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

✧ Bitcoin (as any other cryptocurrency) 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 any other cryptocurrency) 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?
Transactions in the real world

Bob \rightarrow Alice: pay $100

Bob \rightarrow Alice: IOweYou $100
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

Bob → Alice

Bob

<table>
<thead>
<tr>
<th>pay $100</th>
</tr>
</thead>
</table>

IOweYou $100

Alice

A credit network representation

Bob

100

Alice

Bob
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

During a hike with Alice & Bob

A credit network representation
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 ➔ 100 ➔ Alice

Bob ➔ 100 ➔ Dave ➔ 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  ➔  100  ➔  Alice

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

Transactions in the real world

Bob

Bob IOweYou $100

Alice

Bob pay $100

Alice

During a hike with Alice & Bob

Dave

Dave IOweYou $10

Carol

Dave pay $10

Carol

A credit network representation

Bob

Bob 110

Alice

Dave

Dave 10

Carol

Carol
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

Bob → pay $100 → Alice

IOweYou $100 → Bob

During a hike with Alice & Bob

Dave → pay $10 → Carol

IOweYou $10 → Dave

A credit network representation

Bob → 110 → Alice

10 → Dave → 10 → Carol
Credit Network Examples
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

AED 10 ➔ £30
$60 ➔ £45
CAD 100 ➔ £70
Ripple Credit Network

- AED 10
- £30
- £45
- BTC 10
- BTC 5
- £70

- $60
- CAD 100
- Ripple Credit Network
- Reise Bank
- CBW Bank
- RBC
- RBS
Ripple Credit Network

- AED 10 ➔ €30
- CAD 100 ➔ $60
- XID 100 ➔ £70
- BTC 10 ➔ ¥100
- BTC 5 ➔ ¥50
- GDW 10 ➔ ¥100
- FMM 280 ➔ ¥10
Ripple Credit Network

Tx time
Worldwide, inter-currency tx
Integrity
Ripple Credit Network

Tx time
~ 1 day

Worldwide, inter-currency tx
~ 5 seconds

Integrity
Ripple Credit Network

- AED 10
- €30
- $60
- X7ZZ 40
- CAD 100
- XID 100
- BTC 10
- BTC 5
- £70
- CBCB 100
- XID 100
- FMM 280

Tx time
- ~ 1 day
- ~ 5 seconds

Worldwide, inter-currency tx
- Integrity
  - High fees
  - Tiny fees
Ripple Credit Network

- AED 10
- CAD 100
- $60
- €30
- €45
- BTC 10
- BTC 5
- XID 100
- XID 40
- XYZ 40
- FMM 280
- ~ 1 day
- Worldwide, inter-currency tx
- Integrity
- High fees
- Bank only
- ~ 5 seconds
- Tiny fees
- Public verifiability
Ripple can significantly improve cross-currency remittance and settlements.

- **Tx time**: ~1 day
- **Worldwide availability**: Yes
- **Integrity**: Bank only
- **Public verifiability**: Yes
- **Tiny fees**: Yes
- **High fees**: No

Ripple Credit Network

- **AED 10**: CBW BANK
- **CAD 100**: RBC
- **Euros**: Reise Bank
- **BTC 10**: Ripple
- **XID 100**: Ripple
- **FMM 280**: Ripple

**Key Features**

- **~5 seconds**
- **High fees**
- **Tiny fees**
- **Public verifiability**
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>rMnVZ9maUmpScAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBpSquSHKbbfvcKt1c54...</td>
<td>rKoD7VL83AKJZewLxVZeS...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9f55mD4YnnDra16B...</td>
<td>rBeToNo4AwHaNbcRX2n4BNC...</td>
<td>0.0693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rh759dbJMrzMN4QblvOe9...</td>
<td>r95pWA1K55fy7E7Wbj39b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42Wj6vV9MJa41t5QcFBCXn...</td>
<td>rBeToNo4AwhNbcRX2n4BNC...</td>
<td>0.08210580828231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAgHEopZ5...</td>
<td>r3n4ryn0SHFMKcWuJCadL5Y...</td>
<td>1129.916679154465/EUR...</td>
</tr>
<tr>
<td>rw7ufGvzCeZxjXxxUEeZH1G...</td>
<td>rBwGtddzMHnouLk50DJ3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpVzfSTUJ9XRKBSS2Z5W...</td>
<td>rDCgaaSBAWYFsxUXYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

