Bundesanstalt für
Finanzdienstleistungsaufsicht

BaFin

Blockchain aus Anwendersicht

DIN Spiegelgremium zu ISO/TC 307 Blockchain and electronic distributed ledger technologies

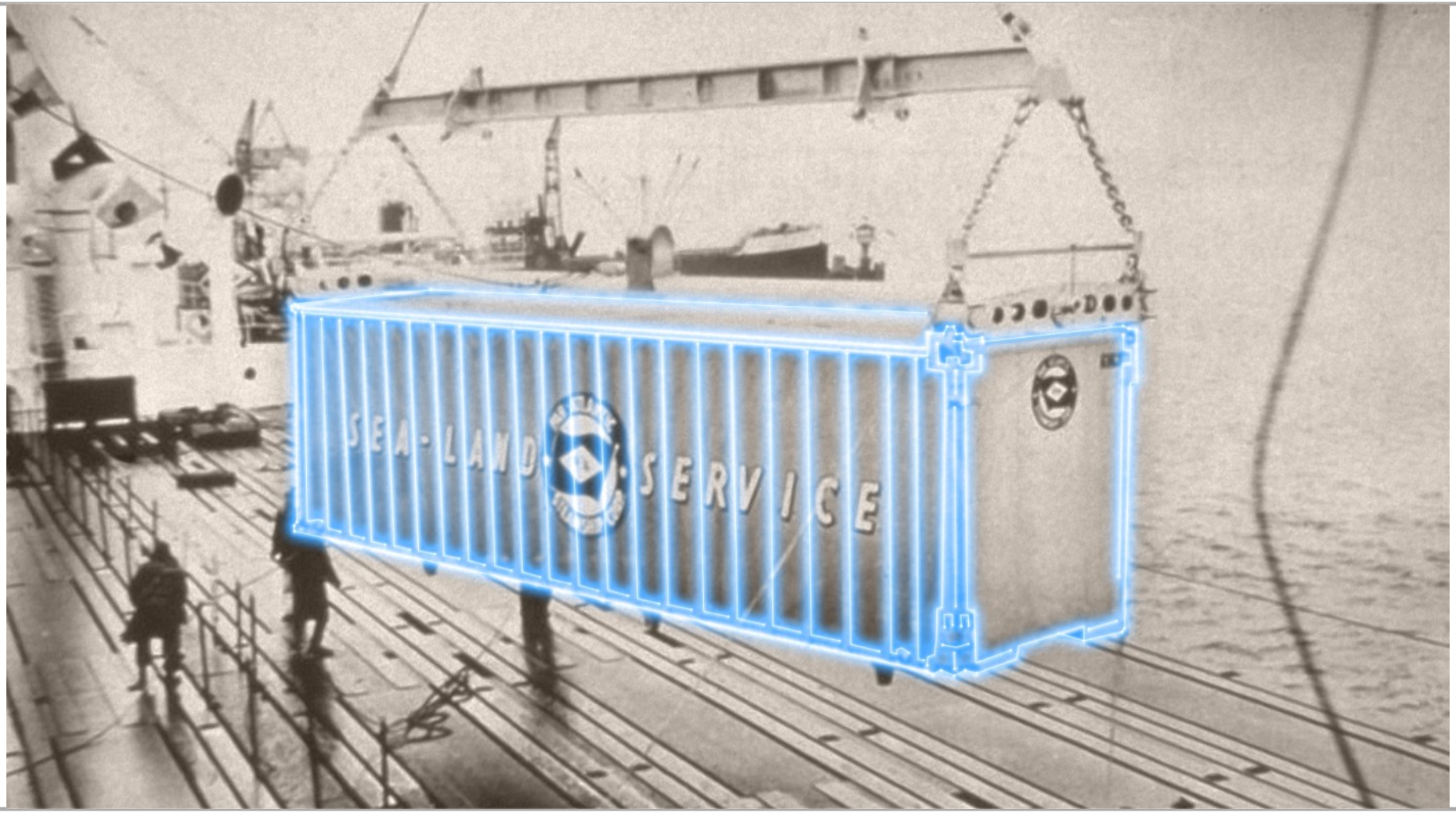
10. Januar 2017, Berlin

History → Cost and complexity

BaFin

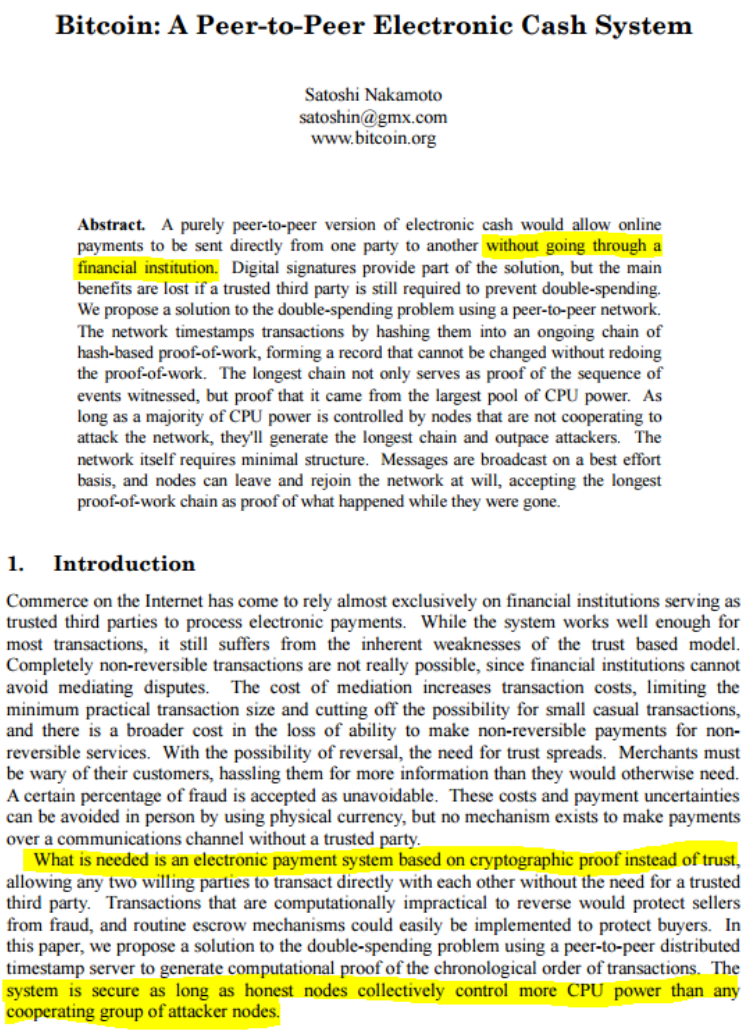
Standardization

BaFin



Globalization

BaFin



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.

1. Introduction

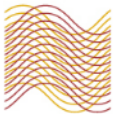
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

"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."
[…]
"an electronic payments system based on **cryptographic proof instead of trust**…"
[…]
"The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes." […]

Trusting organisations → Trusting math!

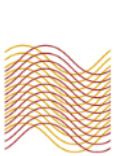
Video: Blockchain, A short introduction



BaFin

https://www.youtube.com/watch?v=WiRFuHXHBhk

Challenges for Blockchain adoption



- Lack of understanding, resources
  - Complex mathematics/cryptography
  - Biased by Bitcoin
  - Limited computational power of participants
- Should everyone know everything?
  - Existing financial infrastructure built on bilateral relationships and limited transparency
- **Industry standard → Which blockchain to trust?**

Why Blockchain standardization?

BaFin

„Cost of operations, Capital, Control, + compliance, …“

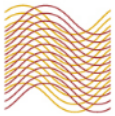
- The World Values Survey
- (www.worldvaluessurvey.org) is a global network of social scientists studying changing values and their impact on social and political life, led by an international team of scholars, with the WVS association and secretariat headquartered in Stockholm, Sweden.
- The survey started first 1981.

The World Values Survey

- Arrow (1972) says that "Virtually every commercial transaction has within itself an element of trust, certainly any transaction conducted over a period of time."
- There is a very strong positive relationship between trust and GDP.
- Algan and Cahuc (2010) predict that, according to their estimates, African countries would have a five-fold increase in GDP per capita if they had the same level of inherited social attitudes as Sweden.

Country by country: Trust vs. GDP per capita

Shown is the share of people agreeing with the statement "most people can be trusted".
For each country the latest available data is shown.



BaFin

Scope of ISO/TC 307

BaFin

ISO/TC 307 Blockchain and electronic distributed ledger technologies

- Standardization of blockchains and distributed ledger technologies to support **interoperability and data interchange** among users, applications and systems.

