

Alba: The Dawn of Scalable Bridges

Lukas Aumayr

Mahsa Bastankhah

Zeta Avarikioti

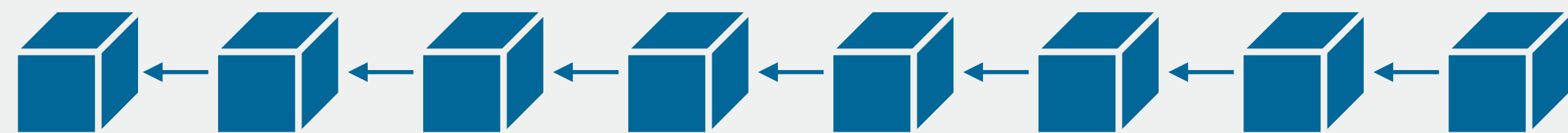
Matteo Maffei

Giulia Scaffino
giulia.scaffino@tuwien.ac.at

NDSS, San Diego
February 24-28, 2025



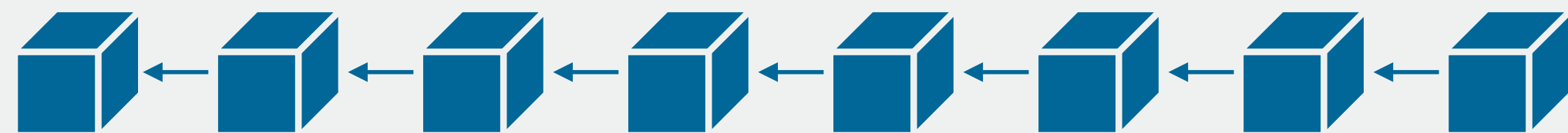
Scalability



Typically, blockchains have low throughput!

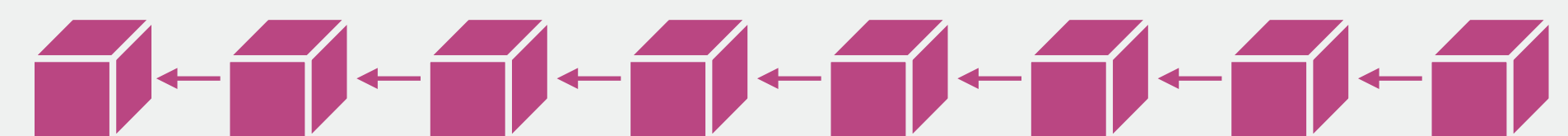
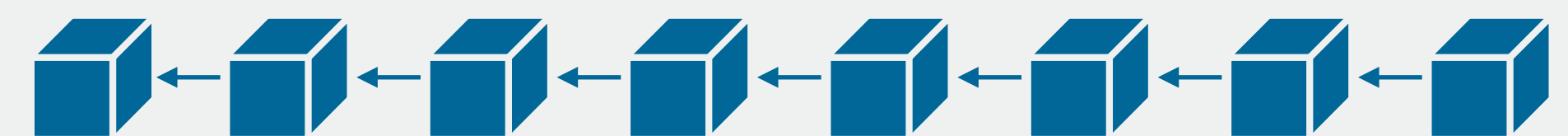
Bitcoin: ~ 8 Tx / sec
Ethereum: ~ 15 Tx / sec
Visa: ~10K Tx / sec

Scalability and Interoperability



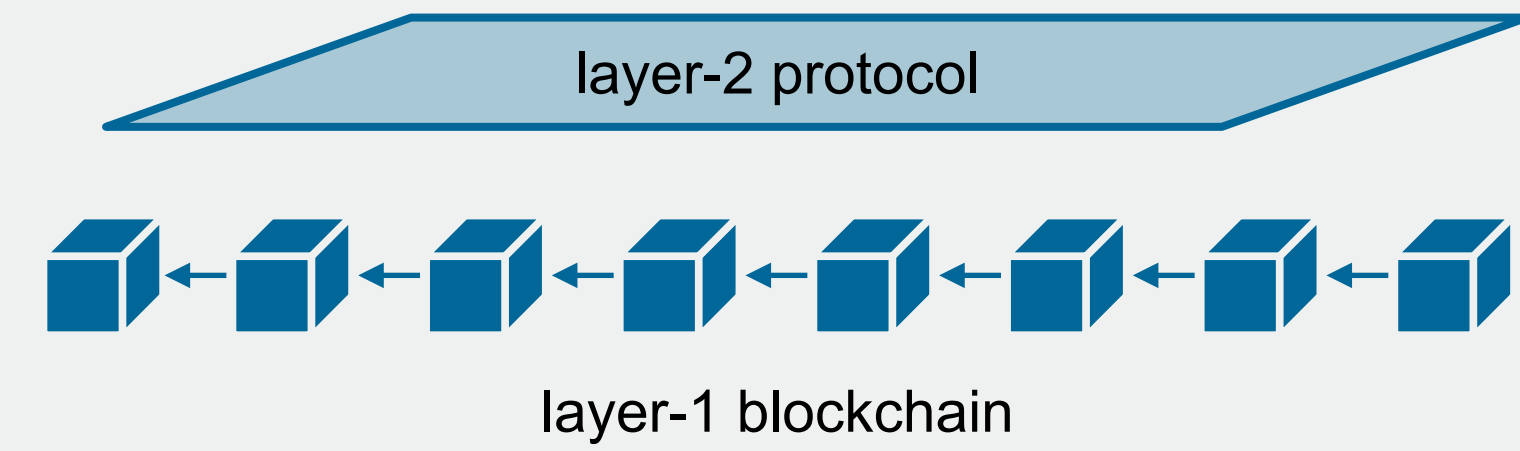
Typically, blockchains have low throughput!

Bitcoin: ~ 8 Tx / sec
Ethereum: ~ 15 Tx / sec
Visa: ~10K Tx / sec

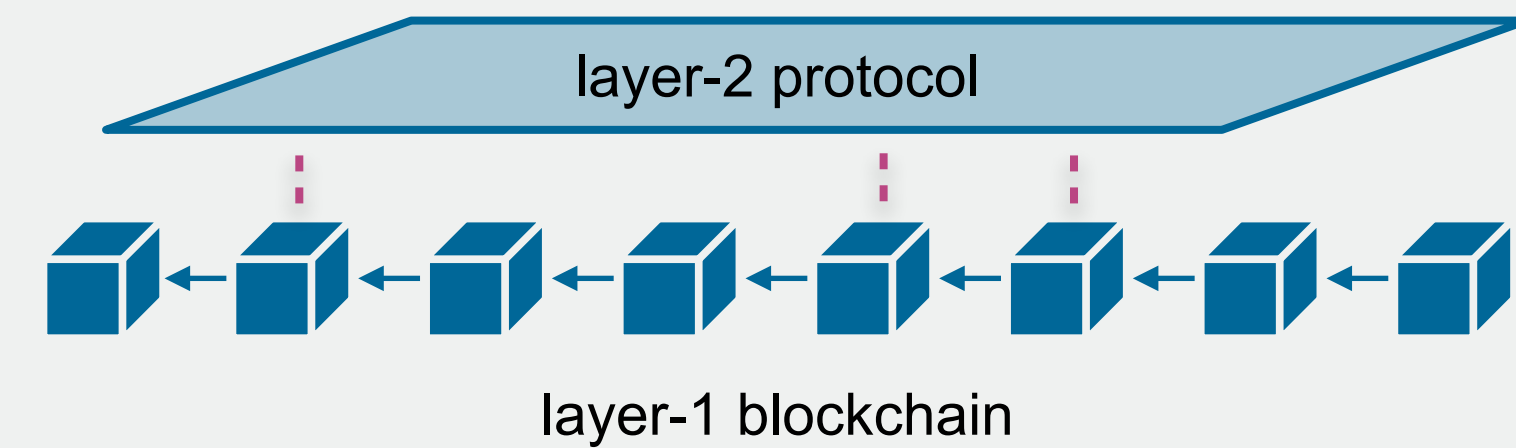


Towards Scalability

- Exchange transactions **off-chain**



Towards Scalability



- Exchange transactions **off-chain**
- Use the blockchain for **security**, i.e., for **disputes** (PCNs, optimistic rollups), **finality** (Polygon - checkpoints)

Payment Channels
and
Payment Channel Networks

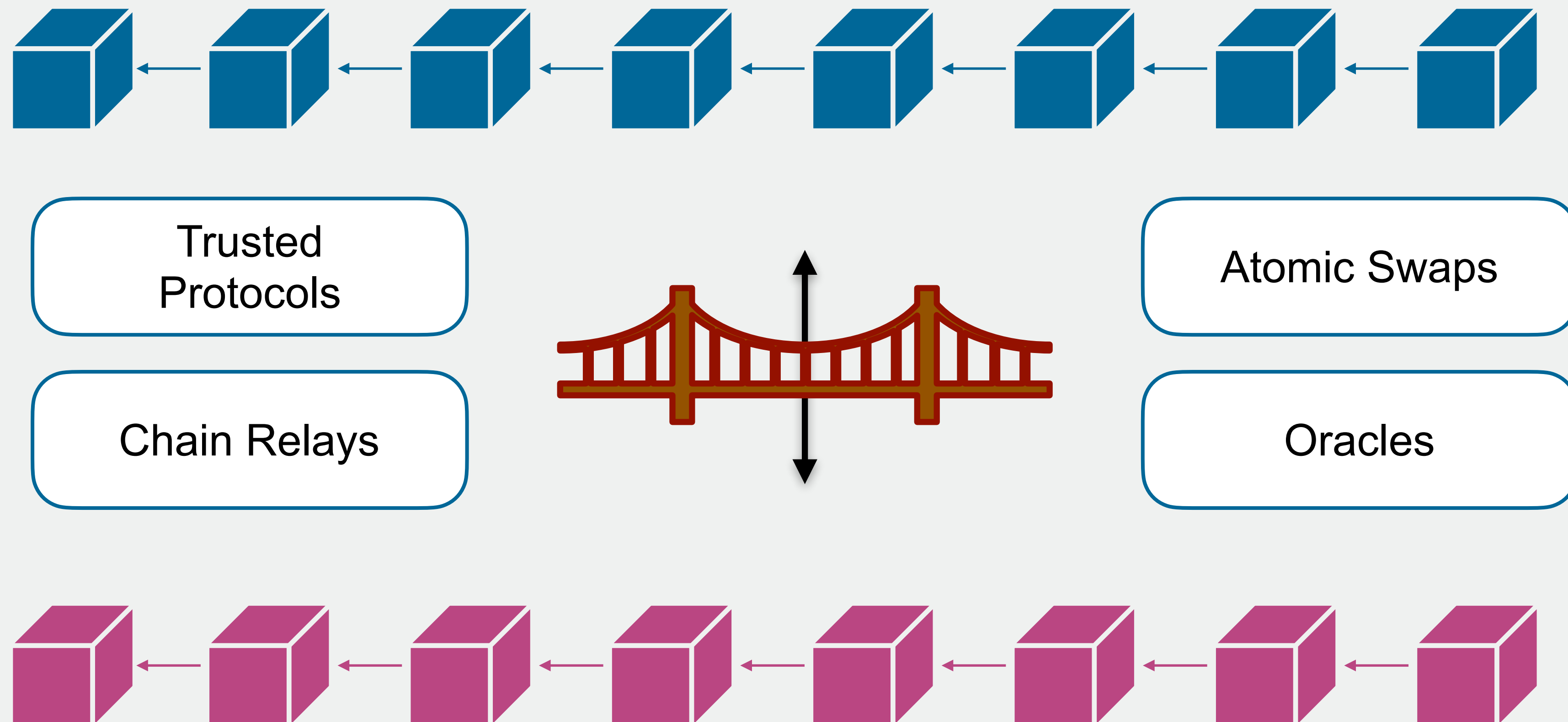
State Channels

Commit Chains
and
Sidechains

Rollups

Layer-2 protocols only **interact** with **their respective layer-1**

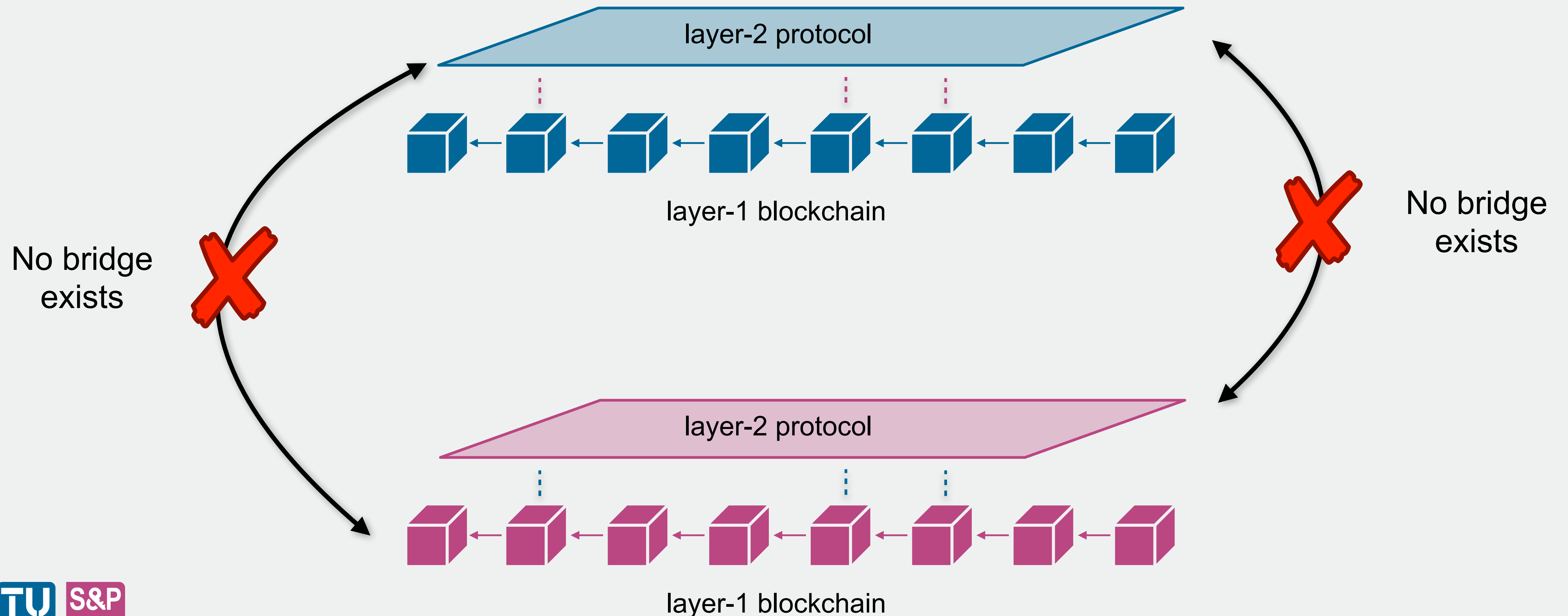
Towards Interoperability



Interoperability Does Not Scale

Existing bridges require transactions to be **on-chain**!

