Privacy-preserving payments in credit networks

Pedro Moreno-Sanchez
CS, Purdue University
Credit Networks 101

Real World

Credit Network
Credit Networks 101

Real World

I need credit

Credit Network
Credit Networks 101

Real World

I need credit

I pay you $20

Credit Network
Credit Networks 101

Real World

I need credit

I pay you $20

I owe you $20

Credit Network
Credit Networks 101

Real World

I need credit

I pay you $20

I owe you $20

Credit Network

20
Credit Networks 101

Real World

I need credit

I pay you $20

I owe you $20

Credit Network

I need credit

I pay you $20

I owe you $20
Why Credit Networks?

- Sybil-resistant applications
Why Credit Networks?

- Sybil-resistant applications
Why Credit Networks?

- Sybil-resistant applications
**Why Credit Networks?**

- **Sybil-resistant applications**

Introducing nodes is much easier than drawing trust from honest nodes.
Why Credit Networks?

✦ Sybil-resistant applications

Introducing nodes is much easier than drawing trust from honest nodes.

Misbehaving user’s effect is:
  - Localized
  - Bounded
Why Credit Networks?

- **Sybil-resistant applications**

Introducing nodes is much easier than drawing trust from honest nodes.

Misbehaving user’s effect is:
- Localized
- Bounded
Why Credit Networks?

- Sybil-resistant applications

Introducing nodes is much easier than drawing trust from honest nodes.

Misbehaving user’s effect is:
- Localized
- Bounded

Several applications:
- Ostra: preventing e-mail spam [NSDI'08]
Why Credit Networks?

✦ Sybil-resistant applications

Introducing nodes is much easier than drawing trust from honest nodes.

Misbehaving user’s effect is:
- Localized
- Bounded

Several applications:
- Ostra: preventing e-mail spam [NSDI’08]
- Bazaar: strengthening e-commerce [NSDI’11]
Why Credit Networks?

✦ Sybil-resistant applications

Introducing nodes is much easier than drawing trust from honest nodes.

Misbehaving user’s effect is:
- Localized
- Bounded

✦ Several applications:
  ✦ Ostra: preventing e-mail spam [NSDI'08]
  ✦ Bazaar: strengthening e-commerce [NSDI'11]
  ✦ SumUp: Sybil-resilient content voting [NSDI'09]
Why Credit Networks?

✧ Sybil-resistant applications

Introducing nodes is much easier than drawing trust from honest nodes.

Misbehaving user’s effect is:
- Localized
- Bounded

✧ Several applications:

✧ Ostra: preventing e-mail spam [NSDI’08]
✧ Bazaar: strengthening e-commerce [NSDI’11]
✧ SumUp: Sybil-resilient content voting [NSDI’09]
✧ Ripple: A real-life online payment network
Ripple Payment Network

