MONASH University

The 83rd IFIP WG.10.4 Workshop

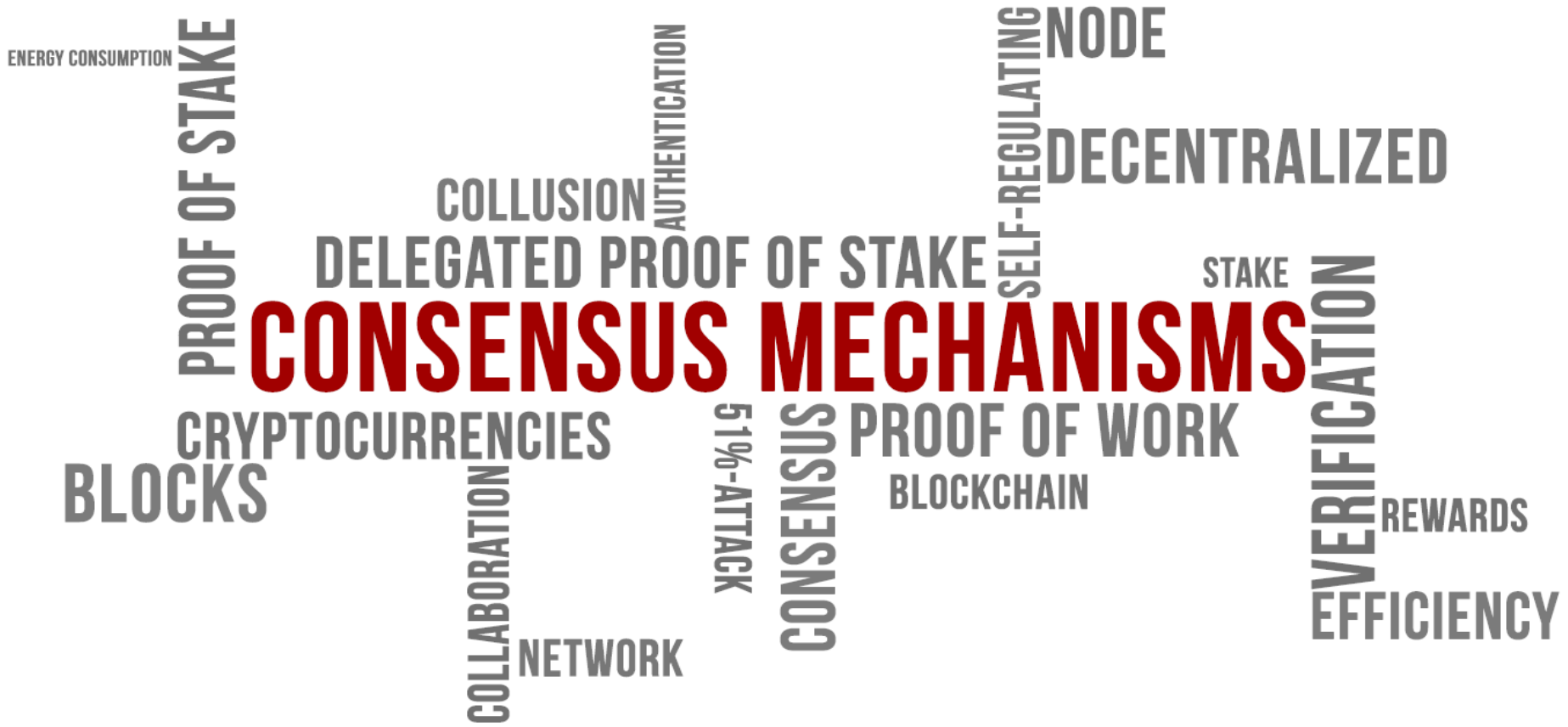
Layer 2 scaling solutions – payment channel network for scriptless blockchain

16 Jan 2023

Presenter: Zhimei Sui

Supervisor: Dr. Jiangshan Yu and Prof. Joseph K. Liu

Blockchain



- Decentralized data structure that records every transaction and allows for public verification.
- Global consensus: the entire blockchain is inspected by everyone.

MONASH University

Privacy

- Since a permissionless blockchain is publicly accessible, the data recorded on-chain can be easily tracked. It causes:
  - the leakage of user identity [1]
  - Frontrunning [2]
  - …
- Some privacy-preserving blockchains are proposed, such as Monero, Zcash, …

[1] Ron, Dorit, and Adi Shamir. "Quantitative analysis of the full bitcoin transaction graph." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013.
[2] https://consensys.github.io/smart-contract-best-practices/attacks/frontrunning/
[3] https://www.getmonero.org/
[4] https://z.cash/

MONASH University

Scriptless Blockchains

While privacy-preserving blockchains are usually scriptless …

Functions Supported by Scriptless Blockchains:

