13th International Conference of Sociocybernetics
Zaragoza, Spain, June 29 – July 3, 2015

Bitcoin: The Emergence of Self-Organized Cryptocurrency

Michael Paetau

Center for Sociocybernetics Studies
www.sociocybernetics.eu
michael.paetau@sociocybernetics.eu

Bitcoin: The Emergence of Self-organized Cryptocurrency

- Bitcoin: An Overview
  - What is Bitcoin? What is the Difference?
  - How it works?
  - What are the Advantages and Disadvantages?
  - Trend of Acceptance and Exchange-Rate
- Pardagigm Shift: Money as Social Relation
- Questions from a sociocybernetic point of view
  - How is circulation and value of bitcoin money controlled by society?
  - How is social action in society controlled by bitcoin as a form of symbolic steering media?

What is „Bitcoin“?

- Peer-to-peer electronic cash
- Using cryptography (Satoshi Nakamoto)
- NOT a regional currency of internet
- Idea: Anonymity, faster, cheaper, more free, prevention for manipulation and missuse of authorities (state, reserve banks), overcome of bureaucratic barriers, protection against freeze of accounts by governments)
- Questions:
  - How is it created? Who? Where?
  - How is money supply regulated?
  - Where we can purchase it?
  - How we can Bitcoin store and transfer?

The Bitcoin-Network

- Everybody can create bitcoins
- Bitcoins can be transferred directly from person to person via the net without going throught a bank or clearing house (this means that fees are much lower)
- one can use it in every country,
- sending bitcoins is simple like sending an email,
- the account cannot be frozen,
- there are no prerequisits or arbitrary limits,
- no possibility to track your shopping behaviour and to identify the trade partners,
- the transfer is anonymous like with money in cash,
- there is no possibility to recall already transferred money.

The „Blockchain“

- How can be guaranted that digital money not be paid twice?
- The solution is a new form of social-technological organsation of the money system: each transaction from one person to another get a „timestamp“ and becomes part of the code
- The timestamp-server works by taking a hash of a block of items to be timestamped and widely publishing the hash like in a newspaper.
- Each timestamp includes the previous timestamp in its hash, forming a chain with aditional timestamp reinforcing the ones before it.
- Transactions are summarized in information-blocks (1 Mbyte), renewed every 10 minutes (Hash Rate): „The Blockchain“
- It guarantees that every transaction is carrying its history with it.
- It is the decentralised ledger, where all transactions of the bitcoin-system since the beginning of the system (2009) are documented, visible and proofiable of everybody under: https://blockchain.info

The „Blockchain“ - Heart of the System

- The Blockchain represent the currency itself: Itemization of debit and credit
- A Bitcoin exists only insofar that it signs a value to a specific bitcoin-address (Nakamoto: „A chain of digital signatures“ (like PGP: each owner signes with his privat key and the public key of the next owner.)
- The Blochchain is used to evidence the rest of the bitcoin-network, that your are legitimate to make a transfer of one address to another
- A bitcoin is not a document or a digital file which one can copy or which can get be lost, you can only lose the right to use this credit if you forget the password or if someone has stolen your notebook or smartphone
- Important is the public character of the blockchain (a big difference to other electronic pay-systems like PayPal).
- But because the encryption there is no possibility to identfy the owner. All transactions are absolutely anonymous.

Money Creation ("Mining") and Money Supply

- Task solving (very difficult algorithm with random numbers, which must be calculated, very cost-intensiv, very high power consum, a lot of concatenated computers are working in so-called computer-farms))

- Every transaction will be recorded and published in the Internet under: "www.blockcain.info" ,

