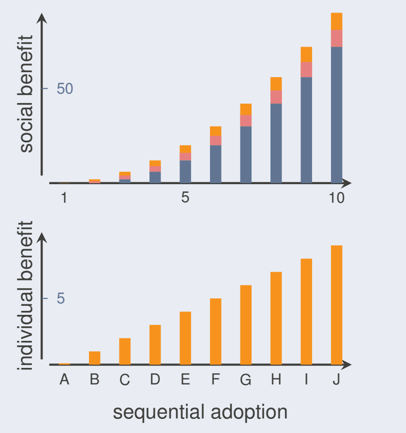
Network Externalities

Connections create utility.



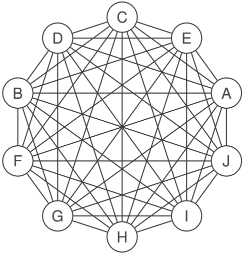
“The value of a network is super-linear in the number of its users.”

Value of the network



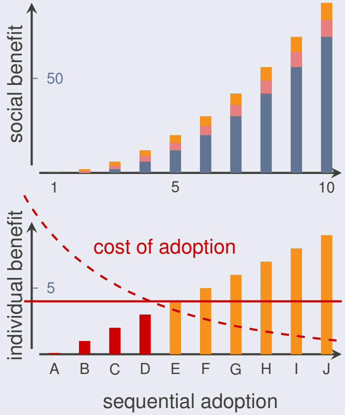
Network Externalities (cont'd)

Connections create utility.



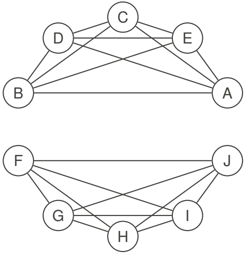
→ critical mass

Value of the network



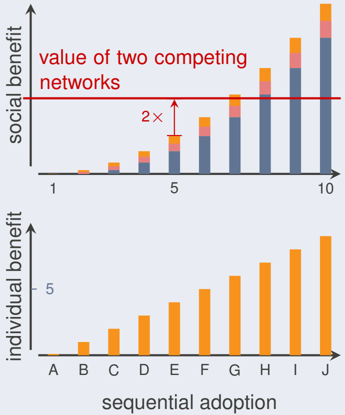
Network Externalities (cont’d)

Connections create utility.



→ natural monopoly

Value of the network



Principles of Network Economics (cont'd)

Adoption decision

- Join network if benefit outweighs cost. This is less likely if q is small.
- No agent is willing to adopt alone, but all agents could benefit if they collectively agree to adopt. → social coordination problem

RFC 5218 lists means to facilitate solutions to this problem.

Timing and uncertainty

- Costs are one-off, sunk, and certain.
- Benefits are uncertain and accumulate over time.

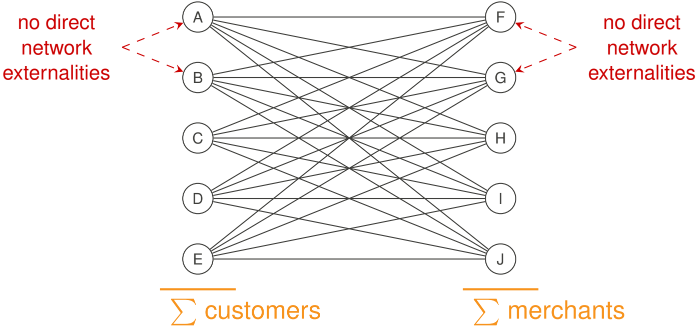
Deadlock if all agents wait to reduce uncertainty.

Network topology

- Example: bipartite graph of merchant–customer relations
- Indirect network externalities depend on q' of the other side.