- **Signatures**
- **Commitments**

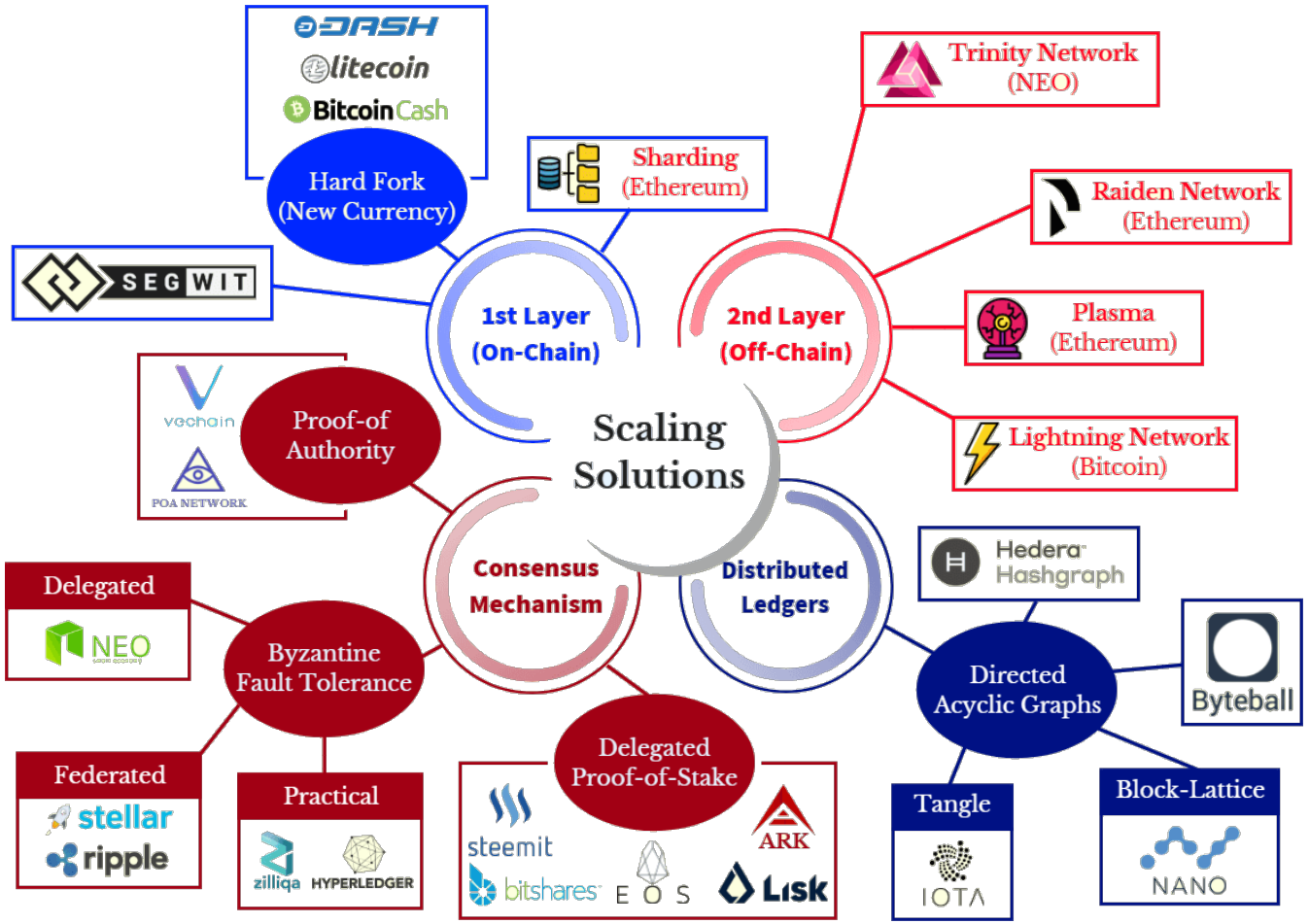
Scriptless cryptocurrencies:

- **Monero** (No. 23, ~ 3.1 Billion USD)
- **Zcash** (No. 59, ~700 million USD)

…

Blockchain Scalability Solutions

- **High** Tx Fees
- **Low** Tx Confirmation Speed
- **Low** Throughput



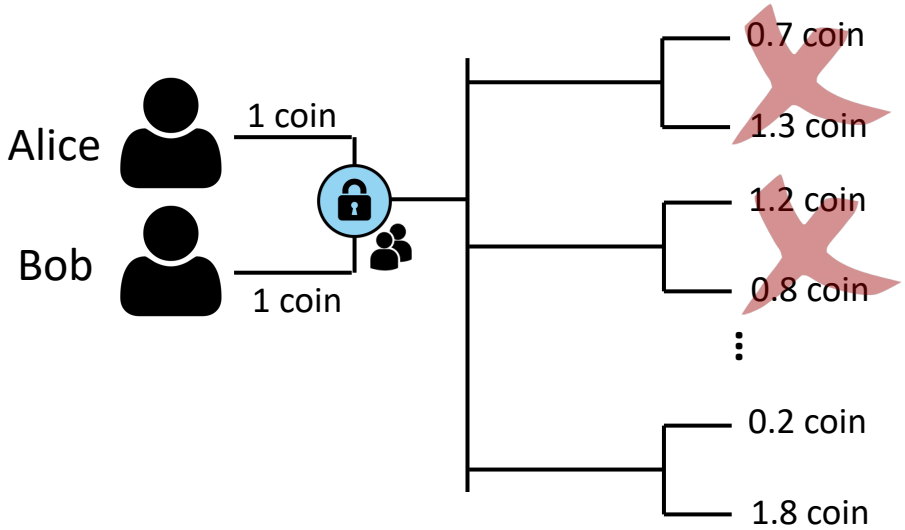
My research topic: payment channel network for privacy-preserving (scriptless) blockchain.

