TALLINN UNIVERSITY OF TECHNOLOGY

Future Money: Paper or Data?

Kuldar Taveter, Professor in Software Engineering, Department of Informatics, Tallinn University of Technology, Estonia

Who am I?

- Name: Kuldar Taveter
- Position: Professor, Chair of Software Engineering
- Education:
  - **Dip.Eng., TUT, 1988**
  - **M.Sc., TUT, 1995**
  - **Ph.D., TUT, 2004**
- Work experience:
  - **1985-1989: Institute of Cybernetics**
  - **1989-1993: Private companies**
  - **1993-1998: Department of Informatics of TUT**
  - **1997-2005: Technical Research Centre of Finland**
  - **2005-2008: The University of Melbourne, Australia**
  - **2008- : Department of Informatics of TUT**
  - **Jan-Aug 2011: University of South Carolina, USA**
- Research areas: Agent-oriented software engineering, engineering of sociotechnical systems, multiagent systems, intelligent systems, ambient intelligence, agent-based simulation

Background

- 63% of all monetary transactions in Estonia are conducted by a debit or credit card
- Getting rid of paper money?
- Mistaken transactions?
- Can we trust centralized banking solutions in any country?
- 50 million digital signatures are given each year in Estonia

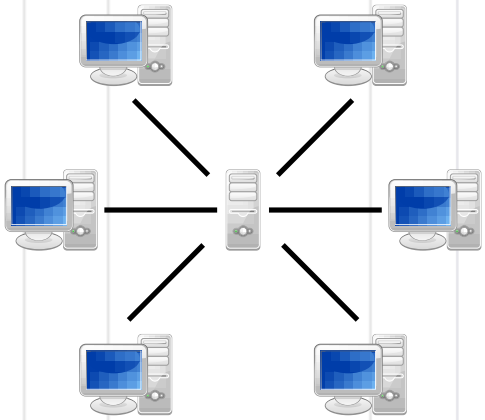
Requirements for money

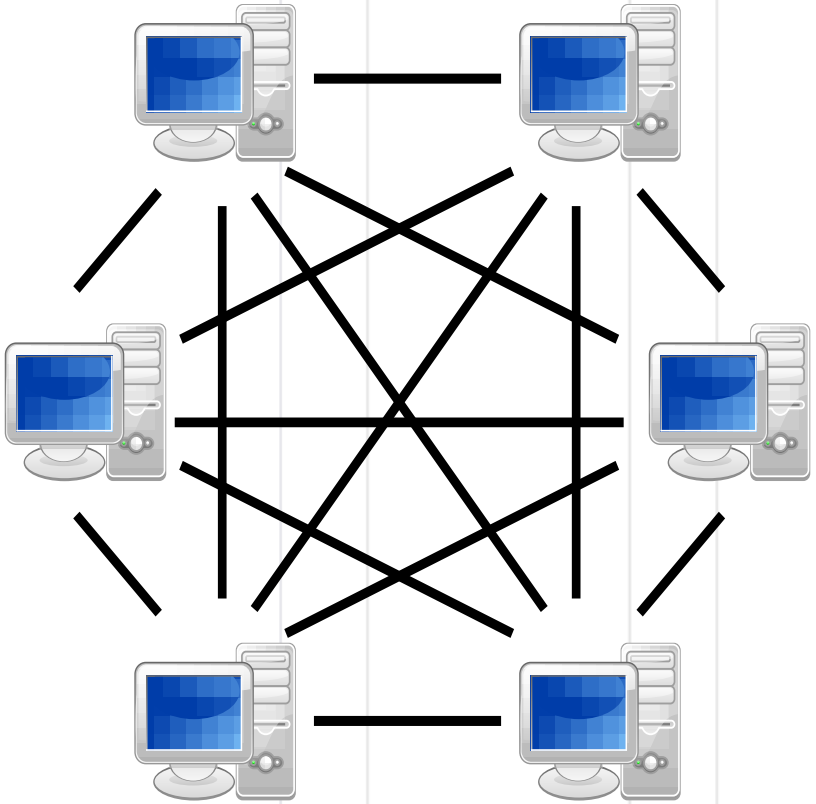
- Durable
- Portable
- Divisible
- Storable
- With intrinsic value

