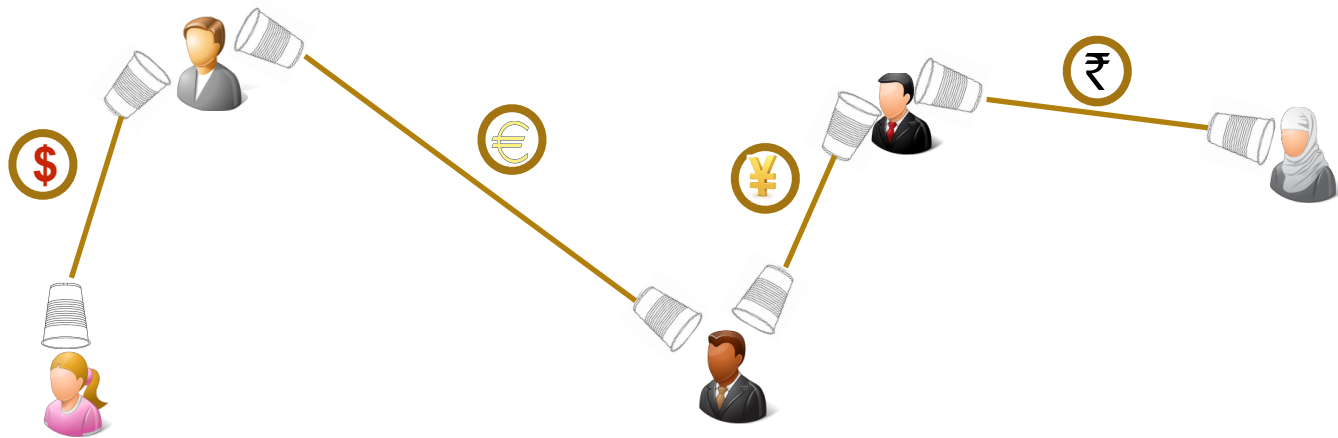


SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks



Giulio Malavolta
Saarland University

Pedro Moreno-Sanchez
Purdue University

Aniket Kate
Purdue University

Matteo Maffei
TU Vienna

Yet Another Talk about Cryptocurrencies?

- ✦ TumbleBit and CoinShuffle++ are excellent ideas to provide privacy in Bitcoin

Yet Another Talk about Cryptocurrencies?

- ◆ TumbleBit and CoinShuffle++ are excellent ideas to provide privacy in Bitcoin
- ◆ Bitcoin (as other permissionless cryptocurrencies) relies on a blockchain:
 - ◆ High storage requirement (>100 GB)
 - ◆ High power consumption for proof-of-work



Yet Another Talk about Cryptocurrencies?

- ◆ TumbleBit and CoinShuffle++ are excellent ideas to provide privacy in Bitcoin
- ◆ Bitcoin (as other permissionless cryptocurrencies) relies on a blockchain:
 - ◆ High storage requirement (>100 GB)
 - ◆ High power consumption for proof-of-work

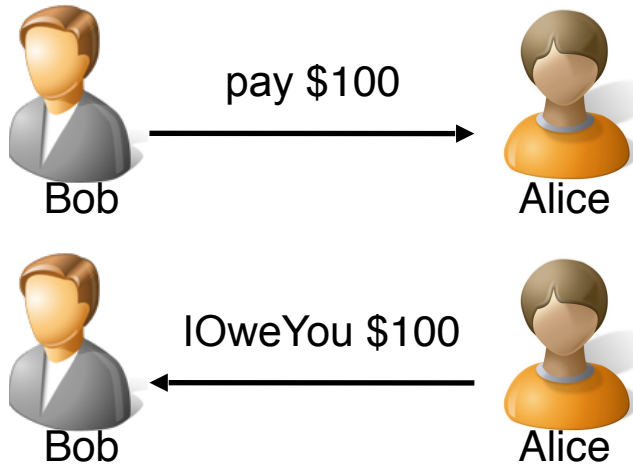


Is it possible to have a decentralized payment system without a blockchain?

Credit (or IOU Settlement) Networks: Basics

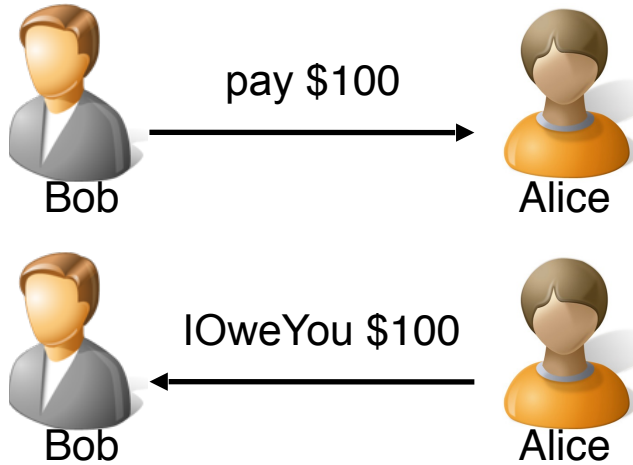
Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

