Privacy Preserving Payments in Credit Networks

Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei and Kim Pecina

CISPA, Saarland University

NDSS 2015
Credit Networks Introduction

Real World

Credit Network
Credit Networks Introduction

Real World

I need credit

Credit Network
Credit Networks Introduction

Real World

I need credit

Credit Network

I pay you 20 $
Credit Networks Introduction

Real World

I need credit

I pay you 20 $

I owe you 20 $

Credit Network
Credit Networks Introduction

Real World

I need credit

I pay you 20 $

I owe you 20 $

Credit Network

20
Credit Networks Introduction

Real World

I need credit

I pay you 20 $

I owe you 20 $

Credit Network

25

115

135

35

30

15

30

20

10
Credit Networks Introduction

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 $
Credit Networks Introduction

Real World

I need credit

I pay you 20 $

I owe you 20 $

Credit Network

Misbehaving user's effect is:

Localized

Bounded
Credit Networks Introduction

**Real World**

I need credit

I pay you 20 $

I owe you 20 $

**Credit Network**

Misbehaving user's effect is:

- Localized
- Bounded

Multiple applications:

- **Ostra**: mitigate spam in email system
- **Bazaar**: strengthen online marketplaces, e.g., eBay Etc.
Credit Networks Application: Payment Systems

➢ Payment systems: Ripple [> 140,000 users, > $15M transaction volume]
Credit Networks Application: Payment Systems

➢ Payment systems: **Ripple [> 140,000 users, > $15M transaction volume]**
Credit Networks Application: Payment Systems

➢ Payment systems: **Ripple [> 140,000 users, > $15M transaction volume]**
Credit Networks Application: Payment Systems

- Payment systems: **Ripple [> 140,000 users, > $15M transaction volume]**
Credit Networks Application: Payment Systems

- Payment systems: **Ripple [> 140,000 users, > $15M transaction volume]**

<table>
<thead>
<tr>
<th></th>
<th>Banking System</th>
<th>Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transaction</strong></td>
<td>~ 1 day</td>
<td>~ 5 seconds</td>
</tr>
<tr>
<td><strong>Multi-currency &amp; worldwide transactions</strong></td>
<td>High fees</td>
<td>Small fees</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Bank-only verifiable</td>
<td>Publicly verifiable</td>
</tr>
</tbody>
</table>
Public Verifiability & Privacy Problem

**Ledger**

| 50 | 30 | 200 | ... |

**Credit links**

**Transaction details**

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rwwctTPLKZqK59f1fXpDkQ...</td>
<td>rMnVZ9maUhp5cAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBp5quSHKbbfvcKt1c94...</td>
<td>rKoD7VL83AKJZezLxYZEs...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9fSSmD4SYmNdral6B...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.6693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759dbJMrzMNL4Qbvoe9...</td>
<td>r95pVA1K55f7EJWq39b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42WJ6vV9MJa4t5Qc8Cnx...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.6021058028231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAqHEopZ5...</td>
<td>r3H4rynDShFMXKuJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7Uf6VzCeZwJxxUEeZHLG...</td>
<td>rBwgTdzzMHouLk5DJD3xd...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpWzSTJX9CrKBSS2Z5W...</td>
<td>rDgaaSBAWyfsxUyhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
Public Verifiability & Privacy Problem

Ledger

| 50 | 30 | 200 |

Credit links

Transaction details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rwxctTPLKZqK59f1fXpDkQ...</td>
<td>rMnZ9maUhwp5CAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBpSQUShKbbfvcKt1c94...</td>
<td>rKoDt7VL83AKZewLxYZE...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428G9fSSnD4YmnDra16B...</td>
<td>rBeToNo4AwHaNbrX2n4BNC...</td>
<td>0.6693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759cbJmrzMN4QbvQe9...</td>
<td>r95piKA1K5fy7EJwrqJ9b...</td>
<td>306/XRP</td>
</tr>
<tr>
<td>r42WjG6vV9MJa4t5Qc8Cnx...</td>
<td>rBeToNo4AwHaNbrX2n4BNC...</td>
<td>0.682105828231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAqHeopZ5...</td>
<td>r3H4rynDShFMKwJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rwJfGvzCeZwJxxUEezHLD...</td>
<td>rBwgdzJHncuLk5DJD3xd...</td>
<td>106/XRP</td>
</tr>
<tr>
<td>rpWzf4TIJX9CrKBSS2Z5W...</td>
<td>rDcgaASBAWYfsxUyhcK1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
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>

