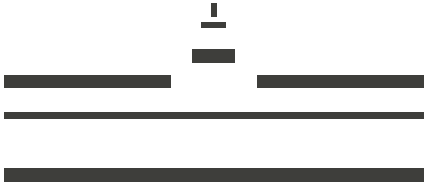


Westfälische
Wilhelms-Universität
Münster

Economics of Bitcoin

GI Workshop & Tutorial on Bitcoin

living.knowledge
WWU Münster

Rainer Böhme

20 September 2012

Size of the Bitcoin Economy

	Euro area		Bitcoin	
Market capitalization			0.09	300.0
Currency in circulation	866	5.9		
Overnight deposits	4 088	4.2		
M1	4 955	4.5		
M3	10 004	3.8		

Levels in billion EUR. Annual growth rates in %.

ECB (31 July 2012), blockchain.info (9 September 2012)

Agenda

1. Monetary, economic, and fiscal perspectives on Bitcoin
2. Ponzi schemes and speculation
3. Transaction costs and transaction risk
4. Incentive issues in the protocol design

Scarcity

The difficulty of printing money defines the value of a currency.

Bakia

Galia

Brakteat

Gulden

Bitcoin

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

Image source: Money Museum

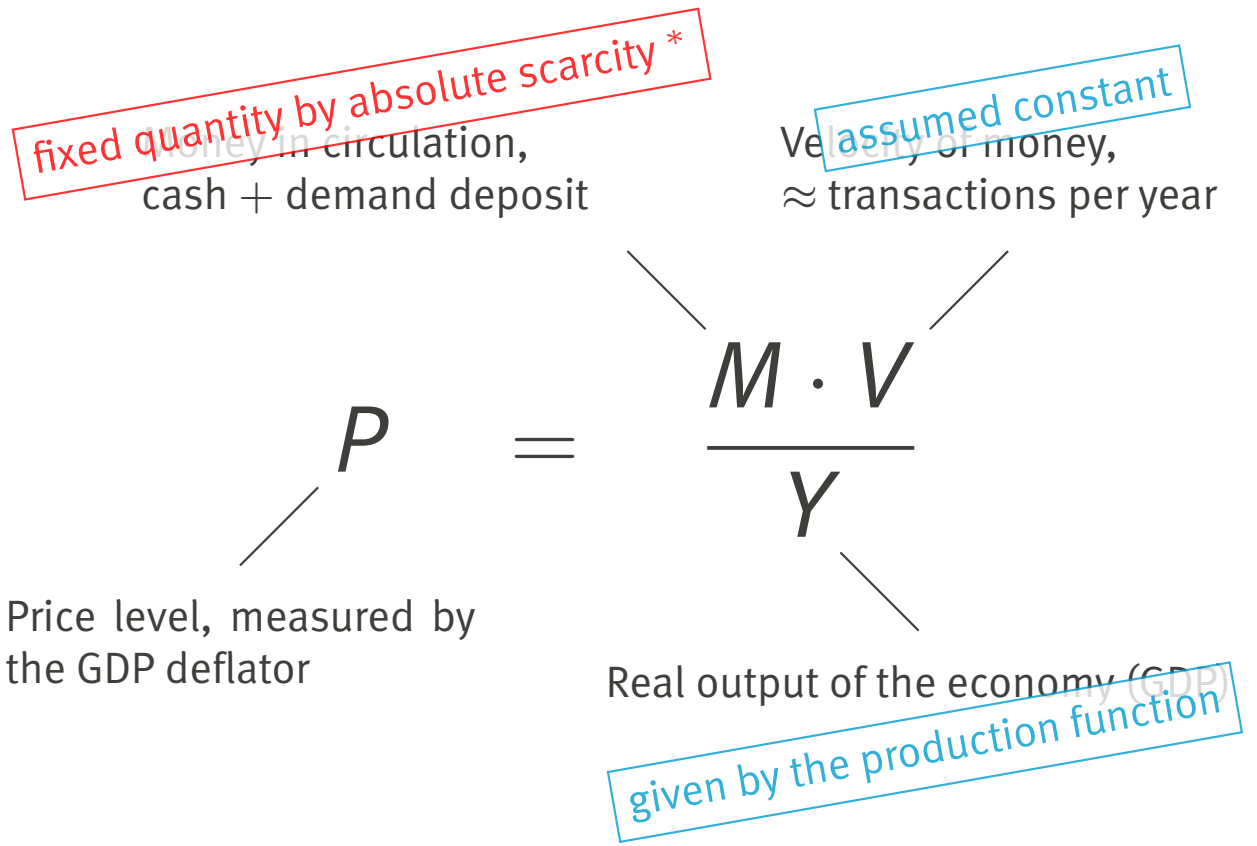
Implications of Absolute Scarcity

No more inflation ?

