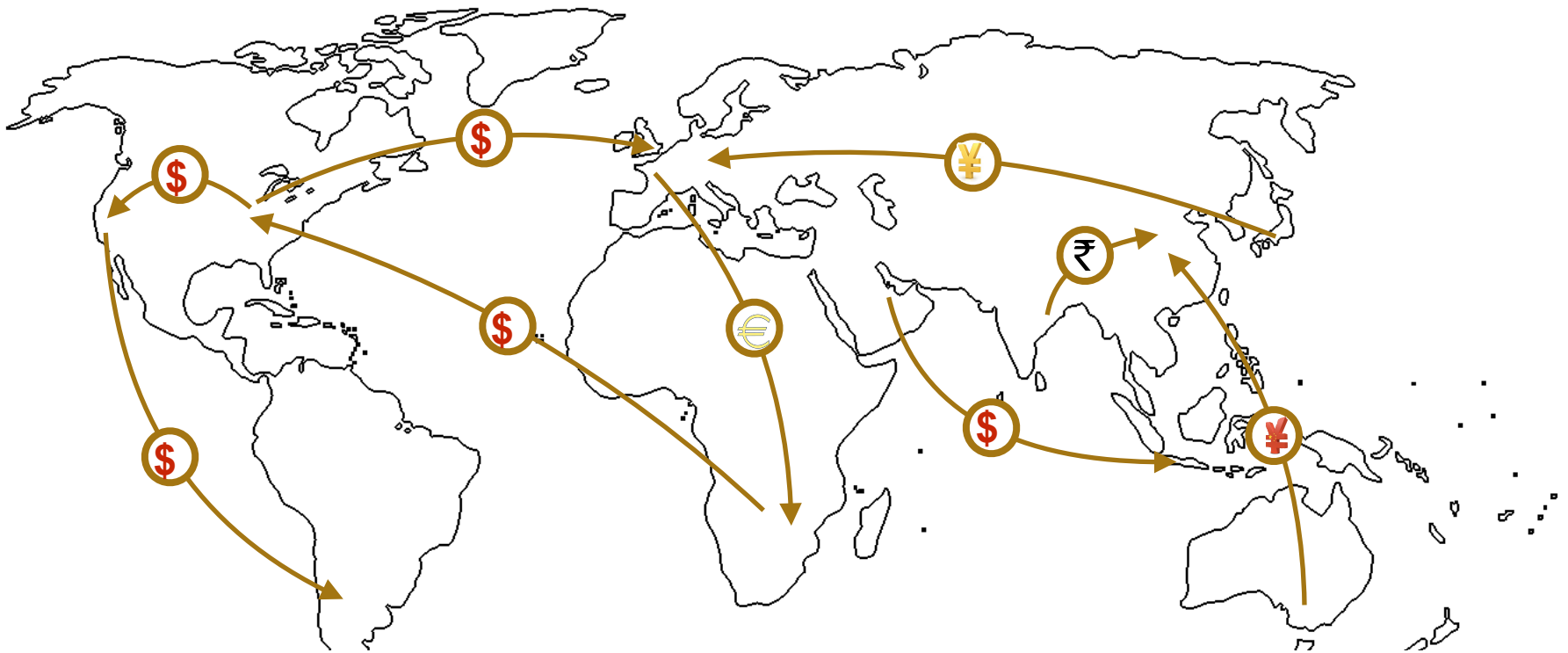


PathShuffle: Credit Mixing and Anonymous Payments for Ripple



Pedro Moreno-Sanchez
Purdue University

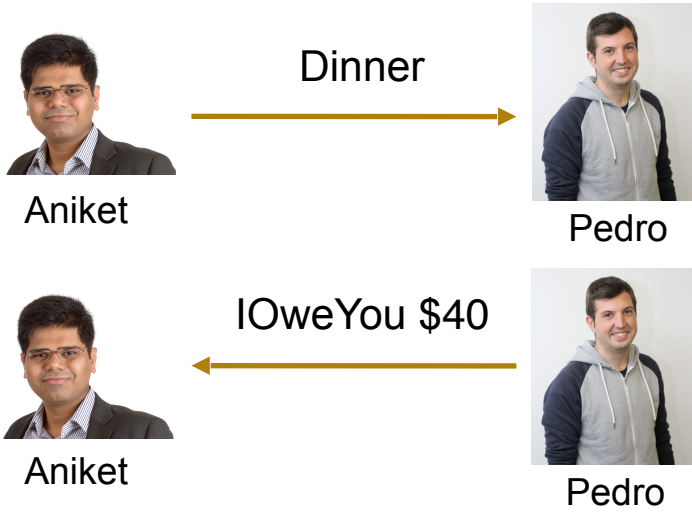
Tim Ruffing
Saarland University

Aniket Kate
Purdue University

Credit (or IOU Settlement) Networks: Basics

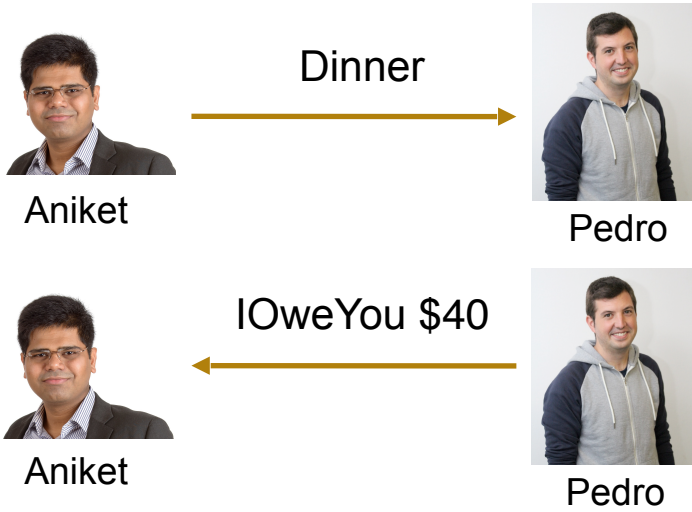
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

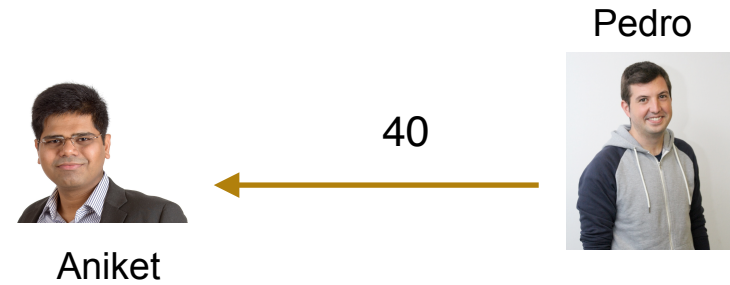


Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

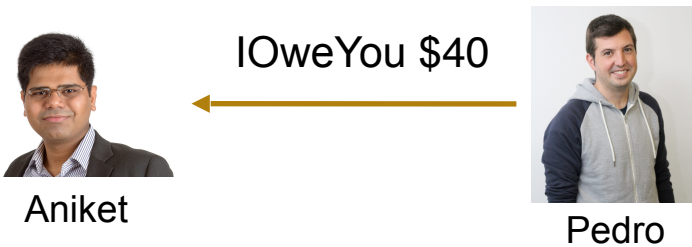
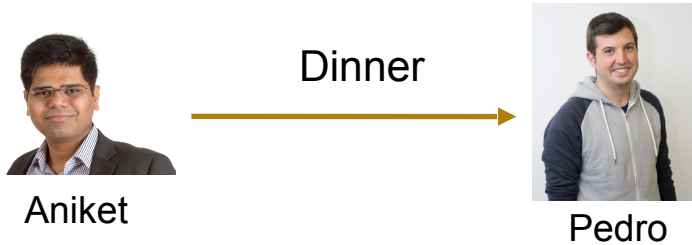


A credit network representation

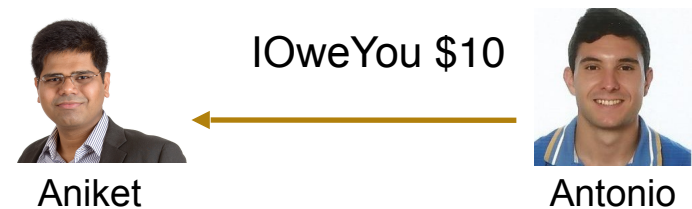


Credit (or IOU Settlement) Networks: Basics

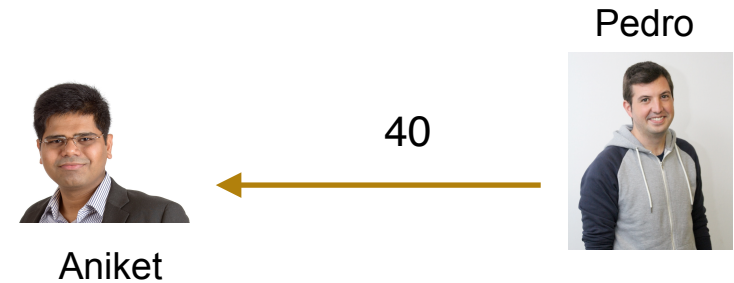
Transactions in the real world



During a visit from Antonio

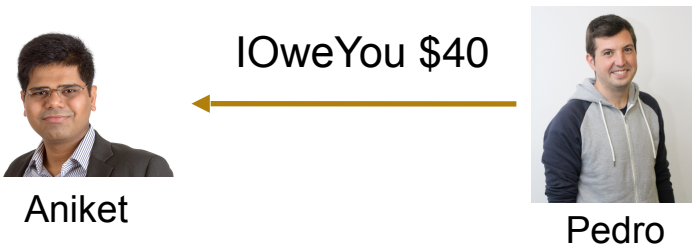
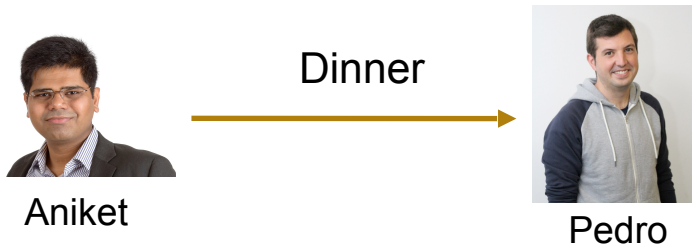


A credit network representation

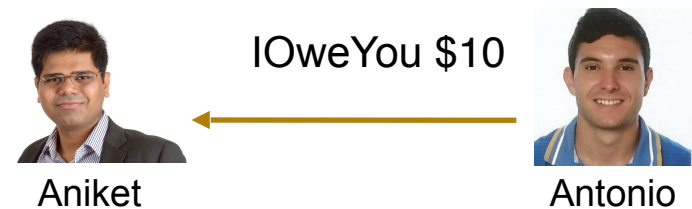


Credit (or IOU Settlement) Networks: Basics

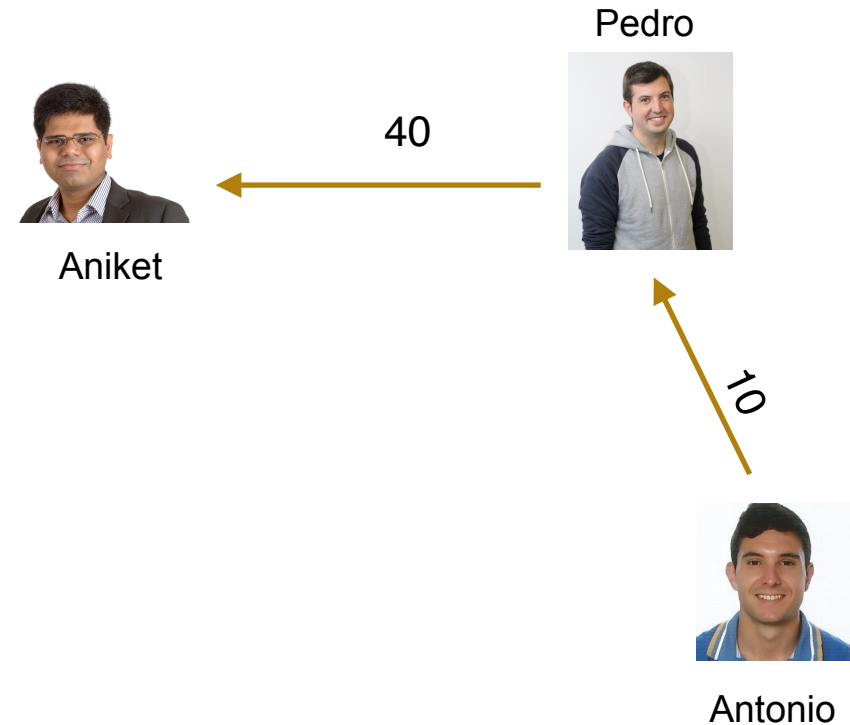
Transactions in the real world



During a visit from Antonio

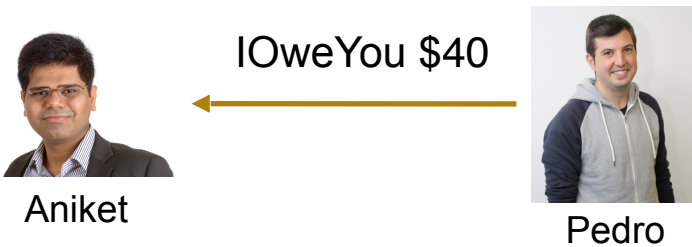
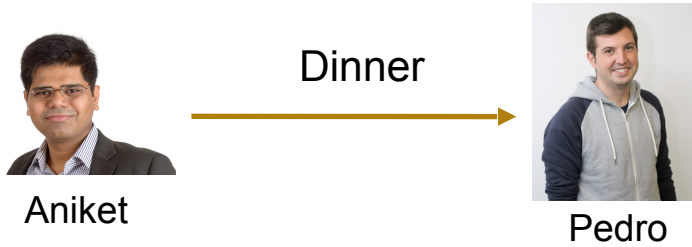


