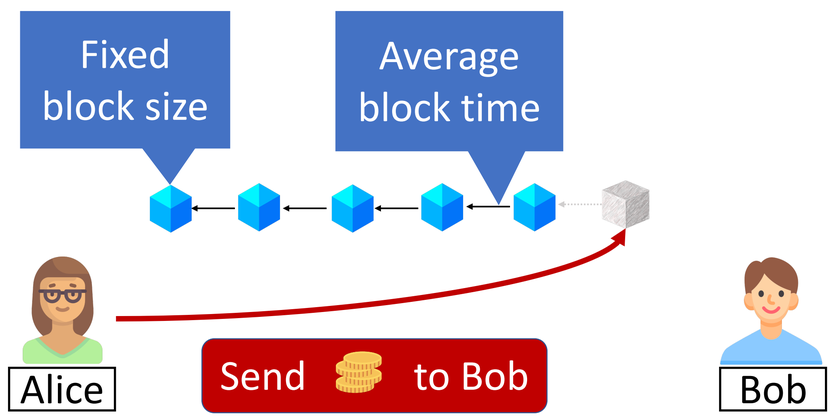
Bitcoin-Compatible Virtual Channels

Lukas Aumayr, Oğuzhan Ersoy, Andreas Erwig, Sebastian Faust, Kristina Hostáková, Matteo Maffei, Pedro Moreno-Sanchez, Siavash Riahi

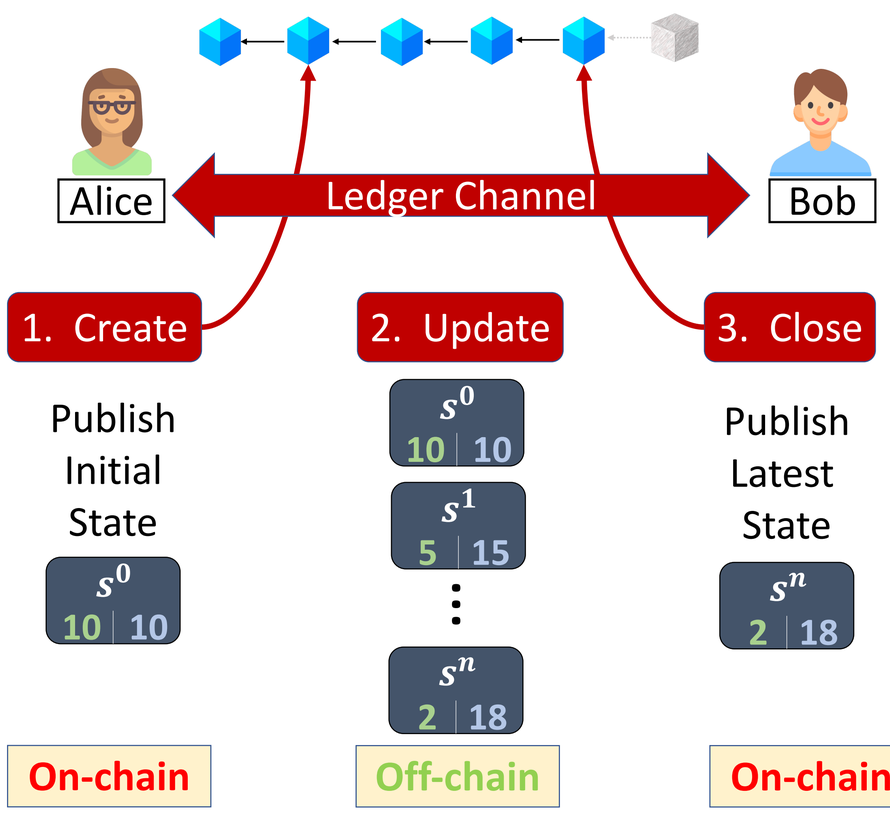
1. Blockchain Scalability Problem



Limited transaction throughput
High transaction fees
Bitcoin: 10 tx/sec vs. Visa: 10K tx/sec

Idea: Off-chain protocols

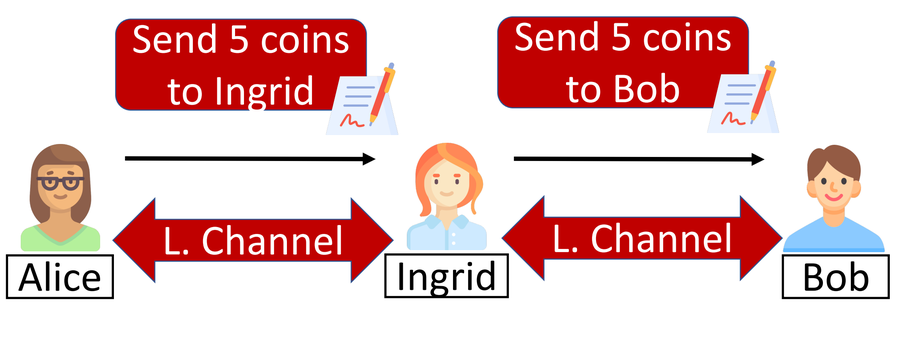
2. Ledger Payment Channels



Arbitrarily many channel updates: Off-chain
Creation and closure of channel: On-chain