Cryptocurrency - Bitcoin

- Durable
- Portable
- Divisible
- Storable
- With intrinsic value
- In addition:
  - ✓ Homogeneous
  - ✓ Easily cognizable
  - ✓ Imperishable
  - ✓ In practice fully shielded from counterfeiting

Foundations for Bitcoin





Biggest P2P system

bitcoin.com | a quick tour

Step 1: Watch the video

Step 2: Get a free "bitcoin wallet"

Create an Online Wallet

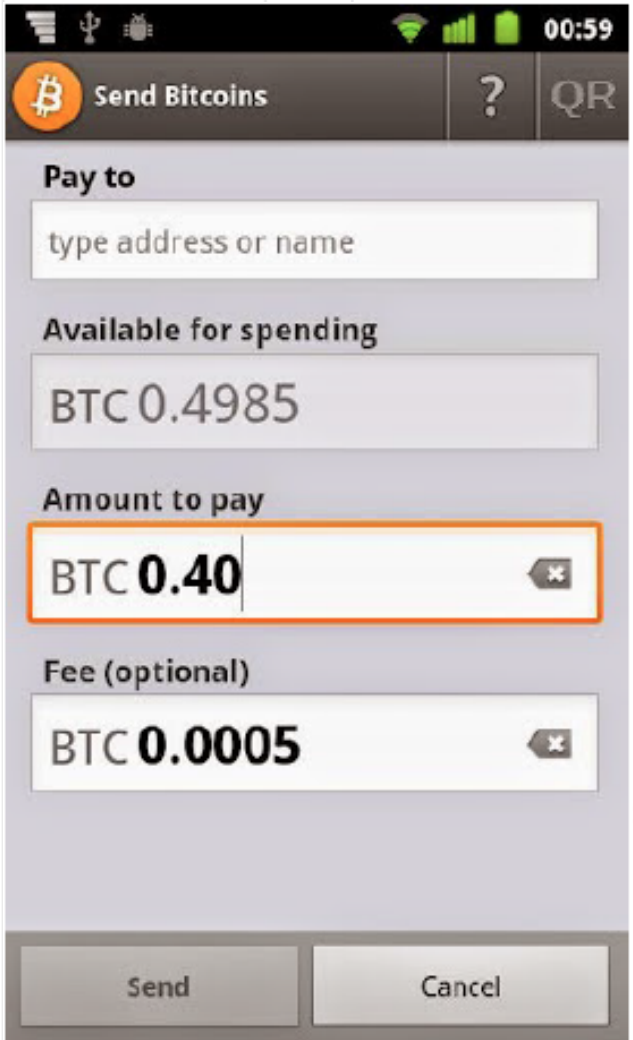
https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

