PERUN: Virtual Payment Hubs over Cryptocurrencies

Stefan Dziembowski

Lisa Eckey

Sebastian Faust

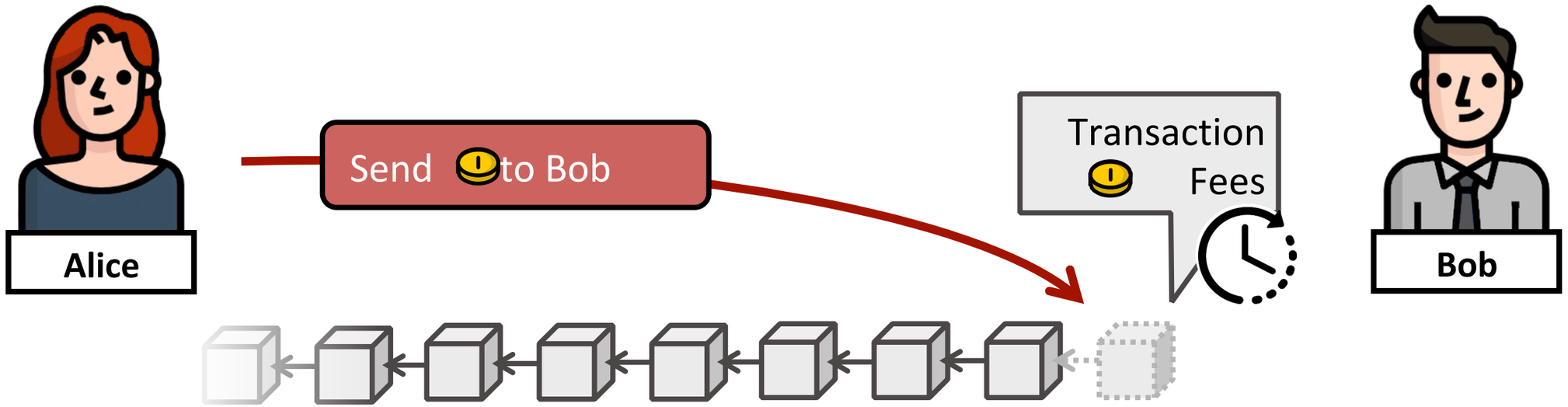
Daniel Malinowski

UNIVERSITY OF WARSAW

TECHNISCHE UNIVERSITÄT DARMSTADT

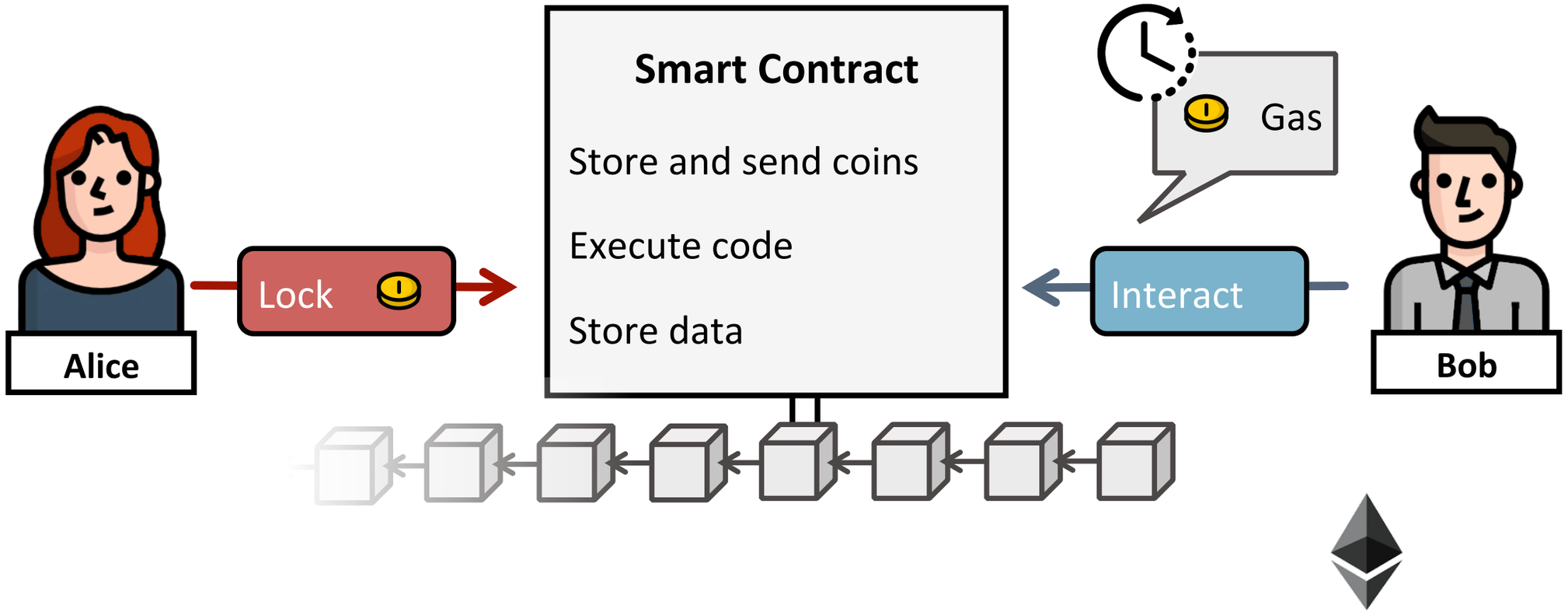
Blockchain Scalability

Problem: Blockchain transactions are slow and expensive



Goal: Cheap Fast Offline Secure Microtransactions

Smart Contracts



Guaranteed by the **underlying cryptocurrency**

PERUN in a Nutshell

New cryptographic protocol that allows microtransactions over cryptocurrencies

