universität innsbruck

Incentives Matter

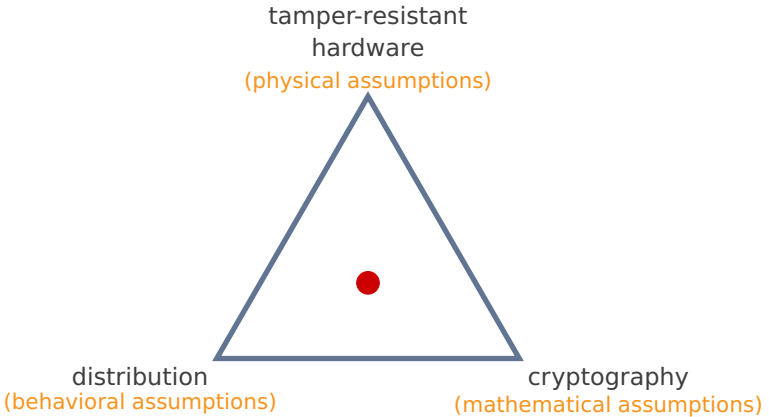
On the Economics and Governance of Blockchain-based Systems

Rainer Böhme

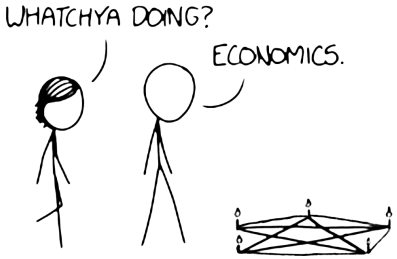
The Hopes of 2015

The Economist, 31 November 2015

Sources of Trust



Economics



~~predict behavior~~

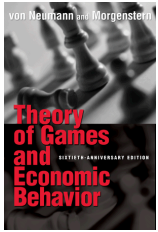
model

Illustration: xkcd.com

Agenda

1. Introduction
2. **Rational Agents and Adversaries**
3. Explaining System Behavior with Externalities
   Adoption · Maintenance · Governance
4. On the Nature of Money

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. Users are agents – "players".

Formalizing Rationality

A **strategic game** Γ is a triple $(N, S, \succeq)$, where:

$N = \{1, \ldots, n\}$	finite set of players
S_i	finite set of strategies (actions), available to player i
$S := S_1 \times \ldots \times S_n$	finite set of strategy profiles
$\succeq_i \subseteq S \times S$	preference relation of player i on S

The preferences of player i are often specified by a **utility function** u_i

$$u_i : S \to \mathbb{R} \quad \forall\, i \in N,$$

where:

$$\begin{aligned}
\boldsymbol{a} \succeq_i \boldsymbol{b} \quad &\Leftrightarrow \quad u_i(\boldsymbol{a}) \geq u_i(\boldsymbol{b}) \quad \forall\, \{\boldsymbol{a}, \boldsymbol{b}\} \in S, \\
\boldsymbol{a} \succ_i \boldsymbol{b} \quad &\Leftrightarrow \quad u_i(\boldsymbol{a}) > u_i(\boldsymbol{b}) \quad \forall\, \{\boldsymbol{a}, \boldsymbol{b}\} \in S, \\
\boldsymbol{a} \sim_i \boldsymbol{b} \quad &\Leftrightarrow \quad u_i(\boldsymbol{a}) = u_i(\boldsymbol{b}) \quad \forall\, \{\boldsymbol{a}, \boldsymbol{b}\} \in S.
\end{aligned}$$

Example: Backoff-Mechanism for Media Access

- Transmission of data packets over a shared medium
  - **correct:** wait for a random period of time before retransmission after collision (back-off)
  - **defect:** no back-off mechanism
- Two network users with strategies $S_i = \{\text{correct, defect}\}\ \forall\ i \in \{1, 2\}$
- Average paket delay as (negative) utility function

User 1 \ User 2	correct	defect
correct	–1, –1	–4, 0
defect	0, –4	–3, –3

Nash equilibrium:
(defect, defect)

A **Nash equilibrium** is a stable state, in which no player can gain an advantage by changing the strategy, assuming that all other players do not change their strategies.