MONASH University

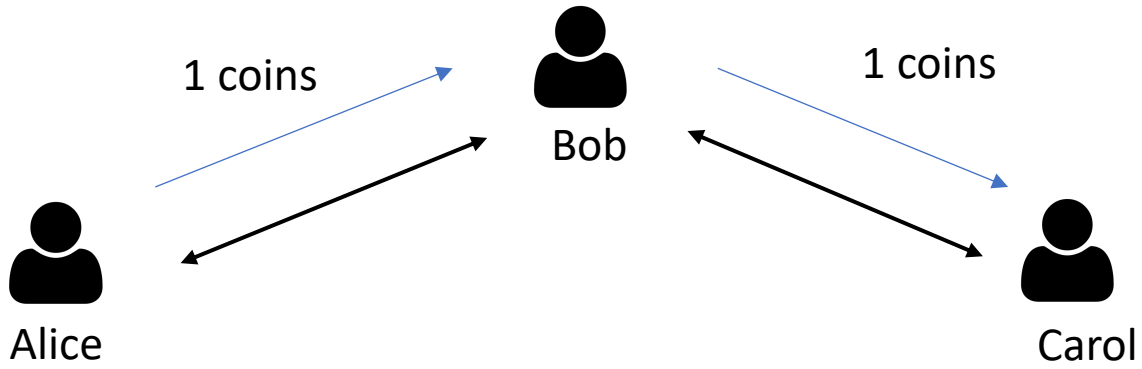
MONASH
University

Payment Channel and its Network

Payment Channel and its Network



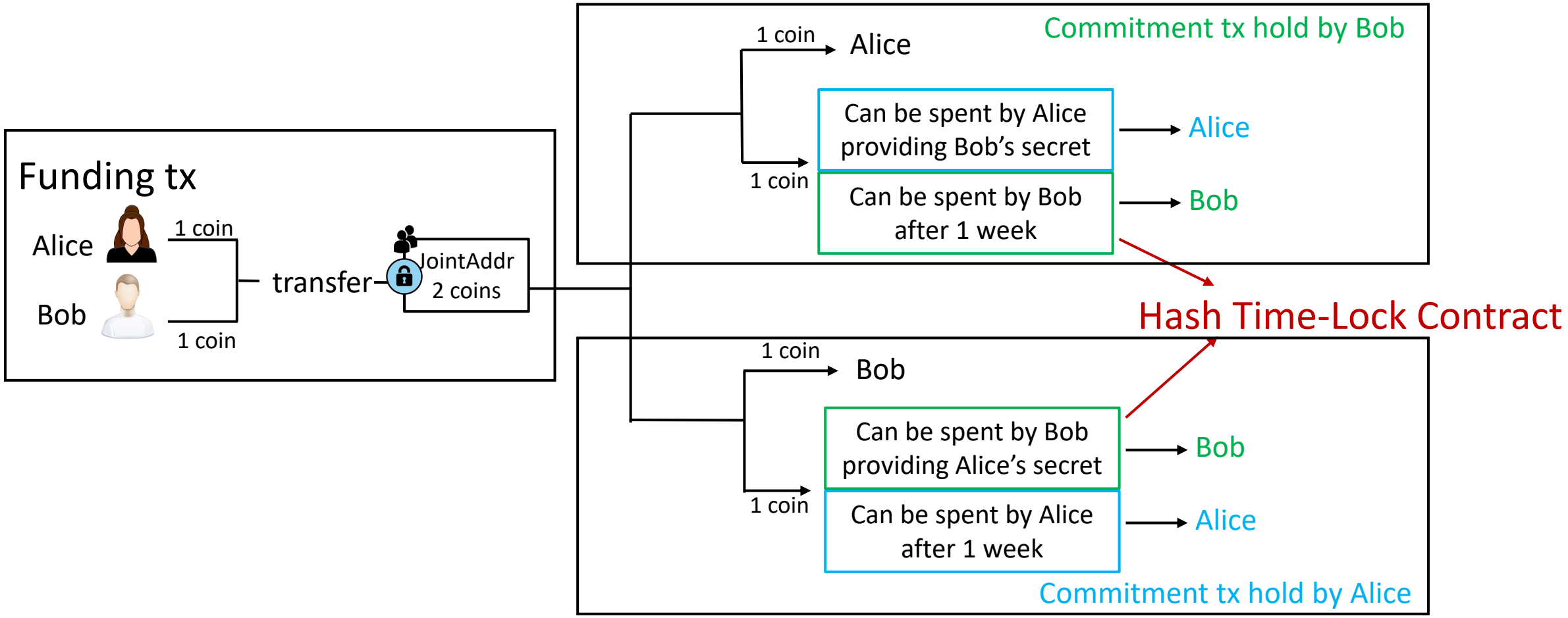
Payment Channel



Payment Channel Network

MONASH University

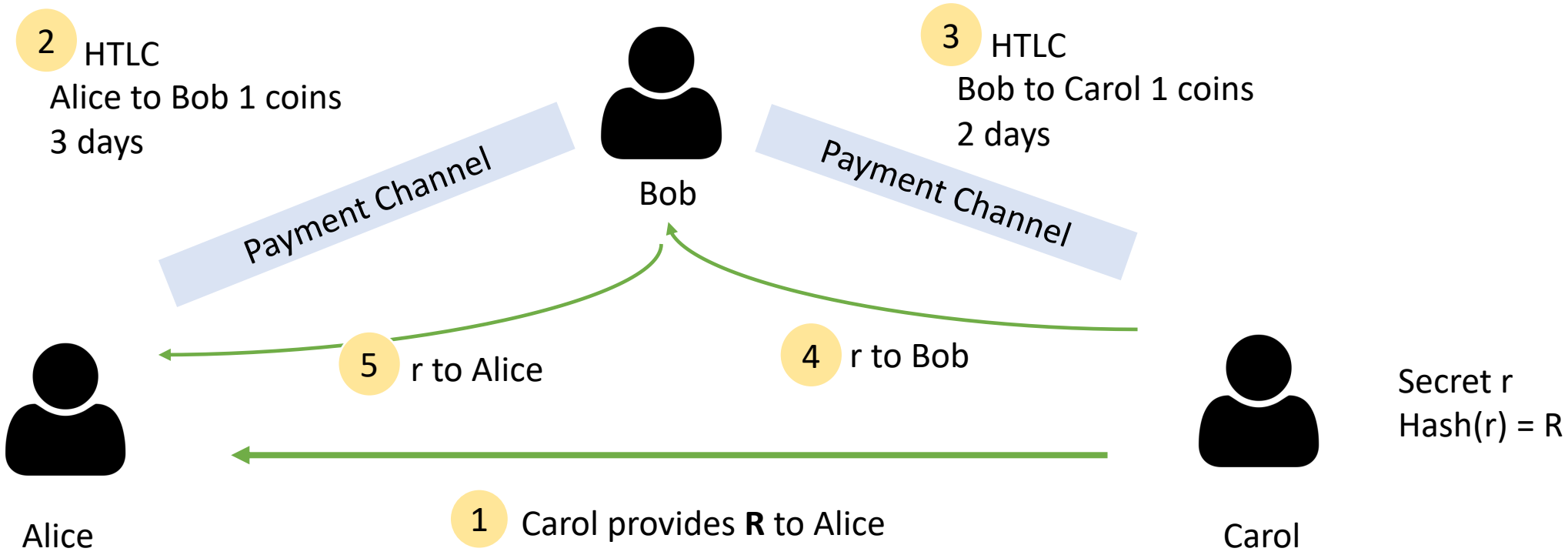