A credit network representation

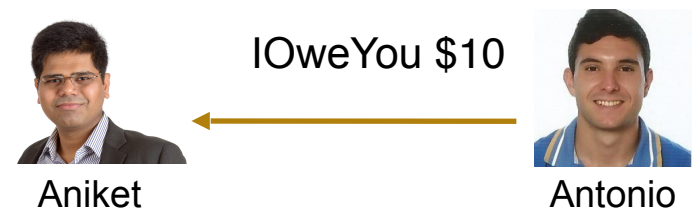


Credit (or IOU Settlement) Networks: Basics

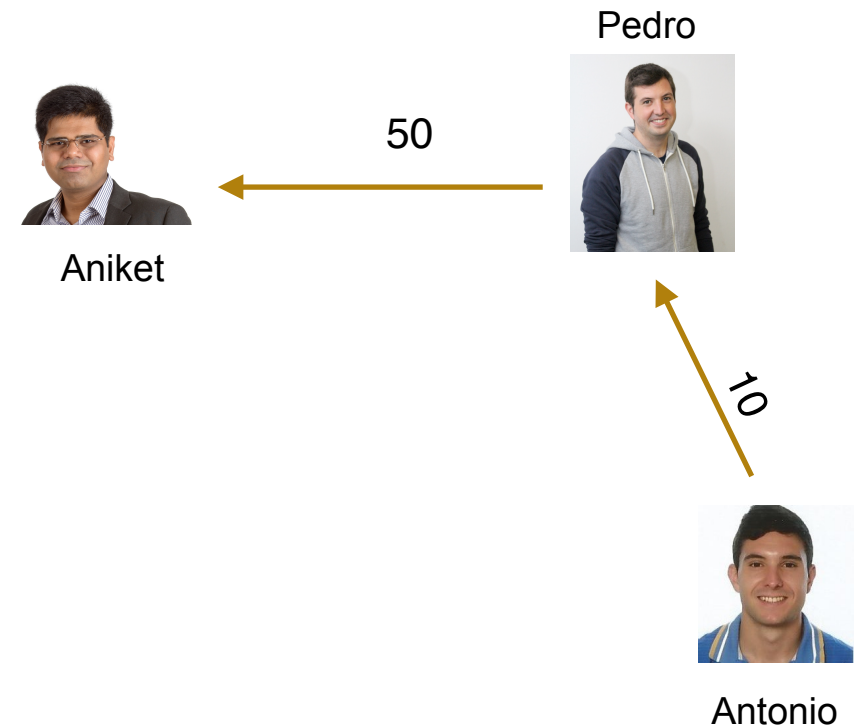
Transactions in the real world



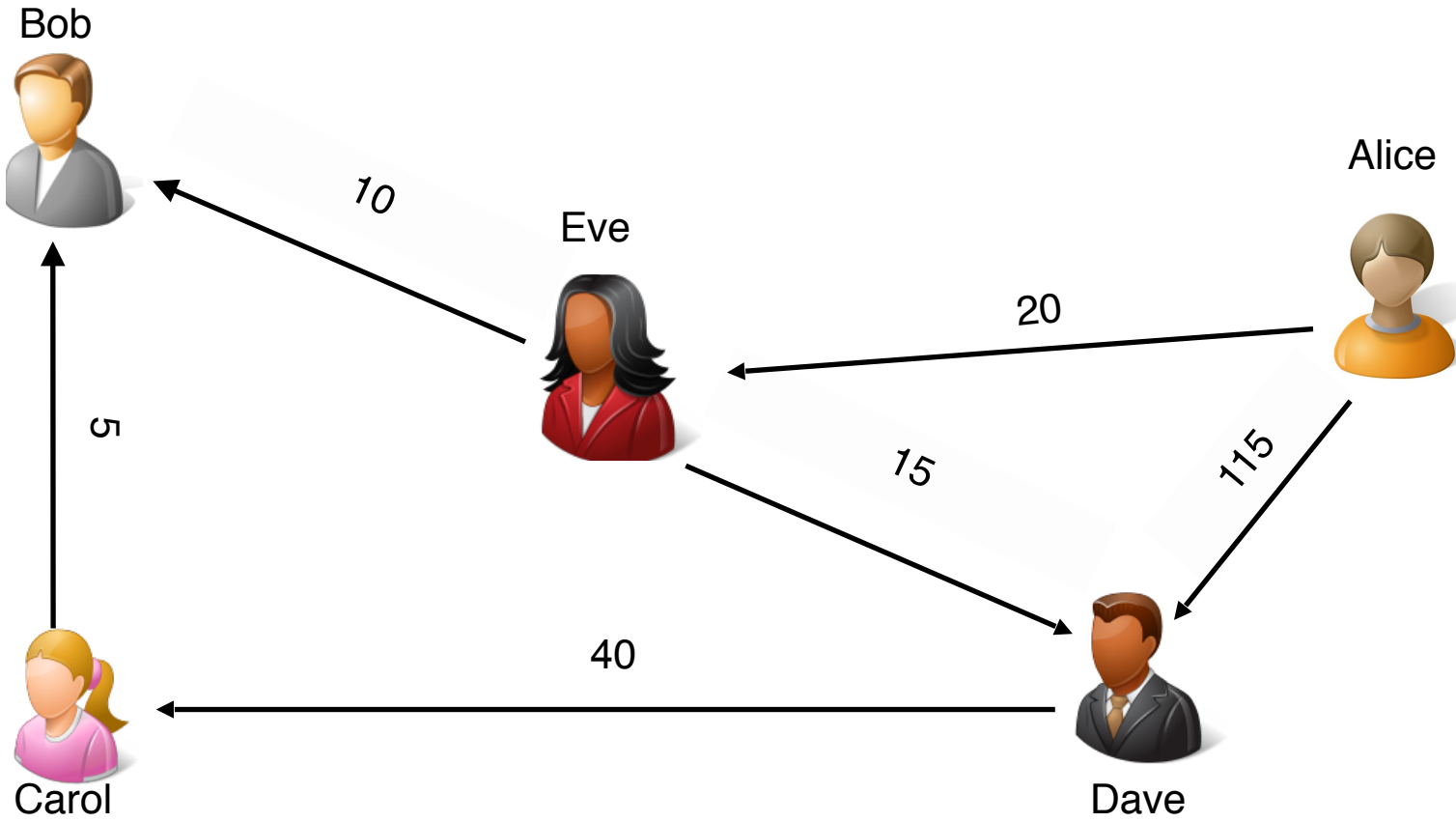
During a visit from Antonio



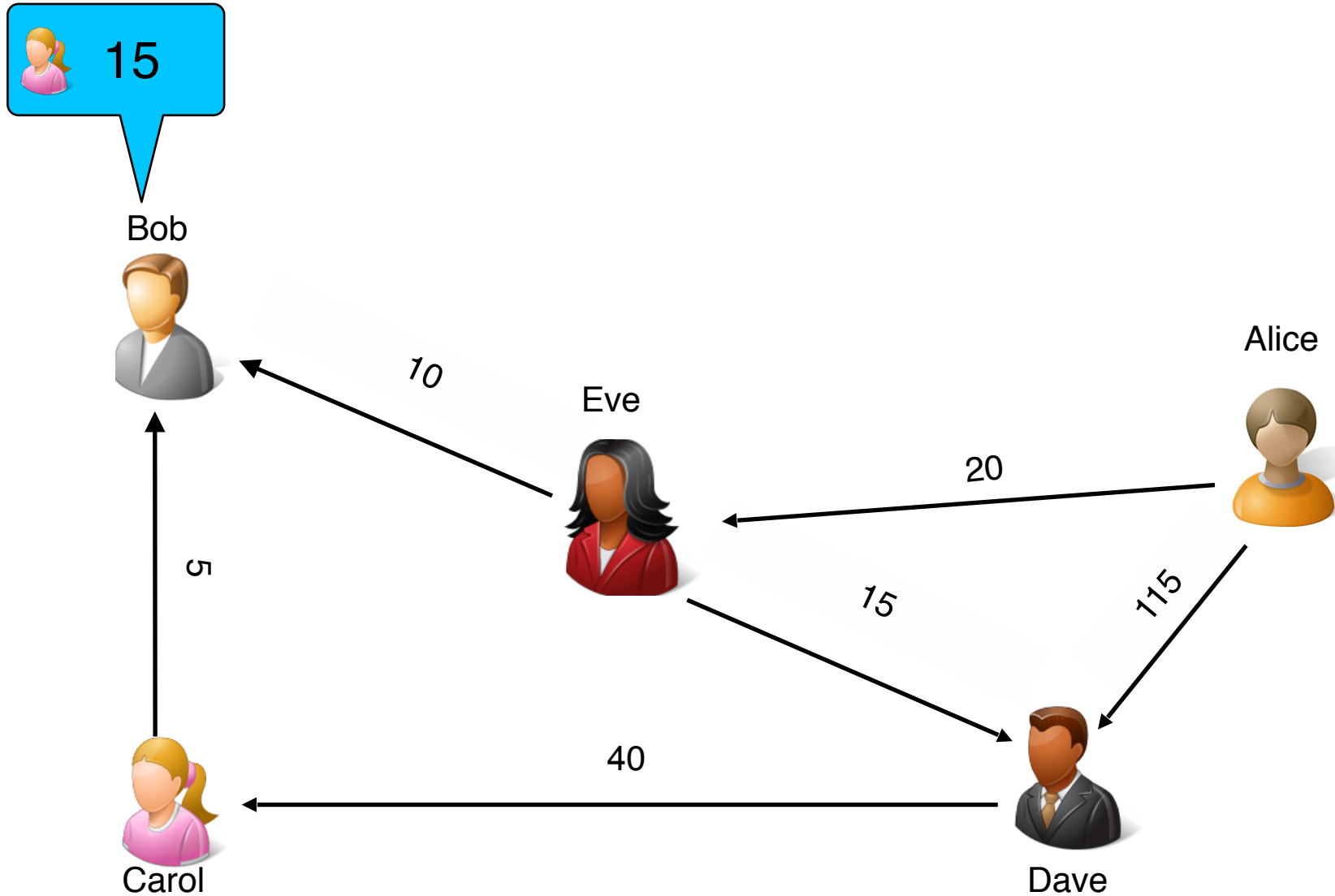
A credit network representation



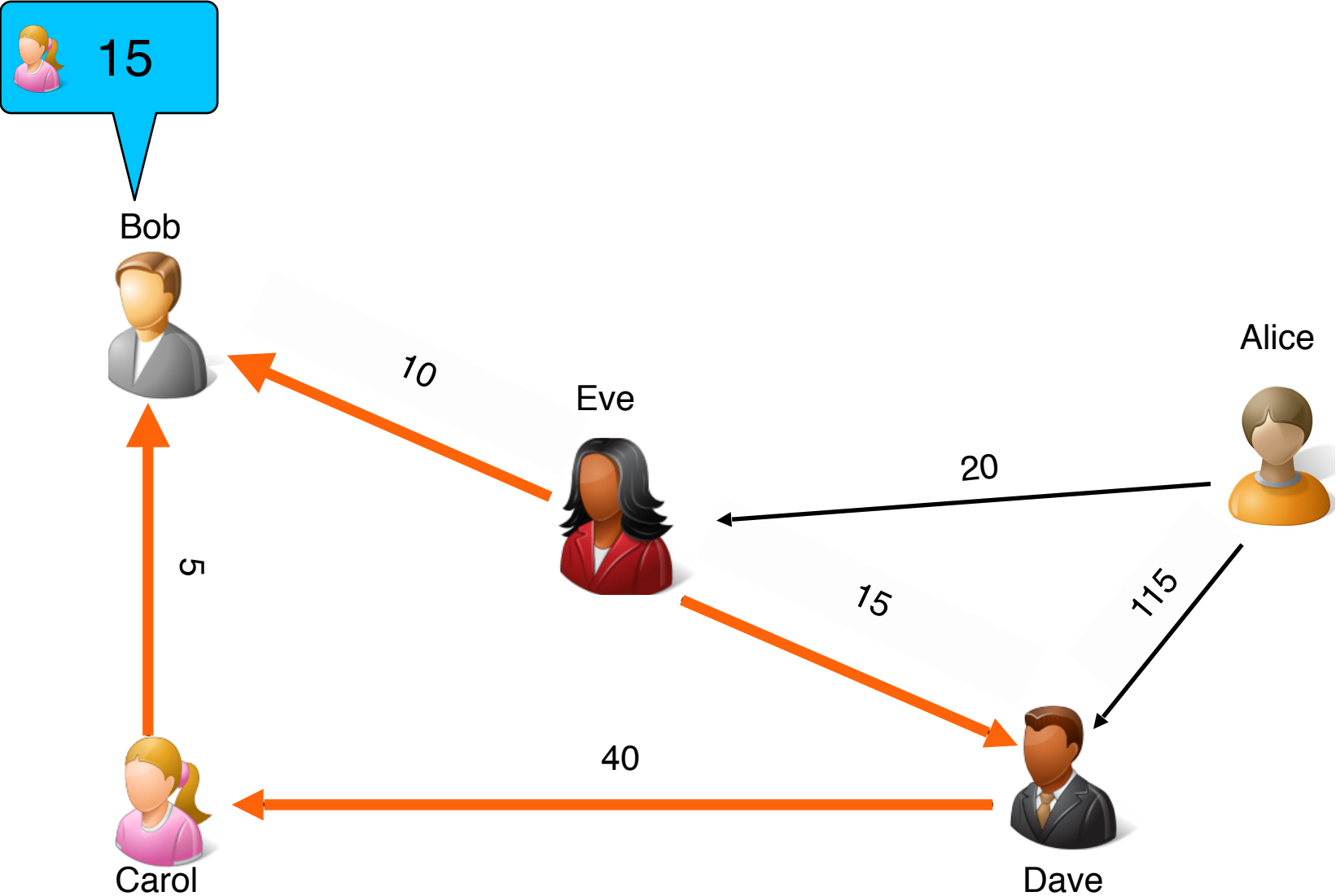
Ripple Credit Network: an Example of Transaction




Ripple Credit Network: an Example of Transaction



Ripple Credit Network: an Example of Transaction

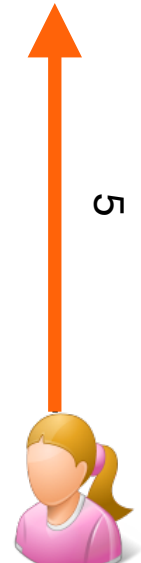


Ripple Credit Network: an Example of Transaction

 15

| | |
|-----------------------|-------|
| Sender | Bob |
| Receiver | Carol |
| Path1 {10}, Path2 {5} | |
| <i>Bob</i> | |

Bob



Carol

Eve



40



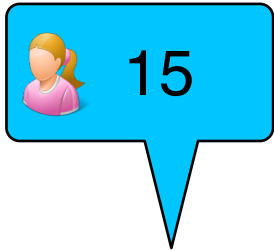
Dave

Alice



Ripple Credit Network: an Example of Transaction

| | |
|-----------------------|-------|
| Sender | Bob |
| Receiver | Carol |
| Path1 {10}, Path2 {5} | |
| <i>Bob</i> | |



Bob



5



Carol

Eve



40

20

Alice



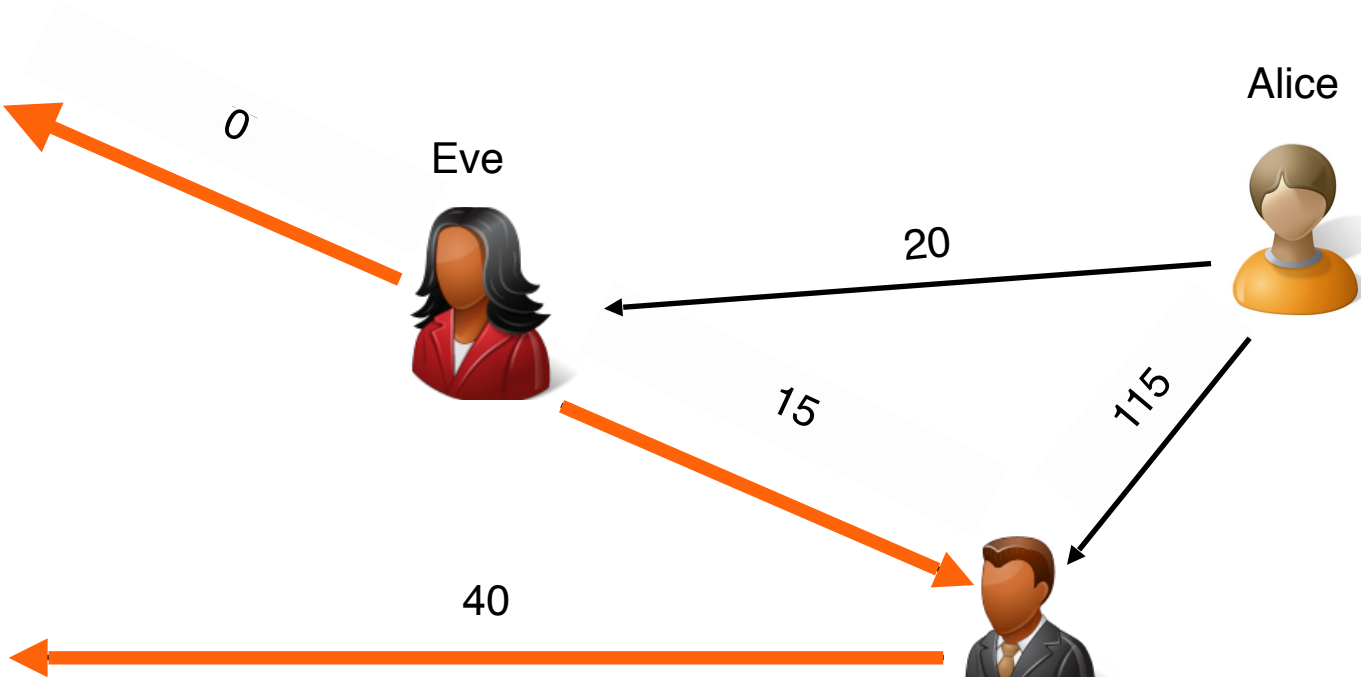
15

115



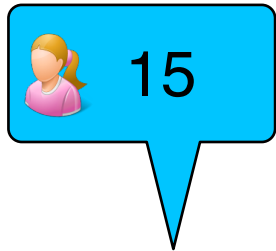
Dave

0

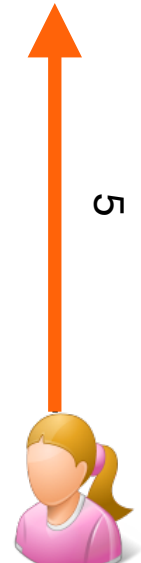


Ripple Credit Network: an Example of Transaction

| | |
|-----------------------|-------|
| Sender | Bob |
| Receiver | Carol |
| Path1 {10}, Path2 {5} | |
| <i>Bob</i> | |