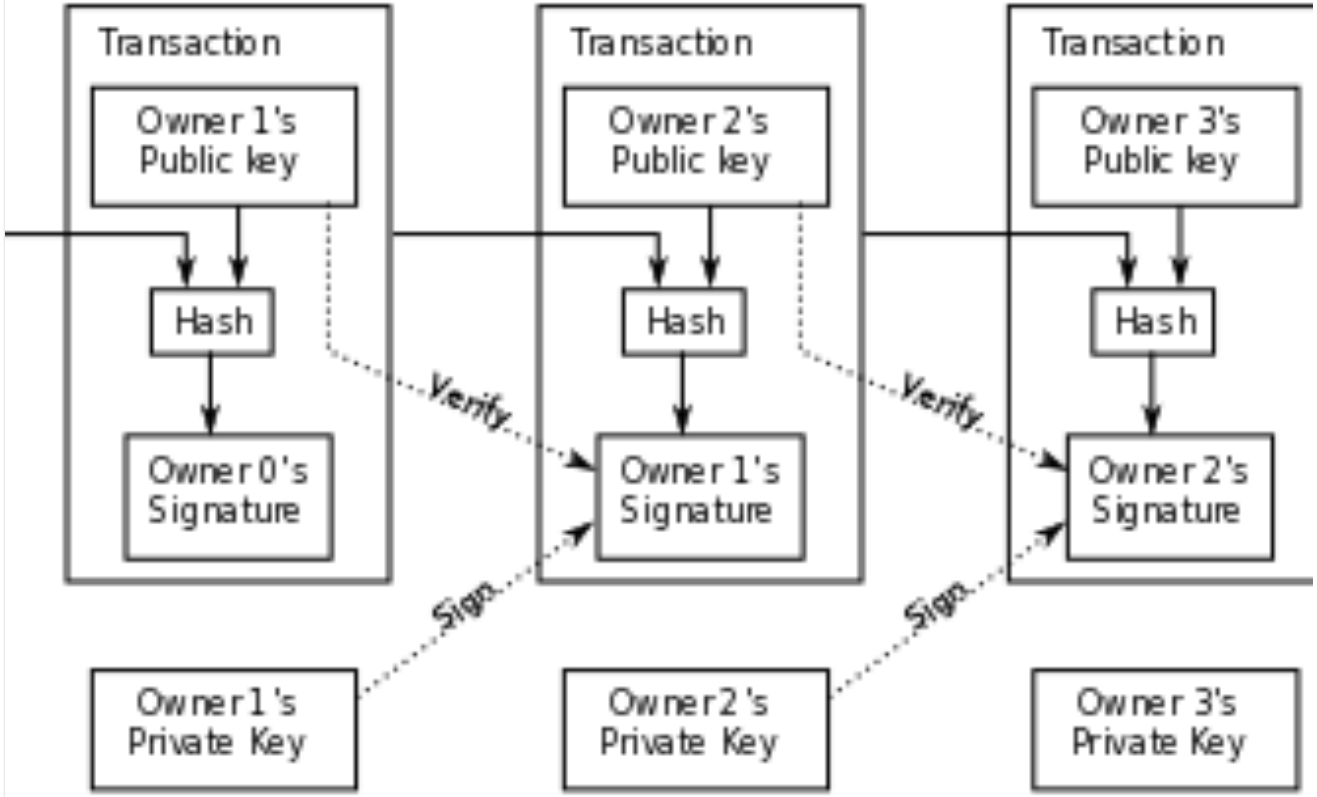
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Sending and receiving money (source: Yevgeniy Brikman)

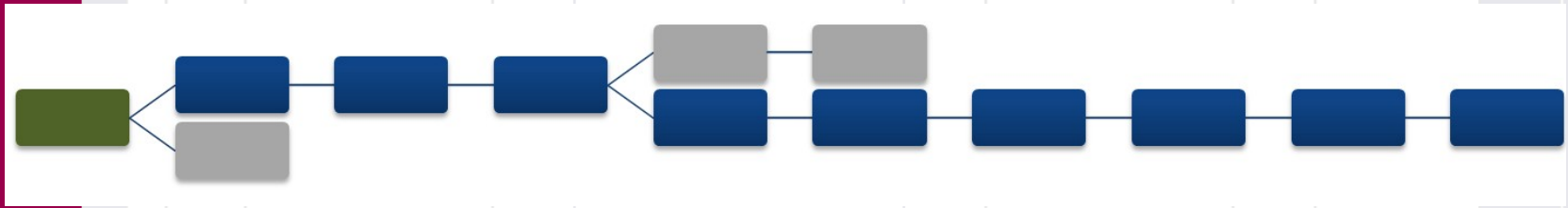


1G8qEUVUS8BBSwSWNM4EWR622vUpGtee66

How does Bitcoin work? (Wikipedia)