Payment Channel



Technical support: script languages, especially time-lock script.
However, some blockchains are scriptless…

Multi-hop Payment

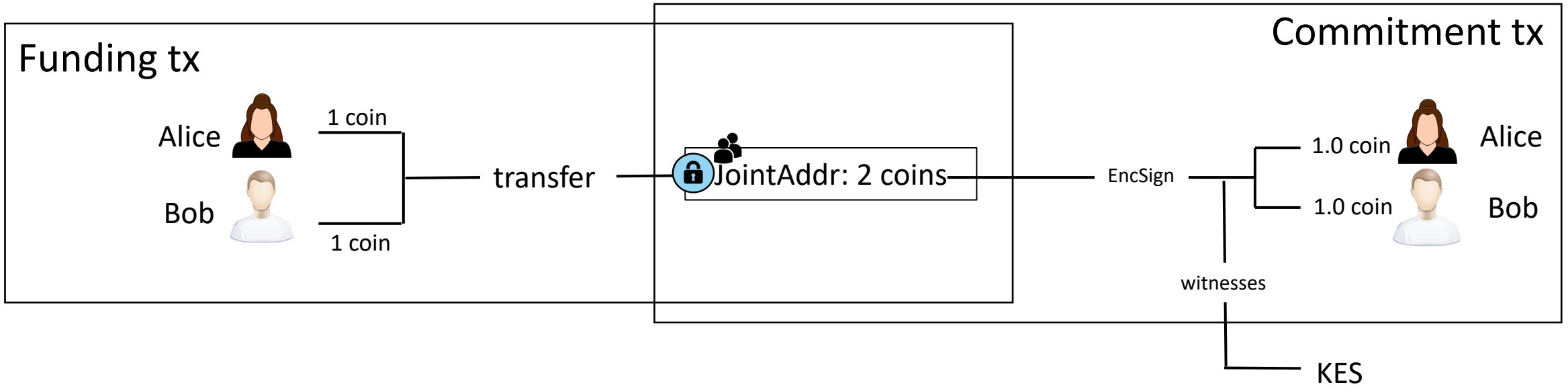
If step 4 failed, since Carol does not pay Bob in 2 days, Bob can close their channel to retrieve the locked coins.