- Payment Network: Ripple
Payment Network: Ripple
Ripple Payment Network

Payment Network: Ripple
Ripple Payment Network

✦ Payment Network: Ripple
Ripple Payment Network

Payment Network: Ripple
Ripple Payment Network

Payment Network: Ripple

<table>
<thead>
<tr>
<th></th>
<th>Banking System</th>
<th>Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transaction time</strong></td>
<td>~ 1 day</td>
<td>~ 5 seconds</td>
</tr>
<tr>
<td><strong>Inter-currency &amp; worldwide transactions</strong></td>
<td>High fees</td>
<td>Small Fees</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Bank-only</td>
<td>Publicly Verifiable</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>rMnVZ9maUWp5cAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBpSquSHKbbfwvcKt1c54...</td>
<td>rKoDt7VL83AKJZewLxVZEd...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9fSSmD4SYmnDra16B...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</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>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.0821058028231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAqHEopZ5...</td>
<td>r3H4rynDSHfMRKWyUcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7UfGvzCeZwJxxUEeZHLG...</td>
<td>rBwgTdzzMHnouLk5DJD3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpVVFSTUJX9CrKBSS2Z5W...</td>
<td>rDCgaaSBAYfsxUYhCk1n2...</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>rwvctTPLKZqK59f1fXpDkO...</td>
<td>rMnVZ9maUWp5cAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBpSquSHKbbfvKt1c54...</td>
<td>rKoD77VL83AKJZeLxVZEs...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9fSSmD4SYmnDra16B...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.0693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759dbJMrzMN4QbvQe9...</td>
<td>r95pWA1K55fy7EJWrqJ9b...</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>r3H4rynDShFMRKWyJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7UfGvzCeZwJxUEeZHLG...</td>
<td>rBwgTdzzMhnuLk5JD3xd...</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>rwvctTPLKZqK59f1fXpDk0...</td>
<td>rMnVZ9maUWp5cAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBPsquSHKbbfvckt1c54...</td>
<td>rKoDt7VL83AKJZewLxVZEd...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r42869fSSmD4SyMnDra16B...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.0693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759dbJMrzmN4bQvQe9...</td>
<td>r95pWKA1K55fy7EJWrqJ9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42W6JgV9JMa4t5QcF8Cnx...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.0821058028231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxYAgHEopZ5...</td>
<td>r3H4rynDSnFMrKwujcaldL...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7Uf6gvXEZwJxxUEeZHLG...</td>
<td>rBwgTdzzTMHouLk5DJD3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpVvzSTUJX9CrKBSS2Z5W...</td>
<td>rDCgaaSBAYWfsxUYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>

**Ledger**

50
30
200

**Credit links**
Public Verifiability & Privacy Problem

Ledger

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200</td>
<td></td>
</tr>
</tbody>
</table>

Credit links

Transaction details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rtwvctTPLKZqK59f1fX...</td>
<td>rMnVZ9maW...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBpSquSHKbbfvcKt...</td>
<td>rKoDt7VL83...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9fSSmD4SYmnDra...</td>
<td>rBeToNo4A...</td>
<td>0.0693402709148/CCK</td>
</tr>
<tr>
<td>rhD759dbJMzNL4QbvQe...</td>
<td>r95pWKA1K55...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42WJGvV9MJa4t5QcF8C...</td>
<td>rBeToNo4A...</td>
<td>0.0821058028231/CCK</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAqHEo...</td>
<td>r3H4rynDShFM...</td>
<td>1129.916679154465/EUR</td>
</tr>
<tr>
<td>rw7UfGvzCeZwJxxUEeZ...</td>
<td>rBwgTdz...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpVVzfSTUJX9CrKBSS2...</td>
<td>rDCgaeSBAW...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
Public Verifiability & Privacy Problem

Ledger

- 30
- 50
- 200

Transaction details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rrwctTPLKZqK59f1fxpDk0...</td>
<td>rMnVZ9maUWp5cAVmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBpSquSHKbbfvckt1c54...</td>
<td>rKoDt7VL83AKJZewLxVZEr...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9f5SmD4SYmDr16B...</td>
<td>rBeToNo4AWhaNbRX2n4BNC...</td>
<td>0.0693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759dBMrzMNl4QbvQe9...</td>
<td>r95pWKA1K55fy7EJWrqJ9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42wJGvV9MJa4tSqcF8Cnx...</td>
<td>rBeToNo4AWhaNbRX2n4BNC...</td>
<td>0.0821058028231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAqHEopZ5...</td>
<td>r3H4rynDShMRKruJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7UfgvzCezwJxxUEeZHlG...</td>
<td>rBwgTdzzMhnoULK5DJD3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpVVzfSTUJX9CrKBSS2Z5W...</td>
<td>rDCgaaSBAYfsxUYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>

Credit links
### Public Verifiability & Privacy Problem

#### Ledger

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>50</td>
</tr>
<tr>
<td>200</td>
<td></td>
</tr>
</tbody>
</table>