Bob



Carol

Eve



Dave

Alice



5

0

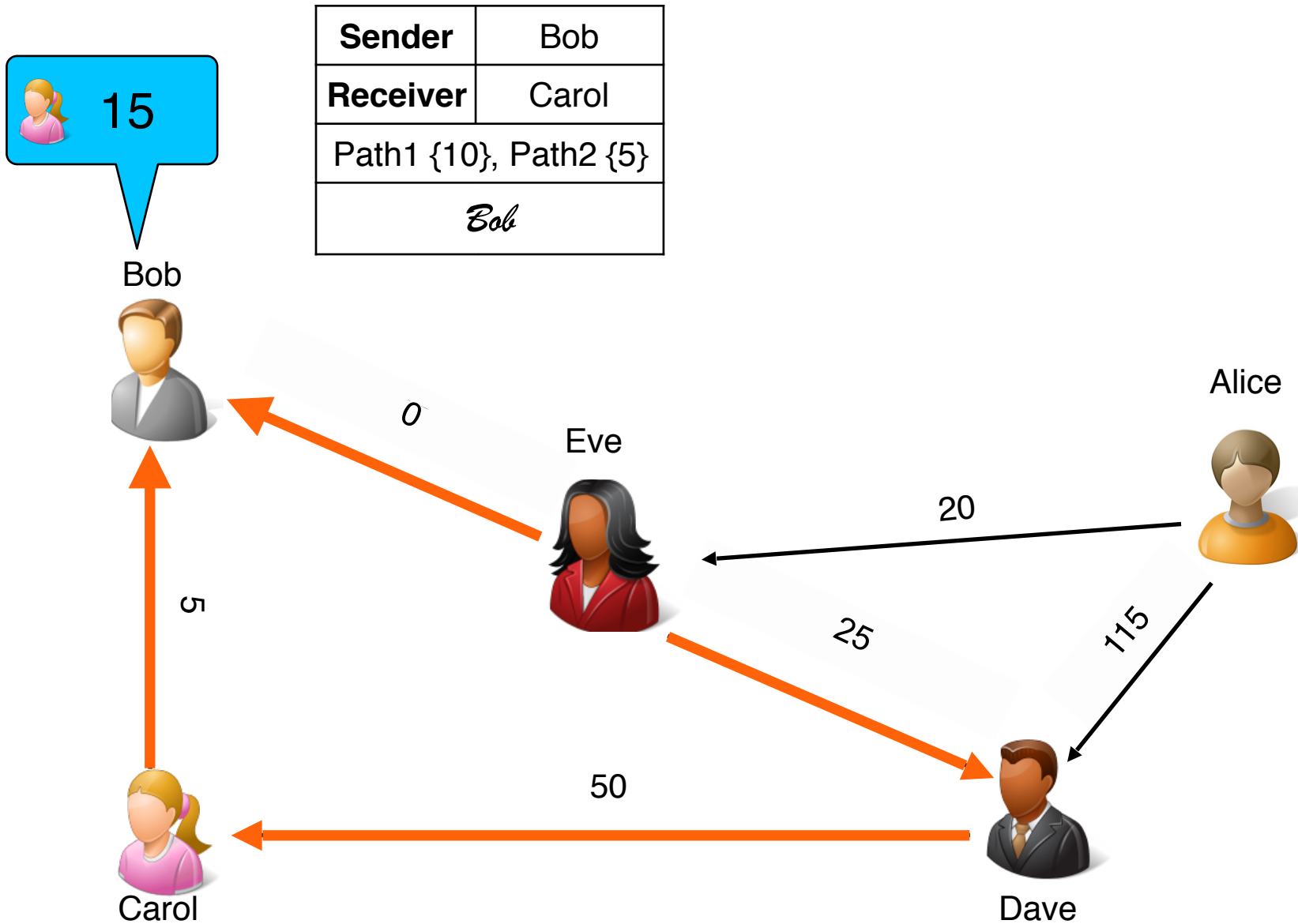
20

25

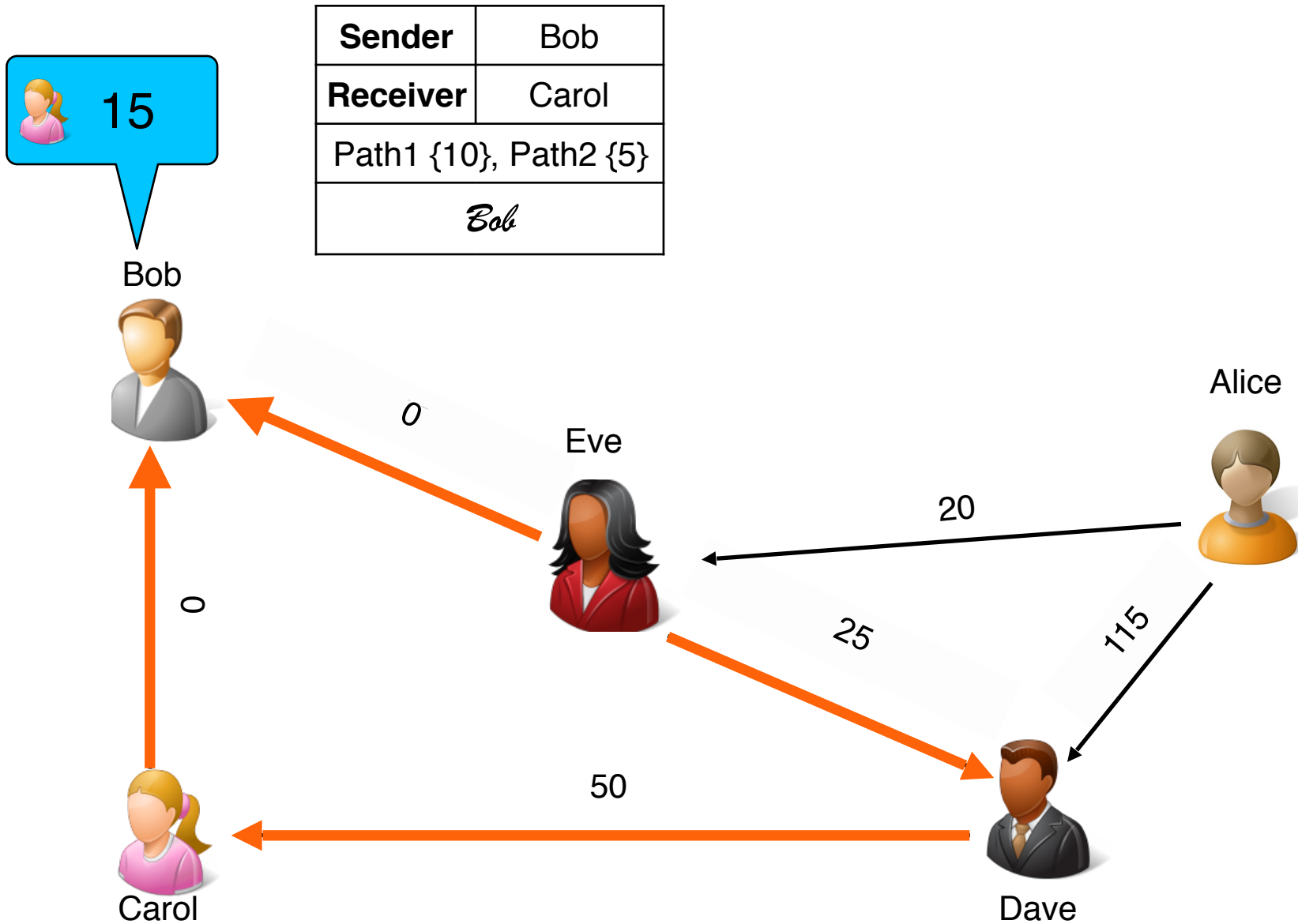
115

40

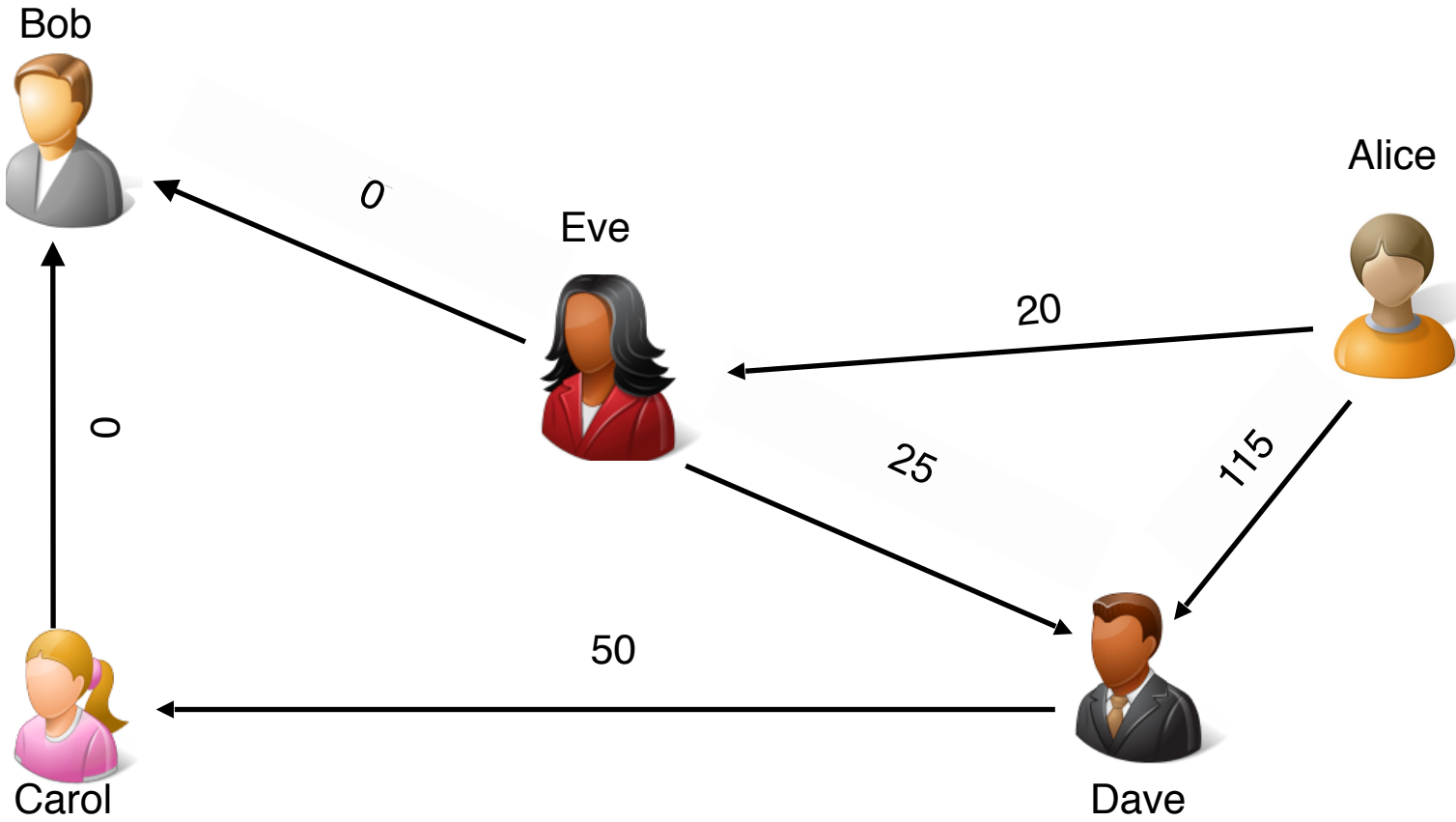
Ripple Credit Network: an Example of Transaction



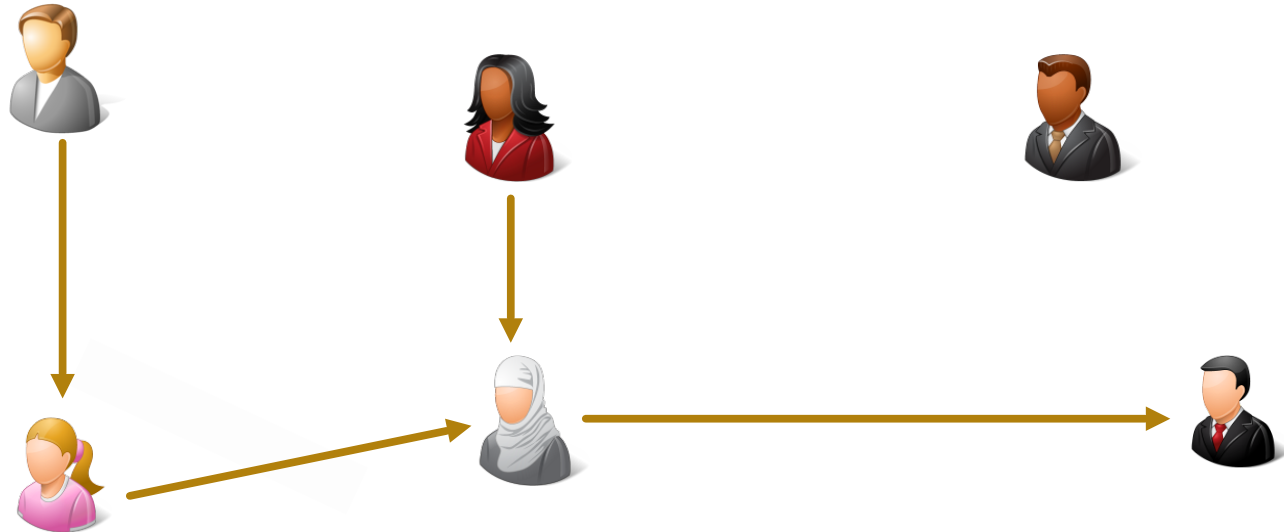
Ripple Credit Network: an Example of Transaction



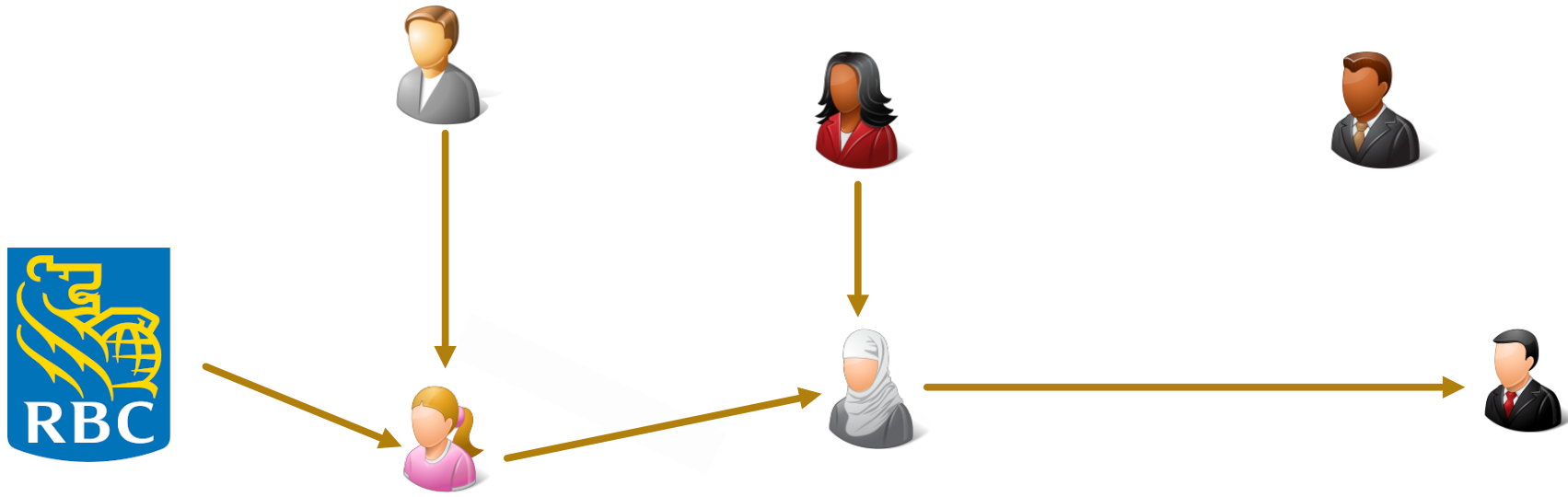
Ripple Credit Network: an Example of Transaction