Idea: Routing payments in a network of channels

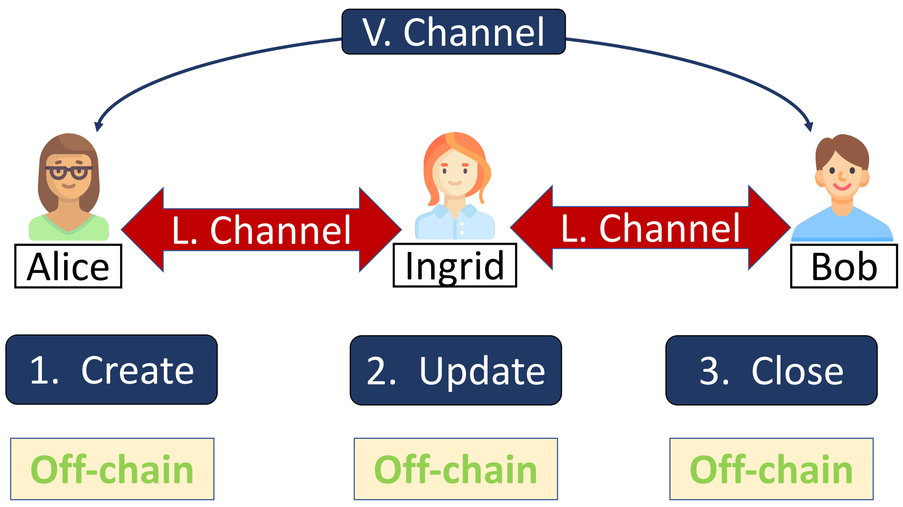
3. Payment Channel Networks



Entirely off-chain
Ingrid must be active/online
No privacy for individual payment amounts

Idea: Virtual Channels

4. Virtual Channels



Entirely off-chain
Ingrid only involved in creation and closure
Privacy-Preserving

Challenge I

Any party can prevent closure of V. Channel

- Parties can refuse to update their L. Channel

Our Solution: Transform V. Channel in L. Channel

4. Offload

Challenge II

Malicious ledger channel update

- Two parties can maliciously update their L. Channel

Our Solution: Honest parties get financially compensated via collaterals

5. Punish

First constructions of virtual channels for UTXO-blockchains

5. Performance

Routing n Payments

PCN

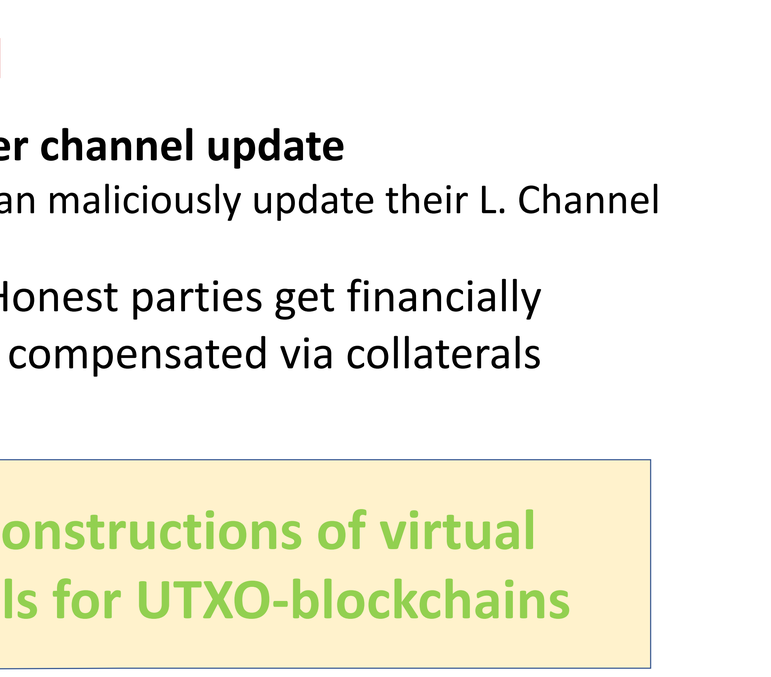
$3026 \cdot n$ bytes,

$8 \cdot n$ transaction

Virtual channels (VC)

$3524 + 695 \cdot n$ bytes,

$9 + 2 \cdot n$ transactions



TU WIEN · TU Delft · Technische Universität Darmstadt · ETH zürich · IMDEA Software Institute