Network Externalities on Special Topologies

Connections create utility – bipartite graph with two agent types


no direct network externalities
A
B
C
D
E
F
G
H
I
J
no direct network externalities
$\overline{\sum \text{customers}}$
$\overline{\sum \text{merchants}}$

Bitcoin’s Starting Position

A list of barriers:

1. failed attempts to establish crypto cash in the 1990/00s
2. dominant and well capitalized incumbents in e-payments
3. glitches and breaches at key players in the ecosystem
4. adverse press, “friendly fire” (e.g., by the EFF)
5. associations with crime, for good reasons
6. legal uncertainty for early adaptors
7. threat of government intervention
8. speculative attacks

Gloomy starting position compared to most Internet protocols.

Bitcoin’s Success Factors

1. **Built-in reward system for early adaptors** — transferable
    - Miners earn shares at an exponentially declining rate; with control loop to adjust difficulty for speed of uptake.

   Addresses social coordination problem.

2. **Adapters in the ecosystem** — transferable
    - Exchanges provide interfaces to conventional payment systems, converting indirect into direct network externalities.

   Resolves unwieldy merchant–customer topology.

3. **Interpretation as money** — not transferable
    - Store of value to solve inter-temporal matching problem of exchange economies.

   Fixes timing (and creates self-fulfilling prophecy).

One More Factor

What success factor have Bitcoin, BitTorrent, and Tor in common ?

Bitcoin as a Model ?

Fall **2013**, IAB/IETF Workshop on Internet Protocol Adoption:

IPv6	IETF standard since 1998	$<$ 2 % adoption
Bitcoin	whitepaper 2008	1 BTC $\approx$ 1 000 USD

Spring **2016**, Corfu BTC school

IPv6	$\approx$ 12 % adoption, doubled in 12 months
Bitcoin	1 BTC $\approx$ 530 USD

Bitcoin and Economics

Motivating questions

- What does it take to engineer money ?
- How successful is Bitcoin and why ?
- How does Bitcoin change the world ?
- Can Bitcoin serve as a social science laboratory ?

- Does my Bitcoin client act in my best interest ?
- Can we enforce the protocol rules ?
- Can we preserve decentralization ?

Size of the Bitcoin Economy

	Euro area		Bitcoin	
Market capitalization			7	110.0
Currency in circulation	1 052	5.9		
Overnight deposits	5 712	11.0		
M1	6 767	10.1		
M3	10 998	5.0		

Levels in billion EUR. Annual growth rates in %.

ECB (March 2016, published 27 April 2016), blockchain.info (30 May 2016)

Scarcity

For a moment: the difficulty of printing money makes a currency valuable.

Bakia

Galia

Gulden

Ionian obol

Bitcoin

For the first time in history, we have **absolute scarcity** tied to the closure of a mathematical expression.

Image source: Money Museum

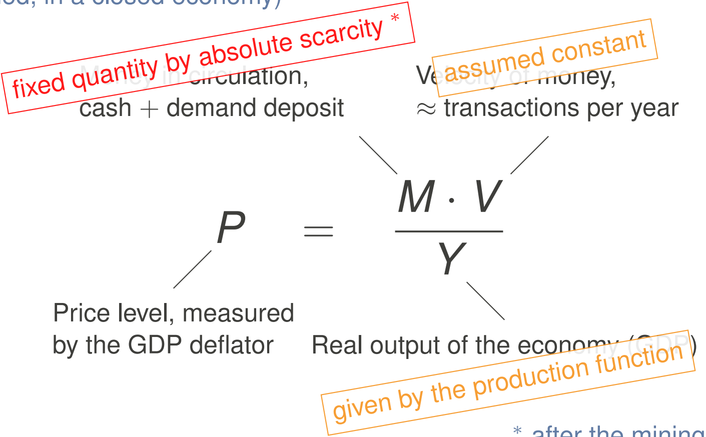
Implications of Absolute Scarcity

No more inflation ?

Curb sovereign debt ?

