PathShuffle: Credit Mixing and Anonymous Payments for Ripple

Pedro Moreno-Sanchez
Purdue University

Tim Ruffing
Saarland University

Aniket Kate
Purdue University
Credit (or IOU Settlement) Networks: Basics
Transactions in the real world

Aniket → Dinner → Pedro

IOweYou $40

Aniket → IOweYou $40 → Pedro
Transactions in the real world:

- Aniket pays Pedro for dinner.
- Aniket owes Pedro $40.

A credit network representation:

- Pedro owes Aniket $40.
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

Aniket

Dinner

Pedro

IOweYou $40

Aniket

Pedro

During a visit from Antonio

Aniket

Beer

Antonio

IOweYou $10

Antonio

A credit network representation

Aniket

Pedro

40

Pedro
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

Aniket ➔ Dinner ➔ Pedro

Aniket ➔ IOweYou $40 ➔ Pedro

Aniket ➔ Beer ➔ Antonio

Aniket ➔ IOweYou $10 ➔ Antonio

A credit network representation

Aniket ➔ 10 → Pedro

Aniket ➔ 40 → Pedro

Pedro ➔ 40 ➔ Aniket

Pedro ➔ 10 ➔ Antonio

Antonio ➔ Pedro
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

- Dinner
  - Aniket → Pedro
  - IOweYou $40
  - Aniket ← Pedro

During a visit from Antonio

- Beer
  - Aniket → Antonio
  - IOweYou $10
  - Aniket ← Antonio

A credit network representation

- Pedro 
  - 50
  - Aniket

- Antonio
  - 10
Ripple Credit Network: an Example of Transaction
Ripple Credit Network: an Example of Transaction

Bob → Eve: 10
Eve → Carol: 5
Eve → Dave: 15
Carol → Dave: 40
Dave → Alice: 115
Ripple Credit Network: an Example of Transaction

Bob

Carol

Eve

Dave

Alice

15

10

5

40

15

20

115
Ripple Credit Network: an Example of Transaction

<table>
<thead>
<tr>
<th>Sender</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td>Carol</td>
</tr>
<tr>
<td>Path1 {10}, Path2 {5}</td>
<td></td>
</tr>
</tbody>
</table>

Sender: Bob
Receiver: Carol
Path1: 10, Path2: 5
Ripple Credit Network: an Example of Transaction

<table>
<thead>
<tr>
<th>Sender</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td>Carol</td>
</tr>
<tr>
<td>Path1 {10}, Path2 {5}</td>
<td></td>
</tr>
</tbody>
</table>

Bob sends 15 units to Carol via Eve.

Carol sends 5 units to Bob via Eve.

Eve sends 0 units to Alice.

Alice sends 20 units to Dave.

Dave sends 115 units to Bob.

Bob sends 40 units to Carol via Eve.

Carol sends 5 units to Bob via Eve.

Eve sends 15 units to Alice.

Alice sends 20 units to Dave.

Dave sends 115 units to Bob.
Ripple Credit Network: an Example of Transaction

<table>
<thead>
<tr>
<th>Sender</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td>Carol</td>
</tr>
<tr>
<td>Path1 {10}, Path2 {5}</td>
<td></td>
</tr>
</tbody>
</table>

Bob

Sender: Bob
Receiver: Carol
Path1: 10, Path2: 5
Ripple Credit Network: an Example of Transaction

<table>
<thead>
<tr>
<th>Sender</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td>Carol</td>
</tr>
<tr>
<td>Path1 {10}, Path2 {5}</td>
<td></td>
</tr>
</tbody>
</table>

Bob → Carol: 15
Carol → Bob: 5
Bob → Eve: 0
Eve → Alice: 20
Alice → Dave: 115
Dave → Bob: 50
Ripple Credit Network: an Example of Transaction

<table>
<thead>
<tr>
<th>Sender</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td>Carol</td>
</tr>
<tr>
<td>Path1</td>
<td>{10}, Path2</td>
</tr>
</tbody>
</table>

Bob

Sender

Receiver

Path1

Path2

Eve

Bob

Carol

Dave

Alice

Sender

Receiver

Path1

Path2

Eve

Bob

Carol

Dave

Alice

Sender

Receiver

Path1

Path2

Eve

Bob

Carol

Dave

Alice

Sender

Receiver

Path1

Path2
Ripple Credit Network: an Example of Transaction

Bob

Carol

Eve

Dave

Alice

0

20

25

50

115
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network
Ripple Credit Network

