Karlsruhe Institute of Technology

Decentralized Systems and Network Services
Research Group
Institute of Telematics

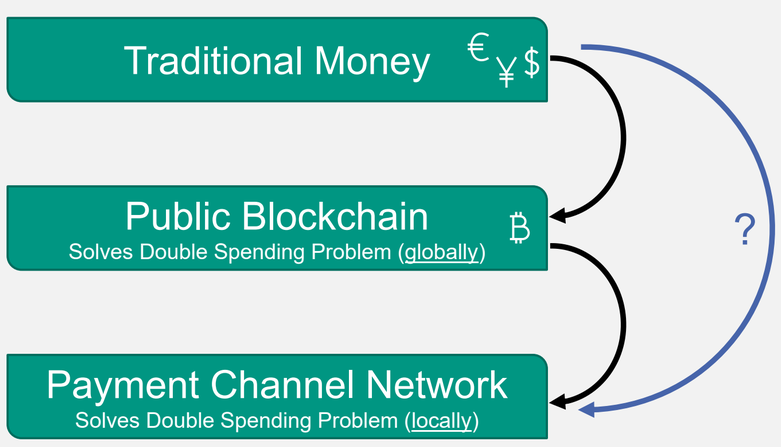
SPONSORED BY THE
Federal Ministry of Education and Research

Do Payment Channel Networks Need a Blockchain?

Rethinking Blockchain Layers

Matthias Grundmann
matthias.grundmann@kit.edu

Hannes Hartenstein
hannes.hartenstein@kit.edu

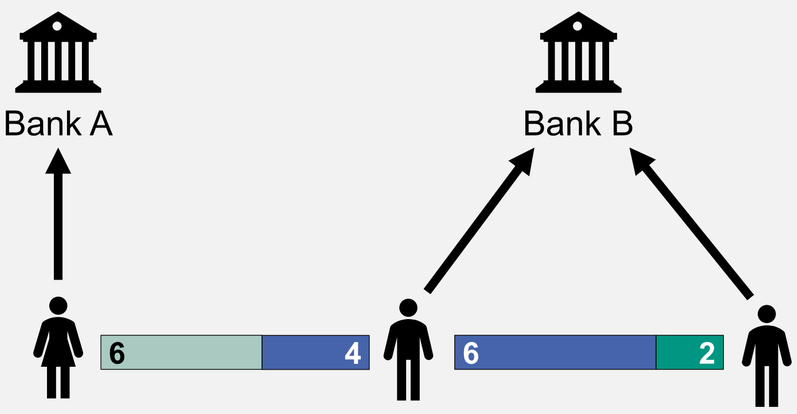


Blockchain cryptocurrencies and payment channel networks solve the problem of preventing double spends.

Can payment channel networks be used **without a blockchain** to create a “to some extent decentralized” architecture for digital payments?

How can **C**entral **B**ank **D**igital **C**urrencies allow for decentralized payments comparable to cash?

Scenario



Channel Protocol

Involved Parties

Create Channel — Alice, Bob, Bank A, Bank B

Banks create channel identifier, lock initial balances, sign initial state

Update Channel — Alice, Bob

Sign new state, send to other party

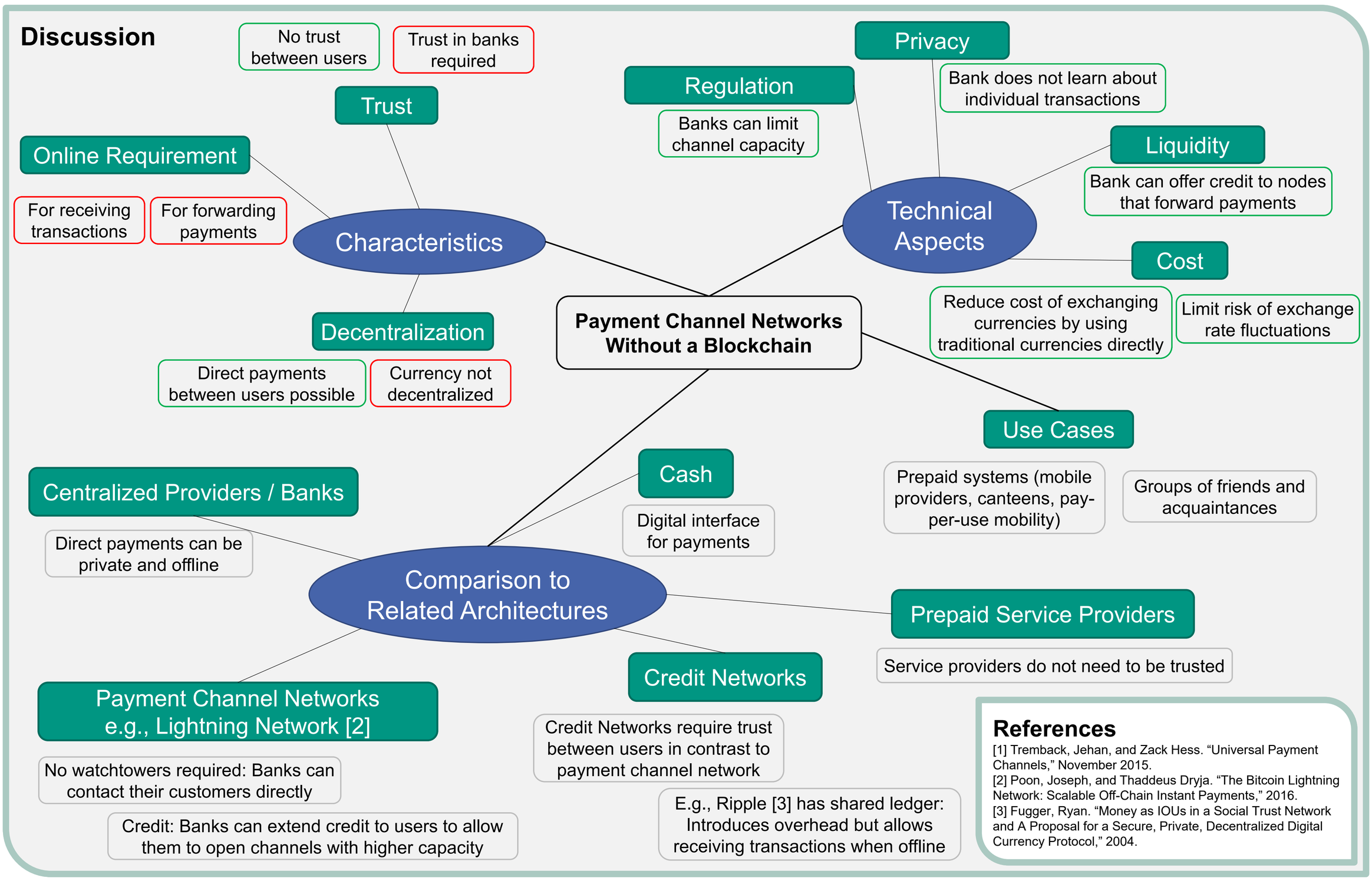
Close Channel — Alice, Bob, Bank A, Bank B

Send state to bank, wait for other party’s confirmation / timeout

Banks perform transfer between each other, update balances

Dispute: *Banks arbitrate, newest state wins*

Discussion



References

[1] Tremback, Jehan, and Zack Hess. “Universal Payment Channels,” November 2015.
[2] Poon, Joseph, and Thaddeus Dryja. “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” 2016.
[3] Fugger, Ryan. “Money as IOUs in a Social Trust Network and A Proposal for a Secure, Private, Decentralized Digital Currency Protocol,” 2004.