Quantity Theory of Money

(simplified, in a closed economy)



fixed quantity by absolute scarcity *

Money in circulation,
cash + demand deposit

assumed constant

Velocity of money,
≈ transactions per year

$$P = \frac{M \cdot V}{Y}$$

Price level, measured
by the GDP deflator

Real output of the economy (GDP)

given by the production function

* after the mining phase

Production Function

(Cobb–Douglas model, constant returns to scale)

Real value of all goods and services (GDP)

Output elasticity of production factors

$$Y = A \cdot L^{\alpha} \cdot K^{(1-\alpha)}$$

Capital input: accumulation

Labor input: population growth ?

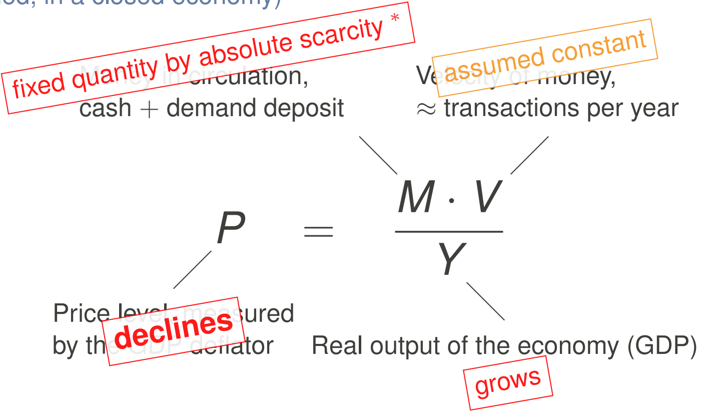
Total factor productivity: technological innovation

Economic growth

Trying to fix the size of the economy means: stop doing research!

Quantity Theory of Money

(simplified, in a closed economy)



fixed quantity by absolute scarcity *

Money in circulation,
cash + demand deposit

assumed constant

Velocity of money,
≈ transactions per year

$$P = \frac{M \cdot V}{Y}$$

Price level, measured
by the GDP deflator

declines

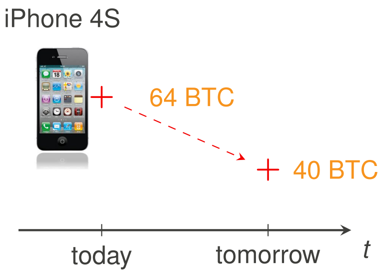
Real output of the economy (GDP)

grows

* after the mining phase

Deflation

(example from fall 2012)



iPhone 4S

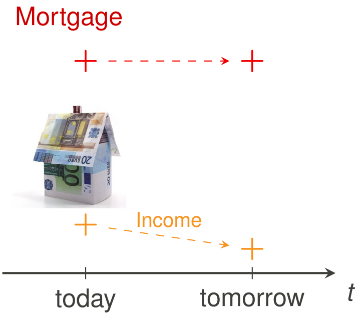
64 BTC

40 BTC

today

tomorrow

t



Mortgage

Income

today

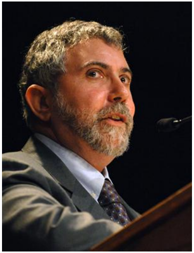
tomorrow

t

Vicious circle

Consumers postpone purchase decisions. Prices fall further.
Enterprises disinvest and cut jobs.

Attribution



Paul Krugman

"To the extent that the [Bitcoin] experiment tells us anything about monetary regimes, it reinforces the case against anything like a new gold standard – because it shows just how vulnerable such a standard would be to money-hoarding, deflation, and depression."

http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/, 7 Sep 2011

Why Depression ?

(Cobb–Douglas model, constant returns to scale)

Real value of all goods and services (GDP)

Equilibrium condition

Demand

$$Y = A \cdot L^{\alpha} \cdot K^{(1-\alpha)} = D$$

Capital input

Labor input

Total factor productivity

Implications of Absolute Scarcity

No moremonetary inflation ?

- Yes, but no guarantee for price stability.
- Risk of deflation.

Curb sovereign debt ?

- Governments borrow against future tax revenues as collateral.
- If sovereign debt is (was) too cheap in real terms, why should the markets err only and consistently on inflation expectations ?
- In principle, Bitcoin could become another reserve currency.