Credit links

**Transaction details**

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rvvctTPLKZqK59f1fXpDk...</td>
<td>rMnZ9maUWp5CAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBp5quSHKbbfvcKt1c94...</td>
<td>rKoD77VL83AKJZeLxYzes...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r28G9fSSmD4SYmNdra16B...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.0693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759dbjMzMN4qBvQe9...</td>
<td>r95piKA1K55fY7EJwrqJ9b...</td>
<td>306/XRP</td>
</tr>
<tr>
<td>r2WJG6vV9MJa4t5Qc8Cnx...</td>
<td>rBeToNo4AwHaNbRX2n4BNC...</td>
<td>0.0821058028231/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSbxyAqHeopZ5...</td>
<td>r3H4rynDShFMxKwuJcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7Uf6vzCeZwJxxUEeZHLG...</td>
<td>rBwgTdzzMHnouLk5DJD3x...</td>
<td>100/XRP</td>
</tr>
<tr>
<td>rpWz5TIIJX9CrKBSS2Z5w...</td>
<td>rDcgaSBABYfesUYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
Public Verifiability & Privacy Problem

Ledger

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

Transaction details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rnvctTPLKZqK59f1fXpDkQ...</td>
<td>rMnZ9maUwp5CAvmqBECZM...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>rLSBp5u5bHkbfvcKt1c94...</td>
<td>rKoDt7VL83AKJZeLxVZEd...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r428Gn9fSSnD4yYmDra16B...</td>
<td>rBeToNo4AwhaNbrRxn4BFnc...</td>
<td>0.6693402709148/CCK/rB...</td>
</tr>
<tr>
<td>rhD759cbJMrzMNl4qbVo9...</td>
<td>r95pKA1K55fy7EJWqrj9b...</td>
<td>306/XRP</td>
</tr>
<tr>
<td>r42WjGvVMJa4t5Qc8Cnx...</td>
<td>rBeToNo4AwhaNbrRxn4BFnc...</td>
<td>0.682105802831/CCK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyAqHEopZ5...</td>
<td>r3H4rynDSHfMnKtwJcadLY...</td>
<td>1129.916679154465/EUR...</td>
</tr>
<tr>
<td>rw7U6vzCeZwJxUEeZHLG...</td>
<td>rBwgTdzzMhncuLk5DJ3Xd...</td>
<td>106/XRP</td>
</tr>
<tr>
<td>rpWzfSTJJX9CrKBSSz5W...</td>
<td>rDCgaa3BAWyFxsUYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>

Credit links

LINKABLE ANONYMITY
Contributions

➢ **Identify privacy problem** as an important issue in credit networks.
Contributions

- **Identify privacy problem** as an important issue in credit networks

- **Define privacy properties** for credit networks: value and receiver privacy
Contributions

- **Identify privacy problem** as an important issue in credit networks
- **PrivPay**: novel architecture combining trusted hardware and oblivious algorithms

---

**Table:**

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rwc1TPRukjyv3v/fT/jsHML...</td>
<td>r6wZJ6gbi6sAgwSp/VCfLC...</td>
<td>380/3DP</td>
</tr>
<tr>
<td>rL8pZyv934sH3Vtvck1C34...</td>
<td>r6wZJ6gbi6sAgwSp/VCfLC...</td>
<td>75/30P</td>
</tr>
<tr>
<td>r200f1otNv4tsw/165...</td>
<td>r6wZJ6gbi6sAgwSp/VCfLC...</td>
<td>153.7/30P</td>
</tr>
<tr>
<td>r0750jHj/2ml.40vdec...</td>
<td>r5y6fA9v7sGfV/3eH6...</td>
<td>380/3DP</td>
</tr>
<tr>
<td>r200f1otNv4tsw/165...</td>
<td>r6wZJ6gbi6sAgwSp/VCfLC...</td>
<td>0.00345027931/30P</td>
</tr>
<tr>
<td>r0750jHj/2ml.40vdec...</td>
<td>r5y6fA9v7sGfV/3eH6...</td>
<td>5,123.7/50P</td>
</tr>
<tr>
<td>r200f1otNv4tsw/165...</td>
<td>r6wZJ6gbi6sAgwSp/VCfLC...</td>
<td>559.99/30P</td>
</tr>
</tbody>
</table>