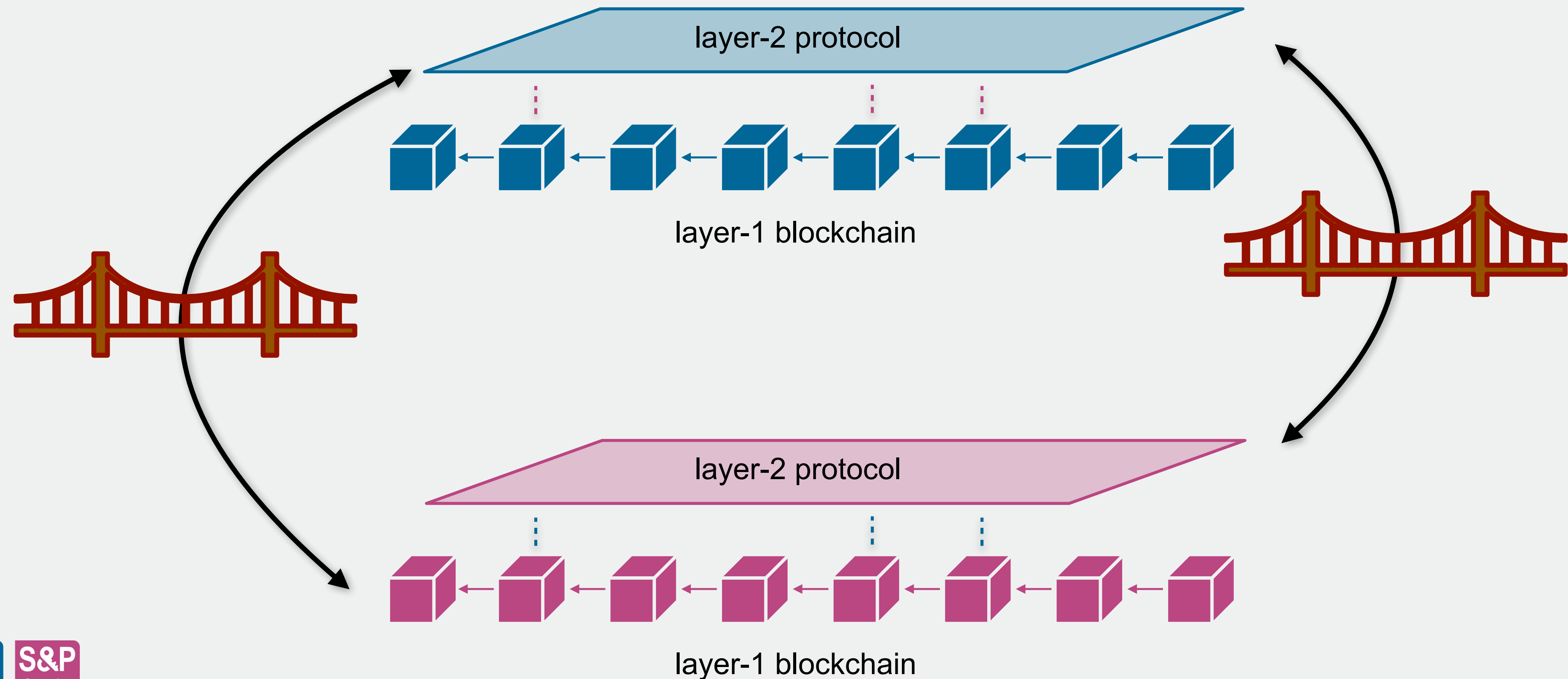
- Hinder scalability of applications
- Missing interoperability between L2-L2 and L2-L1



Scalable Bridges: A New Paradigm

Scalable bridges support off-chain transactions!

- Enhance scalability of applications
- Enable interoperability between L2-L2 and L2-L1
- Inherit good properties from layer-2 protocols

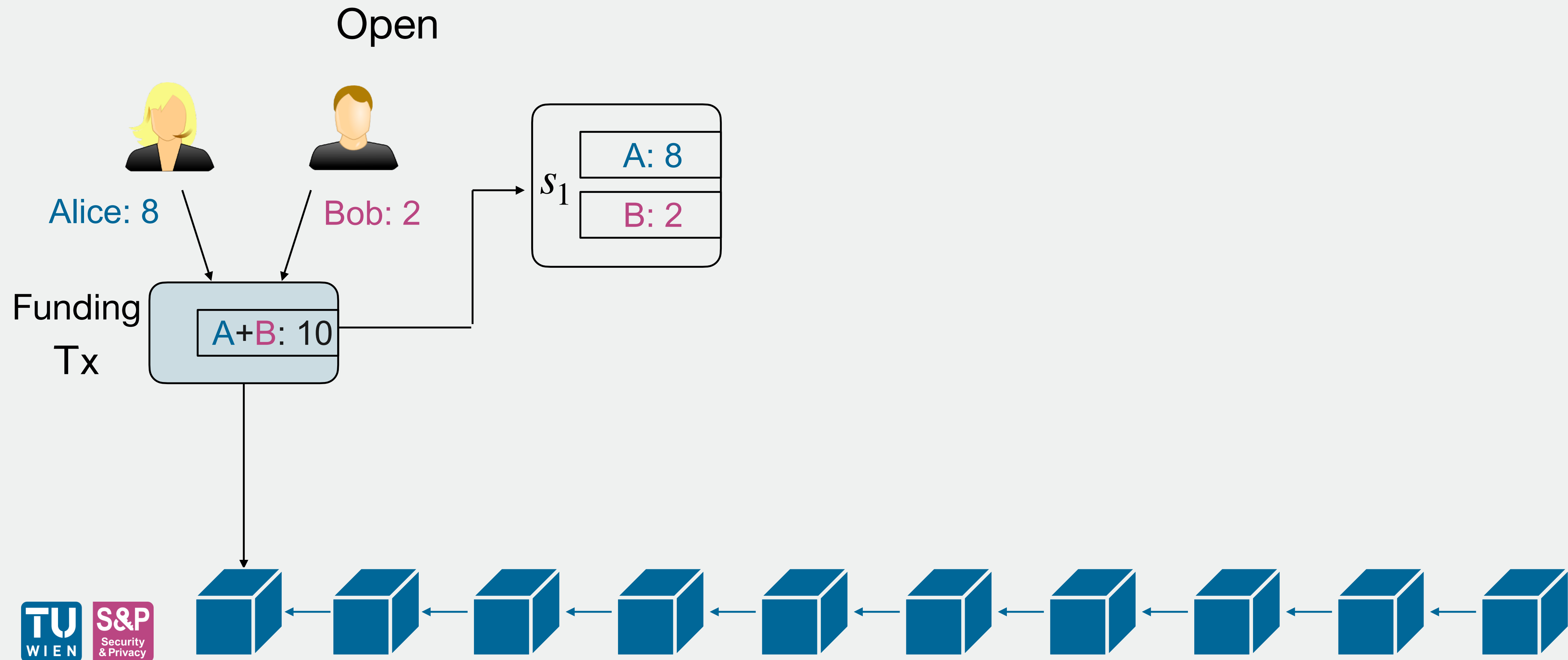


Why Payment Channels?

- Most **mature** and **decentralised** layer-2 solution
- Virtually **compatible** with all existing blockchains
- Effectively **scale** both storage and computation

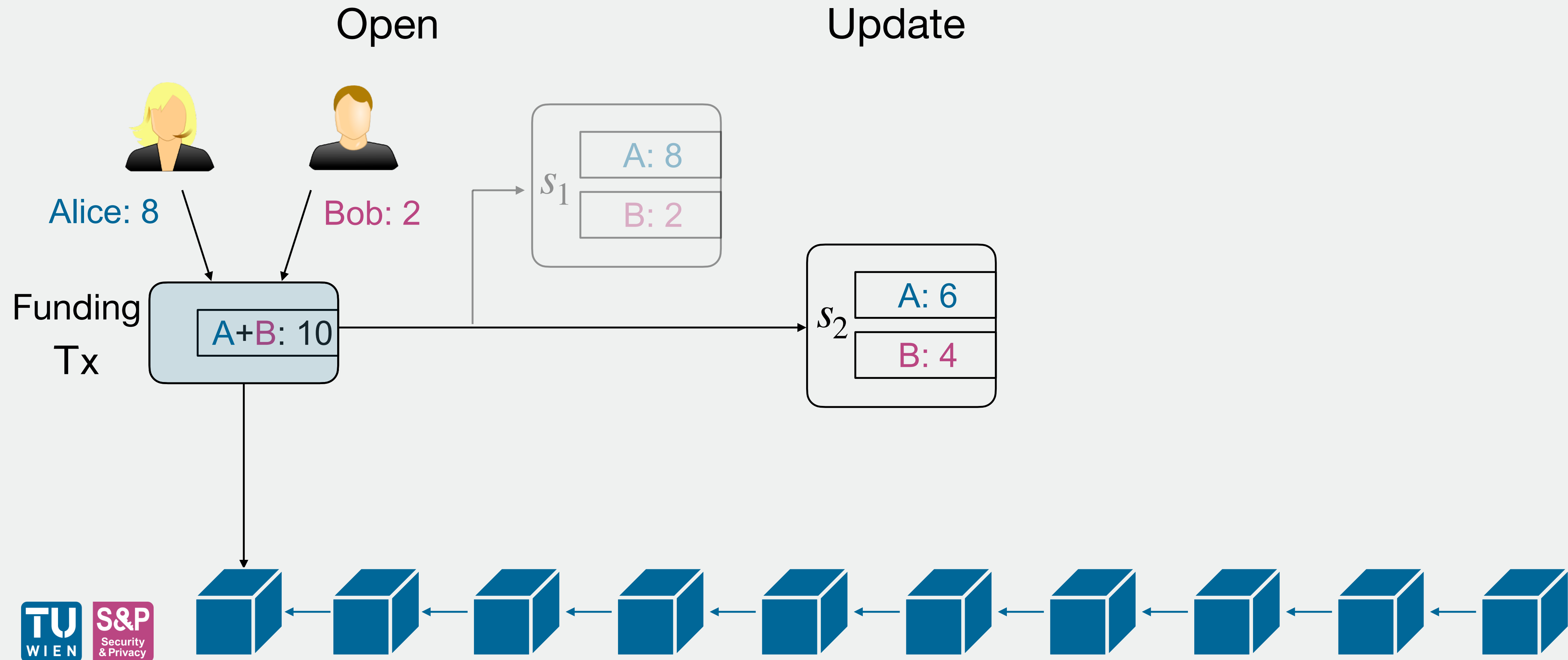
Payment Channel Overview

- Most **mature** and **decentralised** layer-2 solution
- Virtually **compatible** with all existing blockchains
- Effectively **scale** both storage and computation



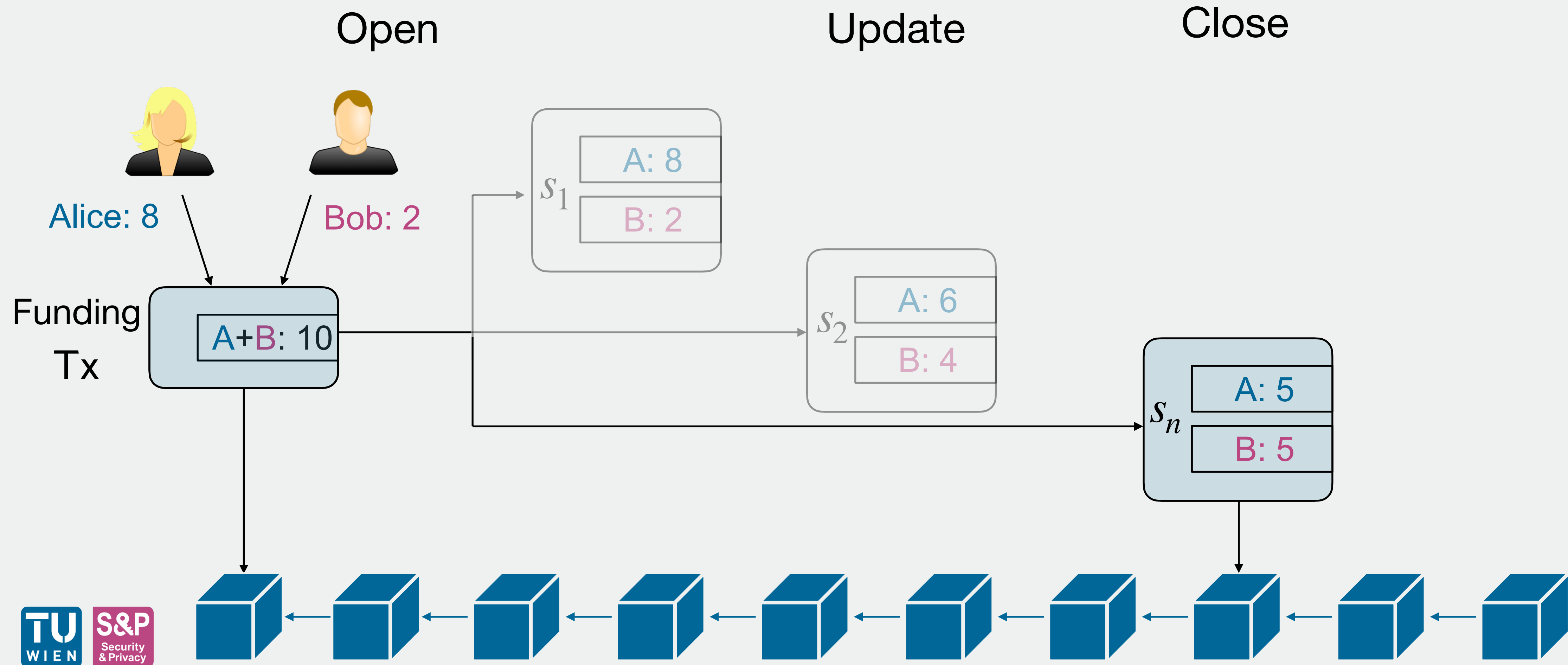
Payment Channel Overview

- Most **mature** and **decentralised** layer-2 solution
- Virtually **compatible** with all existing blockchains
- Effectively **scale** both storage and computation



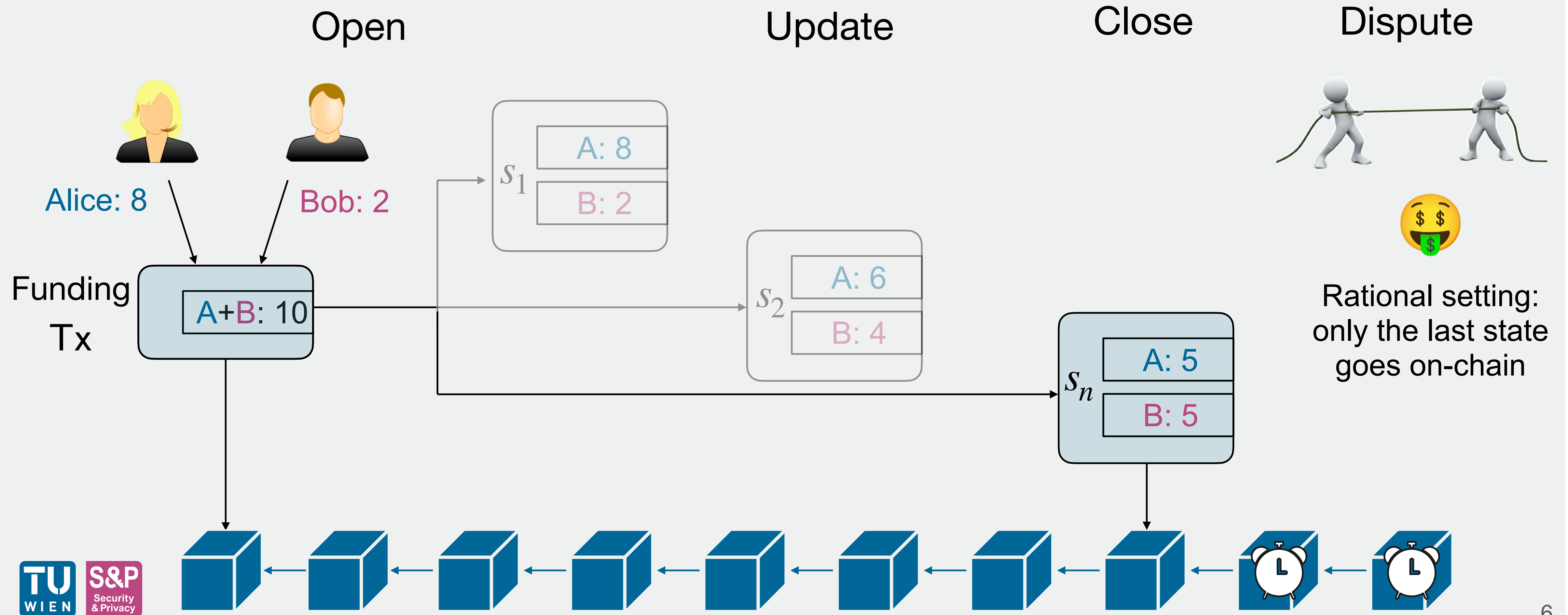
Payment Channel Overview

- Most **mature** and **decentralised** layer-2 solution
- Virtually **compatible** with all existing blockchains
- Effectively **scale** both storage and computation

