Musketeer: Incentive-Compatible Rebalancing for Payment Channel Networks

Zeta Avarikioti, Stefan Schmid, Samarth Tiwari

TU Wien, TU Berlin, CWI

Presented by: Arash Pourdamghani

TU Berlin

PODC 2024

Technische Universität Berlin

TU WIEN

CWI

Research institute for mathematics & computer science in the Netherlands

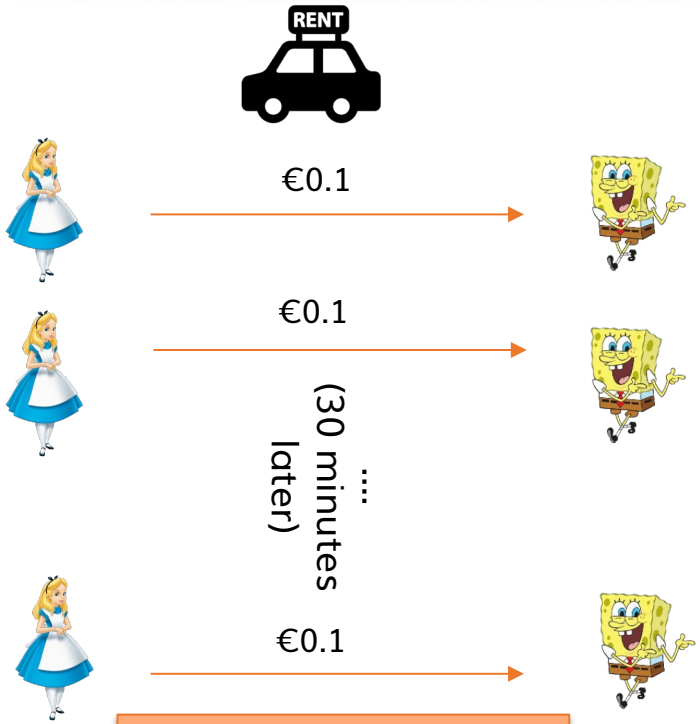
A Challenge in Blockchain: Scalability

7 tx/s

