Blockchain and Payment Systems: A Tale of Re-intermediation

Agnieszka Janczuk-Gorywoda

Utrecht University

A.A.Janczuk-Gorywoda@uu.nl

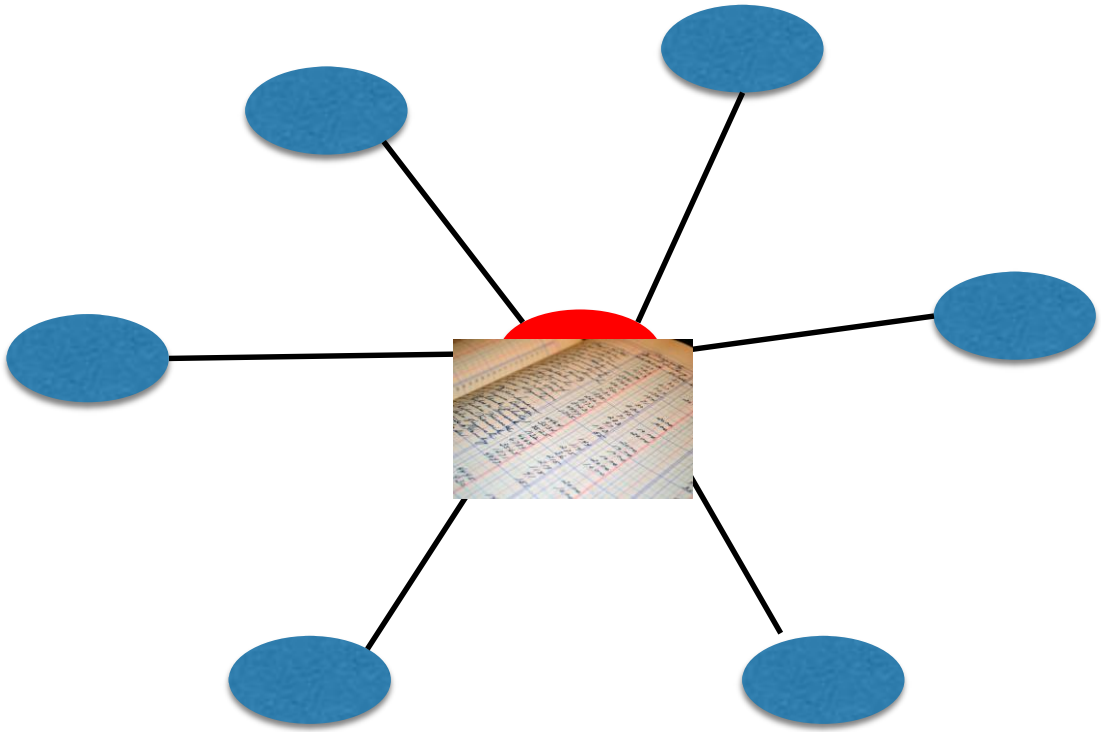
Blockchain and Payment Systems

- What is Blockchain?
- Blockchain's Ideology
- Institutional Dimensions of Money and Payment Systems

