Settling Payments Fast and Private:
Efficient Decentralized Routing for Path-Based Transactions
Limitations of Blockchains

Scalability

7 transactions/s

56,000 transactions/s
Payment Channels

Balance between A and B
Payment Channels

Balance between A and B

A sends Z

Lightning, Interledger, SilentWhispers
Settling Payments Fast and Private

Path-Based Transactions (PBTs)

S wants to send c=5 to R

$\begin{align*}
S & \xrightarrow{5} P \xleftarrow{2} S' \xrightarrow{6} P' \xrightarrow{8} R \\
S & \xrightarrow{5} S' \xrightarrow{5} P \xrightarrow{5} R \\
S & \xrightarrow{0} S' \xrightarrow{1} P \xrightarrow{13} R
\end{align*}$
Contributions

- Privacy goals
- Routing algorithm design
- Privacy evaluation
- Performance evaluation
Privacy Goals

Send ? from ? to ?
Privacy Goals

Send ? from ? to ?

- Value privacy

malicious

honest
Privacy Goals

Send ? from ? to ?

• Value privacy

• Sender/Receiver Privacy

Stefanie Roos
Settling Payments Fast and Private
SpeedyMurmurs: Setup

Payment Channel
SpeedyMurmurs: Setup

![Graph diagram with nodes and edges labeled Payment Channel and Spanning Tree]
SpeedyMurmurs: Setup

Settling Payments Fast and Private

Stefanie Roos
SpeedyMurmurs: Setup

Graph:

- Nodes: (1), (2), ()
- Edges:
  - Payment Channel: (1) to (2)
  - Spanning Tree: (1) to () to (2)

Stefanie Roos
Settling Payments Fast and Private
SpeedyMurmurs: Setup

---

**Tree distance**

\[ \text{dist}(u,v) = |u| + |v| - 2\text{cpl}(u,v) \]

---

**Common Prefix Length**
SpeedyMurmurs: Setup

Tree distance
\[ \text{dist}(u,v) = |u| + |v| - 2 \text{cpl}(u,v) \]

$t$ trees (number of paths)

Common Prefix Length
SpeedyMurmurs: Routing

\[ \sum c(i) = c \]

\( c(i) \): value sent using coordinates in i-th tree
**SpeedyMurmurs: Routing**

1. Select neighbor
   1) closer to receiver
   2) has at least balance $c(i)$

2. $S$
   $c(1)$
   $c(2)$
   $\ldots$
   $c(t)$

   $\sum c(i) = c$

   $c(i)$: value sent using coordinates in i-th tree

![Diagram]

- $c(1) = 5$
- $c(1) = 5$
- $8$
- $5$
- $3$
- $4$
- $(1,2)$
- $(1)$
- $(2)$
Privacy

- Value $c$ hidden from nodes not on paths
- Nodes on paths can estimate $c$

2 trees

Expected $c$: 10
Privacy Analysis

• Value $c$ hidden from nodes not on paths
• Nodes on paths can estimate $c$

5 2 landmarks

Expected $c$: 10

• Sender/Receiver Privacy: obfuscated coordinates (Roos et al., Infocom 2016)
Performance: Success Ratio

Real-world data set: Ripple
(~60,000 nodes, 300,000 transactions)

SW – SilentWhispers
SM – SpeedyMurmurs
FF – Ford-Fulkerson
Performance: Success Ratio

Real-world data set: Ripple
(~60,000 nodes, 300,000 transactions)

SW – SilentWhispers
SM – SpeedyMurmurs
FF – Ford-Fulkerson
Settling Payments Fast and Private

Stefanie Roos

Evaluation: Messages

SW – SilentWhispers
SM – SpeedyMurmurs
FF – Ford-Fulkerson
Evaluation: Messages

49,500

SW – SilentWhispers
SM – SpeedyMurmurs
FF – Ford-Fulkerson
Summary

- **SpeedyMurmurs**
  - Embedding-based routing
  - (Dynamic maintenance)
  - (Concurrency-aware routing)
- **Effective, efficient, scalable, privacy-preserving**
- **Applicable to Lightning, Interledger, SilentWhispers**
- **Data sets and simulation framework:**
  https://crysp.uwaterloo.ca/software/speedymurmurs/