MONASH University

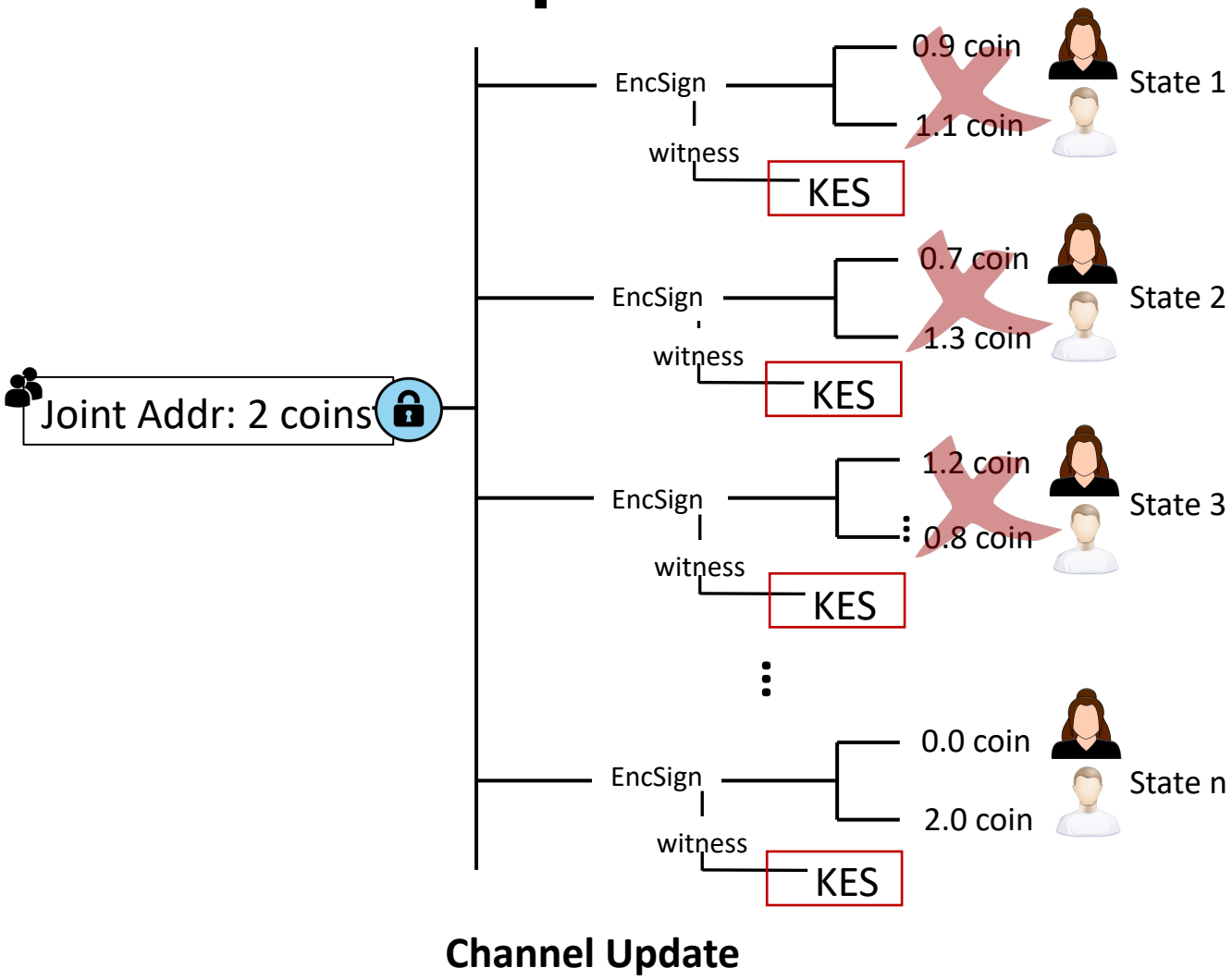
AuxChannel – a payment channel scheme for scripltess blockchain

AuxChannel - (AsiaCCS'22)