Blockchain



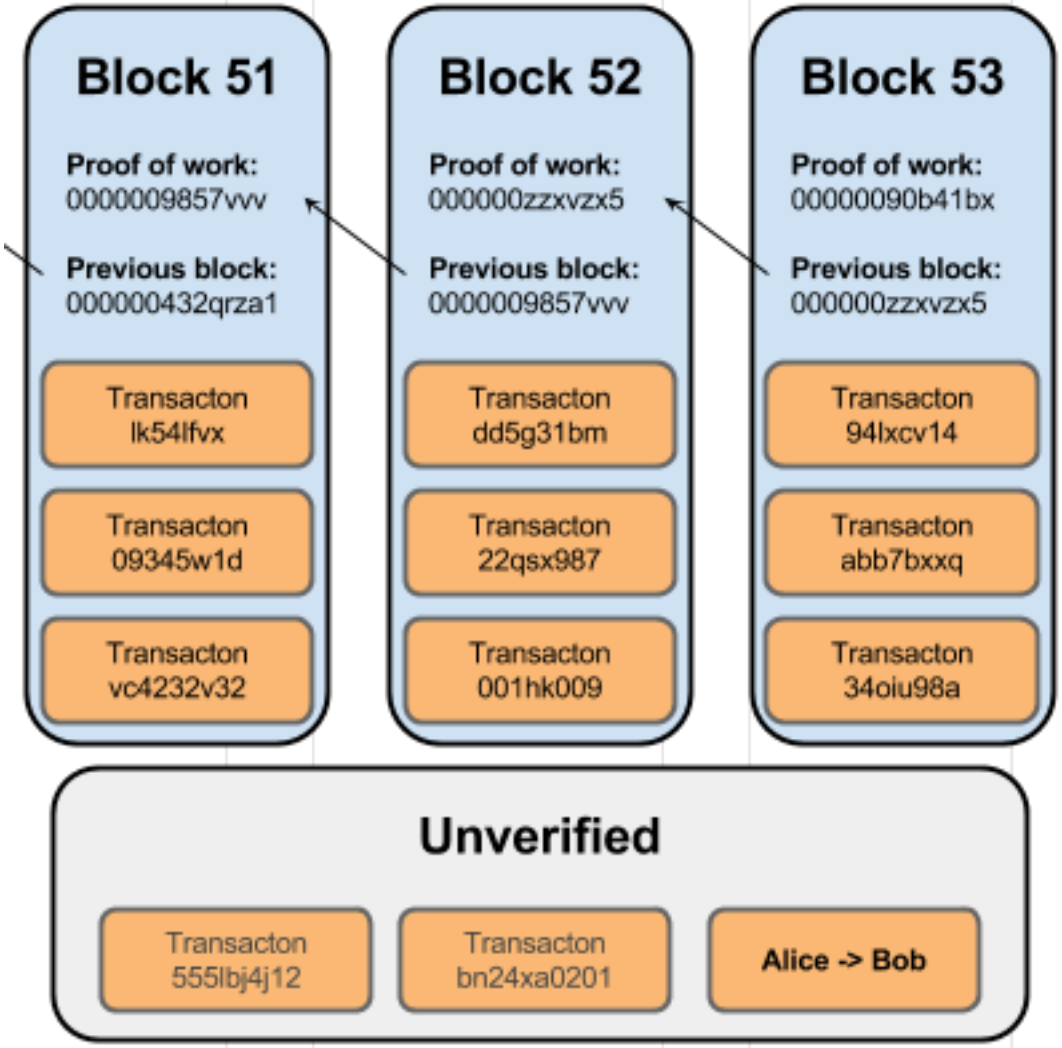
How is scarcity guaranteed?