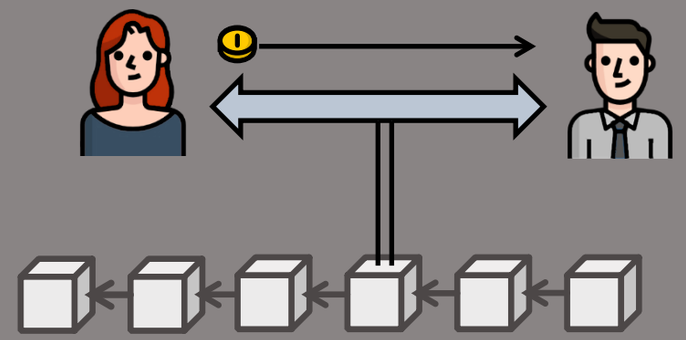
Cheap | Fast | Offline | Secure

- Based on smart contracts
- In a Hub-network

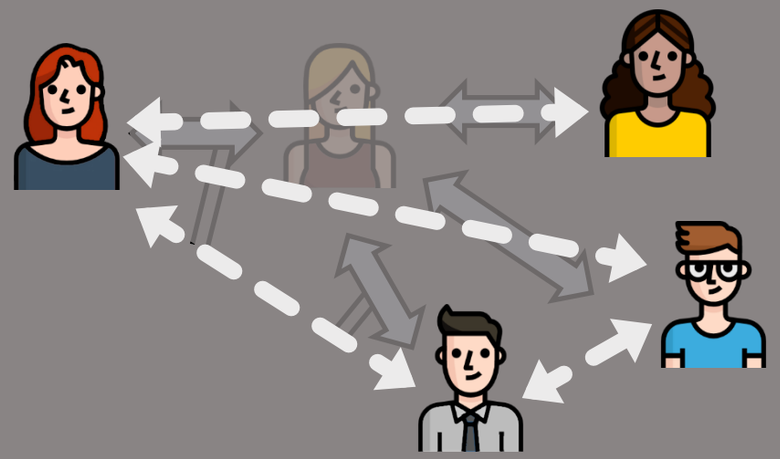
2 Types of payment channels

- **Ledger channels:** build over the blockchain
- **Virtual channels:** build over ledger channels

Ledger Payment Channels

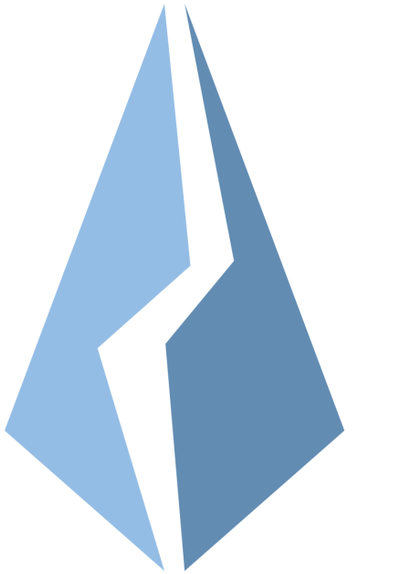


Virtual Payment Channels



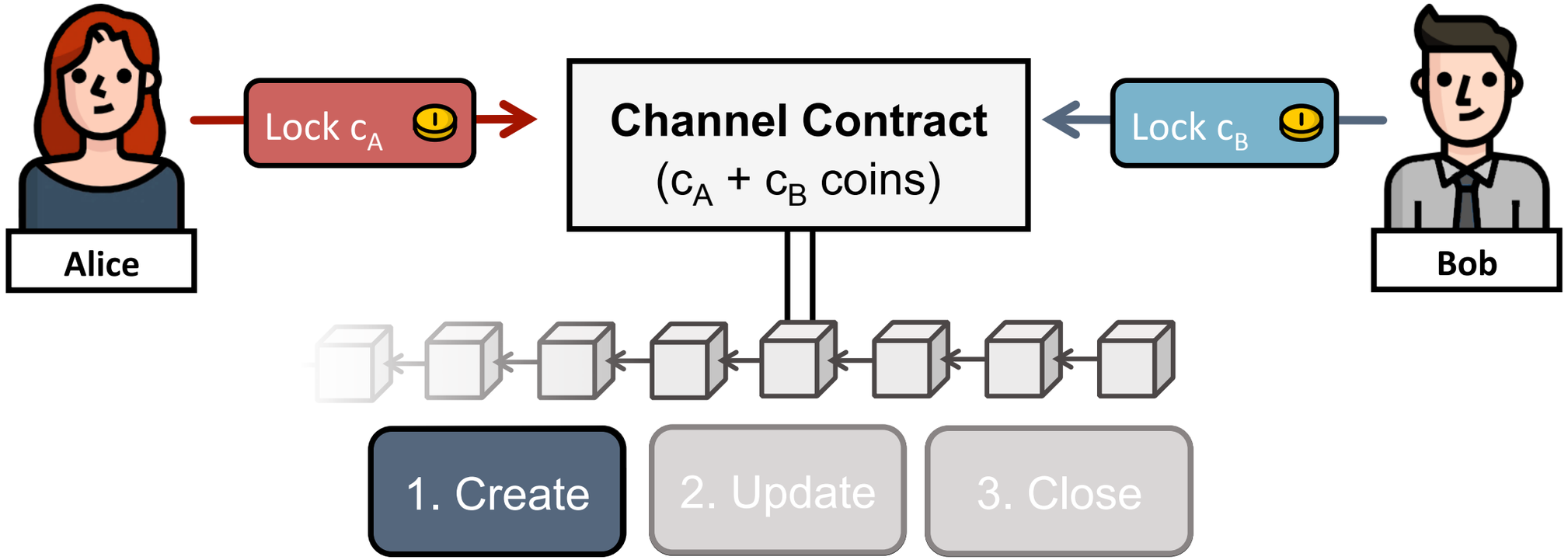
Outline

- Motivation
- **Ledger Payment Channels**
- Virtual Payment Channels
- Security & Performance
- Summary & Outlook