- AED 10 → Reise Bank
- £30 → Reise Bank
- £45 → RBS
- $60 → CBW Bank
- CAD 100 → RBC
- £70 → RBS
Ripple Credit Network

AED 10 → Reise Bank

$60 → CBW BANK

CAD 100 → RBC

BTC 10 → BTC 5

£70
Ripple Credit Network

- AED 10
- $ 60
- CAD 100
- Coffee 4
- Meal 10
- Books 2
- Car rides 3

- Reise Bank
- BTC 10
- BTC 5
- Ripple Credit Network

- CBW BANK
- $ 45
- £ 30
- £ 70

- RBS
Ripple can significantly improve cross-currency remittance and settlements.
Public Verifiability & Privacy Problem

The Ripple Ledger
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rwvctTPLKZqKS9f1fXpDkQ...</td>
<td>rMnVZ9maUWp5cAvmqBECZML...</td>
<td>360/XRP</td>
</tr>
<tr>
<td>rLSBpSquSHkbfvcKt1c54...</td>
<td>rKoDt7VL83AKJZewLxVZeS...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r42bg9fSSmD4SM6mDra168...</td>
<td>rBeToNo4AhHaNBX2n4BNc...</td>
<td>8.0693402789148/CCK/rBL...</td>
</tr>
<tr>
<td>rhD759dBMrzPNL4QqvQe9...</td>
<td>r95pWKA1KS5thy7f3Jr5qJ9h...</td>
<td>360/XRP</td>
</tr>
<tr>
<td>r4zWJGv9MJF7S550CfCnx...</td>
<td>rBeToNo4AhHaNBX2n4BNc...</td>
<td>8.082105828231/CCK/rBL...</td>
</tr>
<tr>
<td>rU1l8r17xku5BxyAgHEopZ5...</td>
<td>r3H4rynD5HMKpXuHcadLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7UfGvZeWJxUEeZHLG...</td>
<td>rBwJt2z2MwnolKL5OJD3xd...</td>
<td>160/XRP</td>
</tr>
<tr>
<td>rpVZfSTUX9CrBSS2Z5W...</td>
<td>rDCgaaSBAWYfsxUYyHck1n2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>

Credit Graph
Public Verifiability & Privacy Problem

The Ripple Ledger

<table>
<thead>
<tr>
<th>Account</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>rwvctTPLKZqKS9f1fXpDkQ...</td>
<td>rMnVZ9maUWp5cAvmqBEC2ML...</td>
<td>380/XRP</td>
</tr>
<tr>
<td>rLSBpSquSHKbfbvctKt1c54...</td>
<td>rKoD7VL83AKJZewLxVZEes...</td>
<td>75/XRP</td>
</tr>
<tr>
<td>r42B69f5SmD4SyDra16BL...</td>
<td>rBeToNo4AvHaNbRX2n4BC...</td>
<td>8.0693402789148/CKK/rB...</td>
</tr>
<tr>
<td>rhD759dBJMrZM4NL4QbVQe9...</td>
<td>r95pWA1K55fy7EJWqJ9b...</td>
<td>380/XRP</td>
</tr>
<tr>
<td>r4ZWHVv9W9Ja4t50CF6BzN...</td>
<td>rBeToNo4AvHaNbRX2n4BC...</td>
<td>8.0821658828231/CKK/rB...</td>
</tr>
<tr>
<td>rUnr1p7xku5BxyAqHeopZ5...</td>
<td>r3H4ynD5HfMRKWiJcdLY...</td>
<td>1129.916679154465/EUR/...</td>
</tr>
<tr>
<td>rw7Uf6vzCeZwJxxUEeZHLG...</td>
<td>rBwTDzzHn0uL5SOJD3xd...</td>
<td>160/XRP</td>
</tr>
<tr>
<td>rPVzFSTUJX9CrKBSS2Z5W...</td>
<td>rDCgaaSBAYFsxyYhCkln2...</td>
<td>999.99/XRP</td>
</tr>
</tbody>
</table>

Credit Graph

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

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

PETS ’16
Can we achieve anonymous payments in the current Ripple network?

