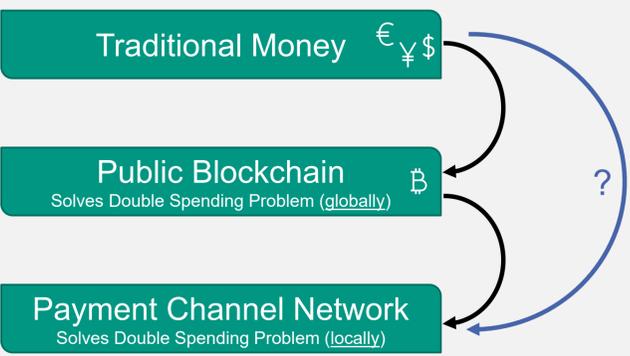


Do Payment Channel Networks Need a Blockchain?

Rethinking Blockchain Layers

Matthias Grundmann
matthias.grundmann@kit.edu

Hannes Hartenstein
hannes.hartenstein@kit.edu

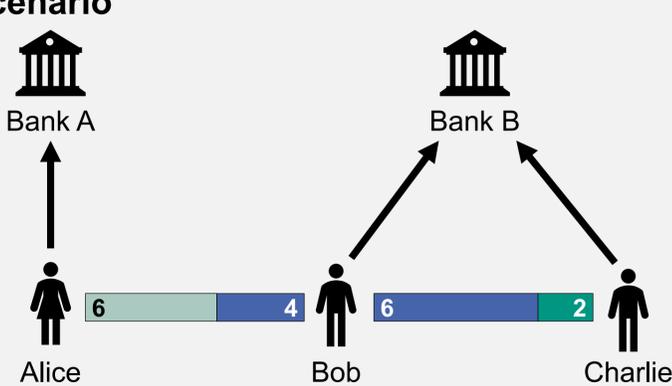


Blockchain cryptocurrencies and payment channel networks solve the problem of preventing double spends.

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

How can **Central Bank Digital Currencies** allow for decentralized payments comparable to cash?

Scenario



Channel Protocol

Involved Parties

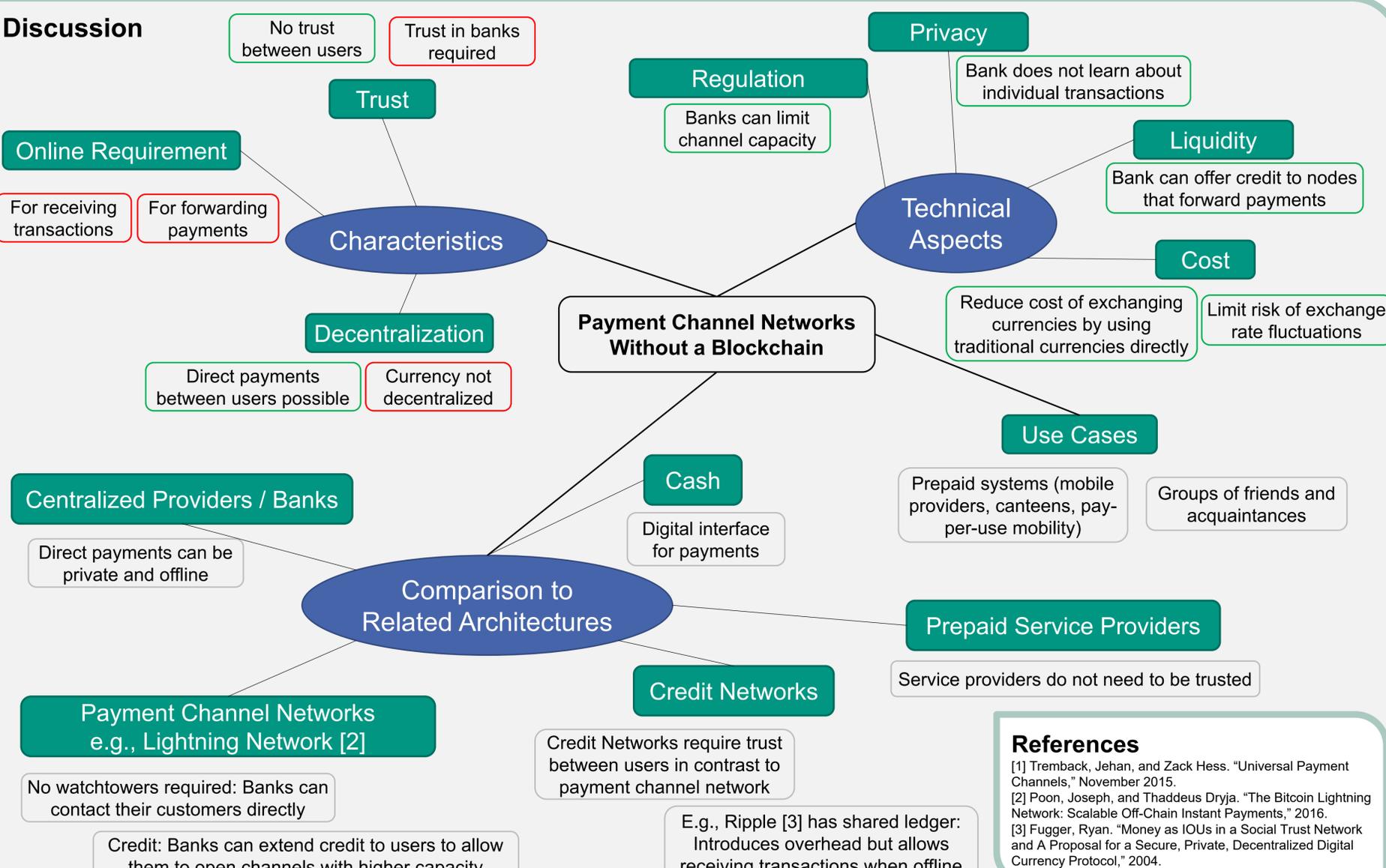
Create Channel: Alice, Bob, Bank A, Bank B
Banks create channel identifier, lock initial balances, sign initial state

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



Trust

- No trust between users
- Trust in banks required

Characteristics

- Online Requirement: For receiving transactions, For forwarding payments
- Decentralization: Direct payments between users possible, Currency not decentralized

Comparison to Related Architectures

- Centralized Providers / Banks: Direct payments can be private and offline
- Payment Channel Networks e.g., Lightning Network [2]: No watchtowers required: Banks can contact their customers directly; Credit: Banks can extend credit to users to allow them to open channels with higher capacity
- Cash: Digital interface for payments
- Credit Networks: Credit Networks require trust between users in contrast to payment channel network; E.g., Ripple [3] has shared ledger: Introduces overhead but allows receiving transactions when offline

Technical Aspects

- Regulation: Banks can limit channel capacity
- Privacy: Bank does not learn about individual transactions
- Liquidity: Bank can offer credit to nodes that forward payments
- Cost: Reduce cost of exchanging currencies by using traditional currencies directly; Limit risk of exchange rate fluctuations
- Use Cases: Prepaid systems (mobile providers, canteens, pay-per-use mobility); Groups of friends and acquaintances
- Prepaid Service Providers: Service providers do not need to be trusted

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.