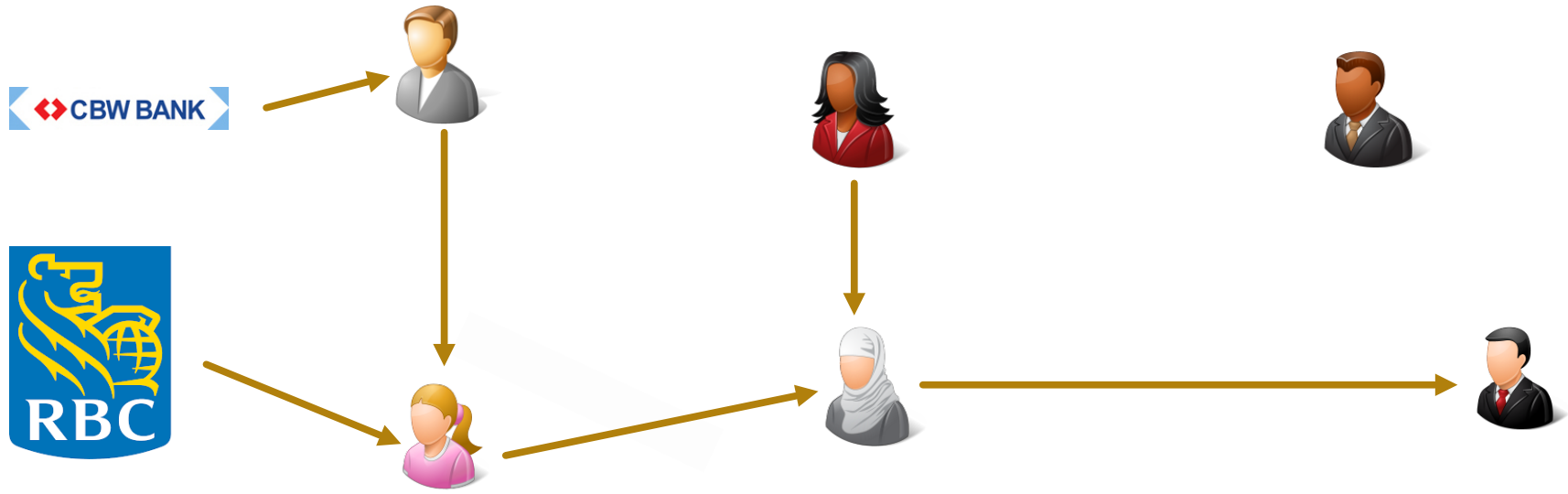
Ripple Credit Network



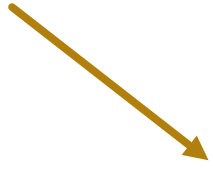
Ripple Credit Network



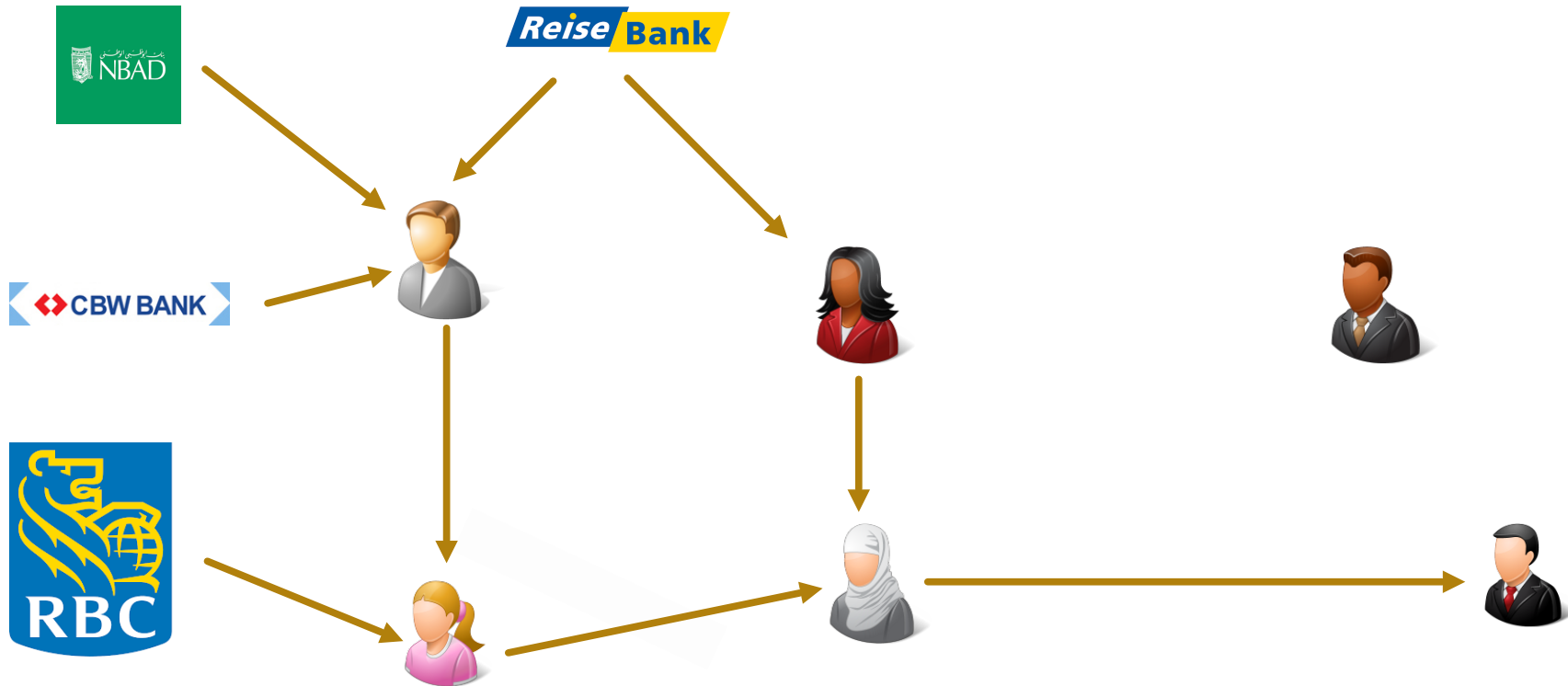
Ripple Credit Network



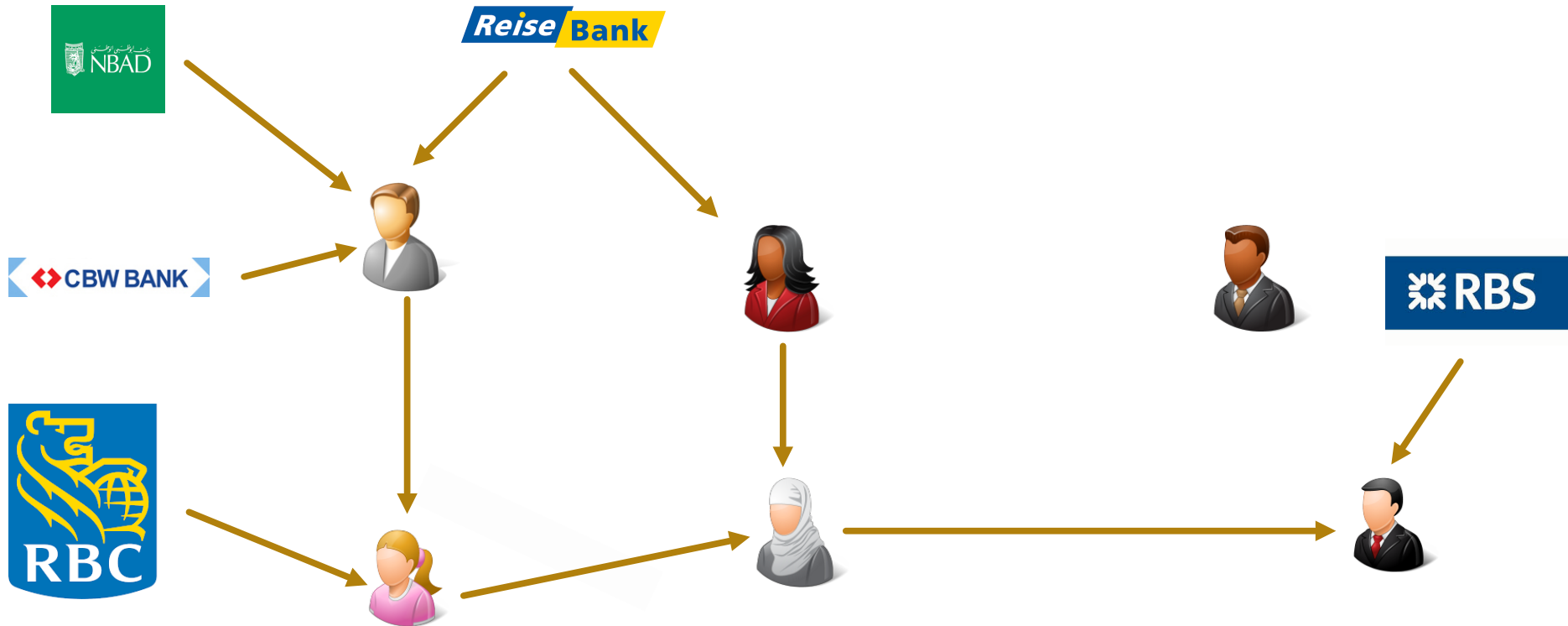
Ripple Credit Network



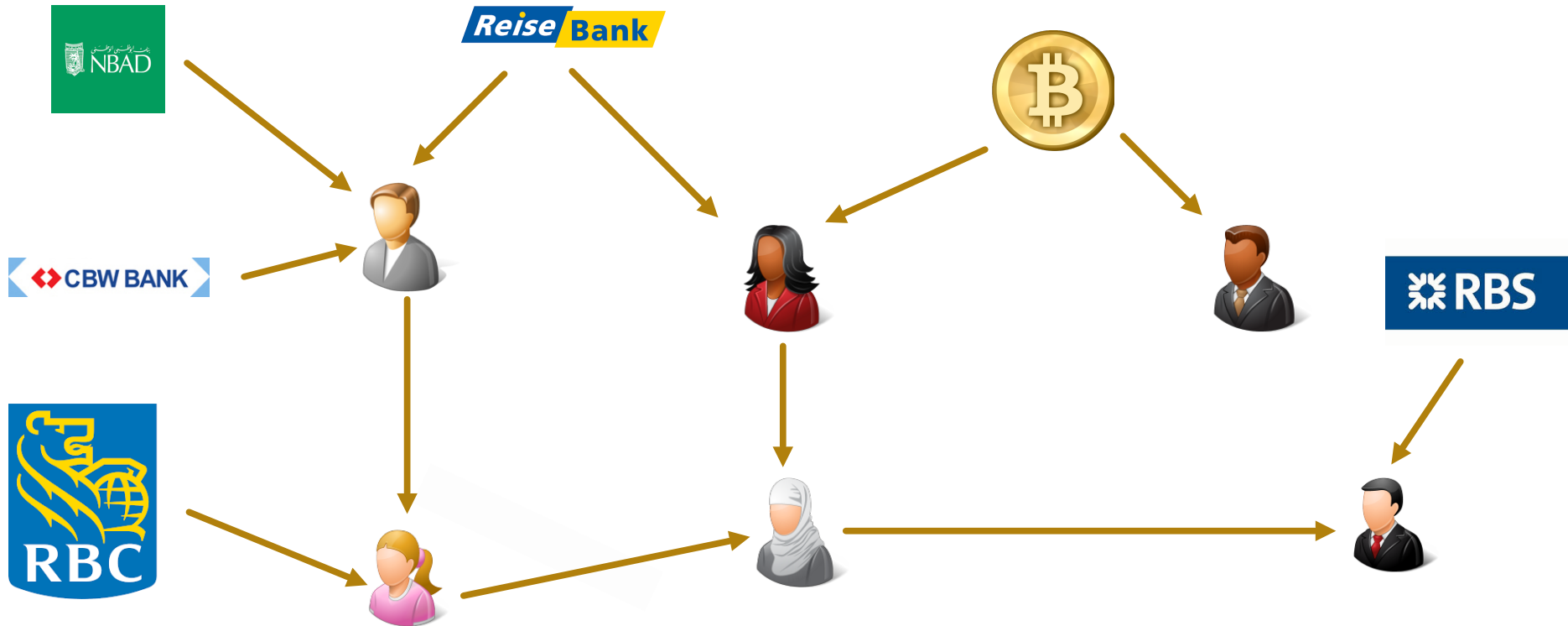
Ripple Credit Network



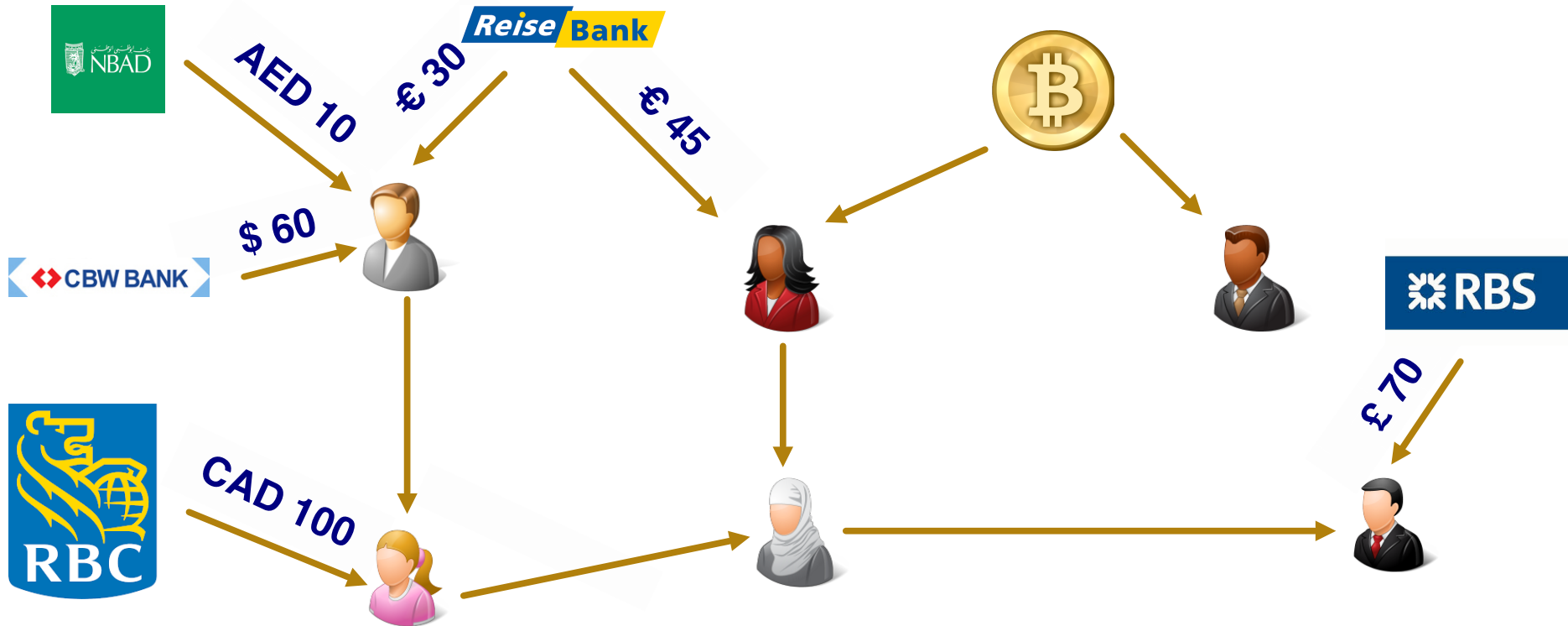
Ripple Credit Network



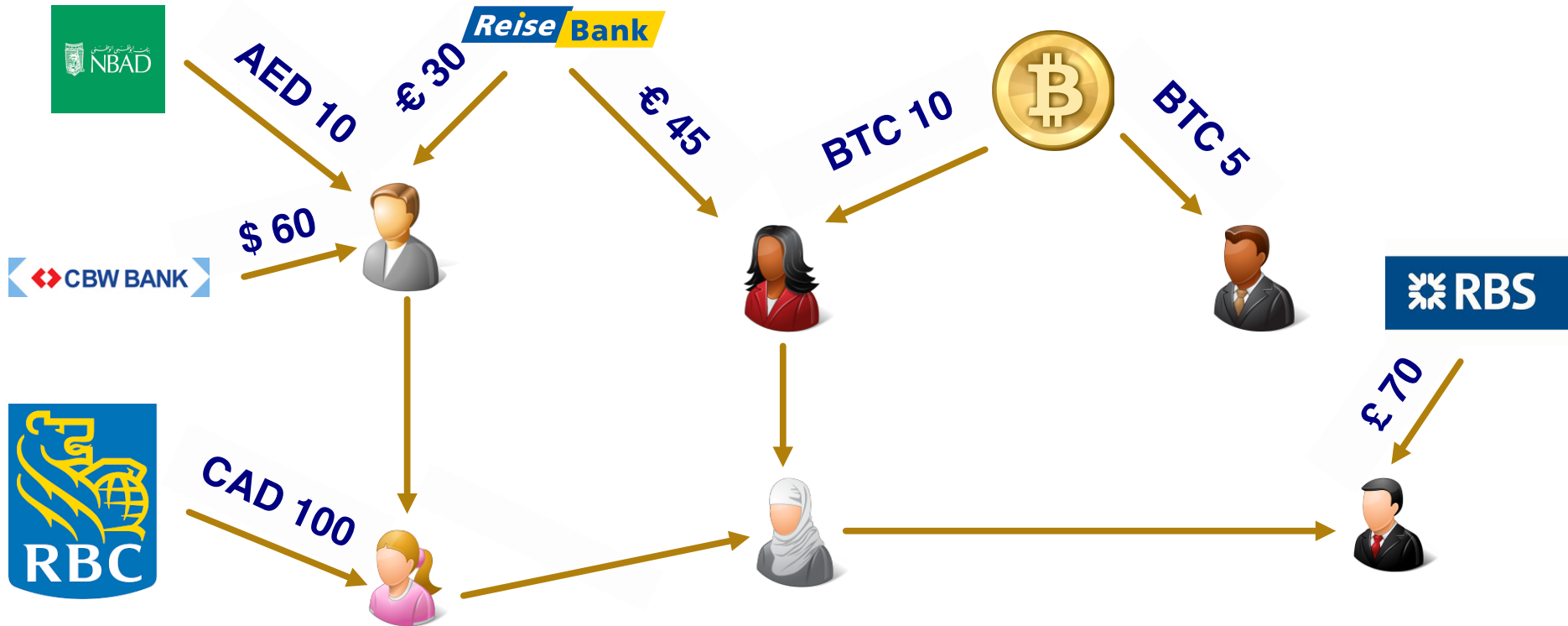
Ripple Credit Network



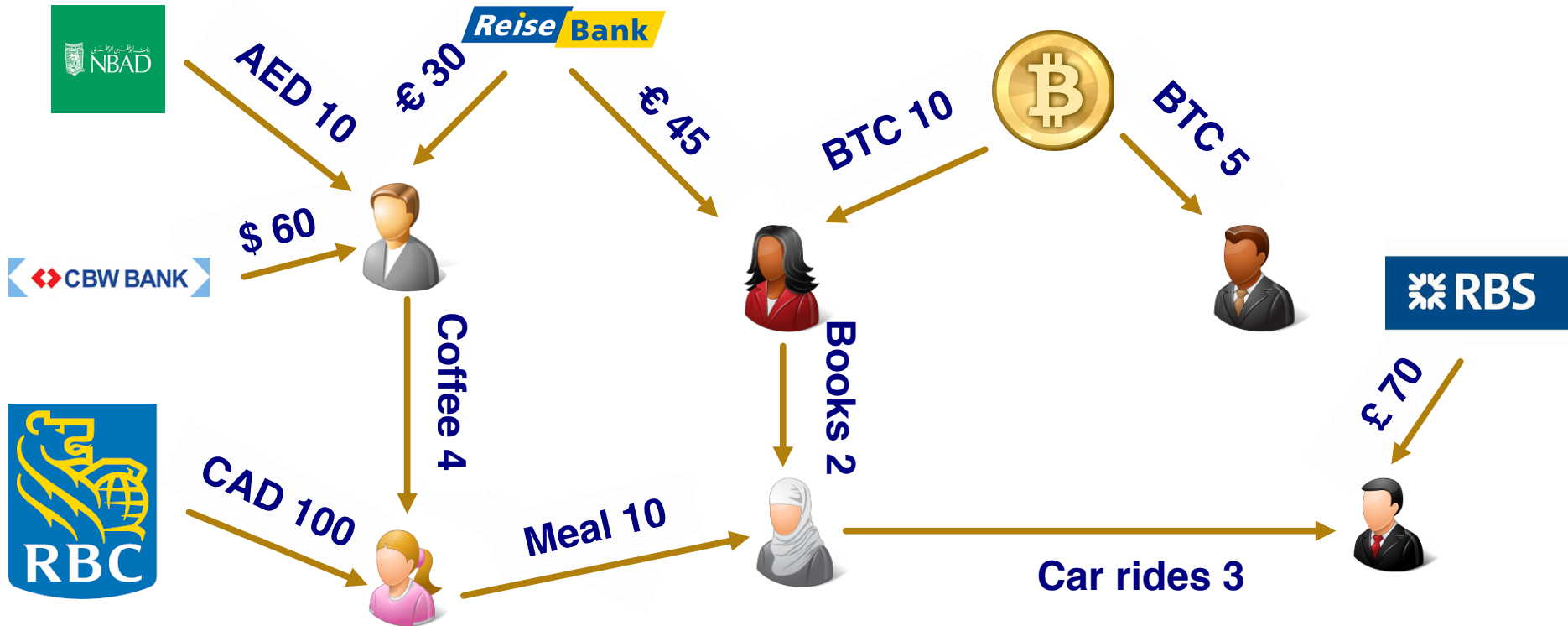
Ripple Credit Network



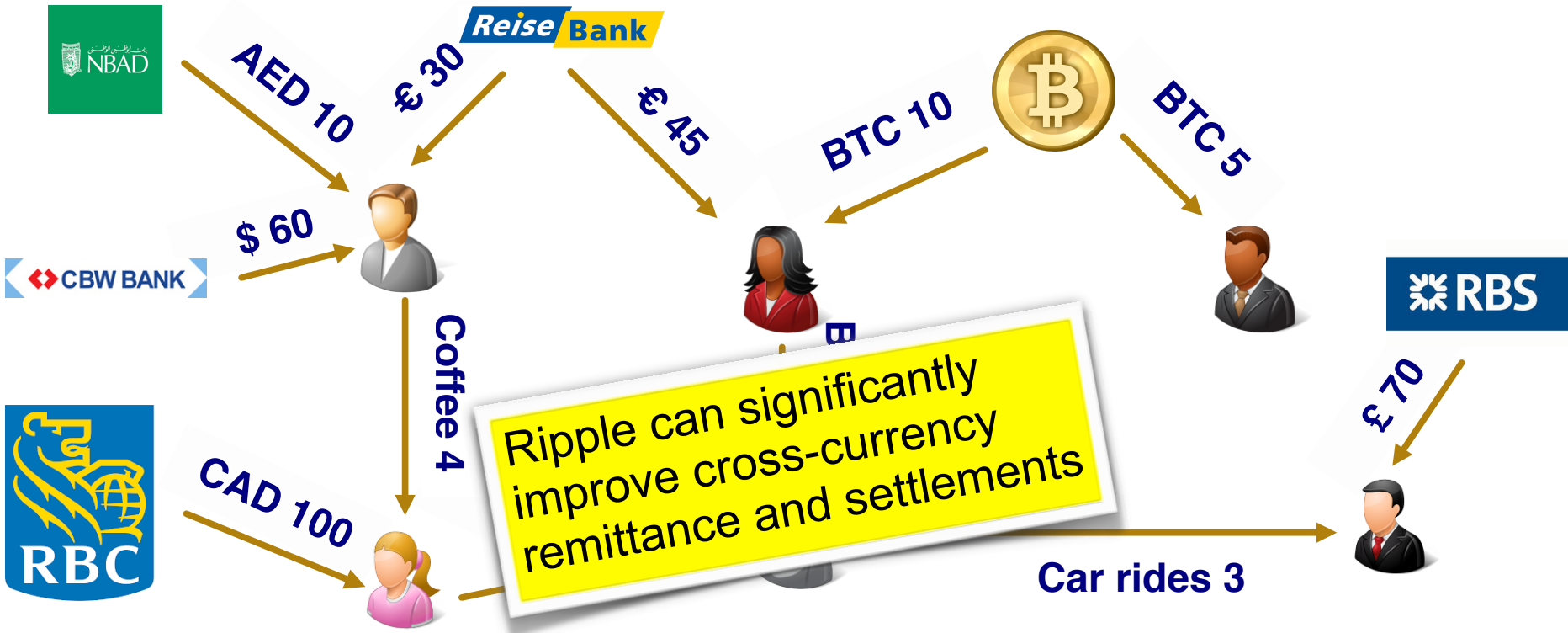
Ripple Credit Network



Ripple Credit Network



Ripple Credit Network



Tx time

~ 1 day

Worldwide,
cross-currency tx

High fees

Integrity

Bank only

~ 5 seconds

Tiny fees

Public verifiability



Public Verifiability & Privacy Problem

The Ripple Ledger

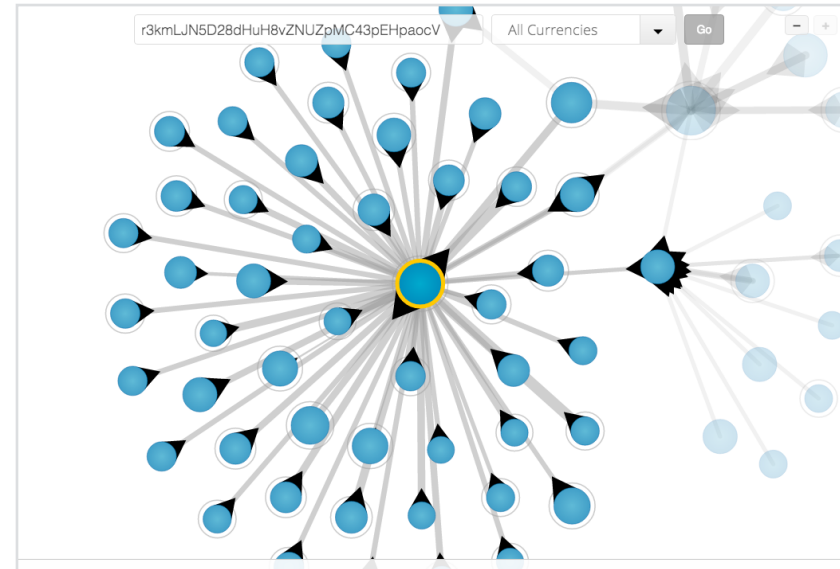
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