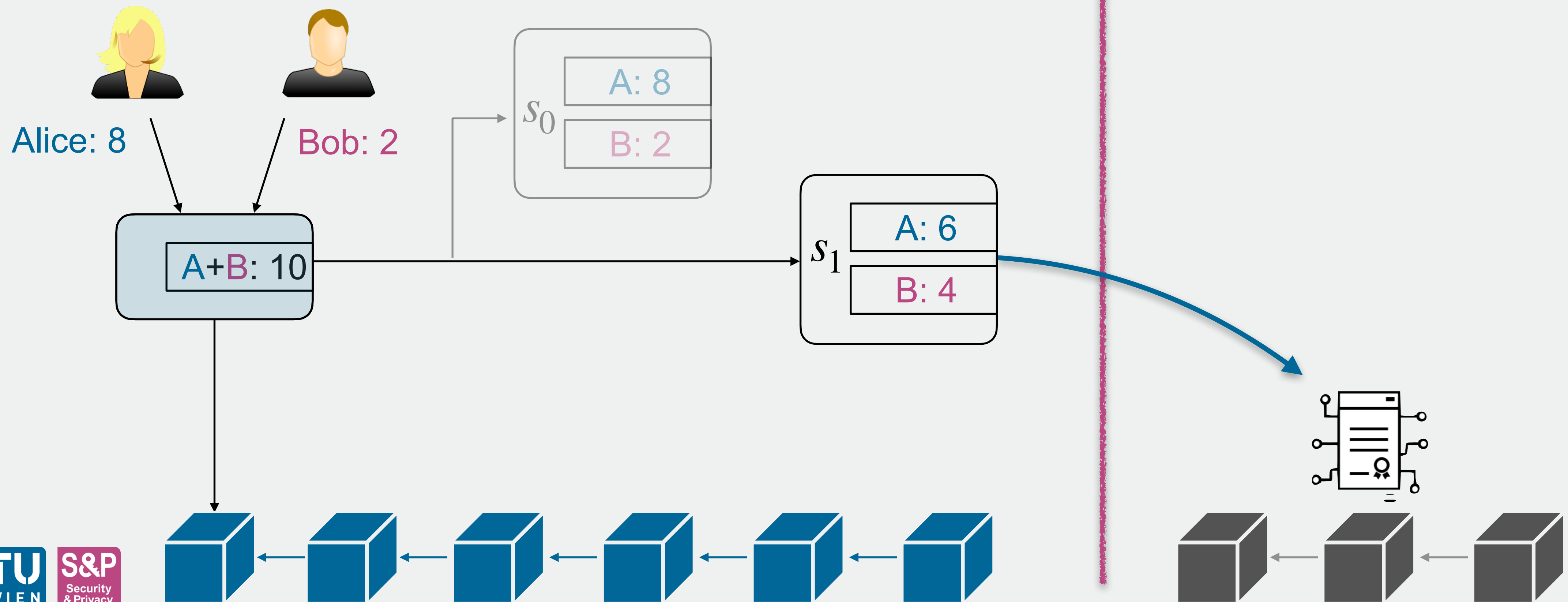


Payment Channel Overview

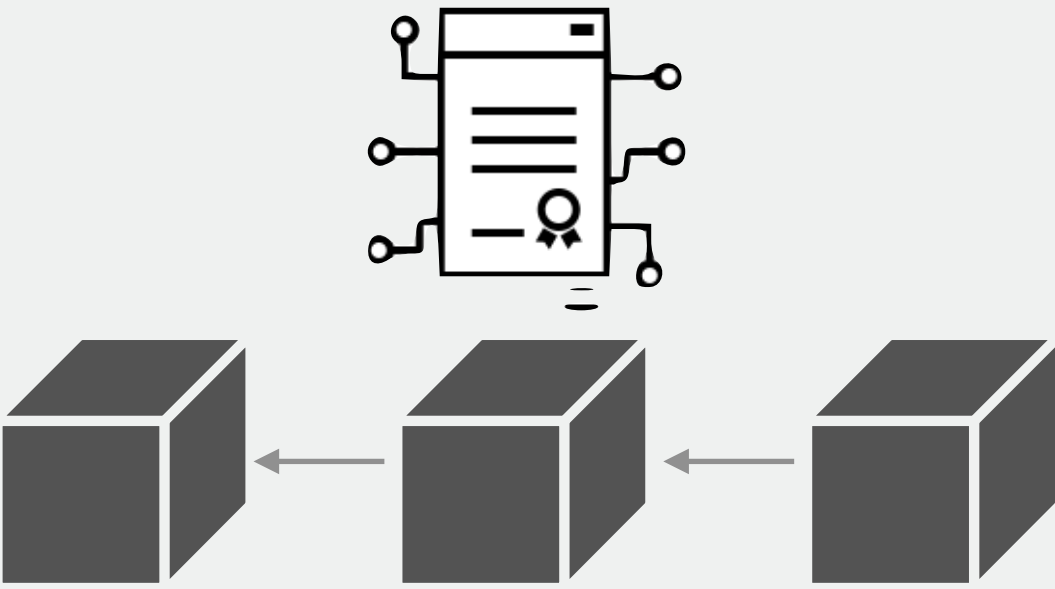
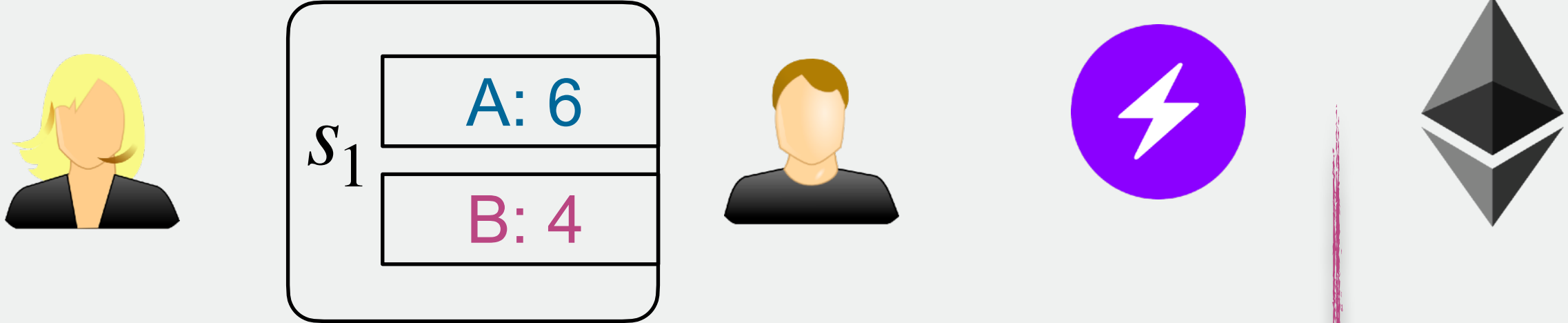
- Most **mature** and **decentralised** layer-2 solution
- Virtually **compatible** with all existing blockchains
- Effectively **scale** both storage and computation



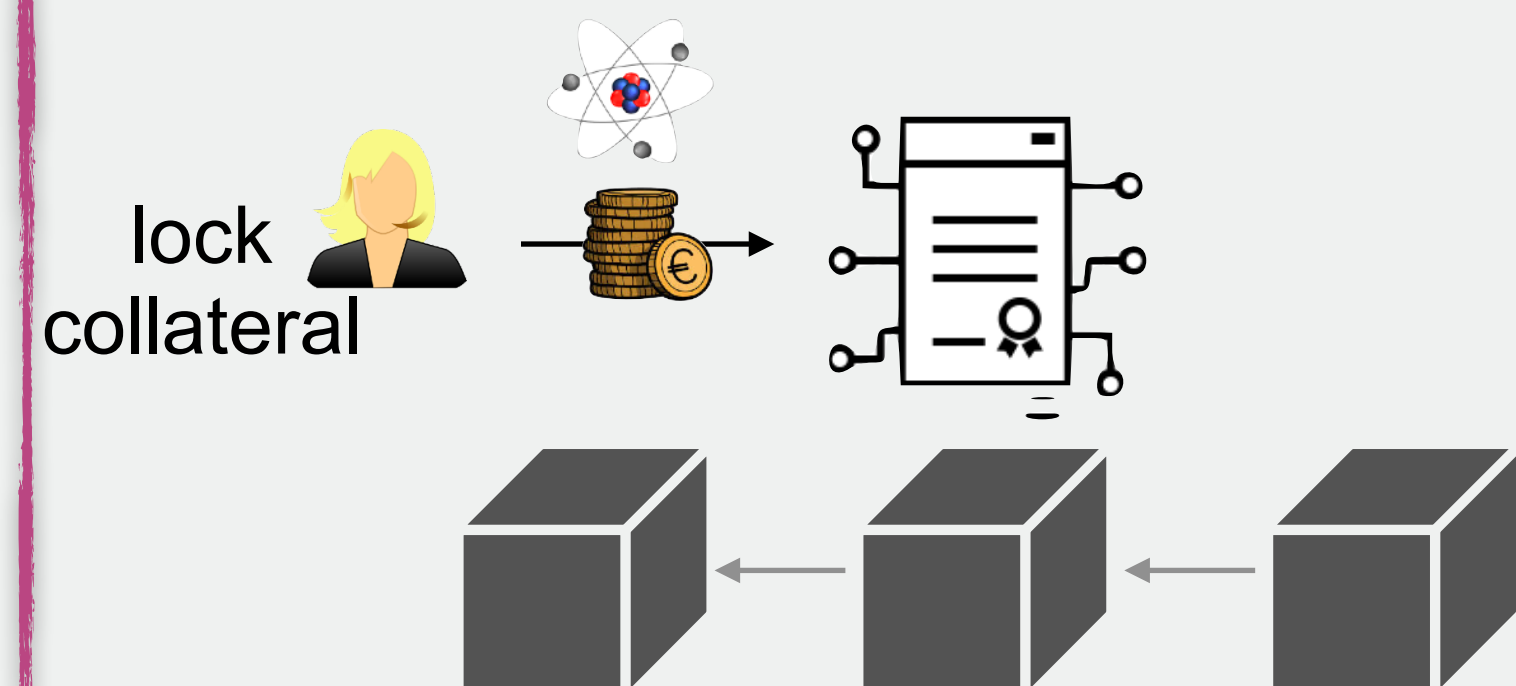
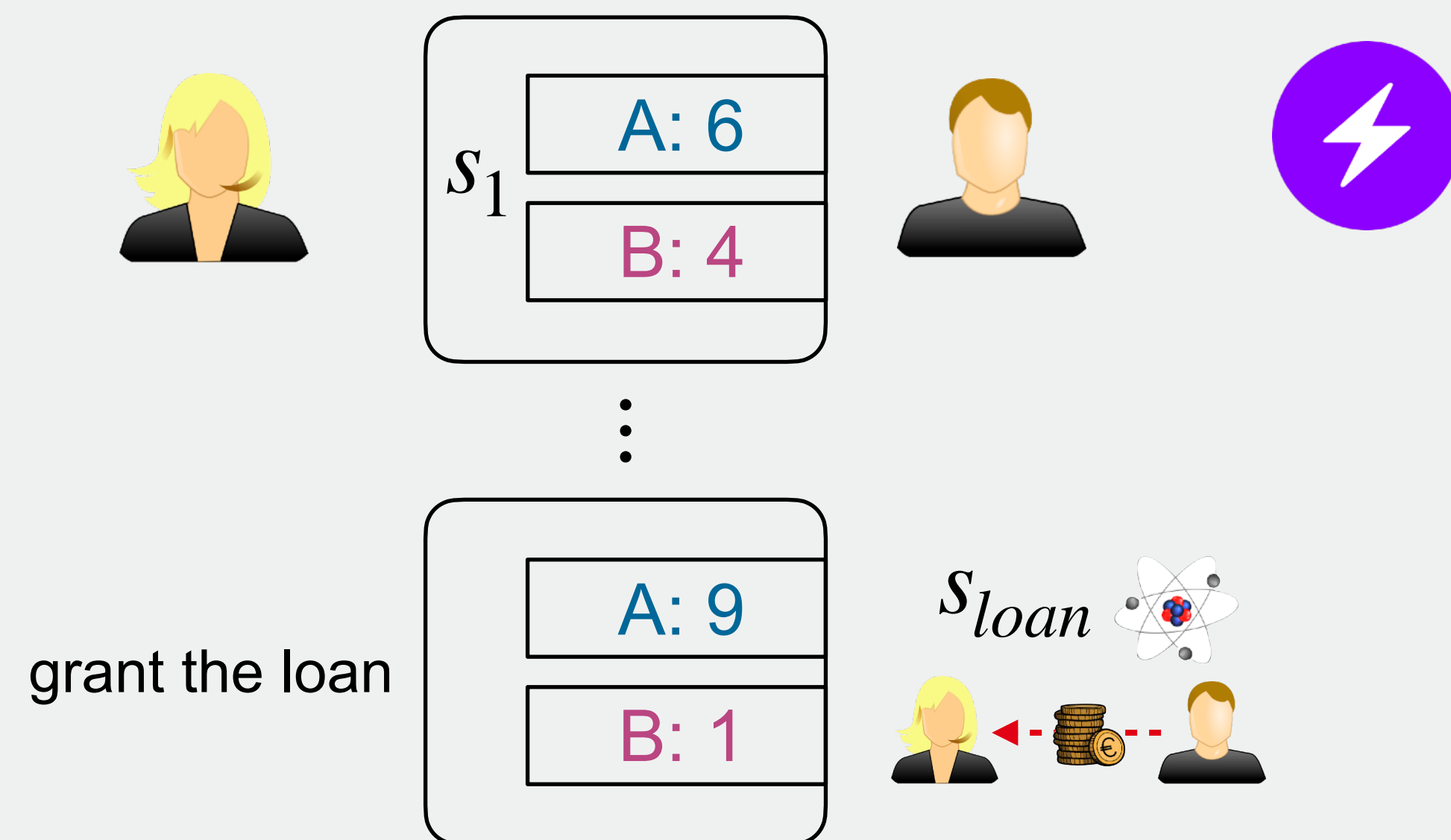
Alba: Prove a Payment in a Channel



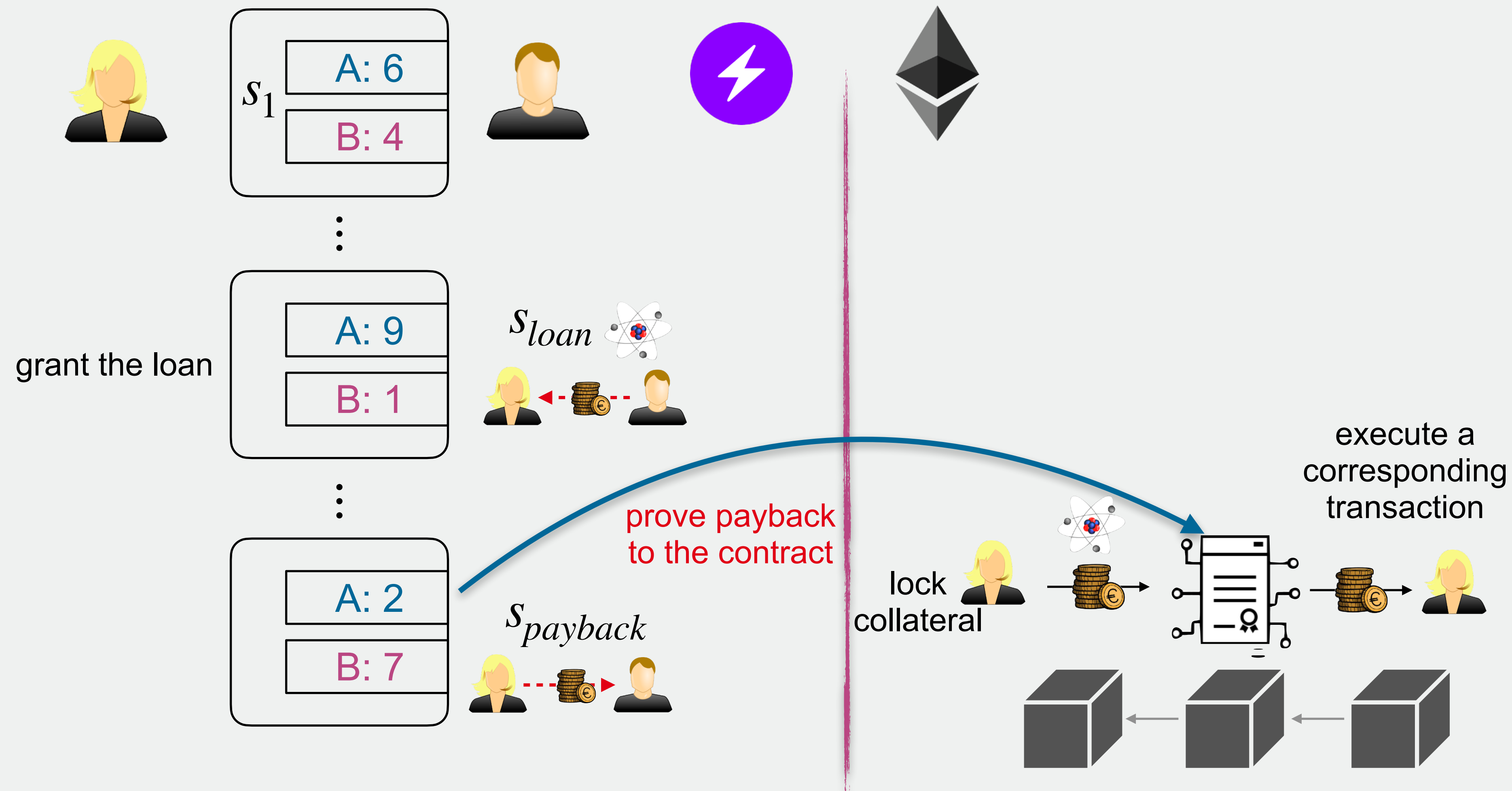
Lending with Alba



Lending with Alba



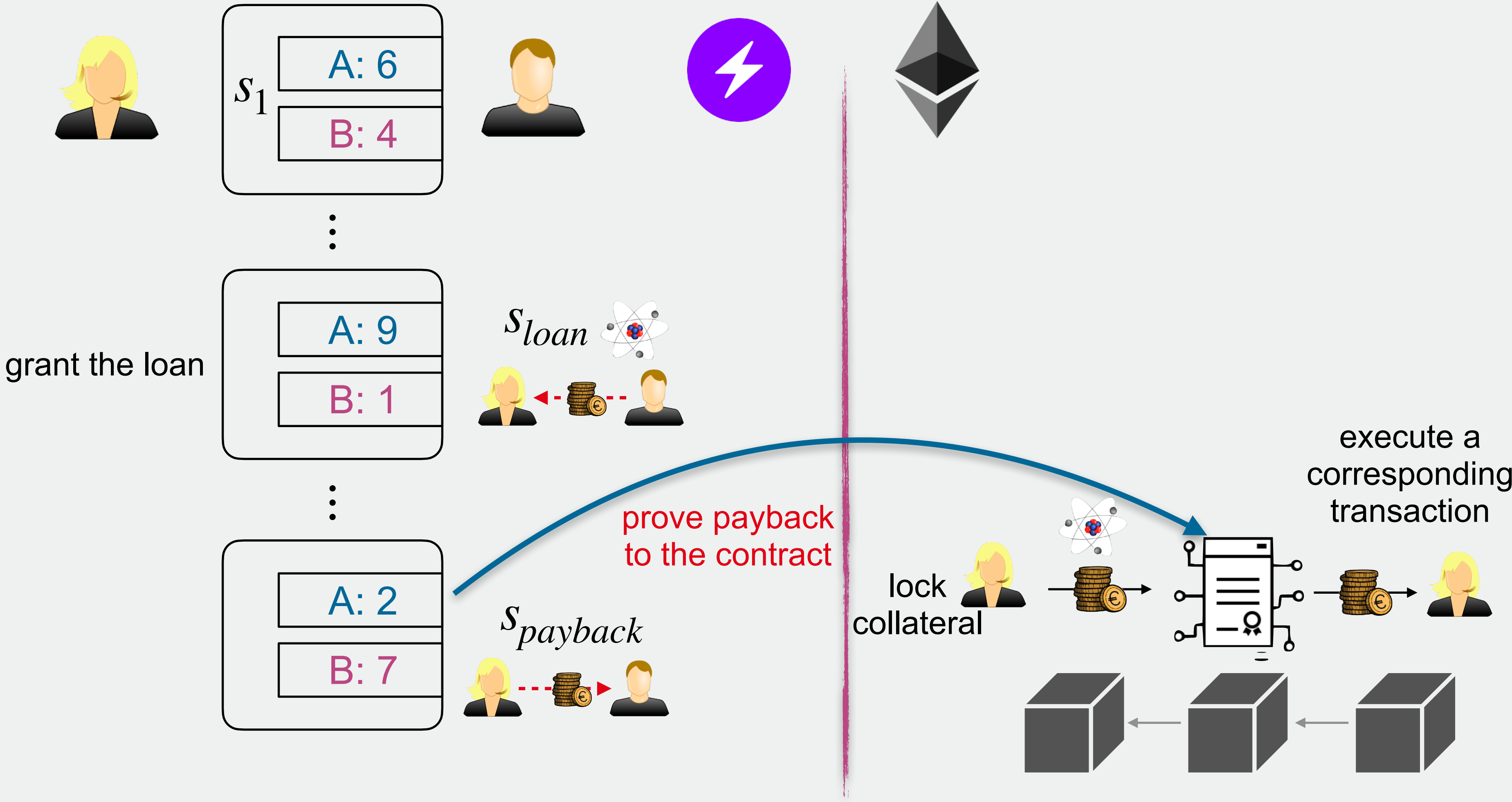
Lending with Alba



Lending with Alba



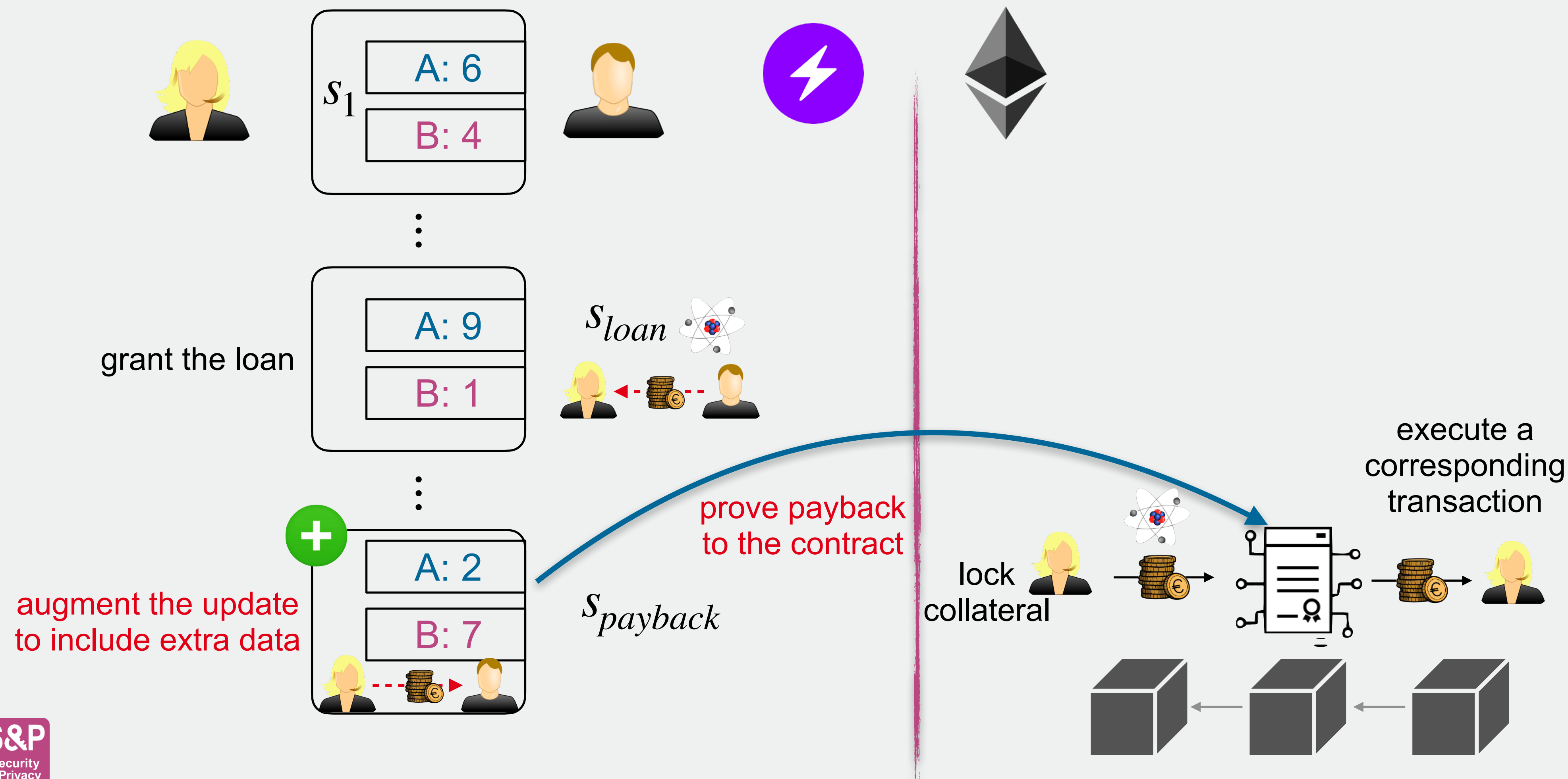
Efficiency
Security



Lending with Alba



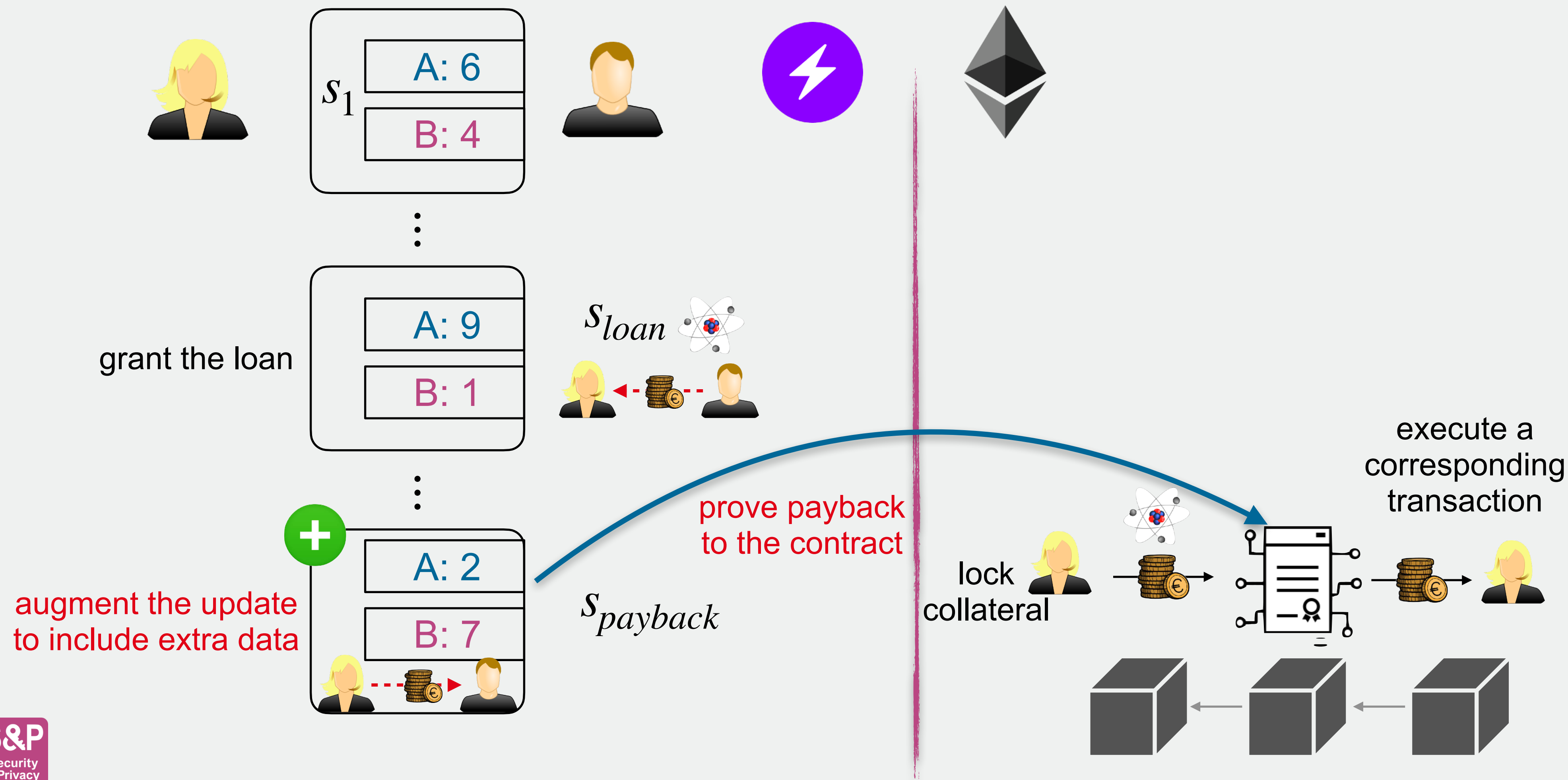
Efficiency
Security



Lending with Alba



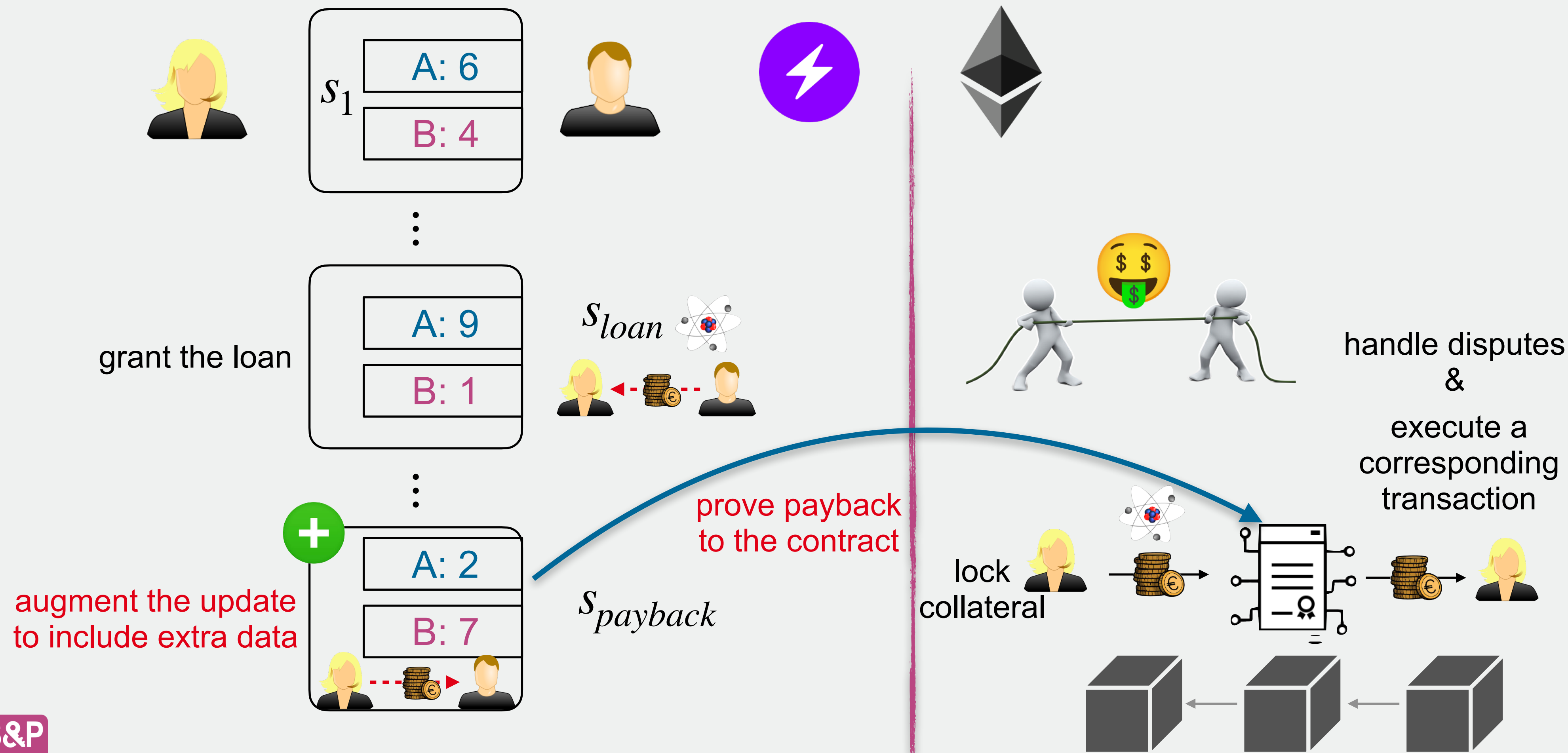
Efficiency
Security



Lending with Alba



Efficiency
Security



Evaluation of Alba

Function	Gas
Setup	390k
Submit Proof	48k / 253k
Dispute	515k
Resolve Dispute	168k
Resolve Dispute (C)	37k
Settle	49k

Standard transfer transaction in Ethereum: **21k gas**



Security: UC + Game Theory

- Security analysis in the **Universal Composability (UC) Framework**
- Alice and Bob submitting a **valid proof** is a **Subgame Perfect Nash Equilibrium**



Properties

Alba is a **scalable bridge** for the **Lightning Network (LN)** which inherits some **good properties** from the LN

	Light Clients	Super-Light Clients	zkBridge	Alba
Information relayed wrt source chain length	$O(C)$	$O(k \text{ polylog } C)$	$O(C)$	$O(1)$
Storage overhead wrt source chain length	$O(C)$	$O(k \text{ polylog } C)$	$O(1)$	$O(1)$
Consensus agnostic				
Instant finality in the rational setting				
Secure against liveness attack on source chain				

More Applications

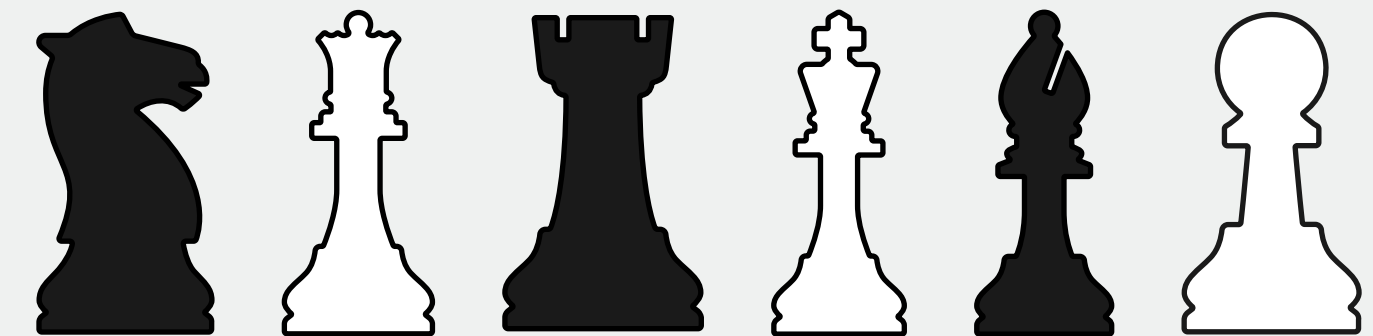
- ▶ Lending



- ▶ Multi-asset payments channels



- ▶ Optimistic stateful computation on payment channels



Conclusions

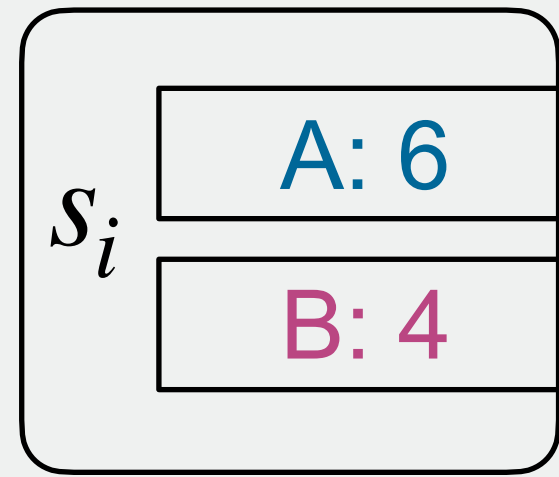
- We introduce the notion of a **scalable bridge**
- We design **Alba**, the first scalable bridge
- We prove its **efficiency** by evaluating its costs
- We analyze its **security** in the UC Framework and with a game theoretical analysis
- We showcase some interesting **applications**