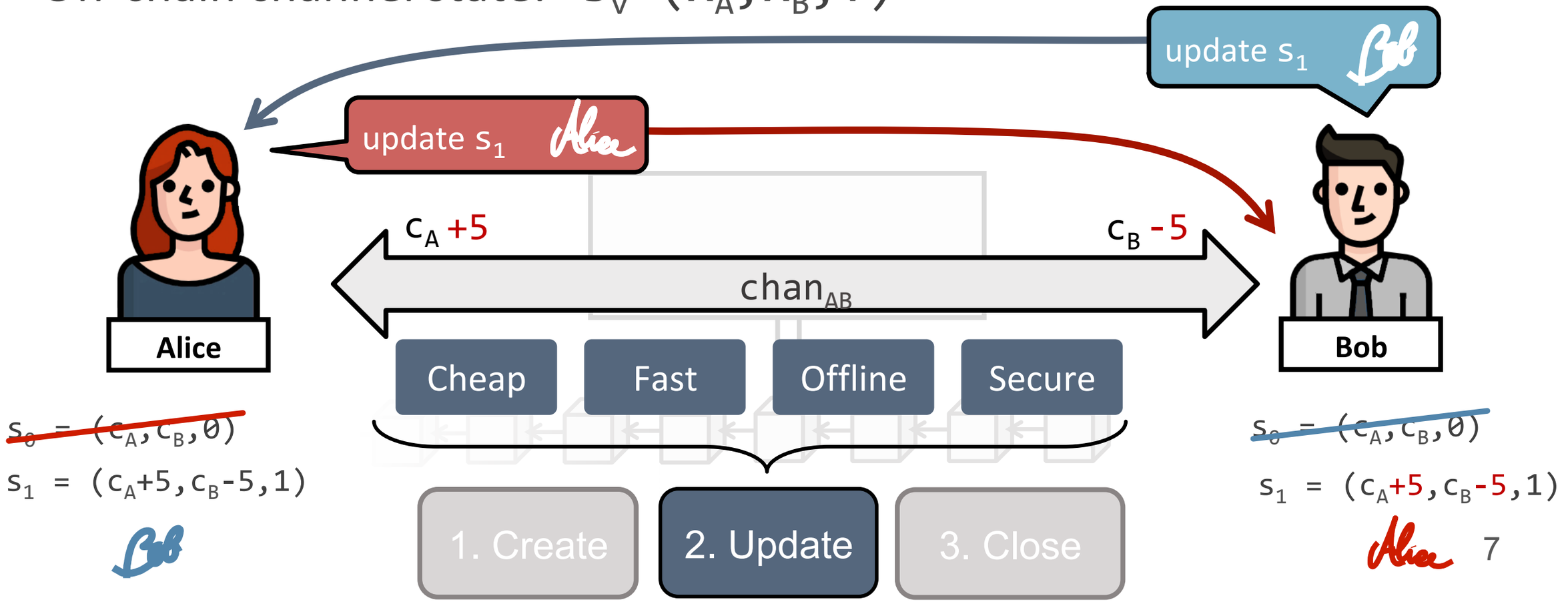
(Ledger) Payment Channels*

* Lightning, Spilman, Duplex, Sprites, Raiden, Counterfactual, L2 ….