| Account | Destination | Amount |
|--------------------------------------------|-------------------------------------------|---------------------------|
| rhwctTPLKZqK59f1fXpDkQ... | rMnVZ9maUWp5cAvmqBECZM... | 300/XRP |
| rLSBpSquSHKbbfvcKt1c54... | rKoDt7VL83AKJZewLxVZE... | 75/XRP |
| r42869fSSmD4SYmnDra16B... | rBeToNo4AwHaNBx2n4BNC... | 0.0693402709148/CCK/rB... |
| rhd759dbJMrzMML4QbvQe9... | r95pwKA1K55fy7EJWrqJ9b... | 300/XRP |
| r42WJGvV9MJJa4t5QcF8Cnx... | rBeToNo4AwHaNBx2n4BNC... | 0.0821058028231/CCK/rB... |
| rUnr1p7xkuSBxyAqHEopZ5... | r3H4rynDShFMRKWuJcadLY... | 1129.916679154465/EUR/... |
| rw7UfGvzCeZwJxxUEeZHLG... | rBwgTdzzMHnouLk5DJD3xd... | 100/XRP |
| rpVVzfSTUJX9CrKBSS2Z5W... | rDCgaaSBAWYfsxUYhCk1n2... | 999.99/XRP |

Credit Graph



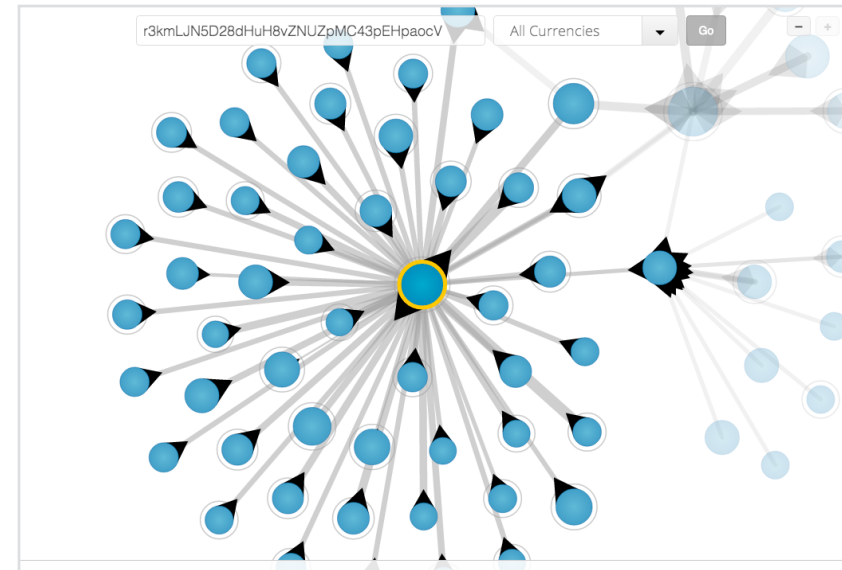
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

| Account | Destination | Amount |
|--------------------------------------------|-------------------------------------------|---------------------------|
| rwwctTPLKZqK59f1fXpDkQ... | rMnVZ9maUWp5cAvmqBECZM... | 300/XRP |
| rLSBpSquSHKbbfvcKt1c54... | rKoDt7VL83AKJZewLxVZE... | 75/XRP |
| r428G9fSSmD4SYmnDra16B... | rBeToNo4AwHaNBRX2n4BNC... | 0.0693402709148/CCK/rB... |
| rhd759dbJMrzMNL4QbvQe9... | r95pwKA1K55fy7EJWrqJ9b... | 300/XRP |
| r42WJGvV9MJJa4t5QcF8Cnx... | rBeToNo4AwHaNBRX2n4BNC... | 0.0821058028231/CCK/rB... |
| rUnr1p7xkuSBxyAqHEopZ5... | r3H4rynDShFMRKWuJcadLY... | 1129.916679154465/EUR/... |
| rw7UfGvzCeZwJxxUEeZHLG... | rBwgTdzzMHnouLk5DJD3xd... | 100/XRP |
| rpVVzfSTUJX9CrKBSS2Z5W... | rDCgaaSBAWYfsxUYhCk1n2... | 999.99/XRP |

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

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

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

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

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)

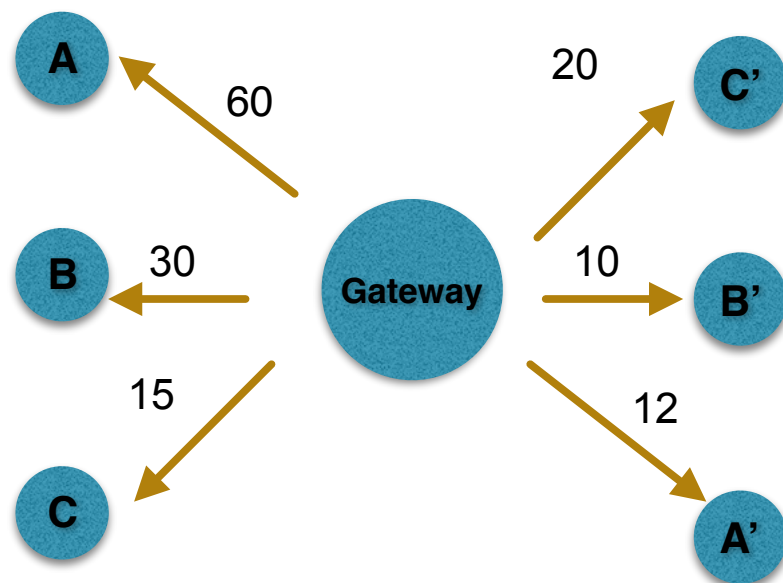
| <i>Input Addresses</i> | <i>Output Addresses</i> |
|----------------------------|-----------------------------|
| A (1 BTC) | B' (1 BTC) |
| B (1 BTC) | C' (1 BTC) |
| C (1 BTC) | A' (1 BTC) |
| <i>Alice</i> | |
| <i>Bob</i> | |
| <i>Carol</i> | |

Path Mixing for Privacy-preserving Transactions



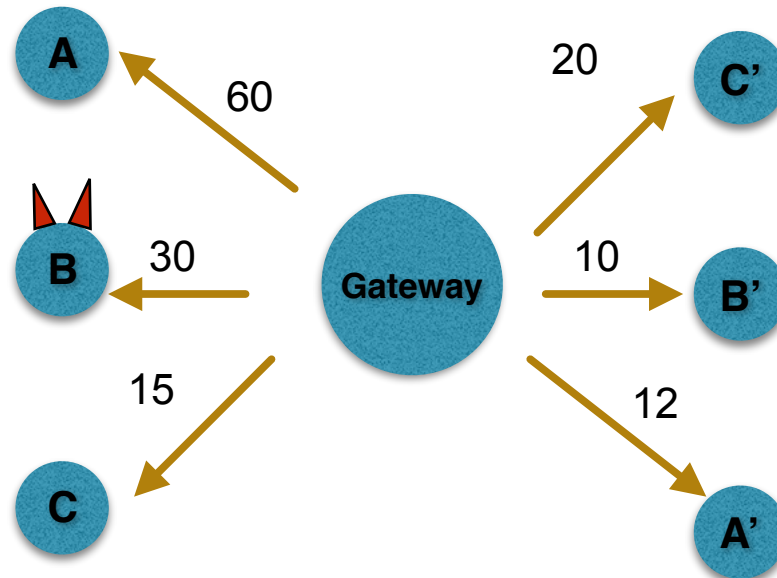
Path Mixing for Privacy-preserving Transactions

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



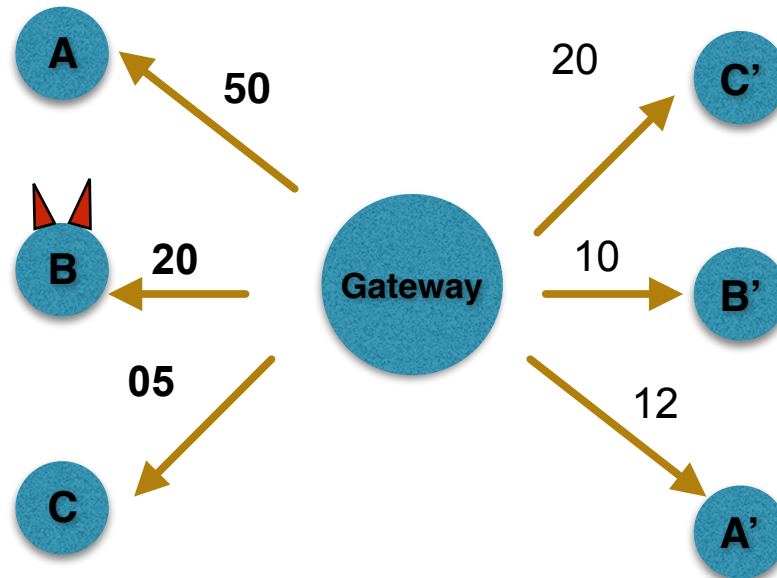
Path Mixing for Privacy-preserving Transactions

- ✦ **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



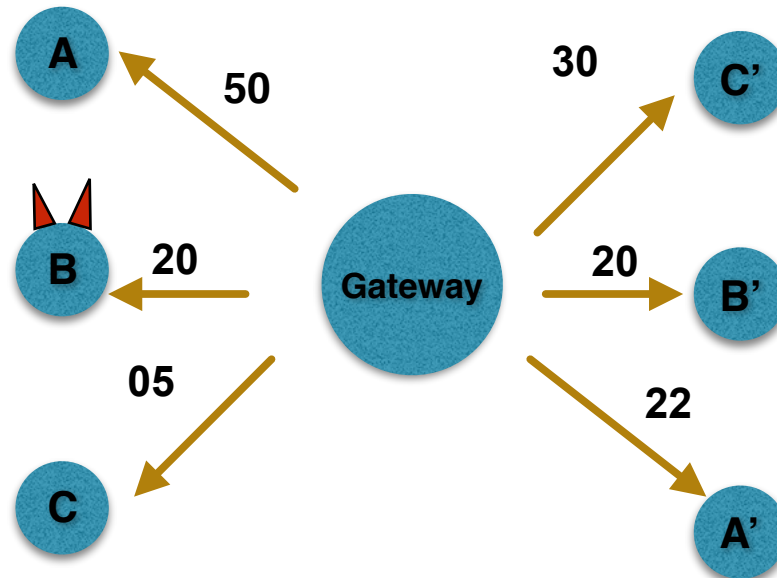
Path Mixing for Privacy-preserving Transactions

- ✦ **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



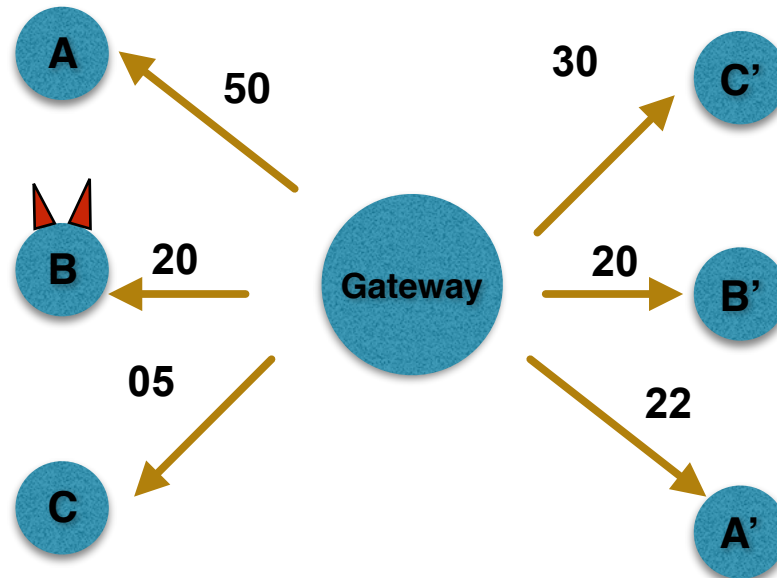
Path Mixing for Privacy-preserving Transactions

- ✦ **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

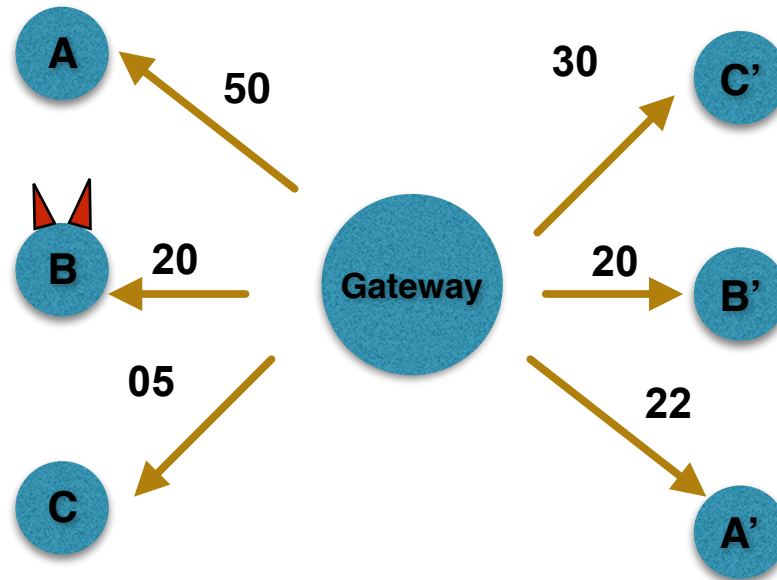
- ✦ **Idea:** Transaction paths sharing a common node can be mixed
- ✦ **Goal:** Hide who pays to whom (unlinkability) from an adversary who controls up to $(n-2)$ input wallets



- ✦ **Multi-input-multi-output (CoinJoin) transaction:** Not supported in Ripple.

Path Mixing for Privacy-preserving Transactions

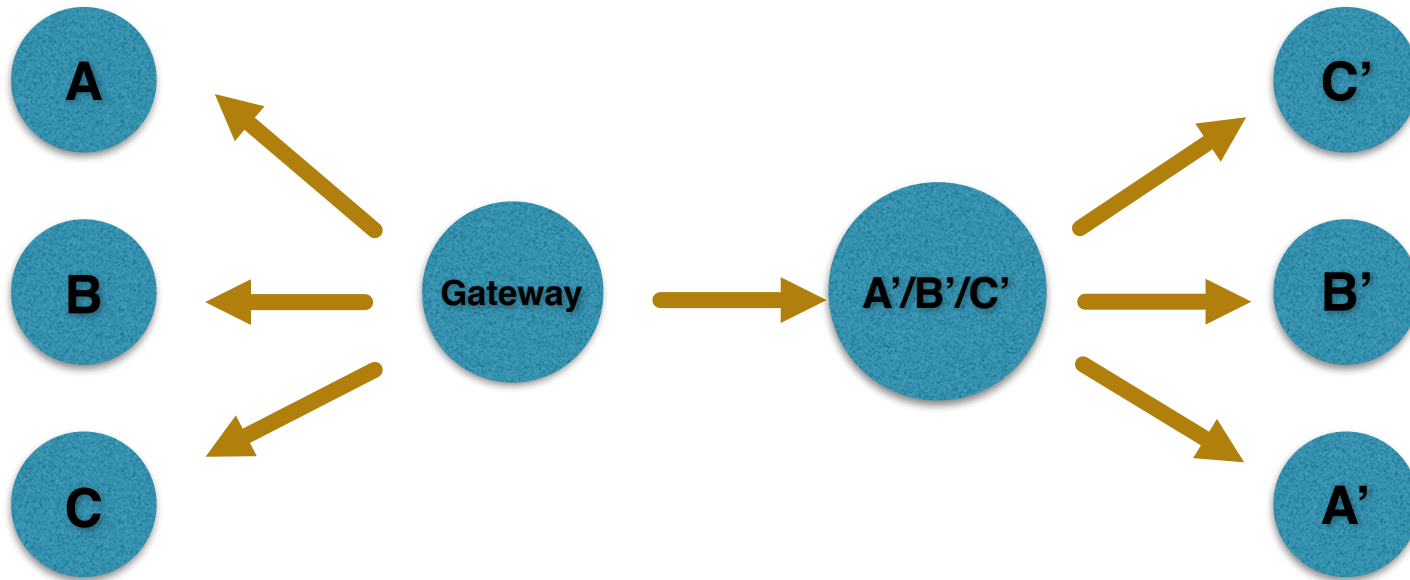
- ◆ **Idea:** Transaction paths sharing a common node can be mixed
- ◆ **Goal:** Hide who pays to whom (unlinkability) from an adversary who controls up to $(n-2)$ input wallets



- ◆ **Multi-input-multi-output (CoinJoin) transaction:** Not supported in Ripple.
- ◆ **Atomicity problem:** Who sends first?

