SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks

Giulio Malavolta
Saarland University

Pedro Moreno-Sanchez
Purdue University

Aniket Kate
Purdue University

Matteo Maffei
TU Vienna

NDSS 2017
Yet Another Talk about Cryptocurrencies?

- TumbleBit and CoinShuffle++ are excellent ideas to provide privacy in Bitcoin.
Yet Another Talk about Cryptocurrencies?

✦ TumbleBit and CoinShuffle++ are excellent ideas to provide privacy in Bitcoin

✦ Bitcoin (as other permissionless cryptocurrencies) relies on a blockchain:
  ✦ High storage requirement (>100 GB)
  ✦ High power consumption for proof-of-work
Yet Another Talk about Cryptocurrencies?

✦ TumbleBit and CoinShuffle++ are excellent ideas to provide privacy in Bitcoin

✦ Bitcoin (as other permissionless cryptocurrencies) relies on a blockchain:
  ✦ High storage requirement (>100 GB)
  ✦ High power consumption for proof-of-work

Is it possible to have a decentralized payment system without a blockchain?
Credit (or IOU Settlement) Networks: Basics
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

Bob → Alice: pay $100

Alice → Bob: IOweYou $100
Transactions in the real world

Bob → Alice: pay $100
Bob ← Alice: IOweYou $100

A credit network representation

Bob → Alice: 100
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

Bob → Alice: pay $100
Bob ← Alice: IOweYou $100

During a hike with Alice & Bob

Dave → Carol: pay $10
Dave ← Carol: IOweYou $10

A credit network representation

Bob → Alice: 100
Bob ← Alice: 10

Carol → Dave: 10
Carol ← Dave: 10
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

Bob → Alice: pay $100
Bob ← Alice: IOweYou $100

During a hike with Alice & Bob
Dave → Carol: pay $10
Dave ← Carol: IOweYou $10

A credit network representation

Bob → Alice: 100
Bob ← Alice

Bob → Dave
Bob ← Dave

Dave → Carol
Dave ← Carol
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

Bob → pay $100 → Alice

Bob → IOweYou $100 → Alice

A credit network representation

Bob → 100 → Alice

Dave → pay $10 → Carol

Dave → IOweYou $10 → Carol

During a hike with Alice & Bob
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

During a hike with Alice & Bob

Bob → pay $100 → Alice

Bob → IOweYou $100 → Alice

Dave → pay $10 → Carol

Dave → IOweYou $10 → Carol

A credit network representation

Bob → 110 → Alice

Dave → 10 → Carol
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

Bob → pay $100 → Alice

Bob → IOweYou $100 → Alice

During a hike with Alice & Bob

Dave → pay $10 → Carol

Dave → IOweYou $10 → Carol

A credit network representation

Bob ← 110 → Alice

Bob ← 10 → Dave

Dave ← 10 → Carol

Carol ← 10 → Alice
Credit Network Examples

- Academic proposals:
  - Ostra: preventing e-mail spam [NSDI’08]
  - Bazaar: strengthening e-commerce [NSDI’11]
  - SumUp: Sybil-resilient content voting [NSDI’09]

- Industry deployments:
  - Ripple: A real-life online payment network
  - Stellar: Another real-life online payment network
Credit Network Examples

✦ Academic proposals:
  ✦ Ostra: preventing e-mail spam [NSDI’08]
  ✦ Bazaar: strengthening e-commerce [NSDI’11]
  ✦ SumUp: Sybil-resilient content voting [NSDI’09]

✦ Industry deployments:
  ✦ Ripple: A real-life online payment network
  ✦ Stellar: Another real-life online payment network
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network

AED 10 $60 CAD 100

€30 €45

Reise Bank

€70

RBS

CBW BANK

NBAD

RBC
Ripple Credit Network

AED 10 ➔ €30 ➔ Reise Bank

$60 ➔ €45 ➔ BTC 10 ➔ BTC 5

CAD 100 ➔ €30 ➔ Reise Bank

BTC 10 ➔ BTC 5

£70 ➔ CBW BANK ➔ CBW BANK

RBC ➔ CBW BANK ➔ CBW BANK

CBW BANK ➔ CBW BANK ➔ CBW BANK

RBS ➔ CBW BANK ➔ CBW BANK

RBC ➔ CBW BANK ➔ CBW BANK

RBS ➔ CBW BANK ➔ CBW BANK
Ripple Credit Network

Tx time  Worldwide, cross-currency tx  Integrity

AED 10  £ 30  CAD 100  XID 100

BTC 10  BTC 5

$ 60  € 45

£ 70

FMM 280

Ripple Credit Network
Ripple Credit Network

Tx time

- ~ 1 day

Worldwide, cross-currency tx

Integrity

- ~ 5 seconds
Ripple Credit Network

- **Reise Bank**: AED 10 → €30 → €45
- **CBW Bank**: CAD 100 → XIDO
- **RBC**: CAD 100 → XIDO 100
- **RBS**: £70
- **BTC 10**: BTC 10
- **BTC 5**: BTC 5
- **GDW 10**: GDW 10
- **FMM 280**: FMM 280

**Tx time**
- ~ 1 day
- ~ 5 seconds

**Worldwide, cross-currency tx**
- High fees
- Tiny fees

**Integrity**
Ripple Credit Network

- Worldwide, cross-currency tx
- Integrity
- High fees
- Bank only
- Tiny fees
- Public verifiability

Tx time:
- ~ 1 day
- ~ 5 seconds
Ripple can significantly improve cross-currency remittance and settlements.
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rnvctTPLKZqKS9f1fXpDkJ...</td>
<td>rMnV29maU6p5cAvmAECZmL...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBp5quSHbbfvtcKt1c54...</td>
<td>rKoaO7V583AKJZwELvVZEs...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9f5SmD4SyndmXa16L...</td>
<td>rBeToNoA4HnNBrX2n4BMC...</td>
<td>8.0693402789148/CCK/rBL...</td>
</tr>
<tr>
<td>rhD7M57bJMrzPNL4qBVqeg9...</td>
<td>r95pWKA1K5sf7EJ3wrqJ9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r4ZvQgV9Mja4tScCFBCnX...</td>
<td>rBeToNoA4HnNBrX2n4BMC...</td>
<td>8.08210580231/CCK/rBL...</td>
</tr>
<tr>
<td>rUnrL1p7xkuSBxyEjHEeop25...</td>
<td>r3H4rynDSSFMFMRWulJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rwUf6vzCe2wJxUeZHLG...</td>
<td>rBw/Itdz2Mh0ulK50JD3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpVzfsTUCX9CrLS5ZS2Z5W...</td>
<td>rDCgaaSBAYWfsxUYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rwvctTPLKZqKS9f1fXpdKq...</td>
<td>rMNvZ9maUwp5cAmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBPsquSHKbbfvcKt1c54...</td>
<td>rKoD7V83AKJ7ZewLxVZe...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r2B8q5fSSmD4SyaDra16B...</td>
<td>rBeToNo4A4WaBcRX2n4B...</td>
<td>8.0693402709148/CCK/rBL...</td>
</tr>
<tr>
<td>rhD79aJrzn9MNL40bVq9e2...</td>
<td>r95pWA1KSsSyjEJwrqJ9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rZwJGvV9Mja4t50cF8CnX...</td>
<td>rBeToNo4A4WaBcRX2n4B...</td>
<td>8.0821058828231/CCK/rBL...</td>
</tr>
<tr>
<td>ruDr17pY5kSflYqHeOzp5...</td>
<td>r3H4rynD5HFMKwUcDLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7VgzwCw2jxXxUE2HLG...</td>
<td>rBwqTdz2MhnuULKSOJ3xD...</td>
<td>160/XRP</td>
</tr>
<tr>
<td>rpV2fSTUJX9CrKBSS2ZSW...</td>
<td>rDCgaaSBAWYfsxUyhcK1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>

Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network

Pedro Moreno-Sanchez, Muhammad Bilal Zafar, Aniket Kate.