#### Transaction details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rrvctTPLKZqK59f1fXpDkQ...</td>
<td>rMnVZ9maUWp5cAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBpSquSHkbffvckt1c54...</td>
<td>rKoDt7VL83AKJZewLxVZEs...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9fSsmD4SyHmmDra16B...</td>
<td>rBeToNo4AwNbrRX2n4BNC...</td>
<td>0.0693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759dbJMrzMNL4Qbve9...</td>
<td>r95pWKA1K55fy7EJWrqJ9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42WJGvV9MJa4t5QcF8Cnx...</td>
<td>rBeToNo4AwNbrRX2n4BNC...</td>
<td>0.0821058028231/CCK/rB...</td>
</tr>
<tr>
<td>rUunr1p7xkSBxyAqHEopZ5...</td>
<td>r3H4rynDSfMRKwuJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7UfGvzCeZwJxxEeZHLG...</td>
<td>rBwgTdzzMhounLk54JD3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpVVzfSTUJJ9CrKBSS2Z5W...</td>
<td>rDCgaaSBAWYfsxUYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
Is privacy a real problem in Ripple?
Interlog Linkability

* The tale of two logs

Bitcoin
Interlog Linkability

✧ The tale of two logs

Bitcoin

Ripple
Interlog Linkability

The tale of two logs

Bitcoin

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice-Bitcoin:</td>
<td>DR-Bitcoin:</td>
</tr>
<tr>
<td>6 BTC</td>
<td>6 BTC</td>
</tr>
</tbody>
</table>

Alice

Ripple
Interlog Linkability

The tale of two logs

**Bitcoin**

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice-Bitcoin:</td>
<td>DR-Bitcoin:</td>
</tr>
<tr>
<td>6 BTC</td>
<td>6 BTC</td>
</tr>
</tbody>
</table>

Alice

**Ripple**

<table>
<thead>
<tr>
<th></th>
<th>DR-Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>Alice-Ripple</td>
</tr>
<tr>
<td>Receiver</td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>6 BTC IOU</td>
</tr>
<tr>
<td>Path</td>
<td>Bob —&gt; Alice</td>
</tr>
</tbody>
</table>

Bob

Diagram of Ripple transactions with nodes and arrows indicating the flow of value.
Interlog Linkability

✧ The tale of two logs

Bitcoin

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice-Bitcoin:</td>
<td>DR-Bitcoin:</td>
</tr>
<tr>
<td>6 BTC</td>
<td>6 BTC</td>
</tr>
</tbody>
</table>

Alice

Ripple

<table>
<thead>
<tr>
<th>Sender</th>
<th>DR-Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice-Ripple</td>
<td>Alice-Ripple</td>
</tr>
<tr>
<td>Value</td>
<td>6 BTC IOU</td>
</tr>
<tr>
<td>Path</td>
<td>Bob —&gt; Alice</td>
</tr>
</tbody>
</table>

6

Alice-Bitcoin

Alice-Ripple
Interlog Linkability

-The tale of two logs

**Bitcoin**

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice-Bitcoin:</td>
<td>DR-Bitcoin:</td>
</tr>
<tr>
<td>6 BTC</td>
<td>6 BTC</td>
</tr>
</tbody>
</table>

Alice

**Ripple**

<table>
<thead>
<tr>
<th>Sender</th>
<th>DR-Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td>Alice-Ripple</td>
</tr>
<tr>
<td>Value</td>
<td>6 BTC IOU</td>
</tr>
<tr>
<td>Path</td>
<td>Bob —&gt; Alice</td>
</tr>
</tbody>
</table>

Bob —> Alice

Alice-Bitcoin
Alice-Ripple

DR-Bitcoin
DR-Ripple
The tale of two logs

**Bitcoin**

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice-Bitcoin: 6 BTC</td>
<td>DR-Bitcoin: 6 BTC</td>
</tr>
</tbody>
</table>

**Alice**

**Ripple**

<table>
<thead>
<tr>
<th>Sender</th>
<th>DR-Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td>Alice-Ripple</td>
</tr>
<tr>
<td>Value</td>
<td>6 BTC IOU</td>
</tr>
<tr>
<td>Path</td>
<td>Bob —&gt; Alice</td>
</tr>
</tbody>
</table>

This is only the tip of the iceberg!