- Collective *mining*: repeatedly verifying and collecting newly broadcast transactions into a new group of unlinked transactions called a *block*
- Each new block is a cryptographic hash of the previous block containing a link to the previous block
- Every approximately 14 days, the difficulty target is adjusted based on the network's recent performance, with the aim of keeping the average time between new blocks at ten minutes
- Incentives for mining:
  - ✓ Newly created Bitcoins
  - ✓ Transaction fees

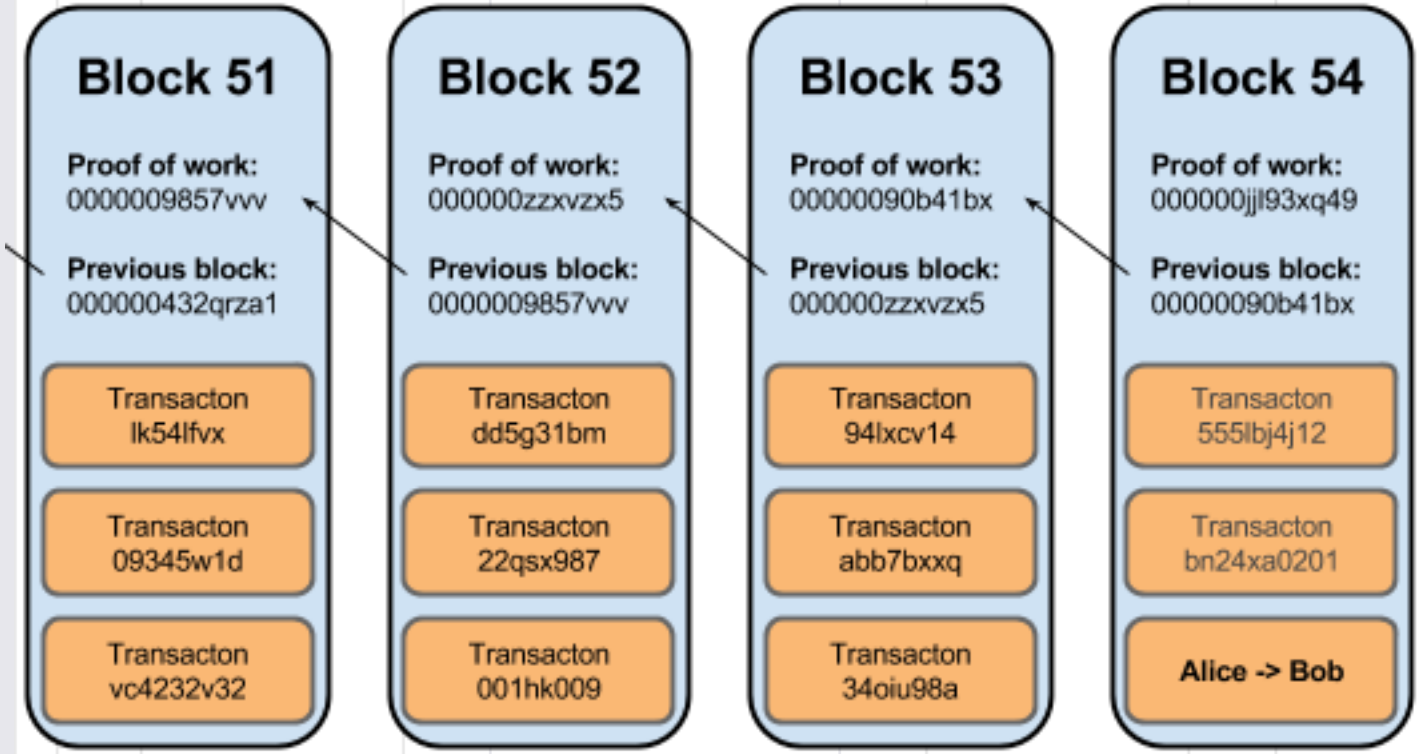
Bitcoin mining farm in Iceland

(Wikipedia: "Cryptocurrency Mining Farm" by Marco Krohn - Own work. Licensed under CC BY-SA 4.0 via Commons)