Channel Establishment

But it is not practical…

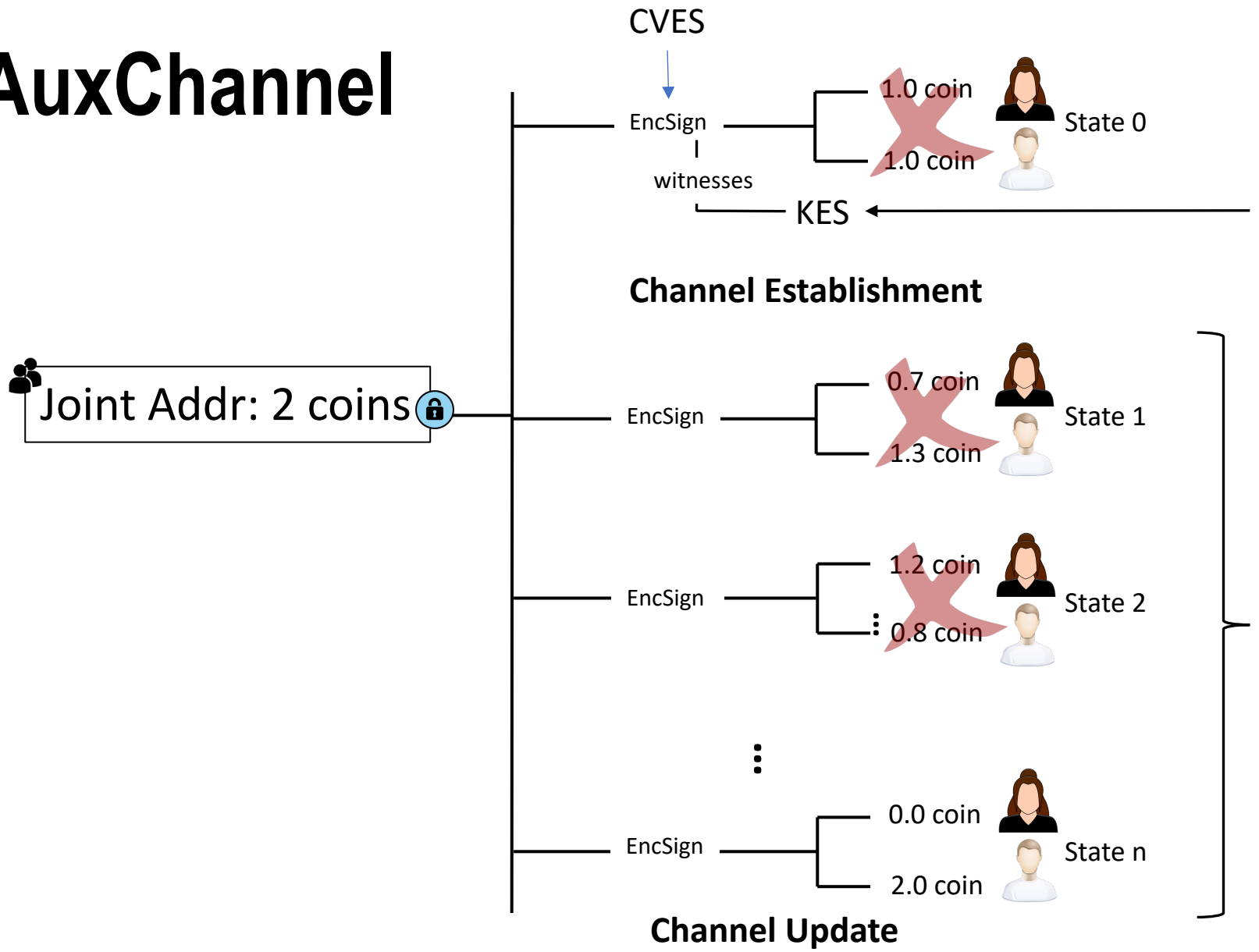


Channel Update

Normally, each transfer within the channel requires an interaction among Alice, Bob and KES, which is **not practical** in the real payment scenario.

