Listening to and Silencing the Whispers of Ripple: Study and Solutions for Privacy in IOweYou Credit Networks

Pedro Moreno-Sanchez  
Purdue University

Aniket Kate  
Purdue University
Transactions in the real world

Bob → Alice: $100

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

Transactions in the real world

Bob ➔ $100 ➔ Alice

Bob ➔ IOweYou $100 ➔ Alice

A credit network representation

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

Transactions in the real world

Bob → $100 → Alice

IOweYou $100 → Bob

During a hike with Alice & Bob

Dave → $10 → Carol

IOweYou $10 → Dave

A credit network representation

Bob

100

→ Alice

Dave

Carol

Bob

100

→ Alice
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

Bob ➔ $100 ➔ Alice

IOweYou $100 ➔ Bob

Bob ➔ Alice

IOweYou $100 ➔ Bob

During a hike with Alice & Bob

Dave ➔ $10 ➔ Carol

IOweYou $10 ➔ Dave

Dave ➔ Carol

A credit network representation

Bob ➔ 100 ➔ Alice

Dave ➔ Carol

Carol ➔ Bob

Carol ➔ Dave

Dave ➔ Carol
Transactions in the real world

Bob $100 Alice

Bob IOweYou $100 Alice

During a hike with Alice & Bob

Dave $10 Carol

Dave IOweYou $10 Carol

A credit network representation

Bob 110 Alice

Bob 10 Dave

Dave 10 Carol
Credit Network (CN): an Example
Credit Network (CN): an Example
Credit Network (CN): an Example

Bob

Carol

5

Eve

10

30

Dave

15

20

115

Alice

0

5
Credit Network (CN): an Example
Credit Network (CN): an Example

Bob → Eve: 0
Bob → Carol: 0
Eve → Dave: 20
Eve → Alice: 115
Carol → Eve: 20
Dave → Eve: 5
Alice → Eve: 20
Why Credit Networks Matter?

- Sybil-resistant applications
Why Credit Networks Matter?

✦ Sybil-resistant applications
Why Credit Networks Matter?

- Sybil-resistant applications
Why Credit Networks Matter?

- Sybil-resistant applications
Why Credit Networks Matter?

✦ Sybil-resistant applications

Introducing nodes is much easier than drawing trust from well-behaved nodes.
Why Credit Networks Matter?

- Sybil-resistant applications

Introducing nodes is much easier than drawing trust from well-behaved nodes.

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

✦ Sybil-resistant applications

Introducing nodes is much easier than drawing trust from well-behaved nodes

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

✦ Sybil-resistant applications

Introducing nodes is much easier than drawing trust from well-behaved nodes

Misbehaving user’s effect:
- Bounded
- Localized

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

✦ Sybil-resistant applications

Introducing nodes is much easier than drawing trust from well-behaved nodes.

Misbehaving user’s effect:
- Bounded
- Localized

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

- Sybil-resistant applications

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

Introducing nodes is much easier than drawing trust from well-behaved nodes.

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

❖ Sybil-resistant applications

Introducing nodes is much easier than drawing trust from well-behaved nodes

Misbehaving user’s effect:
- Bounded
- Localized

❖ 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 Credit Network
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network

Tx time
Worldwide, inter-currency tx
Integrity

CBW BANK

$ 60

€ 30

$ 60

€ 45

BTC 10

BTC 5

$ 100

$ 100

XID 100

GDW 10

FMM 280

Santander

£ 70

€ 40

£ 30

€ 45

BTC 10

BTC 5

$ 100
Ripple Credit Network

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

- Ripple
- BTC 10
- BTC 5
- GDW 10
- FMM 280
- XYZ 40
- XID 100
- ~ 5 seconds
- Tiny fees
- Worldwide, inter-currency tx
- Integrity
- High fees
- ~ 1 day

- $60
- €30
- €45
- $100
- £70

- CBW BANK
- cross river bank
- Santander
- fidor BANK
- BANK

- Ripple Credit Network
- CUURR
Ripple Credit Network

- **TX time**: ~ 1 day
- **Worldwide, inter-currency tx**: High fees
- **Integrity**: Bank only
- **~ 5 seconds**
- **Tiny fees**
- **Public verifiability**
Ripple Credit Network

- $1M trade volume
- Several banks use Ripple in production

Tx time: ~5 seconds
Worldwide, inter-currency tx
Public verifiability

High fees
Tiny fees

Integrity
Bank only
Cryptocurrencies vs Credit Networks

We already have cryptocurrencies, then why do we need credit networks?
**Cryptocurrencies vs Credit Networks**

We already have cryptocurrencies, then why do we need credit networks?