Credit Graph

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 use a global ledger

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

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

PETS ‘16
Our Contributions
Our Contributions

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

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

❖ SilentWhispers: Decentralized credit network with security and privacy guarantees

Privacy Preserving Payments in Credit Networks
Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei and Kim Pecina
[NDSS ’15]

In this work, security and privacy properties defined in the UC framework
Our Contributions

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

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

We question the need for a global ledger and global consensus

SilentWhispers: Decentralized credit network with security and privacy guarantees

Privacy Preserving Payments in Credit Networks
Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei and Kim Pecina
[NDSS ’15]

In this work, security and privacy properties defined in the UC framework
Our Contributions

- We question the need for a global ledger and global consensus
- SilentWhispers overcomes several challenges: existence of a path, credit on a path and integrity of transactions

SilentWhispers: Decentralized credit network with security and privacy guarantees

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

Privacy Preserving Payments in Credit Networks
Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei and Kim Pecina
[NDSS ’15]

In this work, security and privacy properties defined in the UC framework
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.
  
  ![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.
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
SilentWhispers: A Decentralized Credit Network

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

\[
\begin{align*}
\text{In-flow} &= 450 \\
\text{Out-flow} &= 40 \\
\text{Net-flow} &= 410
\end{align*}
\]

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

\[
\begin{align*}
\text{In-flow} &= 450 \\
\text{Out-flow} &= 40 \\
\text{Net-flow} &= 410
\end{align*}
\]
SilentWhispers: A Decentralized Credit Network

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

- **CBW BANK**→**Bob**  
  In-flow = 450  
  Out-flow = 40  
  Net-flow = 410

- **Bob**→**Charles**  
  In-flow = 15  
  Out-flow = 25

- **Charles**→**Alice**  
  In-flow = 25  
  Out-flow = 10

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

- **Charles**→**CBW BANK**  
  In-flow = 5  
  Net-flow = 450

- **Bob**→**Charles**  
  In-flow = 445  
  Net-flow = 410

- **Charles**→**Alice**  
  In-flow = 10  
  Out-flow = 25  
  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
Challenges

- Find paths between users?
- Credit available in the path?
- 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 [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 [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 [Tschusiyaka ’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
  - Enough in practice\(^1,2\)
  - More efficient than max-flow\(^1,2\)

\(^1\)[Moreno-Sanchez et al. 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
Given [x] it is not possible to know x

Given “enough” copies of [x] one can reconstruct x
Given $[x]$ it is not possible to know $x$

- Given “enough” copies of $[x]$ one can reconstruct $x$
- Landmarks cannot force credit losses to honest users
Integrity of the transactions
Transaction Integrity: 2-Step Transactions
Transaction Integrity: 2-Step Transactions

- 2-step transaction: on hold and settle
- Example:
Transaction Integrity: 2-Step Transactions

✧ 2-step transaction: on hold and settle
✧ Example:
Transaction Integrity: 2-Step Transactions

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

```
  5
→
  5

(5) (5)

10
15

25
20

(5)
```
Transaction Integrity: 2-Step Transactions

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

\[
\begin{align*}
\text{Person 1} & \quad 5 \\
\text{Person 2} & \quad \rightarrow \\
\text{House} & \quad \text{(5)} & \quad \text{(5)} \\
\text{Person 1} & \quad \leftarrow 15 \\
\text{Person 2} & \quad 20 \rightarrow 25 \\
\text{Ok, received!}
\end{align*}
\]
Transaction Integrity: 2-Step Transactions

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

![Diagram showing a 2-step transaction process]

Ok, received!
Transaction Integrity: 2-Step Transactions

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

Incentive

Ok, received!
Transaction Integrity: 2-Step Transactions

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

✧ Example:

![Diagram]

10 25

Ok, received!

Incentive
Transaction Integrity: 2-Step Transactions

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

```
15
25
10
```

No! our credit is 15!

Incentive

5

Ok, received!
Transaction Integrity: 2-Step Transactions

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

  ![Diagram]

  - Time 1: Init value 15
  - Time 2: Value 25

  No! our credit is 15!

  Ok, received!
Transaction Integrity: 2-Step Transactions

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

![Diagram showing a 2-step transaction process with a transaction initiated at time 1, held for 5 units, then settled at time 2 with a final value of 25 units.]

- time₁: Init value 15
  - time₂: Hold 5 for tx

- time₁: Init value 15
  - time₂: Hold 5 for tx

No! our credit is 15!

Ok, received!
Transaction Integrity: 2-Step Transactions

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

  ![Diagram showing 2-step transaction process]

  time₁: Init value 15
  time₂: Hold 5 for tx
  time₃: Confirmation tx

No! our credit is 15!

Ok, received!
Transaction Integrity: 2-Step Transactions

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

  ![Diagram]

  - time₁: Init value 15
  - time₂: Hold 5 for tx
  - time₃: Confirmation tx

Wrong

Right
Transaction Integrity: 2-Step Transactions

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

No! our credit is 15!

- In case of dispute, users must prove the link values
- Reputation of users is at stake
Evaluation
Evaluation
Evaluation

- C++ prototype implementation
  - MPC-Shared library: https://github.com/Zayat/MPC-Shared
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)
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
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
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/
(Crypto)currencies vs SilentWhispers
### (Crypto)currencies vs SilentWhispers

<table>
<thead>
<tr>
<th>Transfer of funds:</th>
<th>(Crypto)Currencies</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>
</tr>
<tr>
<td></td>
<td>(Crypto)Currencies</td>
<td>SilentWhispers</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<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>
</tr>
<tr>
<td><strong>Transaction flexibility</strong></td>
<td>Fixed currency agreed between sender and receiver</td>
<td>Support for cross-currency transactions</td>
</tr>
</tbody>
</table>
## (Crypto)currencies vs SilentWhispers

<table>
<thead>
<tr>
<th></th>
<th>(Crypto)Currencies</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>
</tr>
<tr>
<td><strong>Transaction flexibility</strong></td>
<td>Fixed currency agreed between sender and receiver</td>
<td>Support for cross-currency transactions</td>
</tr>
<tr>
<td><strong>Transaction verification</strong></td>
<td>Globally verified</td>
<td>Locally verified by users in the path</td>
</tr>
</tbody>
</table>
## (Crypto)currencies vs SilentWhispers

<table>
<thead>
<tr>
<th></th>
<th><strong>(Crypto)Currencies</strong></th>
<th><strong>SilentWhispers</strong></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>
</tr>
<tr>
<td><strong>Transaction flexibility</strong></td>
<td>Fixed currency agreed between sender and receiver</td>
<td>Support for cross-currency transactions</td>
</tr>
<tr>
<td><strong>Transaction verification</strong></td>
<td><strong>Globally</strong> verified</td>
<td><strong>Locally</strong> verified by users in the path</td>
</tr>
<tr>
<td><strong>Scalability:</strong></td>
<td>Limited transaction rate (&lt; 100 tps)</td>
<td>Highly scalable</td>
</tr>
</tbody>
</table>
Take Home Message
Take Home Message

- A credit network does not require a ledger or global consensus
**Take Home Message**

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

- **SilentWhispers**: A **decentralized** credit network that addresses several challenges.
Take Home Message

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

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

✦ SilentWhispers: A decentralized credit network that addresses several challenges
Take Home Message

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

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

✦ SilentWhispers: A decentralized credit network that addresses several challenges

✦ SilentWhispers greatly differs from cryptocurrencies currently available
A credit network does not require a ledger or global consensus

SilentWhispers: A decentralized credit network that addresses several challenges

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

SilentWhispers greatly differs from cryptocurrencies currently available

Thank you!

@pedrorechez