Can We Find a Better Balance ?

Fix the difficulty

$\neq$ fix value

- The relative value of CPU cycles to the rest of Y may change.
- Crypto currency loses its $\{$absolute $|$ predictable$\}$ scarcity.

Fix the exchange rate

- Needs feedback from outside the closed system (exchanges)
- Point of attack until *everything* is digital and cryptographic

Central bank policy: discretion versus rules

Predated by Milton Friedman's proposal of a *k*-percent rule in 1960.

Key questions:

- Do strategy-proof rules exist in practice ? e. g., Taylor 1993
- Does the block chain contain all information to implement them ?

Government Intervention

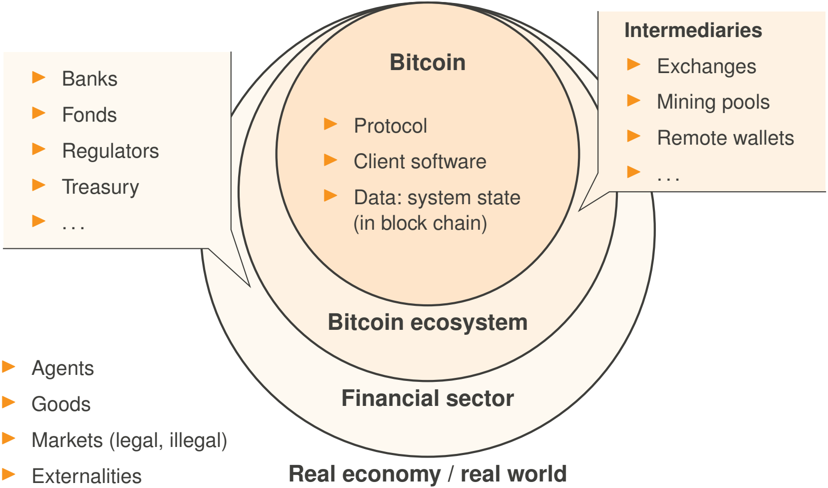
Why regulate ?

- Consumer protection – at small and at large (financial stability)
- Fighting and preventing crime – AML, CTF
- Fixing market failure – internalize externalities, hope for growth
- Controlling monetary supply – monetary and economic policy
- Securing a tax base – provision of public goods, redistribution

And why not (now) ?

- No way – wishful thinking
- Too marginal
- Wait and see – international coordination
- Encroachment on fundamental rights – a constraint

Bitcoin in Context



Bitcoin

- Protocol
- Client software
- Data: system state (in block chain)

Bitcoin ecosystem

Intermediaries

- Exchanges
- Mining pools
- Remote wallets
- . . .

Financial sector

- Banks
- Fonds
- Regulators
- Treasury
- . . .

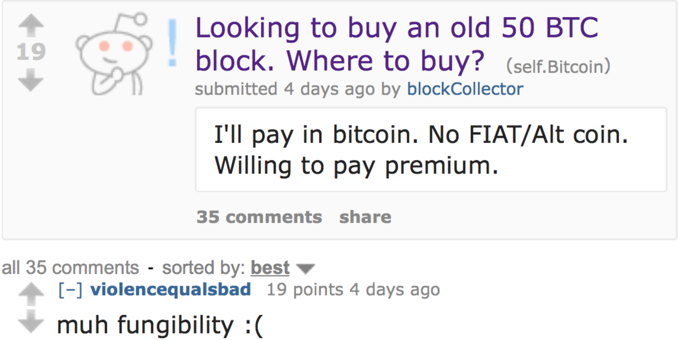
Real economy / real world

- Agents
- Goods
- Markets (legal, illegal)
- Externalities

Fungibility

Every Bitcoin has a unique history documented in the block chain.

One of the most contentious issues in Bitcoin:



19

Looking to buy an old 50 BTC block. Where to buy? (self.Bitcoin)

submitted 4 days ago by blockCollector

I'll pay in bitcoin. No FIAT/Alt coin. Willing to pay premium.