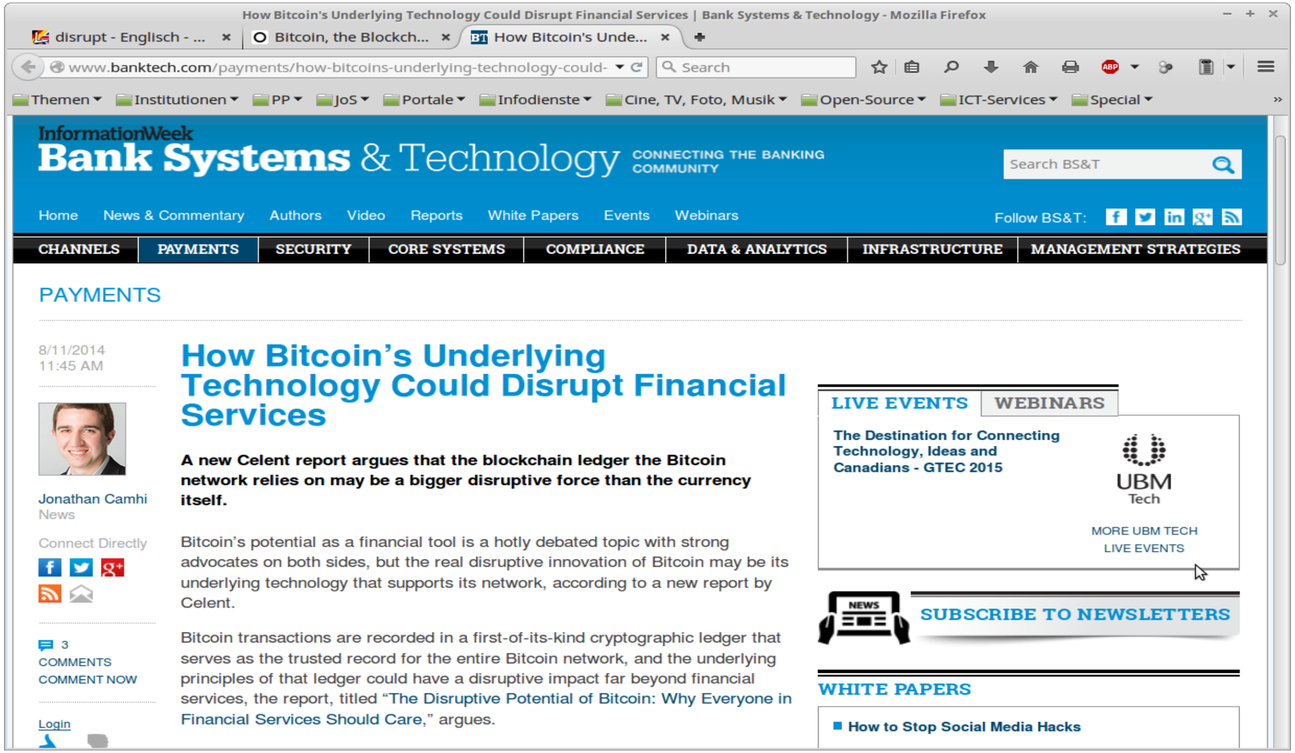
- Hash Rate (every 10 Minutes one block per 1 Mbyte = 144 Blocks per day.

- The incentive: currently 25 BTC per block = 3600 BTC p/d (2009 – 2014 = 50 BTC per block = 7.200 BTC p/d; after 2016 = 12,5 BTC per block = 1.800 BTC p/d.)

- The volume is limited: 21 Mio (unchanchable; Current status ca. 14,3 Mio.)

- Increasing data processing capacity, but also increasing difficulty of the algorythm (increasing effort and costs)

Financial Revolution?



PAYMENTS

8/11/2014
11:45 AM

Jonathan Camhi
News

Connect Directly

3
COMMENTS
COMMENT NOW

Login

How Bitcoin's Underlying Technology Could Disrupt Financial Services

A new Celent report argues that the blockchain ledger the Bitcoin network relies on may be a bigger disruptive force than the currency itself.

Bitcoin's potential as a financial tool is a hotly debated topic with strong advocates on both sides, but the real disruptive innovation of Bitcoin may be its underlying technology that supports its network, according to a new report by Celent.

Bitcoin transactions are recorded in a first-of-its-kind cryptographic ledger that serves as the trusted record for the entire Bitcoin network, and the underlying principles of that ledger could have a disruptive impact far beyond financial services, the report, titled "The Disruptive Potential of Bitcoin: Why Everyone in Financial Services Should Care," argues.