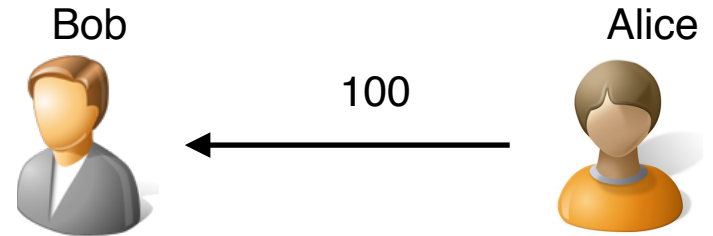


Credit (or IOU Settlement) Networks: Basics

Transactions in the real world

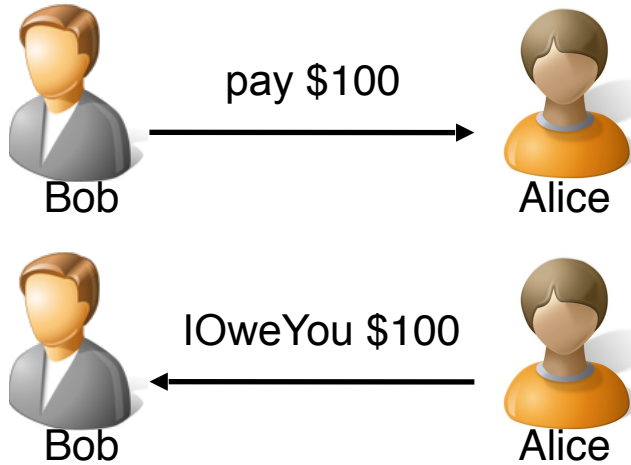


A credit network representation

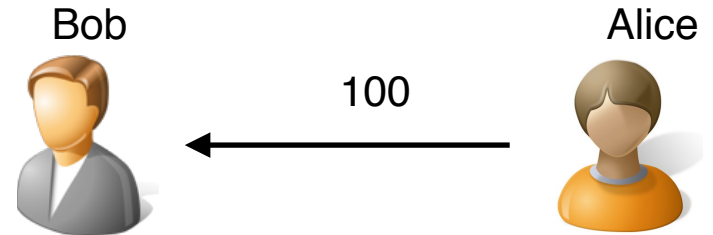


Credit (or IOU Settlement) Networks: Basics

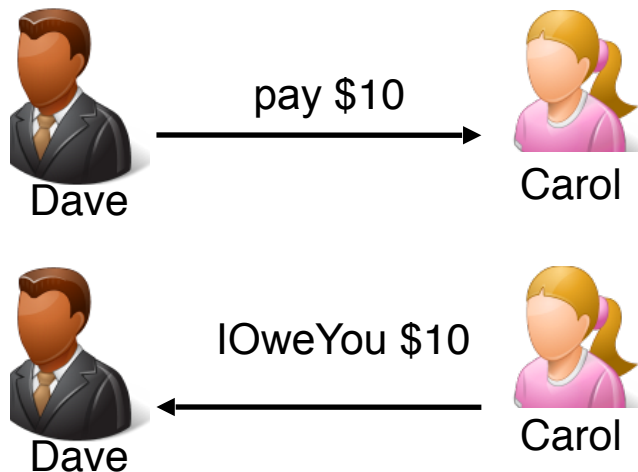
Transactions in the real world



A credit network representation

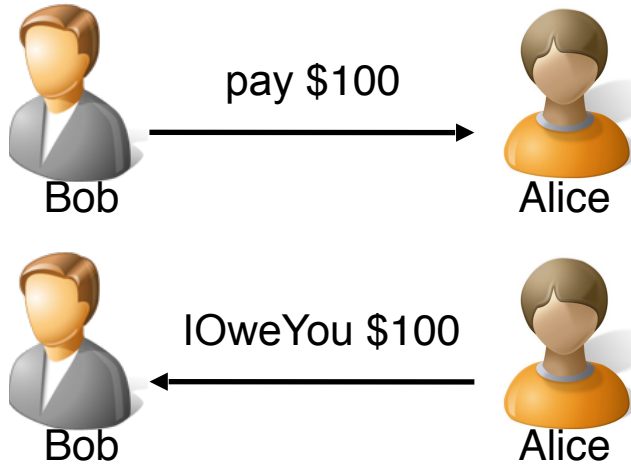


During a hike with Alice & Bob

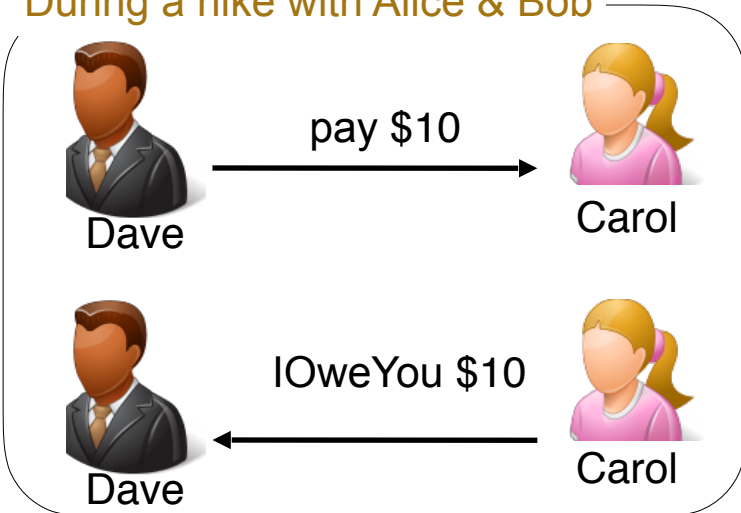


Credit (or IOU Settlement) Networks: Basics

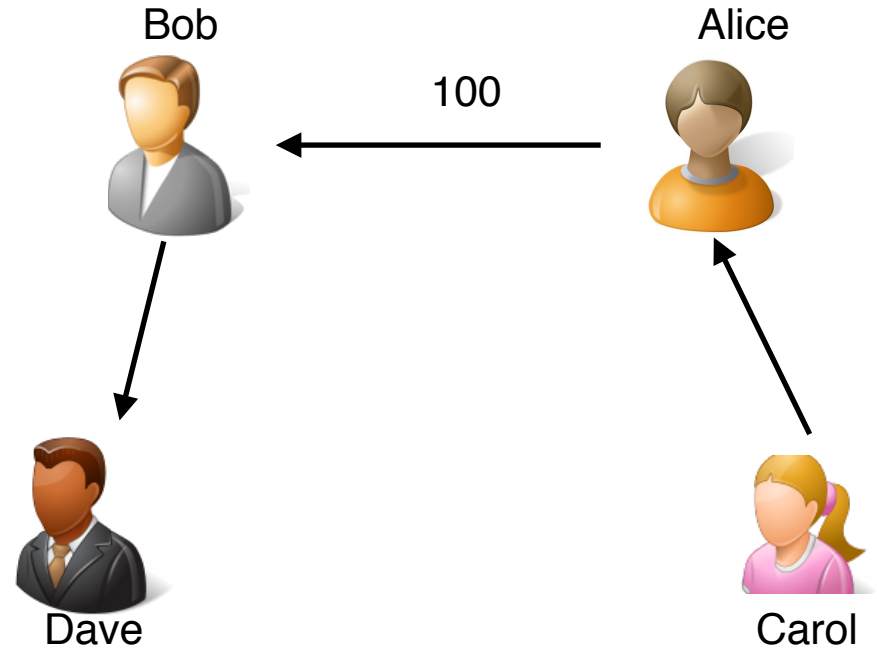
Transactions in the real world



During a hike with Alice & Bob

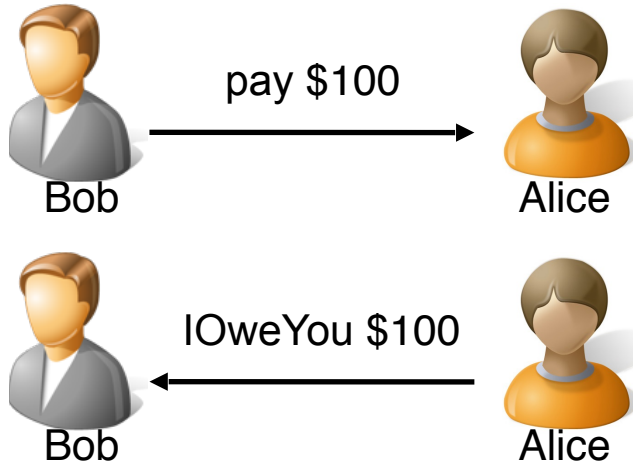


A credit network representation

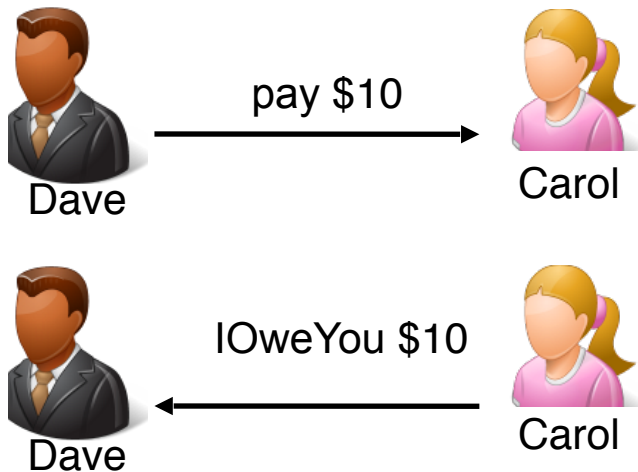


Credit (or IOU Settlement) Networks: Basics

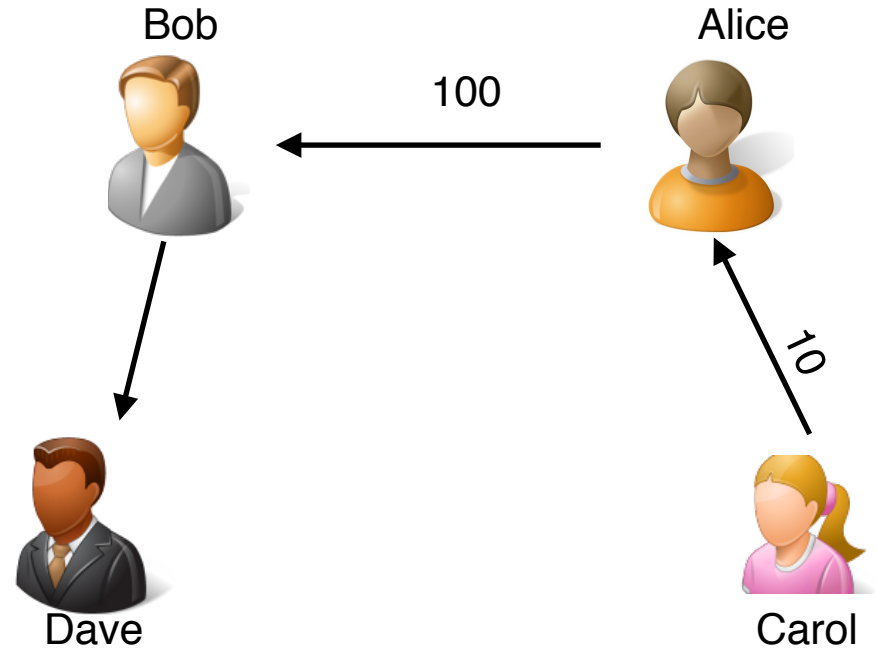
Transactions in the real world



During a hike with Alice & Bob

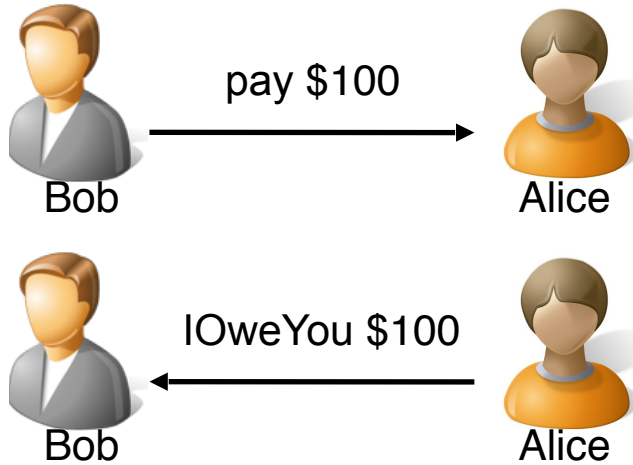


A credit network representation

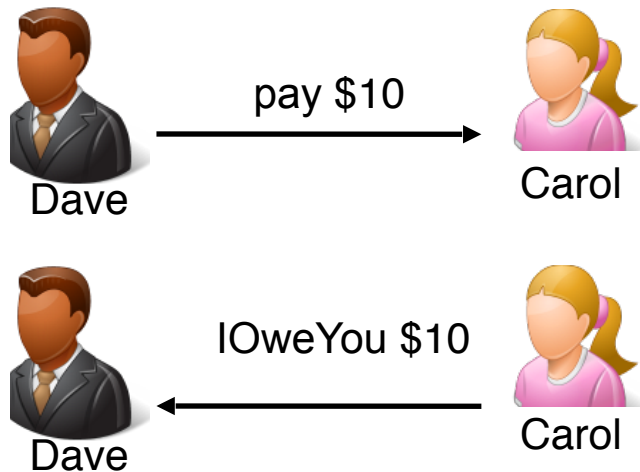


Credit (or IOU Settlement) Networks: Basics

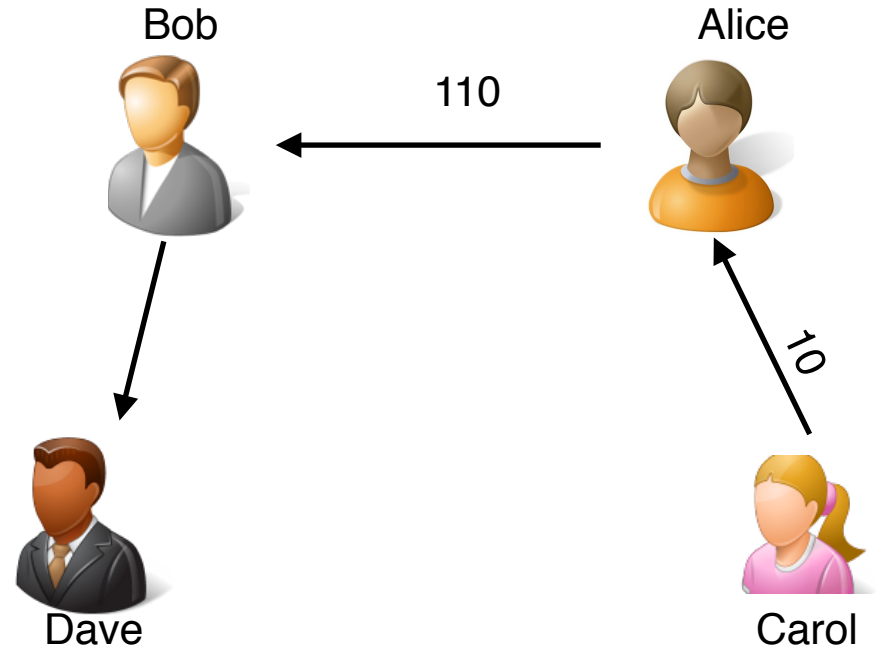
Transactions in the real world



During a hike with Alice & Bob

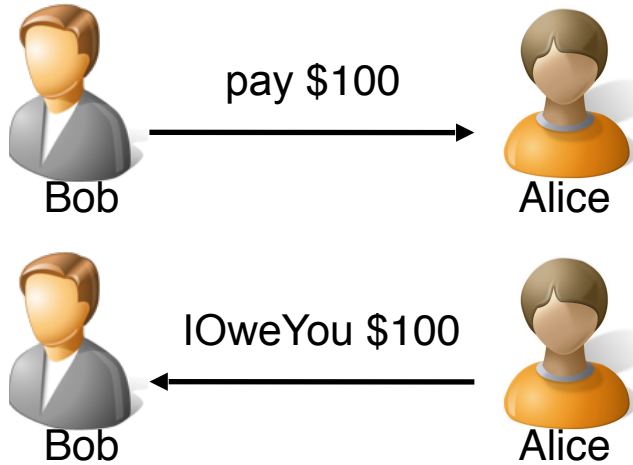


A credit network representation

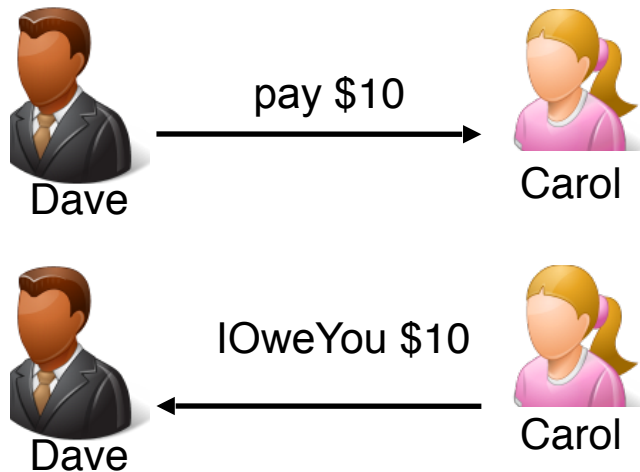


Credit (or IOU Settlement) Networks: Basics

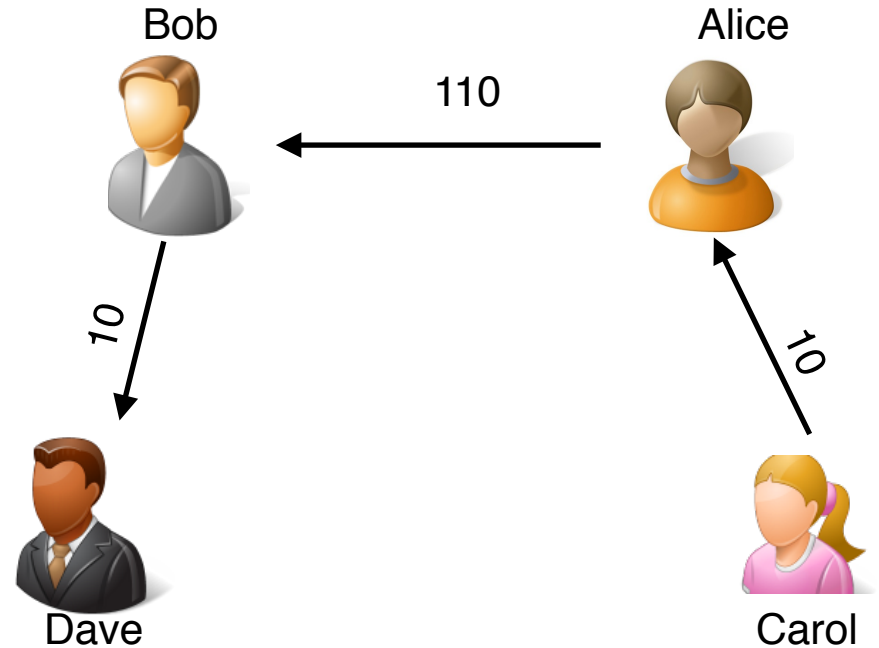
Transactions in the real world



During a hike with Alice & Bob



A credit network representation



Credit Network Examples

- ◆ Academic proposals:

- ◆ Ostra: preventing e-mail spam [NSDI'08]



- ◆ Bazaar: strengthening e-commerce [NSDI'11]



- ◆ SumUp: Sybil-resilient content voting [NSDI'09]



- ◆ Industry deployments:

- ◆ Ripple: A real-life online payment network



- ◆ Stellar: Another real-life online payment network



Credit Network Examples

- ◆ Academic proposals:

- ◆ Ostra: preventing e-mail spam [NSDI'08]



- ◆ Bazaar: strengthening e-commerce [NSDI'11]



- ◆ SumUp: Sybil-resilient content voting [NSDI'09]



- ◆ Industry deployments:

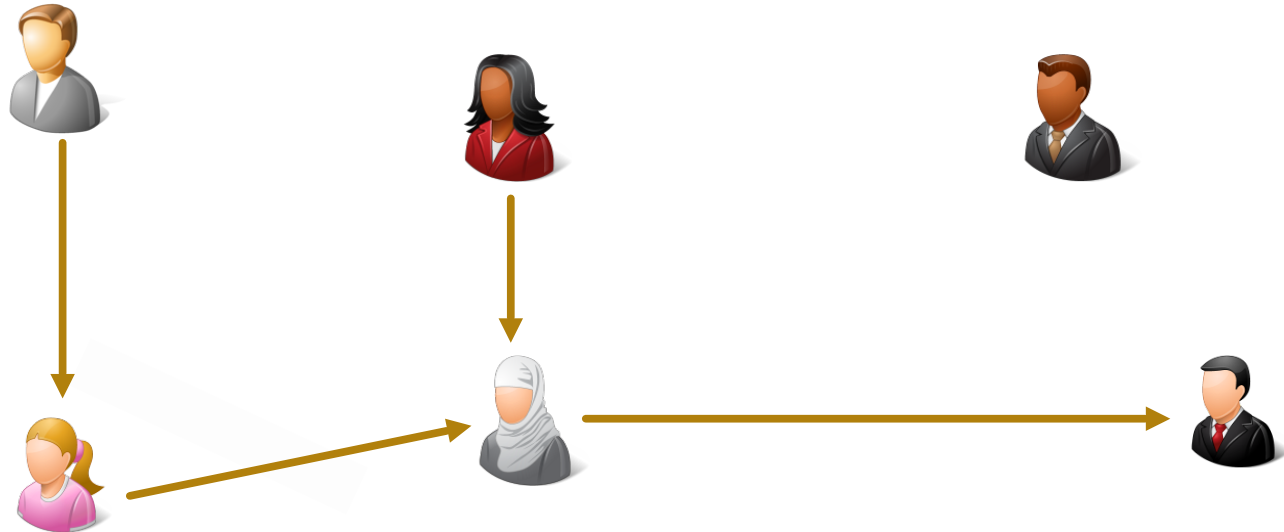
- ◆ Ripple: A real-life online payment network



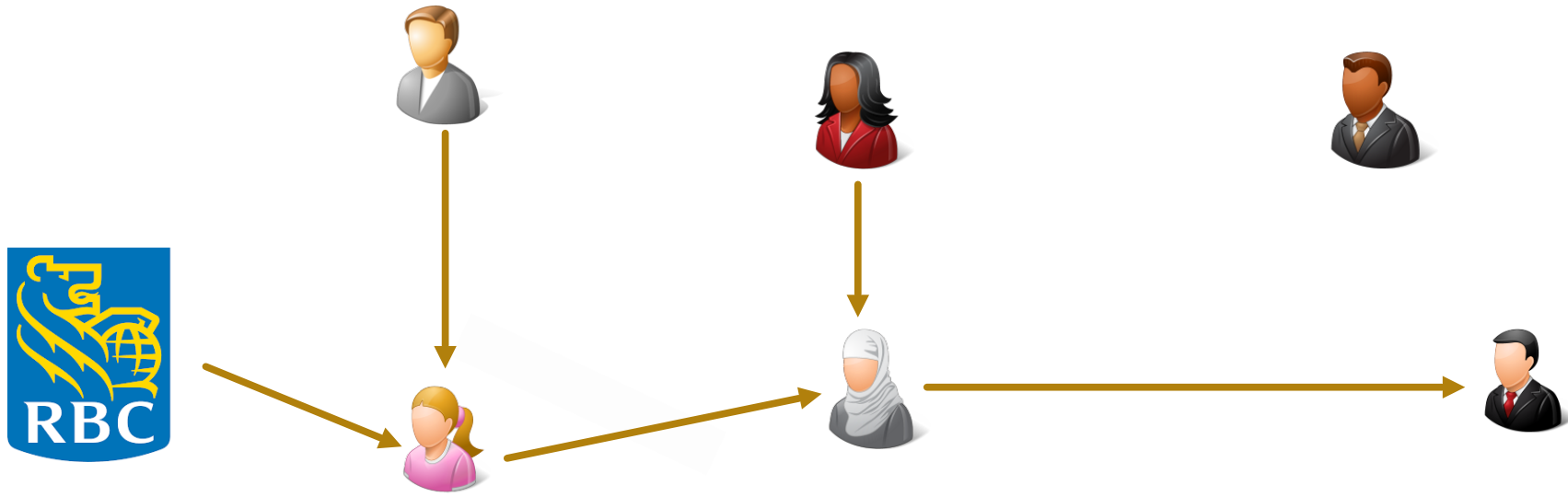
- ◆ Stellar: Another real-life online payment network