How to have privacy-preserving payments in a credit network?
Credit Network Payment

Diagram showing a network with various connections and numbers representing payments or interactions.
Credit Network Payment
Credit Network Payment
Credit Network Payment
Credit Network: Routing Challenge
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver
- Existing systems using max-flow approach. Inefficient
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver
- Existing systems using max-flow approach. Inefficient
- Landmark routing [Tschusiya’98]: Calculate subset of all possible routes
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver
- Existing systems using max-flow approach. Inefficient
- Landmark routing [Tschusiya’98]: Calculate subset of all possible routes
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver
- Existing systems using max-flow approach. Inefficient
- Landmark routing [Tschusiya’98]: Calculate subset of all possible routes
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver
- Existing systems using max-flow approach. Inefficient
- Landmark routing [Tschusiya’98]: Calculate subset of all possible routes
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver
- Existing systems using max-flow approach. Inefficient
- Landmark routing [Tschusiy̦a’98]: Calculate subset of all possible routes
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver.
- Existing systems using max-flow approach. Inefficient.
- Landmark routing [Tschusiya’98]: Calculate subset of all possible routes.
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver
- Existing systems using max-flow approach. Inefficient
- Landmark routing [Tschusiya’98]: Calculate subset of all possible routes

[Diagram: Tree structures representing credit network with landmark universe]
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver
- Existing systems using max-flow approach. Inefficient
- Landmark routing [Tschusiyia’98]: Calculate subset of all possible routes
Credit Network: Routing Challenge

- Routing: Determine credit route from sender to receiver
- Existing systems using max-flow approach. Inefficient
- Landmark routing [Tschusiya’98]: Calculate subset of all possible routes
Privacy Definitions

Transaction Value Privacy

$\approx$
Privacy Definitions

Transaction Value Privacy

Transaction Receiver Privacy

10

≈

5

30

≈

5

…”
Transaction Value Privacy: Definition (I)

Challenger

Attacker

payment
change link
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

payment
change link
Transaction Value Privacy: Definition (I)

Query phase

**Challenger**
- change link()
  - payment()
  - test-link()
  - test-credit()

**Attacker**
- payment
- change link
Query phase

**Challenger**
- change link()
- payment()
- test-link()
- test-credit()

**Attacker**
- payment
- change link

+35
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

payment
change link

+35

35
Transaction Value Privacy: Definition (I)

Query phase

Challenger
- Change link()
- Payment()
- Test-link()
- Test-credit()

Attacker
- Change link
- Payment

+35
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

change link()

payment()

test-link()

test-credit()

payment

change link

+35
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

payment
change link

change link()
payment()
test-link()
test-credit()

+35

5
30
35
Transaction Value Privacy: Definition (I)

Query phase

Challenger

35
5
30

Attacker

payment
change link

Challenge phase

Challenger

35
5
30

Attacker

+35

change link()
payment()
test-link()
test-credit()
Transaction Value Privacy: Definition (I)

Query phase

Challenger

35

payment()
test-link()
test-credit()  
5
30

Attacker

+35

Challenge phase

5
35
30

payment
change link

-10
-30
Transaction Value Privacy: Definition (I)

Query phase

Challenger

5

35

30

Attacker

payment

change link

+35

Challenge phase

Challenger

5

35

30

Attacker

-30
Transaction Value Privacy: Definition (I)

Query phase

- Attacker
  - Change link
  - Payment
- Challenger
  - Change link
  - Payment
  - Test-link
  - Test-credit
- Balancing transaction