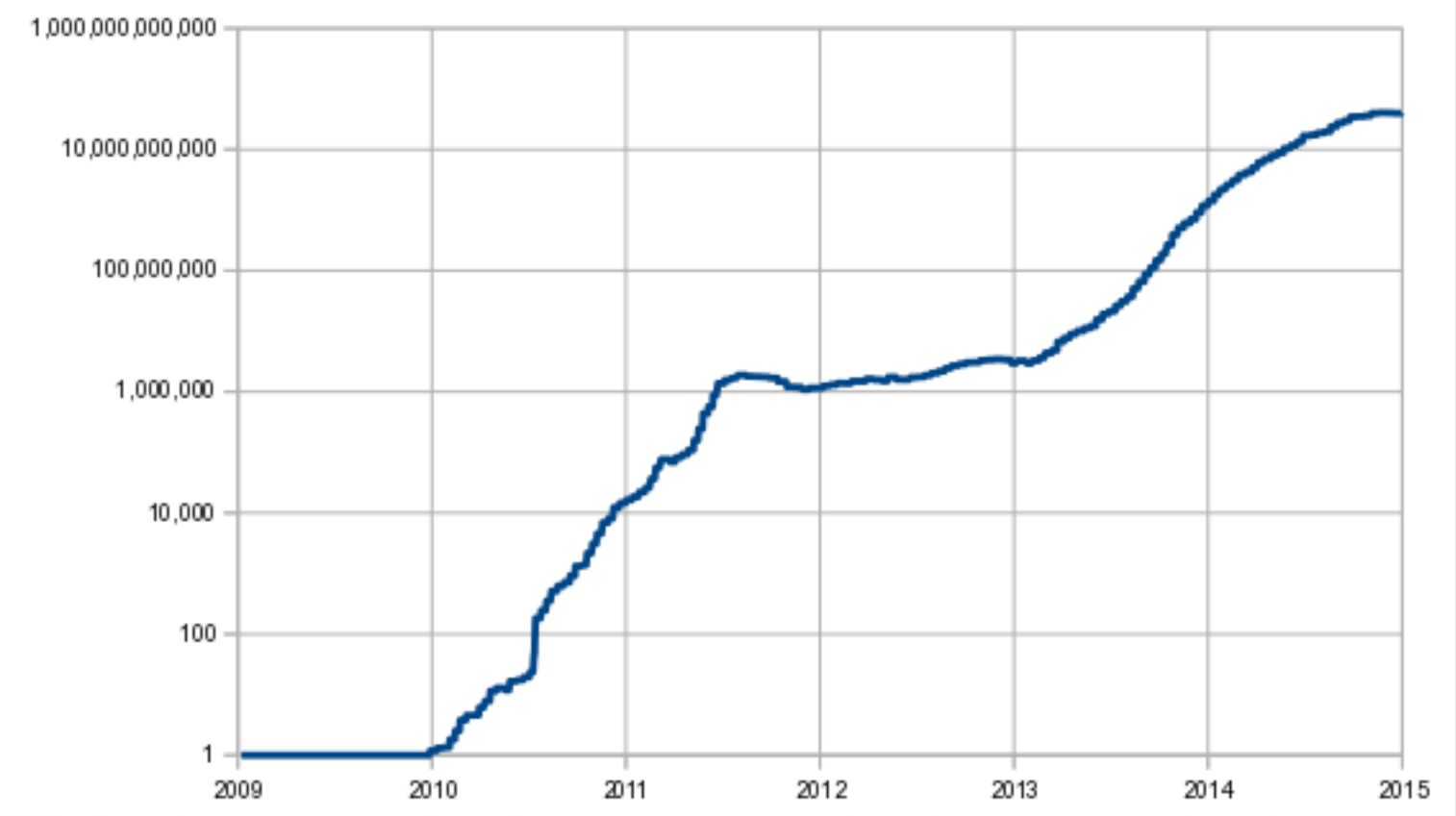
Adding a block by mining (source: Yevgeniy Brikman)