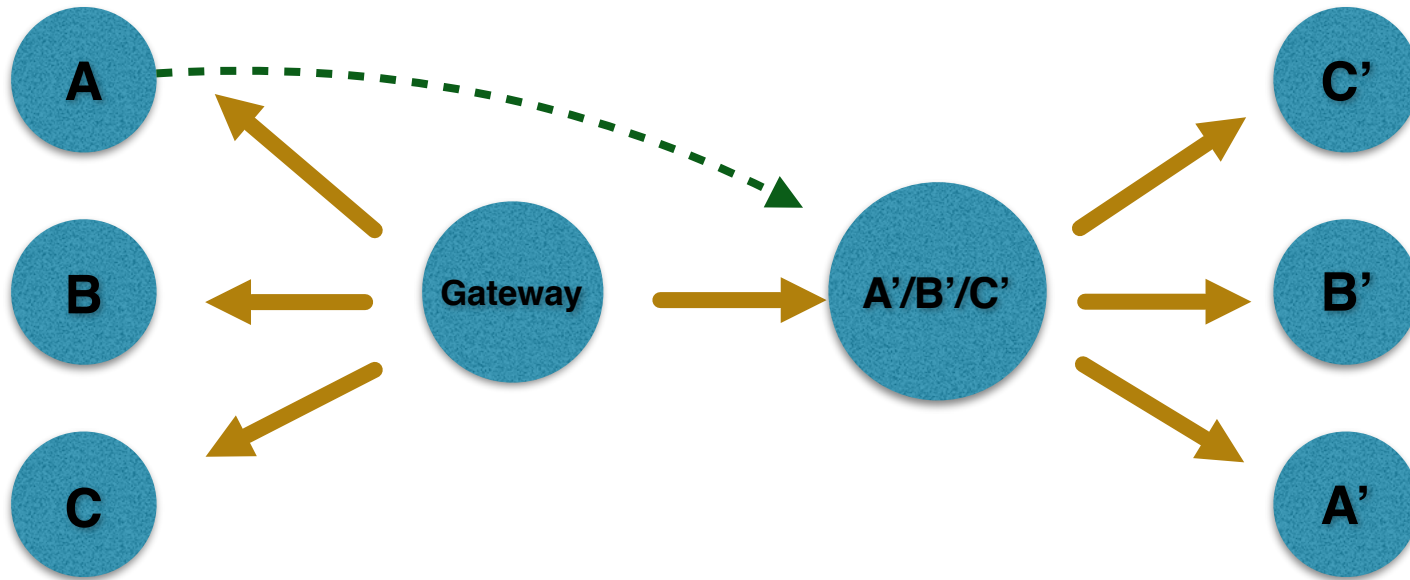
Key Idea: Synchronization Using Shared Wallets

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



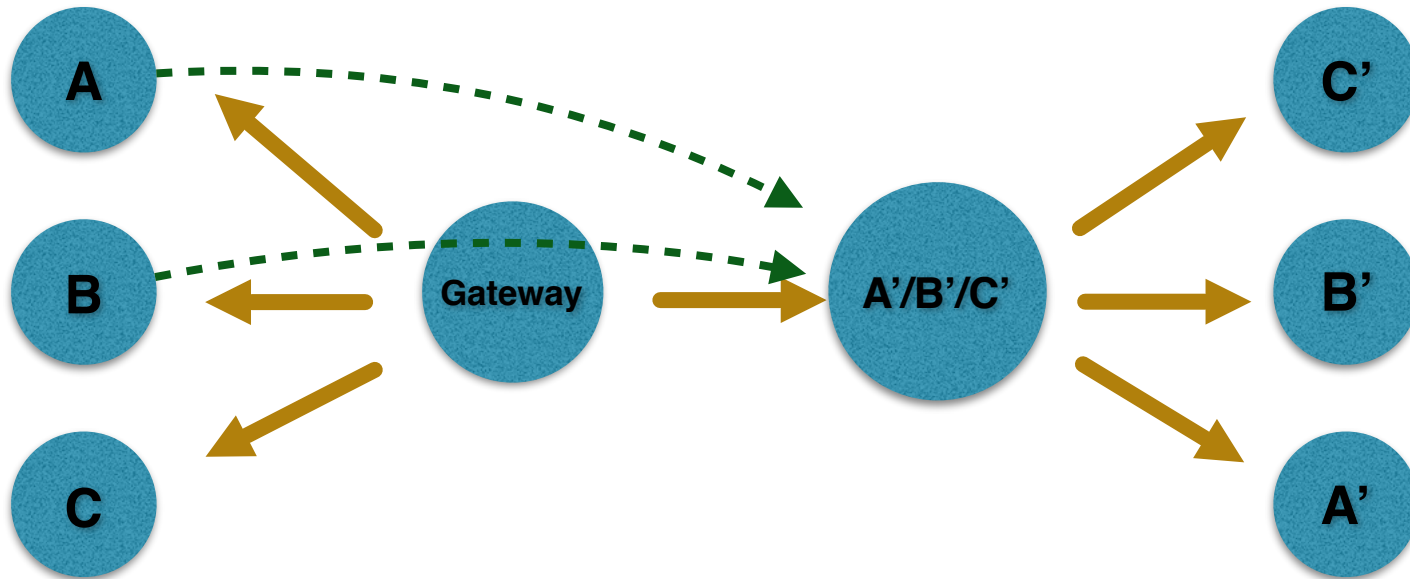
Key Idea: Synchronization Using Shared Wallets

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



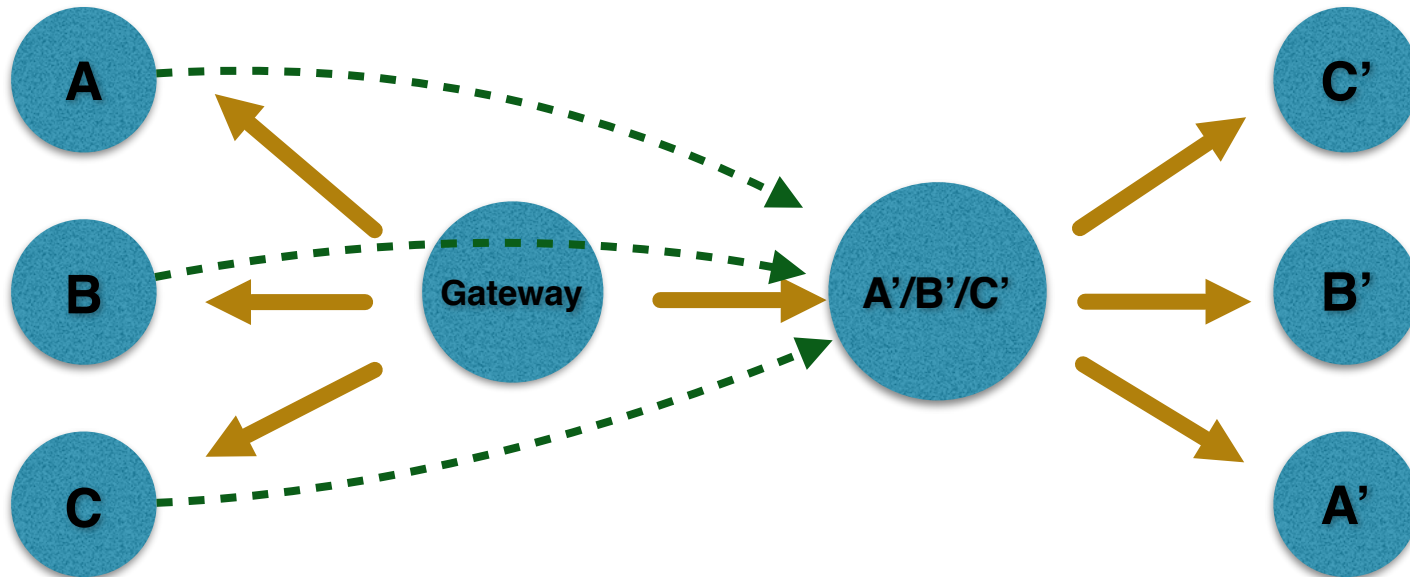
Key Idea: Synchronization Using Shared Wallets

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



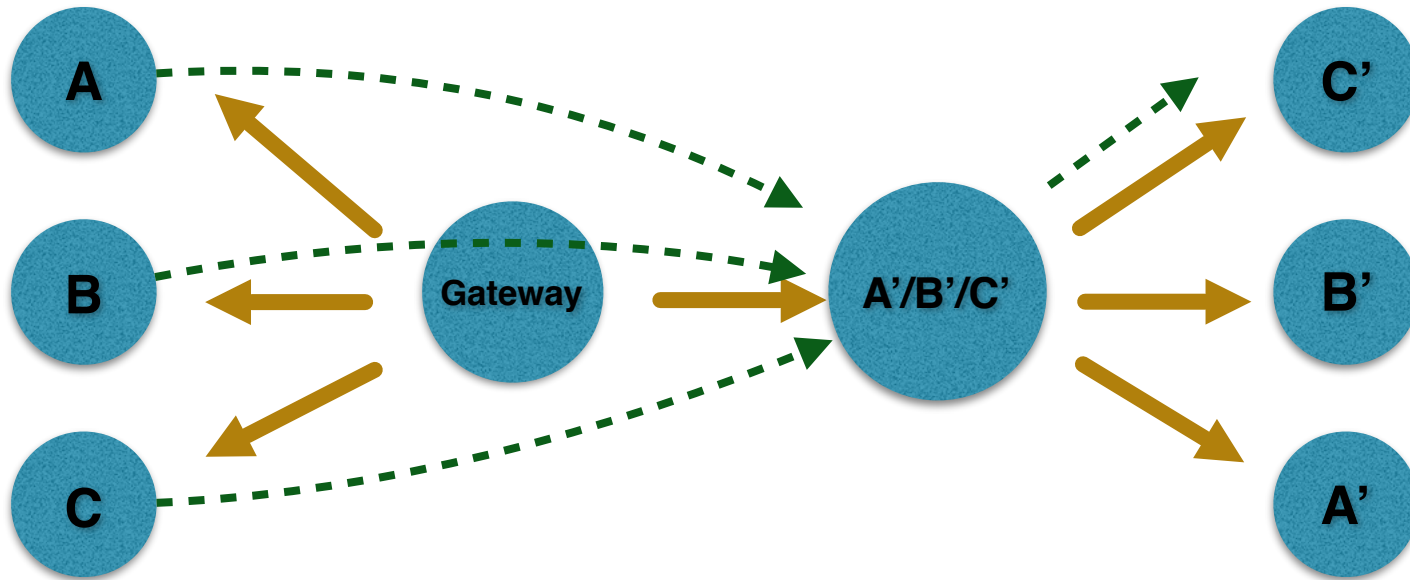
Key Idea: Synchronization Using Shared Wallets

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



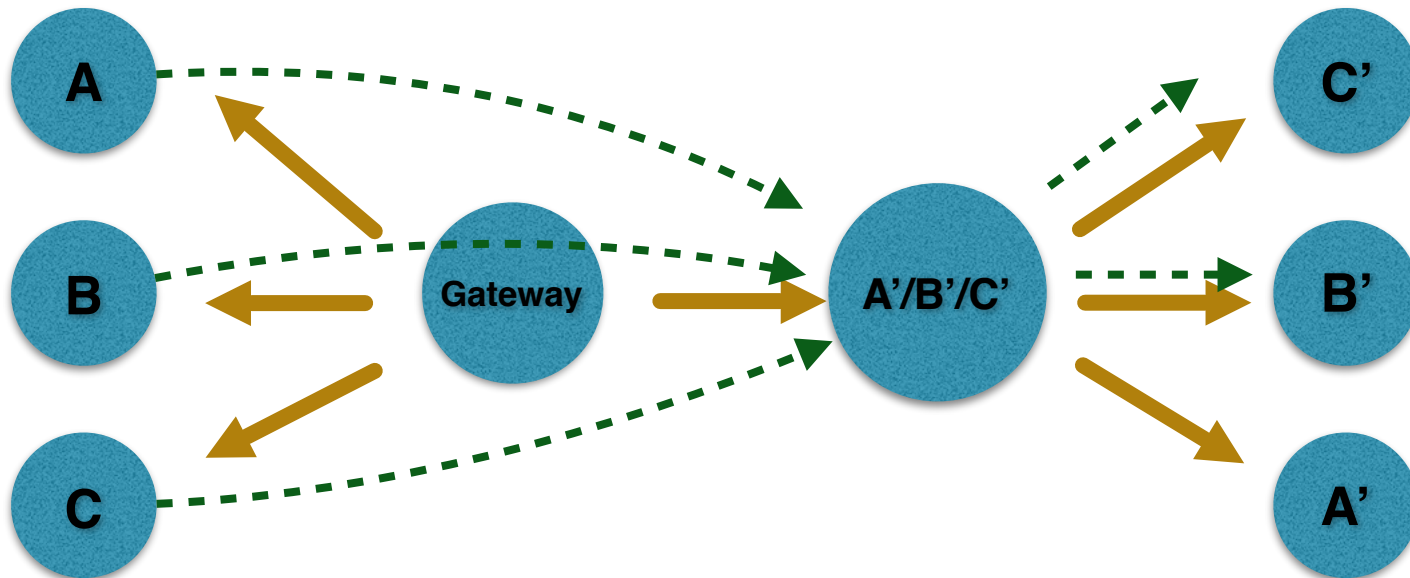
Key Idea: Synchronization Using Shared Wallets

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



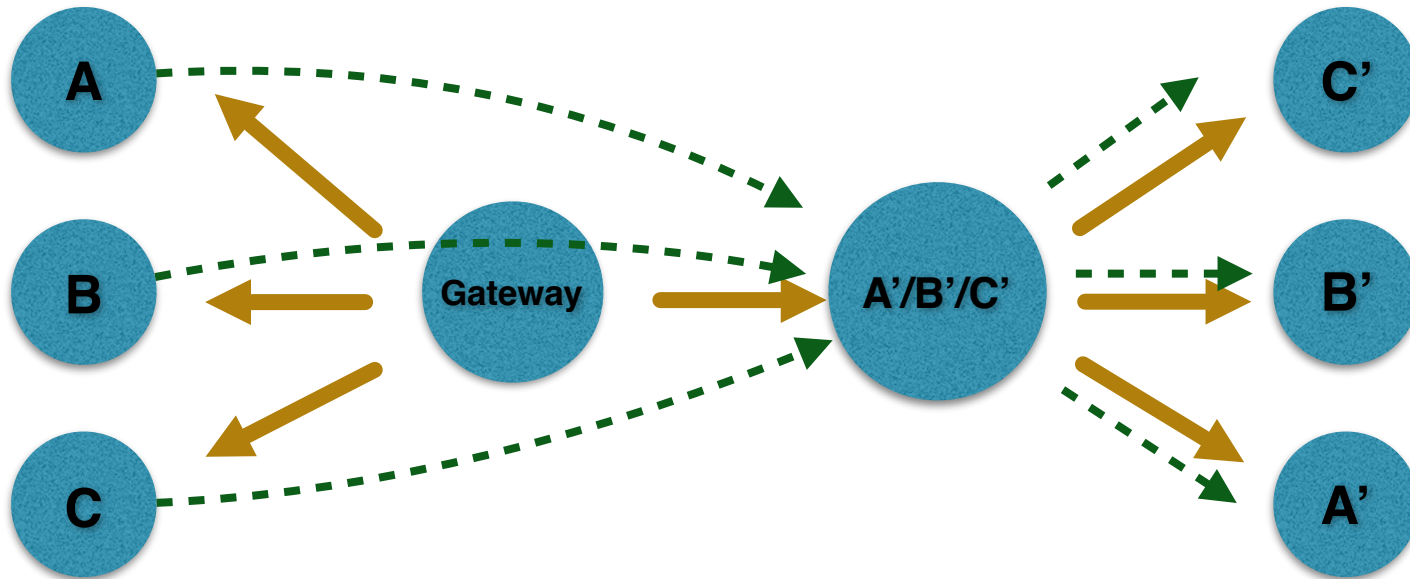
Key Idea: Synchronization Using Shared Wallets

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



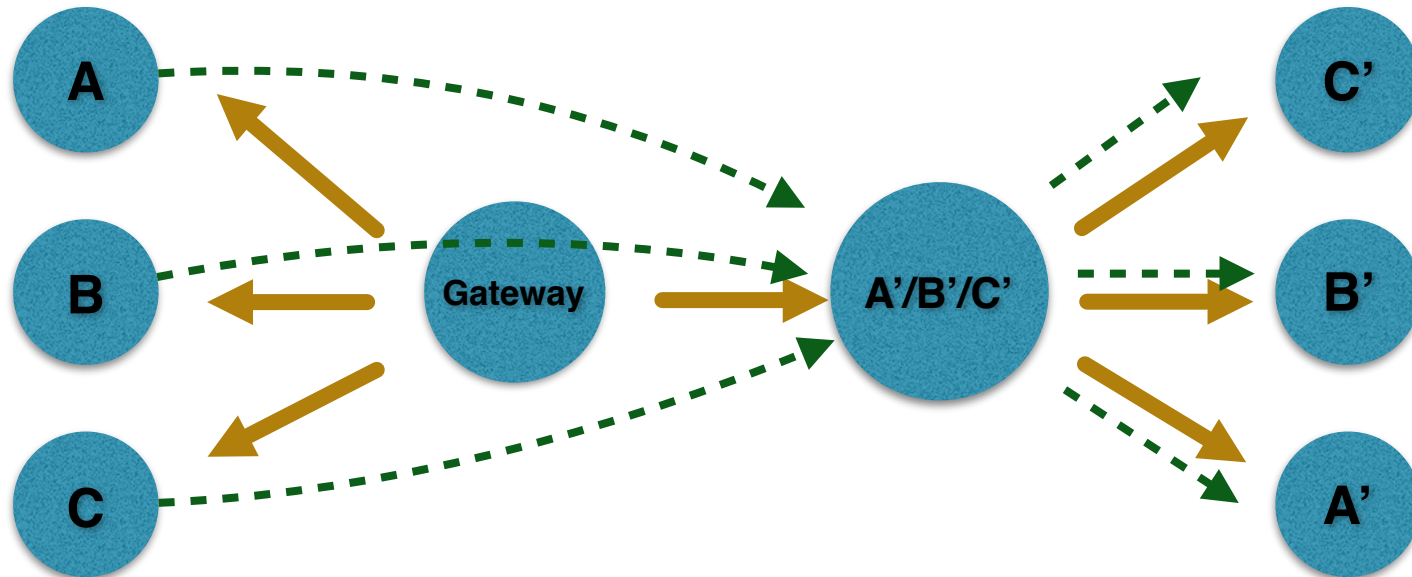
Key Idea: Synchronization Using Shared Wallets