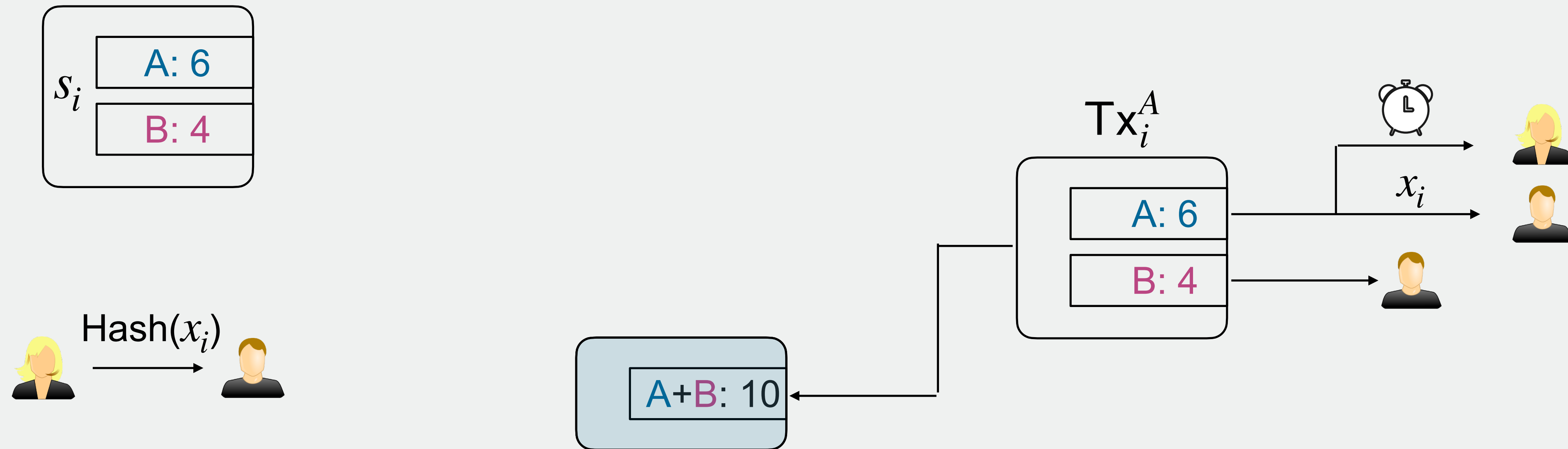
giulia.scaffino@tuwien.ac.at

Backup

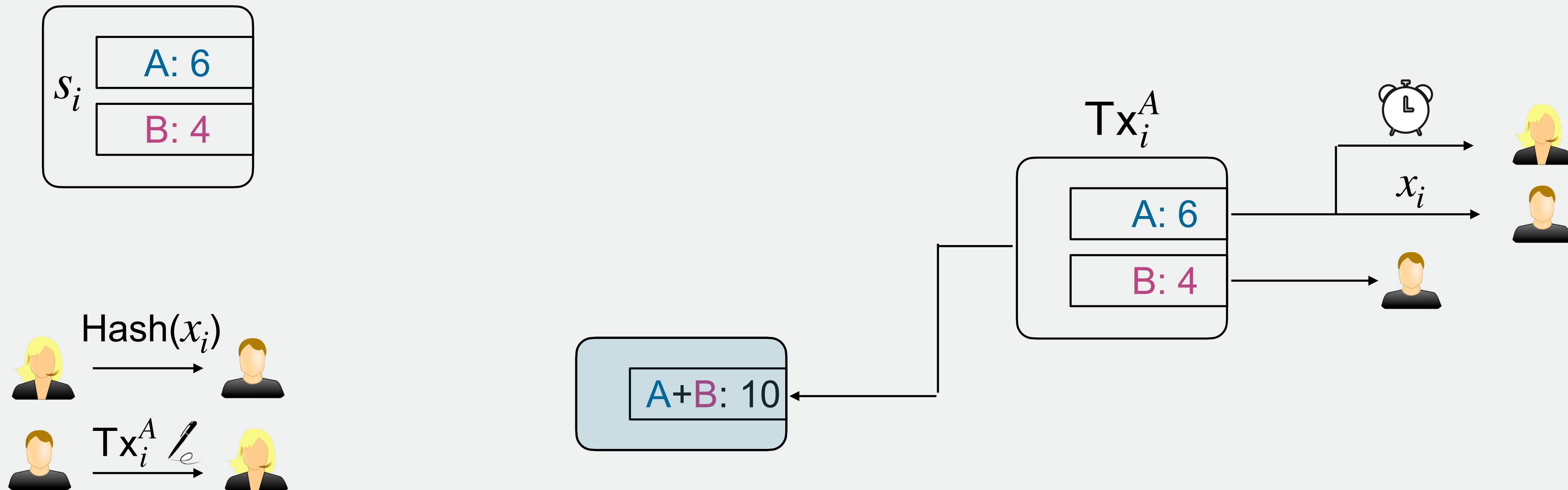
Channel Update



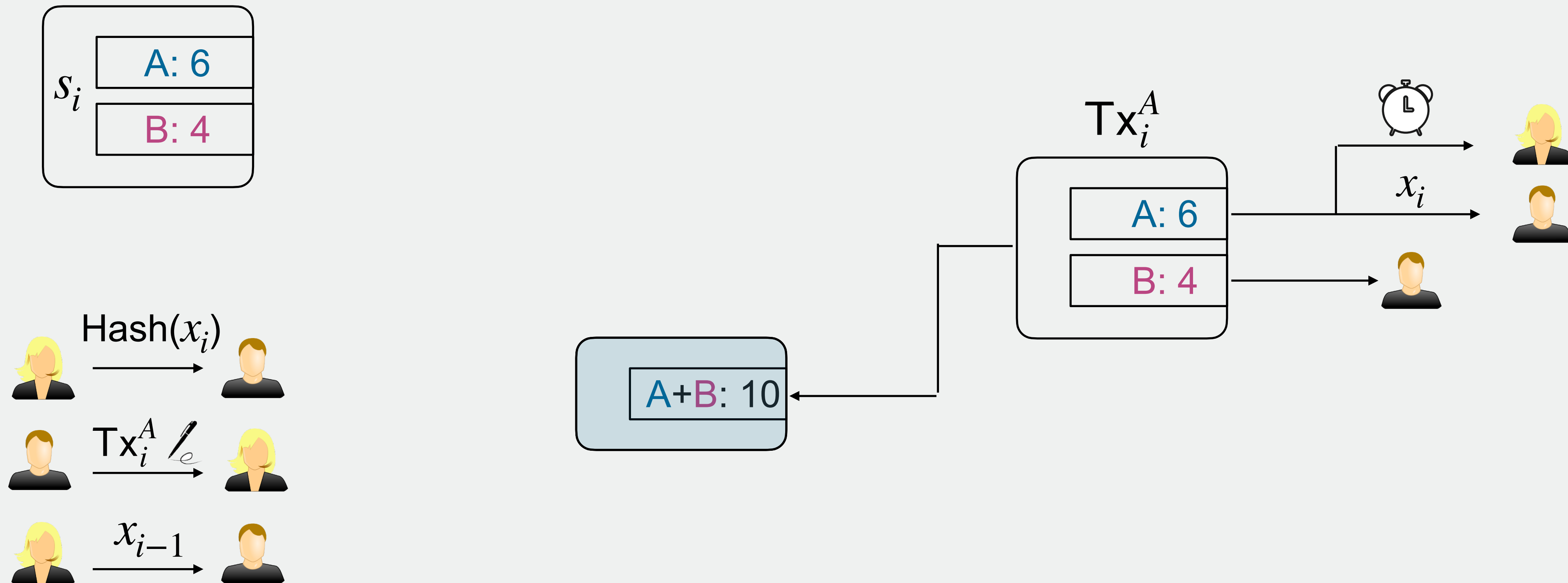
Channel Update



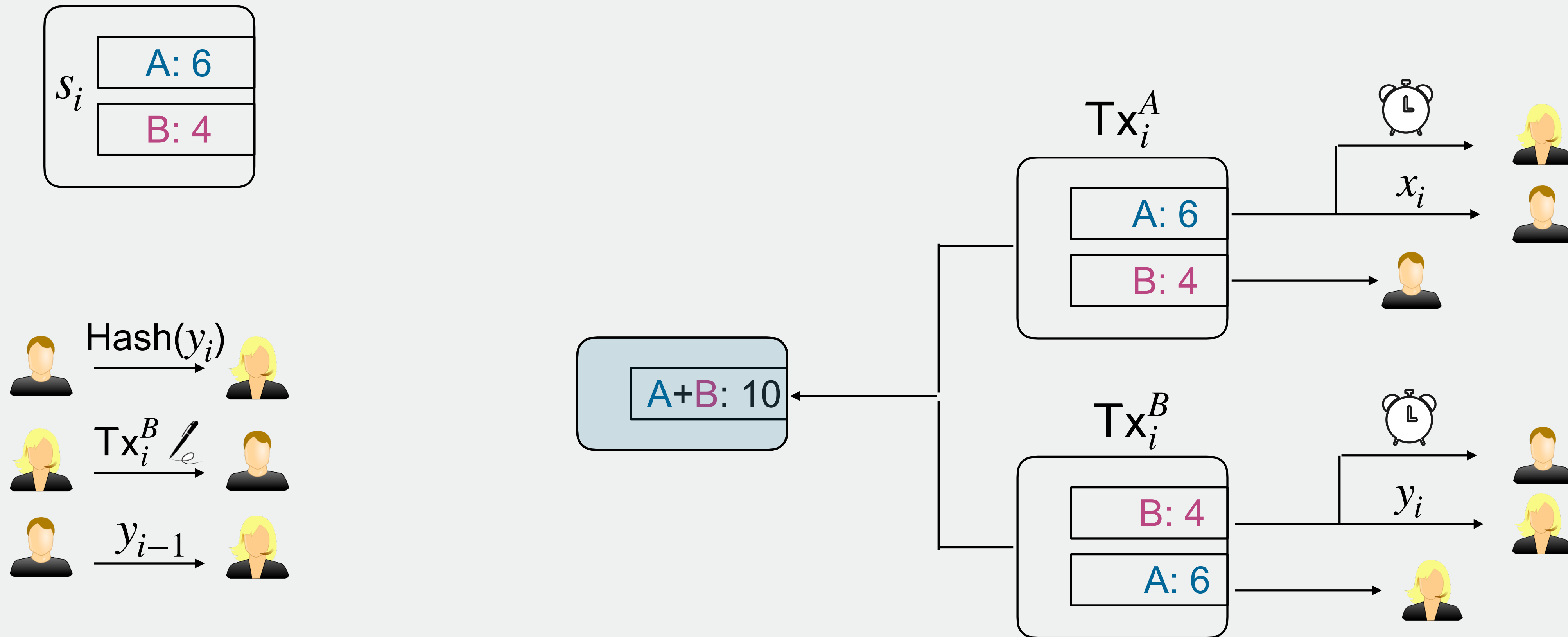
Channel Update