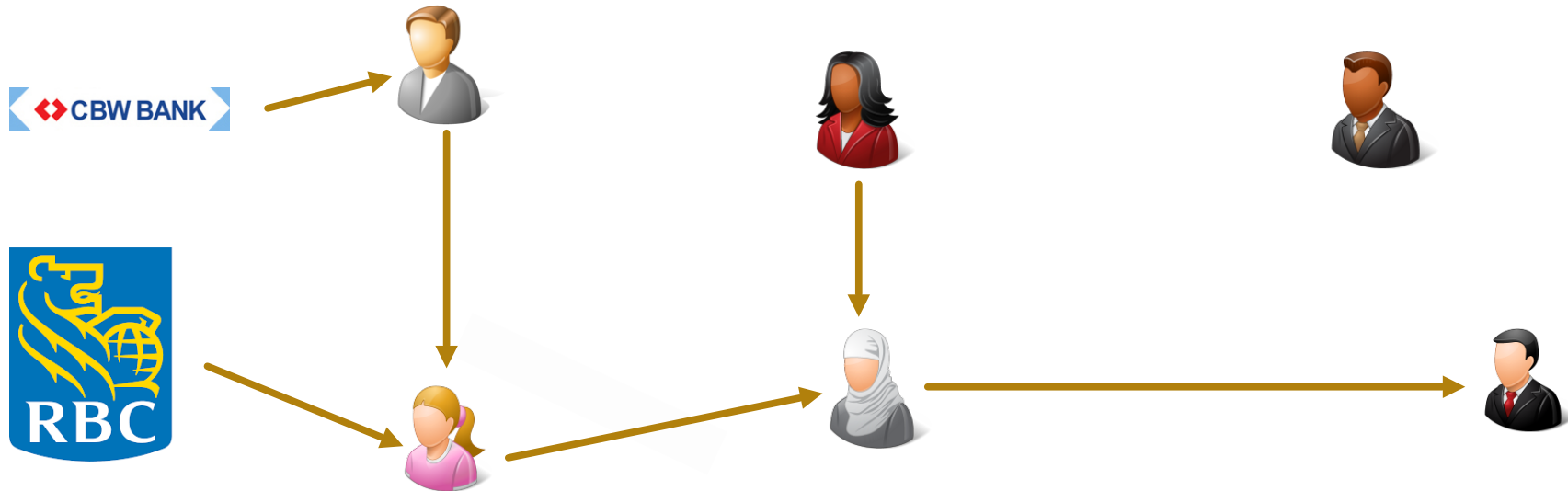
Ripple Credit Network



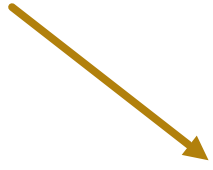
Ripple Credit Network



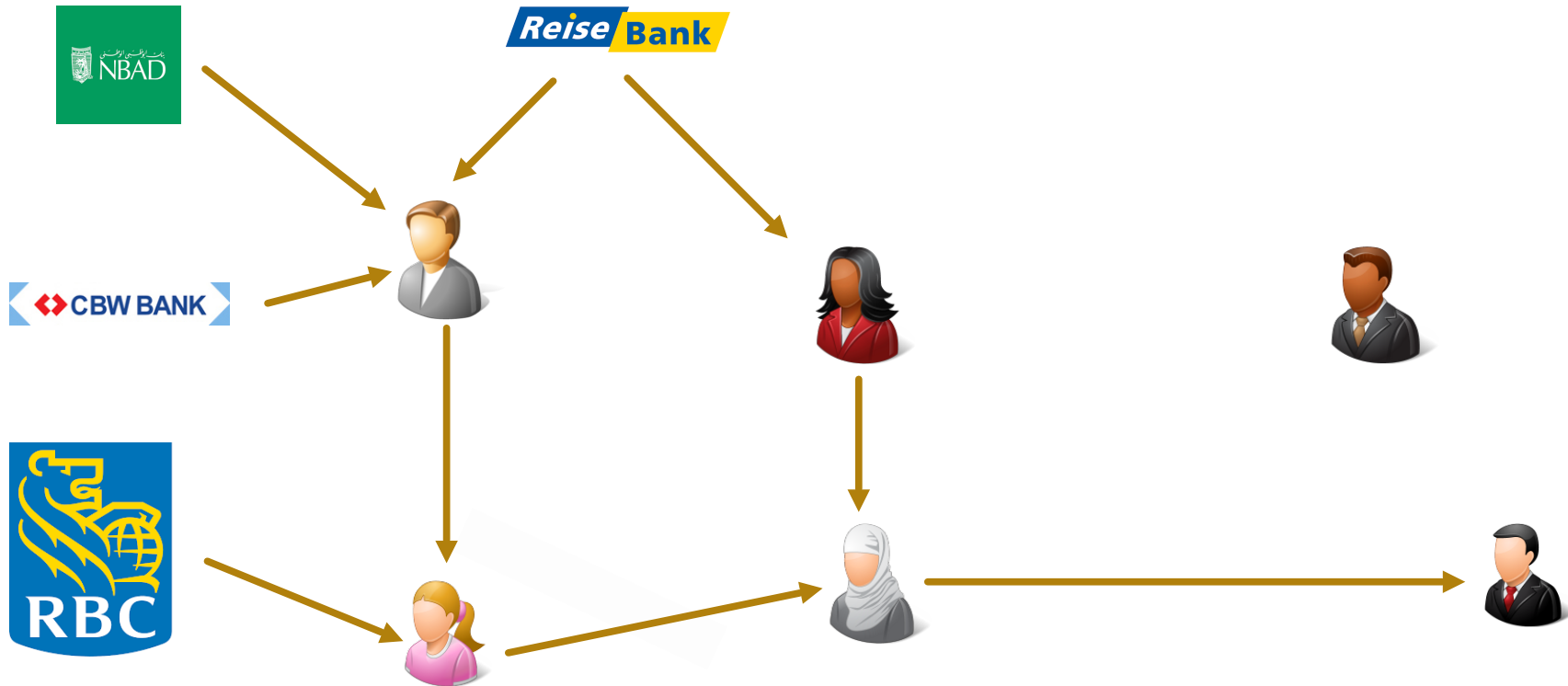
Ripple Credit Network



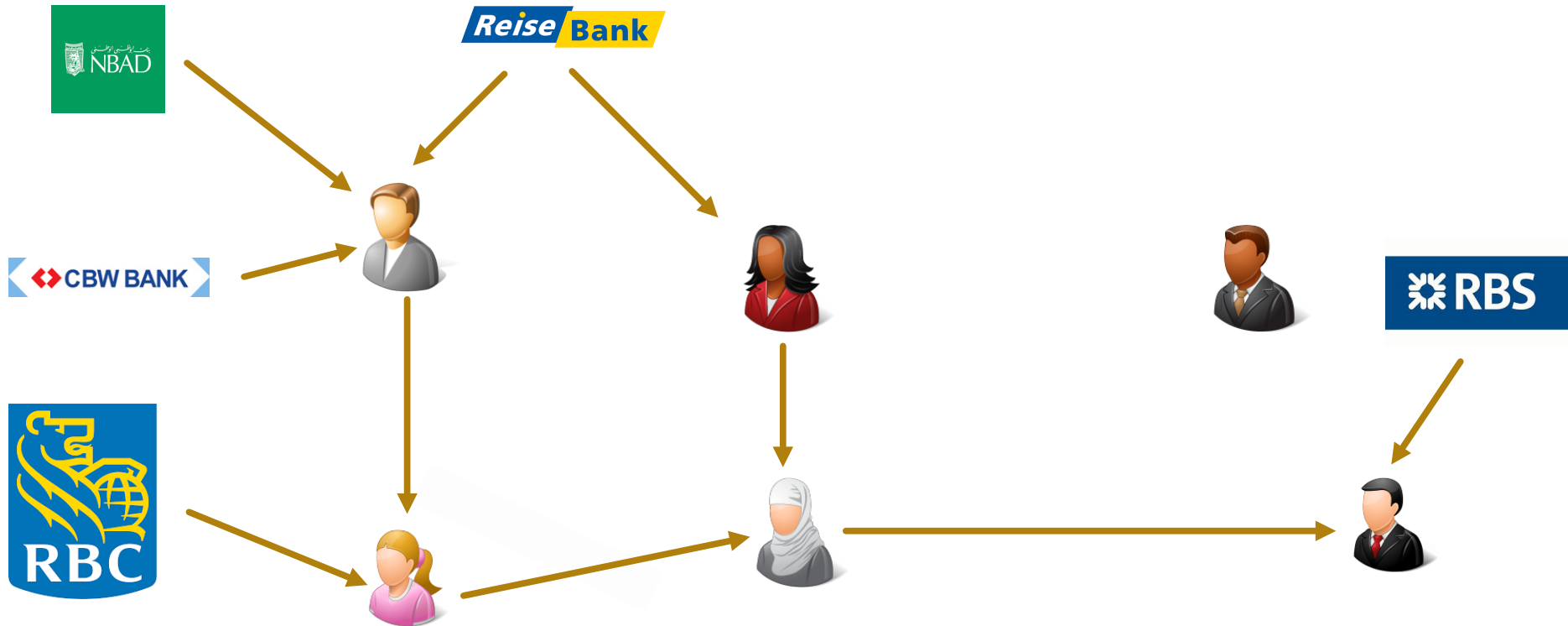
Ripple Credit Network



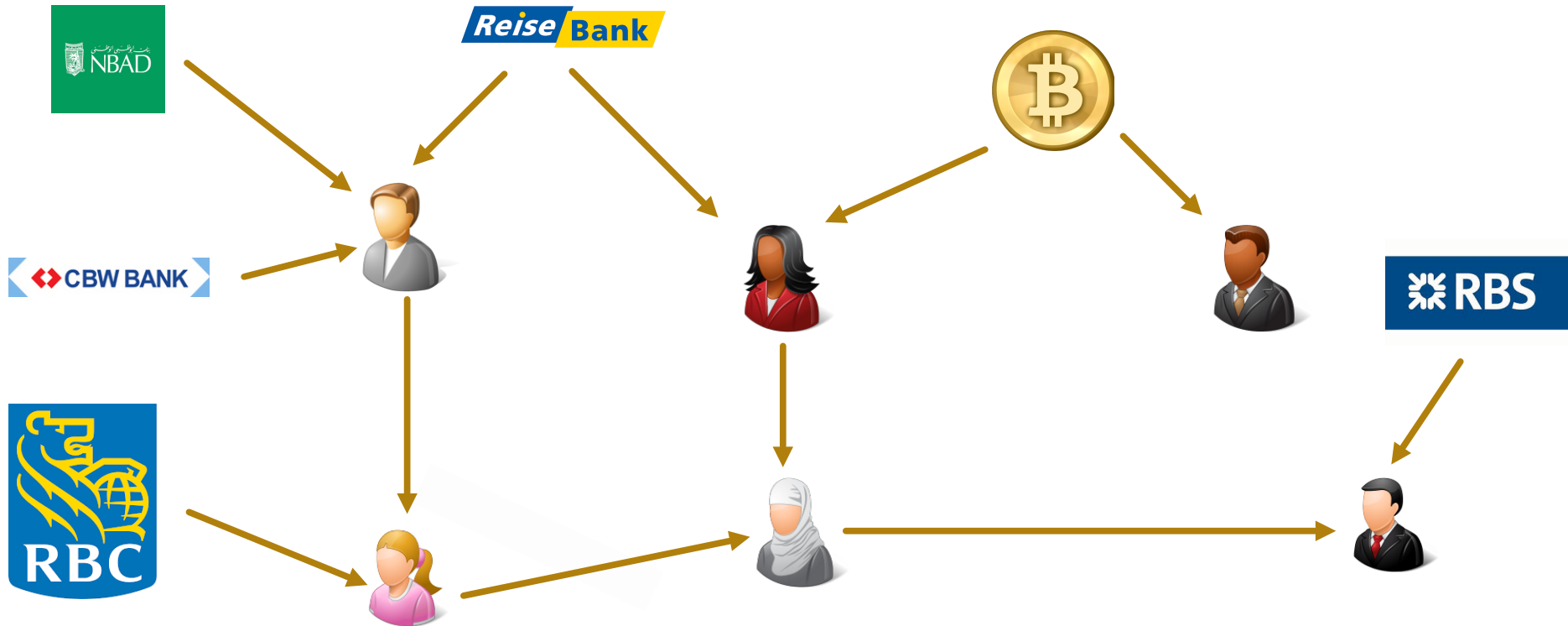
Ripple Credit Network



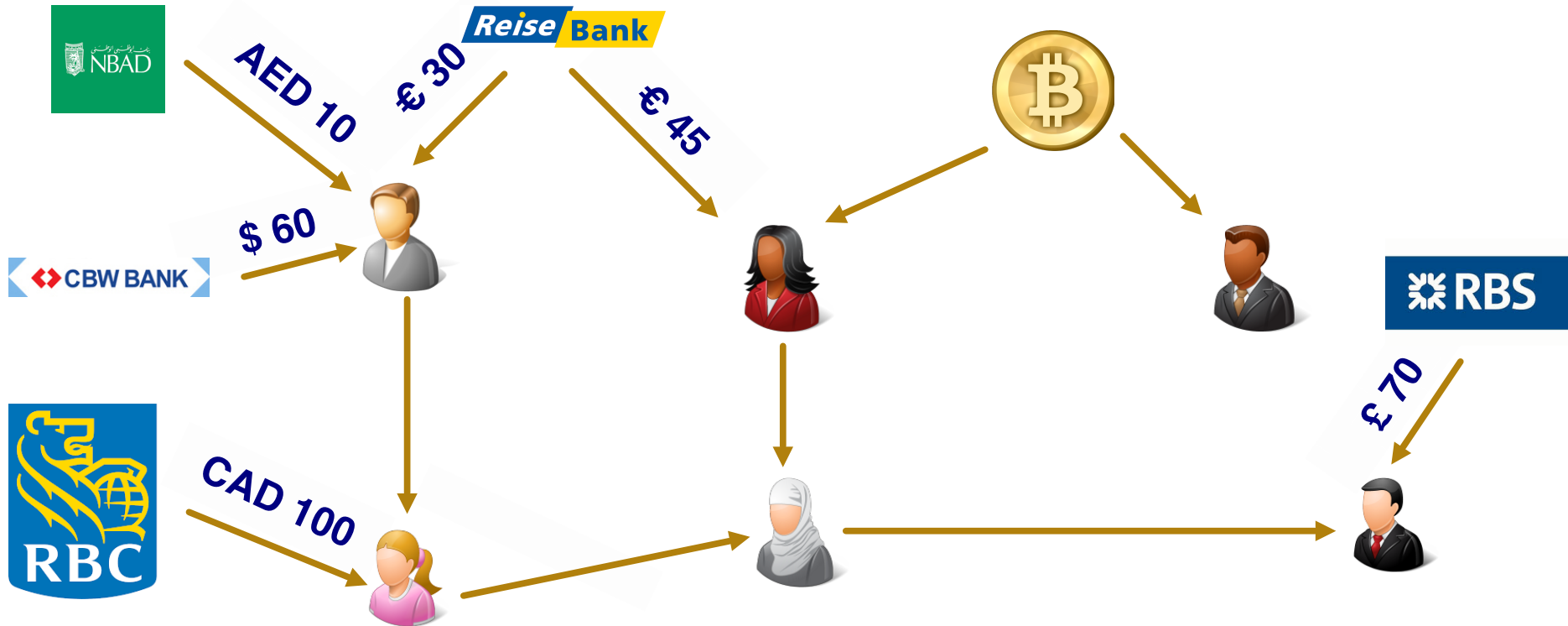
Ripple Credit Network



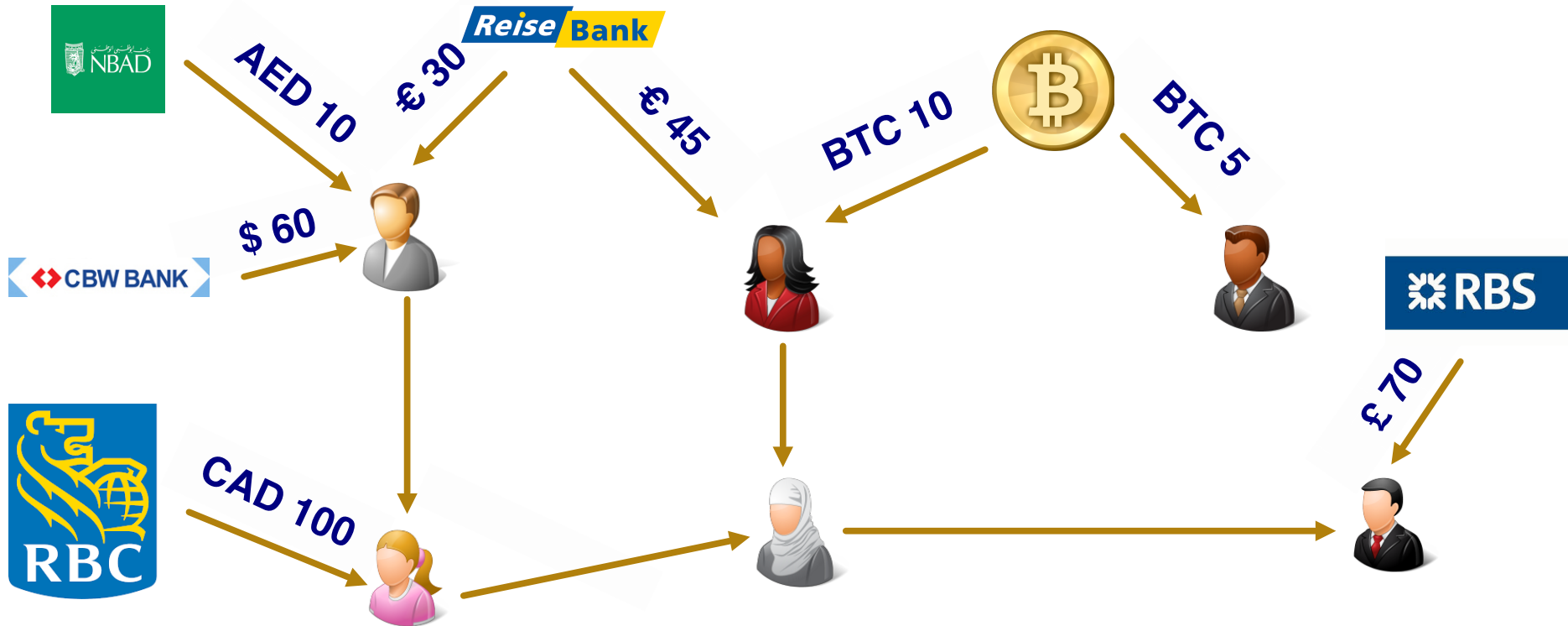
Ripple Credit Network



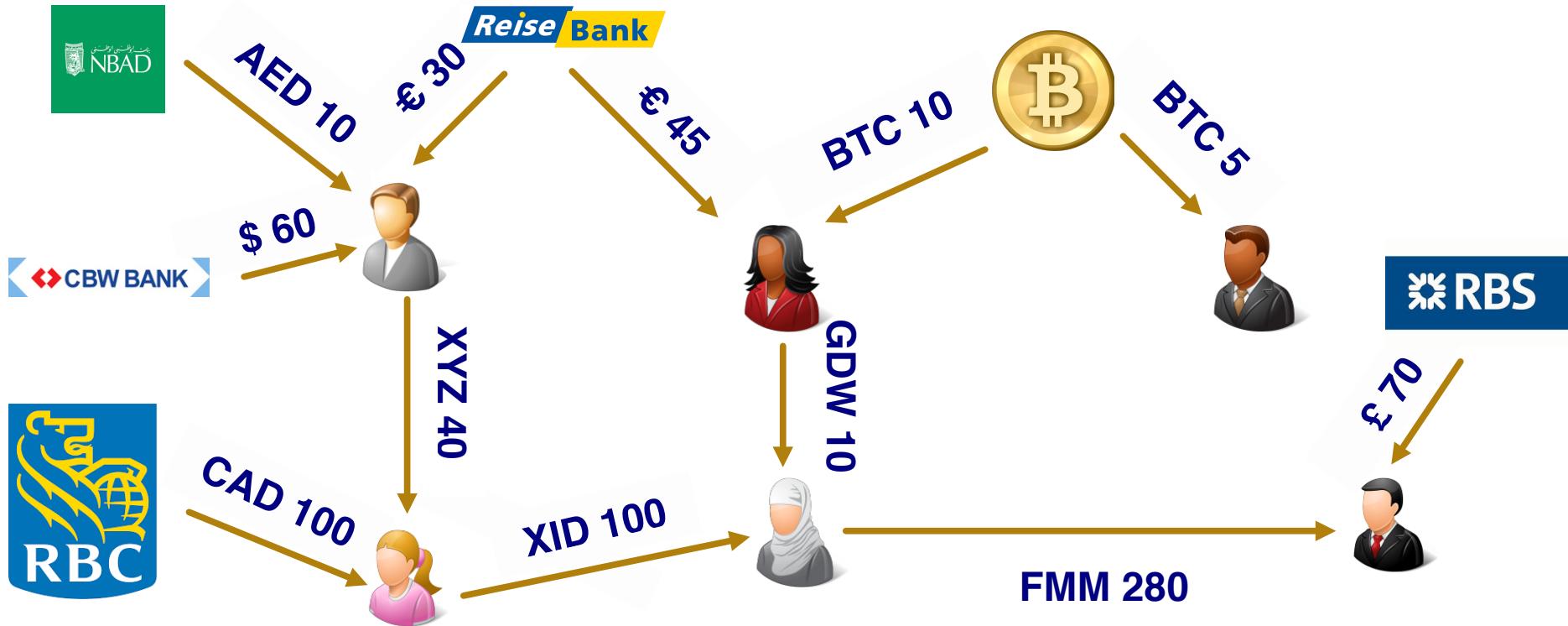
Ripple Credit Network



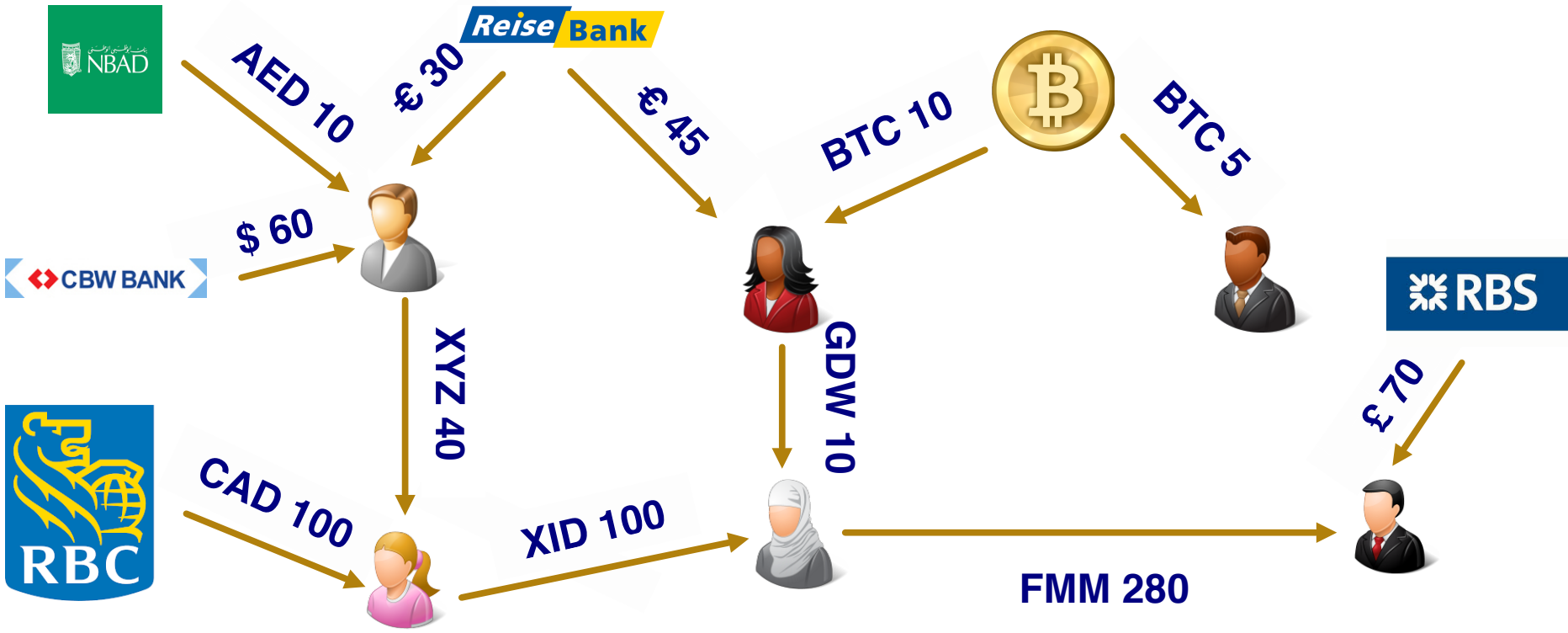
Ripple Credit Network



Ripple Credit Network



Ripple Credit Network



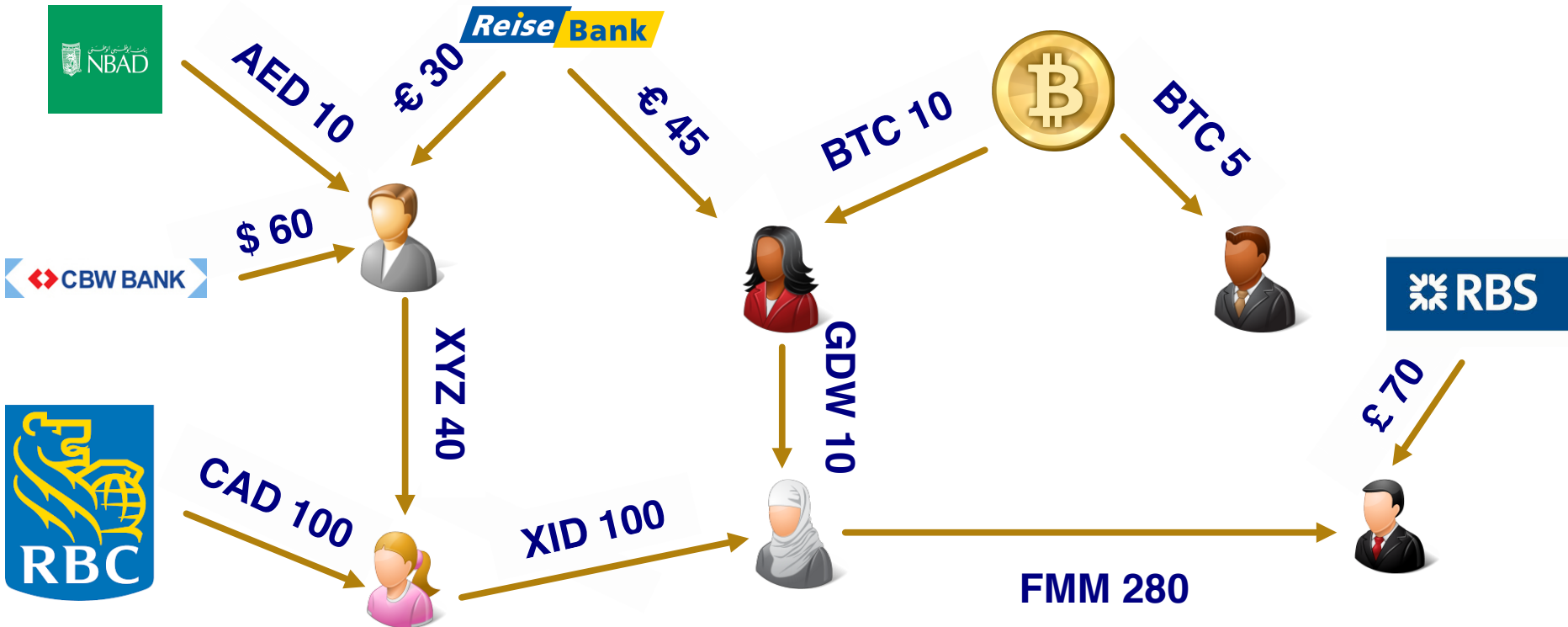
Tx time

Worldwide,