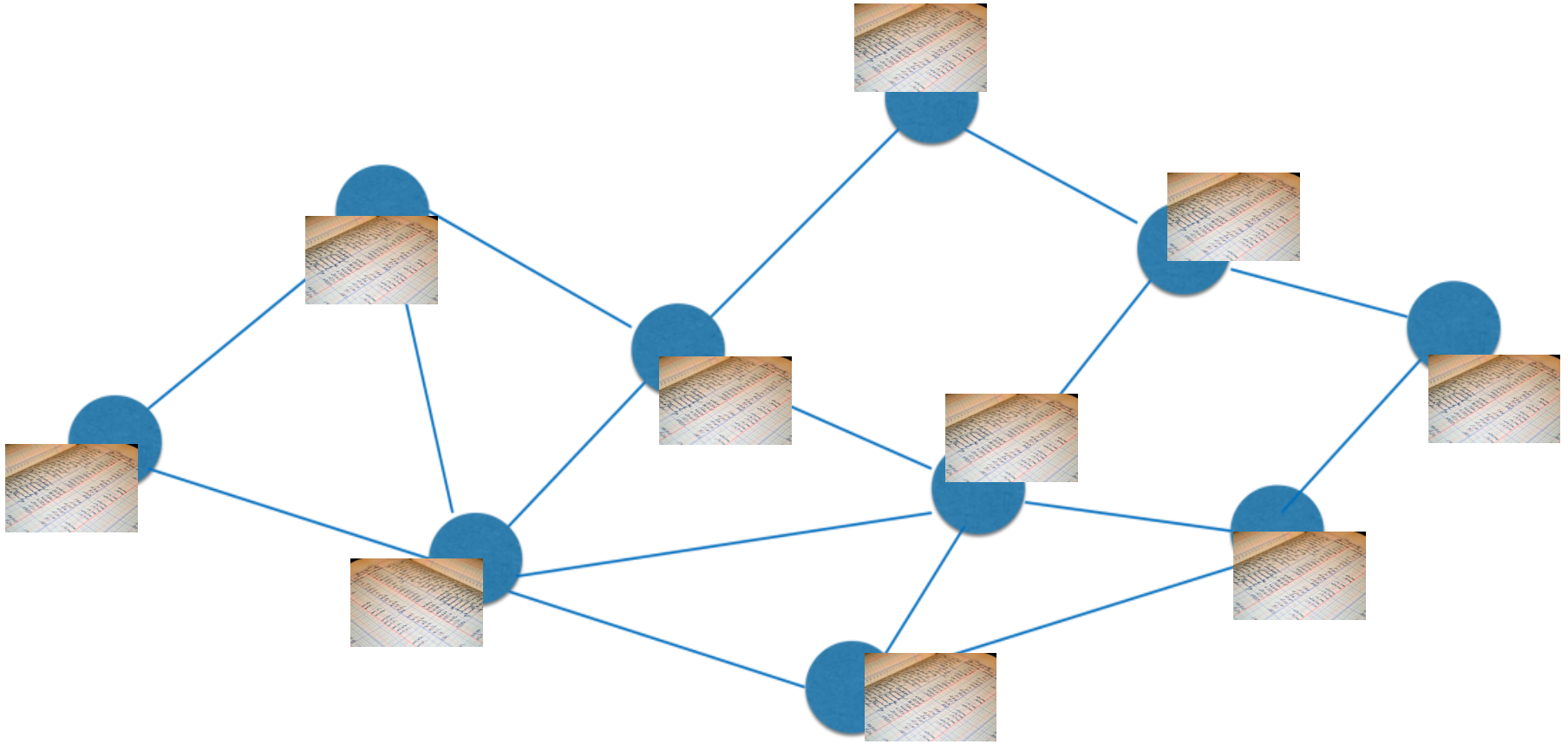
- Will public Blockchain-based currencies become mainstream payment systems?
- Can technology replace institutions of the state and central intermediaries to build trust necessary for the functioning of a large-scale and complex payment system?

What is Blockchain?