Challenge phase

- Attacker
  - Balancing transaction
  - Payment
- Challenger
  - Change link

5 35 30 5 35 30

+35 +30 5 5 30 30

-30 -30
Transaction Value Privacy: Definition (I)

Query phase

- Attacker
- Challenger
- Balancing transaction

Challenge phase

- Attacker
- Challenger

payment
change link

Balancing transaction

change link()
payment()
test-link()
test-credit()
Transaction Value Privacy: Definition (I)
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Challenger action:
- change link()
- payment()
- test-link()
- test-credit()

Attacker

Attacker action:
- payment
- change link

Challenge phase

Balancing transaction

Transaction value:
- 35
- 25
- 5
- 30
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

+35

35

30

5

Challenge phase

Balancing transaction

Query phase

...
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Change link()

payment()

test-link()

test-credit()

Attacker

+35

Challenge phase

Balancing transaction

Query phase

Guess phase

???

-10

-30
A credit network satisfies value privacy if:

Transaction Value Privacy: Definition (II)

Pr

Challenge transaction is -30

≈

-30

Balancing transaction

Challenge transaction

Pr

Challenge transaction is -30

≈

-30

Balancing transaction

Challenge transaction
Credit Network: Privacy challenge

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rnvctTPLKZqK9f1f7oPDK...</td>
<td>rMnVZ9maUK6pqCAvmeqBECZ9L...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLS8p5q59HkbbFvcKit1c54...</td>
<td>rKoD7V7L83AKJZewLvVZEm...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9f5SShD45ymDra18bL...</td>
<td>rBeToM044wHumBdx2n4BNc...</td>
<td>0.069346270148/CKK/fRL...</td>
</tr>
<tr>
<td>rhD759dBMrz4NL4gbvq9e9...</td>
<td>r95pmKAK35fy7EJwrqj9B...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42kf3V9mO3a4t50c69C6x...</td>
<td>rBeToM044wHumBdx2n4BNc...</td>
<td>0.0821058202231/CKK/fRL...</td>
</tr>
<tr>
<td>rUnr1p7xku5BxyAqHlEpz2z...</td>
<td>r3H4ryn0ShFMA9NwUcadjLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7uf6vzCe2w3xxUEcZHL...</td>
<td>rBgTdzHMouLk5JD3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rPv2fSTU3X9cKBsS2Z5W...</td>
<td>rBcgsxSBWYFxsxYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
Providing privacy is challenging:
Credit Network: Privacy challenge

✦ Providing privacy is challenging:
✦ Hide transactions values —> What is the paid amount?

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rwcctTPLKZQgK9f1fXq0PK...</td>
<td>rynYZjm0rMgDCArnq8B8CZL...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rL58p5q6fiHkbVxctK11cS...</td>
<td>r6qDs7YzL83AK3ZewLxvZ2E...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r4269f5Smd45YmU01a108L...</td>
<td>rBET0Mb4AhHnBx248BNC...</td>
<td>0.0593462709148/CKK/rB...</td>
</tr>
<tr>
<td>rh079dbJMrZnNLqBvqo9...</td>
<td>r95wKAKJ353fy7EJWrq9...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r4263J9V9M3a4t50cF8CN...</td>
<td>rBET0Mb4AhHnBx248BNC...</td>
<td>0.0821058028231/CKK/rB...</td>
</tr>
<tr>
<td>rUrh1p7xku5BxyAq1EopZ5...</td>
<td>rJHryn0ShFM9WnuJcadL...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7Uf6vzCe2wJxxUeZHL...</td>
<td>rBekTdzMKhouLk5DID3xh...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rPzUstUJX9CrKBSSZ9W...</td>
<td>rDgwaSBAYFjdxJYKhC1n...</td>
<td>999.95/XRP</td>
</tr>
</tbody>
</table>
Credit Network: Privacy challenge

- Providing privacy is challenging:
- Hide transactions values —> What is the paid amount?
- Hide transaction participants —> Who are the sender and the receiver?
Credit Network: Privacy challenge

✦ Providing privacy is challenging:
✦ Hide transactions values —> What is the paid amount?
✦ Hide transaction participants —> Who are the sender and the receiver?

