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

Bank A

Bank B

Alice

Bob

Charlie

Channel Protocol

Create Channel

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

Update Channel

Sign new state, send to other party

Close Channel

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

Online Requirement

For receiving transactions

For forwarding payments

Trust

No trust between users

Trust in banks required

Regulation

Banks can limit channel capacity

Privacy

Bank does not learn about individual transactions

Decentralization

Direct payments between users possible

Currency not decentralized

Payment Channel Networks

Without a Blockchain

Cost

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

Technical Aspects

Reduce cost of exchanging currencies by using traditional currencies directly

Comparison to Related Architectures

Payment Channel Networks

e.g., Lightning Network [2]

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

Cash

Digital interface for payments

References