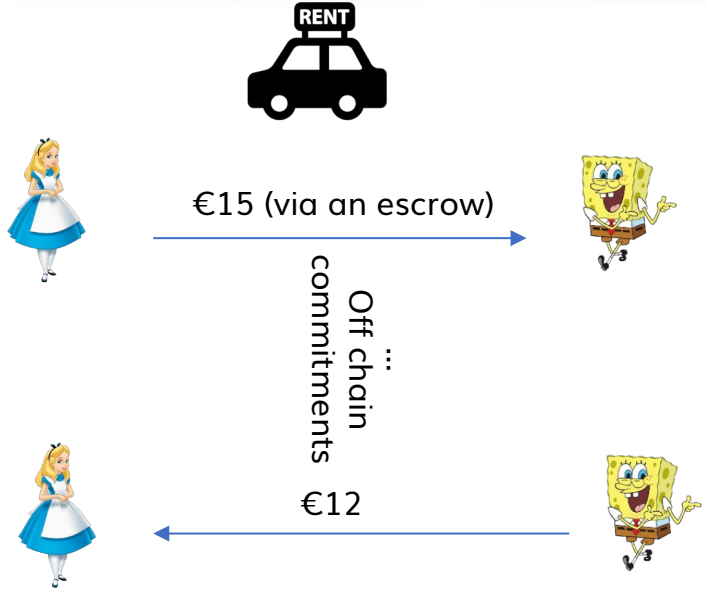
15 tx/s

65.000 tx/s

A Solution: Payment Channels

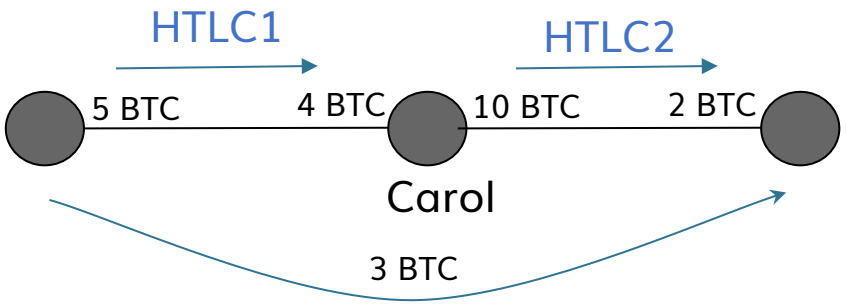


Traditional On-Chain Method



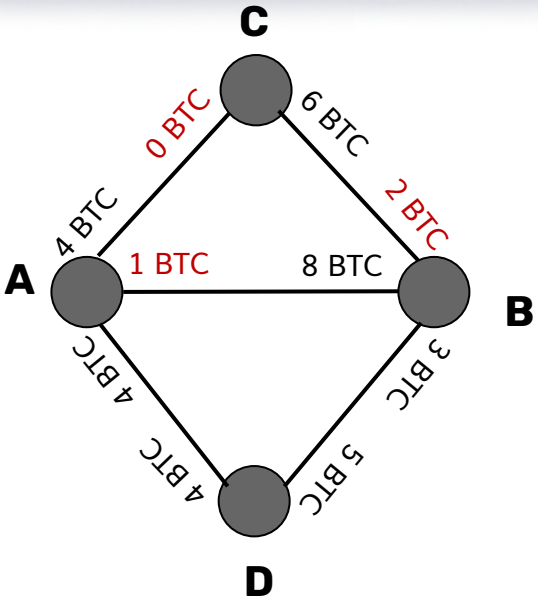
Payment Channels

Payment Channel Networks (PCNs)



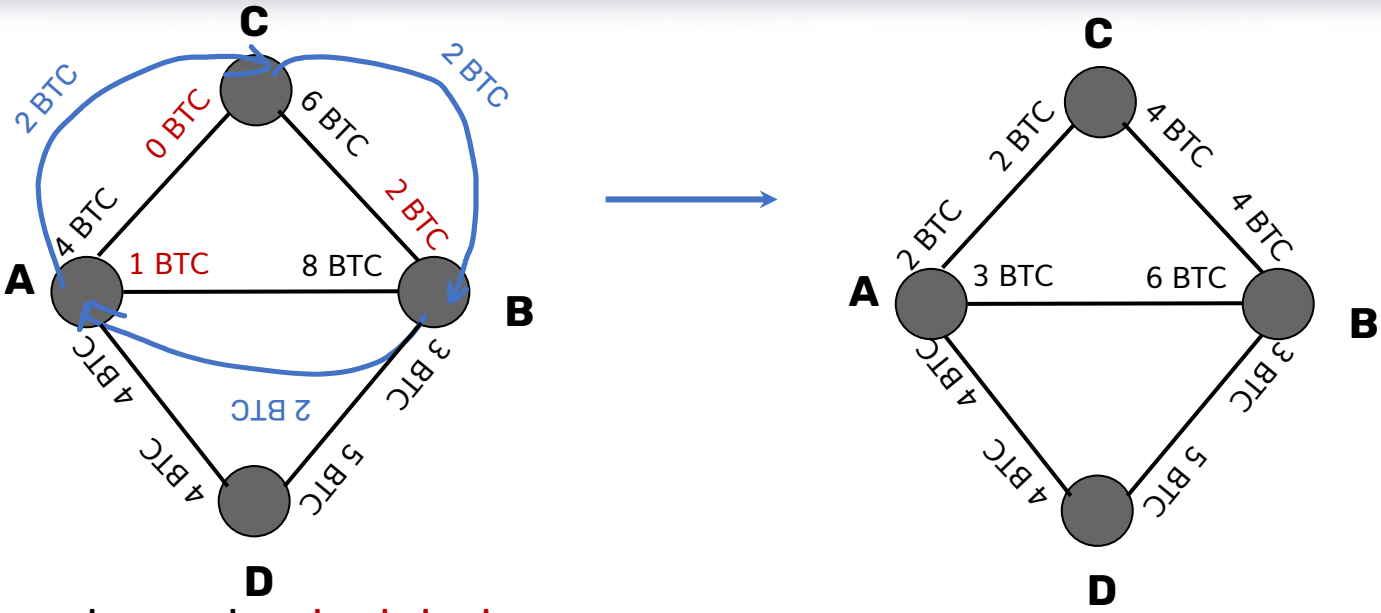
- Payments are possible along multiple channels
- Security through HTLCs
- Intermediaries ask for service fees