Traditional system of trust – trusted third party



Blockchain as a distributed ledger

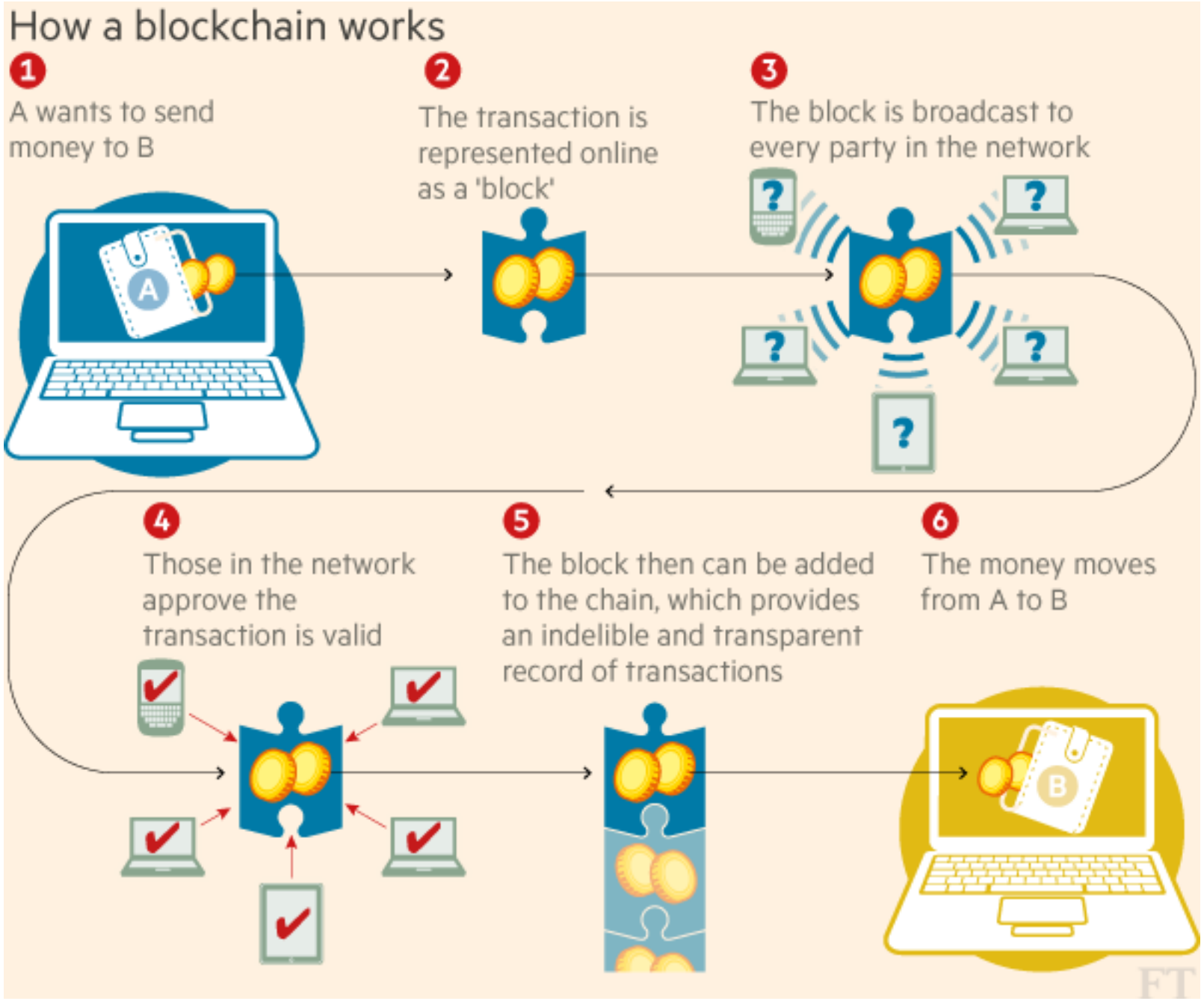


Protocol

- In an information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interaction between the communicating entities.
  - “How we do things”
- TCP/IP, 1980 – led to the Internet
- HTTP, 1990 – enabled the World Wide Web
- Bitcoin, 2008

