



The Post-Bitcoin Era

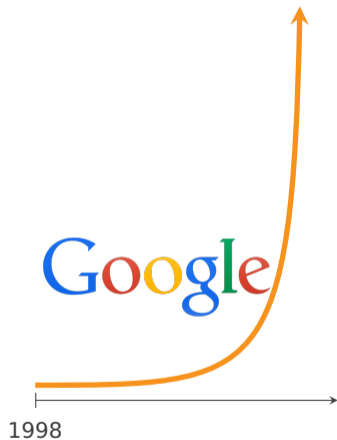
Cryptocurrencies Are Here to Stay

Rainer Böhme

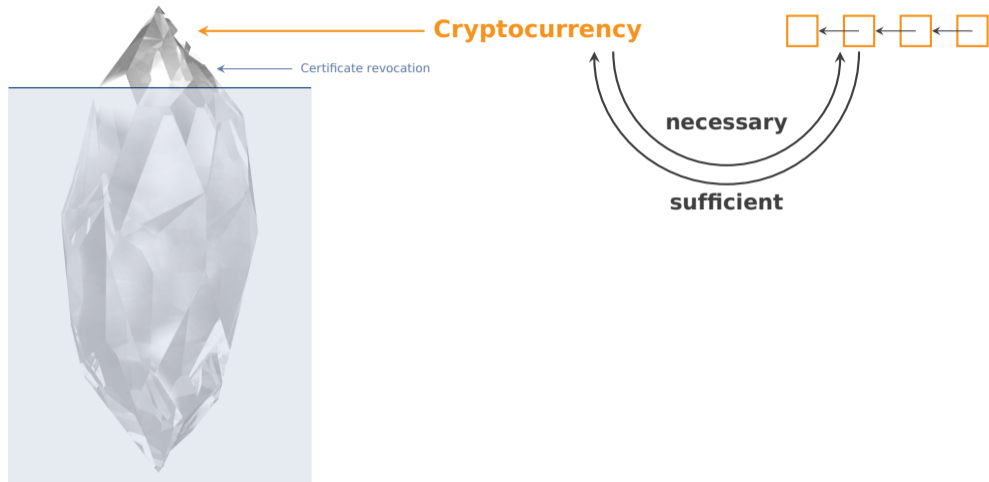
Agenda

- 1. Past**
2. Present
3. Future

Different Adoption Paths



Searching for the Blockchain Killer App



Searching for the Blockchain Killer App



Economic Potential

Number of feasible allocations depending on the development of institutions

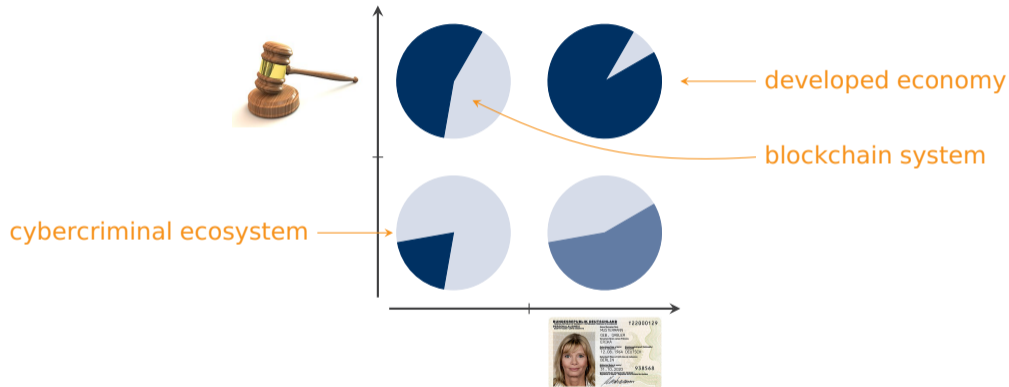
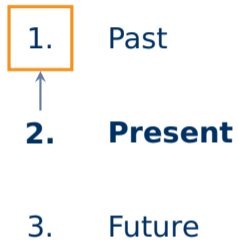
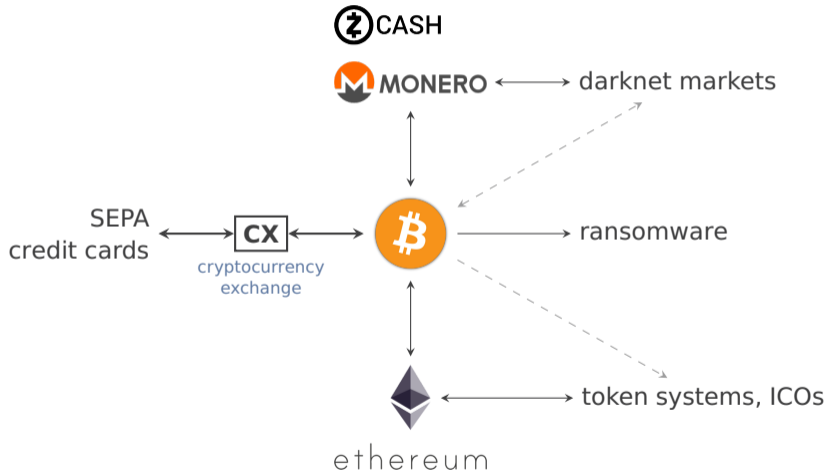