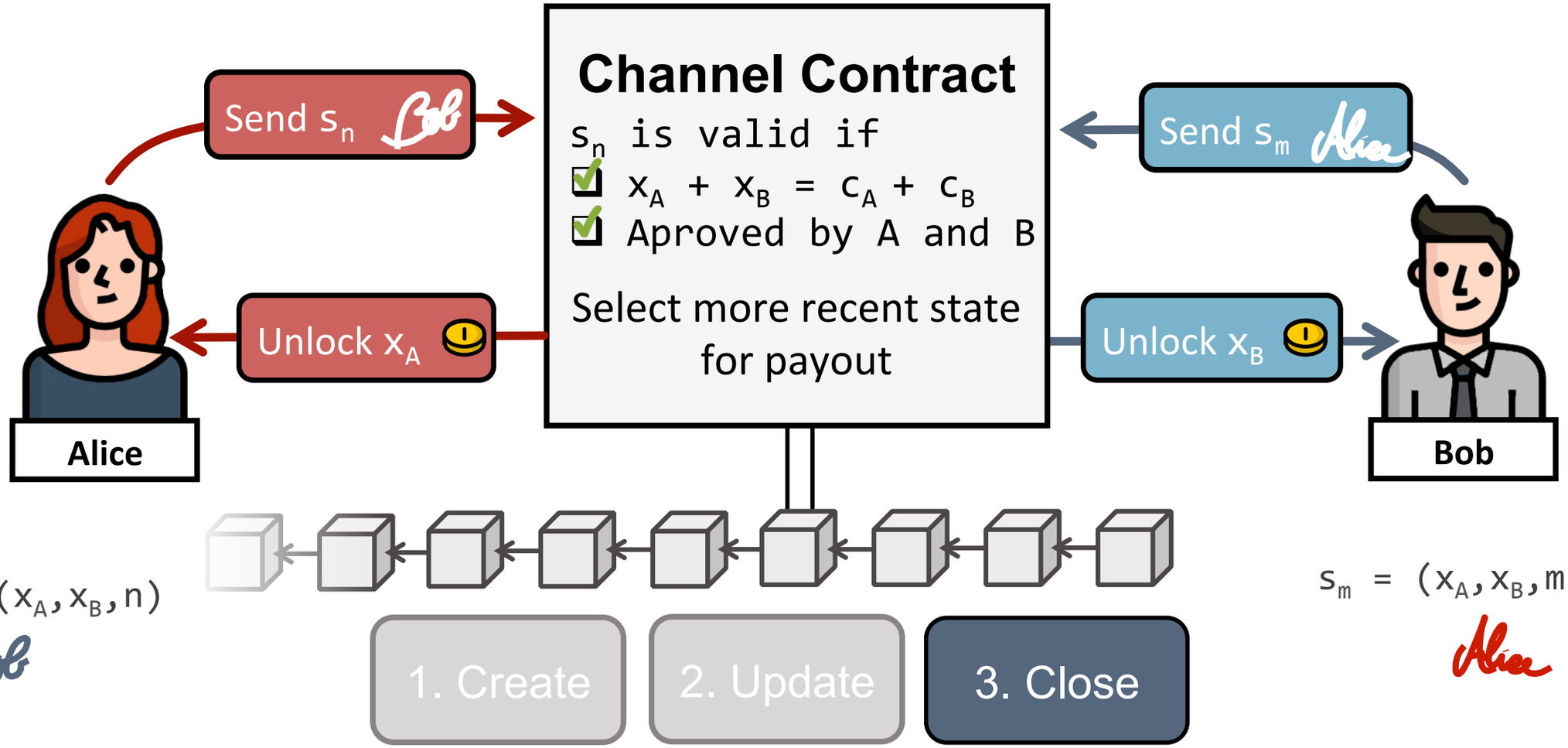


(Ledger) Payment Channels

Off-chain channel state: $s_v=(x_A,x_B,v)$



(Ledger) Payment Channels

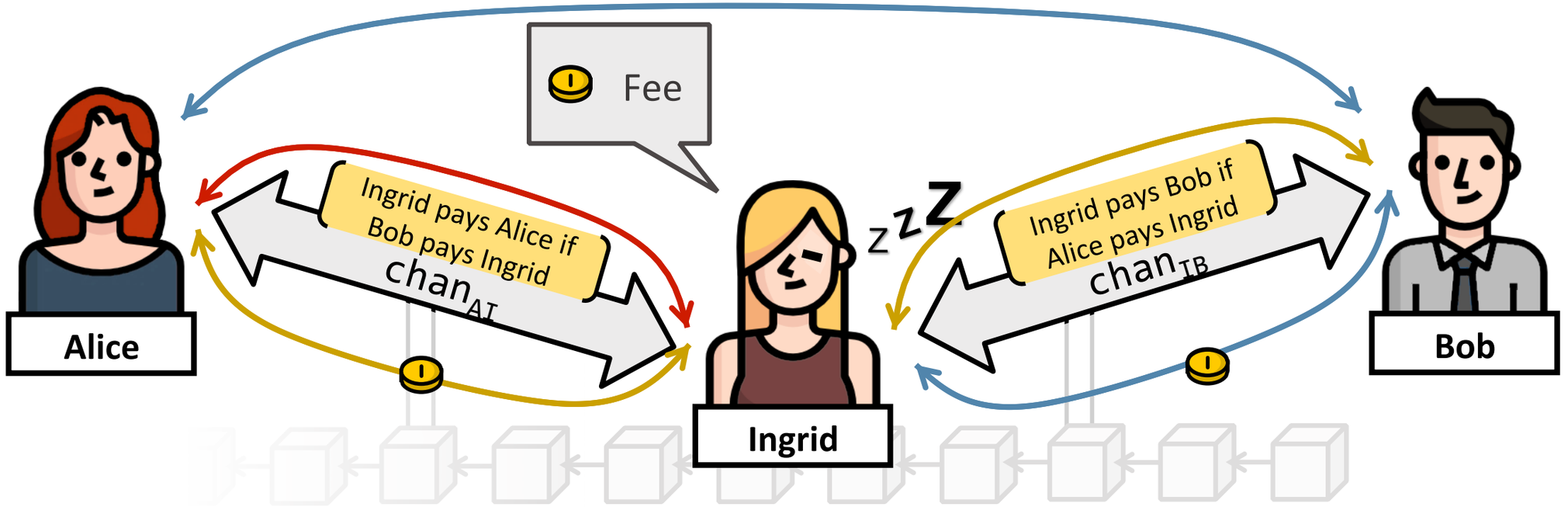


Outline

- Motivation
- Ledger Payment Channels
- **Virtual Payment Channels**
- Security & Performance
- Summary & Outlook