- ◆ **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)



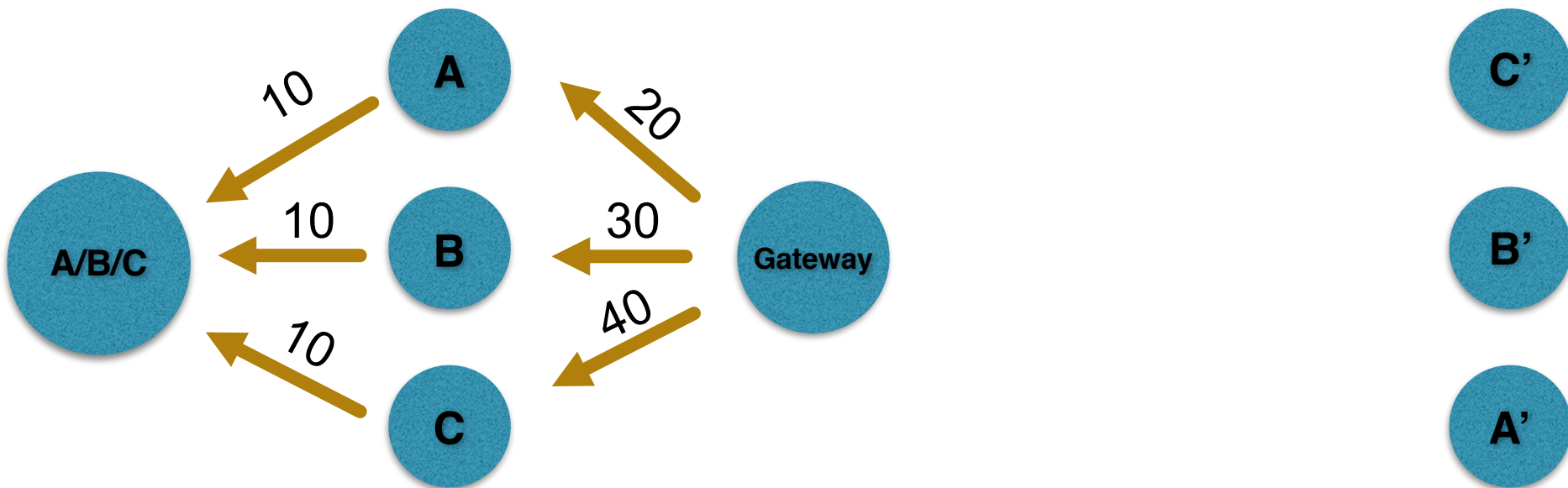
Our Protocol for Atomic Transactions: PathJoin

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



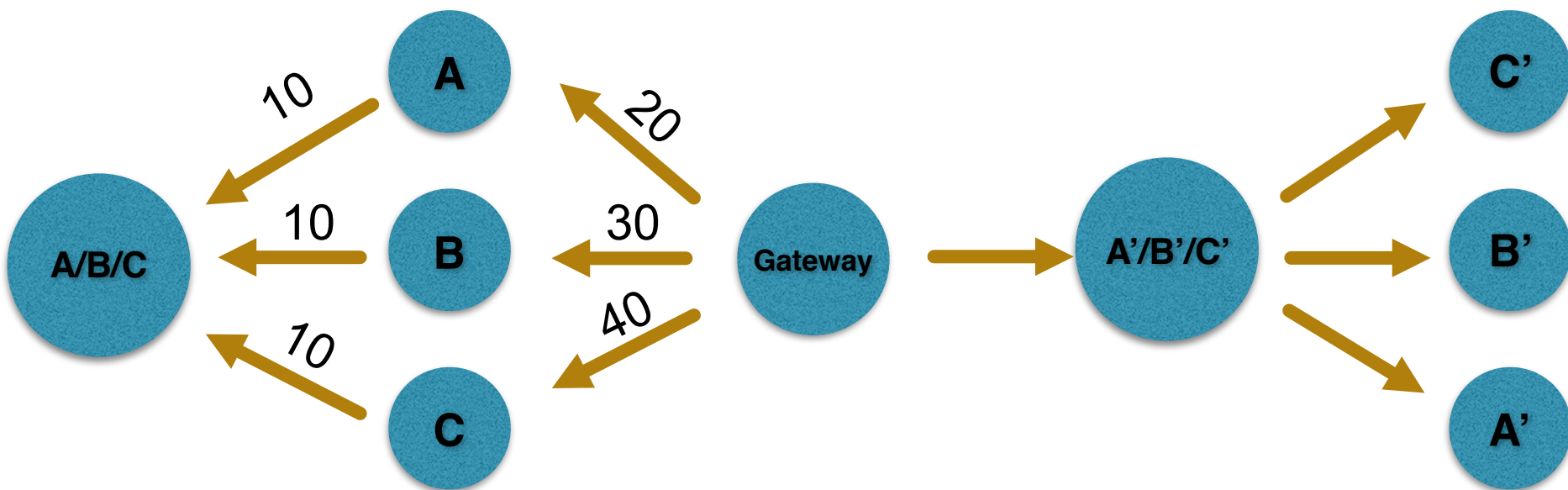
Our Protocol for Atomic Transactions: PathJoin

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



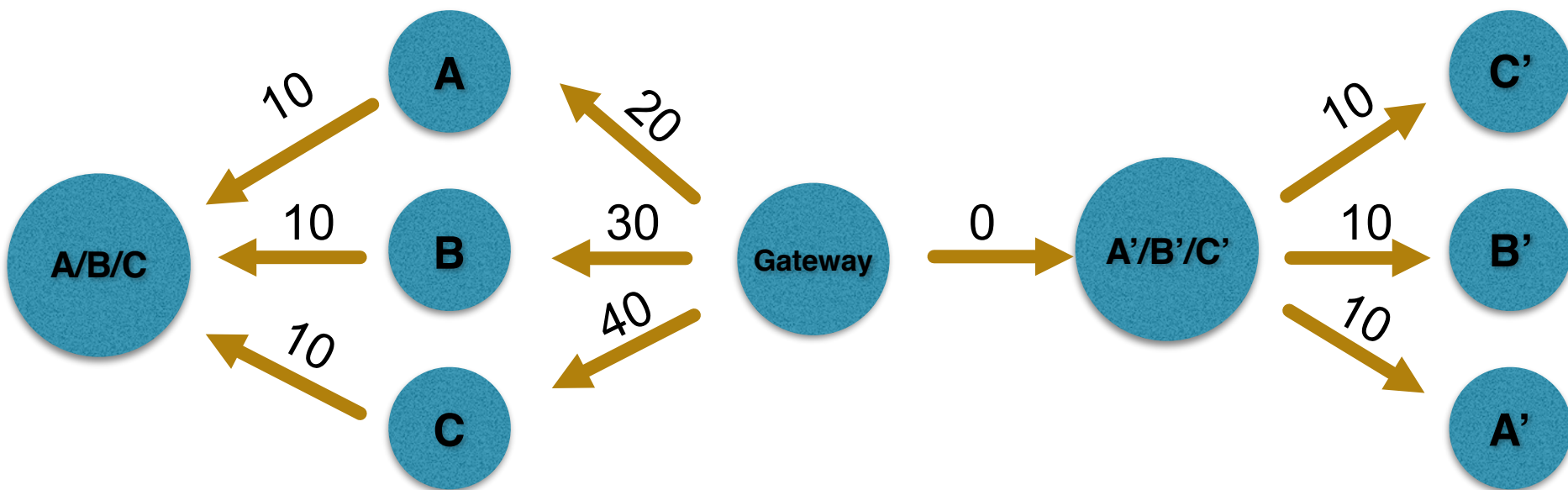
Our Protocol for Atomic Transactions: PathJoin

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



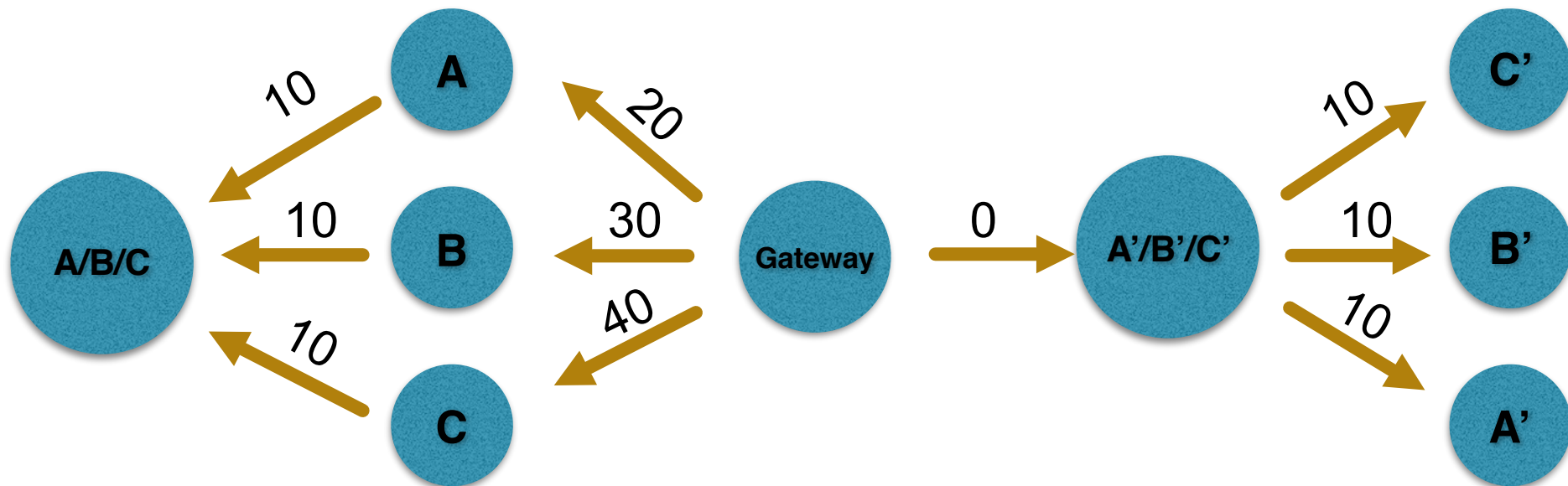
Our Protocol for Atomic Transactions: PathJoin

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



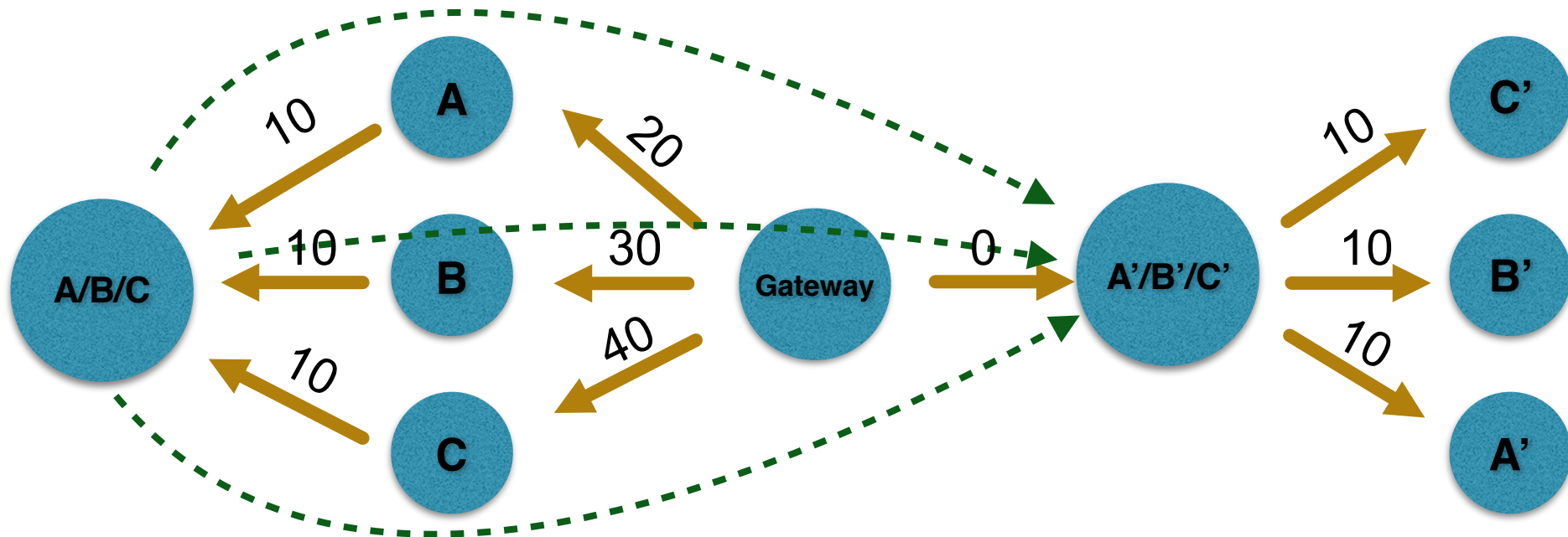
Our Protocol for Atomic Transactions: PathJoin

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



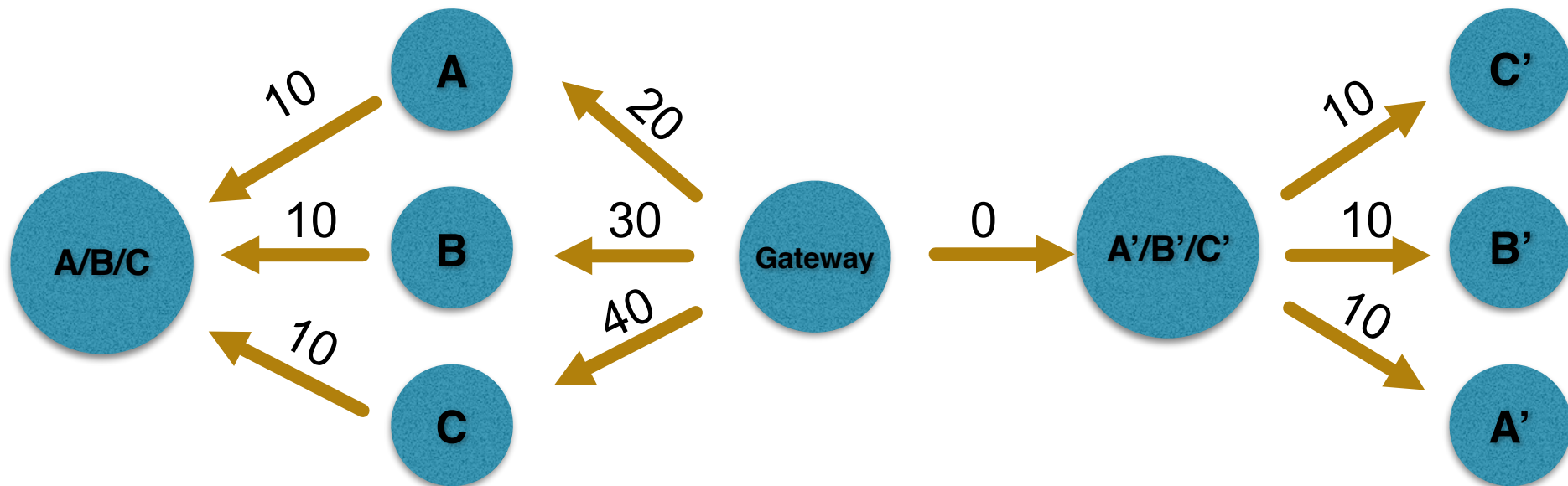
Our Protocol for Atomic Transactions: PathJoin

- ◆ 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



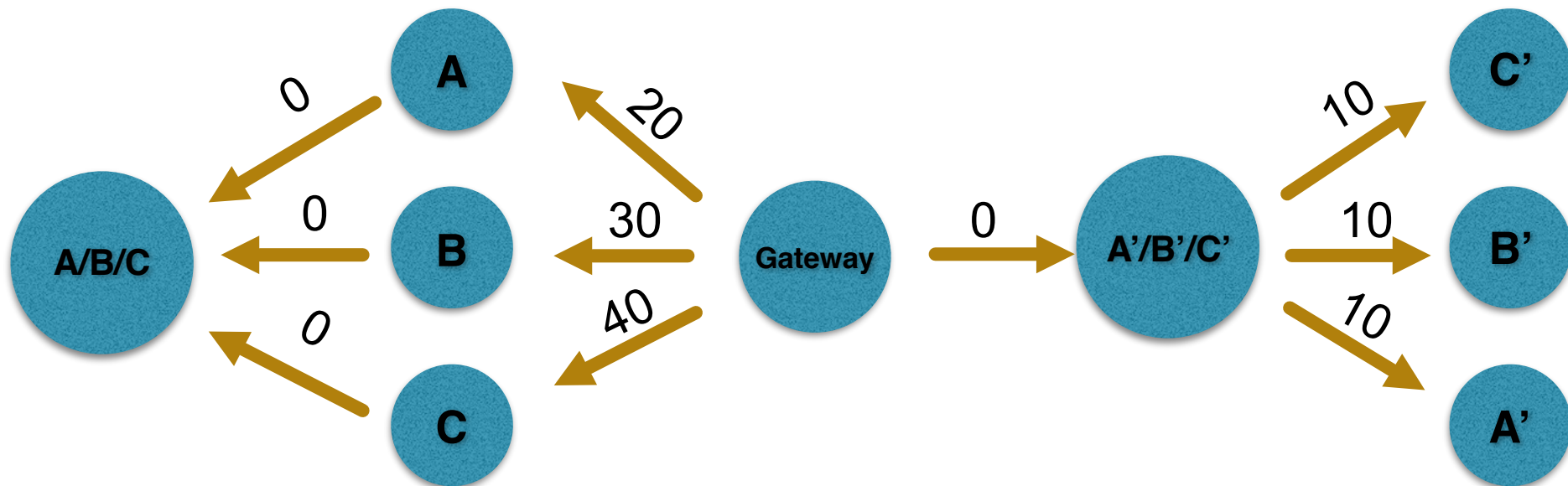
Our Protocol for Atomic Transactions: PathJoin