cross-currency tx

Integrity



Ripple Credit Network



Tx time

Worldwide,
cross-currency tx

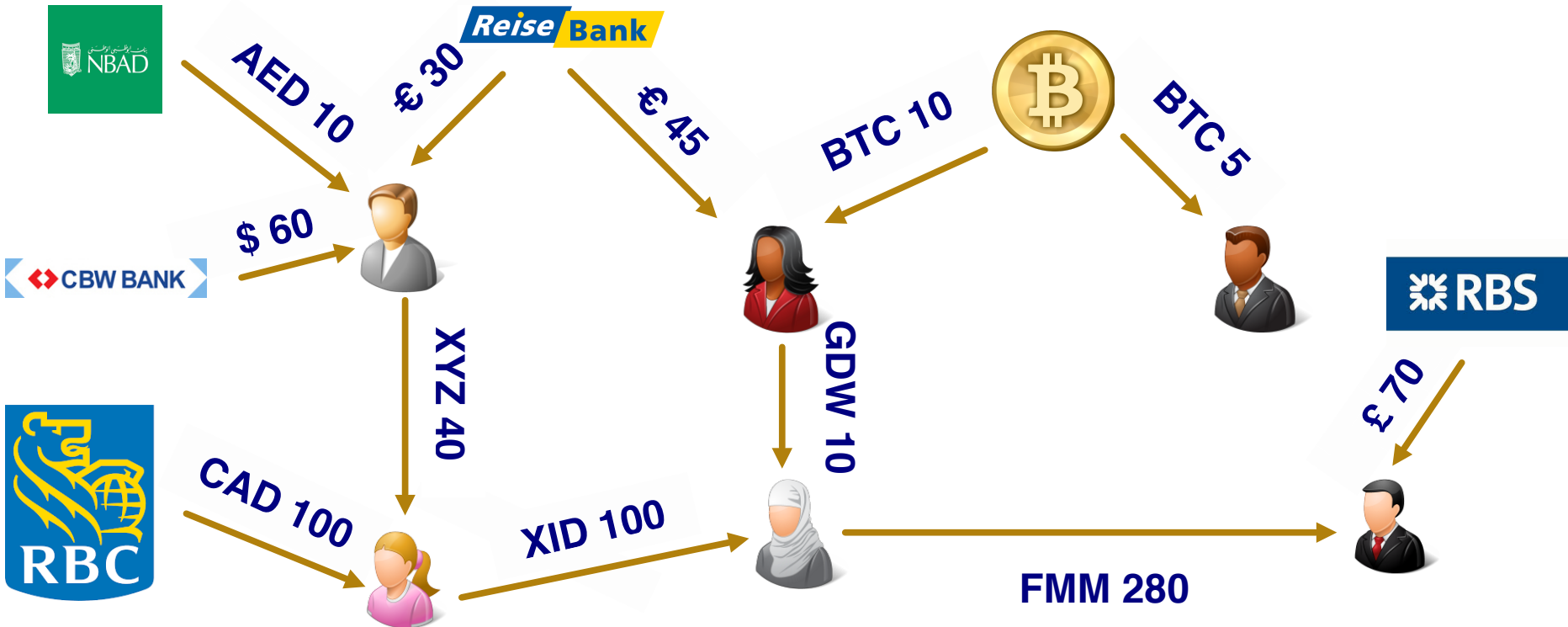
Integrity

~ 1 day

~ 5 seconds



Ripple Credit Network



Tx time

~ 1 day

~ 5 seconds

Worldwide,
cross-currency tx

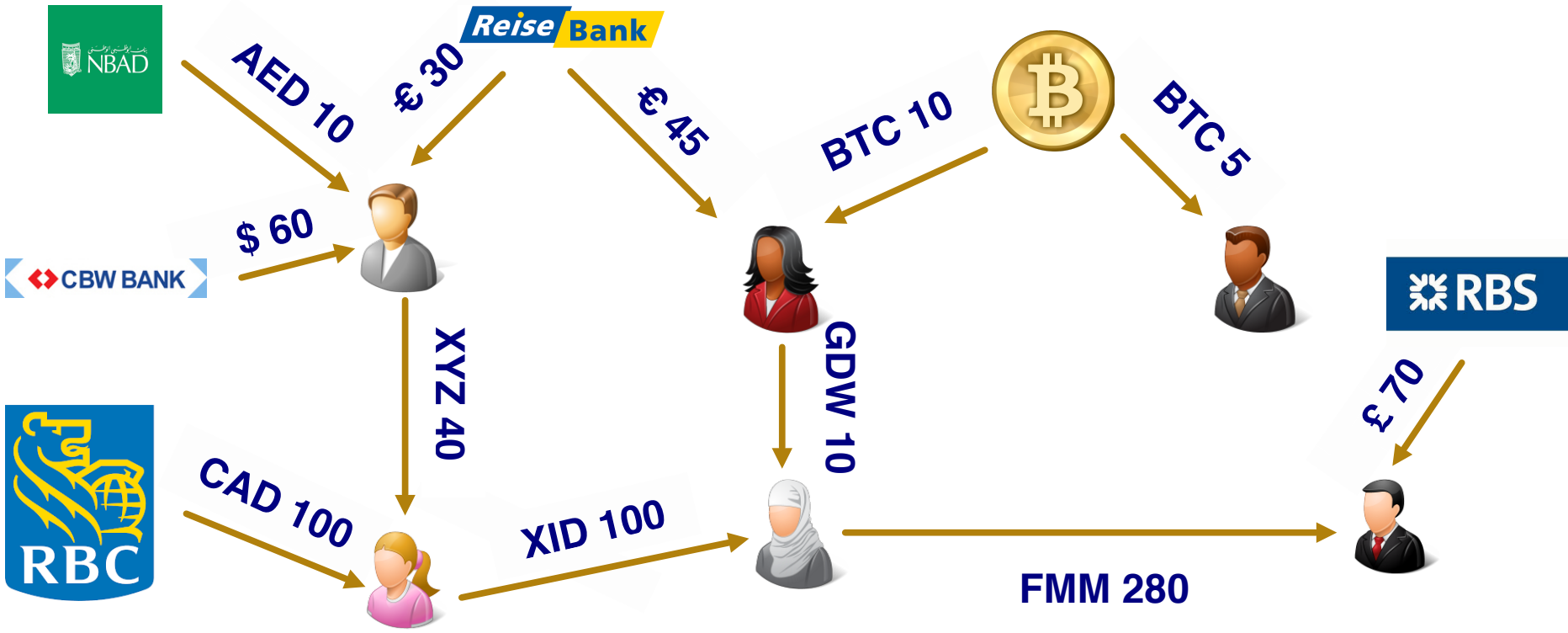
High fees

Tiny fees

Integrity



Ripple Credit Network



Tx time

~ 1 day

Worldwide,
cross-currency tx

High fees

Integrity

Bank only

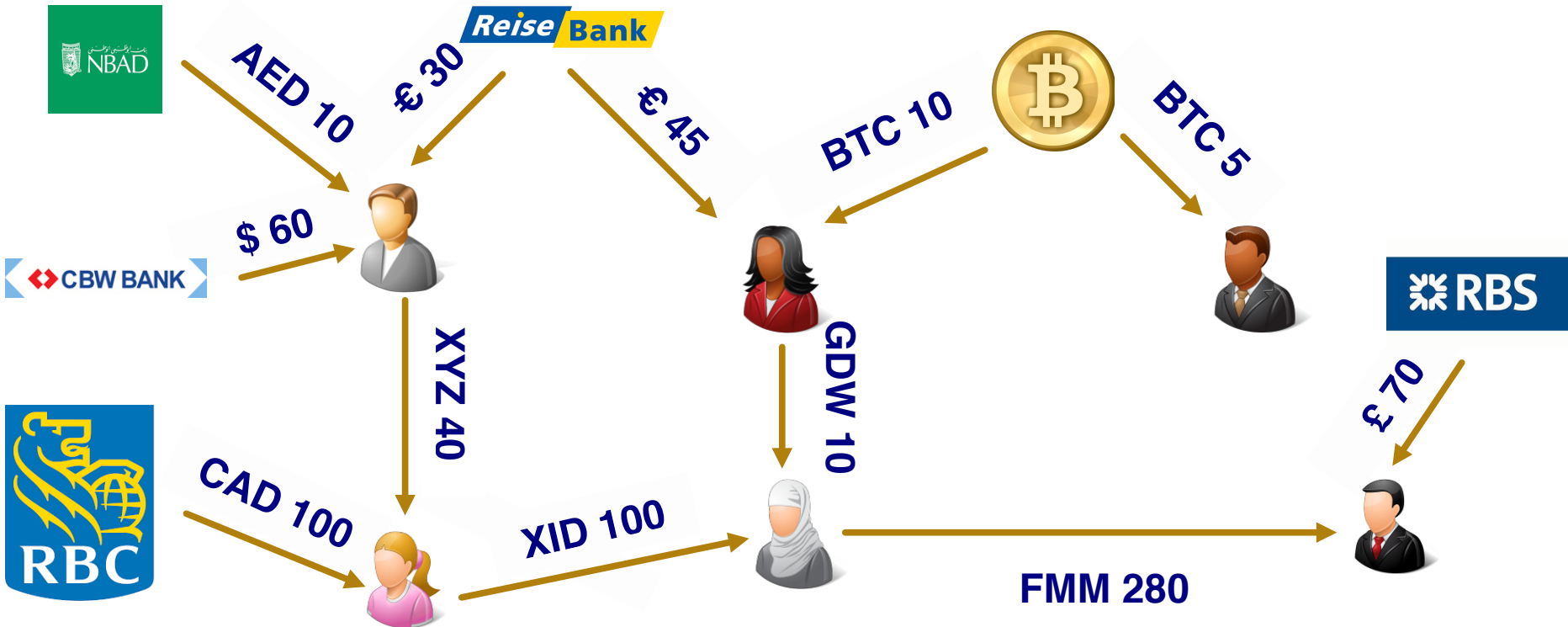
~ 5 seconds

Tiny fees

Public verifiability



Ripple Credit Network



Tx time
Worldwide,
cross-currency

Integrity

~ 10
~ 5 sec
Ripple can significantly
improve cross-currency
remittance and settlements
any fees