Curb sovereign debt ?

Quantity Theory of Money

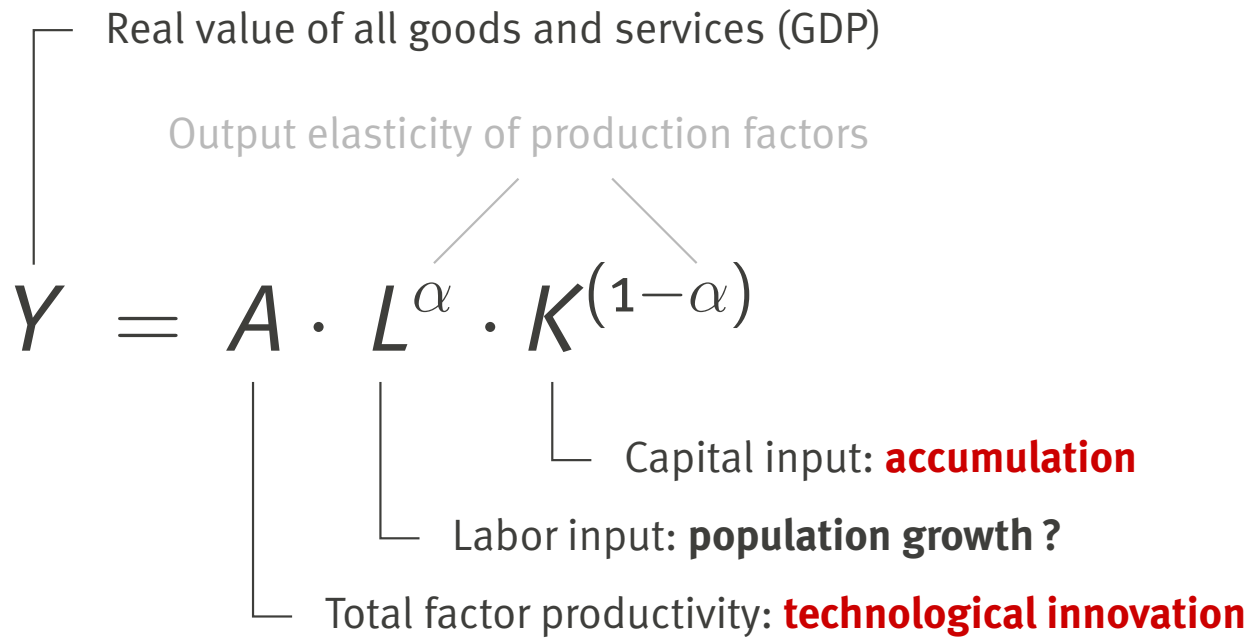
(simplified, in a closed economy)



* after the mining phase

Production Function

(Cobb–Douglas model, constant returns to scale)