---

**Define privacy properties** for credit networks: value and receiver privacy
Contributions

➢ **Identify privacy problem** as an important issue in credit networks

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>50</td>
<td>200</td>
</tr>
</tbody>
</table>

➢ **PrivPay**: novel architecture combining trusted hardware and oblivious algorithms

➢ **Define privacy properties** for credit networks: value and receiver privacy

➢ **Evaluation**: feasible to deploy in practice
Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - Inefficient algorithms: $O(V^3)$ or $O(V^2 \log(E))$

- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes
Routing: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 \log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes
Routing: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 \log(E))$

- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes
**Routing**: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 \log(E))$

- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes
Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 \log(E))$

- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes
Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: \( O(V^3) \) or \( O(V^2 \log(E)) \)

- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes
Routing: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 \log(E))$

- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes

![Credit Network Diagram]

**Landmark Universe**
Routing: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 \log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes
Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

➢ Existing systems use the max-flow approach:
  ✗ Inefficient algorithms: $O(V^3)$ or $O(V^2 \log(E))$

➢ Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes
Transaction Value Privacy

\[ \approx \]
Credit Network: Privacy Definitions

Transaction Value Privacy

\[ \approx \]

Transaction Receiver Privacy

\[ \approx \]
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

payment
change link
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

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

Query phase

Challenger

Attacker

payment
change link

+35
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

payment
change link

35
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

35
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

payment
change link
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

Challenge phase
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

Challenge phase

-30
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Payment

Attacker

Challenge phase

Balancing transaction
Transaction Value Privacy: Definition (I)

Query phase

Challenge phase

Challenger

Attacker

5

35

payment

change link

5

30

55

-30
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

Challenge phase
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

Challenge phase

payment
change link
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

Challenge phase

Query phase
Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

Challenge phase

Query phase

Guess phase

payment
change link
A credit network satisfies transaction value privacy if:

\[
\text{Challenge transaction is } -30 
\]

\[
\text{Balancing transaction} 
\]

\[
\text{Challenge transaction} 
\]

\[
\text{Balancing transaction} 
\]

\[
\text{Challenge transaction} 
\]

\[
\text{Balancing transaction} 
\]

\[
\text{Challenge transaction} 
\]
Credit Network: Privacy Challenge

Providing privacy is challenging:

➢ Hide transaction values → What is the paid amount?
➢ Hide transaction participants → Who are the sender and the receiver?

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>nwctTPlKZqK59f1fXp0q0L...</td>
<td>rMnvZ9maLmp5cAvmqBECZL...</td>
<td>380/XRP</td>
</tr>
<tr>
<td>rL5p5quS8KbbYvJTXt1c5...</td>
<td>rKo0t7VLB3AKJ2ewLYRzE...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r42G9fSSmD4SYmDra16L...</td>
<td>rBeToNo4AwhKvRB2n4BNC...</td>
<td>0.6693402789148/CK/ /R...</td>
</tr>
<tr>
<td>rhD759dBMrzMNIL4qbgvQe9L...</td>
<td>r9SpwKA1K55fy7EJWrq1j9b...</td>
<td>300/XRP</td>
</tr>
<tr>
<td>r42W3G6V99I3aHt30cF8Cnx...</td>
<td>rBeToNo4AwhKvRB2n4BNC...</td>
<td>0.8821858628231/CK/ /R...</td>
</tr>
<tr>
<td>rUnr1p7xkuSBxyQgEospZS...</td>
<td>r3H4rynDShFP86WuJcadL...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7Uf6yzCe2wJxdlUeZHL...</td>
<td>rBwdzjzHmouLkJ5SJ3d3x...</td>
<td>180/XRP</td>
</tr>
<tr>
<td>rpVZf9STUXBckBSZS25NL...</td>
<td>rDGaanSBnWyfsxUYhCk1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>
Credit Network: Privacy Challenge

Providing privacy is challenging:

➢ Hide transaction values → What is the paid amount?
➢ Hide transaction participants → Who are the sender and the receiver?