PETS ‘16
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rwvctTPLKZqKS9f1fXpDkQ...</td>
<td>rMnVZ9maUnp5cAvmqBECZL...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLS8pSquSHKbbfvcKtv1c5...</td>
<td>rKoO7tVL83AKJzewLxVZe...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r42BG9fSSm4SYanDra16B...</td>
<td>rBeToNo4AvHaN8RX2n4BNC...</td>
<td>8.0693402789148/CCK/rBL...</td>
</tr>
<tr>
<td>rhD759dB3r2MN4QbQe9...</td>
<td>r95pXKAIK5fS7EJwrqJ9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r4ZWJ6vV9Ja4tS0CF8Cnx...</td>
<td>rBeToNo4AvHaN8RX2n4BNC...</td>
<td>8.0821588228231/CCK/rBL...</td>
</tr>
<tr>
<td>rUnr1p7Xku5BxyAgHE0pZ5...</td>
<td>r3H4rynDShFMKMWJcadL...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7Ug2wTeZw3XUEeZH6...</td>
<td>rBwJdZz2MhnoULk5OJ3x...</td>
<td>188/XRP</td>
</tr>
<tr>
<td>rpWzfSTUX99CrKBSSZ5...</td>
<td>rDCgaaSBAWYfsxUyYhCkIn2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>

Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network

Pedro Moreno-Sanchez, Muhammad Bilal Zafar, Aniket Kate.

PETS ‘16

Current credit networks employ a global ledger
Our Contributions

- We question the need for a global ledger and global consensus.

![The Ripple Ledger](Image)

<table>
<thead>
<tr>
<th>Transaction Details</th>
<th>Credit Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Amount</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td></td>
</tr>
</tbody>
</table>

![Image]
Our Contributions

- We question the need for a global ledger and global consensus

- SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

Inspired by our work in NDSS’15
Our Contributions

- We question the need for a global ledger and global consensus

- SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

- SilentWhispers overcomes several challenges: existence of a path, credit on a path and integrity of transactions

Inspired by our work in NDSS’15
Our Contributions

- We question the need for a global ledger and global consensus

- SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

- SilentWhispers uses distributed landmark routing, secure multi-party computation and 2-step transactions

- Inspired by our work in NDSS’15

- SilentWhispers overcomes several challenges: existence of a path, credit on a path and integrity of transactions
Our Contributions

- We question the need for a global ledger and global consensus

- SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

- SilentWhispers uses distributed landmark routing, secure multi-party computation and 2-step transactions

- SilentWhispers is feasible in practice and offers interesting alternatives to current emerging payment systems

- SilentWhispers overcomes several challenges: existence of a path, credit on a path and integrity of transactions
SilentWhispers: A Decentralized Credit Network
Local Information suffices: Credit links of a user determine his credit in the network
Local Information suffices: Credit links of a user determine his credit in the network

In-flow = 450
Out-flow = 40
Net-flow = 410
SilentWhispers: A Decentralized Credit Network

- **Local Information suffices**: Credit links of a user determine his credit in the network.

  - In-flow = 450
  - Out-flow = 40
  - Net-flow = 410

- **Net-flow is what matters**: Net-flow of a user must not change without the user’s consent.

  - In-flow = 450
  - Out-flow = 40
  - Net-flow = 410
SilentWhispers: A Decentralized Credit Network

- **Local Information suffices**: Credit links of a user determine his credit in the network.

  ![Diagram](image)

  - In-flow = 450
  - Out-flow = 40
  - Net-flow = 410

- **Net-flow is what matters**: Net-flow of a user must not change without the user’s consent.

  ![Diagram](image)

  - In-flow = 450
  - Out-flow = 40
  - Net-flow = 410
SilentWhispers: A Decentralized Credit Network

✦ Local Information suffices: Credit links of a user determine his credit in the network

- CBW BANK → Bob (450)
- Bob → Charles (15)
- Charles → Alice (25)

In-flow = 450
Out-flow = 40
Net-flow = 410

✦ Net-flow is what matters: Net-flow of a user must not change without the user’s consent

- Charles → CBW BANK (5)
- CBW BANK → Charles (450)
- Bob → Charles (10)
- Charles → Alice (25)

In-flow = 450
Out-flow = 40
Net-flow = 410
SilentWhispers: A Decentralized Credit Network

✦ **Local Information suffices**: Credit links of a user determine his credit in the network