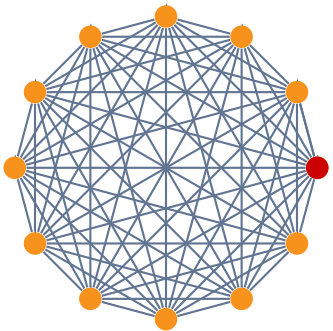
Weak Identities

Games on networks 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

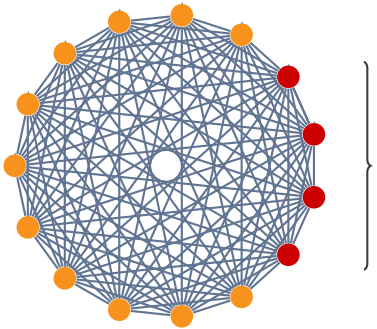
Games on networks without central identity provider:



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.

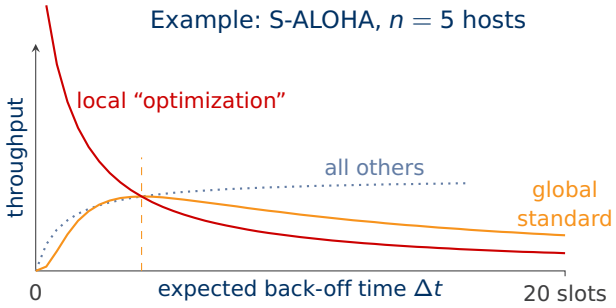
Weak Identities

Games on networks 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.

Detour: Public Blockchains as Shared Medium

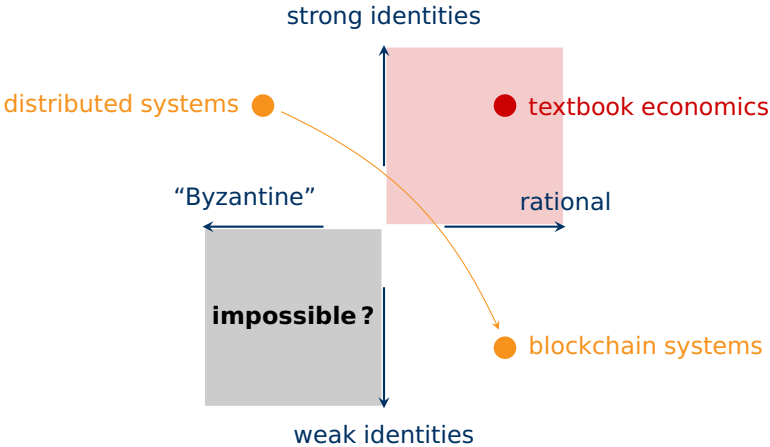


- Every node wants to append its transactions first.
- There is no way to enforce a random back-off (“oops, I’m lucky again”)

Solution: The probabilistic proof-of-work algorithm imposes a self-enforcing rate limit for block completion.

Lessons Learned

Systematizing behavior-regulating assumptions:



Agenda

1. Introduction
2. Rational Agents and Adversaries
3. **Explaining System Behavior with Externalities**
   Adoption · Maintenance · Governance
4. On the Nature of Money

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.