<table>
<thead>
<tr>
<th>Definition</th>
<th>Cryptocurrencies</th>
<th>IOU Credit Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Currency</td>
<td>Transaction network</td>
</tr>
</tbody>
</table>
Cryptocurrencies vs Credit Networks

We already have cryptocurrencies, then why do we need credit networks?

<table>
<thead>
<tr>
<th>Definition:</th>
<th>Cryptocurrencies</th>
<th>IOU Credit Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Currency</td>
<td>Transaction network</td>
</tr>
<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>
</tbody>
</table>
# Cryptocurrencies vs Credit Networks

We already have cryptocurrencies, then why do we need credit networks?

<table>
<thead>
<tr>
<th></th>
<th>Cryptocurrencies</th>
<th>IOU Credit Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition:</strong></td>
<td>Currency</td>
<td>Transaction network</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>Scalability:</strong></td>
<td>Limited transaction rate (&lt; 100 tps)</td>
<td>Highly scalable</td>
</tr>
</tbody>
</table>
## Cryptocurrencies vs Credit Networks

We already have cryptocurrencies, then why do we need credit networks?

<table>
<thead>
<tr>
<th></th>
<th>Cryptocurrencies</th>
<th>IOU Credit Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition:</strong></td>
<td>Currency</td>
<td>Transaction network</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>Scalability:</strong></td>
<td>Limited transaction rate (&lt; 100 tps)</td>
<td>Highly scalable</td>
</tr>
</tbody>
</table>

Public verifiability of transactions
Attacks on Privacy of Ripple Links & Transactions

Ripple provides **pseudonymity** to its users by employing public-key hashes as identities.
Is privacy a real problem in Ripple?

Privacy attacks: *Innocent until proven guilty*

P. Moreno-Sanchez, M. B. Zafar, A. Kate:
*Linking Wallets and Deanonymizing Transactions in the Ripple Network.*
*PETS ’16.*
Heuristic 1: The Tale of Two Public Logs

Bitcoin

Ripple

Only €!
Heuristic 1: The Tale of Two Public Logs

<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

Only €!
## Heuristic 1: The Tale of Two Public 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></th>
<th>DR-Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>Alice-Ripple</td>
</tr>
<tr>
<td>Receiver</td>
<td>Bob —&gt; Alice</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

---

**Only €!**
Heuristic 1: The Tale of Two Public 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>

### 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>

---

Only €!
Heuristic 1: The Tale of Two Public 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>

### 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>

Only €!
Heuristic 1: The Tale of Two Public 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>

**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>

Alice

DR-Bitcoin

DR-Ripple

Bob

Dividend

Rippler

Only €!

This is only the tip of the iceberg!
Heuristic 1: The Tale of Two Public Logs

<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

✦

This is only the tip of the iceberg!

Link wallets across payment systems!

Bitcoin

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 → Alice</td>
</tr>
</tbody>
</table>

Only €!

✧ This is only the tip of the iceberg!
Heuristic 2: Hot-Cold Wallets

€ 100,000
Heuristic 2: Hot-Cold Wallets

€ 100,000
Heuristic 2: Hot-Cold Wallets

€ 40
Heuristic 2: Hot-Cold Wallets

€ 20
Heuristic 2: Hot-Cold Wallets

€ 20
Heuristic 2: Hot-Cold Wallets

€ 150
Heuristic 2: Hot-Cold Wallets

Ripple network:

€ 150

€ 2300

€ 5500
Heuristic 2: Hot-Cold Wallets

Ripple network:

- €150
- €2300
- €5500

Cold

BITSTAMP

Bank

Restaurant
Heuristic 2: Hot-Cold Wallets

Ripple network:

€ 150

€ 200

€ 5500

€ 2300

Cold

BITSTAMP

BITSTAMP
Heuristic 2: Hot-Cold Wallets

Ripple network:

- € 150
- € 2300
- € 200
- € 5500

Hot

Cold
Heuristic 2: Hot-Cold Wallets

Ripple network:

- €150

- €2300

- €5500

- €200
Heuristic 2: Hot-Cold Wallets

Ripple network:

Link hot and cold wallets!!
Heuristic 2: Our Approach

- Correlation between network topology and transactions

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>
Heuristic 2: Our Approach

- Correlation between network topology and transactions

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>

- Cold wallet only issues credit
Heuristic 2: Our Approach

- Correlation between network topology and transactions

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>

- Cold wallet only issues credit
Heuristic 2: Our Approach

- Correlation between network topology and transactions

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>

- Cold wallet only issues credit
Heuristic 2: Our Approach

- Correlation between network topology and transactions

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>

- Cold wallet only issues credit
- Cold wallet must top off hot wallet
Heuristic 2: Our Approach

- Correlation between network topology and transactions

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>

- Cold wallet only issues credit
- Cold wallet must top off hot wallet
Heuristic 2: Our Approach

- Correlation between network topology and transactions

Cold wallet only issues credit
- Cold wallet must top off hot wallet

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>
Heuristic 2: Our Approach

- Correlation between network topology and transactions

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>

- Cold wallet only issues credit
- Cold wallet must top off hot wallet
- Hot wallet used to fund client wallets
Heuristic 2: Our Approach

- Correlation between network topology and transactions

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>

- Cold wallet only issues credit
- Cold wallet must top off hot wallet
- Hot wallet used to fund client wallets
Heuristic 2: Our Approach

- Correlation between network topology and transactions

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>

- Cold wallet only issues credit
- Cold wallet must top off hot wallet
- Hot wallet used to fund client wallets
Heuristic 2: Our Approach

- Correlation between network topology and transactions

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>€275</td>
</tr>
<tr>
<td>B</td>
<td>D</td>
<td>€30</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>€10</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>€45</td>
</tr>
</tbody>
</table>

- Cold wallet only issues credit
- Cold wallet must top off hot wallet
- Hot wallet used to fund client wallets

A, B belong to the same user
Transactions in the Ripple Network Linked to Gateways (Jan-13 — Dec-15)

- **Known**
- **Deanonymized**

**Unknown transactions**

- **Sharing the same owner**

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Known</th>
<th>Deanonymized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitstamp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RippleFox</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SnapSwap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chriswen</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dividend</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rippler</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DYM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Motivating an Interesting Research Field
Motivating an Interesting Research Field

✈️ I worked as an intern at Ripple
   ✈️ This work triggered discussions on privacy
   ✈️ Banks are strongly demanding privacy
   ✈️ Ripple community is concerned about privacy
Motivating an Interesting Research Field

✧ I worked as an intern at Ripple
  ✧ This work triggered discussions on privacy
  ✧ Banks are strongly demanding privacy
  ✧ Ripple community is concerned about privacy

✧ Going on discussions on Ripple forums
Motivating an Interesting Research Field

- I worked as an intern at Ripple
  - This work triggered discussions on privacy
  - Banks are strongly demanding privacy
  - Ripple community is concerned about privacy

- Going on discussions on Ripple forums

- Inspire the use of PETs in credit networks
Towards privacy-preserving transactions in credit networks

What does it mean privacy in credit networks?

P. Moreno-Sanchez, A. Kate, M. Maffei, K. Pecina: Privacy Preserving Payments in Credit Networks
NDSS ‘15
Defining Privacy for a Credit Network

Transaction value privacy

\[ \approx \]

Transaction receiver privacy

\[ \approx \]

Transaction sender privacy can be defined similarly
Our Centralized Approach

PrivPay [NDSS ’15]

- A server maintains the CN. Privacy challenge even if CN encrypted
- We use minimal trusted hardware and oblivious algorithms
- Provides strong privacy guarantees for the first time
- Emulate transaction from Ripple
Our Distributed Approach

SilentWhispers [NDSS ’17]
Our Distributed Approach

SilentWhispers [NDSS ’17]

- Links locally stored by users. Net-flow is all that matters!
- No need for privacy-invasive ledger or proof of work
- Strong privacy guarantees
- Emulate transaction from Ripple
What about privacy in Ripple today?