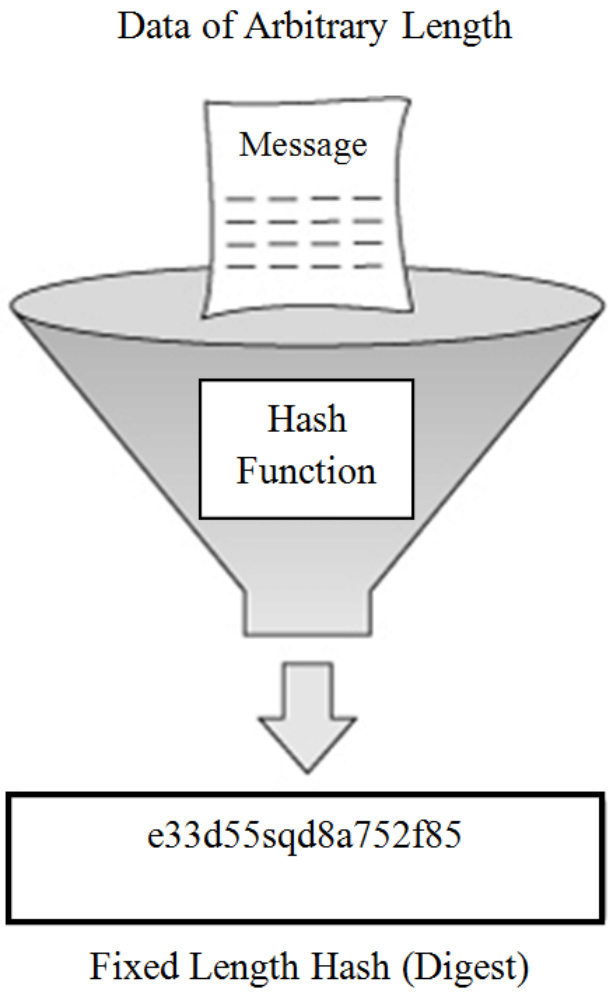
Consensus protocol

- Miners
  - Collect transactions
  - Verify transactions
  - Create new blocks
  - Invest power and electricity
  - Get rewarded
  - Guarantee the blockchain consensus
- Proof of Work
  - Hard computation
  - Takes time
- Others:
  - Proof of Stake etc.



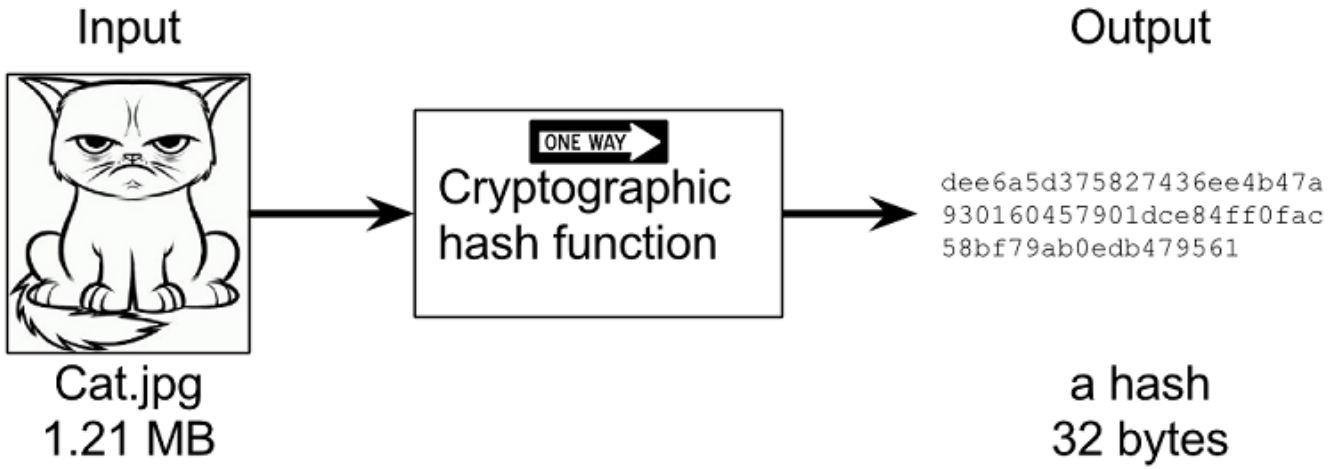
Security

- Tamper proof
- A hash function is a set of procedures and steps or a mathematical function that can be used to convert a a large amount of data into a small data string and integers that can be used as an index as an array.
- A digital fingerprint of a file