In our approach, the credit network is:
✦ stored in server environment,
✦ accessed obliviously,
✦ using trusted hardware
PrivPay: Overview

P. Moreno-Sanchez, M. Maffei, A. Kate, K. Pecina. *Privacy Preserving Payments in Credit Networks*. In NDSS’15.
PrivPay: Evaluation

- Implemented as a multithreaded C++ library
- Tested with Ripple transactions (Oct’13 — Jan’14)

<table>
<thead>
<tr>
<th></th>
<th>Non-Private [1]</th>
<th>PrivPay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment (ms)</td>
<td>0.078</td>
<td>1510</td>
</tr>
<tr>
<td>Change Link (ms)</td>
<td>0.005</td>
<td>95</td>
</tr>
<tr>
<td>Landmark universe creation (ms)</td>
<td>50</td>
<td>22000</td>
</tr>
<tr>
<td>[Background process]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage</td>
<td>97%</td>
<td>95%</td>
</tr>
</tbody>
</table>

PrivPay: Evaluation

- Implemented as a multithreaded C++ library
- Tested with Ripple transactions (Oct’13 — Jan’14)

<table>
<thead>
<tr>
<th></th>
<th>Non-Private [1]</th>
<th>PrivPay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment (ms)</td>
<td>0.078</td>
<td>1510</td>
</tr>
<tr>
<td>Change Link (ms)</td>
<td>0.005</td>
<td>95</td>
</tr>
<tr>
<td>Landmark universe creation (ms)</td>
<td>50</td>
<td>22000</td>
</tr>
<tr>
<td>[Background process]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage</td>
<td>97%</td>
<td>95%</td>
</tr>
</tbody>
</table>


Deployable in practice
Ripple (~5 sec)
PrivPay: Evaluation

- Implemented as a multithreaded C++ library
- Tested with Ripple transactions (Oct’13 — Jan’14)

<table>
<thead>
<tr>
<th></th>
<th>Non-Private [1]</th>
<th>PrivPay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment (ms)</td>
<td>0.078</td>
<td>1510</td>
</tr>
<tr>
<td>Change Link (ms)</td>
<td>0.005</td>
<td>95</td>
</tr>
<tr>
<td>Landmark universe creation (ms)</td>
<td>50</td>
<td>22000</td>
</tr>
<tr>
<td>[Background process]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage</td>
<td>97%</td>
<td>95%</td>
</tr>
</tbody>
</table>

Is this system the perfect solution?
PrivPay: Deployment Challenges
PrivPay: Deployment Challenges

✧ Who should maintain the complete network and the trusted hardware?
PrivPay: Deployment Challenges

- Who should maintain the complete network and the trusted hardware?
- Removing the trusted hardware does not help either
Is there an alternative?
Distributed Credit Network

- Each user maintains her own credit links
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 = 45
Out-flow = 25
Net-flow = 20
Credit links of a user determine his credit in the network

In-flow = 45
Out-flow = 25
Net-flow = 20

A user checks net-flow does not change
Motivation

- Credit links of a user determine his credit in the network
  - In-flow = 45
  - Out-flow = 25
  - Net-flow = 20

- A user checks net-flow does not change
  - In-flow = 45
  - Out-flow = 25
  - Net-flow = 20
Motivation

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

  ![Diagram showing credit flows](image1)

  - In-flow = 45
  - Out-flow = 25
  - Net-flow = 20

- A user checks net-flow does not change

  ![Diagram showing updated credit flows](image2)

  - In-flow = 45
  - Out-flow = 25
  - Net-flow = 20
Credit links of a user determine his credit in the network:

- \( \text{In-flow} = 45 \)
- \( \text{Out-flow} = 25 \)
- \( \text{Net-flow} = 20 \)

A user checks net-flow does not change:

- \( \text{In-flow} = 45 \)
- \( \text{Out-flow} = 25 \)
- \( \text{Net-flow} = 20 \)
Credit links of a user determine his credit in the network

A user checks net-flow does not change
Challenges
Challenges

 ✦ Credit available in the path?
Challenges

- Credit available in the path?
- How to ensure credit links form a path?
Challenges

✦ Credit available in the path?