P. Moreno-Sanchez, T. Ruffing, A. Kate:

**PathShuffle: Credit Mixing and Anonymous Payments for Ripple**
[In submission]

Path Mixing for Privacy-preserving Transactions
**Path Mixing for Privacy-preserving Transactions**

- **Idea:** Perform several transactions simultaneously enables privacy-preserving transactions over paths sharing a common node. *PathShuffle*
Path Mixing for Privacy-preserving Transactions

- **Idea**: Perform several transactions simultaneously enables privacy-preserving transactions over paths sharing a common node. PathShuffle
Path Mixing for Privacy-preserving Transactions

**Idea:** Perform several transactions simultaneously enables privacy-preserving transactions over paths sharing a common node. *PathShuffle*
Path Mixing for Privacy-preserving Transactions

- **Idea**: Perform several transactions simultaneously enables privacy-preserving transactions over paths sharing a common node. **PathShuffle**

- **Similar to CoinJoin in Bitcoin**

---

### Coinjoin transaction

<table>
<thead>
<tr>
<th>Input Addresses</th>
<th>Output Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>A (1 BTC)</td>
<td>B’ (1 BTC)</td>
</tr>
<tr>
<td>B (1 BTC)</td>
<td>C’ (1 BTC)</td>
</tr>
<tr>
<td>C (1 BTC)</td>
<td>A’ (1 BTC)</td>
</tr>
</tbody>
</table>

- Alice
- Bob
- Carol

---
Path Mixing for Privacy-preserving Transactions

- **Idea**: Perform several transactions simultaneously enables privacy-preserving transactions over paths sharing a common node. **PathShuffle**

![Diagram showing path mixing in Ripple](image)

- **Similar to CoinJoin in Bitcoin**
- **Problem**: Ripple only allows single sender/receiver transactions
  - **Solution**: shared wallets (distributed signatures)

**Coinjoin transaction**

<table>
<thead>
<tr>
<th>Input Addresses</th>
<th>Output Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>A (1 BTC)</td>
<td>B' (1 BTC)</td>
</tr>
<tr>
<td>B (1 BTC)</td>
<td>C' (1 BTC)</td>
</tr>
<tr>
<td>C (1 BTC)</td>
<td>A' (1 BTC)</td>
</tr>
</tbody>
</table>

- **Alice**
- **Bob**
- **Carol**
PathShuffle: Discussion
PathShuffle: Discussion

- It enables atomic transactions:
  - Interesting applications other than privacy (e.g., crowdfunding)
PathShuffle: Discussion

- It enables atomic transactions:
  - Interesting applications other than privacy (e.g., crowdfunding)

- Fully compatible with the Ripple network
  - Successfully tested in the real Ripple network!
  - Compatible with other credit networks (e.g., Stellar)
PathShuffle: Discussion

- It enables atomic transactions:
  - Interesting applications other than privacy (e.g., crowdfunding)

- Fully compatible with the Ripple network
  - Successfully tested in the real Ripple network!
  - Compatible with other credit networks (e.g., Stellar)

- PathShuffle is a simple smart contract
  - However, Ripple does not have script language
  - Are other contracts possible? Limitations?
Next Steps

✧ Other emerging credit networks
  ✧ Stellar is gaining traction
  ✧ https://www.stellar.org/
Next Steps

- Other emerging credit networks
  - Stellar is gaining traction
  - [https://www.stellar.org/](https://www.stellar.org/)

- Bitcoin payment channels and lightning network
  - [http://lightning.network/](http://lightning.network/)
  - Designing privacy-preserving distributed solutions for lightning networks
Next Steps

✦ Other emerging credit networks
  ✦ Stellar is gaining traction
  ✦ https://www.stellar.org/

✦ Bitcoin payment channels and lightning network
  ✦ http://lightning.network/
  ✦ Designing privacy-preserving distributed solutions for lightning networks

✦ I am open for collaborations
Thanks to my Collaborators

Aniket Kate

Matteo Maffei

Muhammad Bilal Zafar

Sonia Fahmy

Tim Ruffing

Kim Pecina

Giulio Malavolta

Srivatsan Ravi
Thanks to my Collaborators

Aniket Kate
Matteo Maffei
Muhammad Bilal Zafar
Sonia Fahmy
Tim Ruffing
Kim Pecina
Giulio Malavolta
Srivatsan Ravi

To make credit networks great again!
Take Home Message
Take Home Message

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

Why Credit Networks?