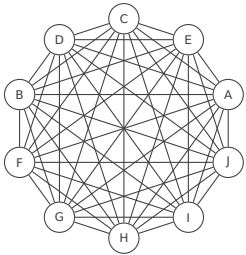
$$u_j(\ldots, a_i, \ldots)$$

Network externality – special case

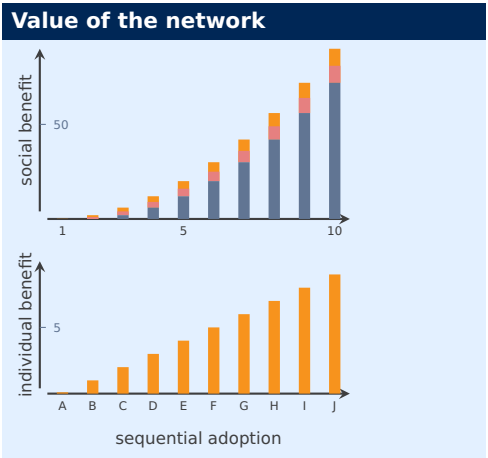
- Binary actions: join or not to join. Each agent's benefit of joining a network grows with the fraction of agents who join, $q \in [0, 1]$.

Network Externalities

Connections create utility.

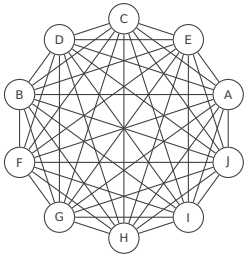


“The value of a network is super-linear in the number of its users.”

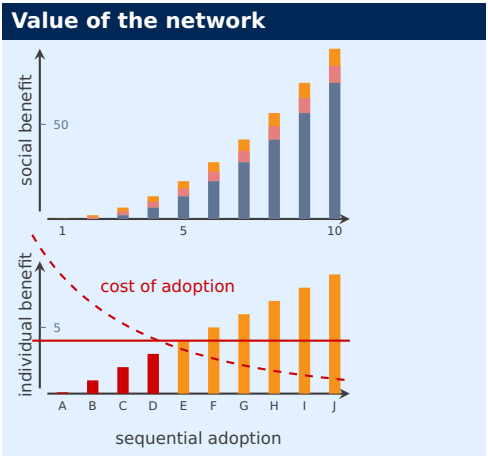


Network Externalities (cont'd)

Connections create utility.

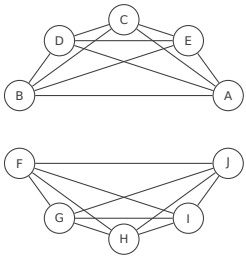


→ critical mass

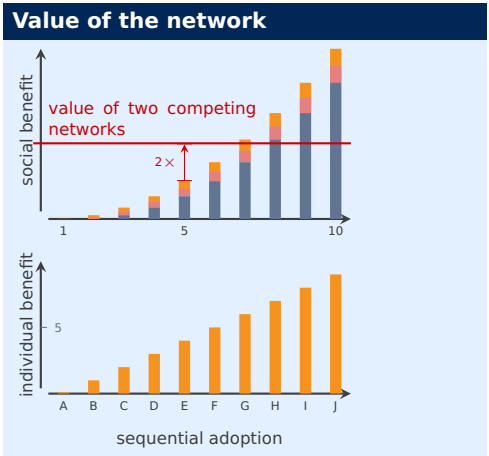


Network Externalities (cont'd)

Connections create utility.



→ natural monopoly



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. $\rightarrow$ 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.

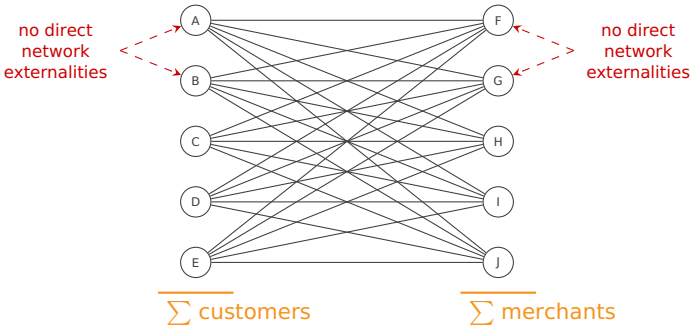
Deadlock if all agents wait to reduce uncertainty.