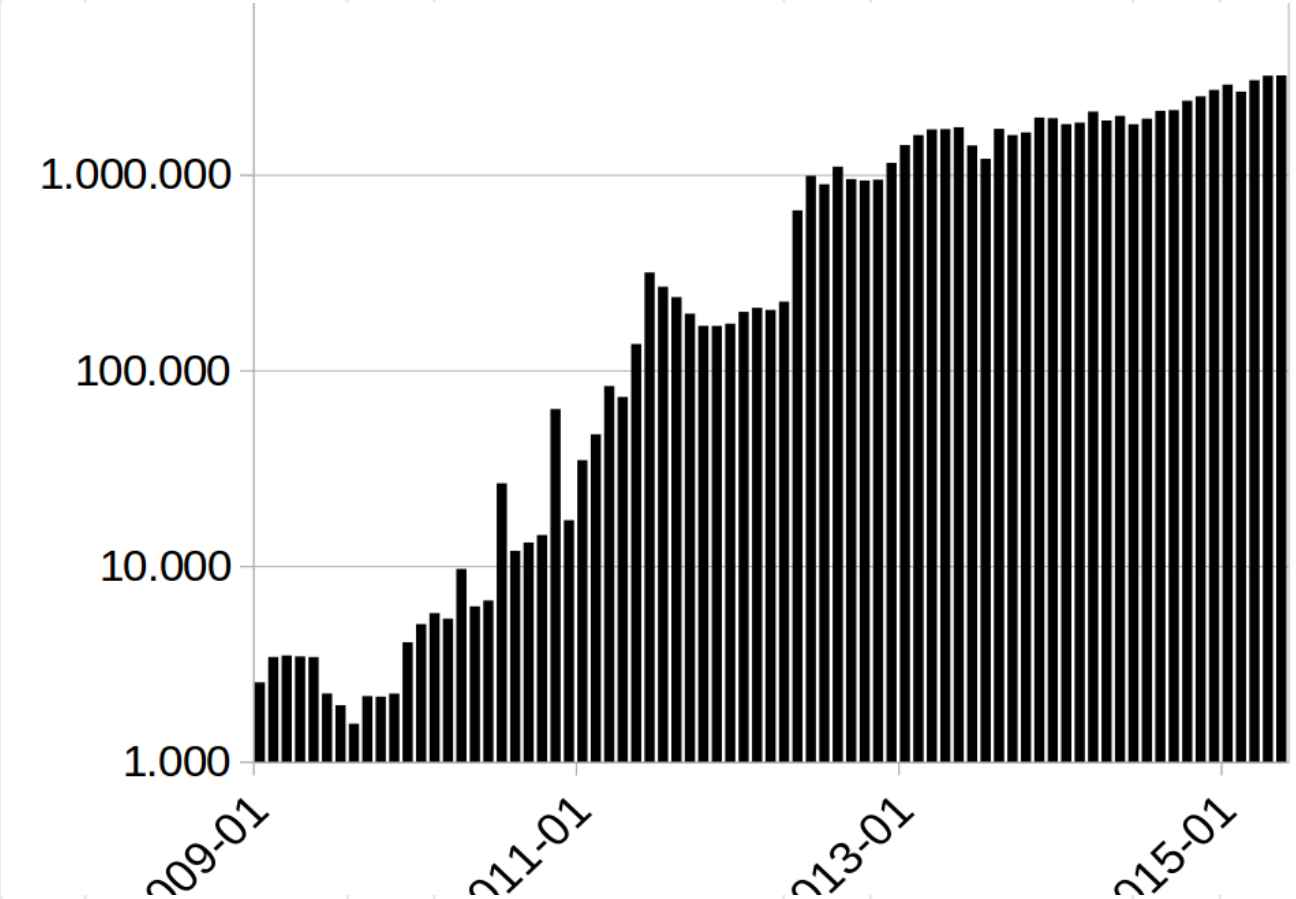
Adding a block by mining (source: Yevgeniy Brikman)