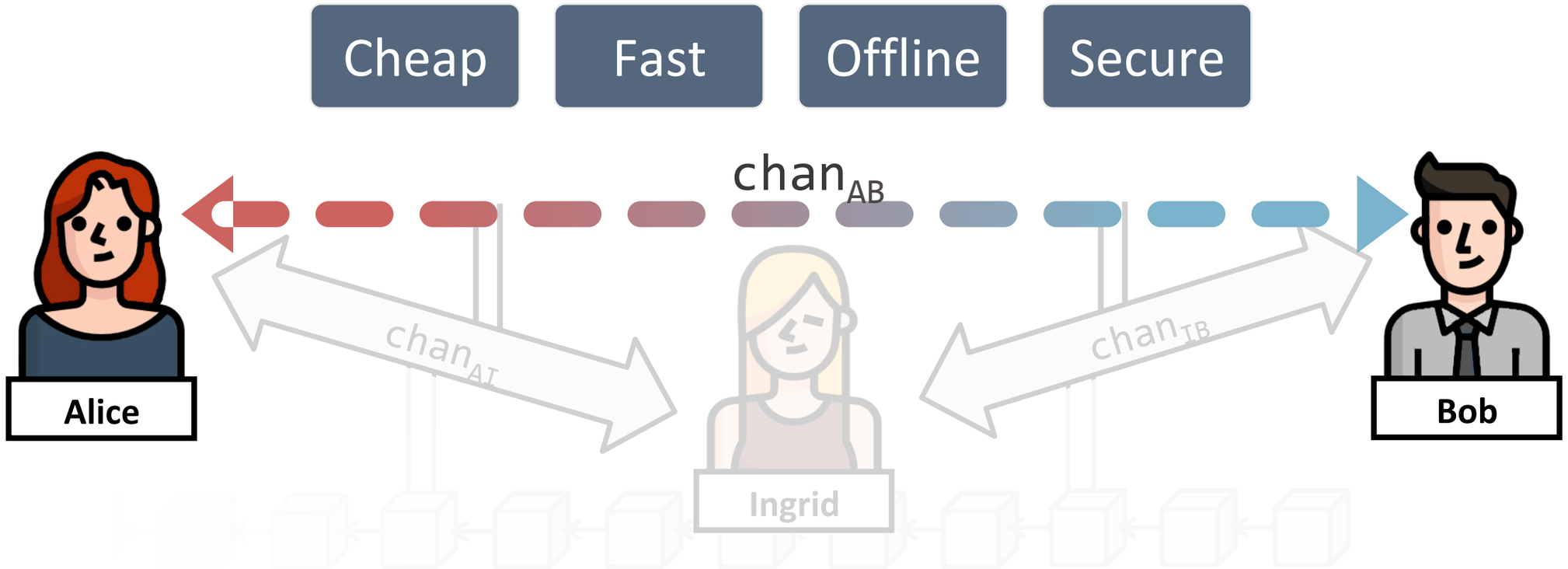
Hashed Time Locked Contracts (HTLC)*

Idea: Route every transaction via intermediary

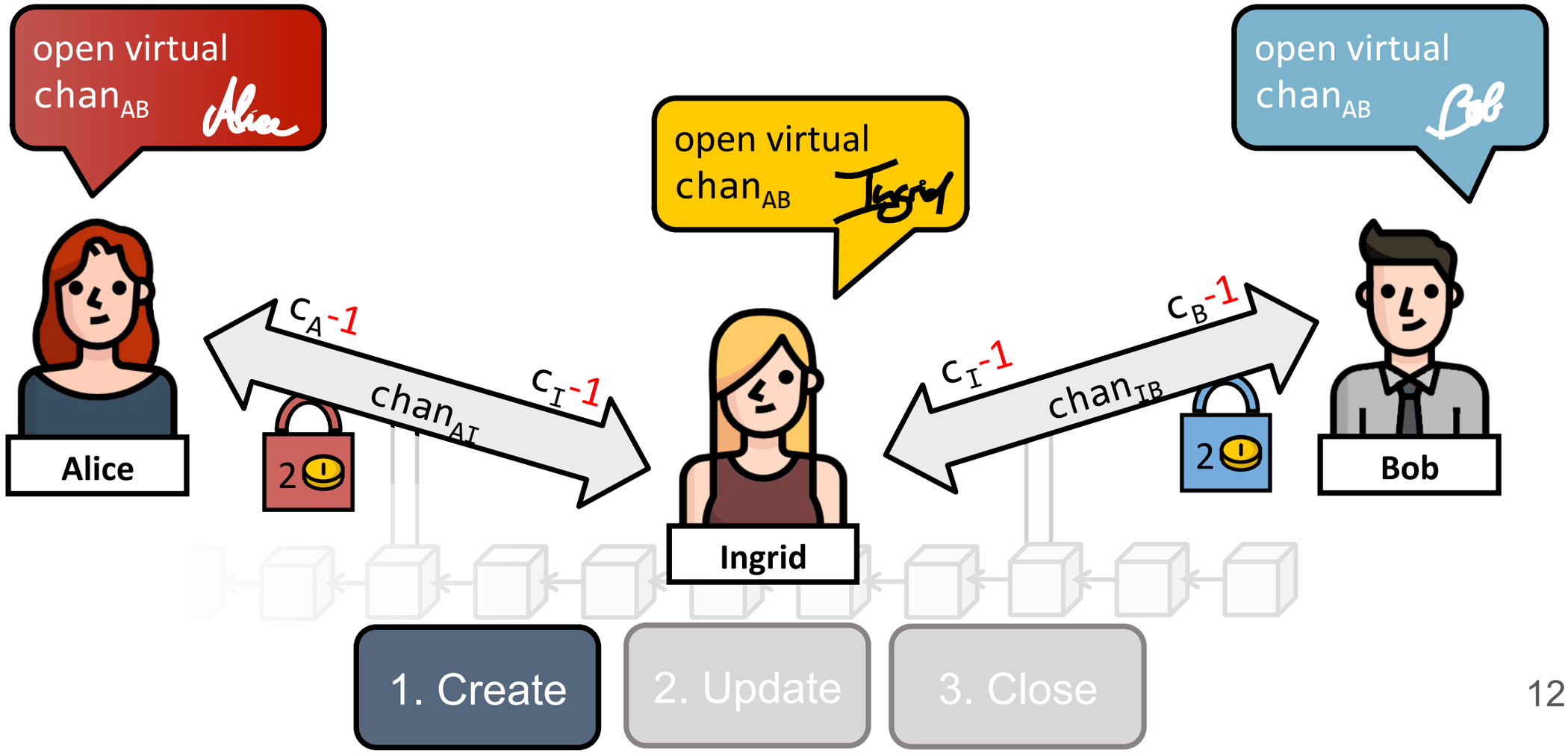


* J. Poon, T. Dryja: The bitcoin lightning network: Scalable off-chain instant payments. (2016)