Thus, we introduce **Consecutive Verifiably Encrypted Signature (CVES)**…

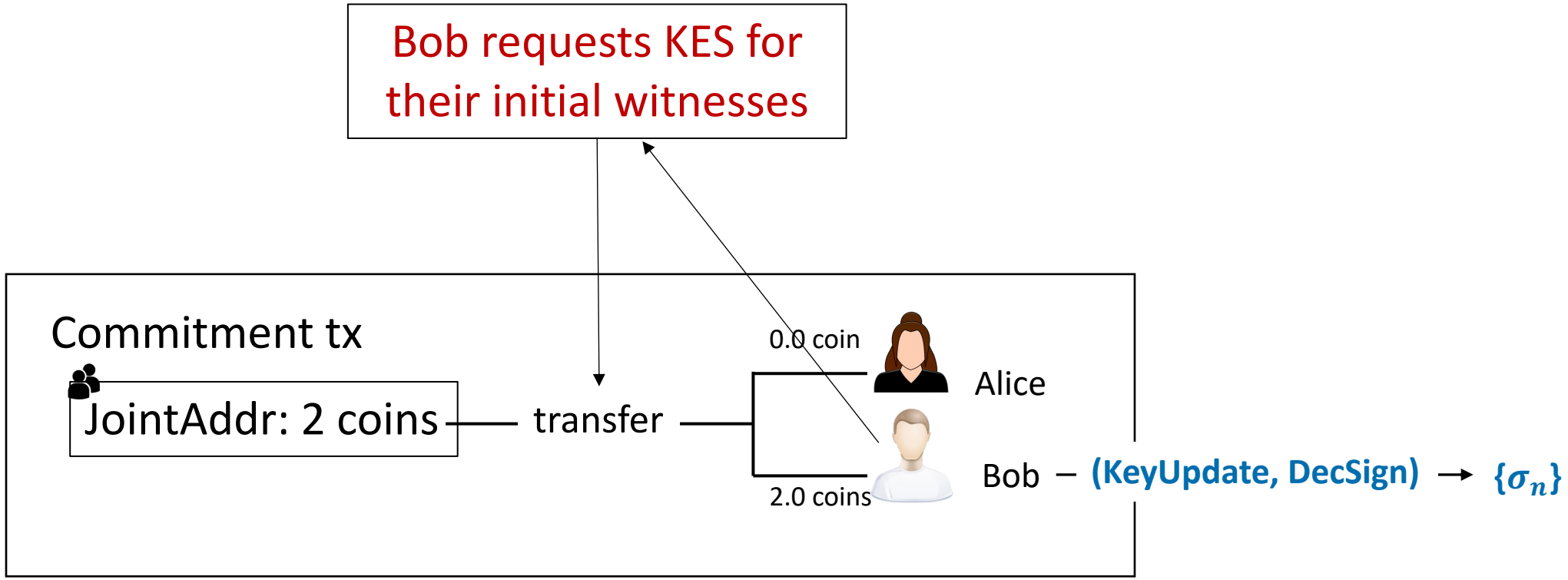
AuxChannel



Escrow the initial key only

No interaction needed with KES during the channel update phase

AuxChannel



Channel Closure

MONASH
University

MoNet – Payment Channel Network for Monero

Issues

- Due to the privacy features, additional data is attached to each transaction, significantly increasing the size of the blockchain.
    - At the time of this presentation, Monero blockchain size is around **95-100GB** and will continue to grow with wider adoption, **hurting usability**.

- Comparing to the throughput of visa (24,000 TPS), Monero also **needs to be scaled**.

- Payment channel network: recording most transactions off-chain.

Monero-compatible payment channels

Comparison among the Monero-compatible channels

	DLSAG Channel	PayMo Channel	Sleepy Channel	AuxChannel
Hard Fork	Yes	No	No	No
Uni- or Bi-	Uni-	Uni-	Bi-	Bi-
Fungibility	No	Yes	Yes	Yes
Life-time	Limited	Limited	Limited	Unlimited
Collateral	No	No	Yes	No

MoNet - ICDCS'22

- Verifiable Consecutive One-way Function (VCOF)
  - 2-Party Consecutive Linkable Ring Adaptor Signature (2P-CLRAS)

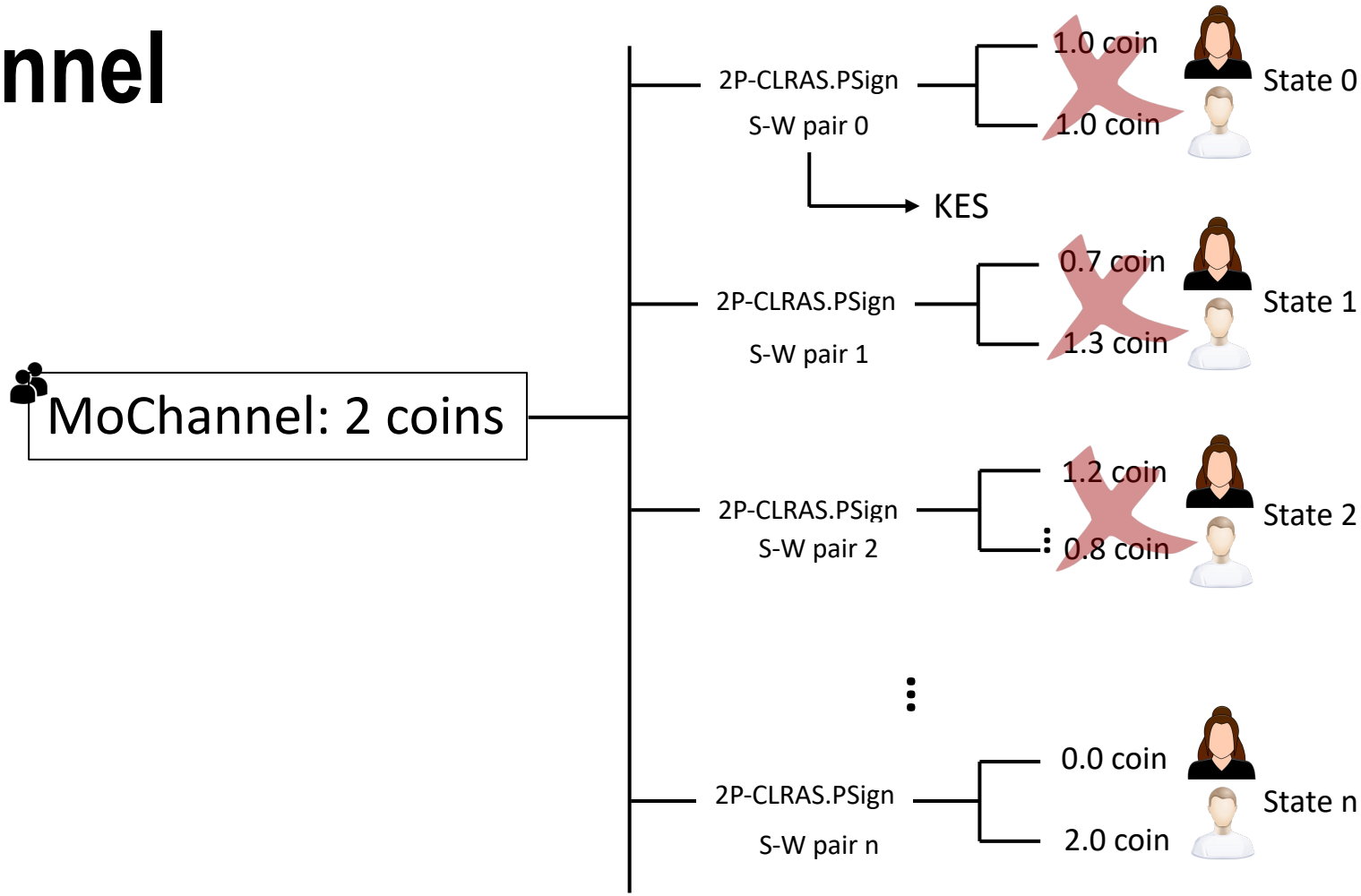
- MoChannel: enabling bi-directional payment channel for Monero by using 2P-CLRAS