35 comments share

all 35 comments - sorted by: best

[–] violencequalsbad 19 points 4 days ago

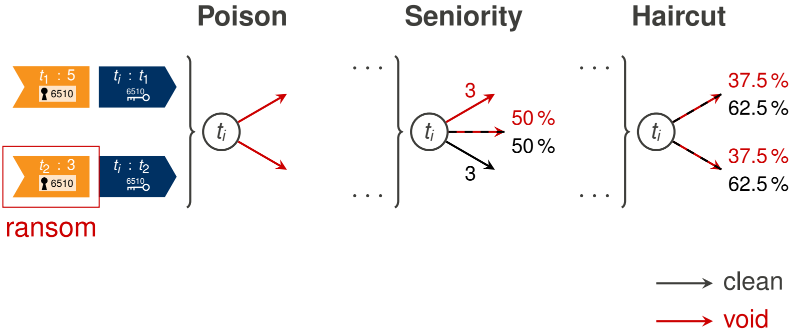
muh fungibility :(

Source: reddit.com, November 2015

Blacklisting Policies

An independent blacklisting infrastructure

- can be an overlay on the block chain
- references transactions (not addresses)
- may discourage crime and dry out anonymizers



Bitcoin and Economics

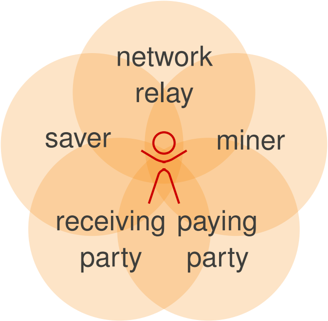
Motivating questions

- What does it take to engineer money ?
- How successful is Bitcoin and why ?
- How does Bitcoin change the world ?
- Can Bitcoin serve as a social science laboratory ?

- Does my Bitcoin client act in my best interest ?
- Can we enforce the protocol rules ?
- Can we preserve decentralization ?

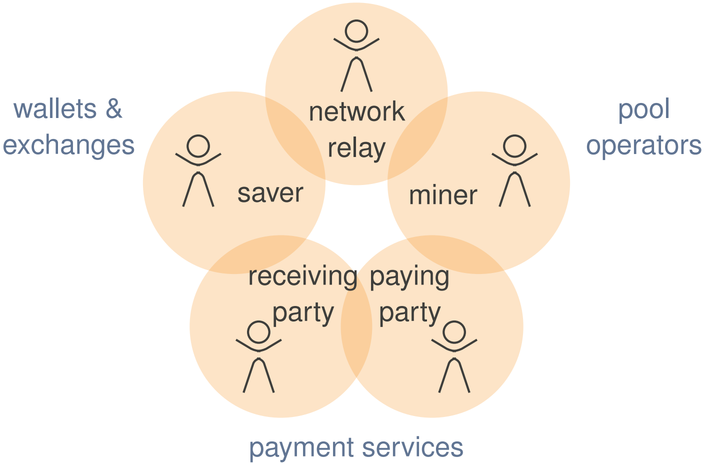
Different Roles of Network Participants

Satoshi's likely working assumption



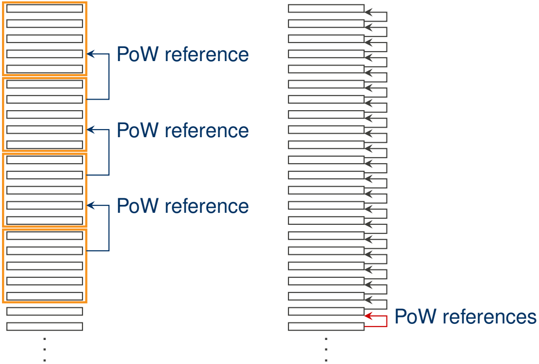
Different Roles of Network Participants

Specialization in the real world



Why Blocks ?

