PERUN: Virtual Payment Hubs over Cryptocurrencies

Stefan Dziembowski
Lisa Eckey
Sebastian Faust
Daniel Malinowski
Goal: Microtransactions

Problem: Blockchain transactions are slow and expensive

Alice

Send 😞 to Bob

Transaction Fees

Bob

Cheap Fast Offline Secure

Microtransactions
Smart Contracts

Guaranteed by the **underlying cryptocurrency**
PERUN in a Nutshell

New cryptographic protocol that allows microtransactions over cryptocurrencies

- 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
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: \( s_v = (x_A, x_B, v) \)

Alice

Bob

\[ s_0 = (c_A, c_B, \theta) \]
\[ s_1 = (c_A + 5, c_B - 5, 1) \]

1. Create
2. Update
3. Close

Cheap  Fast  Offline  Secure
(Ledger) Payment Channels

Channel Contract

$s_n$ is valid if

- $x_A + x_B = c_A + c_B$
- Approved by A and B

Select more recent state for payout

1. Create
2. Update
3. Close

$s_n = (x_A, x_B, n)$

$s_m = (x_A, x_B, m)$

Send $s_n$ to Bob

Unlock $x_A$

Send $s_m$ to Alice

Unlock $x_B$

Select more recent state for payout
Outline

- Motivation
- Ledger Payment Channels
- Virtual Payment Channels
- Security & Performance
- Summary & Outlook
Hashed Time Locked Contracts (HTLC)*

Idea: Route every transaction via intermediary

PERUN Virtual Channels

Alice — chan_{AB}

Bob — chan_{IA}

Ingrid — chan_{IB}
PERUN Virtual Channels

1. Create
2. Update
3. Close
PERUN Virtual Channels

1. Create
2. Update
3. Close
PERUN Virtual Channels

last state: vs\textsubscript{n} \text{Alice} \rightarrow \text{Bob}

last state: vs\textsubscript{m} \text{Alice} \rightarrow \text{Bob}

1. Create
2. Update
3. Close
PERUN Virtual Channels

Ingrid stays financially neutral

1. Create
2. Update
3. Close
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

Channel Opening
- on-chain
- off-chain/direct

Update
- off-chain/via Ingrid

Agreement
- on-chain
- 50 ct.

Disagreement
- on-chain
- 55 ct.

Closing

Ledger Channel
- on-chain
- 12 ct.

HTLC Network
- off-chain/via Ingrid
- Fee/Validity
- Fee/Payment
- 84 ct.

Virtual Channel
- off-chain/direct
- 84 ct.
Outline

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

@ CCS 2018
@ Eurocrypt 2019
Thank you for your attention!

For more information visit:

www.perun.network