Bank only

Public verifiability



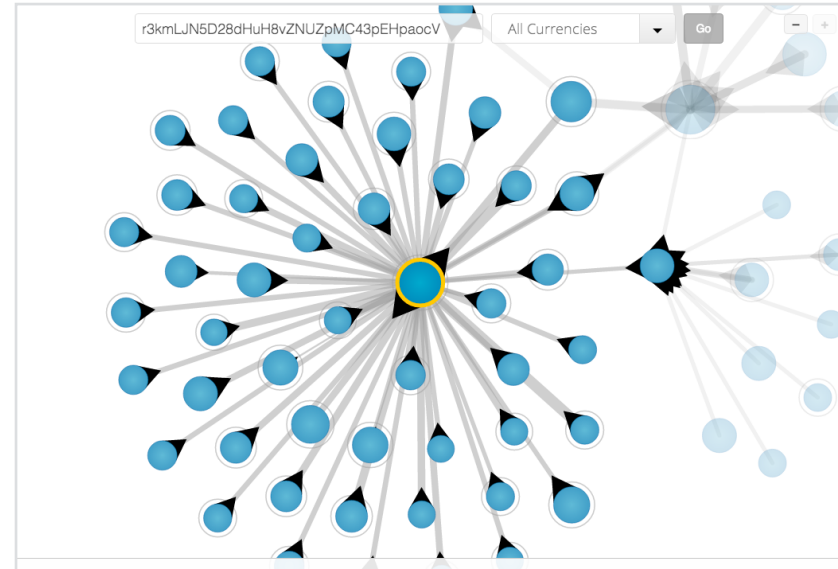
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

Account	Destination	Amount
rhwctTPLKZqK59f1fXpDkQ...	rMnVZ9maUWp5cAvmqBECZM...	300/XRP
rLSBpSquSHKbbfvcKt1c54...	rKoDt7VL83AKJZewLxVZE...	75/XRP
r428G9fSSmD4SYmnDra16B...	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



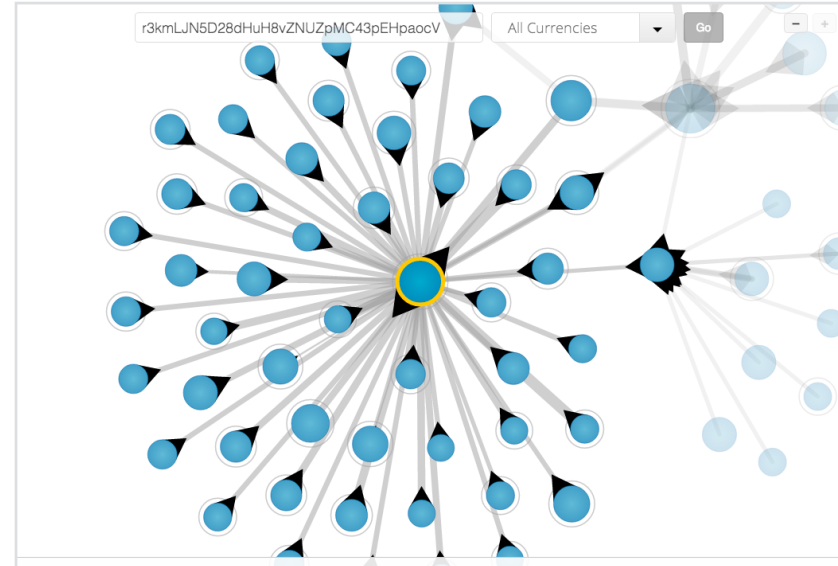
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

Account	Destination	Amount
rwcctTPLKZqK59f1fXpDkQ...	rMnVZ9maUWp5cAvmqBECZM...	300/XRP
rLSBpSquSHKbbfvcKt1c54...	rKoDt7VL83AKJZewLxVZE...	75/XRP
r428G9fSSmD4SYmnDra16B...	rBeToNo4AwHaNBRX2n4BNC...	0.0693402709148/CCK/rB...
rhd759dbJMrzMML4QbvQe9...	r95pwKA1K55fy7EJWrqJ9b...	300/XRP
r42WJGvV9MJJa4t5QcF8Cnx...	rBeToNo4AwHaNBRX2n4BNC...	0.0821058028231/CCK/rB...
rUnr1p7xkuSBxyAqHEopZ5...	r3H4rynDShFMRKwuJcadLY...	1129.916679154465/EUR/...
rW7UfGvzCeZwJxxUEeZHLG...	rBwgTdzMHnouLk5DJJD3xd...	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

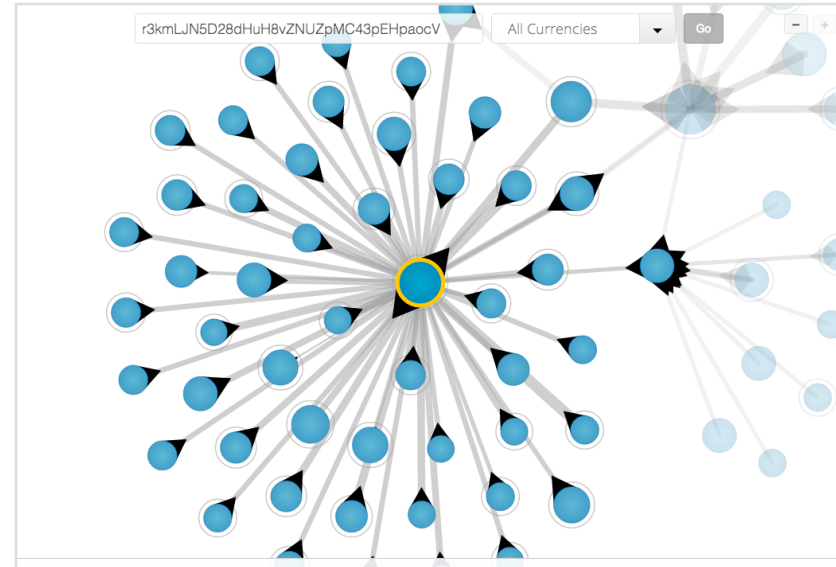
Public Verifiability & Privacy Problem

The Ripple Ledger

Transaction Details

Account	Destination	Amount
rwcctTPLKZqK59f1fXpDkQ...	rMnVZ9maUwp5cAvmqBECZM...	300/XRP
rLSBpSquSHKbbfvcKt1c54...	rKoDt7VL83AKJZewLxVZE...	75/XRP
r428G9fSSmD4SYmnDra16B...	rBeToNo4AwHaNbrX2n4BNC...	0.0693402709148/CCK/rB...
rhd759dbJMrzMML4QbvQe9...	r95pwKA1K55fy7EJWrqJ9b...	300/XRP
r42WJGvV9MJJa4t5QcF8Cnx...	rBeToNo4AwHaNbrX2n4BNC...	0.0821058028231/CCK/rB...
rUnr1p7xkuSBxyAqHEopZ5...	r3H4rynDShFMRKwuJcadLY...	1129.916679154465/EUR/...
rw7UfGvzCeZwJxxUEeZHLG...	rBwgTdzMHnouLk5DJD3xd...	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

Current credit networks employ a global ledger

Our Contributions

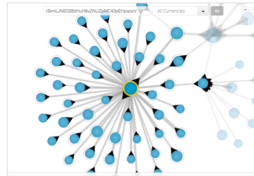
- ◆ We question the need for a global ledger and global consensus

The Ripple Ledger

Transaction Details

Account	Destination	Amount
rwwc1TFLZq39F17g9dL...	rRvZ9hMq5cAv8EBCPL	300/XRP
rLS8tq5p8BbFvcc1c3L...	rR0T7UL3kC2wAYZL...	75/XRP
r4289FS0n45Fmra30L...	rBcT0h4wH9K2H4B...	8.8693482795148/CCK/rL...
rD798J9r9ML30v0L...	rSG6u1235F7L3wL378L	300/XRP
r42K5vV9P54H75QFBC1L...	rBcT0h4wH9K2H4B...	8.862350828231/CCK/rL...
rBv1p7k5B8y8q25L...	r3H4Yy05P980uL3u4L...	1129.916678134485/rBv1...
rW7Uf0c2a3u0E63L...	rBwT6Z9H0uL350303L...	100/XRP
r9Wz75TL3KcH85S25L...	rCQas8MVF5aVWck3L...	999.99/XRP

Credit Graph



Our Contributions

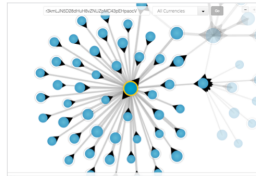
- ◆ We question the need for a global ledger and global consensus

The Ripple Ledger

Transaction Details

Account	Destination	Amount
rwc1TFLZq391E7q9dL...	rWvZ3hMq5cAv8ECP...	300/00P
rL8p5q8b8Fvcc1c3L...	rK0T7LE3kC2wAYZL...	75/00P
r4289F5Dn493mra3D...	rBc7m64wH8RQZ4H8C...	8.869382795148V/CX/rL...
r8D7983W9r8L8D0...	r5G8u1235F7E3wL378...	380/00P
r42K5v9R54472qF8C...	rBc7m64wH8RQZ4H8C...	8.86235882321V/CX/rL...
rBw1p7k658yq8q25...	r384ry058P980u3u8L...	1129.91667813485V/8U...
rW7U6c6Zu3x8E8d6L...	rWq7G298u6LL5D303...	100/00P
rgw2T5TL3KcH85S25...	rCqas8M75aV7Kck3i...	999.99/00P

Credit Graph



- ◆ SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

Inspired by our work in NDSS'15

Our Contributions

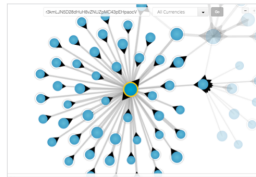
- ◆ We question the need for a global ledger and global consensus

The Ripple Ledger

Transaction Details

Account	Destination	Amount
rwaCTPLAZq391E7q9AL	rWRZ3hMq5CAv8EJCPL	300/00P
rLSBtpq8BbFvcc1c3AL	rR0T7LE3kC2d6AYZEL	75/00P
r4289F5Dm43Fmra32L	rBc7m64wH8RQZ4H8C...	8.869382795148/CDK/rL
r8D7983JWf9ML83Ud9L	r5GmU233F712d3mL	300/00P
r4K25U9f9S4472d7BCAL	rBc7m64wH8RQZ4H8C...	8.862358828231/CDK/rL
rBhr7p7k6u8Bykq8QZL	r384ry02M990u3u4L...	1129.916678134485/USD...
rW7Uf0c2Za3x8E8AL	rWq75Z29H8uL5S03uL	100/00P
rgW2T5TU3KcH852Z9L	rCqas8Mf7sAVrck3uL	999.99/00P

Credit Graph



- ◆ SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

Inspired by our work in NDSS'15

- ◆ SilentWhispers overcomes several challenges: existence of a path, credit on a path and integrity of transactions



Our Contributions

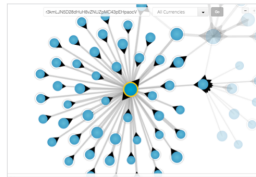
- ◆ We question the need for a global ledger and global consensus

The Ripple Ledger

Transaction Details

Account	Destination	Amount
rweCtPLuZq39117q9nL...	rRvZ3hMq5Cv8BECPL...	300/00P
rL5Btpq8m3bFvcc1c3L...	rR0T7LE3kC2wAYZL...	75/00P
r4289FT5d849Fmra30L...	rBc7m64wH8RQZ4H8C...	8.869382795148/COX/rL...
rB07983W9r8L30u0nL...	r5G8uJ235F71Z3u7nL...	300/00P
r42K5u9R54472u78CnL...	rBc7m64wH8RQZ4H8C...	8.86235082321/COX/rL...
rB8r1g7k6u8By8g8n2L...	r388ry028F980u3u8L...	1129.91667813485/8UR...
rW07f0c2e2a3x868nL...	rB87t028R8uL5503uL...	100/00P
rgW07f0c2e2a3x868nL...	rCq8u8M75aV7K31oL...	999.99/00P

Credit Graph



- ◆ SilentWhispers uses distributed landmark routing, secure multi-party computation and 2-step transactions



- ◆ SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

Inspired by our work in NDSS'15

- ◆ SilentWhispers overcomes several challenges: existence of a path, credit on a path and integrity of transactions



Our Contributions

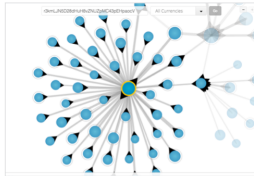
- ◆ We question the need for a global ledger and global consensus

The Ripple Ledger

Transaction Details

Account	Destination	Amount
rwc1TFLZq3S1L7qDnL	rRvZ3MhM5CvAm8ECPzL	300/00P
rL8p5q8b8Fvcc1c3L	rR0T7LE3kC2d6AYZL	75/00P
r4289F5Dn43Fmra3dL	rBc7m64wH8RQZmH8C	8.869382795148/CDK/rL
rB79583Wf9M830v0zL	r5GmHJ235F7L3wL37mL	300/00P
r42K509H5475QvF8CzL	rBc7m64wH8RQZmH8C	8.86235082321/CDK/rL
rB7m64wH8RQZmH8C	r384ry02M980u3u4L	1129.91667813485/USD/rL
rB7m64wH8RQZmH8C	rBw7t02M980u3u4L	100/00P
rgw12TtL3KcH855Z5wL	rCqas8MfT5aVtKck3oL	999.99/00P

Credit Graph



- ◆ SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

Inspired by our work in NDSS'15

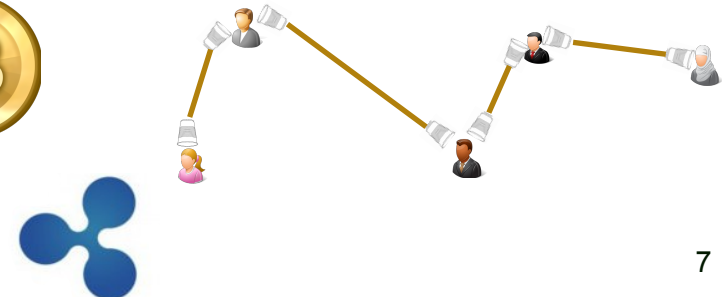
- ◆ SilentWhispers overcomes several challenges: existence of a path, credit on a path and integrity of transactions



- ◆ SilentWhispers uses distributed landmark routing, secure multi-party computation and 2-step transactions



- ◆ SilentWhispers is feasible in practice and offers interesting alternatives to current emerging payment systems



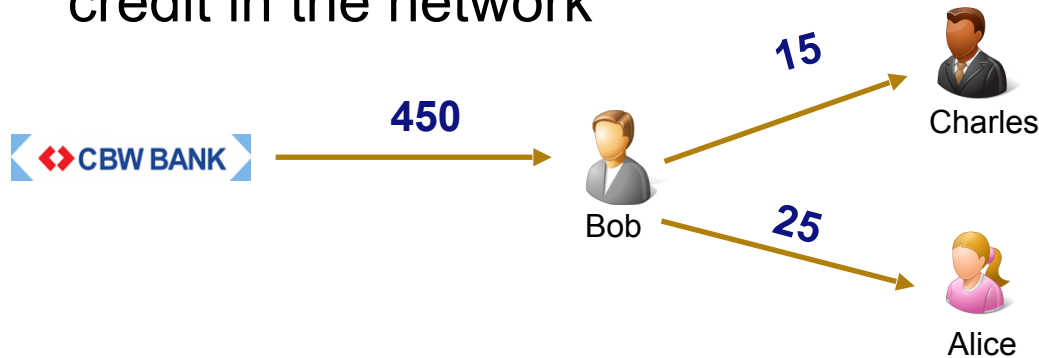
SilentWhispers: A Decentralized Credit Network

SilentWhispers: A Decentralized Credit Network

- ◆ **Local Information suffices:** Credit links of a user determine his credit in the network

SilentWhispers: A Decentralized Credit Network

- ◆ **Local Information suffices:** Credit links of a user determine his credit in the network