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



2009, . . . , 2011, 2012: 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

Bitcoin had a gloomy starting position compared to most Internet protocols.

Böhme, R. *Internet Protocol Adoption: Learning from Bitcoin.* 2013. IAB Workshop on Internet Technology Adoption and Transition (ITAT), Cambridge, England.

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?

The BITCRIME research project: https://www.bitcrime.de

Agenda

1. Introduction
2. Rational Agents and Adversaries
3. **Explaining System Behavior with Externalities**
   Adoption · **Maintenance** · Governance
4. On the Nature of Money

Searching for Dynamic Steady States

Blockchain-based systems have many moving parts.

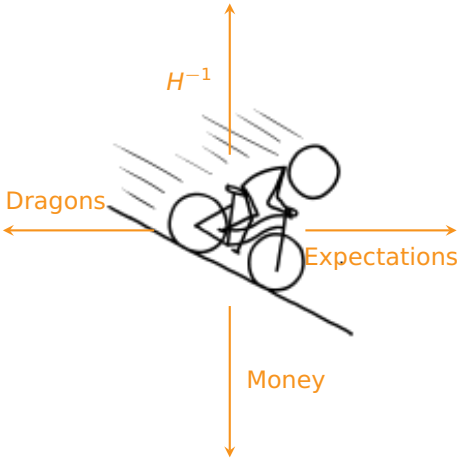
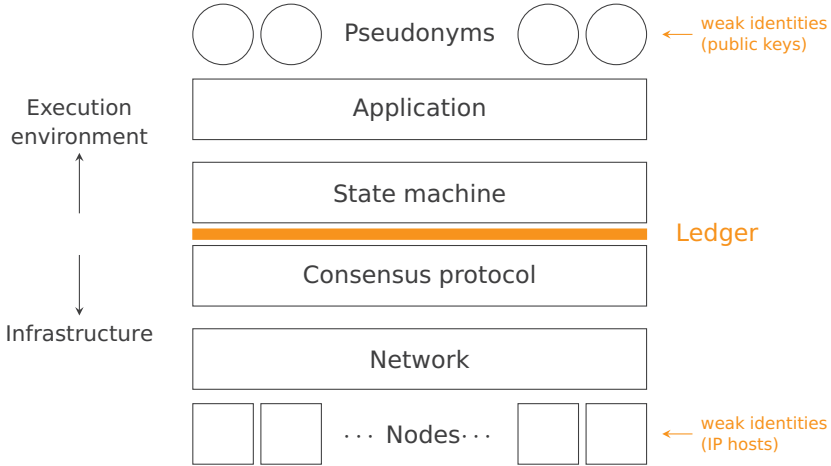


Image source: xkcd.com

Technology Stack



Compensation for Infrastructure Service

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

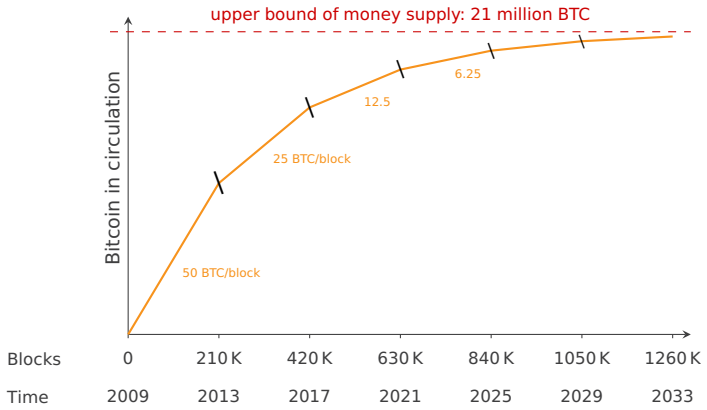
Blockchain systems need a payment method, so that pseudonyms can pay nodes.