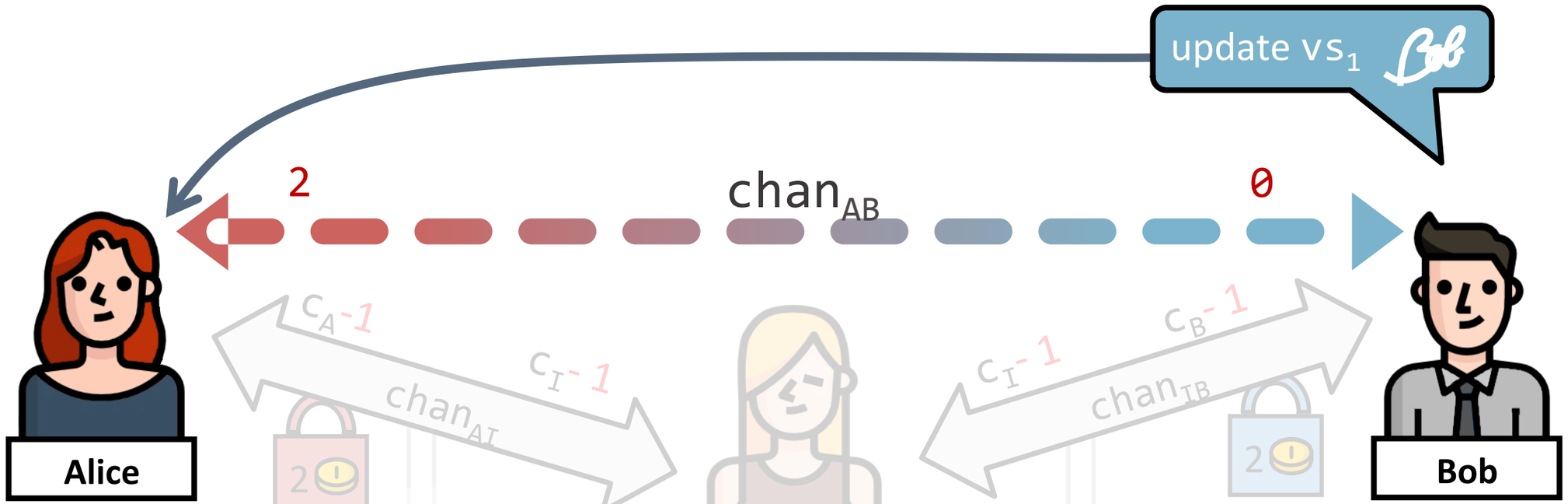
PERUN Virtual Channels



PERUN Virtual Channels



PERUN Virtual Channels



$s_m = (c_A\text{-}1,\ c_I\text{-}1,\ m)$

~~$vs_0 = (1,\ 1,\ 0)$~~

$vs_1 = (2,\ 0,\ 1)$

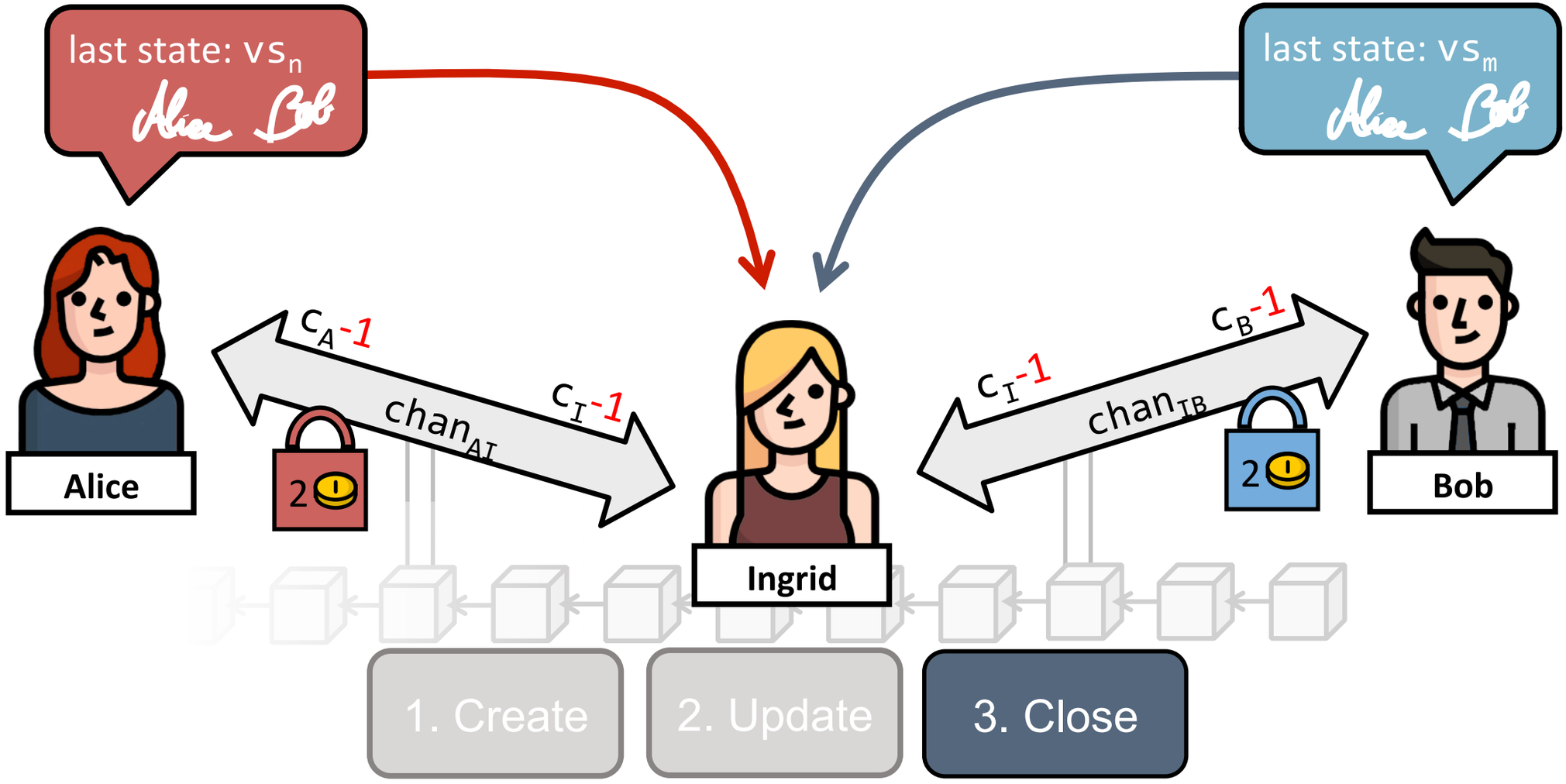
$s_n = (c_I\text{-}1,\ c_B\text{-}1,\ n)$