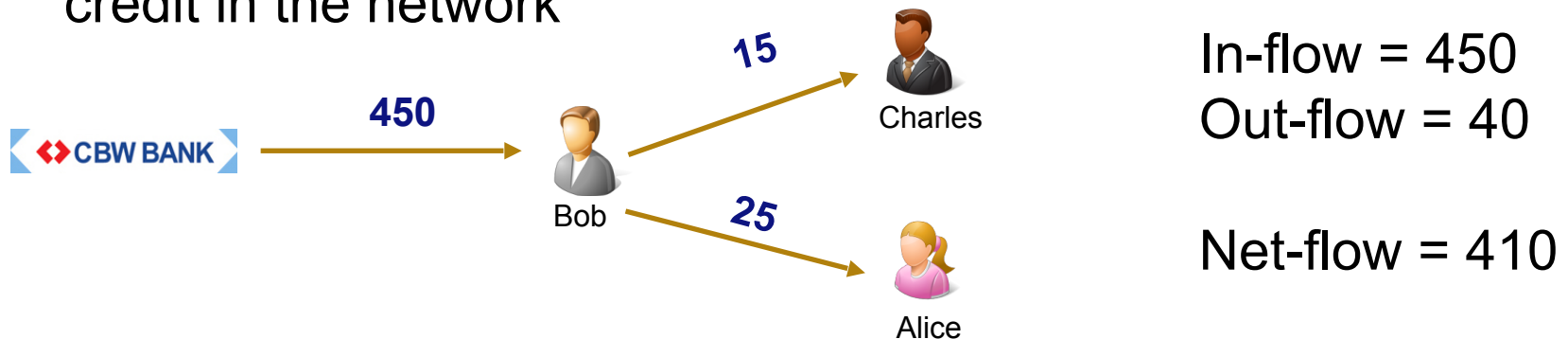
In-flow = 450

Out-flow = 40

Net-flow = 410

SilentWhispers: A Decentralized Credit Network

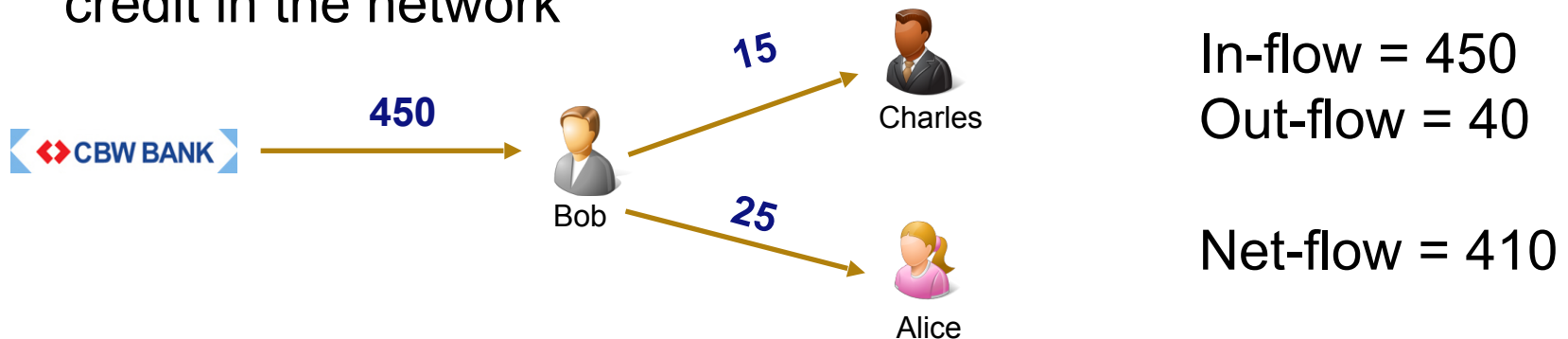
- ◆ **Local Information suffices:** Credit links of a user determine his credit in the network



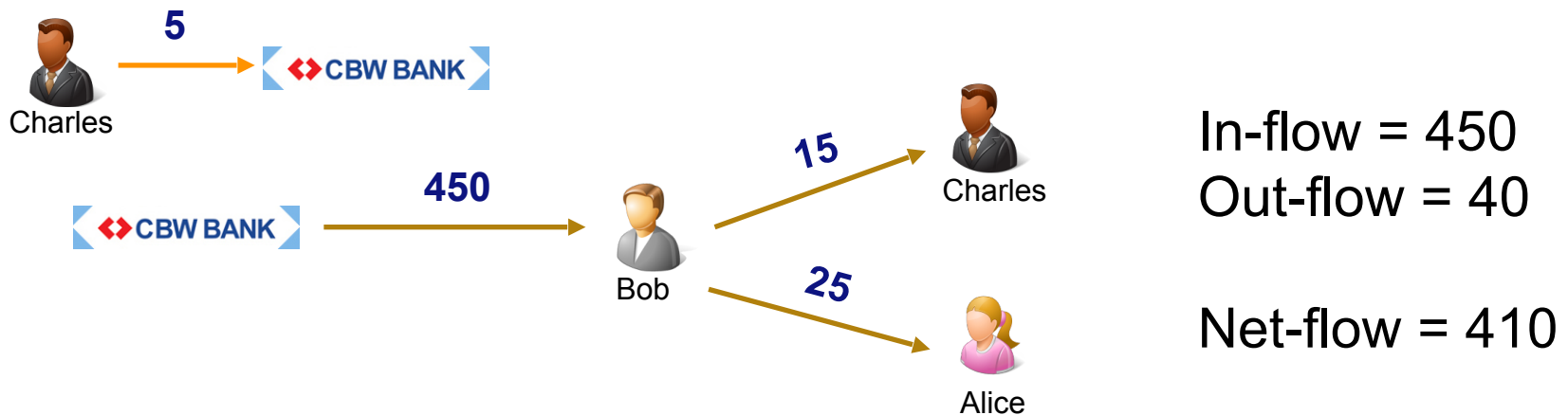
- ◆ **Net-flow is what matters:** Net-flow of a user must not change without the user's consent

SilentWhispers: A Decentralized Credit Network

- ◆ **Local Information suffices:** Credit links of a user determine his credit in the network

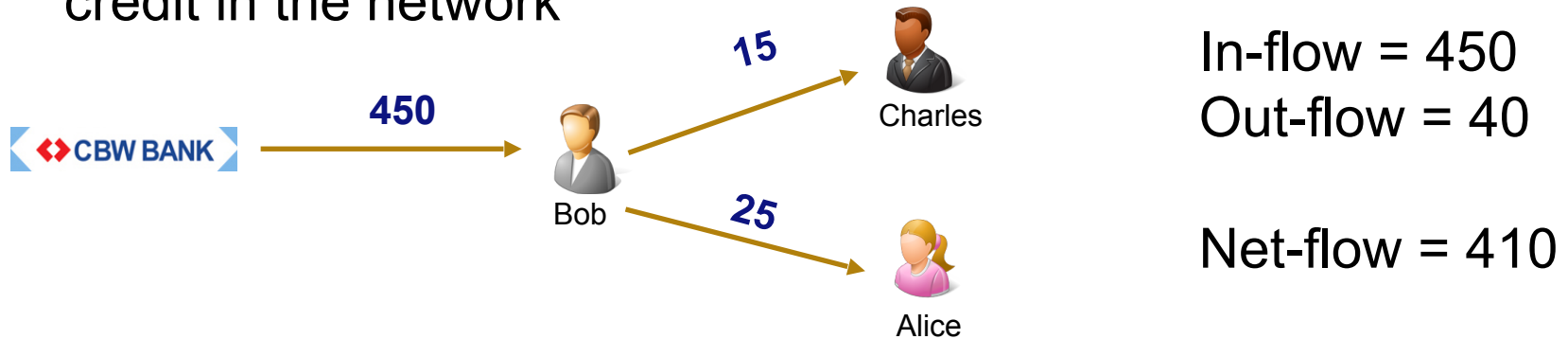


- ◆ **Net-flow is what matters:** Net-flow of a user must not change without the user's consent

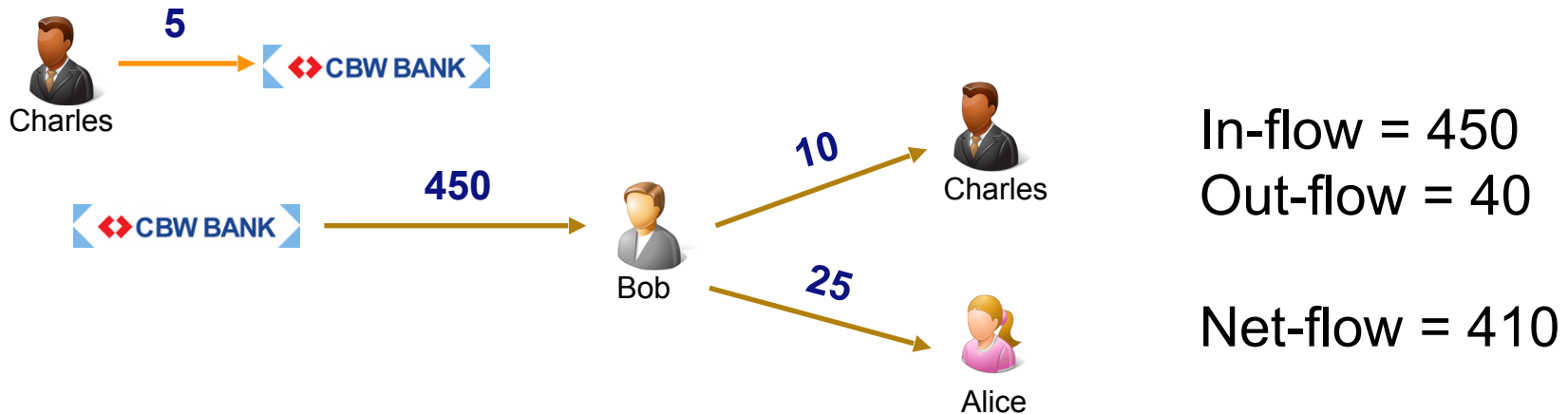


SilentWhispers: A Decentralized Credit Network

- ◆ **Local Information suffices:** Credit links of a user determine his credit in the network

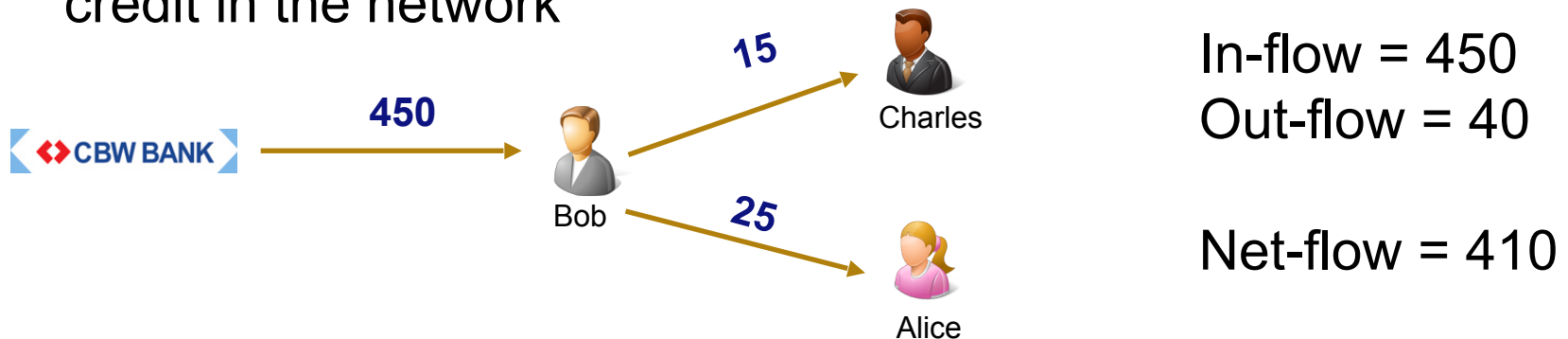


- ◆ **Net-flow is what matters:** Net-flow of a user must not change without the user's consent

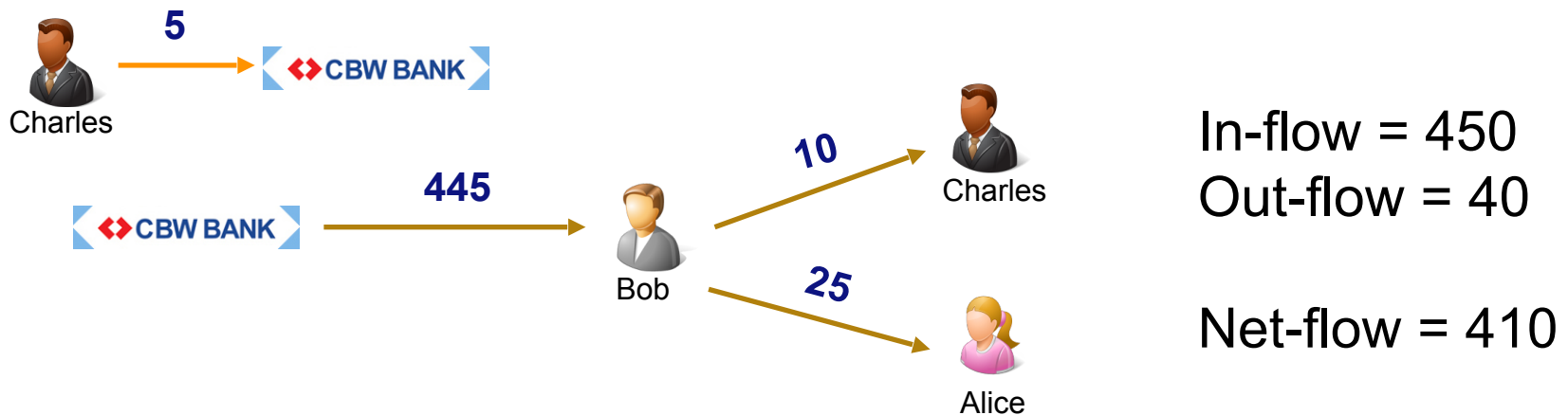


SilentWhispers: A Decentralized Credit Network

- ◆ **Local Information suffices:** Credit links of a user determine his credit in the network

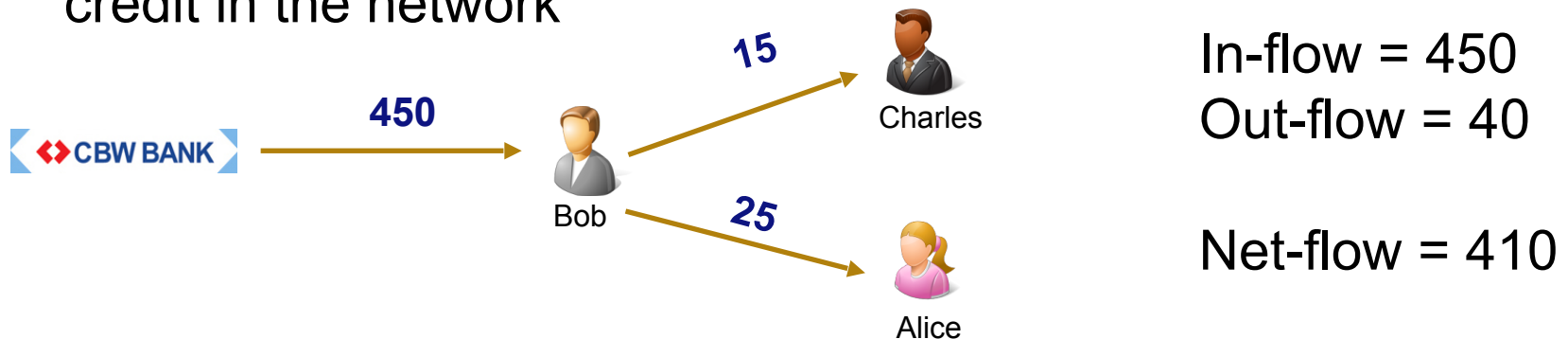


- ◆ **Net-flow is what matters:** Net-flow of a user must not change without the user's consent

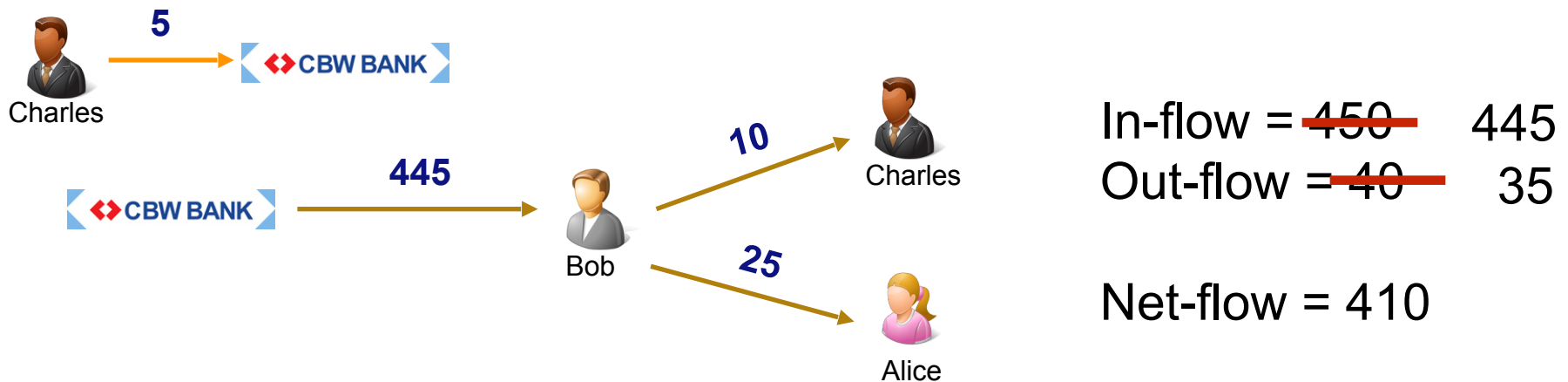


SilentWhispers: A Decentralized Credit Network

- ◆ **Local Information suffices:** Credit links of a user determine his credit in the network

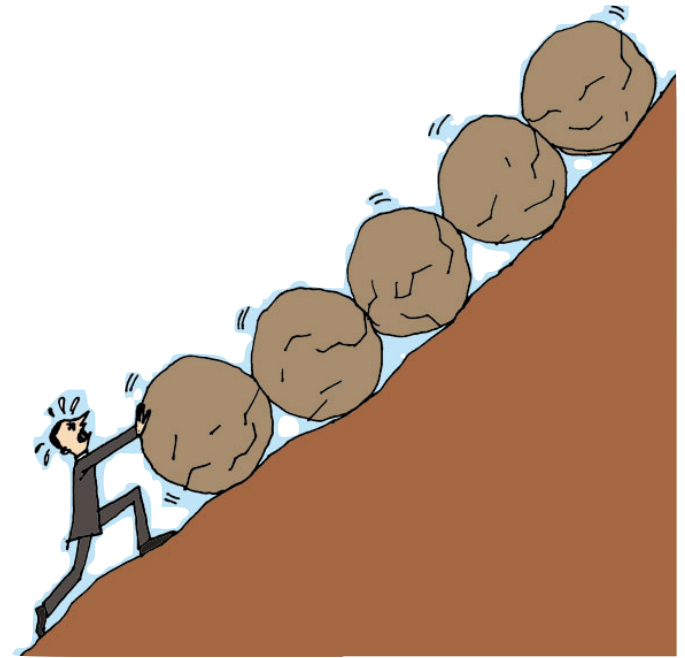


- ◆ **Net-flow is what matters:** Net-flow of a user must not change without the user's consent



Challenges

- ◆ Find paths between users
- ◆ Calculate credit available in the path
- ◆ Ensure integrity of transactions
- ◆ And more ...



