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

- ** Paradigm 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 misuse 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 through 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 prerequisites 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 organisation 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 additional 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 proofable of everybody under: https://blockchain.info
The „Blockchain“ - Heart of the System

- The Blockchain represents 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 signs with his private key and the public key of the next owner. )
- The Blockchain is used to evidence the rest of the bitcoin-network, that you 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 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 payment systems like PayPal).
- But because the encryption there is no possibility to identify 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-intensive, very high power consumption, 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 (unchangeable; Current status ca. 14,3 Mio.)

- Increasing data processing capacity, but also increasing difficulty of the algorithm (increasing effort and costs)
Financial Revolution?

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.

Dr. Michael Paetau

Center for Sociocybernetics Studies
Mining with Paper and Pencil
(https://www.youtube.com/watch?v=y3dqhixzGVo)
Mining Rig
Mining by Combining Graphic Boards
Biggest Mining Farm in USA
Volume of Money in Circulation (€)

- Money created by commercial banks from fractional reserve banking (78%): 5,256
- The central bank, representing the monetary base (22%): 300
- Euro area M1 in EUR bn: 879
- Holding of money as deposits: 4,077
- Reserves: 300
- Notes and coins: 879

© DGC | Radoslav Albrecht
Currency Rate (1 Year, US-$)
Challenge

Bitcoin Challenges: Three Perspectives

End-users
1. Poor user experience
2. Safety of funds
3. Volatility

Bitcoin Challenges
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?

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

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?

• „Blockchain Economy“:
  - Money as a social relation
  - Money is 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 necessity
    - to reason its motivation or
    - deliberate the prerequisites of collaboration 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

- Luhmann, Niklas: Die Wirtschaft der Gesellschaft, Frankfurt am Main 1989: Suhrkamp
- Marx, Karl: Das Kapital, Band I, Berlin 1969
- 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