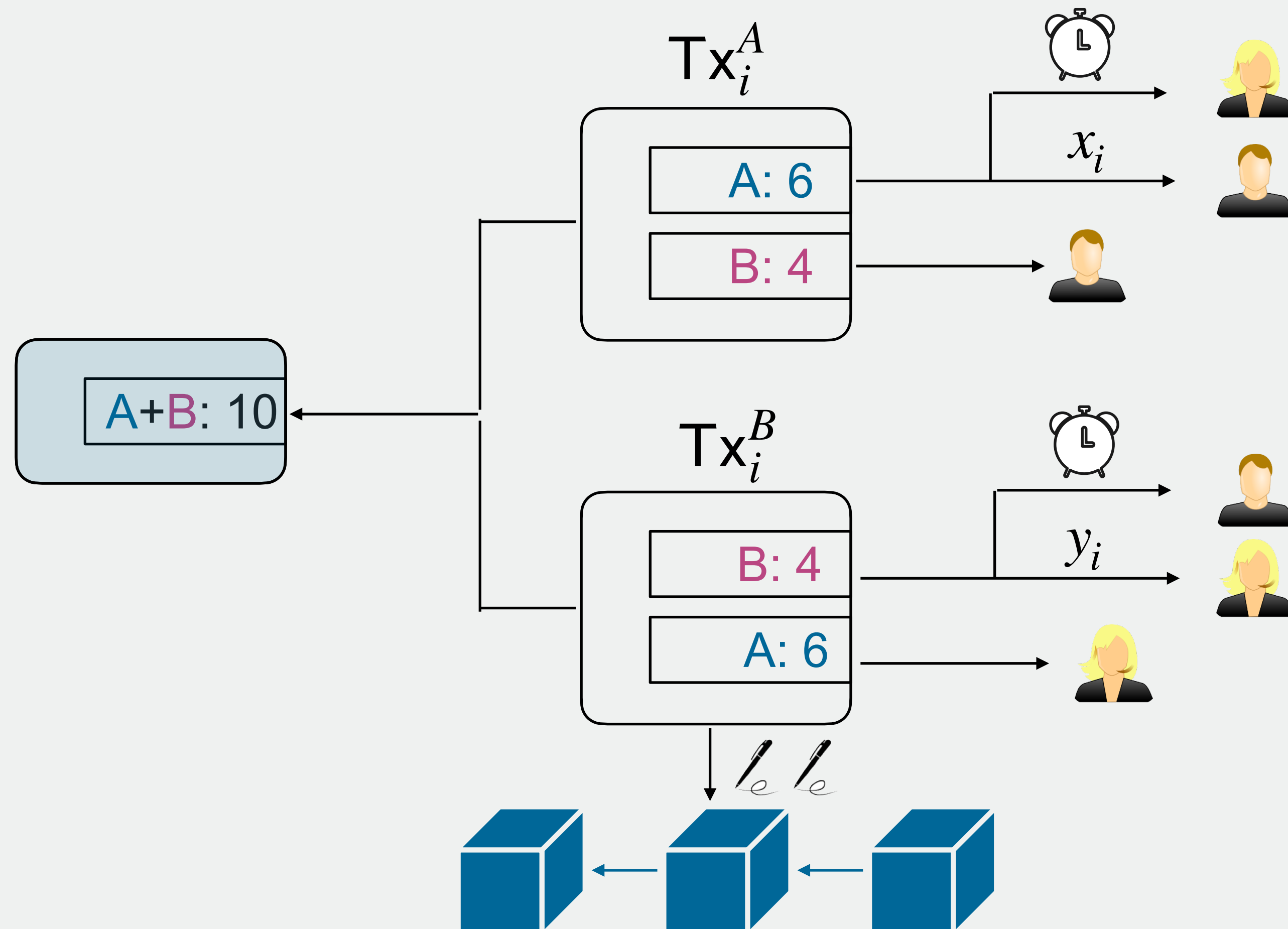
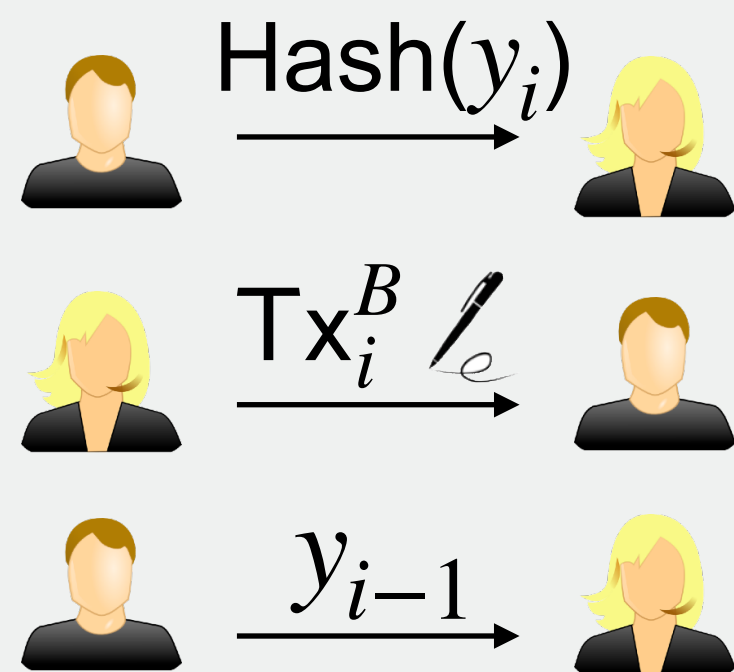
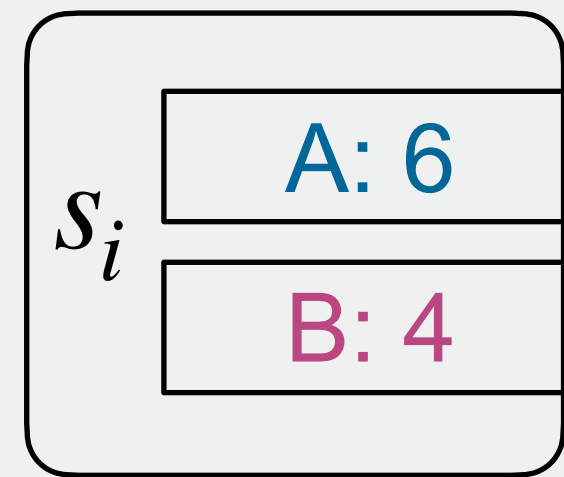
Channel Update



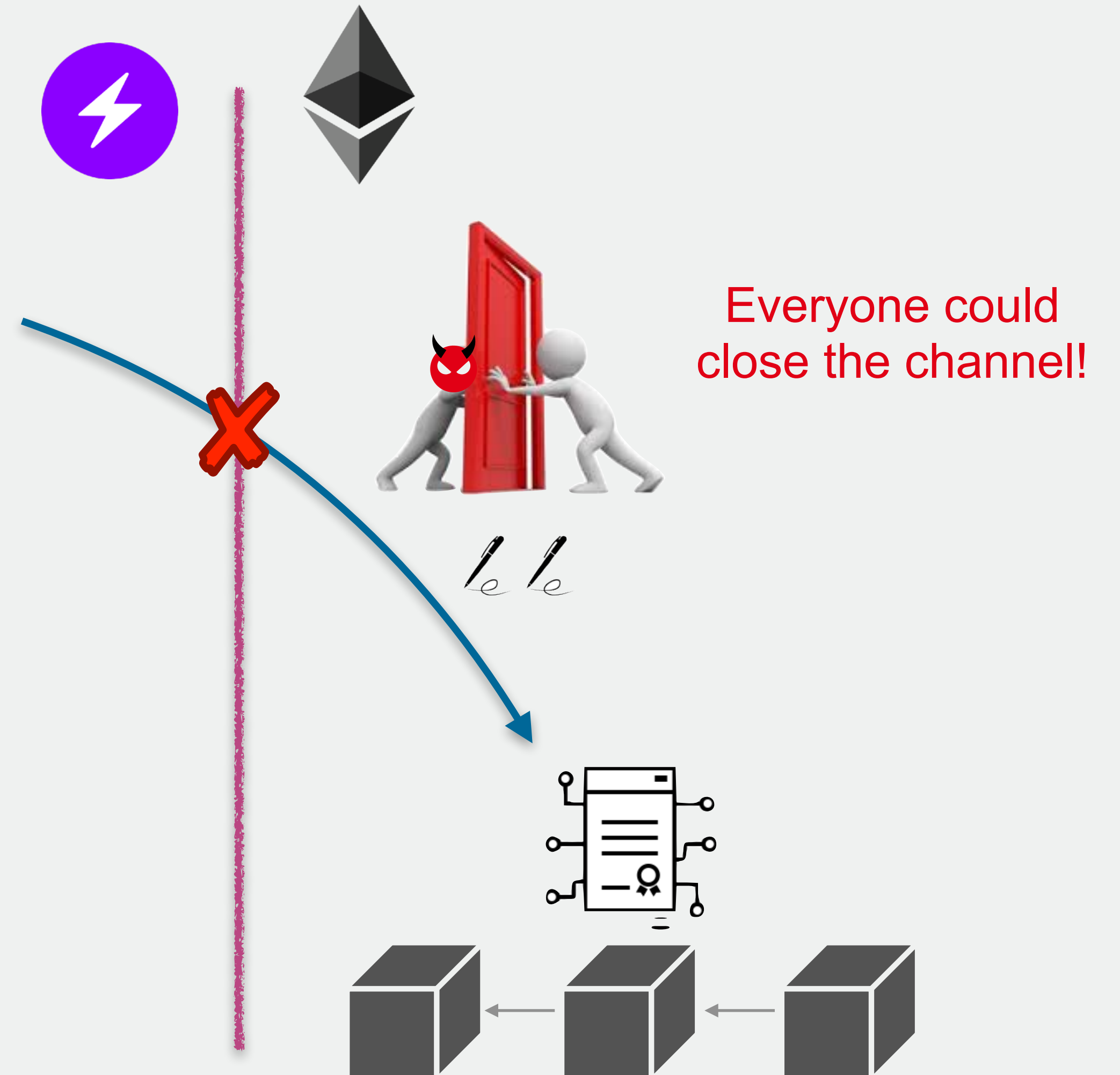
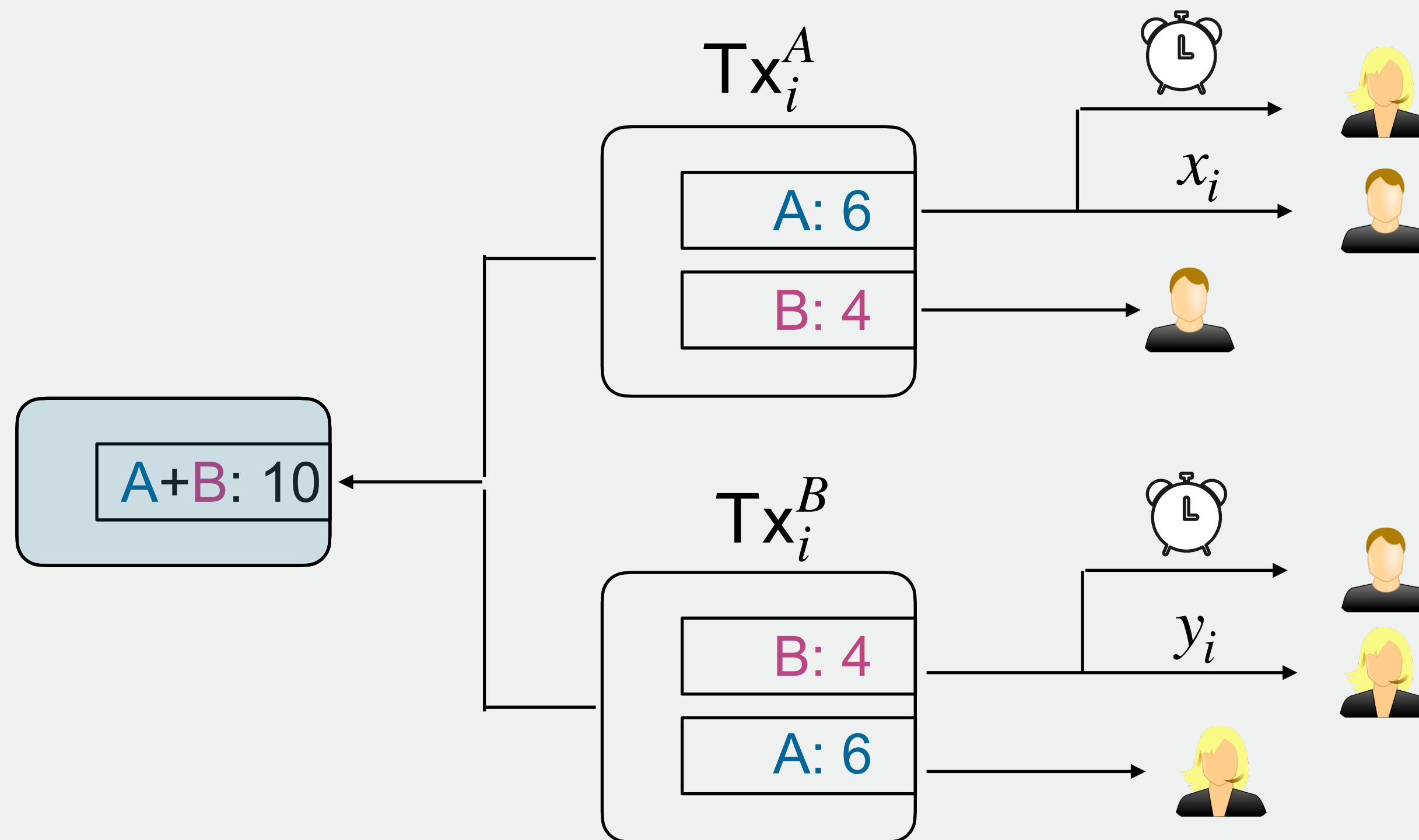
Channel Update