The routing challenge

Routing Challenge: Landmark Routing

Routing Challenge: Landmark Routing

- ✦ Determine credit path from sender to receiver

Routing Challenge: Landmark Routing

- ✦ Determine credit path from sender to receiver
- ✦ Common problem in standard networks and ad-hoc networks

Routing Challenge: Landmark Routing

- ◆ Determine credit path from sender to receiver
- ◆ Common problem in standard networks and ad-hoc networks
- ◆ The max-flow approach:
 - ◆ Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$

Routing Challenge: Landmark Routing

- ◆ Determine credit path from sender to receiver
- ◆ Common problem in standard networks and ad-hoc networks
- ◆ The max-flow approach:
 - ◆ Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- ◆ Landmark routing [Tschusiya '89]
 - ◆ Calculate subset of all paths

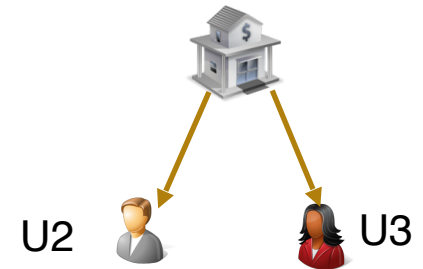
Routing Challenge: Landmark Routing

- ◆ Determine credit path from sender to receiver
- ◆ Common problem in standard networks and ad-hoc networks
- ◆ The max-flow approach:
 - ◆ Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- ◆ Landmark routing [Tschusiya '89]
 - ◆ Calculate subset of all paths



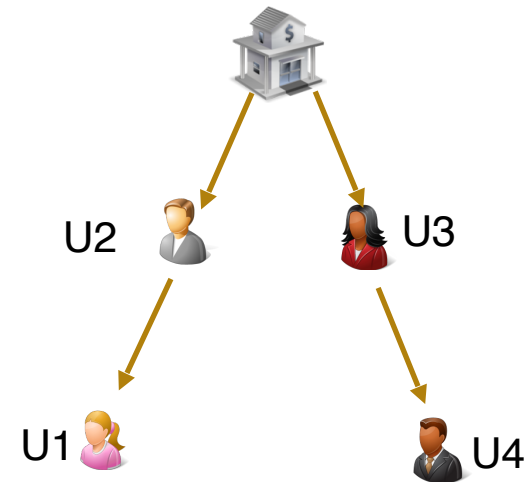
Routing Challenge: Landmark Routing

- ◆ Determine credit path from sender to receiver
- ◆ Common problem in standard networks and ad-hoc networks
- ◆ The max-flow approach:
 - ◆ Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- ◆ Landmark routing [Tschusiya '89]
 - ◆ Calculate subset of all paths



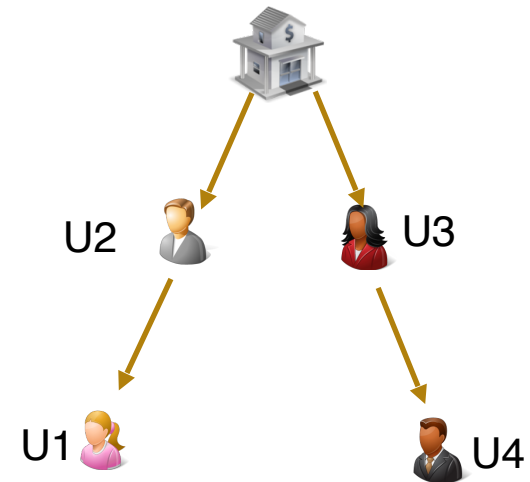
Routing Challenge: Landmark Routing

- ◆ Determine credit path from sender to receiver
- ◆ Common problem in standard networks and ad-hoc networks
- ◆ The max-flow approach:
 - ◆ Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- ◆ Landmark routing [Tschusiya '89]
 - ◆ Calculate subset of all paths



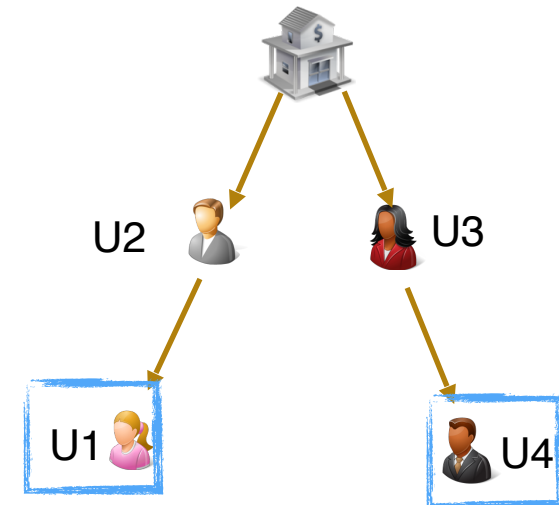
Routing Challenge: Landmark Routing

- ◆ Determine credit path from sender to receiver
- ◆ Common problem in standard networks and ad-hoc networks
- ◆ The max-flow approach:
 - ◆ Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- ◆ Landmark routing [Tschusiya '89]
 - ◆ Calculate subset of all paths
 - ◆ Distributed BFS: Local information suffices



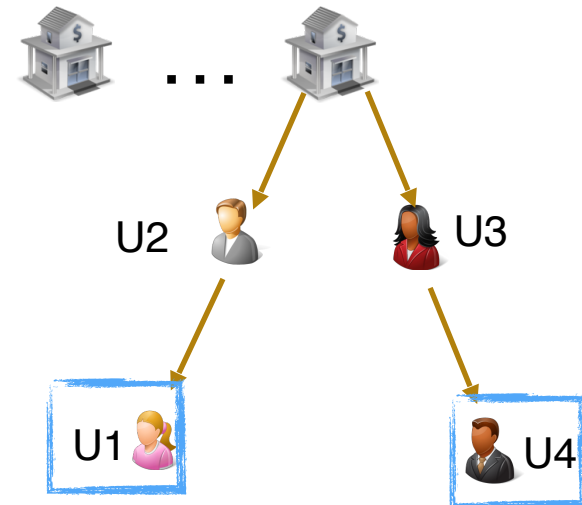
Routing Challenge: Landmark Routing

- ◆ Determine credit path from sender to receiver
- ◆ Common problem in standard networks and ad-hoc networks
- ◆ The max-flow approach:
 - ◆ Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- ◆ Landmark routing [Tschusiya '89]
 - ◆ Calculate subset of all paths
 - ◆ Distributed BFS: Local information suffices



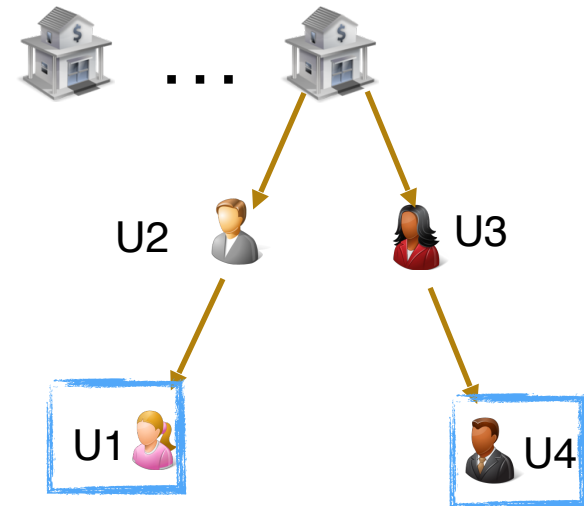
Routing Challenge: Landmark Routing

- ◆ Determine credit path from sender to receiver
- ◆ Common problem in standard networks and ad-hoc networks
- ◆ The max-flow approach:
 - ◆ Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- ◆ Landmark routing [Tschusiya '89]
 - ◆ Calculate subset of all paths
 - ◆ Distributed BFS: Local information suffices



Routing Challenge: Landmark Routing

- ◆ Determine credit path from sender to receiver
- ◆ Common problem in standard networks and ad-hoc networks
- ◆ The max-flow approach:
 - ◆ Not scalable enough: $O(V^3)$ or $O(V^2 \log(E))$
- ◆ Landmark routing [Tschusiyu '89]
 - ◆ Calculate subset of all paths
 - ◆ Distributed BFS: Local information suffices
 - ◆ Enough in practice^{1,2}
 - ◆ More efficient than max-flow^{1,2}



¹[Our work in NDSS '15]

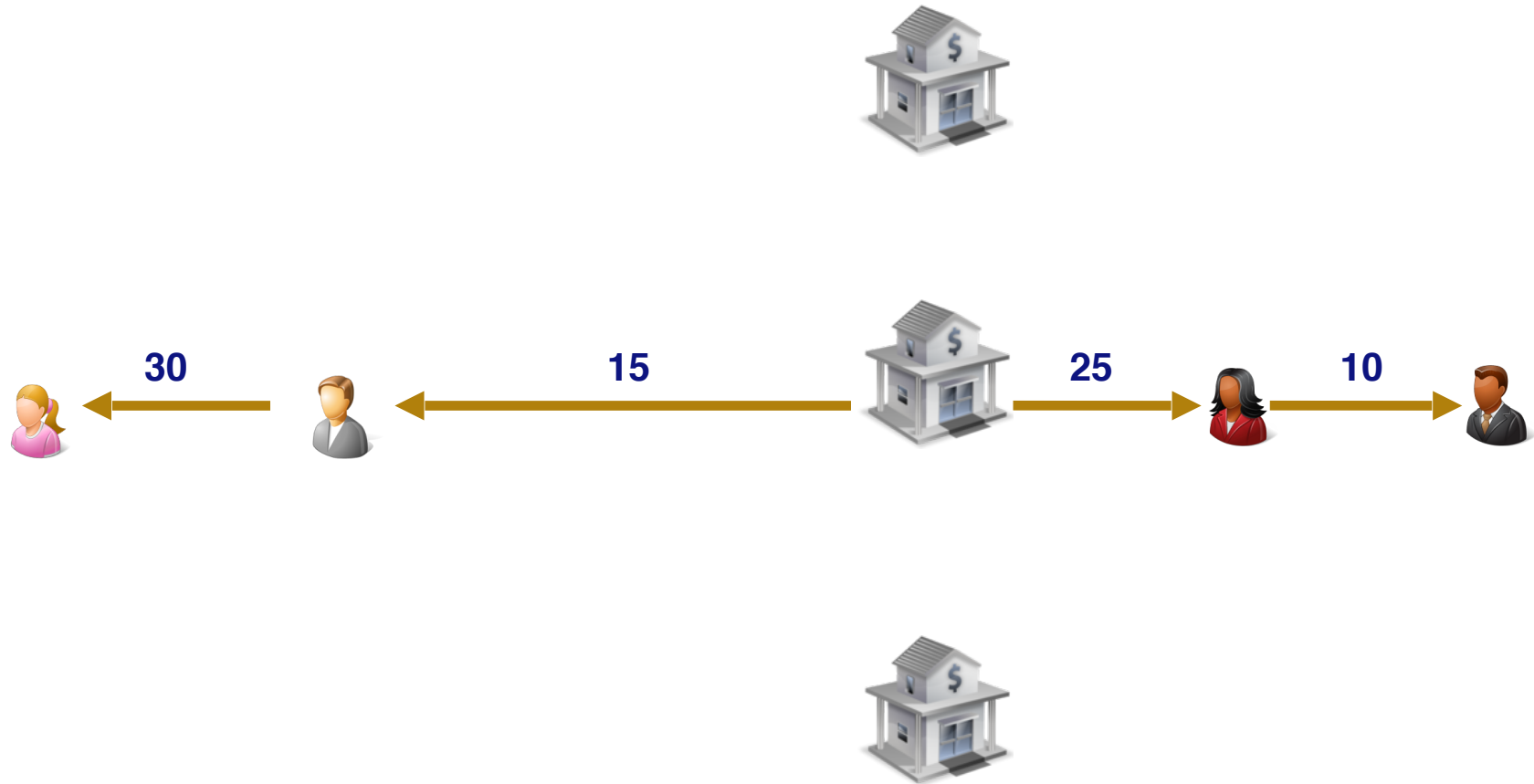
²[Viswanath et al. EUROSYS '12]