Two common schemes (also in combination):

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

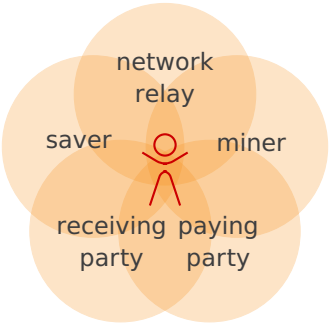
Note: Minting is often prescribed in the protocol, while fees are set (in principle) by market mechanisms at runtime.

Bitcoin Minting Rewards

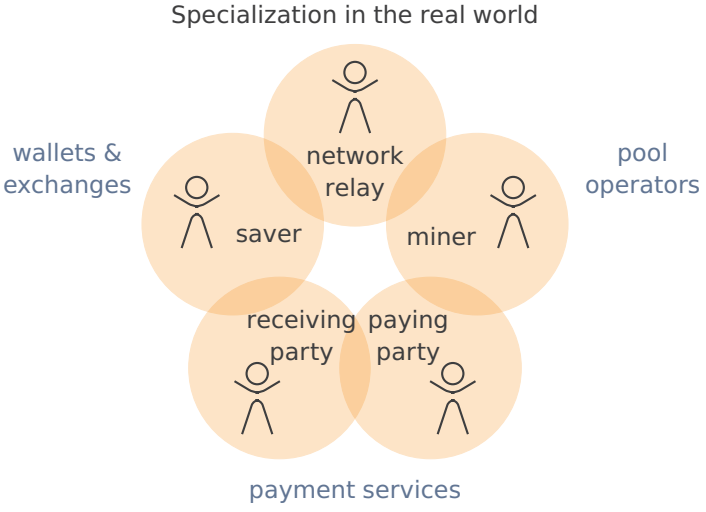


Different Roles of Network Participants

Satoshi's likely working assumption

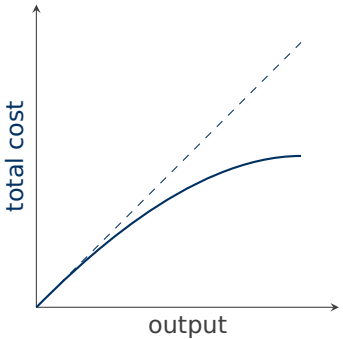


Different Roles of Network Participants

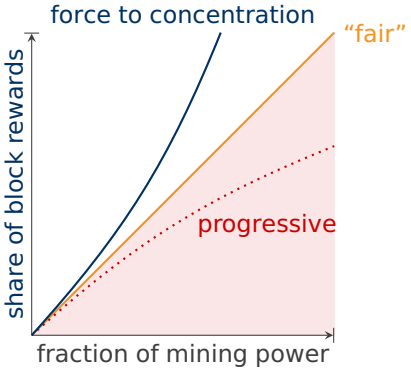


The Enemy of Decentralization

Economies of scale



Proof-of-work



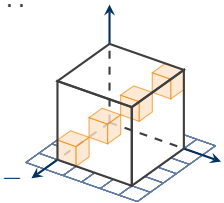
The area under the diagonal (progressive) is not achievable with **weak identities**.

Agenda

1. Introduction
2. Rational Agents and Adversaries
3. **Explaining System Behavior with Externalities**
   Adoption · Maintenance · **Governance**
4. On the Nature of Money

Governance

Question Who decides about the (further) development of a blockchain system?
Developer community, users, miners, firms, nation states, . . .



How do we find consensus on the consensus mechanism?

Model as **coordination game** in strategic form:

Player 1 \ Player 2	Protocol A	Protocol B
Protocol A	1, 1	0, 0
Protocol B	0, 0	1, 1

Nash equilibria

Schelling, T. *The Strategy of Conflict*, Wiley, 1960.

Signals

How does a running system find other possible Nash equilibria?

(Classical game theory is silent about the problem of which of many equilibria is reached.)

- Participants agree on **symbols** to communicate their response to other strategies.