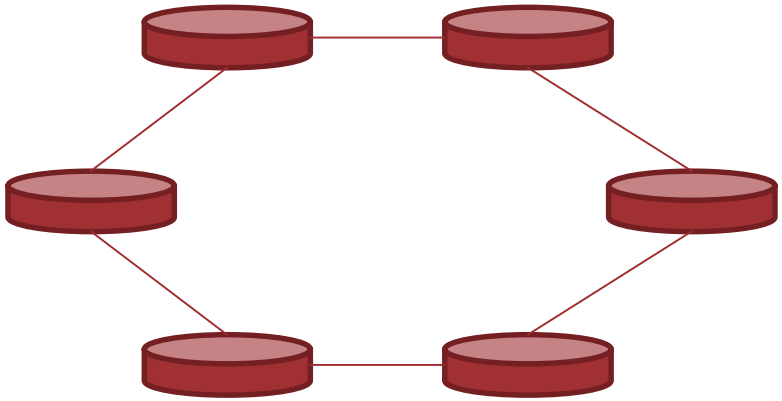
Demands for the supporting infrastructure

BaFin

- Very high transaction volumes
- Immediate/Instant transactions, worldwide
- Trivial unit cost
- Minimal or no transaction fees
- No delays, no failures

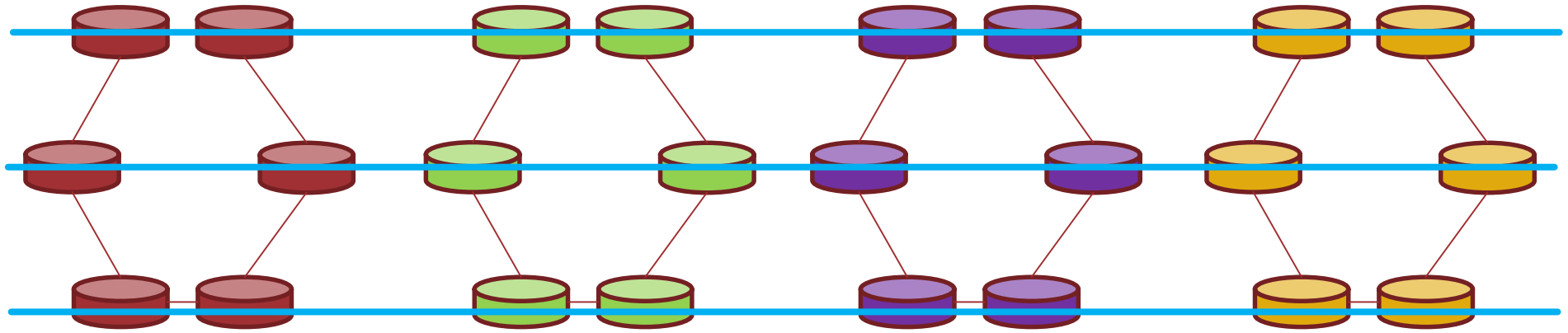
Blockchain concept

BaFin



A different way how transactions are recorded.

Interoperability and data interchange



BC-1 BC-2 BC-3 BC-4

Status Quo → Blockchain

Expectation all features of existing (payment) systems…
+ secure, scalable, reduce cost, set free capital
increase speed, …

Understanding → Knowing/remembering

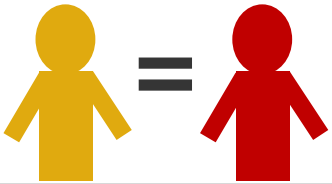
→ Understanding

→ Applying

→ Analysing

→ Evaluating

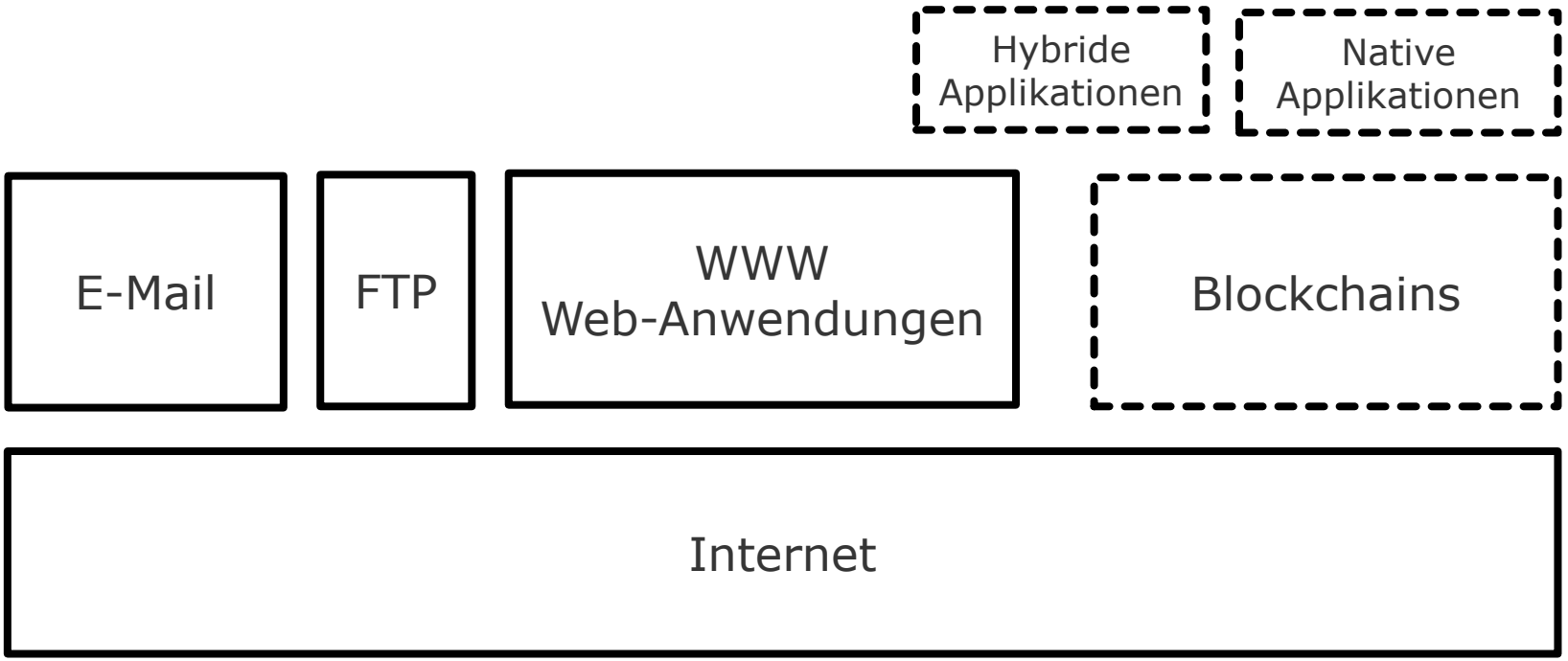
→ Creating (Creativity)



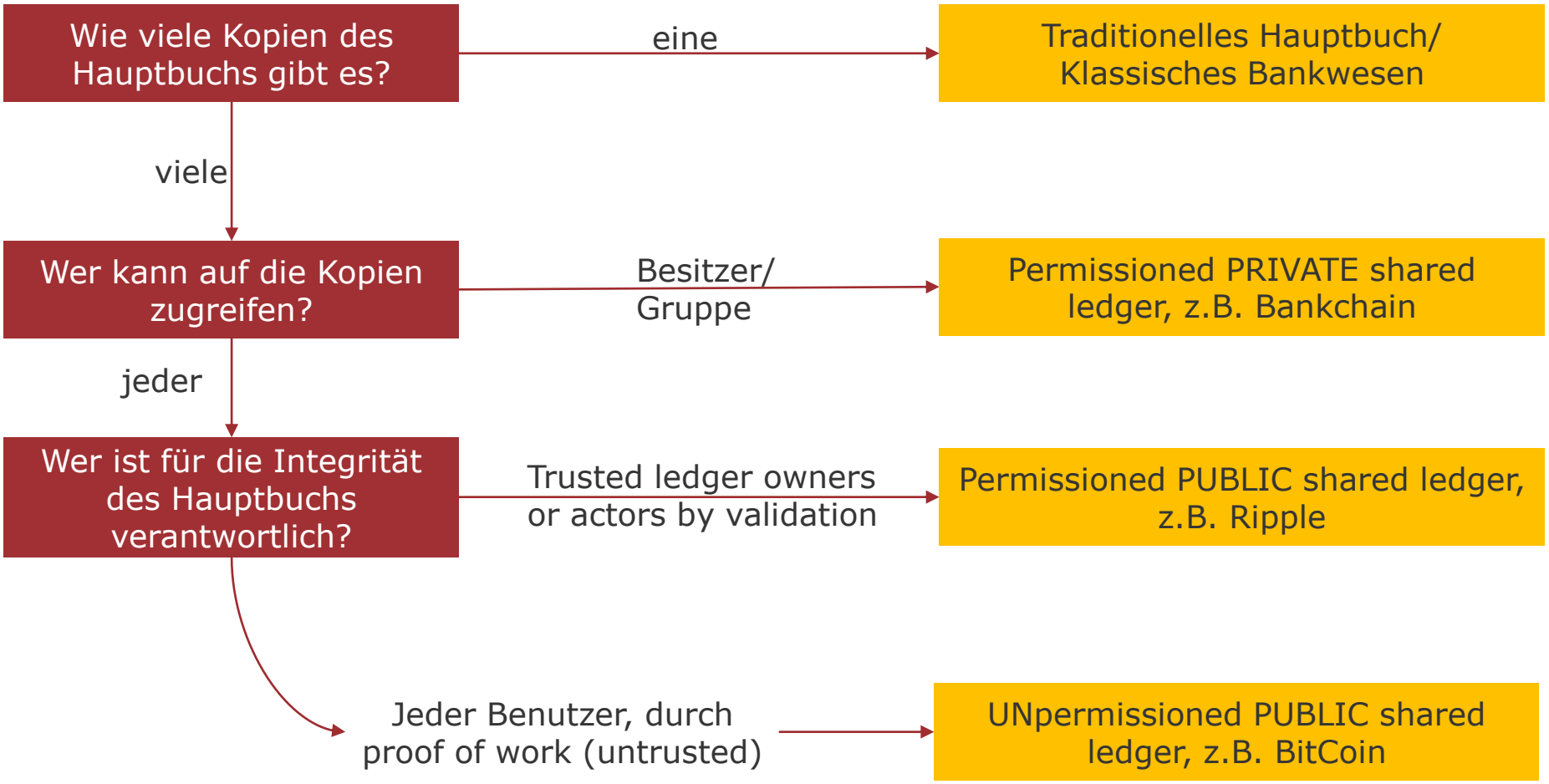
Source: Bloom's taxonomy

Blockchain-Taxonomie

BaFin



Blockchain-Taxonomie



Principles of industrialization

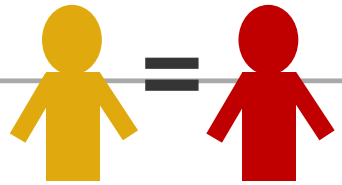
BaFin

1. Standardization
2. Specialization
3. Automatization
4. Quality orientation

Source: Riese, 2006, page 53 ff.

Possible standardization points (1)

BaFin

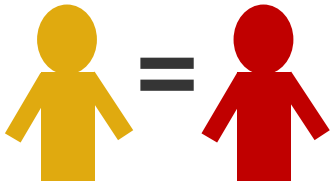


1. Terminology and ontology
2. Current requirements (for Financial transactions specifically: AML regulation, PSD2, KWG, ZAG)
3. Interfaces, API
4. Time → How to enable Instant-Transactions with End-to-End confirmation?
5. Finality – Immutability/guarantee of transactions?
6. Real World-API – How to connect goods, services or currencies of the real world with the Blockchain?

Possible standardization points (2)

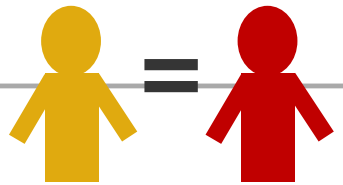
BaFin

7. What Governance-Model should be implemented?
8. Which Governance questions should be addressed?
9. How will Governance be continuously developed?
10. Code is the law. vs. Hard Fork?
11. Smart contracts and interoperability
12. Integration vs. Disruption? → How would a standardized Blockchain fit into existing (Finacial) Markets?



Possible standardization points (3)

13. Changing of underlying cryptography?
14. Data Privacy → Is a full transaction history in accordance with data protection rules?
15. Law → So far no landmark decision of a court regarding a transaction purely based on a blockchain. High degree of uncertainty!
16. Risk of strength of Cryptography
17. Risk of monopoly of resources (PoW)
18. What security model/rules will be implemented to adress i.e. Cyberattacks?



Blockchain-interoperability → an overview

BaFin

- Ripple → Interledger Protocol
- BigChainDB
- PolkaDotPaper (Gavin Wood)
- ISO TC 307…

Discussion

Questions,

indications,

suggestions, …

Christoph Kreiterling
christoph.kreiterling@bafin.de
0228-4108-2464
BA 51- Competence centre IT security