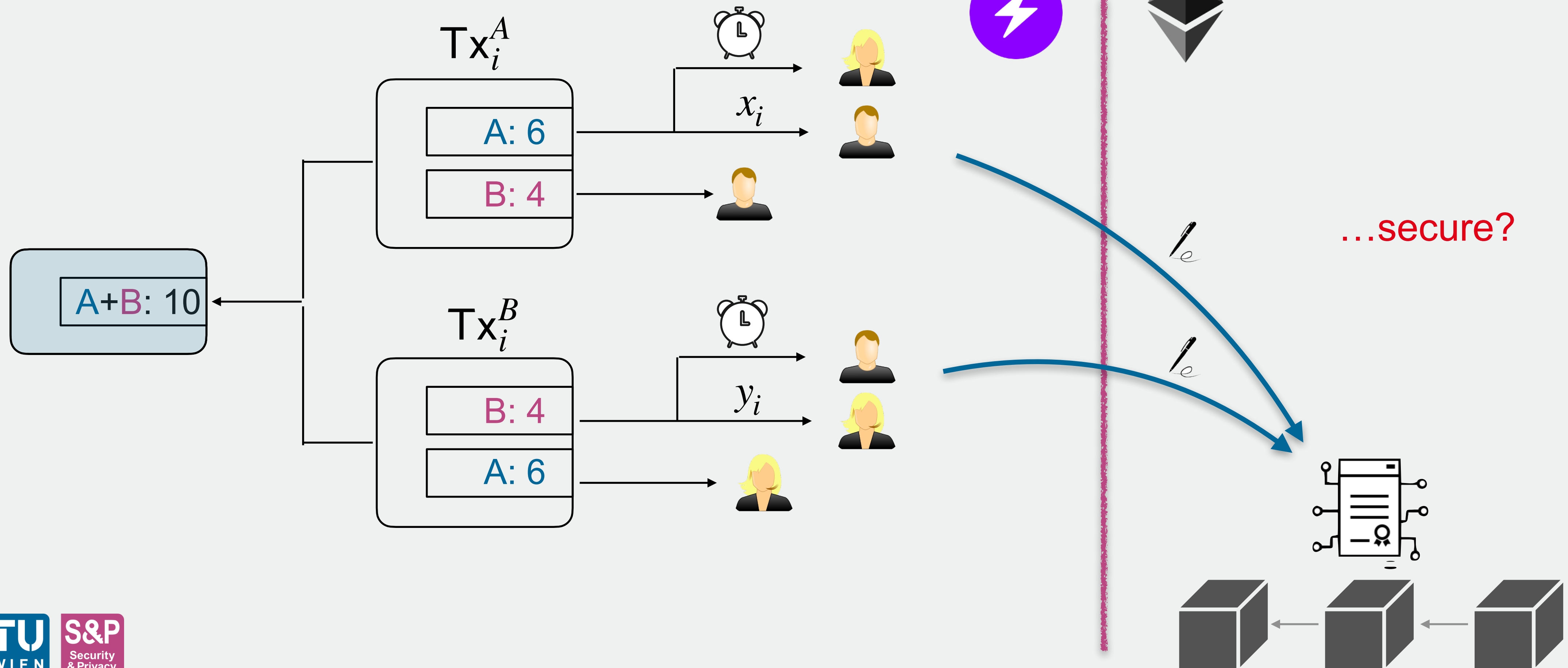
Channel Update



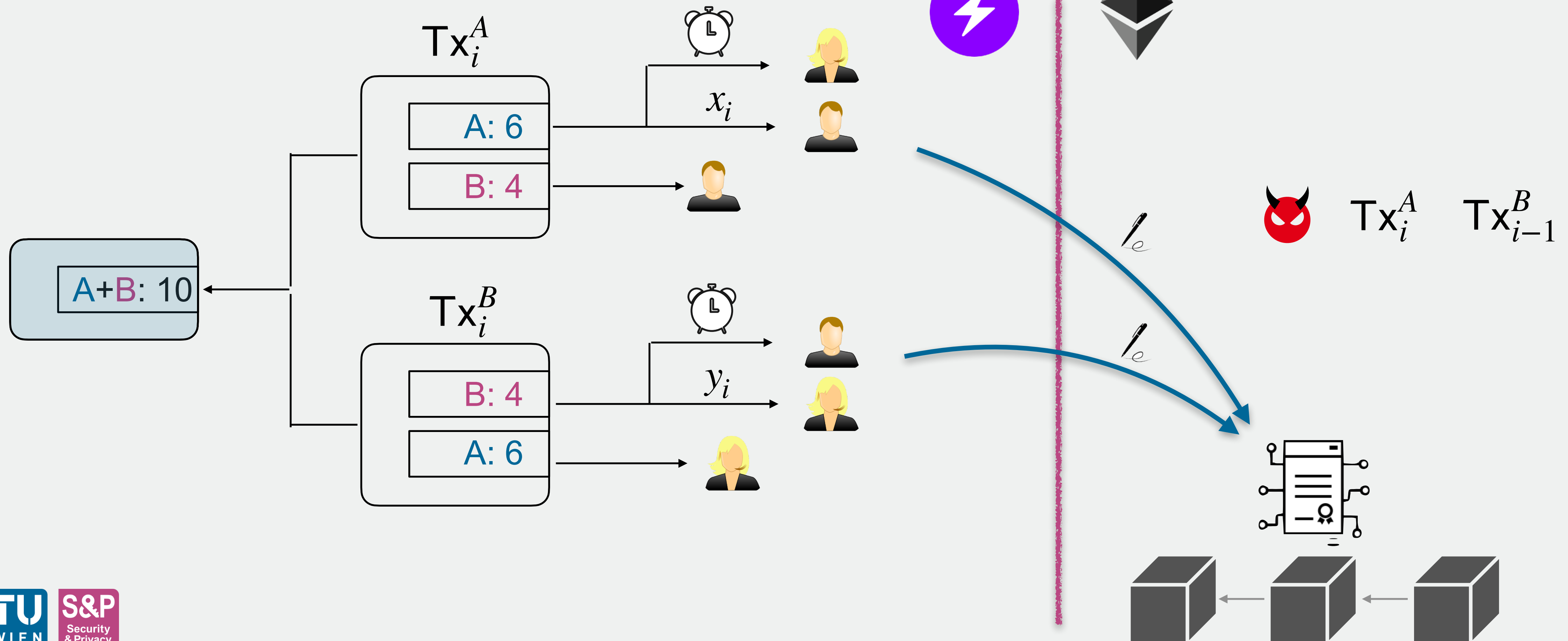
We need to be careful!



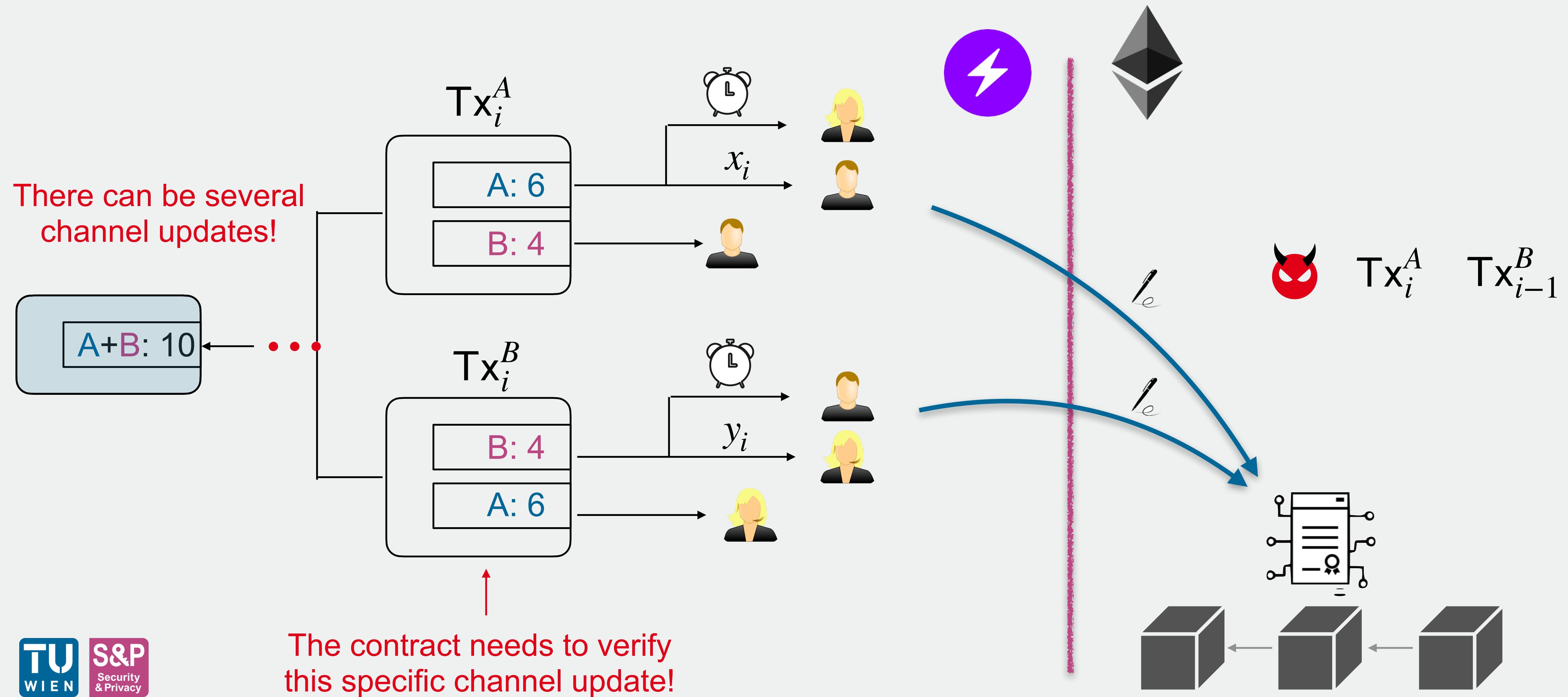
We need to be careful!



We need to be careful!

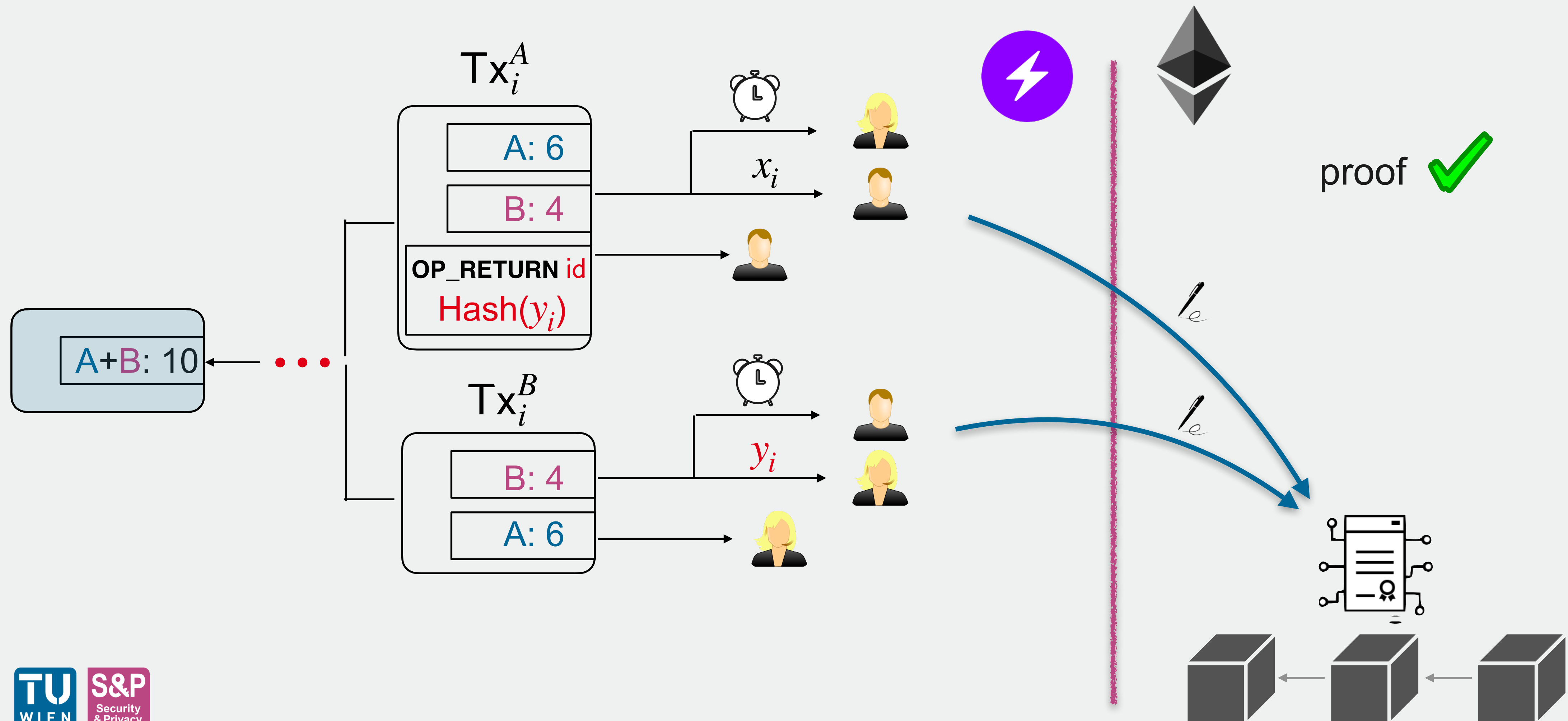


We need to be careful!