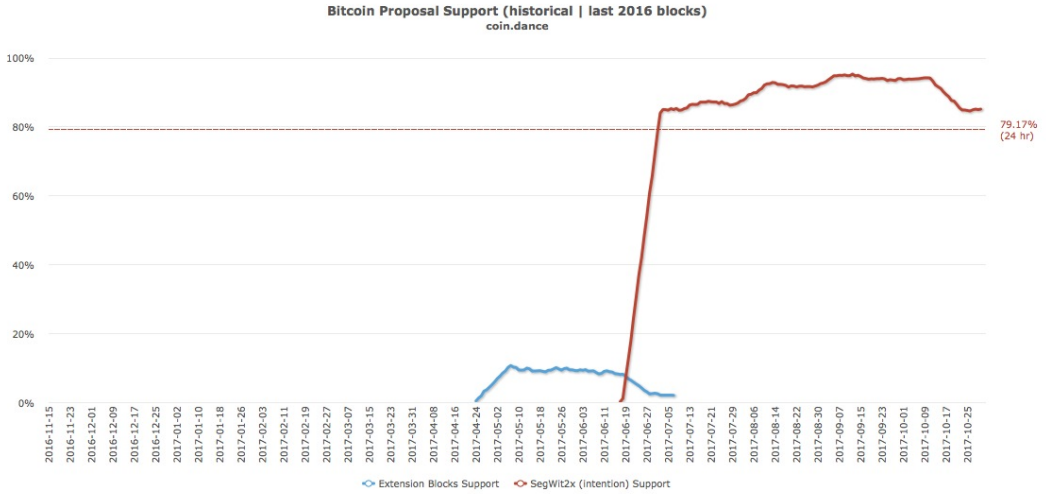
  A simple case is **“cheap talk”**: there are no consequences, i. e. bluffing is possible.
- **Signals** in the narrow sense are symbols which are more costly to emit if their value deviates from one’s own preference than if it coincides.

Protocol update procedures in blockchain systems

Miner Activated Soft Fork (MASF) according to BIP 9:

- Miners can set special-purpose bits in the block header.
- If a quorum is reached, the protocol update gets implemented after a grace period.

Example

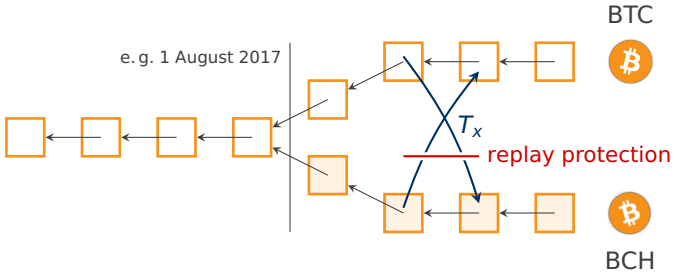


Source: `https://coin.dance/blocks#proposals`, retrieved on 30 October 2017

Blockchain Fork

Dissent with common history

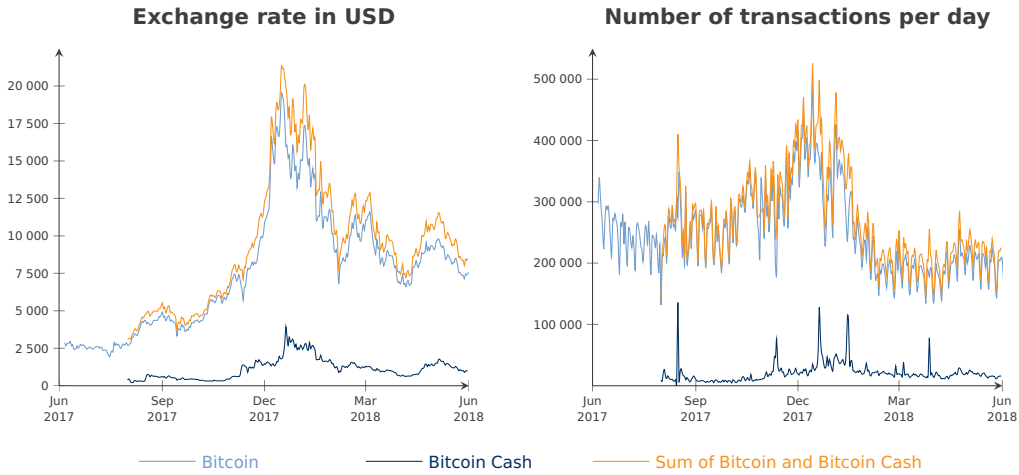
- Apply different rules to continue appending data to the public ledger.
- Miners collectively decide on success or failure of each branch.