In our approach, credit network information

- stored on untrusted server,
- accessed obliviously,
- using trusted hardware
PrivPay: Overview

Service Provider

Credit Network

Landmark Universe

Transaction

Universe Creator

Clients
PrivPay: Overview

Service Provider

Credit Network

Landmark Universe

Transaction

Universe Creator

Secure Processor

Clients
PrivPay: Overview

Service Provider

Credit Network

Landmark Universe

Transaction

Universe Creator

Clients
PrivPay: Universe Creator

Credit Network

Landmark Universe

Universe Creator
PrivPay: Universe Creator

Credit Network | Landmark Universe
---|---

Universe Creator

LANDMARK UNIVERSE

Landmark 1

Landmark k
PrivPay: Universe Creator

**ObliBFS:** Standard BFS augmented with ORAM to ensure that “no information is leaked”
PrivPay: Universe Creator

ObliBFS: Standard BFS augmented with ORAM to ensure that “no information is leaked”

$G, G'$: input graphs of the same size
PrivPay: Universe Creator

**ObliBFS**: Standard BFS augmented with ORAM to ensure that “no information is leaked”

$G, G'$: input graphs of the same size

$A(G)$: sequence of ObliBFS memory accesses
ObliBFS: Standard BFS augmented with ORAM to ensure that “no information is leaked”

$G, G'$: input graphs of the same size
$A(G)$: sequence of ObliBFS memory accesses

$$A(G) \approx A(G')$$
PrivPay: Transaction

Credit Network

Landmark Universe

Transaction

Landmark 1
PrivPay: Transaction

Credit Network

Landmark Universe

Transaction

LANDMARK UNIVERSE

Landmark 1

. . .
Oblivious transactions: Transaction algorithm augmented with ORAM to ensure that “no information about input is leaked”
PrivPay: Transaction

Oblivious transactions: Transaction algorithm augmented with ORAM to ensure that “no information about input is leaked”

\[ I(G, U), I'(G', U'): input information \]
Oblivious transactions: Transaction algorithm augmented with ORAM to ensure that “no information about input is leaked”

\[ I(G,U), I'(G',U'): \text{input information} \]
\[ A(I): \text{sequence of oblivious transactions} \]
\[ \text{memory accesses} \]
**PrivPay: Transaction**

**Oblivious transactions:** Transaction algorithm augmented with ORAM to ensure that “no information about input is leaked”

\[ I(G, U), I'(G', U'): \text{input information} \]
\[ A(I): \text{sequence of oblivious transactions} \]
\[ A(I) \approx A(I') \]
PrivPay: Evaluation

➢ We have implemented PrivPay as a multithreaded C++ library
➢ We use Ripple transactions over a period of four months (Oct'13 – Jan'14)
   • network: 14,317 nodes and 14,176 links

<table>
<thead>
<tr>
<th></th>
<th>Non-Private setting [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>Oblivious BFS (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

- We have implemented PrivPay as a multithreaded C++ library
- We use Ripple transactions over a period of four months (Oct'13 – Jan'14)
  - network: 14,317 nodes and 14,176 links

<table>
<thead>
<tr>
<th></th>
<th>Non-Private setting [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>Oblivious BFS (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

- We have implemented PrivPay as a multithreaded C++ library
- We use Ripple transactions over a period of four months (Oct'13 – Jan'14)
  - network: 14,317 nodes and 14,176 links

<table>
<thead>
<tr>
<th></th>
<th>Non-Private setting [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>Oblivious BFS (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)

No false positives

Credit networks have interesting properties and are used in multiple application scenarios.
Credit networks have **interesting properties** and are used in **multiple application scenarios**

Privacy is an **important and challenging problem** in credit networks
Take Home Message

➢ Credit networks have interesting properties and are used in multiple application scenarios

➢ Privacy is an important and challenging problem in credit networks

➢ Define privacy properties for credit networks
Take Home Message

➢ Credit networks have **interesting properties** and are used in **multiple application scenarios**

➢ **Define privacy properties** for credit networks

➢ **PrivPay**: novel architecture combining trusted hardware and oblivious algorithms

➢ **Privacy** is an **important** and **challenging** problem in credit networks
Take Home Message

- Credit networks have **interesting properties** and are used in **multiple application scenarios**

- **Define privacy properties** for credit networks

- **PrivPay**: novel architecture combining trusted hardware and oblivious algorithms

- **Privacy** is an **important and challenging** problem in credit networks

- **PrivPay** is **feasible to deploy** in practice