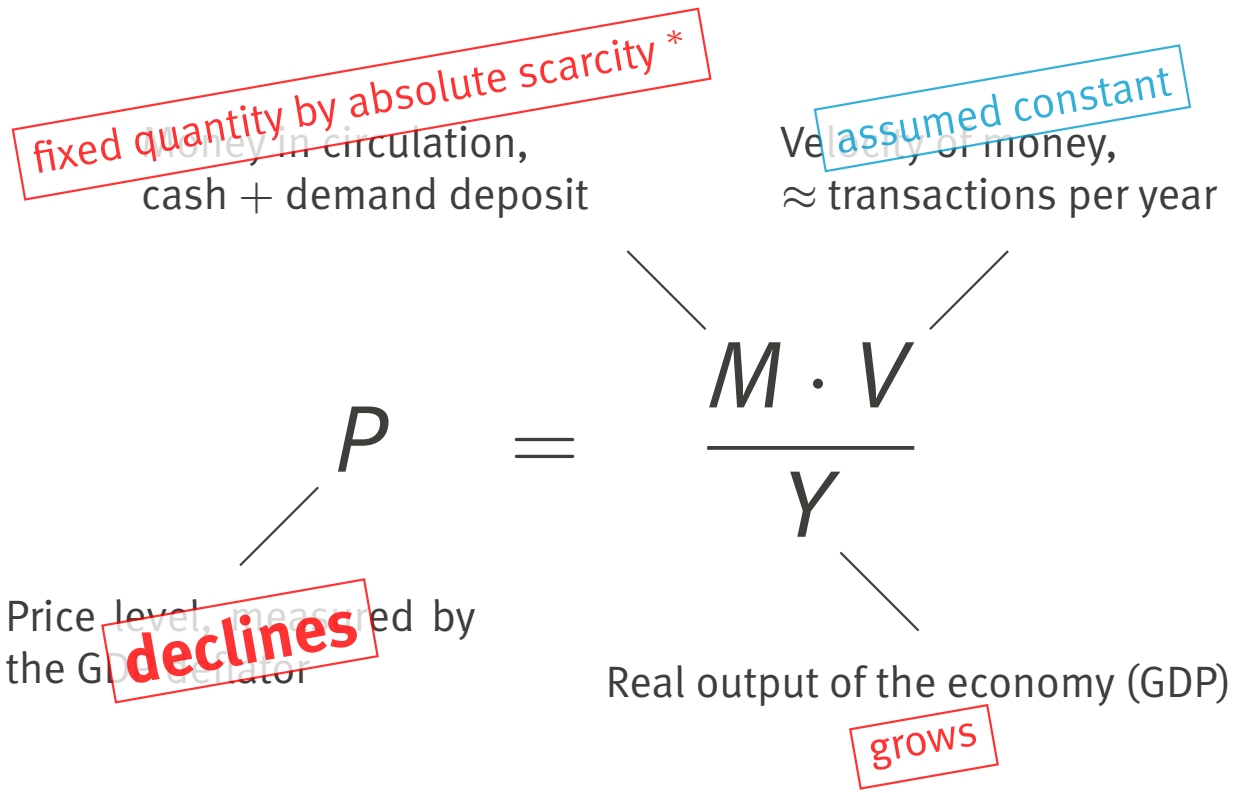


Economic growth

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

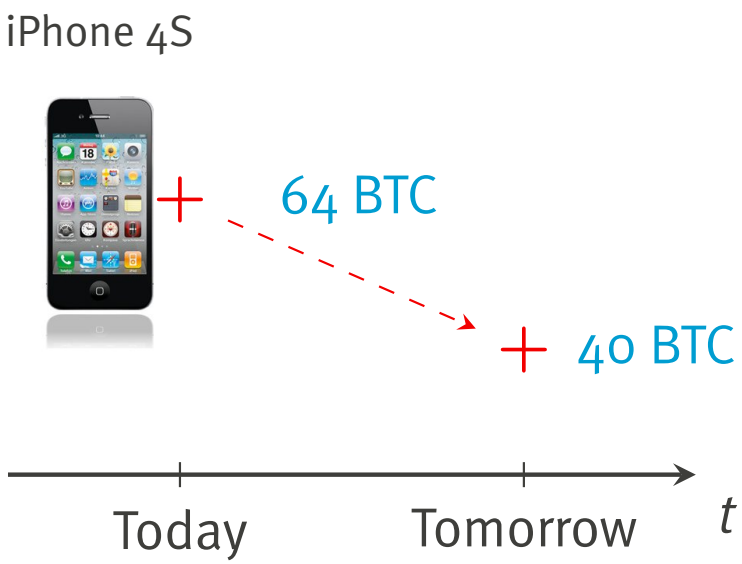
Quantity Theory of Money

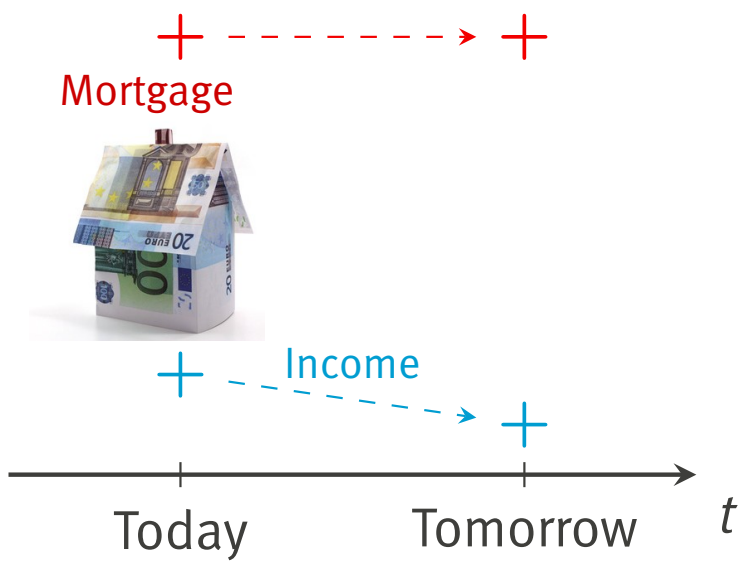
(simplified, in a closed economy)



* after the mining phase

Deflation

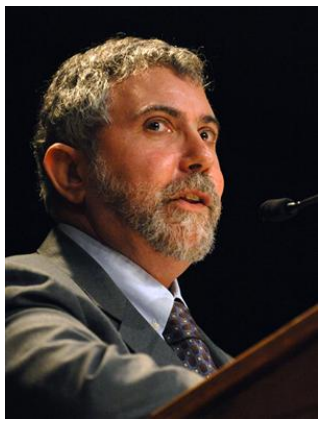




Vicious circle

Consumers postpone purchase decisions. Prices fall further.