- MoNet: making multi-hop payments building upon MoChannel
  - Preserving the privacy properties (fungibility and anonymity) of Monero ledger

- Security: MoNet is UC-secure and preserves Monero's privacy

MONASH University

MoChannel



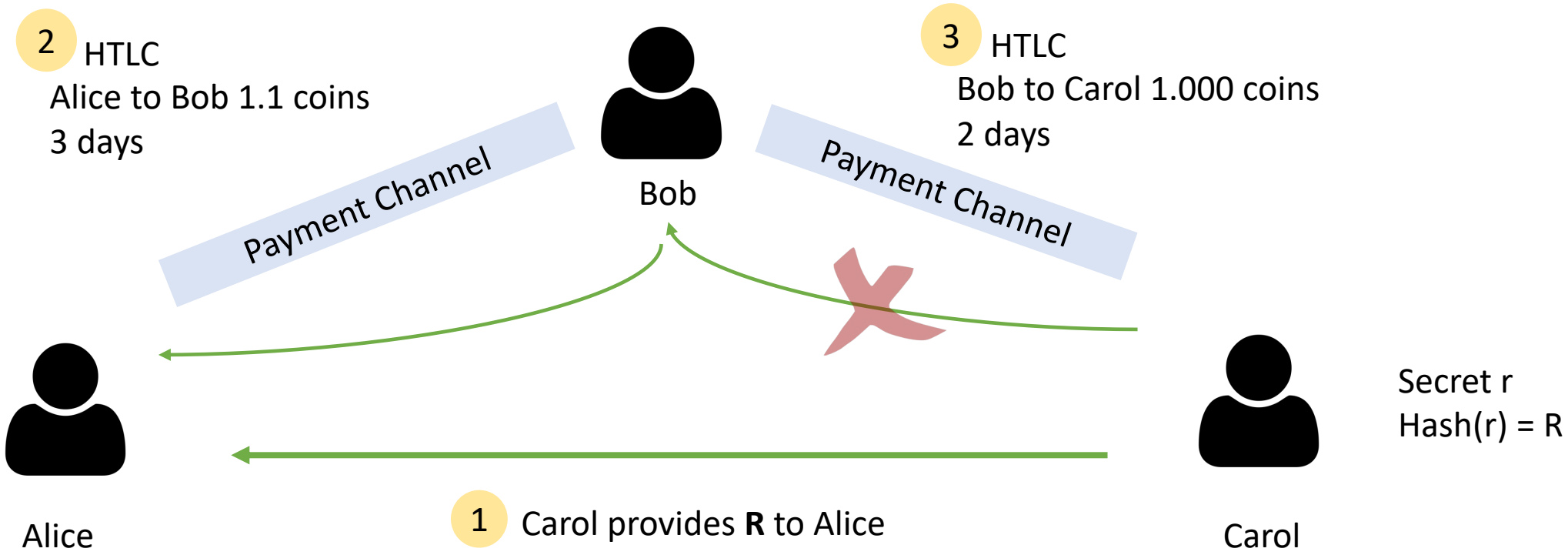
By employing **2-Party Consecutive Linkable Ring Adaptor Signatures (2P-CLRAS),**

we enable such a bi-directional payment channel for Monero.

MONASH University

MoNet

If step 4 failed, Bob can close their channel and retrieve the locked coins by requesting Carol's initial witness from KES.



MONASH University

Performance

We provide the proof-of-concept implementation **2P-CLRAS** in golang, and evaluate the performance of making off-chain transactions.

To process an off-chain transaction in a single MoChannel:

	Original MoChannel	**Optimized MoChannel**
Generate a payment	33.5 ms	3.5 ms
Verify a payment	333.4 ms	3.4 ms

After optimized : if MoNet can reaches the same scale of LN (80, 000 channels), the same throughput level of LN (the PCN for Bitcoin)

MONASH University

Q & A

Thank you!

MONASH University