- CBW BANK $\rightarrow$ 450 $\rightarrow$ Bob $\rightarrow$ 15 $\rightarrow$ Charles
- In-flow = 450
- Out-flow = 40
- Net-flow = 410

✦ **Net-flow is what matters**: Net-flow of a user must not change without the user’s consent

- Charles $\rightarrow$ 5 $\rightarrow$ CBW BANK
- In-flow = 450
- Out-flow = 40
- Net-flow = 410

- CBW BANK $\rightarrow$ 445 $\rightarrow$ Bob $\rightarrow$ 10 $\rightarrow$ Charles
- In-flow = 450
- Out-flow = 40
- Net-flow = 410

- Bob $\rightarrow$ 25 $\rightarrow$ Alice

SilentWhispers: A Decentralized Credit Network

- **Local Information suffices**: Credit links of a user determine his credit in the network

  - CBW BANK → Bob (450)
  - Bob → Charles (15)
  - Charles → Alice (25)

  - In-flow = 450
  - Out-flow = 40
  - Net-flow = 410

- **Net-flow is what matters**: Net-flow of a user must not change without the user’s consent

  - Charles → CBW BANK (5)
  - CBW BANK → Charles (445)
  - Charles → Bob (10)
  - Bob → Alice (25)

  - In-flow = 450
  - Out-flow = 40
  - Net-flow = 410
Challenges

- Find paths between users
- Calculate credit available in the path
- Ensure integrity of transactions
- And more …
The routing challenge
Routing Challenge: Landmark Routing
Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
- Common problem in standard networks and ad-hoc networks
Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
- Common problem in standard networks and ad-hoc networks
- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
- Common problem in standard networks and ad-hoc networks

- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$

- Landmark routing [Tschusiya ’89]
  - Calculate subset of all paths
Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver

- Common problem in standard networks and ad-hoc networks

- The max-flow approach:
  - Not scalable enough: \(O(V^3)\) or \(O(V^2\log(E))\)

- Landmark routing [Tschusiy '89]
  - Calculate subset of all paths
Routing Challenge: Landmark Routing

✦ Determine credit path from sender to receiver

✦ Common problem in standard networks and ad-hoc networks

✦ The max-flow approach:
  ✦ Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$

✦ Landmark routing [Tschusiya '89]
  ✦ Calculate subset of all paths
Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
- Common problem in standard networks and ad-hoc networks

The max-flow approach:
- Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$

Landmark routing [Tschusiya ’89]
- Calculate subset of all paths
Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver

- Common problem in standard networks and ad-hoc networks

- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$

- Landmark routing [Tschusiy ‘89]
  - Calculate subset of all paths
  - Distributed BFS: Local information suffices
Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
- Common problem in standard networks and ad-hoc networks
- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- Landmark routing [Tschusiyä ’89]
  - Calculate subset of all paths
  - Distributed BFS: Local information suffices
Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
- Common problem in standard networks and ad-hoc networks
- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- Landmark routing [Tschusiy '89]
  - Calculate subset of all paths
  - Distributed BFS: Local information suffices
Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
- Common problem in standard networks and ad-hoc networks
- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- Landmark routing [Tschusiy a ’89]
  - Calculate subset of all paths
  - Distributed BFS: Local information suffices
  - Enough in practice$^{1,2}$
  - More efficient than max-flow$^{1,2}$

$^1$[Our work in NDSS ’15]
$^2$[Viswanath et al. EUROSYS ’12]
Calculation of credit available in a path
Credit in a Path: SMPC
Credit in a Path: SMPC
Credit in a Path: SMPC

[x]: Secret share of x
Credit in a Path: SMPC

[x]: Secret share of x

✦ Given [x] it is not possible to know x
Credit in a Path: SMPC

[x]: Secret share of x

✦ Given [x] it is not possible to know x
Credit in a Path: SMPC

[x]: Secret share of x

✦ Given [x] it is not possible to know x
Credit in a Path: SMPC

[x]: Secret share of x

Given [x] it is not possible to know x
Credit in a Path: SMPC

[x]: Secret share of x

✦ Given [x] it is not possible to know x
Credit in a Path: SMPC

[x]: Secret share of x

Given [x] it is not possible to know x
Credit in a Path: SMPC

[latex]x[/latex]: Secret share of $x$

- Given [latex]x[/latex] it is not possible to know $x$
- Given “enough” copies of [latex]x[/latex] one can reconstruct $x$
Integrity of the transactions
Transaction Integrity and Dispute Resolution
Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
Transaction Integrity and Dispute Resolution