Alternative PoW-based back-off for every record (transaction)



Stronger Together

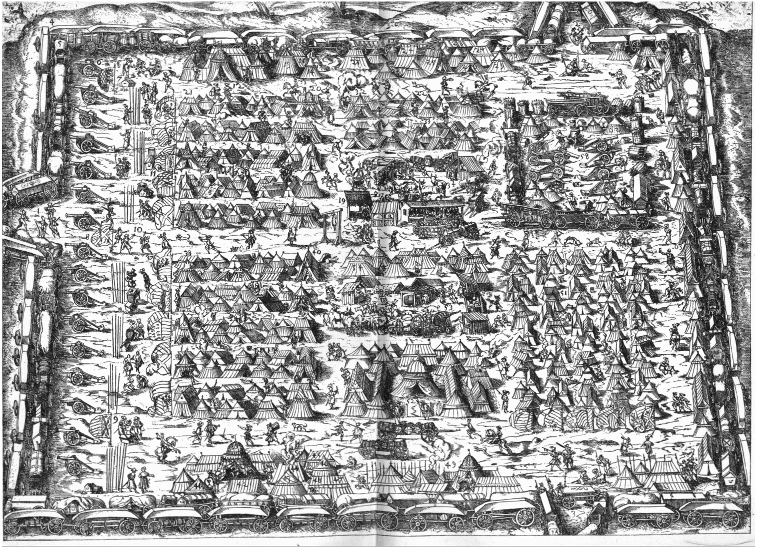


Image source: Wikimedia Commons, public domain

The Block Chain as a Public Good ?

Public Choice 41: 371-386 (1983)
© 1983 Martinus Nijhoff Publishers, The Hague. Printed in the Netherlands

From weakest-link to best-shot:
The voluntary provision of public goods

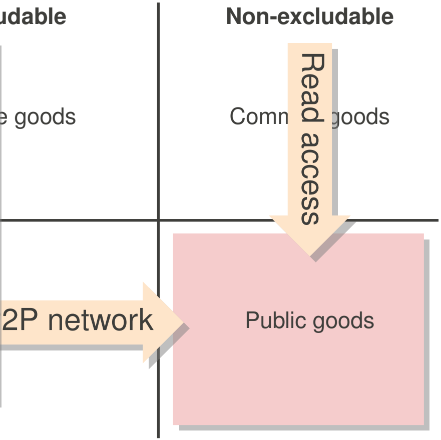
JACK HIRSHLEIFER*

Abstract

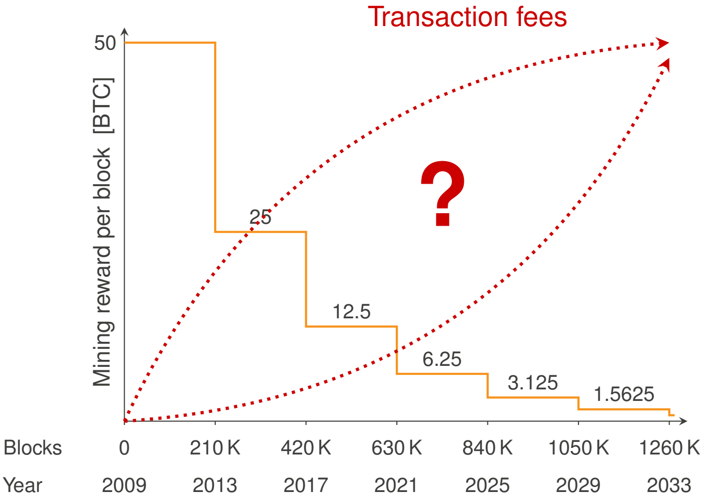
It has traditionally been assumed that the socially available amount X of a public good is the simple sum of the separate amounts x_i produced by the $i = 1, \ldots, \bar{I}$ members of the community. But there are many other possibilities of practical importance. Among them are: (i) Weakest-link rule, where the socially available amount is the *minimum* of the quantities individually provided, and (ii) Best-shot rule, where the socially available amount is the *maximum* of the individual quantities. The former tends to arise in linear situations, where each individual has a veto on the total to be provided (e.g., if each is responsible for one link of a chain); the latter tends to arise when there is a single prize of overwhelming importance for the community, with any individual's effort having a chance of securing the prize.