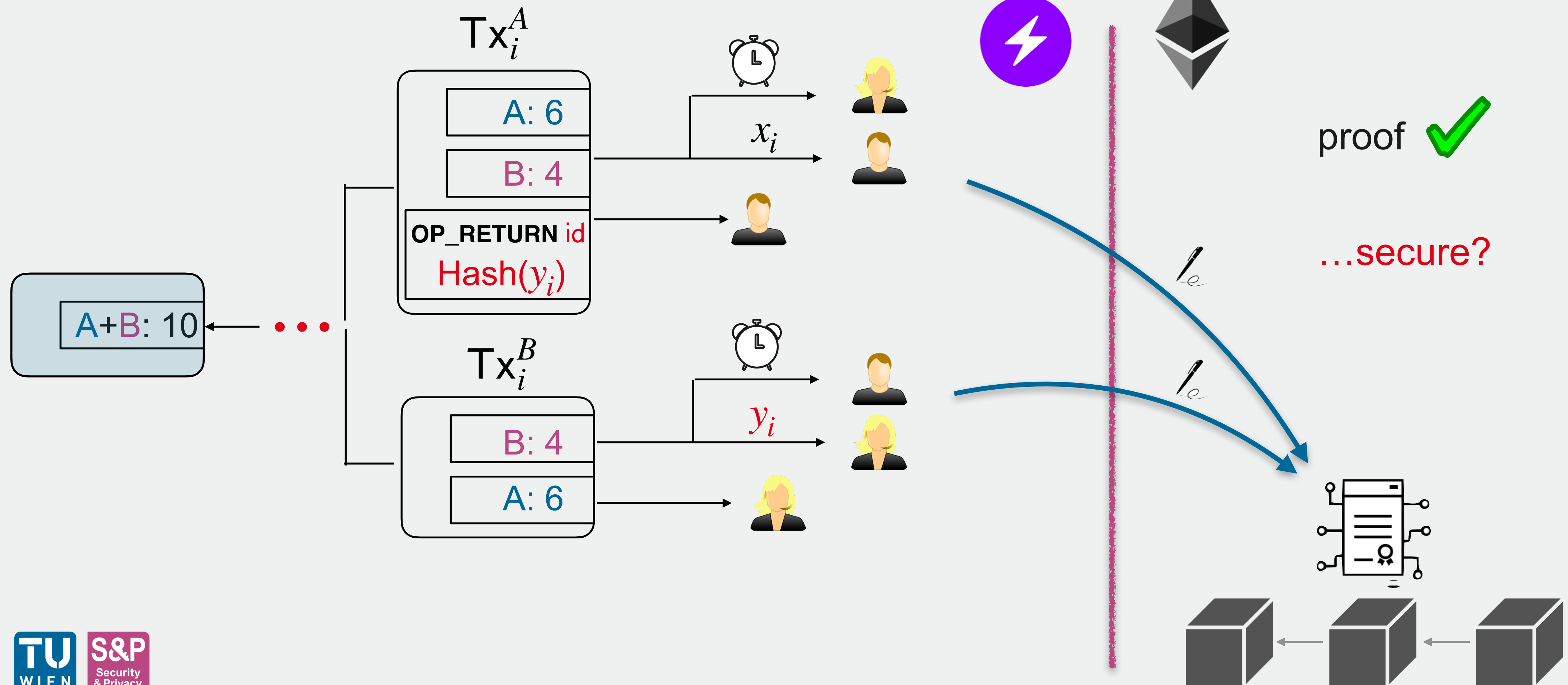
Towards security

Embed protocol-relevant information within Tx_i^A

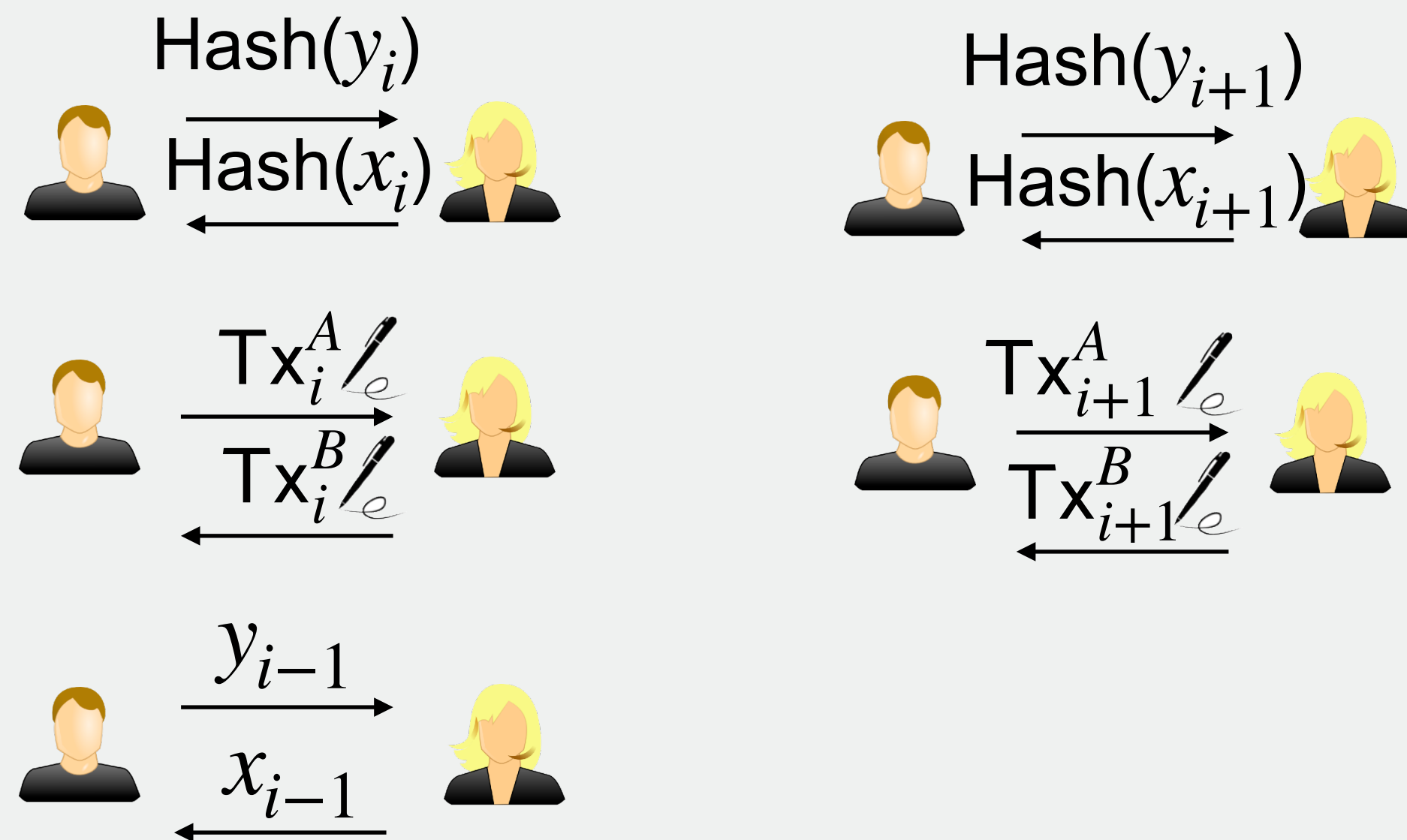


Towards security

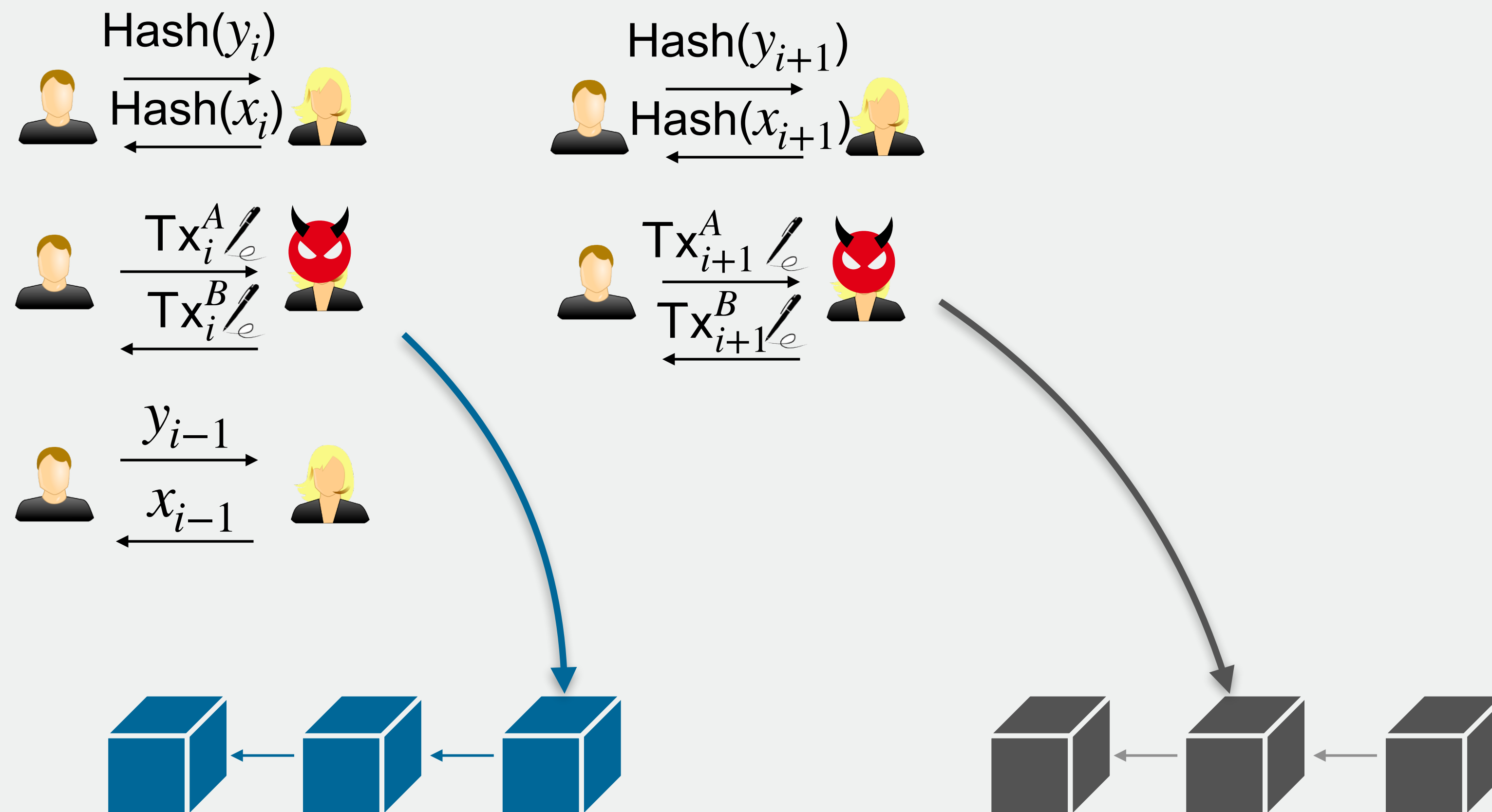
Embed protocol-relevant information within Tx_i^A



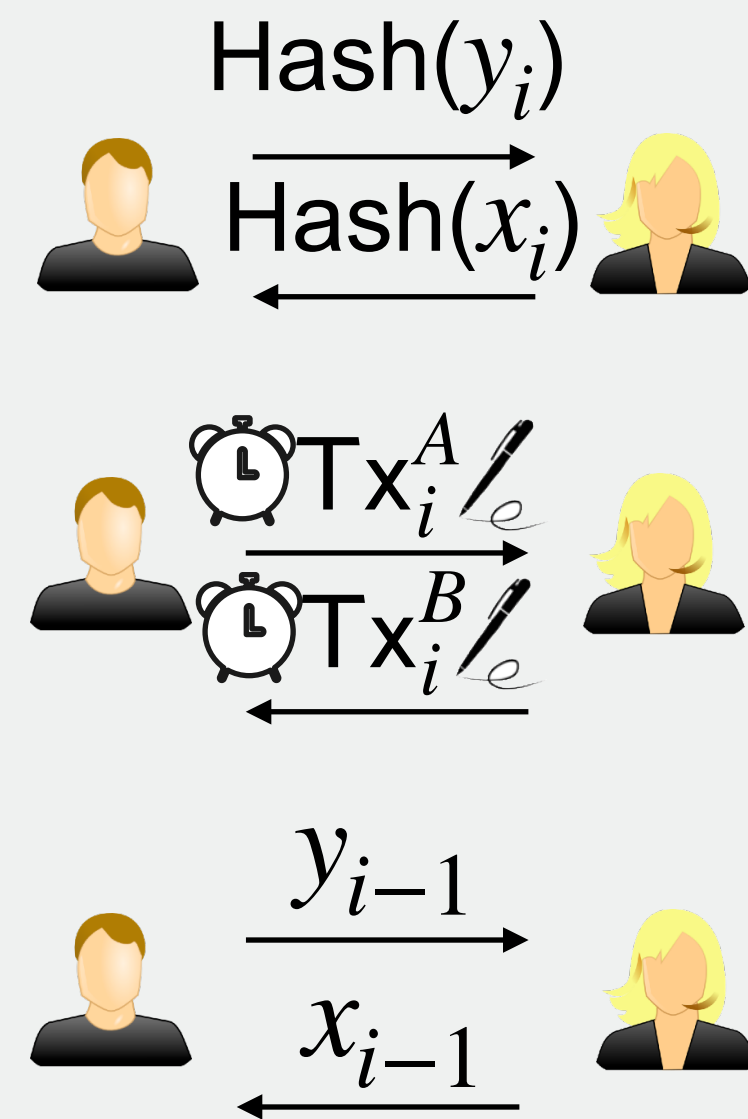
Towards security



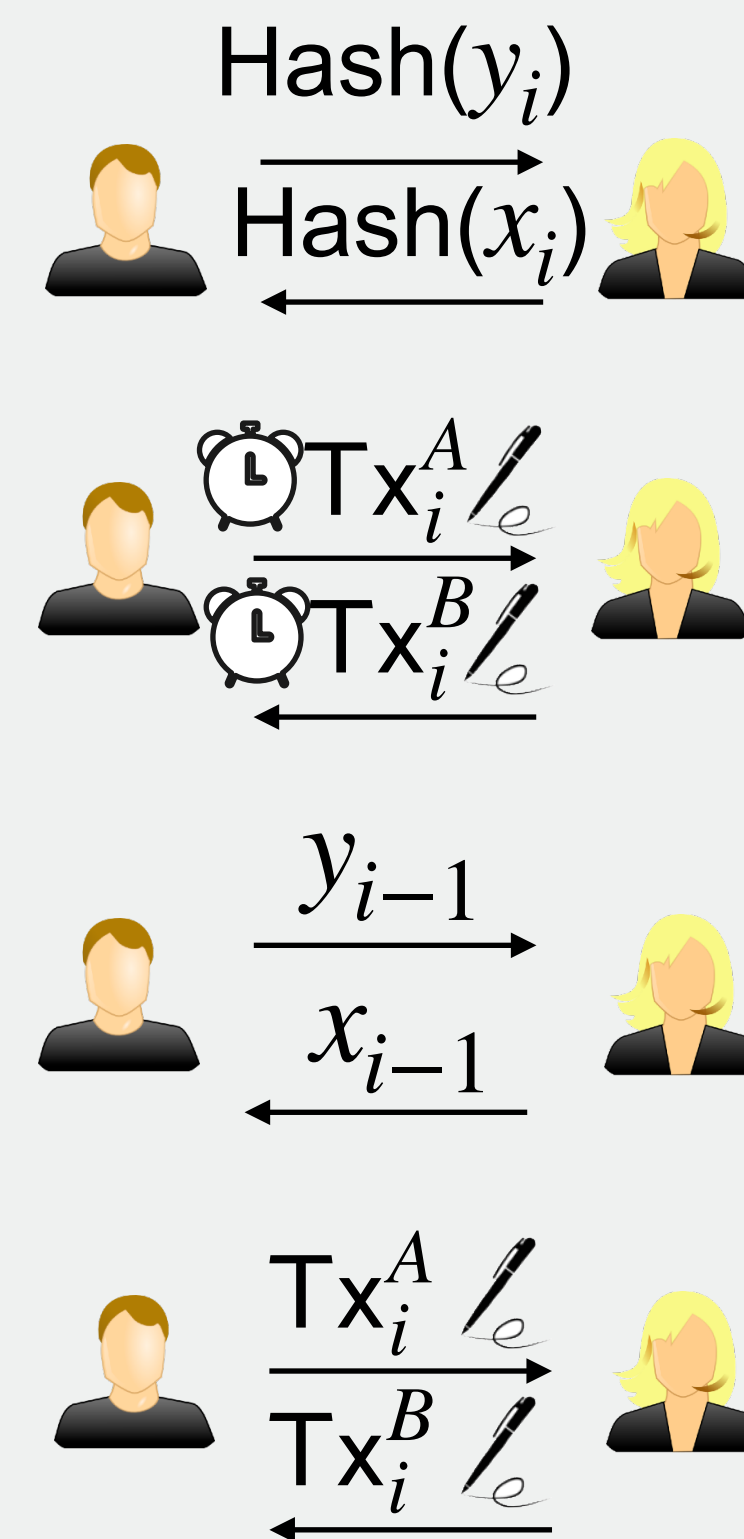
Towards security



Towards security



while Alba is active



when closing Alba