✧ 2-step transaction: on hold and settle
✧ Example: 

```
      5

         15

              20
```

```
Transaction Integrity and Dispute Resolution

✧ 2-step transaction: on hold and settle
✧ Example:

![Diagram showing a 2-step transaction process with amounts 5, 10, 15, and 20]
Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example:
2-step transaction: on hold and settle

Example:
Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example:
Transaction Integrity and Dispute Resolution

✧ 2-step transaction: on hold and settle
✧ Example:

![Diagram of transaction process](image)

Incentive

(5) Ok, received!
Transaction Integrity and Dispute Resolution

✧ 2-step transaction: **on hold** and **settle**
✧ Example:

![Diagram showing a transaction with incentive and two steps: on hold and settle.](image-url)

Incentive

Ok, received!
Transaction Integrity and Dispute Resolution

✧ 2-step transaction: on hold and settle
✧ Example:

[Integrity]
✧ All landmarks cannot make the user lose credit
Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle

- Example:  
  ![Diagram](image)

- Integrity:
  - All landmarks cannot make the user lose credit
Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle

- Example:

  ![Diagram showing a transaction with two users and an incentive]

No! our credit is 15!

Integrity:
- All landmarks cannot make the user lose credit

Accountability:
- In case of dispute, users must prove the link value
- Local logs suffice to determine the valid current value
- The disputed value is bounded
Evaluation
Evaluation and Discussion
Evaluation and Discussion

✧ C++ prototype implementation
  ✧ Secret Sharing-based MPC library: https://github.com/Zayat/MPC-Shared
Evaluation and Discussion

- C++ prototype implementation
  - Secret Sharing-based MPC library: https://github.com/Zayat/MPC-Shared

- Setup using Ripple transactions:
  - Maximum path length: 10 links
  - Maximum number of paths: 7 landmarks (Ripple Gateways)
Evaluation and Discussion

- C++ prototype implementation
  - Secret Sharing-based MPC library: https://github.com/Zayat/MPC-Shared

- Setup using Ripple transactions:
  - Maximum path length: 10 links
  - Maximum number of paths: 7 landmarks (Ripple Gateways)

- Computing available credit on a path in ~1.3 seconds
  - Different paths in parallel
Evaluation and Discussion

✧ C++ prototype implementation
  ✧ Secret Sharing-based MPC library: https://github.com/Zayat/MPC-Shared

✧ Setup using Ripple transactions:
  ✧ Maximum path length: 10 links
  ✧ Maximum number of paths: 7 landmarks (Ripple Gateways)

✧ Computing available credit on a path in ~1.3 seconds
  ✧ Different paths in parallel

Feasible to run in practice current Ripple transactions
Evaluation and Discussion

✧ C++ prototype implementation
  ✧ Secret Sharing-based MPC library: https://github.com/Zayat/MPC-Shared

✧ Setup using Ripple transactions:
  ✧ Maximum path length: 10 links
  ✧ Maximum number of paths: 7 landmarks (Ripple Gateways)

✧ Computing available credit on a path in ~1.3 seconds
  ✧ Different paths in parallel

Feasible to run in practice current Ripple transactions

✧ SilentWhispers has attracted attention from industry:
  ✧ KOINA: https://koina.cc/
The Landscape of Emerging Payment Systems
## The Landscape of Emerging Payment Systems

<table>
<thead>
<tr>
<th>Transfer of funds</th>
<th>Cryptocurrencies</th>
<th>Ripple</th>
<th>SilentWhispers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Direct transactions between any two wallets</td>
<td>Transactions only via a path with enough credit</td>
<td></td>
</tr>
</tbody>
</table>
## The Landscape of Emerging Payment Systems

<table>
<thead>
<tr>
<th></th>
<th>Cryptocurrencies</th>
<th>Ripple</th>
<th>SilentWhispers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transfer of funds</strong></td>
<td>Direct transactions between any two wallets</td>
<td>Transactions only via a path with enough credit</td>
<td></td>
</tr>
<tr>
<td><strong>Transaction flexibility</strong></td>
<td>Fixed currency agreed between sender and receiver</td>
<td>Support for cross-currency transactions</td>
<td></td>
</tr>
</tbody>
</table>
# The Landscape of Emerging Payment Systems

<table>
<thead>
<tr>
<th></th>
<th>Cryptocurrencies</th>
<th>Ripple</th>