LIVE EVENTS | WEBINARS

The Destination for Connecting Technology, Ideas and Canadians - GTEC 2015

UBM Tech

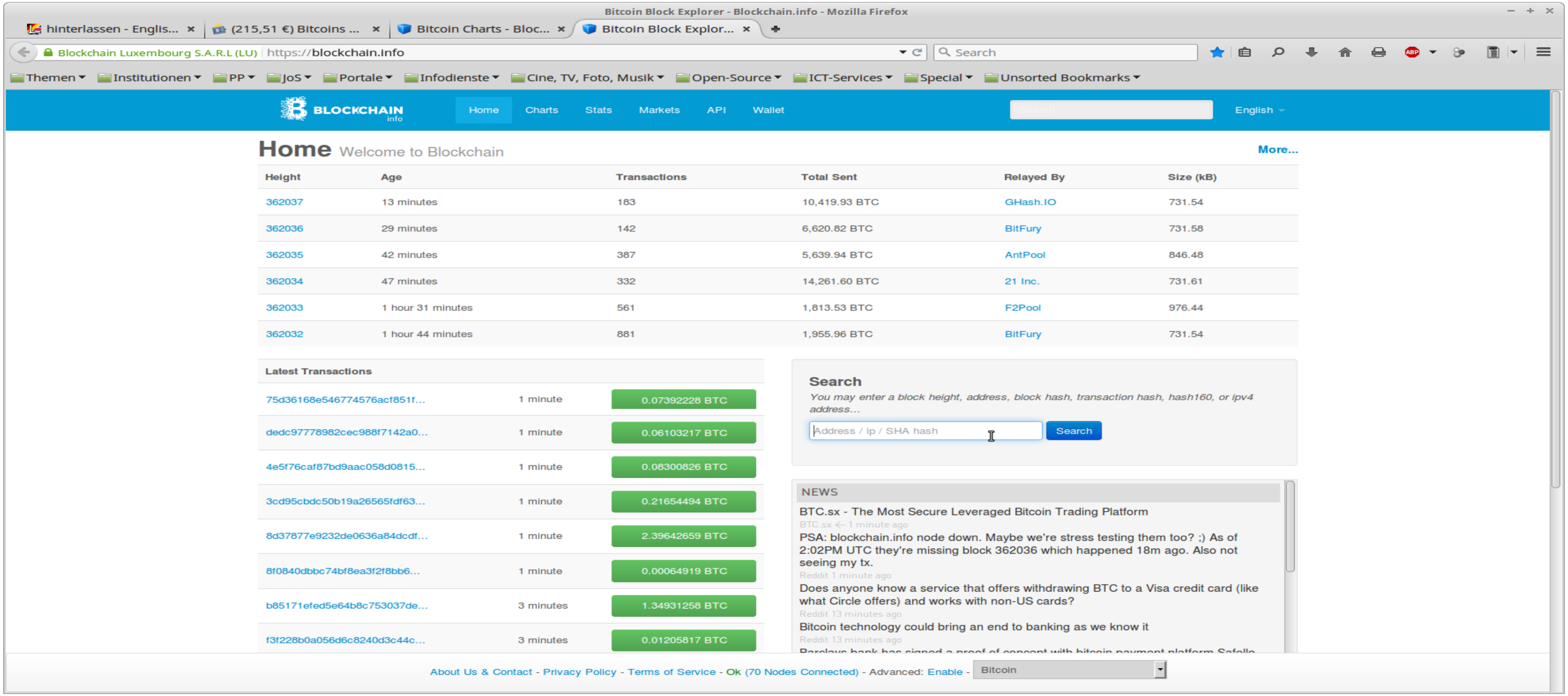
MORE UBM TECH LIVE EVENTS

SUBSCRIBE TO NEWSLETTERS

WHITE PAPERS

- **How to Stop Social Media Hacks**

Blockchain Screenshot of June 22, 2015, 16:15 h



Home Welcome to Blockchain

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
362037	13 minutes	183	10,419.93 BTC	GHash.IO	731.54
362036	29 minutes	142	6,620.82 BTC	BitFury	731.58
362035	42 minutes	387	5,639.94 BTC	AntPool	846.48
362034	47 minutes	332	14,261.60 BTC	21 Inc.	731.61
362033	1 hour 31 minutes	561	1,813.53 BTC	F2Pool	976.44
362032	1 hour 44 minutes	881	1,955.96 BTC	BitFury	731.54

Latest Transactions		
75d36168e546774576acf851f...	1 minute	0.07392228 BTC
dedc97778982cec988f7142a0...	1 minute	0.06103217 BTC
4e5f76caf87bd9aac058d0815...	1 minute	0.08300826 BTC
3cd95cbdc50b19a26565fdf63...	1 minute	0.21654494 BTC
8d37877e9232de0636a84dcdf...	1 minute	2.39642659 BTC
8f0840dbbc74bf8ea3f2f8bb6...	1 minute	0.00064919 BTC
b85171efed5e64b8c753037de...	3 minutes	1.34931258 BTC
f3f228b0a056d6c8240d3c44c...	3 minutes	0.01205817 BTC

Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

Address / ip / SHA hash [Search]

NEWS

BTC.sx - The Most Secure Leveraged Bitcoin Trading Platform
BTC.sx ← 1 minute ago

PSA: blockchain.info node down. Maybe we're stress testing them too? ;) As of 2:02PM UTC they're missing block 362036 which happened 18m ago. Also not seeing my tx.
Reddit 1 minute ago

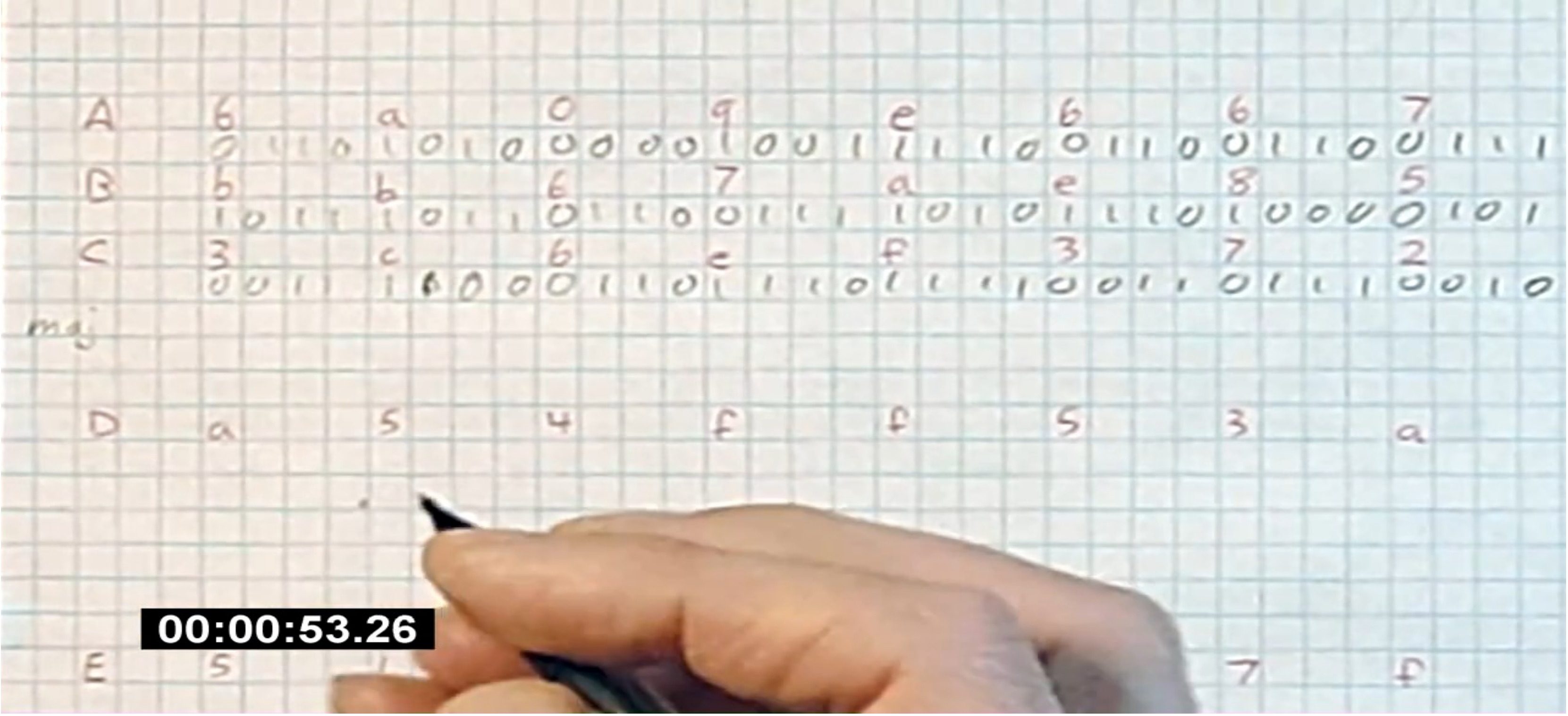
Does anyone know a service that offers withdrawing BTC to a Visa credit card (like what Circle offers) and works with non-US cards?
Reddit 13 minutes ago