In comparison with the standard Summation formula of ordinary public-good theory, it is shown that underprovision of the public good tends to considerably moderated when the Weakest-link function is applicable, but aggravated when the Best-shot function is applicable. In time of disaster, where the survival of the community may depend upon each person's doing his duty, the conditions for applicability of the Weakest-link rule are approximated. This circumstance explains the historical observation that disaster conditions tend to elicit an extraordinary amount of unselfish behavior.

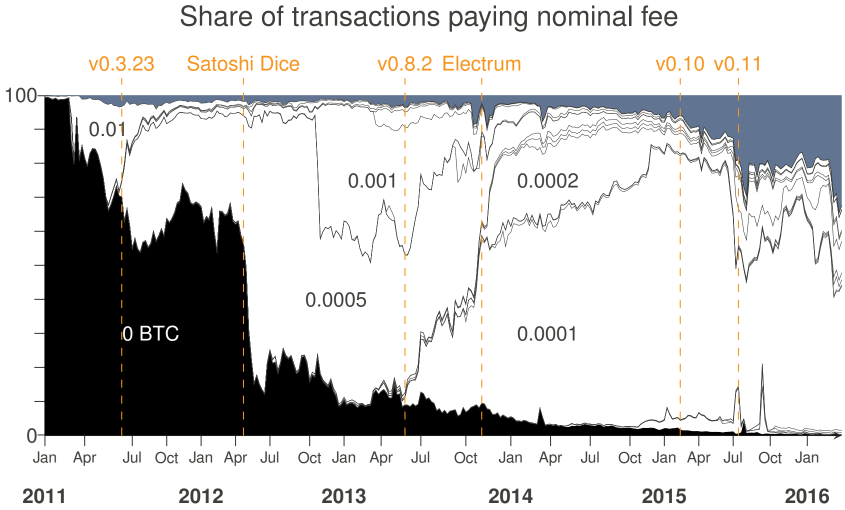
cf. Hirshleifer 1983



Mining Rewards



Transaction Fees Over Time



updated from Möser & Böhme 2015

Are Fair Transaction Fees Possible ?

Cost to others arise in two forms

- Proof-of-work → *miners*
- Storing the transaction record → *all full nodes*

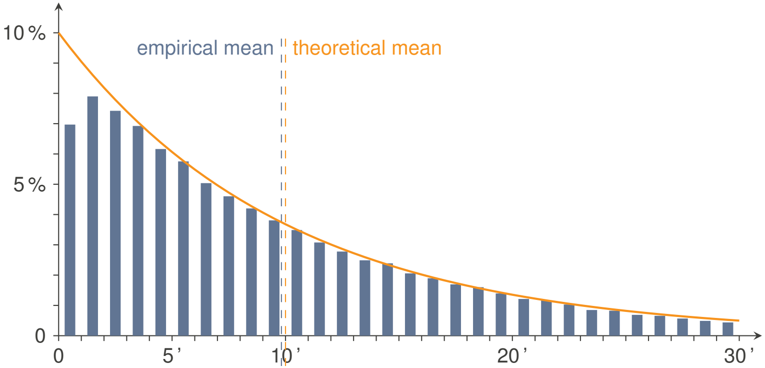
Factors influencing the cost

	Known at the time of creation
Transaction size	✓
Time until all outputs are spent	X
Number of redundant copies in the network	X

Monetary inflation might be a closer approximation than fees.