✦ How to ensure credit links form a path?

✦ And maintaining strong privacy guarantees…
Credit in a Path

30

15

25

10
Credit in a Path
Given [x] it is not possible to know x
Given [x] it is not possible to know x
How to ensure that [x] comes from a user in a path?
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
Proof of Credit Links

sk₁ → sk₂ → sk₃
Proof of Credit Links

- $sk_1$
- $sk_2$
- $sk_3$

Link Signature
Proof of Credit Links

- Anonymous credential $\sigma_{1-2}$: certificate for Alice $\rightarrow$ Bob issued by the landmark.
Proof of Credit Links

- Anonymous credential $\sigma_{1-2}$: certificate for Alice $\rightarrow$ Bob issued by the landmark.

- Secret keys remain secret after Link Signature.
Proof of Credit Links

- Anonymous credential $\sigma_{1-2}$: certificate for Alice $\rightarrow$ Bob issued by the landmark.

- Secret keys remain secret after Link Signature.

- Alice and Bob identities are not revealed to the landmark.
Credit in a Path

30 → 15 → 25 → 10
Credit in a Path

[Diagram with numbers 30, 15, 25, 10, and σ_{1-2} connections]
Credit in a Path

[30], σ₁-2
[30], σ₂-3
[15], σ₂-3
[25], σ₃-4
[25], σ₃-4
[10], σ₄-5
[10], σ₄-5

30 → 15 → 25 → 10
Credit in a Path

- It is possible to check that certified links form a path
Credit in a Path

- It is possible to check that certified links form a path
- Properties: $[x] + [y] = [x + y]$; $[x] \times [y] = [x \times y]$
It is possible to check that certified links form a path
Properties: \([x] + [y] = [x + y]; [x] \ast [y] = [x \ast y]\)
It is possible to check that certified links form a path

Properties: \([x] + [y] = [x + y]; [x] \times [y] = [x \times y]\)

Given enough “copies” of \([x]\) it is possible to recover \(x\)
Gossip neighbor to neighbor
Gossip neighbor to neighbor
Payment

✧ Gossip neighbor to neighbor
Gossip neighbor to neighbor
Payment

- Gossip neighbor to neighbor

- Local changes are visible anyways, no privacy loss
Payment

- Gossip neighbor to neighbor

Local changes are visible anyways, no privacy loss

Possible to handle other system issues:
Payment

- Gossip neighbor to neighbor

- Local changes are visible anyways, no privacy loss

- Possible to handle other system issues:
  - User churn, faulty users, concurrent payments, etc.

Take Home Message

- Credit networks have **interesting properties** and can be used in **multiple scenarios**.
Take Home Message

✦ Credit networks have interesting properties and can be used in multiple scenarios

✦ Privacy is a real and challenging problem in credit networks
Take Home Message

- Credit networks have interesting properties and can be used in multiple scenarios
- Define privacy properties of interest for credit networks
- Privacy is a real and challenging problem in credit networks
Take Home Message

- Credit networks have interesting properties and can be used in multiple scenarios.
- Define privacy properties of interest for credit networks.
- Privacy is a real and challenging problem in credit networks.
- PrivPay: novel architecture combining trusted hardware and oblivious algorithms.
Take Home Message

- Credit networks have interesting properties and can be used in multiple scenarios
- Define privacy properties of interest for credit networks
- Privacy is a real and challenging problem in credit networks
- PrivPay: novel architecture combining trusted hardware and oblivious algorithms
- Alternatively, distributed architecture for enforcing privacy in credit networks