Bitcoin technology could bring an end to banking as we know it
Reddit 13 minutes ago

Barclays bank has signed a proof of concept with bitcoin payment platform Safello

About Us & Contact - Privacy Policy - Terms of Service - Ok (70 Nodes Connected) - Advanced: Enable - Bitcoin

Mining with Paper and Pencil
(https://www.youtube.com/watch?v=y3dqhixzGVo)

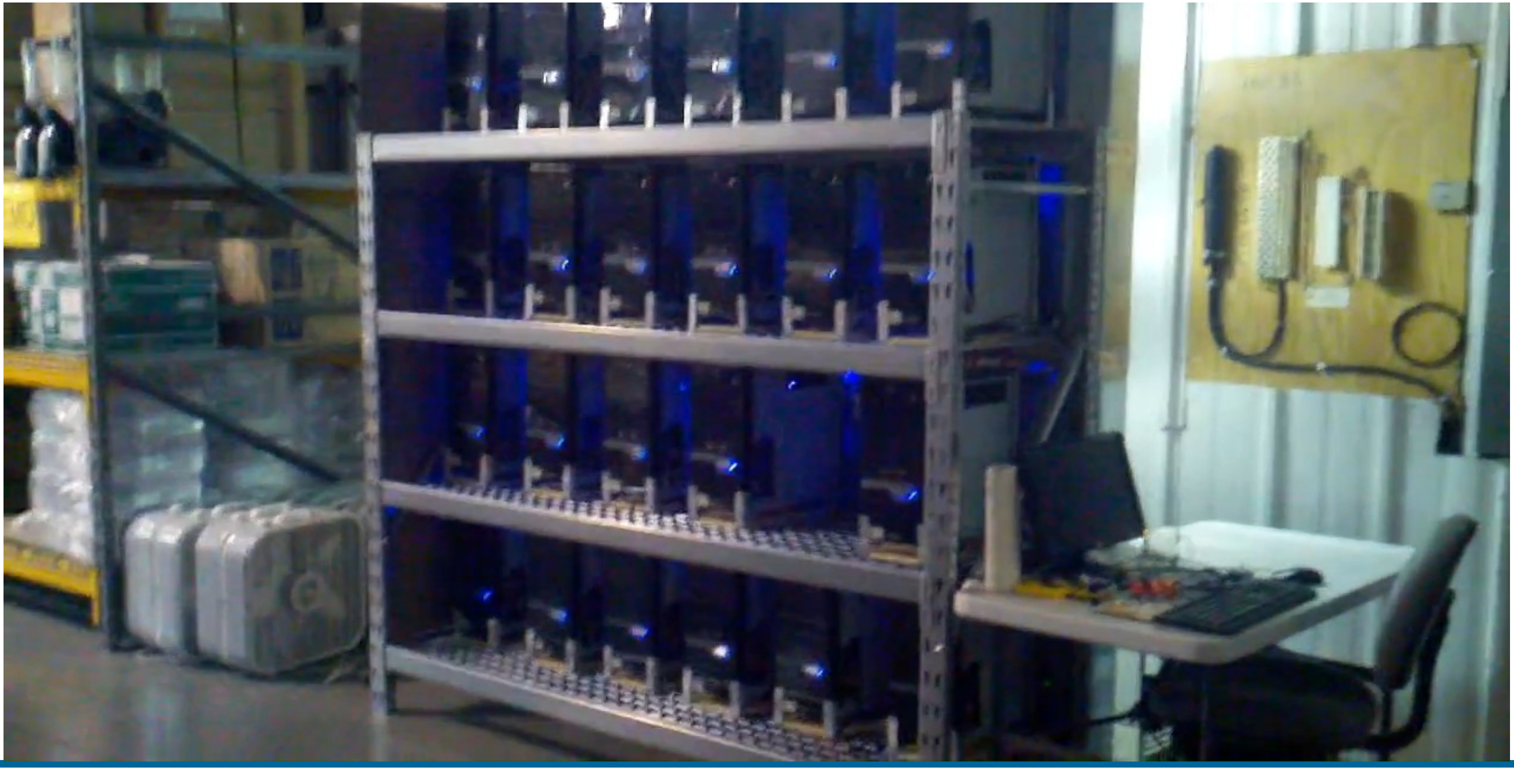


A	6	a	0	9	e	6	6	7
	0110	1010	0000	1001	1110	0110	0110	0111
B	b	b	6	7	a	e	8	5
	1011	1011	0110	0111	1010	1110	1000	0101
C	3	c	6	e	f	3	7	2
	0011	1100	0110	1110	1111	0011	0111	0010
maj								
D	a	5	4	f	f	5	3	a
E	5	1					7	f

Dr. Michael Paetau

Center for Sociocybernetics Studies

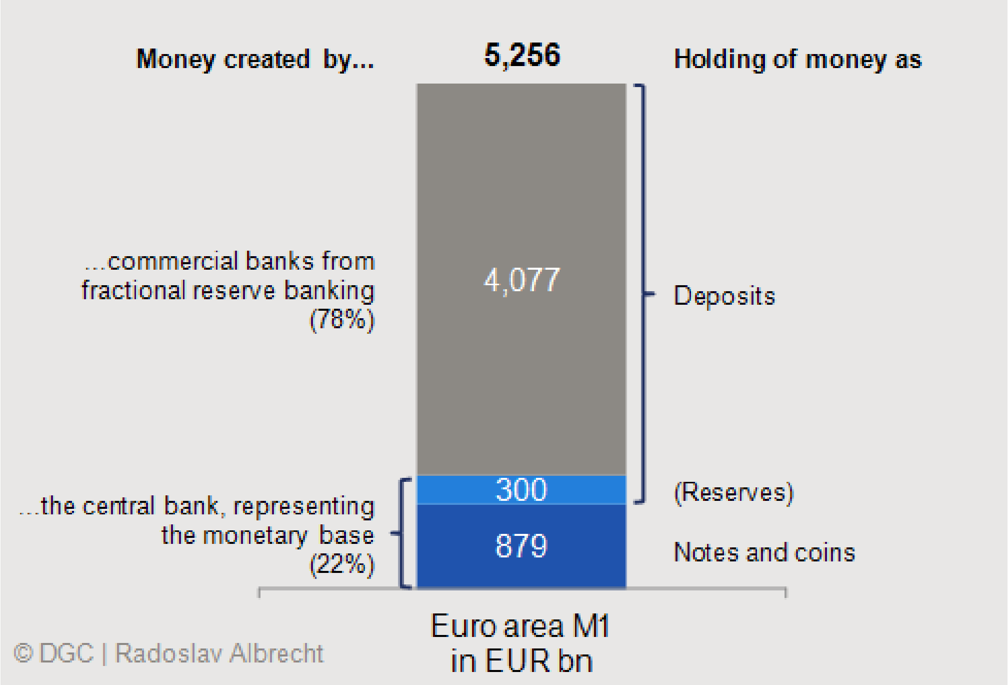
Mining Rig



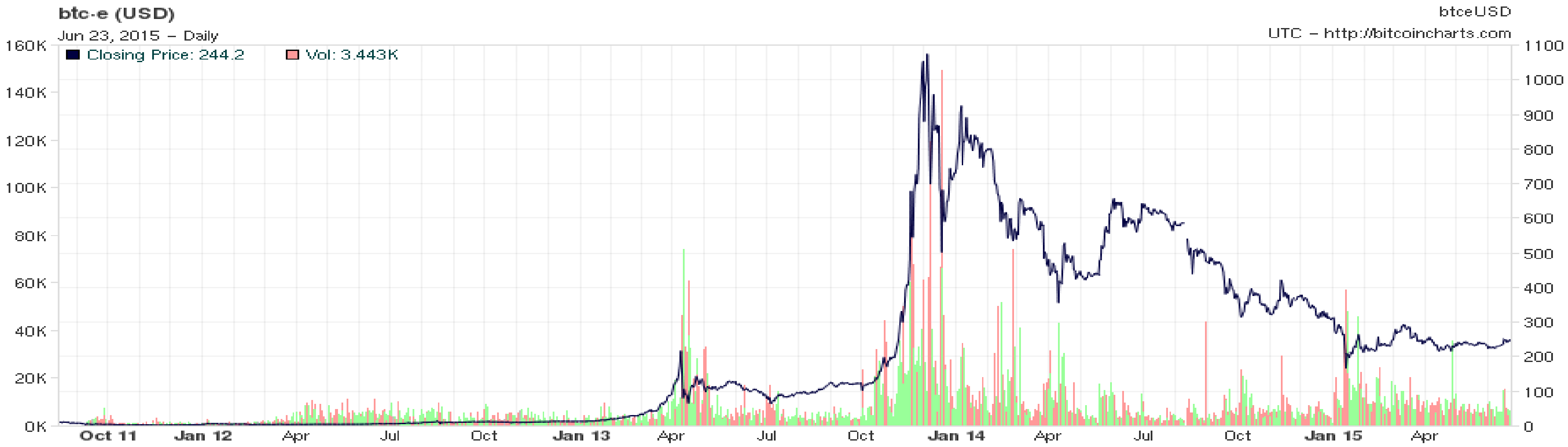
Mining by Combining Graphic Boards