Image sources: Bundesrepublik Deutschland, CC-BY-2.0 Chris Potter

Agenda

1. Past
 2. **Present**
 3. Future
- 

Bitcoin is the Entry Point to the Post-Bitcoin Universe



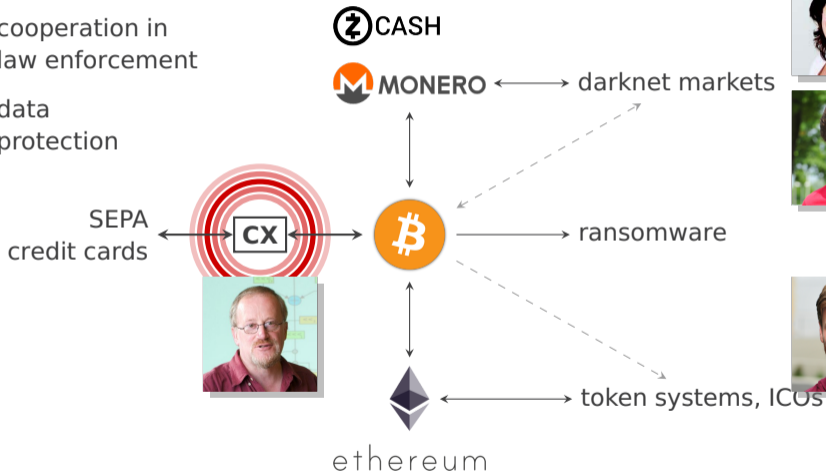
Mapping Today's Talks



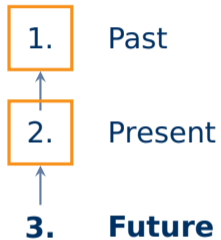
cooperation in
law enforcement



data
protection



Agenda



Scalability

Motivation in numbers

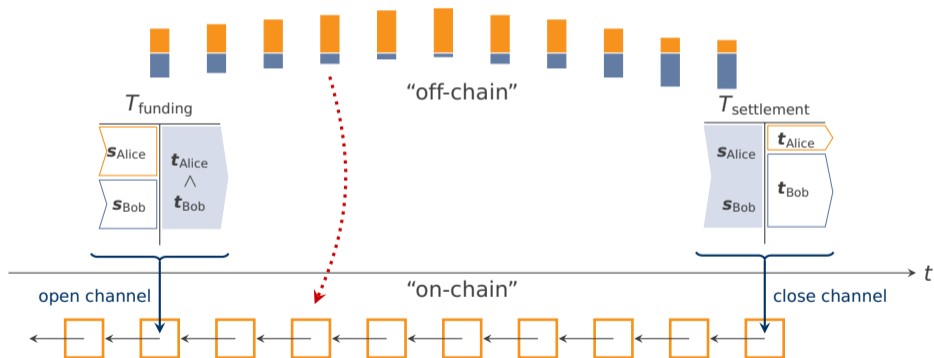
Transactions per second	Bitcoin	Visa
Average		2 000
current (24 h)	3.1	
Peak		56 000
1 MB block size	7	
90 % of P2P nodes	27	

Sources: blockchain.info, 16 October 2018, Visa Tech Matters, 2014, Croman, K., et al. On Scaling Decentralized Blockchains. In Clark, J., et al. *3rd Workshop on Bitcoin and Blockchain Research*, LNCS 9604, Springer, Berlin, 2016, 106–125.

Off-chain Payment Channels

Analogy Turn the blockchain from a global sales check to an archive of court records.

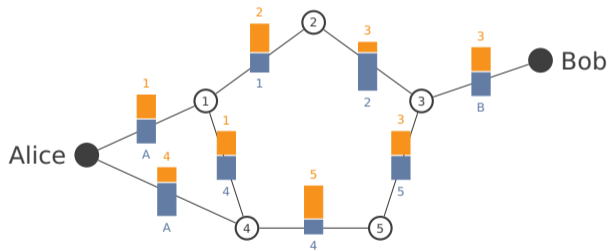
- Transaction partners put money aside and keep local accounts.
- In case of dispute, the **last agreed** state can be enforced on the blockchain.