$vs_0 = (1,\ 1,\ 0)$

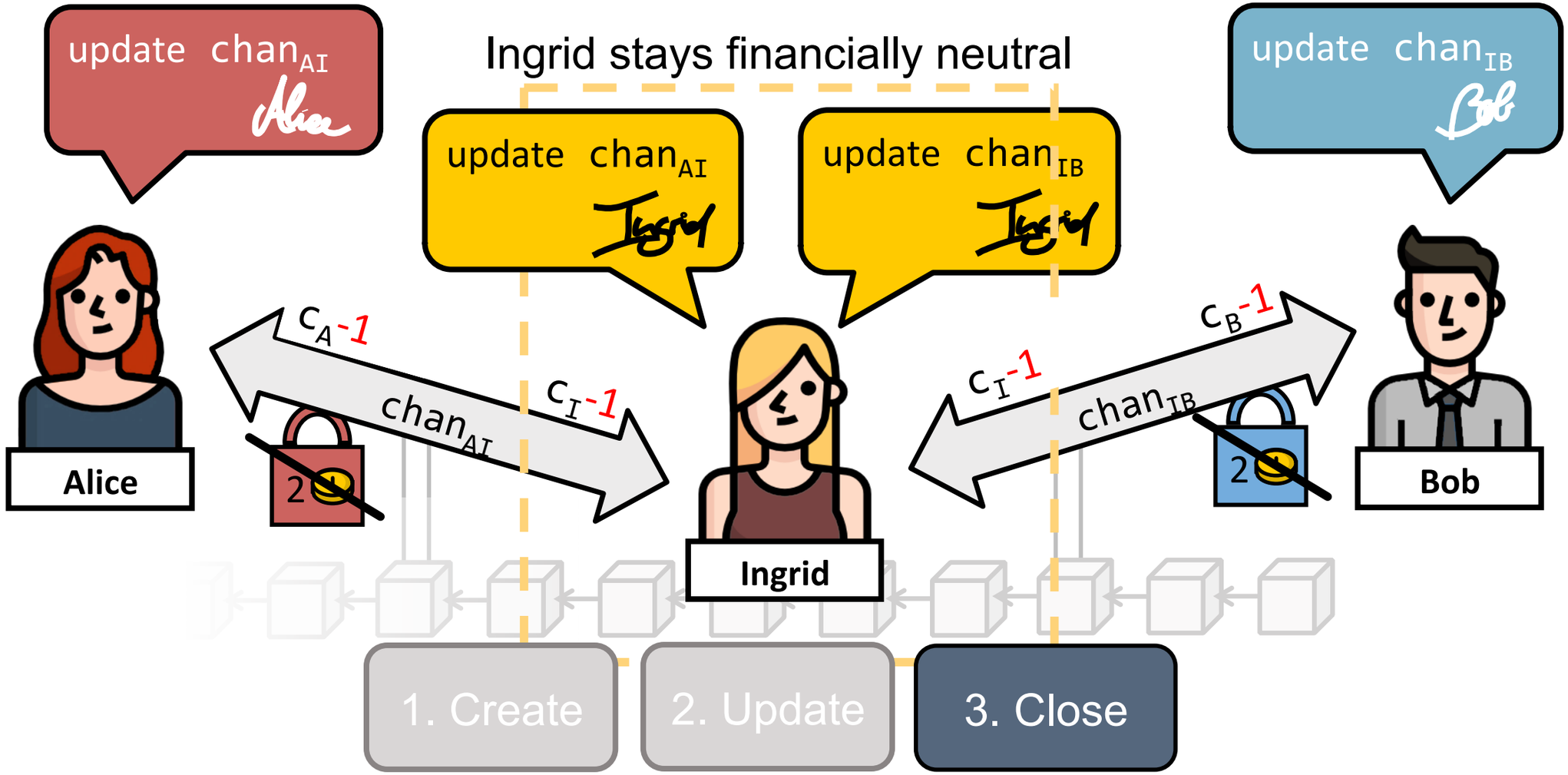
$vs_1 = (2,\ 0,\ 1)$

1. Create | **2. Update** | 3. Close

PERUN Virtual Channels



PERUN Virtual Channels

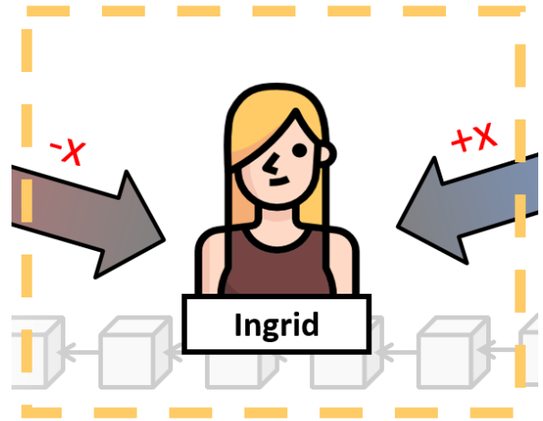


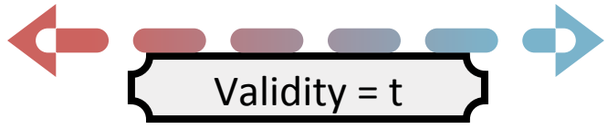
Outline

- Motivation
- Ledger Payment Channels
- Virtual Payment Channels
- **Security & Performance**
- Summary & Outlook