## Related Work

### Privacy Preserving Credit Networks

<table>
<thead>
<tr>
<th>Privacy Preserving Payments in Credit Networks</th>
<th>SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, Kim Pecina</td>
<td>Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei</td>
</tr>
<tr>
<td>NDSS ‘15</td>
<td>NDSS ‘17</td>
</tr>
</tbody>
</table>
Related Work

Privacy Preserving Credit Networks

Privacy Preserving Payments in Credit Networks
Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, Kim Pecina
NDSS ‘15

SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks
Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei
NDSS ‘17

Require structural changes in the Ripple network
Privacy Preserving Credit Networks

Privacy Preserving Payments in Credit Networks
Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, Kim Pecina
NDSS ‘15

SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks
Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei
NDSS ‘17

Require structural changes in the Ripple network

Privacy Preserving Cryptocurrencies
Monero, Zcash, …
Related Work

Privacy Preserving Credit Networks

<table>
<thead>
<tr>
<th>Privacy Preserving Payments in Credit Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, Kim Pecina</td>
</tr>
<tr>
<td>NDSS ’15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei</td>
</tr>
<tr>
<td>NDSS ’17</td>
</tr>
</tbody>
</table>

Require structural changes in the Ripple network

Privacy Preserving Cryptocurrencies

Monero, Zcash, …

Solutions tied to cryptocurrencies:
- Specific cryptographic algorithms
Related Work

Privacy Preserving Credit Networks

Privacy Preserving Payments in Credit Networks
Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, Kim Pecina
NDSS ‘15

SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks
Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei
NDSS ‘17

Require structural changes in the Ripple network

Privacy Preserving Cryptocurrencies
Monero, Zcash, …

Solutions tied to cryptocurrencies:
- Specific cryptographic algorithms

Bitcoin Mixing (CoinJoin)

<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
Path Mixing for Privacy-preserving Transactions

**Idea:** Transaction paths sharing a common node can be mixed.
Path Mixing for Privacy-preserving Transactions

- **Idea**: Transaction paths sharing a common node can be mixed.
- **Goal**: Hide who pays to whom (unlinkability) from an adversary who controls up to (n-2) input wallets.
Path Mixing for Privacy-preserving Transactions

✦ **Idea:** Transaction paths sharing a common node can be mixed

✦ **Goal:** Hide who pays to whom (unlinkability) from an adversary who controls up to \((n-2)\) input wallets
Path Mixing for Privacy-preserving Transactions

- **Idea**: Transaction paths sharing a common node can be mixed
- **Goal**: Hide who pays to whom (unlinkability) from an adversary who controls up to (n-2) input wallets
Path Mixing for Privacy-preserving Transactions

- **Idea**: Transaction paths sharing a common node can be mixed
- **Goal**: Hide who pays to whom (unlinkability) from an adversary who controls up to \((n-2)\) input wallets

- Multi-input-multi-output (CoinJoin) transaction: Not supported in Ripple.
Path Mixing for Privacy-preserving Transactions

- **Idea:** Transaction paths sharing a common node can be mixed
- **Goal:** Hide who pays to whom (unlinkability) from an adversary who controls up to \( (n-2) \) input wallets

- **Multi-input-multi-output (CoinJoin) transaction:** Not supported in Ripple.
- **Atomicity problem:** Who sends first?
Key Idea: Synchronization Using Shared Wallets

- **Shared Wallet**: Using a distributed signature scheme to share the ownership of the wallet
Key Idea: Synchronization Using Shared Wallets

- **Shared Wallet**: Using a distributed signature scheme to share the ownership of the wallet
**Key Idea: Synchronization Using Shared Wallets**

- **Shared Wallet**: Using a distributed signature scheme to share the ownership of the wallet.
Key Idea: Synchronization Using Shared Wallets

- **Shared Wallet:** Using a distributed signature scheme to share the ownership of the wallet.
Key Idea: Synchronization Using Shared Wallets

- **Shared Wallet**: Using a distributed signature scheme to share the ownership of the wallet
Key Idea: Synchronization Using Shared Wallets

- **Shared Wallet**: Using a distributed signature scheme to share the ownership of the wallet

![Diagram showing synchronization using shared wallets]
Key Idea: Synchronization Using Shared Wallets

- **Shared Wallet**: Using a distributed signature scheme to share the ownership of the wallet.
Key Idea: Synchronization Using Shared Wallets

✦ **Shared Wallet**: Using a distributed signature scheme to share the ownership of the wallet