Attribution



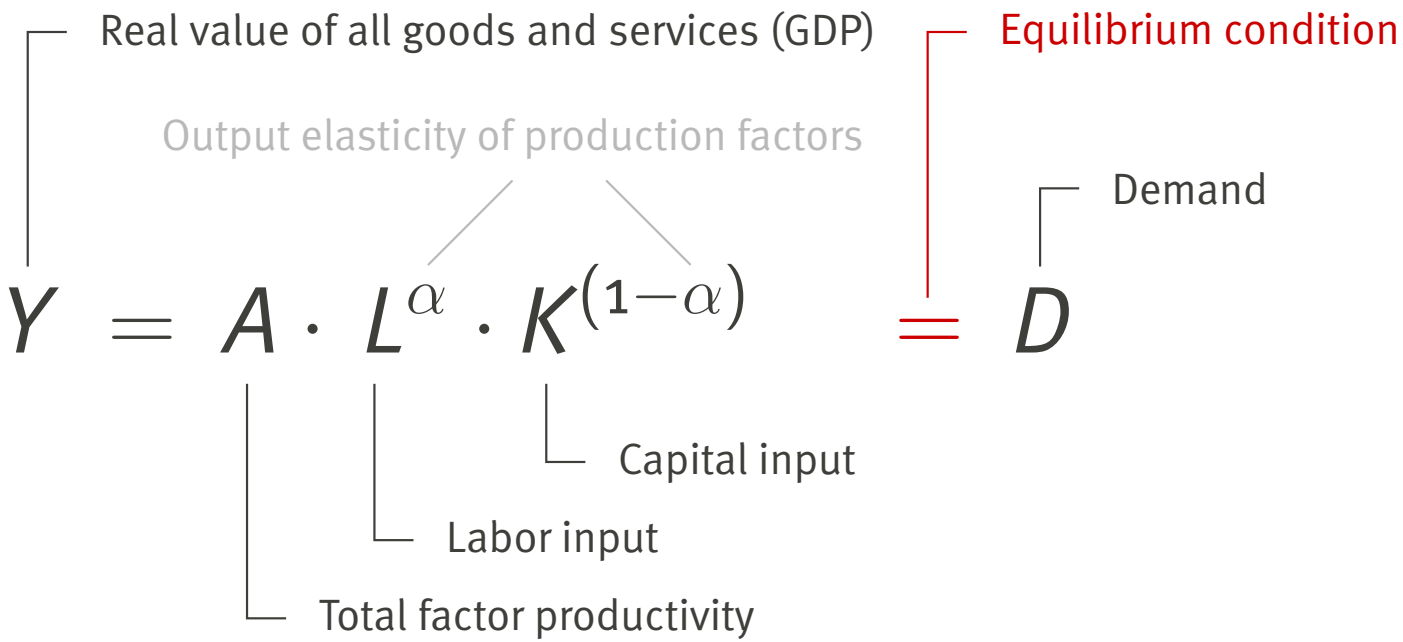
Paul Krugman

"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)



Implications of Absolute Scarcity

No more 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.

Agenda

1. Monetary, economic, and fiscal perspectives on Bitcoin
2. Ponzi schemes and speculation
3. Transaction costs and transaction risk
4. Incentive issues in the protocol design

Is Bitcoin Fair ?

Top 10 richest Bitcoin addresses

as of 6 Sep 2012

8bf24a18a58a ...	157 K BTC	1.41 M €
582431b9e63d ...	106 K BTC	0.95 M €
a0b0d60e5991 ...	80 K BTC	0.72 M €
3d9e561f21d3 ...	53 K BTC	0.47 M €
2004f419e735 ...	50 K BTC	0.45 M €
863ec44fbf7c ...	50 K BTC	0.45 M €
f1c87a5e8ff7 ...	50 K BTC	0.45 M €
ad6043f1806c ...	50 K BTC	0.45 M €
6fbe1851f5d1 ...	47 K BTC	0.42 M €
c52238d4cd96 ...	47 K BTC	0.42 M €

Is Bitcoin Fair ?

"Which is the greater crime, to rob a bank or to own one ?"

Berthold Brecht

"How did you come to rob a bank ?" – "Because that's where the money is."

(attributed to) William Sutton

"Let's own the currency."

Distribution of wealth

We look at the initial distribution of Bitcoins. Redistribution has a complex relationship with money supply and other factors.

A Quick Tour of Investment Scams

Chales Ponzi. Source: Wikimedia

Ponzi schemes

- Fraudulent investment 'opportunity'
- Lie about source of profit: late investors' deposits
- 'Postmodern' variant: be ahead of the pack Moore et al. 2012

Pyramid schemes

- Victims know that their profit depends on converting new entrants.
- Exponential growth, collapse faster than Ponzi schemes

Crypto currencies

- Bitcoin comes with a promise to get rich off the money supply.
- No sign of obvious deception (Unless the crypto has a backdoor.)
- Copycats struggling for critical mass: Solidcoin, Ixcoins, ...

Bitcoin Exchange Rate

Source: bitcoincharts.com

Not exactly a Pyramid scheme

If the Bitcoin economy grows faster than the money supply, the exchange rate against a basket of reference currencies appreciates.

Speculation

> *"The very fact that we have Bitcoin millionaires that did not do anything to earn their millions other than being in the right place at the right time lends an air of disrepute to the project."*
>
> Gunden 2011

Bitcoin valuation

(extremely simplified)

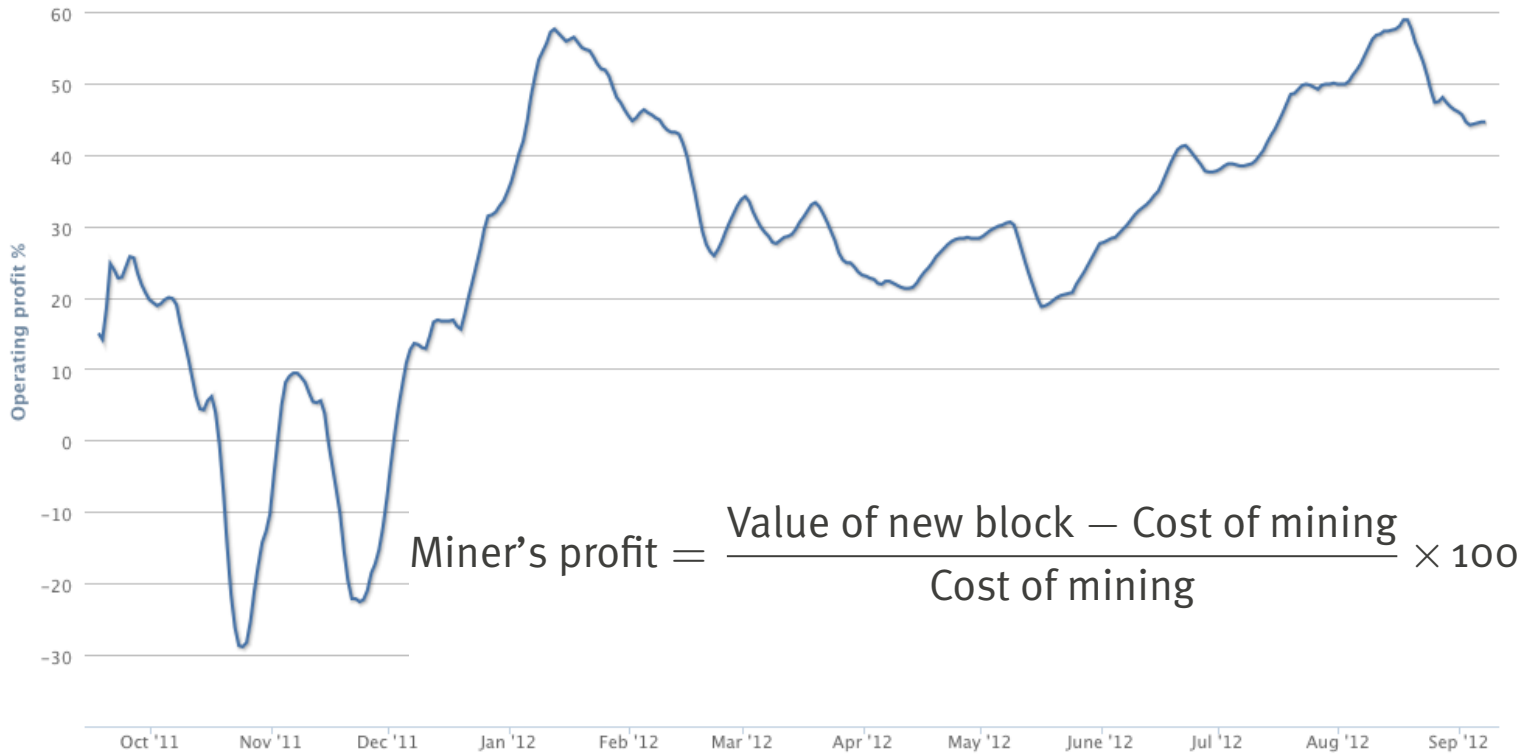
probability of reaching the expected state of the world

$$\text{Value of 1 BTC} = \max\left\{\text{price today}, \frac{p}{1+i} \cdot \text{future price}\right\}$$

risk-free interest rate

- Early investors take the risk that Bitcoin fails.
- Hindsight envy is misplaced.