<th>SilentWhispers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transfer of funds</strong></td>
<td>Direct transactions between any two wallets</td>
<td>Transactions only via a path with enough credit</td>
<td></td>
</tr>
<tr>
<td><strong>Transaction flexibility</strong></td>
<td>Fixed currency agreed between sender and receiver</td>
<td>Support for cross-currency transactions</td>
<td></td>
</tr>
<tr>
<td><strong>Transaction verification</strong></td>
<td></td>
<td>Globally verified</td>
<td>Locally verified by users in the path</td>
</tr>
</tbody>
</table>
Take Home Message
**Take Home Message**

✧ **A credit network does not require a global ledger or global consensus**

**SilentWhispers: A Decentralized Credit Network**

- **Local Information suffices:** Credit links of a user determine his credit in the network.
  - **In-flow = 450**
  - **Out-flow = 40**
  - **Net-flow = 410**

- **Net-flow is what matters:** Net-flow of a user must not change without the user’s consent.
  - **In-flow = 445**
  - **Out-flow = 35**
  - **Net-flow = 410**
A credit network does not require a global ledger or global consensus

SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges

- **Local Information suffices:** Credit links of a user determine his credit in the network.

- **Net-flow is what matters:** Net-flow of a user must not change without the user’s consent.

**Challenges**

- Find paths between users?
- Credit available in the path?
- Integrity of transactions?
- And more...
Take Home Message

✧ A credit network does not require a global ledger or global consensus

✧ SilentWhispers is feasible in practice and it has attracted attention from industry

SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges
Take Home Message

✦ A credit network does not require a global ledger or global consensus

✦ SilentWhispers is feasible in practice and it has attracted attention from industry

✦ SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges

✦ SilentWhispers is an interesting alternative in the landscape of emerging payment systems

**SilentWhispers: A Decentralized Credit Network**

- Local Information suffices: Credit links of a user determine his credit in the network.
- Net-flow is what matters: Net-flow of a user must not change without the user’s consent.

**Evaluation**

- C++ prototype implementation
- MPC-Shared library: https://github.com/Zayat/MPC-Shared
- Setup using Ripple transactions:
  - Maximum path length: 10 links
  - Maximum number of paths: 7 landmarks (Ripple Gateways)
- Computing available credit on a path in ~1.3 seconds
- Different paths in parallel

**Feasible to run in practice current Ripple transactions**

**SilentWhispers has attracted the attention from industry:**

KOINA: A credit network with market-specific currencies
https://koina.cc/

**The Landscape of Emerging Payment Systems**

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Cryptocurrencies</th>
<th>Ripple</th>
<th>SilentWhispers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find paths between users?</td>
<td>Direct transactions between any two wallets</td>
<td>Transactions only via a path with enough credit</td>
<td></td>
</tr>
<tr>
<td>Credit available in the path?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity of transactions?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>And more…</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A credit network does not require a global ledger or global consensus

SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges

SilentWhispers is feasible in practice and it has attracted attention from industry

SilentWhispers is an interesting alternative in the landscape of emerging payment systems

The Landscape of Emerging Payment Systems

<table>
<thead>
<tr>
<th>Cryptocurrencies</th>
<th>Ripple</th>
<th>SilentWhispers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer of funds</td>
<td>Direct transactions between any two wallets</td>
<td>Transactions only via a path with enough credit</td>
</tr>
<tr>
<td>Transaction flexibility</td>
<td>Fixed currency agreed between sender and receiver</td>
<td>Support for cross-currency transactions</td>
</tr>
<tr>
<td>Transaction verification</td>
<td>Globally verified</td>
<td>Locally verified by users in the path</td>
</tr>
</tbody>
</table>

Thanks! @pedrorechez