- (Old) users enjoy a “duplication” of currency units.
- Critical mass is reached instantaneously, contrary to altcoin launches.

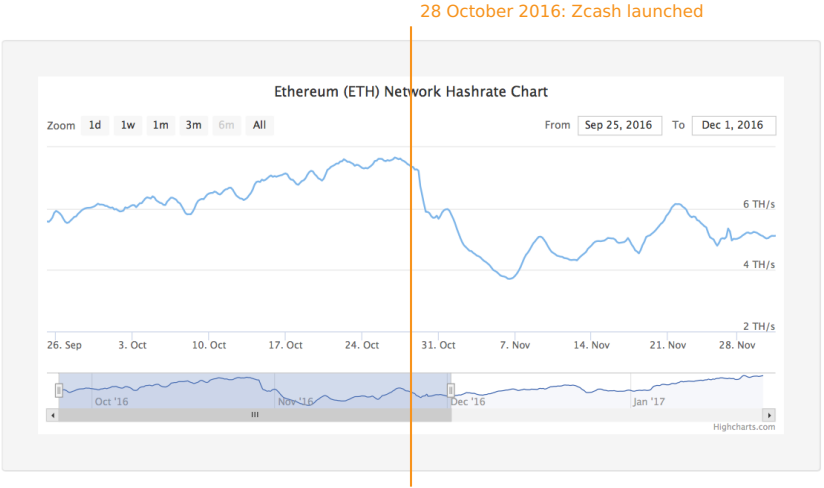
Prediction: Forks will be at the center of the next generation of ICOs.

Market Valuation of the Bitcoin Cash Fork



blockchain.info, bitinfocharts.com, 31 May 2018

Blockchain Competition



Source: coinwarz.com, accessed on 23 January 2017

New Challenges for the Rationality Assumption

Handwaving security arguments:

> *"An attacker would not do this because he is invested in the system and will lose wealth if the virtual currency crashes as the attack becomes public."*

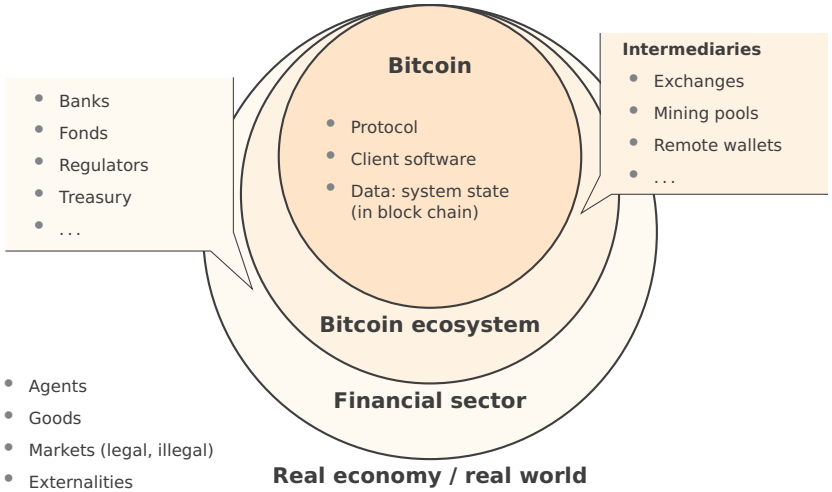
My initial reactions:

- It shows the limits of equating utility with ownership of coins in the system.
- Leaving the lab: if we model exchange rates, we need to model the real world!
- Implicit assumption: incomplete financial markets. (In complete markets, the attacker can short the currency.)