Profit Motive Drives Adoption



$$\text{Miner's profit} = \frac{\text{Value of new block} - \text{Cost of mining}}{\text{Cost of mining}} \times 100\,\%$$

Source: blockchain.info

Minting Premium Puzzle

Observation

- Miner's operating margin is consistently above 20 % for the past three quarters.

Theory

- New miners should enter until the margin is down to zero in equilibrium.

Possible interpretations

- Rigidities in adding mining capacity (unlikely)
- Cost of mining underestimated
- Premium for high risk of Bitcoin collapsing in the short term (e. g., by government crack-down of exchanges)

Can We Find a Better Balance ?

Fix the difficulty

≠ fix value, as claimed by Gunden 2011

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

Fix the exchange rate

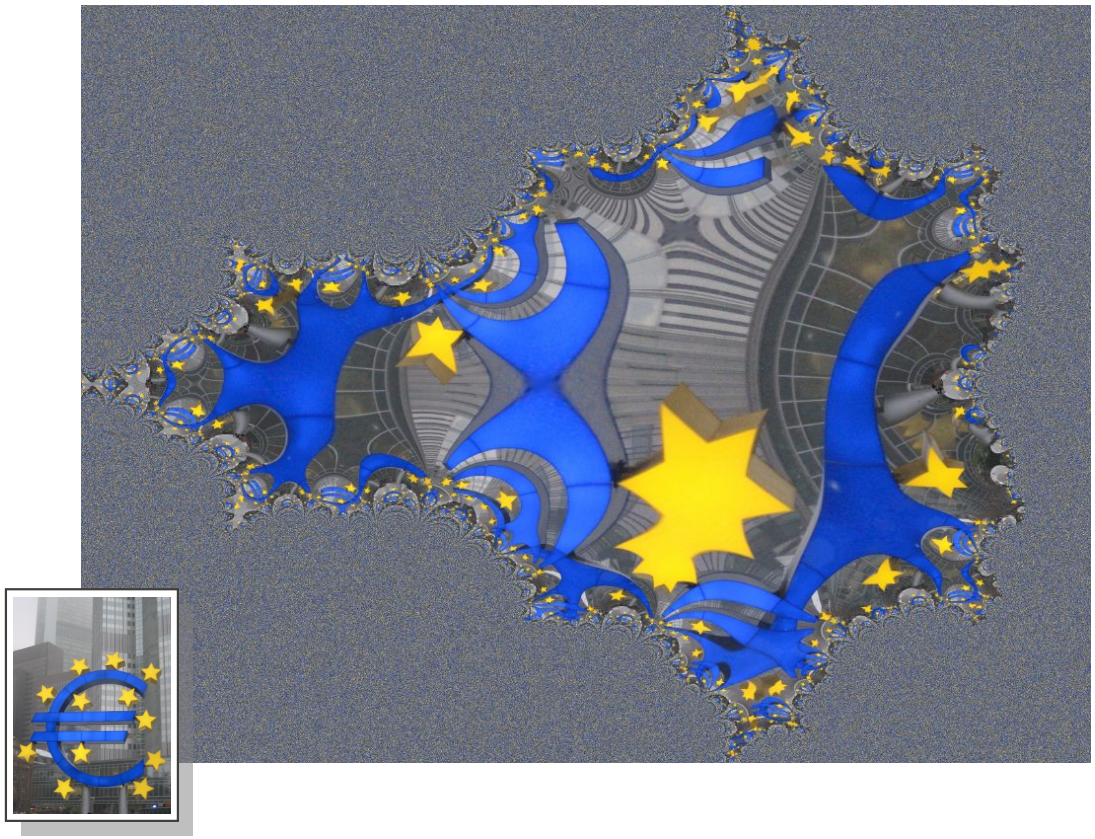
- Needs feedback from outside the closed system (exchanges)
- Point of attack until *everything* is digital and cryptographic

Central bank policy: discretion versus rules

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

Key question: Do strategy-proof rules exist in practice? e. g., Taylor 1993

A Cryptographic Decentral Bank ?



Agenda

1. Monetary, economic, and fiscal perspectives on Bitcoin
2. Ponzi schemes and speculation
3. Transaction costs and transaction risk
4. Incentive issues in the protocol design

Why Look at Transaction Costs and Risks ?

Transaction costs in online payment systems

- act like a tax on the Internet economy,
- impose market-entry barriers, and
- clog innovation.

Anderson 2012

Transaction cost savings is a key argument of Bitcoin advocates.

Transaction costs and risks cannot be separated. Risks need to be priced and add to risk-adjusted transaction costs.

Transaction Costs in a Nutshell

Operating cost
\+ Banker's margin

= **Transaction costs**

Illustration: Kenneth Ray

Transaction Costs in a Nutshell

	Operating cost
+	Exchange rate risk
+	Transaction risk
=	**Transaction costs**

Illustration: Kenneth Ray

Operating Costs

Observations

- Cost of proof-of-work network is underpriced in current transactions.
- If we believe blockchain.info's mining cost estimates, the operating costs per transaction are in the order of 4 % !
- Today: subsidized by money creation and growth of Bitcoin

Projection

- The operating cost of authorizing n transactions at a time is $\mathcal{O}(1)$.
- Hence, operating costs per transaction decline as the volume grows.

Security

- Security determines a lower bound for total operating costs.
- More in Dominic Breuker's talk this afternoon.

Exchange Rate Risk

Not much to say here:

- If fluctuations are bias-free, only risk-averse users feel the cost.
- Positive network externalities: risk will vanish with liquidity.
- Attacks against exchanges may be subsumed here.

Transaction Risk

Transaction risk comes in two forms:

1. Risk of dealing with a double-spender
2. Risk of transactions remaining unauthorized (more later)

How to deal with it ?

- Speed up authorization by generous transaction fee (if possible)
- Insure at a premium (or self-insure)
- Add local intermediary

Business model: the best of both worlds

Intermediaries issue 'fast' tokens (e. g., Chaum's cash) at a competitive fee. They take Bitcoin as collateral and use it as 'slow' settlement system. This replaces the two forms of transaction risk by a counter-party risk.

Agenda

1. Monetary, economic, and fiscal perspectives on Bitcoin
2. Ponzi schemes and speculation
3. Transaction costs and transaction risk
4. Incentive issues in the protocol design

Motivating Example

Raffle sells k tickets at € 1. Each ticket has the same probability of winning a single prize of value v. k is endogenous.

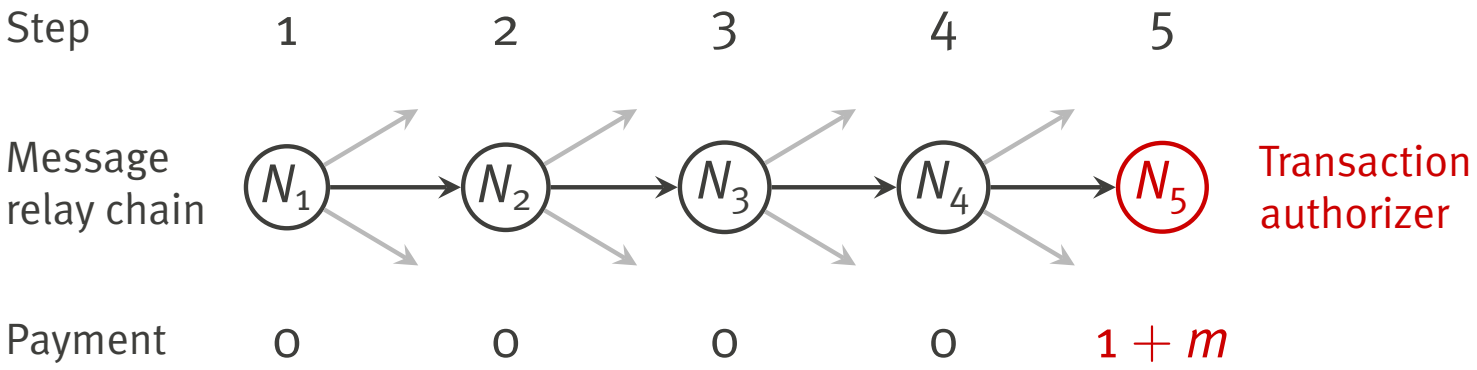
$$\text{Organizers's profit} = k - v \quad [€]$$

$$\text{Participant's exp. profit} = \frac{v}{k} - 1 \quad [€]$$

Tension between information propagation and competition

- Organizer wants as many people to find out about the raffle.
- Participants want to increase individual chances of winning.

Why Should Clients Broadcast Bitcoin Transactions ?