- ◆ 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



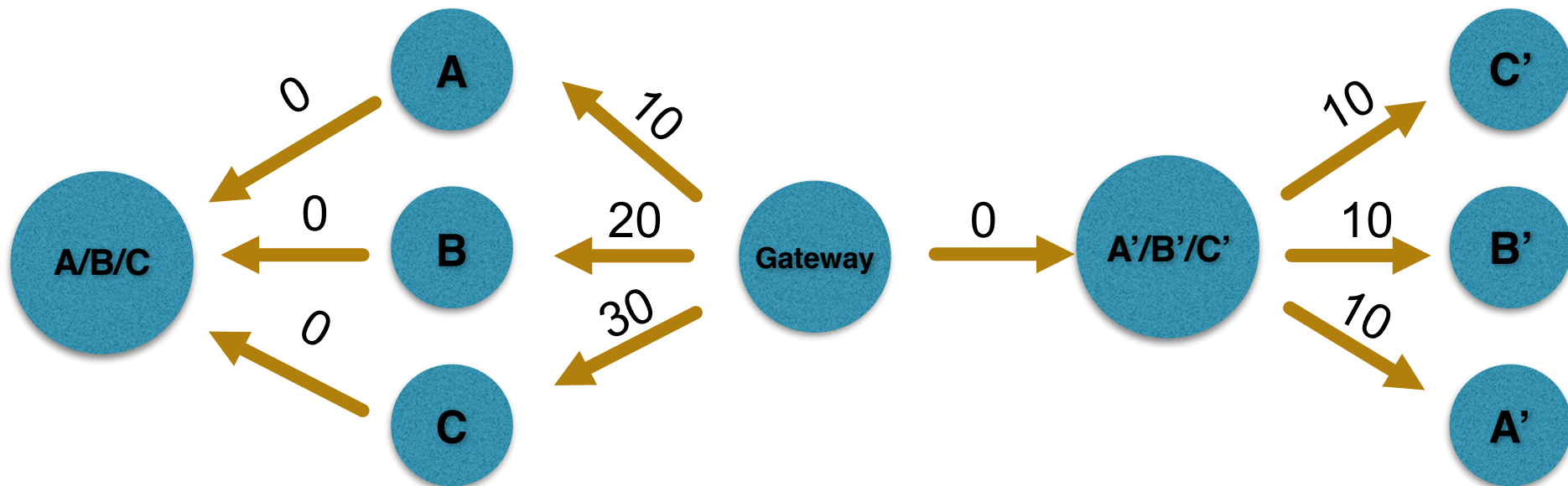
Our Protocol for Atomic Transactions: PathJoin

- ◆ 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



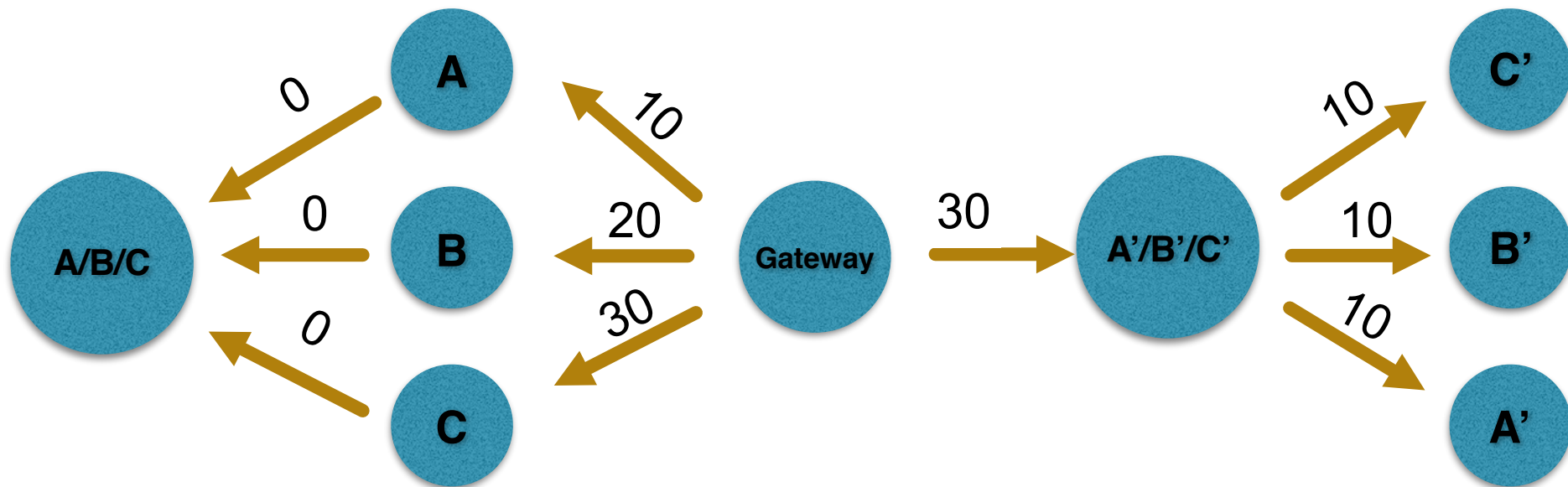
Our Protocol for Atomic Transactions: PathJoin

- ◆ 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



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)

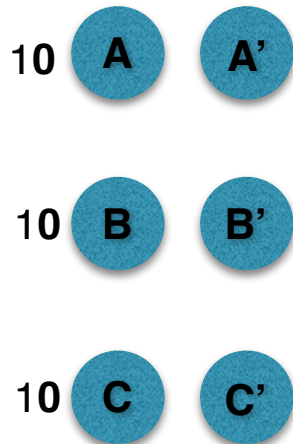
10 **A**

10 **B**

10 **C**

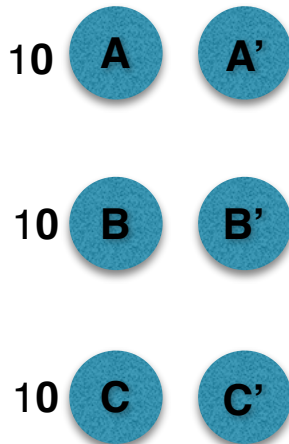
PathShuffle: PathJoin + DiceMix

- ✦ 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)



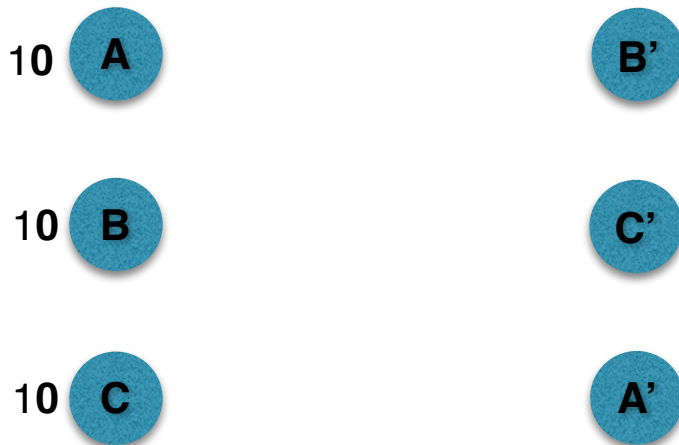
P2P Mixing and Unlinkable Bitcoin Transactions

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)



P2P Mixing and Unlinkable Bitcoin Transactions

Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate.

NDSS '17

Discussion

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)

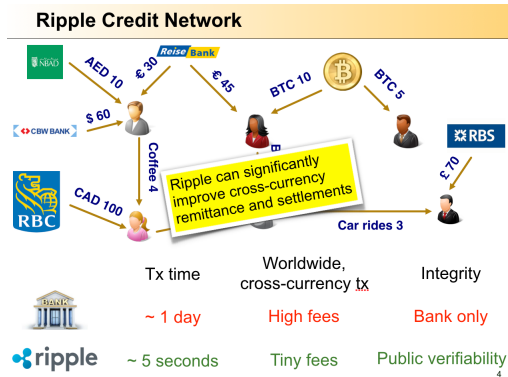
Discussion

- ◆ 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)
- ◆ PathShuffle is a simple smart contract
 - ◆ However, Ripple does not have script language
 - ◆ Are other “scriptless” contracts possible? Limitations?

Take Home Message

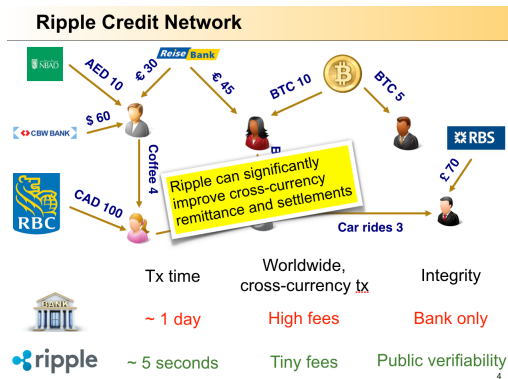
Take Home Message

- ◆ 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

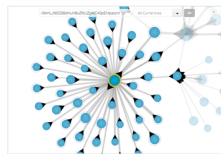
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

| Account | Destination | Amount |
|-----------------------|----------------------|-------------------------|
| rs171242g20f11f4p8kL | rs1729w8n6cvAm8eCZL | 300/USD |
| rL8p9d988Fm11s1L4 | rs1717uL3dMz2DmL4V2L | 75/USD |
| r128P75G8m9W180112L | rs1718uL4uAM8Fv8H8L | 8.88838279948100/USD |
| r12734L8Jm_0Rm_8k0u8L | r125q8L3X517J7C1817L | 300/USD |
| r1263v9P8u1501P81Ch | rs1718uL4uAM8Fv8H8L | 8.8823888232L/USD |
| r12617uL8uY8F8e82L | r1261y03P8F896X1u8L7 | 1127.33817514883183/USD |
| r12618uL3L3u820L | rs1717uL3dMz2DmL4V2L | 300/USD |
| rs171242g20f11f4p8kL | r125q8L3X517J7C1817L | 999.98/USD |

Credit Graph



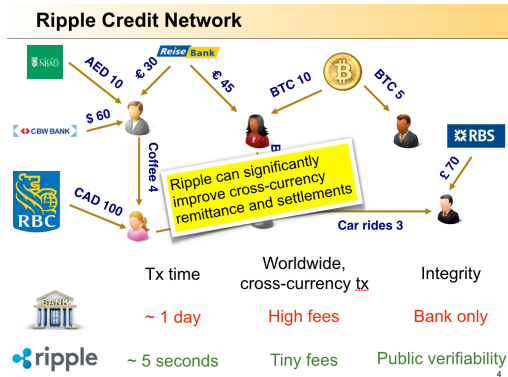
Listening to Whispers of Ripple: Linking Wallets and Deanonimizing Transactions in the Ripple Network

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

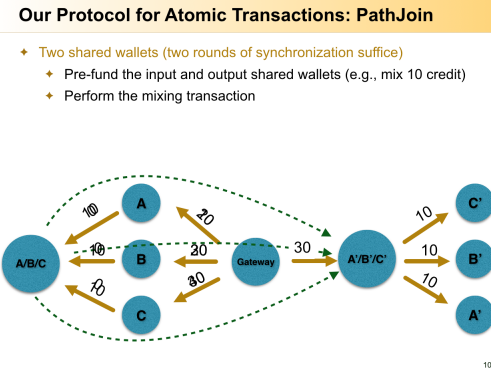
PETS '16

Take Home Message

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



- ◆ **PathJoin**: protocol for **atomic payments** in Ripple with interesting applications



- ◆ There exist **privacy breaches** because of the publicly available Ripple ledger

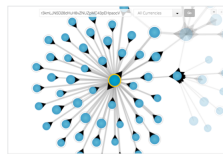
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

| Account | Destination | Amount |
|------------------------|---------------------|---------|
| hsv1TFLKzqzG0F11Fq9kSL | rf9VZ9w989cVAmg8CZL | 300 XRP |
| FL8p9d989Fm11S1SL | rf9VZ9w989cVAmg8CZL | 75 XRP |
| h289T9G989Fm11S1SL | rf9VZ9w989cVAmg8CZL | 8 XRP |
| H279d989Fm11S1SL | rf9VZ9w989cVAmg8CZL | 300 XRP |
| h289T9G989Fm11S1SL | rf9VZ9w989cVAmg8CZL | 8 XRP |
| h289T9G989Fm11S1SL | rf9VZ9w989cVAmg8CZL | 8 XRP |
| h289T9G989Fm11S1SL | rf9VZ9w989cVAmg8CZL | 8 XRP |
| h289T9G989Fm11S1SL | rf9VZ9w989cVAmg8CZL | 8 XRP |
| h289T9G989Fm11S1SL | rf9VZ9w989cVAmg8CZL | 8 XRP |

Credit Graph



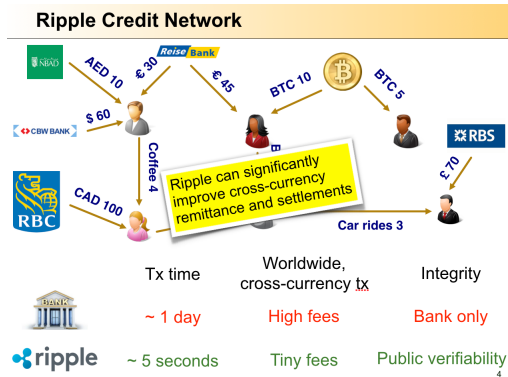
Listening to Whispers of Ripple: Linking Wallets and Deanonimizing Transactions in the Ripple Network

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

PETS '16

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

Public Verifiability & Privacy Problem

The Ripple Ledger Credit Graph

Transaction Details

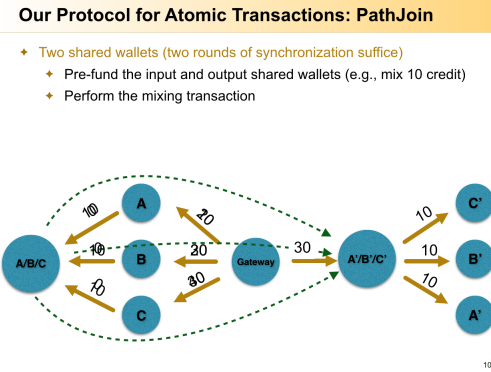
| Account | Destination | Amount |
|---------------------|---------------------|-------------|
| rvnTFLK2g0r311Fq9RL | rvnV2m9n8vAmg8CZL | 300/USD |
| rL8p9d9M8Fm11S1L | rvnRT7uL3dM2ZmAVZC | 75/USD |
| r428P75G5d9W91E18L | rvnT7uL3dM2ZmAVZC | 8/800/USD |
| rH775dL9rJmL8d9dL | rF9gMkA3X5T7C9H3TmL | 300/USD |
| r428P75G5d9W91E18L | rvnT7uL3dM2ZmAVZC | 8/800/USD |
| rH775dL9rJmL8d9dL | rF9gMkA3X5T7C9H3TmL | 300/USD |
| r428P75G5d9W91E18L | rvnT7uL3dM2ZmAVZC | 112/338/USD |
| rH775dL9rJmL8d9dL | rF9gMkA3X5T7C9H3TmL | 300/USD |
| r428P75G5d9W91E18L | rF9gMkA3X5T7C9H3TmL | 999/98/USD |

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

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

PETS '16

- ◆ **PathJoin**: protocol for **atomic payments** in Ripple with interesting applications



- ◆ **PathShuffle**: protocol for **anonymous payments fully compatible** with current Ripple

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)

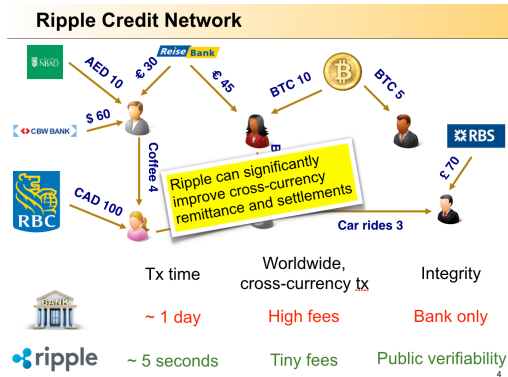
P2P Mixing and Unlinkable Bitcoin Transactions

Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate.

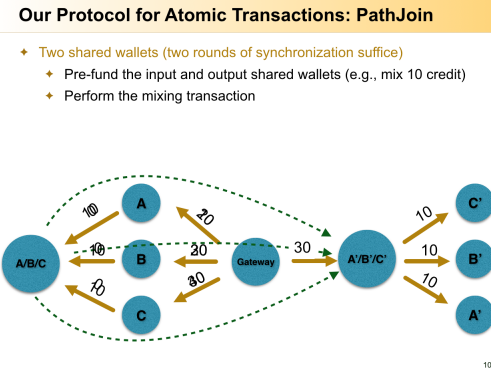
NDSS '17

Take Home Message

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



- ◆ **PathJoin**: protocol for **atomic payments** in Ripple with interesting applications



- ◆ There exist **privacy breaches** because of the publicly available Ripple ledger

Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

| Account | Destination | Amount |
|---------------------|---------------------|------------|
| hsv1TFLK2g0F11FqRkL | rfv2Zm9h8cVAmg8CzL | 300/ripple |
| HL8p9d9M8Fm11S1L | rfv1TFLK2g0F11FqRkL | 75/ripple |
| h2B75G10d9M8Fm11S1L | rfv1TFLK2g0F11FqRkL | 8/ripple |
| H275d9M8Fm11S1L | rfv2Zm9h8cVAmg8CzL | 300/ripple |
| h2K9V9p9d9M8Fm11S1L | rfv1TFLK2g0F11FqRkL | 8/ripple |
| rfv1TFLK2g0F11FqRkL | rfv2Zm9h8cVAmg8CzL | 112/ripple |
| h2K9V9p9d9M8Fm11S1L | rfv1TFLK2g0F11FqRkL | 300/ripple |
| h2K9V9p9d9M8Fm11S1L | rfv2Zm9h8cVAmg8CzL | 999/ripple |

Credit Graph

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

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

PETS '16

- ◆ **PathShuffle**: protocol for **anonymous payments fully compatible** with current Ripple

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

Thanks!
@pedrorechez