Rebalancing PCNs



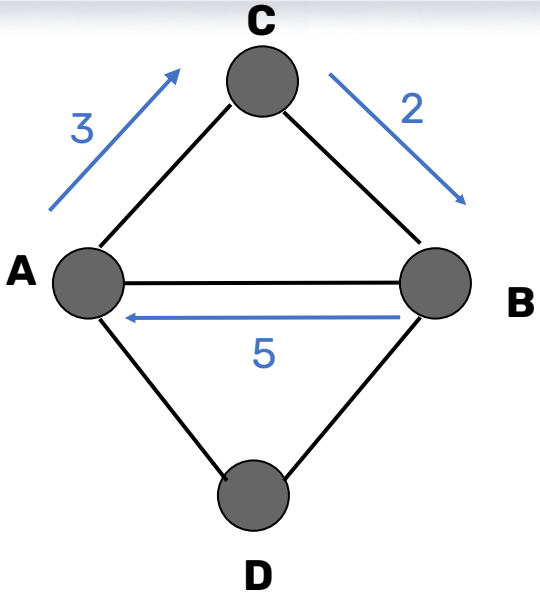
- Channels can be depleted
- Solving it either with on-chain top-up or

Rebalancing PCNs



- Channels can be depleted
- Solving it either with on-chain top-up or
- Off-chain top-ups using rebalancing

Rebalancing PCNs



- Users might have different rebalancing request!
- Obtain a directed (sub)graph with edge capacities:

Rebalancing = circulations = flows with zero net-flow through each vertex

State of The Art

- **Local peer-to-peer search for a cycle**
- **Revive** (CCS'17)**,** globally coordinated mechanism
- **Hide&Seek** (FC'22)**,** privacy-concerning mechanism

These approaches only include parties that wish to rebalance!

So, many channels that may route transactions for low fees are neglected: limited liquidity

Paper's Contribution

- **Incentivize all PCN users, to maximize liquidity and throughput**

- Users can participate as **buyers** (paying fees to rebalance) or **sellers** (charging fees to route transactions)

- Users submit their liquidity and bid for every one of their channels
  - **Liquidity:** coins they are willing to use for routing/rebalancing
  - **Bid:** how much fee they are willing to pay per coin for rebalancing the specific channel

Why Is It Technically Interesting?

- General desired properties - tailored to unique PCN characteristics

  Maximizing Social Welfare + Individual Rationality + Truthfulness

- A property tailored to unique PCN characteristics:

  Cyclic Budget Balance: for every individual rebalancing cycle zero-net flow

- **Impossible** to achieve all 4 properties (from double auction impossibility)

Musketeer Solutions

- **Variant 1**
  - Users know in advance max/min fees (posted-price auction)
  - Satisfies all, but it is a restricted setting
- **Variant 2**
  - VCG-type auction only for buyers
  - Satisfies all, but does not treat sellers as strategic agents
- **Variant 3**
  - First-price auction considering both buyers and sellers
  - Satisfies all, but truthfulness
- **Variant 4**
  - Double auction that **leverages time delays**
  - Satisfies all, but users incur some cost in terms of execution delay

Limitations & Future Work

- **Variable delay costs**
  - Consider distinct levels of utility loss from delays

- **Repeated games**
  - Can users benefit from the repeated nature of rebalancing by e.g. underbidding?

Check the preprint version:

Follow our group:

Send an email to Zeta: