Whispers: A Distributed Architecture for Enforcing Privacy in Credit Networks

Aniket Kate
Purdue University

Matteo Maffei
CISPA, Saarland University

Giulio Malavolta
CISPA, Saarland University

Pedro Moreno-Sanchez
Purdue University

HotPETS 2016
22 July 2016
Credit Networks 101

Real World

Credit Network
Can you take care of Chloe?
Credit Networks 101

Real World

Can you take care of Chloe?

Credit Network

I owe you 20 CAT
Can you take care of Chloe?

I owe you 20 CAT
Can you take care of Chloe?

I owe you 20 CAT

Credit Networks 101
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network

- CBW BANK
  - $60
  - $100

- $100
  - €30
  - €45

- B10

- B5

- Santander
  - £70

- fidor BANK

- Ripple Credit Network

- cross river bank
Ripple Credit Network

- CBW BANK
- CAT 40
- PIG 100
- COW 280
- Santander
- B 10
- B 5
- $ 60
- $ 100
- $ 100
- $ 70
- £ 70

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

- **Tx time**: ~1 day
- **Worldwide, inter-currency tx**: ~5 seconds
- **Integrity**
Ripple Credit Network

Tx time

~ 1 day

Worldwide, inter-currency tx

~ 5 seconds

Integrity

High fees

Tiny fees
Ripple Credit Network

- CBW Bank
- cross river bank
- fidor Bank
- Santander
- ripple

Tx time:
- ~ 1 day
- ~ 5 seconds

Worldwide, inter-currency tx:
- High fees
- Tiny fees

Integrity:
- Bank only
- Public verifiability
We already have Bitcoin, why do we need Ripple?
Ripple vs Bitcoin

We already have Bitcoin, why do we need Ripple?
Ripple vs Bitcoin

**Definition:**

<table>
<thead>
<tr>
<th>Definition</th>
<th>Currency</th>
<th>Transaction network</th>
</tr>
</thead>
</table>

We already have Bitcoin, why do we need Ripple?
Ripple vs Bitcoin

**Definition:**

<table>
<thead>
<tr>
<th>Currency</th>
<th>Transaction network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>Only via a path with enough credit</td>
</tr>
</tbody>
</table>

**Transfer of funds:**

- Direct transactions between any two wallets
- Transactions only via a path with enough credit

*We already have Bitcoin, why do we need Ripple?*
### Ripple vs Bitcoin

We already have Bitcoin, why do we need Ripple?

<table>
<thead>
<tr>
<th>Definition:</th>
<th>Currency</th>
<th>Transaction network</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>Scalability:</td>
<td>Limited transaction rate</td>
<td>Highly scalable</td>
</tr>
</tbody>
</table>
Ripple vs Bitcoin

We already have Bitcoin, why do we need Ripple?

<table>
<thead>
<tr>
<th>Definition:</th>
<th>Currency</th>
<th>Transaction network</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>Scalability:</td>
<td>Limited transaction rate</td>
<td>Highly scalable</td>
</tr>
</tbody>
</table>

Public verifiability of transactions
Public Verifiability & Privacy Problem
## Public Verifiability & Privacy Problem

### Transaction details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rnvctTPLKZqK59f1fXpDkQ...</td>
<td>rMnVZ9maUwp5cAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBpSquSHKbbfvcKt1c54...</td>
<td>rKoDt7VL83AKJZewLxVZEs...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9fSSmD4SYmnDra16B...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.0693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759dbJMrzMNL4OqvQe9...</td>
<td>r95pWKA1K55fy7EJWrqJ9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42WJGvV9MJa4t5QcF8Cnx...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.0821058028231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAqHEopZ5...</td>
<td>r3H4rynDShFMRWkJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7UfGvzCeZwJxUEeZHLG...</td>
<td>rBwgTdzzMhnouLk5JD3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpVVzfSTUJX9CrKBSS2Z5W...</td>
<td>rDCgaaSBAWYfsxUYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
## Public Verifiability & Privacy Problem

### Transaction details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rnvctTPLKZq59f1fXpDkQ...</td>
<td>rMnVZ9maUwp5cAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBpSquSKbbfvcKt1c54...</td>
<td>rKoDt7V83AKJZewLxVZEs...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9fSSmD4SYmnDra16B...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.0693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759dbJMzMN4QbVqe9...</td>
<td>r95pWKA1K55f7EJWrqJ9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42WJGvV9MJ4t5qcF8Cnx...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.0821058028231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAqHEopZ5...</td>
<td>r3H4rynDSfFMRKWuJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7Ub0vzCeZxWxeZHLG...</td>
<td>rBwgtDzzMhncuLk5DJD3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpVzfSTUX9CrKBSS2Z5W...</td>
<td>rDCgaaSBAYfsxUYhCkIn2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
## Public Verifiability & Privacy Problem

### Transaction details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rWvctTPLKZqK59f1fXpDkQ...</td>
<td>rMnVZ9maUwp5cAvmqBECZ...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBpSquSHKBbfvcKt1c54...</td>
<td>rKoDt7VL83AKJZewLxVZEs...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9fSSmD4SYmnDra16B...</td>
<td>rBeToNo4AwHaNbx2n4BNC...</td>
<td>0.0693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759dbJMrzMNL4QbvQE9...</td>
<td>r95pWKA1K55fy7EJWrqJ9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42WJGvV9MJa4t5QcF8Cnx...</td>
<td>rBeToNo4AwHaNbx2n4BNC...</td>
<td>0.0821058028231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAqHEopZ5...</td>
<td>r3H4rynDShFMRKWyJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rW7UfGvzCeZwJxUEeZHLL...</td>
<td>rBwgTdzzMnouLk5DJD3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rPVzfSTUJX9CrKBSS2Z5W...</td>
<td>rDCgaaSBAWYfsxUYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>

### Credit links

---

**Pseudonymity does not equate privacy**
Public Verifiability & Privacy Problem

Transaction details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rvwctTPLKZqK59f1fXpDkQ...</td>
<td>rMnVZ9maUWp5cAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBP5HbbfvcKt1c54...</td>
<td>rKoD77V83AKJZewLxVZEs...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9fSSmD4SYmnDra16B...</td>
<td>rBeToNo4AwhSNbRX2n4BNC...</td>
<td>0.0.0693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759dBJMrzMNL4QbvQe9...</td>
<td>r95pWKA1K55fy7EJWpJ9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42WJGvV9MA4t5QcF8Cnx...</td>
<td>rBeToNo4AwhSNbRX2n4BNC...</td>
<td>0.0821058028231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAqHEopz5...</td>
<td>r3H4rynDSfFMRKWuJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7UfGvZcZwJxxUeZHLL...</td>
<td>rBwgTdzzMHnouLk5PH3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpVVzSTULX9CrKB5S2Z5W...</td>
<td>rDCgaaSBAWYfsxUYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>

Credit links

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

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

PETS ‘16
Privacy Definitions

Transaction Value Privacy

\[ 10 \approx 30 \]
Privacy Definitions

Transaction Value Privacy

Transaction Receiver Privacy

≈

≈
Distributed Credit Network

- Each user maintains her own credit links
Distributed Credit Network

- Each user maintains her own credit links
Distributed Credit Network

- Each user maintains her own credit links
Credit links of a user determine his credit in the network
Credit links of a user determine his credit in the network

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

A user checks net-flow does not change.

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

✦ Credit links of a user determine his credit in the network

CBW BANK

\[ \text{In-flow} = 450 \]
\[ \text{Out-flow} = 40 \]
\[ \text{Net-flow} = 410 \]

✦ A user checks net-flow does not change

CBW BANK

\[ \text{In-flow} = 450 \]
\[ \text{Out-flow} = 40 \]
\[ \text{Net-flow} = 410 \]
Motivation

✦ Credit links of a user determine his credit in the network

✦ A user checks net-flow does not change

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

✦ Credit links of a user determine his credit in the network

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

✦ A user checks net-flow does not change

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

✦ Credit links of a user determine his credit in the network

![Diagram](image)

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

✦ A user checks net-flow does not change

![Diagram](image)

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

✦ Credit links of a user determine his credit in the network

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

✦ A user checks net-flow does not change

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

✦ How to find paths between users?
Challenges

✦ How to find paths between users?
✦ Credit available in the path?
Challenges

✦ How to find paths between users?
✦ Credit available in the path?
✦ How to ensure credit links form a path?
Challenges

✦ How to find paths between users?
✦ Credit available in the path?
✦ How to ensure credit links form a path?
✦ And maintaining strong privacy guarantees…
Challenges

✦ How to find paths between users?
✦ Credit available in the path?
✦ How to ensure credit links form a path?
✦ And maintaining strong privacy guarantees…

Let’s go one by one!
Routing Challenge
Routing Challenge

- Determine credit path from sender to receiver
Routing Challenge

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

✦ Determine credit path from sender to receiver

✦ Common problem in standard networks and ad-hoc networks

✦ The max-flow approach:
   ✦ Inefficient algorithms: $O(V^3)$ or $O(V^2 \log(E))$
Routing Challenge

✦ Determine credit path from sender to receiver

✦ Common problem in standard networks and ad-hoc networks

✦ The max-flow approach:
  ✦ Inefficient algorithms: $O(V^3)$ or $O(V^2 \log(E))$

✦ Landmark routing [Tschusiyaa’98]:
  ✦ Calculate only a subset of all possible paths
  ✦ Enough in practice*
  ✦ More efficient than max-flow*

Routing Challenge: Landmark routing

Landmark: Highly connected node
Routing Challenge: Landmark routing

Landmark: Highly connected node
Routing Challenge: Landmark routing

Landmark: Highly connected node
Routing Challenge: Landmark routing

Landmark: Highly connected node
Routing Challenge: Landmark routing

Landmark: Highly connected node
Routing Challenge: Landmark routing

Landmark: Highly connected node

L1 – parent L1
U2
L1 – parent U2
U1

L1 – parent L1
U3

L1 – parent U3
U4
Routing Challenge: Landmark routing

U2

L1 – parent L1

U3

L1 – parent L1

U1

L1 – parent U2

U4

L1 – parent U3

Landmark: Highly connected node
Routing Challenge: Landmark routing

L1

U2

L1 – parent L1

U1

L1 – parent U2

U3

L1 – parent L1

U4

L1 – parent U3

Landmark: Highly connected node
Credit in a Path

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

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

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

[x]: Secret share of x

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

[x]: Secret share of x

✧ Given [x] it is not possible to know x
✧ How to ensure that [x] comes from a user in a path?
Credit in a Path

[x]: Secret share of x

Given [x] it is not possible to know x

How to ensure that [x] comes from a user in a path?
Proof of Credit Links in a Path

30
Proof of Credit Links in a Path

$sk_1, vk_1 \rightarrow 30 \rightarrow sk_2, vk_2$
Proof of Credit Links in a Path

\[ \sigma_1 := \text{Sig}(sk_1, ([30], vk_1, vk_2)) \]
\[ \sigma_2 := \text{Sig}(sk_2, ([30], vk_1, vk_2)) \]
Proof of Credit Links in a Path

\[ \sigma_1 := \text{Sig}(sk_1, ([30], vk_1, vk_2)) \]
\[ \sigma_2 := \text{Sig}(sk_2, ([30], vk_1, vk_2)) \]
Proof of Credit Links in a Path

\[ \sigma_1 := \text{Sig}(sk_1, ([30], vk_1, vk_2)) \]
\[ \sigma_2 := \text{Sig}(sk_2, ([30], vk_1, vk_2)) \]

Correct proof for a path

\((vk_1, vk_2), (vk_2, vk_3), (vk_3, vk_4), \ldots\)
Proof of Credit Links in a Path

\[ \sigma_1 := \text{Sig}(sk_1, ([30], vk_1, vk_2)) \]
\[ \sigma_2 := \text{Sig}(sk_2, ([30], vk_1, vk_2)) \]

Correct proof for a path

\[ (vk_1, vk_2), (vk_2, vk_3), (vk_3, vk_4), \ldots \]
Proof of Credit Links in a Path

\[ \sigma_1 := \text{Sig}(sk_1, ([30], vk_1, vk_2)) \]
\[ \sigma_2 := \text{Sig}(sk_2, ([30], vk_1, vk_2)) \]

Correct proof for a path

\[(vk_1, vk_2), (vk_2, vk_3), (vk_3, vk_4), \ldots\]

Fresh keys per transaction
Up to now, what we can do is:
Up to now, what we can do is:

$\{30\}, \text{vk}_{\{1,2\}}, \sigma_{\{1,2\}}$
Up to now, what we can do is:
Up to now, what we can do is:
Up to now, what we can do is:
Privacy-preserving Credit in a Path

Up to now, what we can do is:

- Homomorphic properties: \([x] + [y] = [x + y]; c \cdot [x] = [c \cdot x]\)
Privacy-preserving Credit in a Path

Up to now, what we can do is:

Homomorphic properties: $[x] + [y] = [x + y]; c \cdot [x] = [c \cdot x]$
Privacy-preserving Credit in a Path

Up to now, what we can do is:

- Homomorphic properties: \([x] + [y] = [x + y]; c \cdot [x] = [c \cdot x]\)
- Given enough “copies” of \([x]\) it is possible to recover \(x\)
Transaction

- Gossip neighbor to neighbor
Transaction

- Gossip neighbor to neighbor
- Two-step transaction: on hold and settle
- Gossip neighbor to neighbor
- Two-step transaction: on hold and settle
- Example:
Transaction

- Gossip neighbor to neighbor
- Two-step transaction: on hold and settle
- Example:
Transaction

- Gossip neighbor to neighbor
- Two-step transaction: on hold and settle
- Example:

![Diagram showing transactions with amounts and incentives]
Transaction

✦ Gossip neighbor to neighbor
✦ Two-step transaction: on hold and settle
✦ Example:

Example:

5

Incentive

5

(5)

25

(5)

10

10
Transaction

- Gossip neighbor to neighbor
- Two-step transaction: on hold and settle
- Example:

\[
\begin{align*}
&\text{Incentive} \\
&\text{(5)} \quad \text{(5)} \\
&10 \quad 25
\end{align*}
\]

"Ok, received!"
Transaction

- Gossip neighbor to neighbor
- Two-step transaction: on hold and settle
- Example:

  ![Diagram showing a two-step transaction process with an incentive and a confirmation message.](image-url)
Transaction

- Gossip neighbor to neighbor
- Two-step transaction: on hold and settle
- Example:

```
  5

  10

  25

Incentive

Ok, received!
```
Transaction

✦ Gossip neighbor to neighbor
✦ Two-step transaction: on hold and settle
✦ Example:

Incentive

5

Ok, received!

10

30

15

25

10
Take Home Message
Credit networks has **advantages** over current banking. However, there are **privacy issues**

Pseudonymity does not equate privacy

Listening to Whispers of Ripple: Linking Wallets and De-anonymizing Transactions in the Ripple Network

Pablo Moreno-Sanchez, Muhammad Bilal Zahir, Sypher Kale.
Take Home Message

- Credit networks have advantages over current banking. However, there are privacy issues.

- Decentralized credit network with privacy guarantees.

Public Verifiability & Privacy Problem

Distributed Credit Network

- Each user maintains her own credit links.

Pseudonymity does not equate privacy.

Listening to Whispers of Ripple: Linking Wallets and De-anonymizing Transactions in the Ripple Network
Pablo Moreno-Sanchez, Mohsen Bilal, Zahir Zafar, Syed Kale.
Take Home Message

- Credit networks have advantages over current banking. However, there are privacy issues.

- Several challenges we address in this work:
  - calculate credit on a path
  - check existence of a path
  - carry out the transaction

- Decentralized credit network with privacy guarantees