Biggest Mining Farm in USA

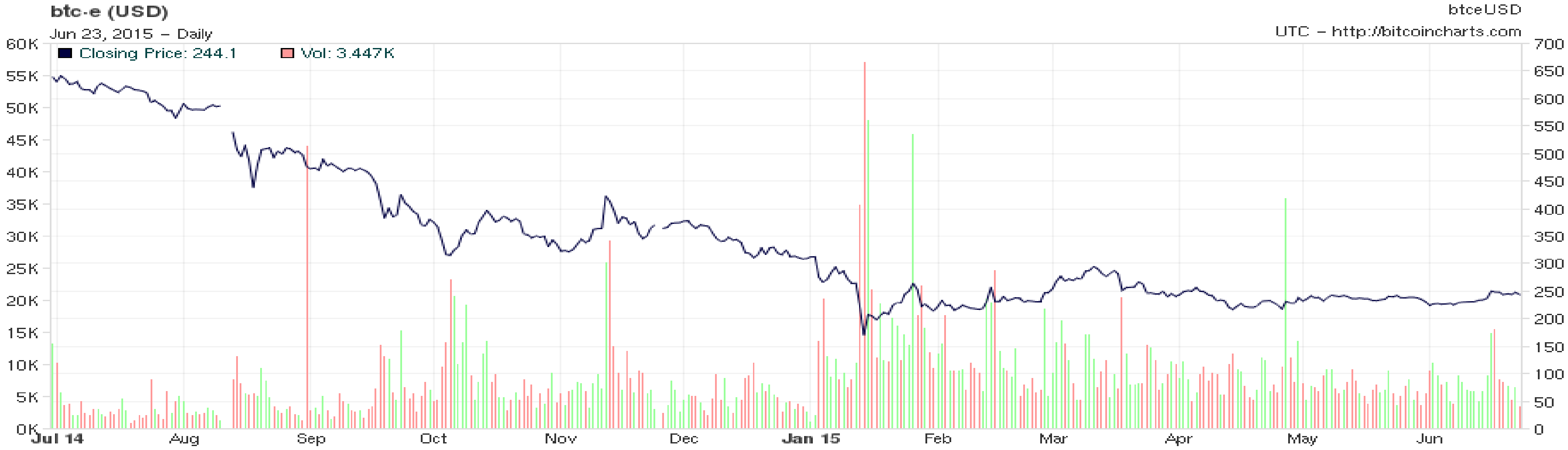
Volume of Money in Circulation (€)



Currency Rate (2009 – 2014, US-$)



Currency Rate (1 Year, US-$)