Getting It Right on Average is Not Enough

Example: distribution of block inter-arrival time

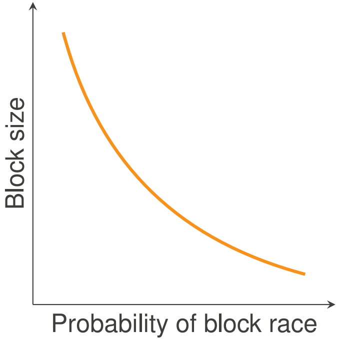


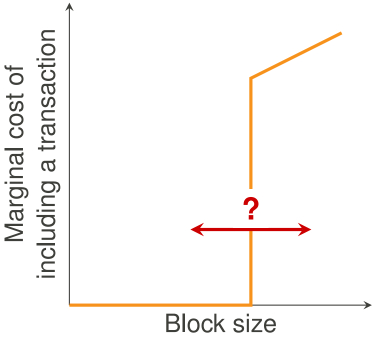
Risk of block race: $P(\Delta t = 5\,'') = 0.8\,\%$, $P(\Delta t = 12\,'') = 2.0\,\%$, ...

Data: Jan–Dec 2014

Factors Influencing Miners’ Best Responses

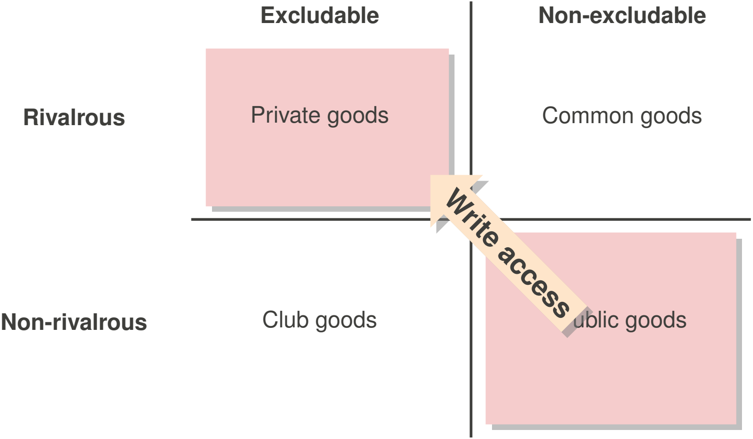
Stylized examples





Problem: standard economic models assume smooth functions.

The Block Chain as a Private Good ?



	Excludable	**Non-excludable**
Rivalrous	Private goods	Common goods
Non-rivalrous	Club goods	ublic goods

Known Issues

Information withholding

- Selfish mining — Eyal and Sirer 2014, Sapirshtein et al. 2016
- Selective transaction forwarding — Babaioff et al. 2012

Loose coupling

- Empty blocks — Hoey 2014a
- Externalities and transaction fees — Hoey 2014b, Möser and Böhme 2015
- Pool hopping (in early mining pools) — Rosenfeld 2011, Joe Bonneau's talk
- Rewarding early adopters — Böhme 2014

Preserving decentralization

- Only under adversarial settings — Johnson et al. 2014, Eyal 2015

Bitcoin is approximately incentive compatible at best.

Take Home Messages

- Bitcoin is closer to a (long-running) *payment* protocol than a substitute for *money* in the economic or *currency* in the legal sense.
- It is an open question whether crypto currencies can implement meaningful monetary policy and if this is socially desirable.

- Bitcoin depends on its ecosystem consisting of (competing) centralized parties.
- There may be reasons to regulate Bitcoin. Regulators $\{$c$\|$sh$\}$ould target the ecosystem.
- Transaction blacklisting is possible because bitcoins are not fungible.

- Many parties follow conventions against their own best interest.
- Protocols should avoid discontinuities for better tractability of the economic analysis. (e. g., use lotteries with caution)

Bitcoin and Economics

Motivating questions

- What does it take to engineer money ?
- How successful is Bitcoin and why ?
- How does Bitcoin change the world ?
- Can Bitcoin serve as a social science laboratory ?

- Does my Bitcoin client act in my best interest ?
- Can we enforce the protocol rules ?
- Can we preserve decentralization ?

- **Can we design more predictable protocols ?**

Plug

We have tried 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