(Informal) PERUN Security

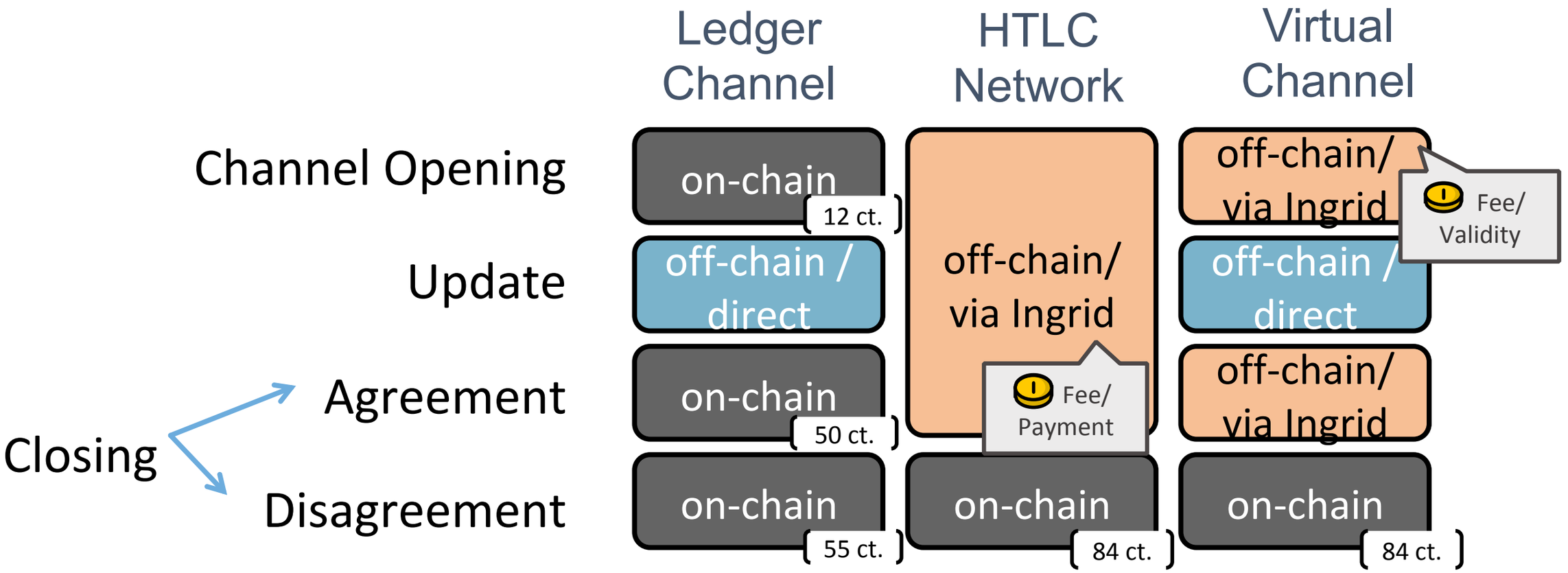
- Balance neutrality for intermediary
- Consensus on channel creation and update
- Guaranteed balance payout for Alice & Bob
- Guaranteed channel closing





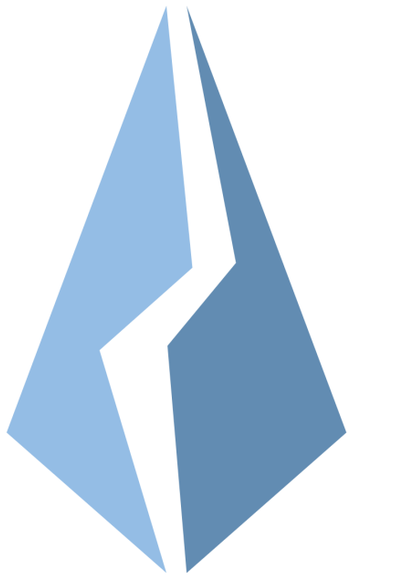
This must hold even if ALL other players collude

PERUN Performance



Outline

- Motivation
- Ledger Payment Channels
- Virtual Payment Channels
- Security & Performance
- **Summary & Outlook**



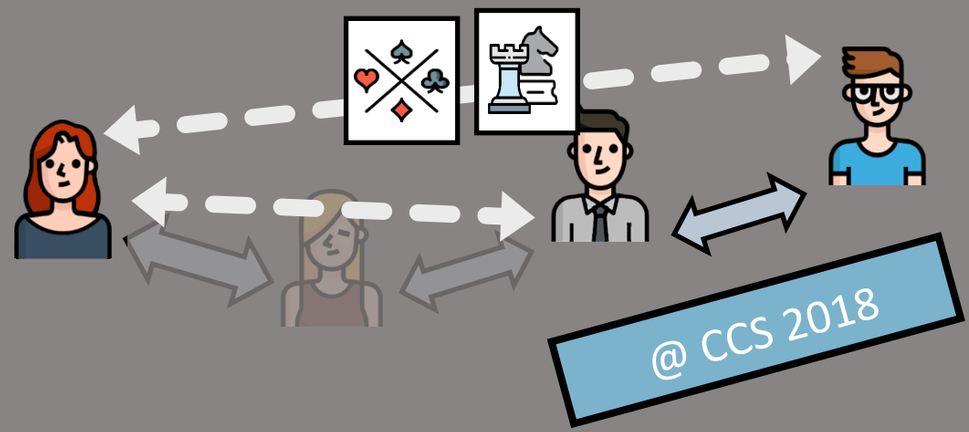
PERUN

Summary

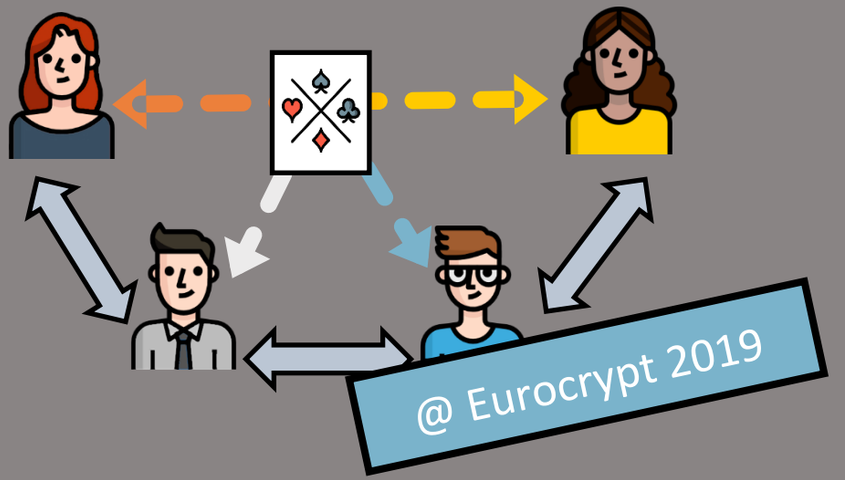
- New formalism for payment channels
- Virtual payment channels
  - Can be opened and closed off-chain
  - Can be updated without intermediary
- Provable secure protocol
  - New model of DL and Smart Contracts
  - Rigorous security proof in UC model

Extensions

General State Channel Networks



Multi-party Virtual State Channels



Thank you for your attention!

For more information visit:

www.perun.network