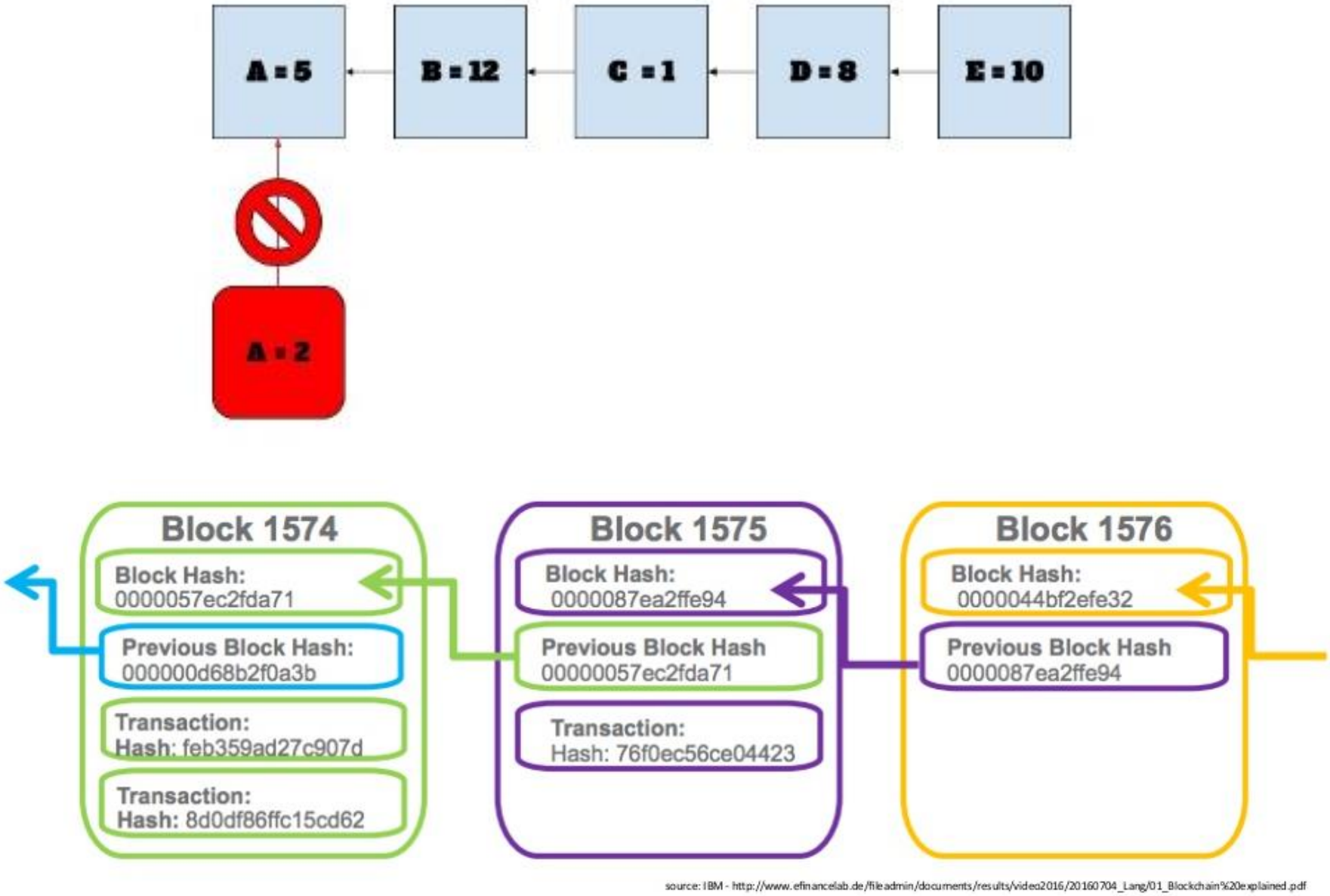
Cryptography

- a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it
- complexity is injected into data so that only those who possess a key can remove the complexity intended message, while those without the key will not be able to retrieve the hidden message in a timely manner.