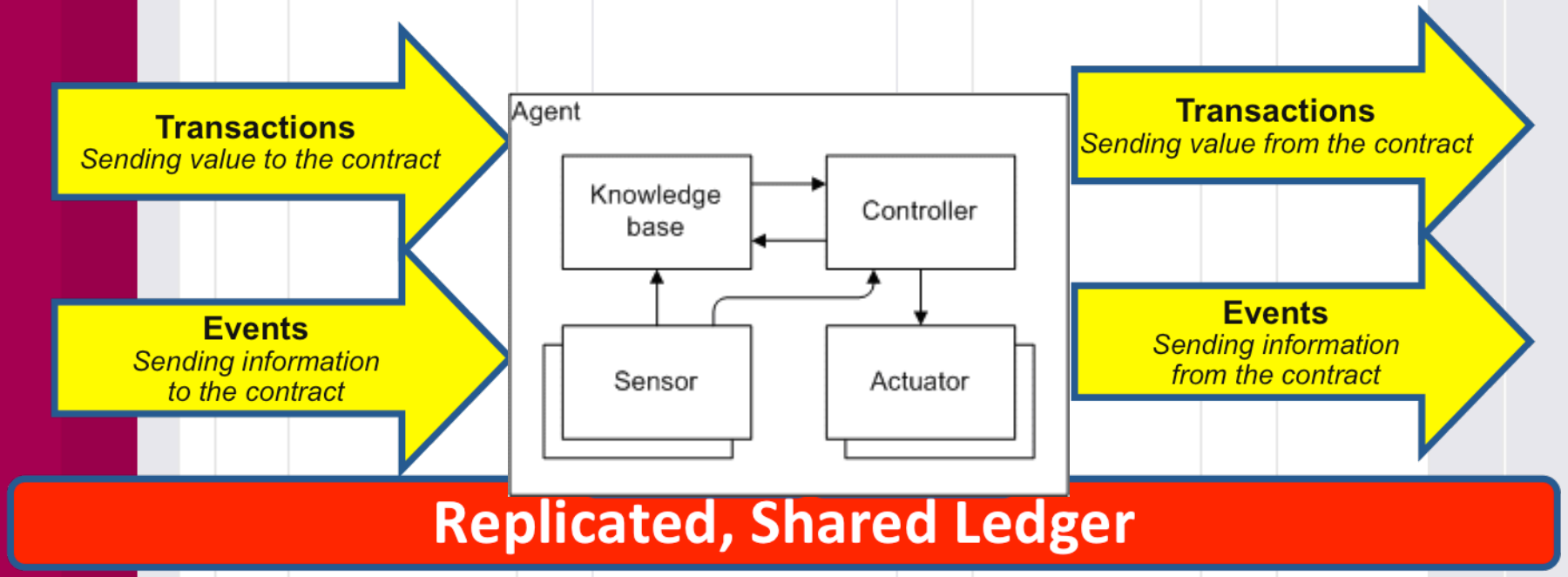
Increase of the mining difficulty (Wikipedia)



Number of Bitcoin transactions per month (Wikipedia)



Smart Contracts and Agents



Pros and Cons of a Cryptocurrency

- Pros:
  - ✓ Intrinsic value is *collectively* rather than voluntarily assigned
  - ✓ Anonymity is preserved
  - ✓ Lower transaction fees
  - ✓ Repudiation of transactions is *not* possible
  - ✓ Supports smart contracts
- Cons:
  - ✓ Requires both parties of the exchange to possess the necessary technology that gives access to Bitcoins or units of other cryptocurrencies
  - ✓ One may have to wait until the transaction gets registered in a new block
  - ✓ Requires the acceptance by the governments

Future Money: Paper or Data?