✦ The atomicity problem persists
  ✦ Who sends first to the shared wallet?
  ✦ Funds can be locked
Our Protocol for Atomic Transactions: PathJoin
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
  - Pre-fund the input and output shared wallets (e.g., mix 10 credit)
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
  - Pre-fund the input and output shared wallets (e.g., mix 10 credit)
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
  - Pre-fund the input and output shared wallets (e.g., mix 10 credit)
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
- Pre-fund the input and output shared wallets (e.g., mix 10 credit)
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
- Pre-fund the input and output shared wallets (e.g., mix 10 credit)
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
  - Pre-fund the input and output shared wallets (e.g., mix 10 credit)
  - Perform the mixing transaction
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
  - Pre-fund the input and output shared wallets (e.g., mix 10 credit)
  - Perform the mixing transaction
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
  - Pre-fund the input and output shared wallets (e.g., mix 10 credit)
  - Perform the mixing transaction
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
  - Pre-fund the input and output shared wallets (e.g., mix 10 credit)
  - Perform the mixing transaction
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
  - Pre-fund the input and output shared wallets (e.g., mix 10 credit)
  - Perform the mixing transaction
Our Protocol for Atomic Transactions: PathJoin

- Two shared wallets (two rounds of synchronization suffice)
  - Pre-fund the input and output shared wallets (e.g., mix 10 credit)
  - Perform the mixing transaction

Diagram:

- A/B/C
- B
- C
- Gateway
- A'/B'/C'
- C'
- B'
- A'
PathShuffle: PathJoin + DiceMix
PathShuffle: PathJoin + DiceMix

- Atomic transactions (PathJoin) alone do not suffice
  - How to know the output wallets in the first place?
PathShuffle: PathJoin + DiceMix

- Atomic transactions (PathJoin) alone do not suffice
  - How to know the output wallets in the first place?
- We require:
  - Mechanism to find participants (bootstrapping)
PathShuffle: PathJoin + DiceMix

✦ Atomic transactions (PathJoin) alone do not suffice
  ✦ How to know the output wallets in the first place?
✦ We require:
  ✦ Mechanism to find participants (bootstrapping)
  ✦ Anonymously construct the list of output wallets (DiceMix)
PathShuffle: PathJoin + DiceMix

- Atomic transactions (PathJoin) alone do not suffice
  - How to know the output wallets in the first place?
- We require:
  - Mechanism to find participants (bootstrapping)
  - Anonymously construct the list of output wallets (DiceMix)

P2P Mixing and Unlinkable Bitcoin Transactions

Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate.

NDSS ‘17
PathShuffle: PathJoin + DiceMix

- Atomic transactions (PathJoin) alone do not suffice
  - How to know the output wallets in the first place?
- We require:
  - Mechanism to find participants (bootstrapping)
  - Anonymously construct the list of output wallets (DiceMix)
Discussion

✦ PathJoin enables atomic transactions
  ✦ Interesting applications other than privacy (e.g., crowdfunding)
  ✦ Discussion on forums (e.g., ICO):
    https://www.xrpchat.com/topic/6879-pathjoin/
Discussion

✦ PathJoin enables atomic transactions
  ✦ Interesting applications other than privacy (e.g., crowdfunding)
  ✦ Discussion on forums (e.g., ICO):
    https://www.xrpchat.com/topic/6879-pathjoin/

✦ PathShuffle enables path mixing in the Ripple network
  ✦ Successfully tested in the real Ripple network!
  ✦ Compatible with other credit networks (e.g., Stellar)
PathJoin enables atomic transactions

- Interesting applications other than privacy (e.g., crowdfunding)
- Discussion on forums (e.g., ICO):
  https://www.xrpchat.com/topic/6879-pathjoin/

PathShuffle enables path mixing in 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 “scriptless” contracts possible? Limitations?
Take Home Message
Take Home Message

✦ Credit Networks (e.g., Ripple) allow **worldwide, fast, cheap, cross-currency transactions**
Take Home Message

✦ Credit Networks (e.g., Ripple) allow worldwide, fast, cheap, cross-currency transactions

✦ There exist privacy breaches because of the publicly available Ripple ledger
Credit Networks (e.g., Ripple) allow worldwide, fast, cheap, cross-currency transactions.

There exist privacy breaches because of the publicly available Ripple ledger.

PathJoin: protocol for atomic payments in Ripple with interesting applications.
Credit Networks (e.g., Ripple) allow worldwide, fast, cheap, cross-currency transactions.

There exist privacy breaches because of the publicly available Ripple ledger.

PathJoin: protocol for atomic payments in Ripple with interesting applications.

PathShuffle: protocol for anonymous payments fully compatible with current Ripple.
Credit Networks (e.g., Ripple) allow worldwide, fast, cheap, cross-currency transactions.

There exist privacy breaches because of the publicly available Ripple ledger.

PathJoin: protocol for atomic payments in Ripple with interesting applications.

PathShuffle: protocol for anonymous payments fully compatible with current Ripple.

Thanks! @pedrorechez