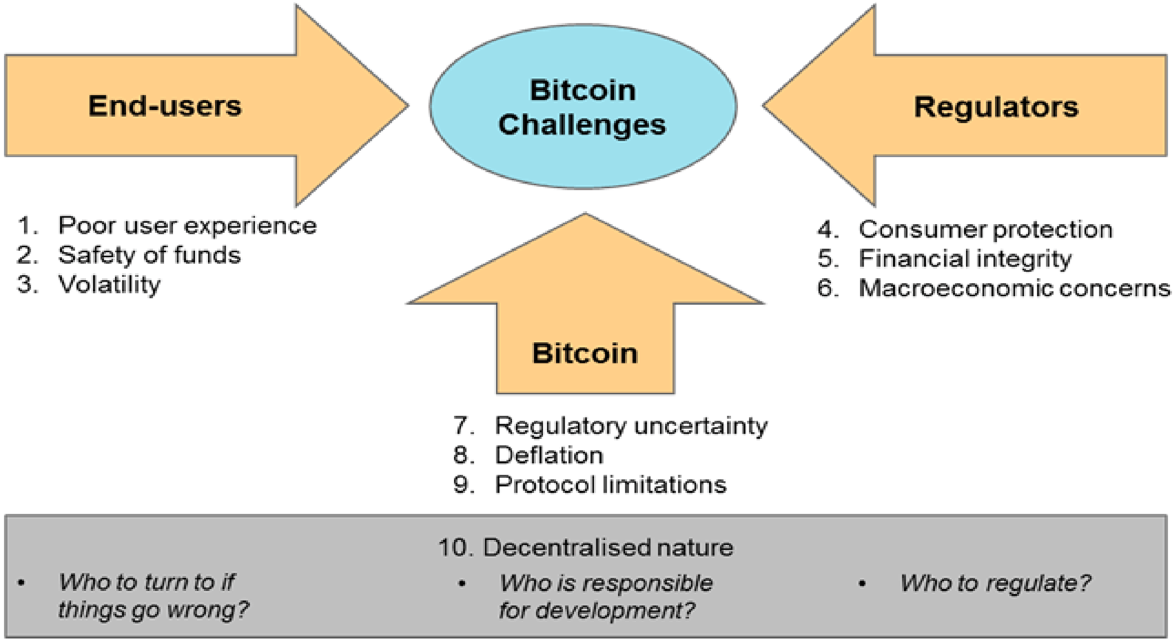


Dr. Michael Paetau

Center for Sociocybernetics Studies

Challenge

Bitcoin Challenges: Three Perspectives



End-users

1. Poor user experience
2. Safety of funds
3. Volatility

Bitcoin Challenges

Regulators

4. Consumer protection
5. Financial integrity
6. Macroeconomic concerns

Bitcoin

7. Regulatory uncertainty
8. Deflation
9. Protocol limitations

10. Decentralised nature

- *Who to turn to if things go wrong?*
- *Who is responsible for development?*
- *Who to regulate?*

Source: Zilvinas Bareisis, 11.08.2014: http://www.celent.com/reports/disruptive-potential-bitcoin-why-everyone-financial-services-should-care

A new Understanding of Money?

- Is the old story a myth?
  - Sequence from barter to money and credit/debit (by classical economy)?
  - Overestimating the materiality of money (by „Metallistes“)?
  - Overestimating the role of the state (by „Chartalists“)?
  - Were there other forms in ancien societies to regulate the distribution of goods (e.g. complexe codes of behaviour to account debits and credits)?

- What are the alternatives?

Paradigm Shift ?

- „Blochchain Economy“:
  - Money as a social relation
  - Money ist not a special good with particular properties
  - Money is the system of of credit account and their clearing that currency represents
  - Money is a special form of credit (and debits) instead of credit a special form of money

- Sociologization of Economics?
  - Money as symbolically generalized media of interchange

Money as symbolically-generalized Medium of Communication

- **Medium**
  - High-complex information in symbolic form
  - concatenated to chains of communication or social actions
  - Without nessecity
    - to reason its motivation or
    - deliberate the prerequisites of colaboration at each time

> „Probably money was generated not with respect to its intermediate function for exchange but as a sign Germany doesn't want to save Greece. It seems to want to humiliate Greece.for unbalanced performance ratios, first probably in household economies.(...) The function of the symbolically generalized medium is to such an extent impossible, that it never could serve as an driving factor for evolution. It was visible first in a just functioning economy of money." (Luhmann Gesellschaft der Gesellschaft, S. 348 f.).

Literature

- Hayek, Friedrich von: Denationalisation of Money, London 1976
- Luhmann, Niklas: Die Wirtschaft der Gesellschaft, Frankfurt am Main 1989: Suhrkamp
- Martin, Felix: Money. The unauthorized Biography. New York, 2013: Knopf – Borzoi
- Marx, Karl: Das Kapital, Band I, Berlin 1969
- Mey, Stefan: Das Bitcoin-Experiment. Le Monde Diplomatique 6/2015 (German Edition), pp. 3 ff.
- Platzer, Jörge: Bitcoin. Banking ohne Banken. Köln 2014: O'Reilly
- Simmel, Georg: Philosophie des Geldes, Frankfurt 1989, Suhrkamp
- Swan, Melanie: Blockchain. Blueprint for a New Economy. Sebastopol, CA (USA), 2015: O'Reilly
- Vigna, Paul & Casey, Michael: The Age of Cryptocurrency: How Bitcoin and Cybermoney are Challenging the Global Economy Order. 2015