Immutability

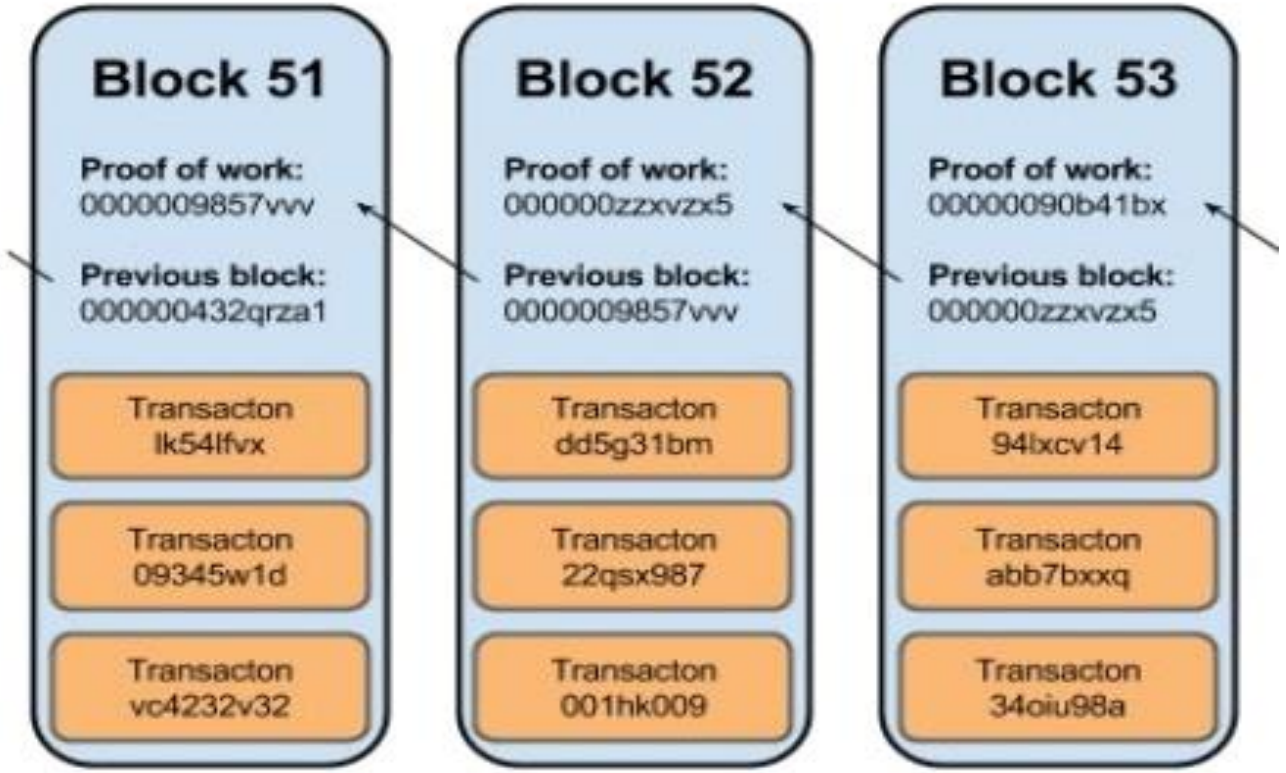
- Unable to be changed over time
- Once recorded, data on the blockchain cannot be changed retroactively without the alteration of all subsequent blocks and a collusion of the network majority.



source: IBM - http://www.efinancelab.de/fileadmin/documents/results/video2016/20160704_Lang/01_Blockchain%20explained.pdf

Transactions are grouped into 'blocks', then stored forever in a 'chain' by linking each new block chronologically with the hash of the preceding block

- Put transactions in Blocks
- Chain the blocks
- Order chronologically



Blockchain and Ideology

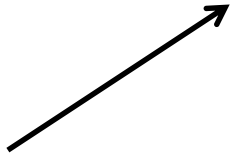
Public versus private blockchain

Public/open/permissionless blockchain

1. Open to anyone
2. Often anonymous
3. No central authority
4. Often several builders
5. Often open source
6. Difficult to organise a form of governance

Private/closed/permissioned blockchain

1. Access only by inventation
2. Not anonymous
3. Central authority is possible
4. Often one builder
5. Often closed source
6. Easier to organise a form of governance



Real blockchain?

Blockchain and Payment Systems

Bitcoin as money

- Self-anchored asset used as means of exchange

Institutional dimensions of payment systems

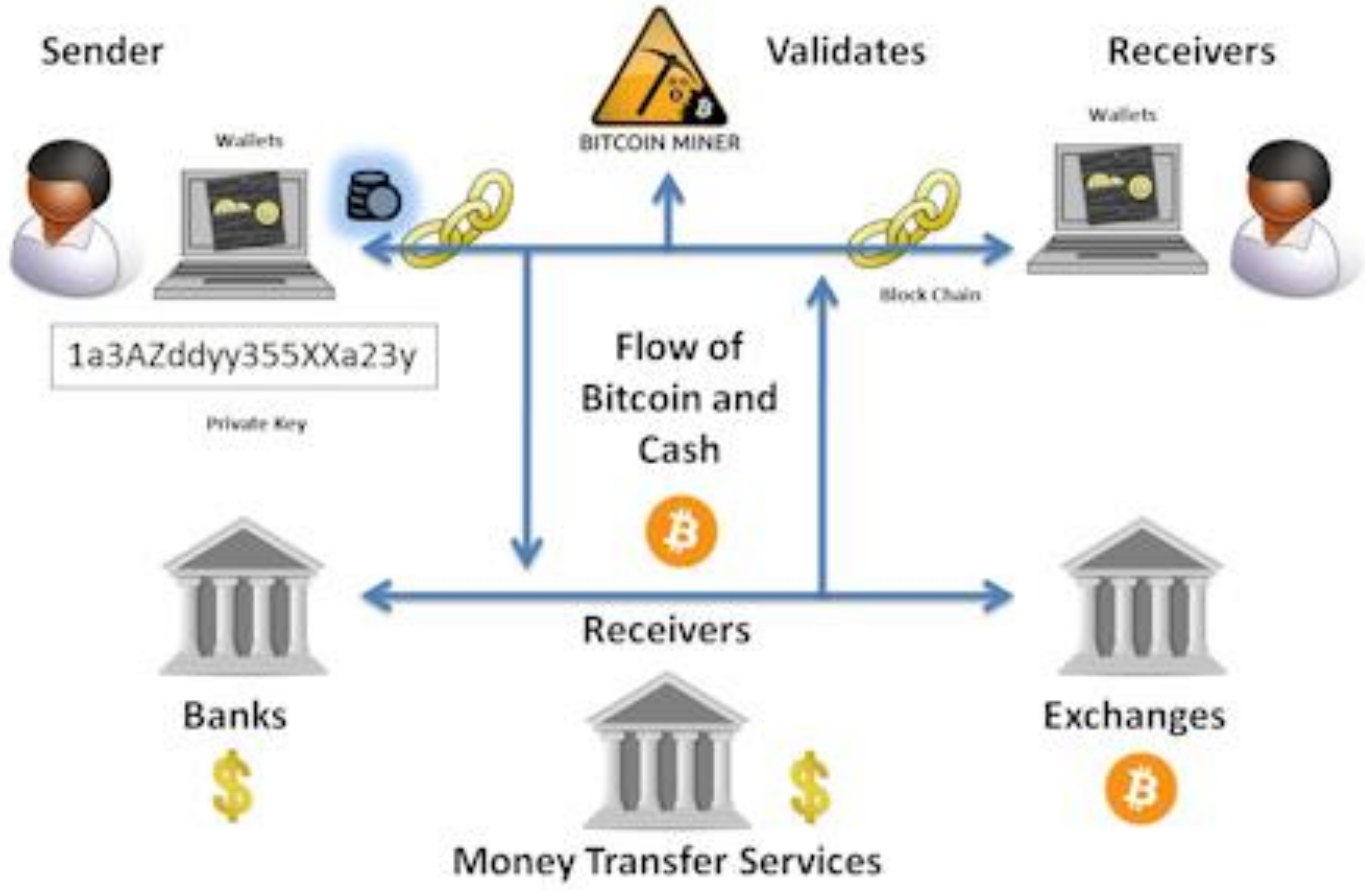
- Rules and enforcement institutions enable transfer of money
- Hierarchy of money: different levels of acceptance
  - → Different price, liquidity etc
-

Public acceptance of money is based on trust

- (1) that its issuer is capable of – and that it will – maintain the money's value over time,
- (2) that the money will be available even in times of financial stress,
- (3) that the money is capable of discharging monetary obligations, and
- (4) that the money's functionality and convenience of use is reliable.

→ For that the institutional and legal framework supporting money, including the payment system, is crucial!

Bitcoin as a Payment System



Advantages of Blockchain for Domestic Payments

- Shorter settlement times?
- Lower Costs?
- Protection against fraud?
- Pseudonymity

- Stability of value?
- Legal certainty?
- Consumer protection?

Advantages of Blockchain for Cross-border Payments

- Cheaper and faster ✓
- International remittances
- Transactions between business partners
- Transactions between strangers

The trustless trust?

- Delivery-versus-Payment
- Escrow Accounts and … Intermediaries

Conclusion

- Blockchain will not lead to the development of major decentralised payment systems
- In contrast:
- It will either lead to the emergence of new powerful intermediaries
- Or it will be embraced by the established payment services providers
  - Other then pseudonymity, Blockchain is not competitive enough when compared to national payment systems
  - The existing decentralized Blockchain solution does not solve the problem of the lack of trust between the parties to transnational transactions