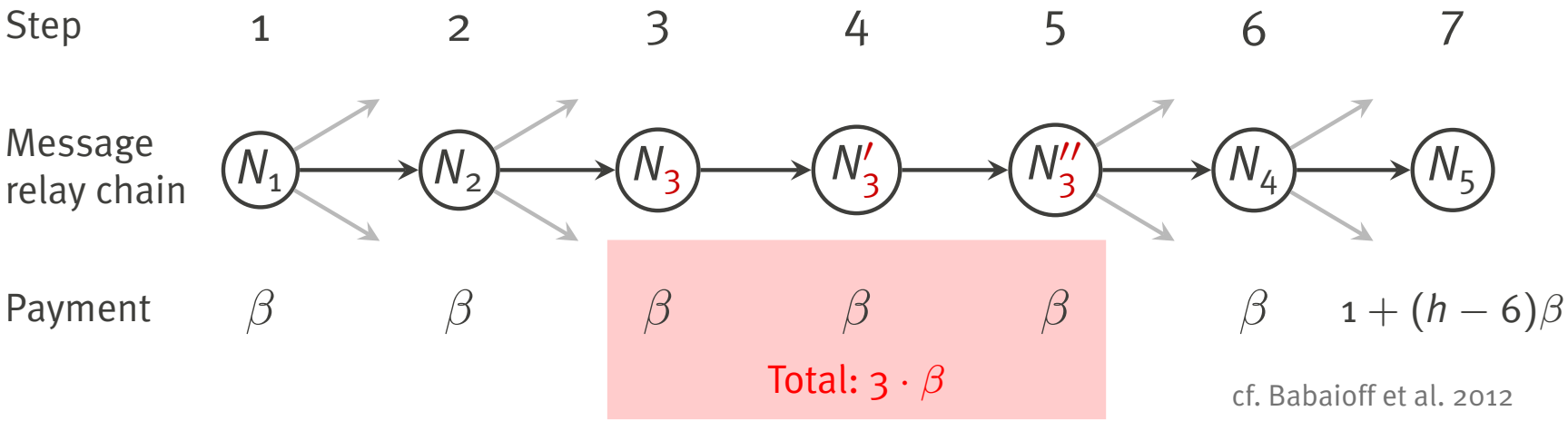


cf. Babaioff et al. 2012

Altruistic broadcast

The Bitcoin client does not implement the user's best interest.

Why Should Clients Broadcast Bitcoin Transactions ?



cf. Babaioff et al. 2012

Solution approach

- Distribution reward: share transaction fee with forwarders.
- **BUT:** Do not encourage fake identities (Sybill-proofness).

Finding the Optimal Distribution Reward

Absolute Sybill-proofness is hard to obtain. (Many negative results.)

Tipping point argument:

probability of being in the winning chain

number of fake identities

$$\text{Node's expected distribution reward} = p \cdot (1 + q) \cdot \beta$$

If sufficiently many independent nodes are aware of the transaction, then any given node *on average*

- prefers to use one less fake identity ($q--$),
- and instead distributes the transaction to increase its expected distribution reward by raising p.

This triggers an arms race converging to $q = 0$.

Babaioff et al.'s Result

Result

Specific *hybrid rewarding scheme*, which

- incentivizes information propagation
- without encouraging fake identities,
- while requiring small rewards and few seed nodes ($t \geq 14$).

Proven by iterative elimination of dominant strategies.

Limitations

- Negative result for dominant strategy equilibria.
- Result is valid for t complete d-ary trees, not for general networks.
- (Urgent) need to relax assumption of constant CPU power per node.

Summary

1. **Monetary, economic, and fiscal perspectives on Bitcoin**
   - Fixing the quantity of money leads to deflation and depression
   - No cure to sovereign over-indebtedness

2. **Ponzi schemes and speculation**
   - Most likely no deception, hence the Ponzi critique is misplaced
   - Tweaks to money supply are no quick fixes against speculation

3. **Transaction costs and transaction risk**
   - Claimed cost savings do not price in transaction risk
   - Also listen to Dominic Breuker's talk this afternoon

4. **Incentive issues in the protocol design**
   - Protocol is not strategy-proof against selfish clients
   - Maybe fixable by redistribution of transaction costs

Thank you for your attention.

References

R. Anderson (2012): Risk and Privacy Implications of Consumer Payment Innovation. Mimeo. Kansas Fed.

M. Babaioff, S. Dobzinski, S. Oren & A. Zohar (2012): On Bitcoin and Red Balloons. 13th ACM conference on Electronic Commerce (EC), 56–73.

D. Breuker et al. (2012): Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. *Workshop on the Economics of Information Security (WEIS)*, Berlin.

O. Gunden (2011): A Third Endgame for Bitcoin. Or, Creating a Truly Free Coin. `http://www.phauna.org/papers/freecoin/freecoin.pdf`.

P. Krugman (2011): Golden Cyberfetters. `http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/`.

T. Moore, J. Han & R. Clayton (2012): The Postmodern Ponzi Scheme: Empirical Analysis of High-Yield Investment Programs. In A. Keromytis (ed.): *Financial Cryptography and Data Security*, LNCS 7397, Springer, Berlin, 41–56.

J. Taylor (1993): Discretion versus Policy Rules in Practice. *Carnegie–Rochester Conference Series on Public Policy* 39 (1), 195–214.