- Sybil-resistant applications
  - Introducing nodes is much easier than drawing trust from well-behaved nodes
  - Several applications:
    - Ostra: preventing e-mail spam [NSDI’08]
    - Bazaar: strengthening e-commerce [NSDI’11]
    - SumUp: Sybil-resistant content voting [NSDI’09]
    - Ripple: A real-life online settlement network
Take Home Message

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

Why Credit Networks?

✦ Sybil-resistant applications

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 settlement network

✦ Introducing nodes is much easier than drawing trust from well-behaved nodes

Ledgers provide verifiability, but make privacy a real problem in credit networks

The tale of two Public Logs

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

✦ How to link these two events?
Credit networks have interesting properties and can be used in multiple scenarios:

- Sybil-resistant applications
  - 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 settlement network

- Introducing nodes is much easier than drawing trust from well-behaved nodes

- Ledgers provide verifiability, but make privacy a real problem in credit networks

PrivPay, SilentWhispers and PathShuffle: centralized, distributed and compatible solutions to provide privacy-preserving transactions in credit networks

The tale of two Public Logs

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

Our Centralized Approach

- PRIV

Our Decentralized Approach

- PRIV

Path Mixing for Privacy-preserving Transactions

- PRIV

- Similar to Calculus and ColdShuffle in Bitcoin
- Prevents ripple only allows single sender to external transactions
- Solution: shared secrets (predefined signatures)

How to link these two events?
Take Home Message

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

Why Credit Networks?

✦ Sybil-resistant applications
  - Well-behaved nodes
  - Sybil nodes
  - Introducing nodes is much easier than drawing trust from well-behaved nodes

✦ Several applications:
  - Ostra: preventing e-mail spam [NSDI'08]
  - Bazaar: strengthening e-commerce [NSDI'11]
  - SumUp: Sybil-resistant content voting [NSDI'09]
  - Ripple: A real-life online settlement network

PrivPay, SilentWhispers and PathShuffle: centralized, distributed and compatible solutions to provide privacy-preserving transactions in credit networks

Ledgers provide verifiability, but make privacy a real problem in credit networks

Several questions remain unanswered leaving lots of interesting open problems

The tale of two Public Logs

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

<table>
<thead>
<tr>
<th>Sender</th>
<th>DRI-Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice-Bitcoin</td>
<td>Alice-Ripple</td>
</tr>
<tr>
<td>DR-Bitcoin</td>
<td>DR-Ripple</td>
</tr>
</tbody>
</table>

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

How to link these two events?

Next Steps

✦ Other emerging credit networks
  - Stellar is gaining traction
    - https://www.stellar.org/

✦ Bitcoin payment channels and lightning network
  - http://lightning.network/
  - Designing privacy-preserving distributed solutions for lightning networks

✦ I am open for collaborations
Take Home Message

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

Why Credit Networks?

- Sybil-resistant applications
- Several applications:
  - Ostra: preventing e-mail spam [NSDI'08]
  - Bazaar: strengthening e-commerce [NSDI'11]
  - SumUp: Sybil-resistant content voting [NSDI'09]
  - Ripple: A real-life online settlement network

- Ledgers provide verifiability, but make privacy a real problem in credit networks

- Introducing nodes is much easier than drawing trust from well-behaved nodes
- Several questions remain unanswered leaving lots of interesting open problems

Our Centralized Approach

Senders maintain the CN: Privacy challenge where for is not enough
- Can use internal trusted hardware and offline algorithms
- Provides stronger privacy guarantees for the first time
- Includes transaction from Ripple

Our Decentralized Approach

- Similar to Calculus and CreditShuffle in Bitcoin
- Proven: Ripple only allows simple send/Receive transactions
- Includes transaction from Ripple

Next Steps

- Other emerging credit networks
- Stellar is gaining traction
  - https://www.stellar.org/
- Bitcoin payment channels and lightning network
  - http://lightning.network/
- Designing privacy-preserving distributed solutions for lightning networks
- I am open for collaborations

Thanks!
@pedrorechez