Generalization to Off-chain Payment Networks

Problem Too many potential payment relations to fund with bilateral channels.

- Connect bilateral channels to a network
- A playground for researchers: routing, fees, topology, atomic end-to-end swaps, security, privacy, . . . , **forensics?**

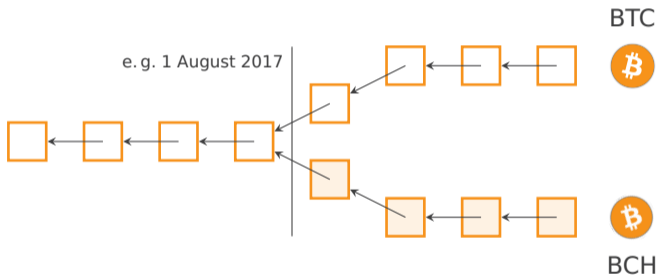


Decker, C., Wattenhofer, R. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. In Pelc, A., Schwazmann, A., eds., *Stabilization, Safety, and Security of Distributed Systems*. LNCS 9212, Springer, Berlin, 2015, 3–28.

Blockchain Forks

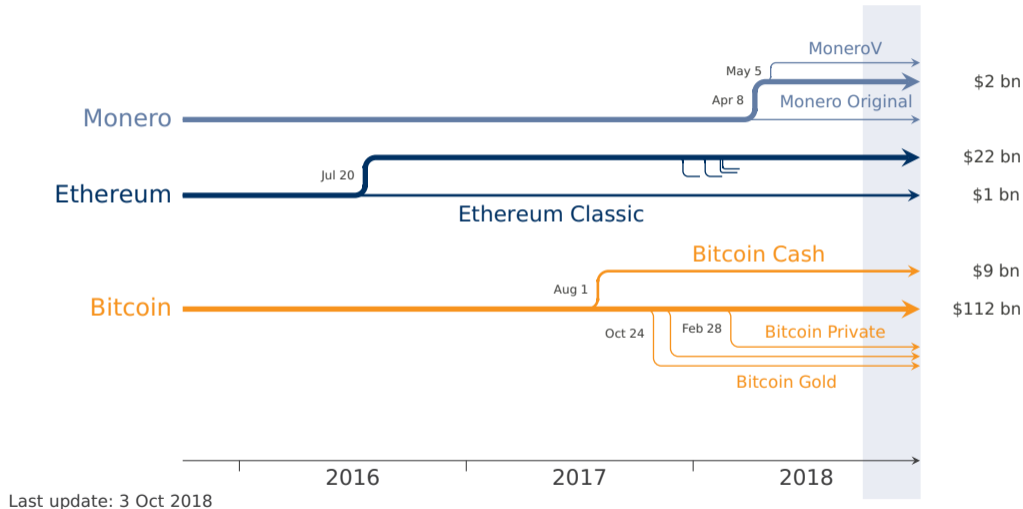
Dissent with common history

- Miners split in fractions who continue the public database using different rulesets.



- (Old) users enjoy a “duplication” of their currency units.
- This yields critical mass quickly, in contrast to conventional altcoin launches.

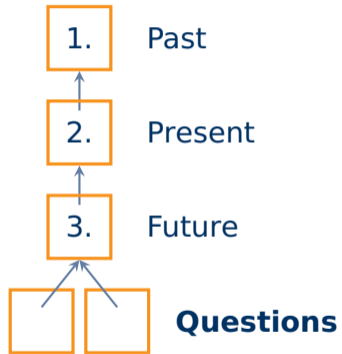
Timeline of Selected Forks



Summary

- The **pace of development** and the **complexity** of the matter render effective regulation and law enforcement difficult.
- Bitcoin's limits have lead to **post-Bitcoin cryptocurrencies** in two ways:
 1. cryptocurrencies that make money-flow tracking harder, and
 2. cryptocurrencies that offer platforms for all kinds of virtual assets.
- Despite undeniable potential, we see very **few legitimate applications** of cryptocurrencies widely adopted in practice.
- The **lack of legal certainty** around cryptocurrencies, combined with excitement and public experiments, has driven consumers into the arms of shady businesses.
- As there is no sign that cryptocurrencies might disappear in their second decade, **it is time for regulators to change the trajectory.**

Agenda





The Post-Bitcoin Era

Thank you for your attention.

Rainer Böhme · rainer.boehme@uibk.ac.at