And here is why we need to fundamentally rethink the blockchain idea:

If chain B's execution environment can evaluate the state of chain A, one can write a "smart contract" in B that pays out b units of B, if it detects a successful attack that costs a units of A, such that $u(b) \gg u(a)$.

Bitcoin in Context



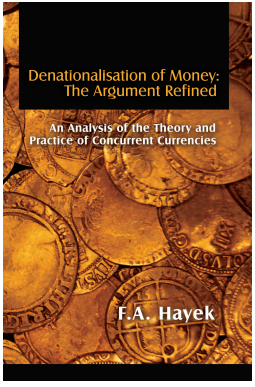
Agenda

1. Introduction
2. Rational Agents and Adversaries
3. Explaining System Behavior with Externalities
   Adoption · Maintenance · Governance
4. **On the Nature of Money**

Currency Competition

Competition between . . .

- conventional currencies
  e. g. euro ↔ pound, dollar ↔ renminbi
- virtual currencies
  e. g. Bitcoin ↔ Ether
- virtual vs conventional
- money vs credit
- state vs private



(1976, 3rd edition, London 1990)

Economic Functions of Money

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 expectation; behavioral

Discussion

- Which of these functions support a **natural monopoly** in the sense of network economics?
- How does this change if we assume **ubiquitous networked devices** ("electronic wallets") between end users and the marketplace?

“Money is Memory”

Results in the new-classical monetary theory:

Ostroy (1973) Money has a record-keeping role in a model where agents engage in pairwise exchanges.

American Economic Review 63, p. 597–610

Lucas (1980) Money is the cheapest means to consider past reallocations of resources in current decisions.

In: Karaken & Wallace, Federal Reserve Bank of Minneapolis

Aiygari & Wallace (1991) Money becomes redundant when agents have access to a historical record of all actions taken in past (pairwise) matches.

Review of Economic Studies 58, p. 901–916

Kocherlakota (1996) Any allocation that is feasible in an environment with money is also feasible in the same environment with memory. (His general model subsumes three modeling approaches, but **no obligations**.)

Research Department Staff Report 218, Federal Reserve Bank of Minneapolis

“Money is Memory”

“Money may only be an imperfect substitute for high quality information storage and access. [. . .] Government’s monopoly on seignorage might be in some jeopardy as information access and storage costs decline.”

Narayana R. Kocherlakota, 1996, S. 28

The Hopes of 2015

The Economist, 31 November 2015

Summary

1. Most blockchain-based systems must support virtual currency as a means to compensate participants for providing a **public good**: the distributed ledger.
2. This lecture started with the notion of **rational agents** and adversaries, which distinguishes the security model of blockchain-based systems from conventional crypto-systems (MPC) and other distributed consensus mechanisms (BFT).

   Rationality motivated **game theory** as a method of analysis.
3. A second cornerstone was the economic notion of **externalities**.

   This concept was used to explain **incentive mechanisms** within systems, **adoption** dynamics, and **competition** between systems (e.g., forks).
4. The lecture closed with selected theories on the **nature of money**, hopefully allowing us to discuss scenarios for the possible role of crypto-currencies within the global financial system.

“Gretchenfrage” for Blockchain-Systems

James Tissot. *Faust und Gretchen im Garten*, 1861. Source: `http://www.bilder-geschichte.de`

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

Interested in a PhD or post-doc opportunity in the heart of the Alps?
Approach me at rainer.boehme@uibk.ac.at and mention keyword “Sardegna school” :-)