Calculation of credit available in a path

Credit in a Path: SMPC

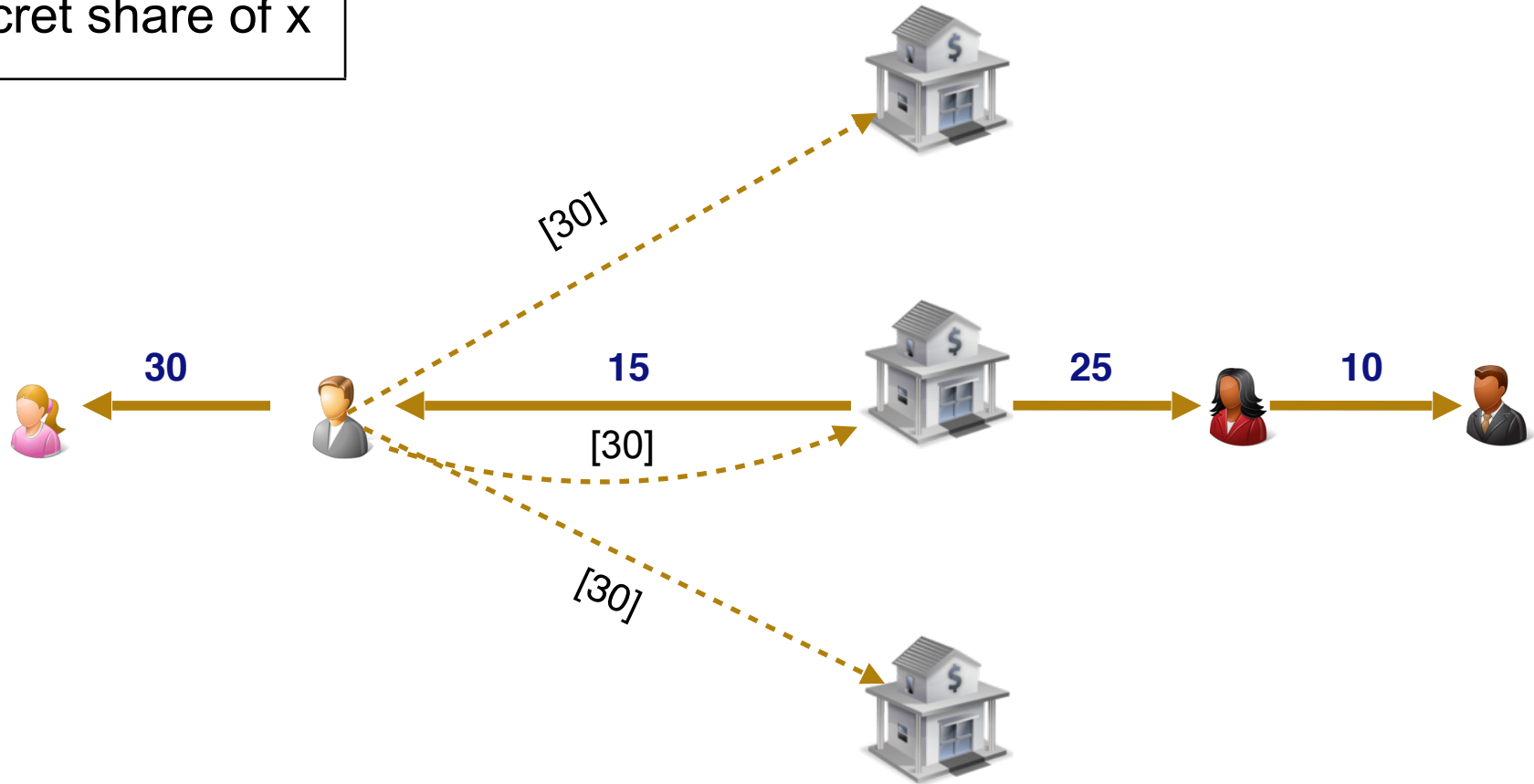


Credit in a Path: SMPC



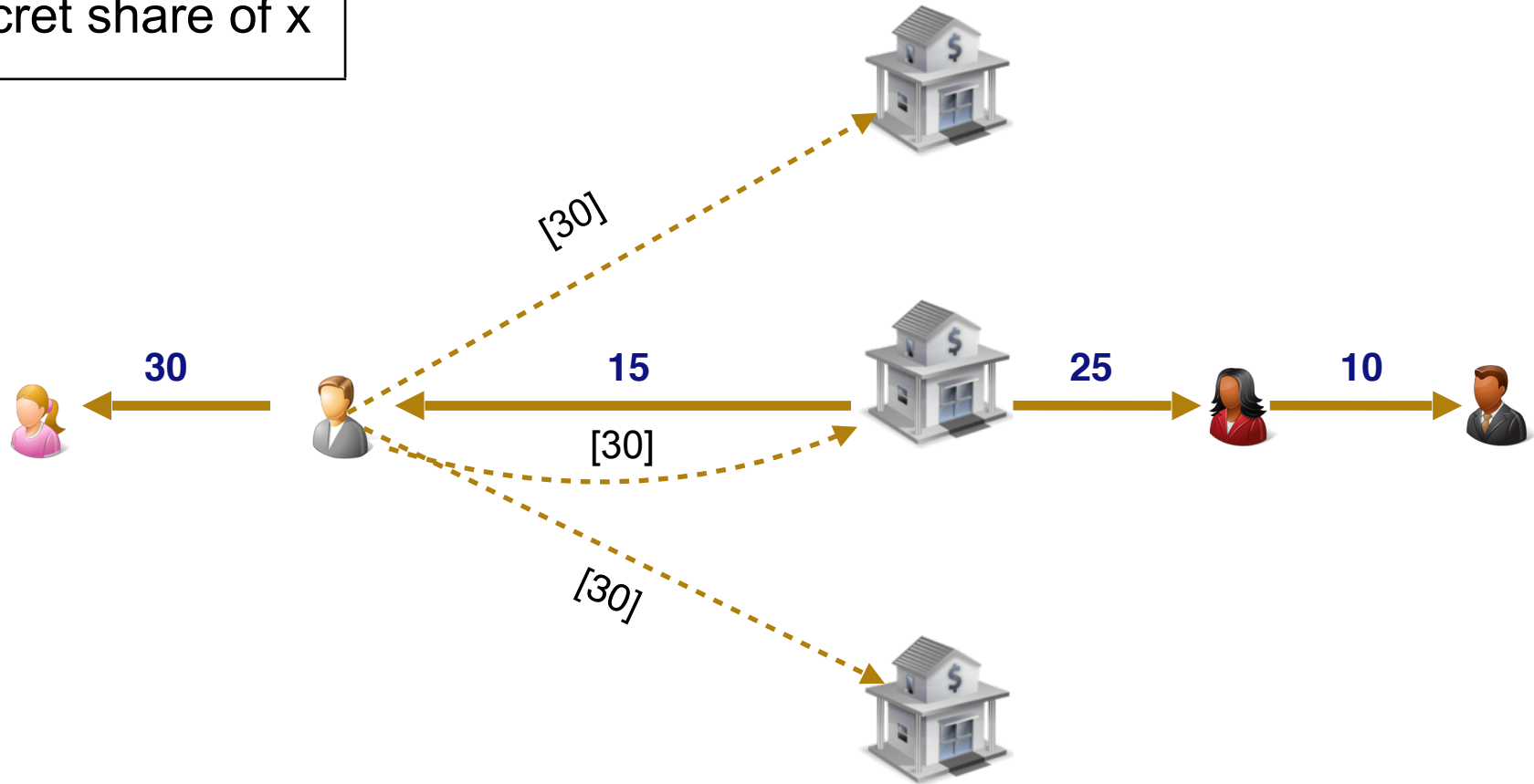
Credit in a Path: SMPC

[x]: Secret share of x



Credit in a Path: SMPC

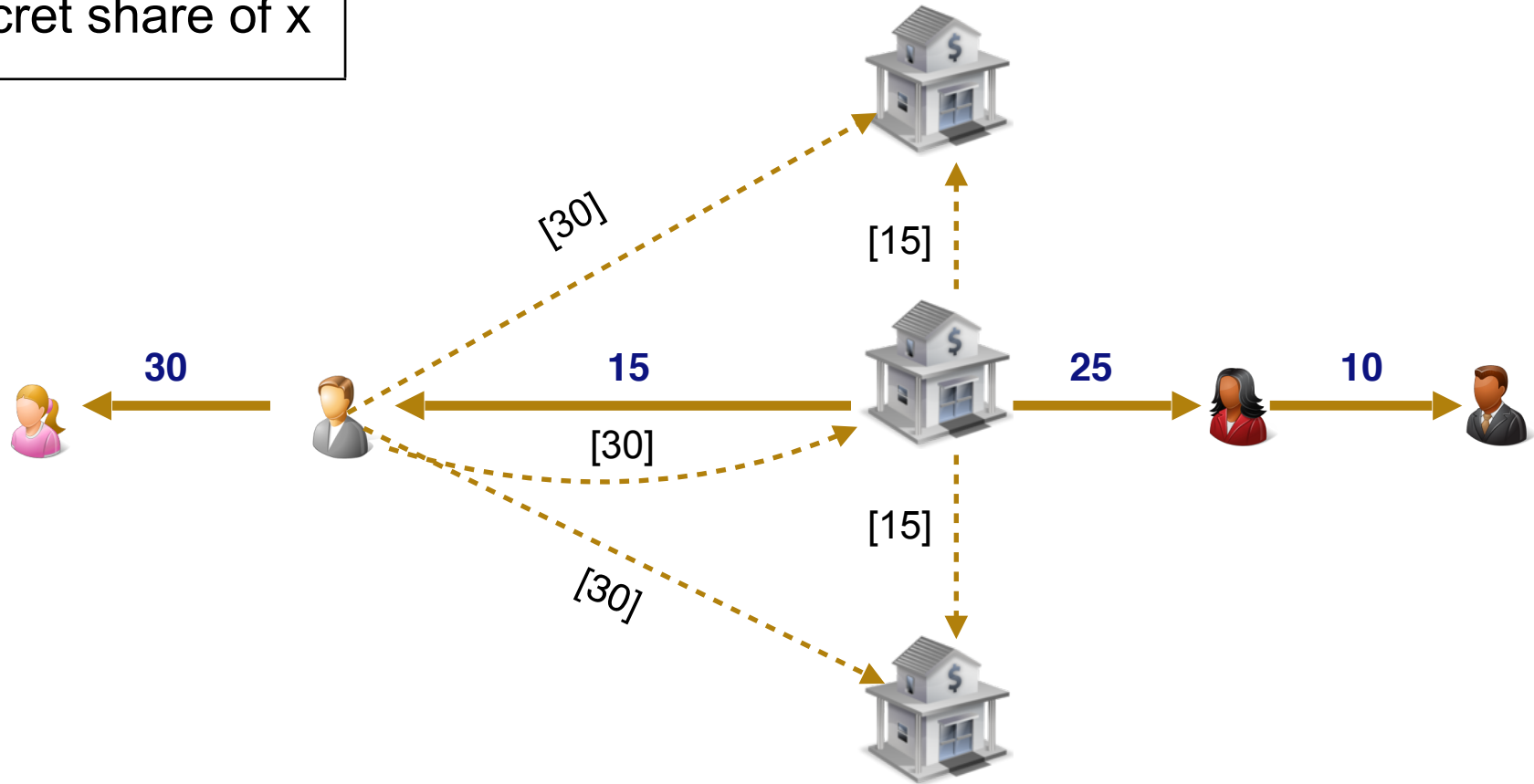
[x]: Secret share of x



- ◆ Given [x] it is not possible to know x

Credit in a Path: SMPC

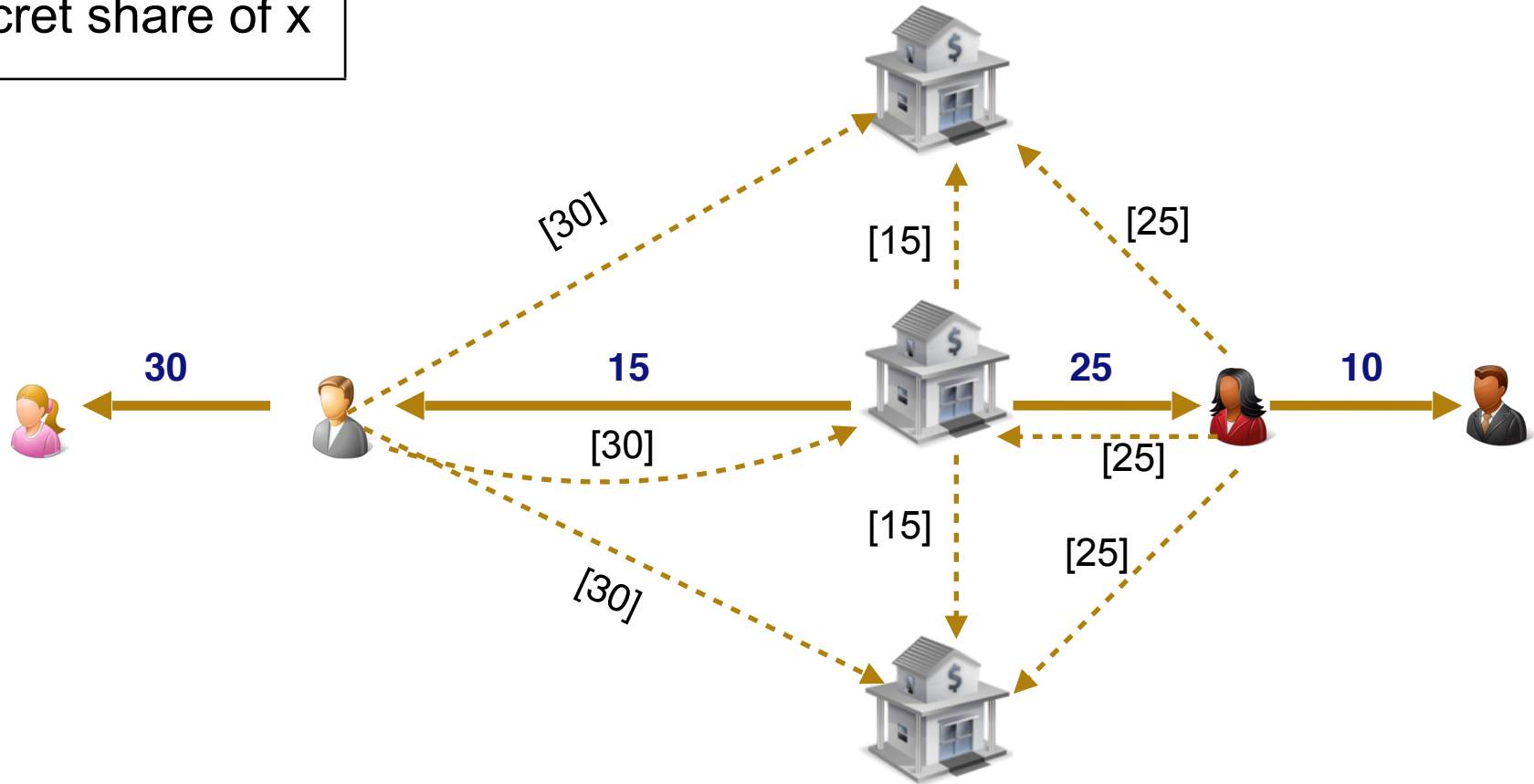
[x]: Secret share of x



- ◆ Given [x] it is not possible to know x

Credit in a Path: SMPC

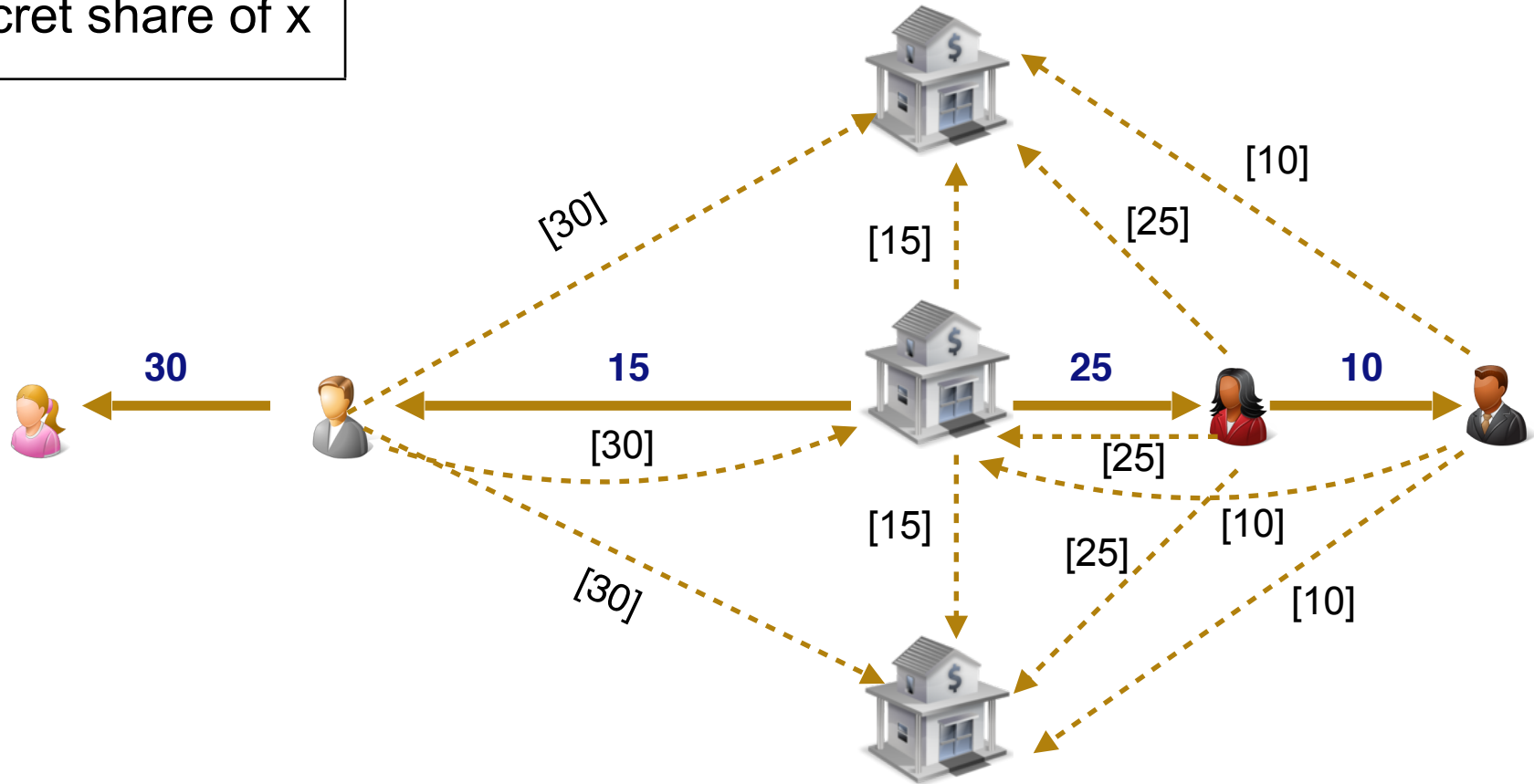
[x]: Secret share of x



- ◆ Given [x] it is not possible to know x

Credit in a Path: SMPC

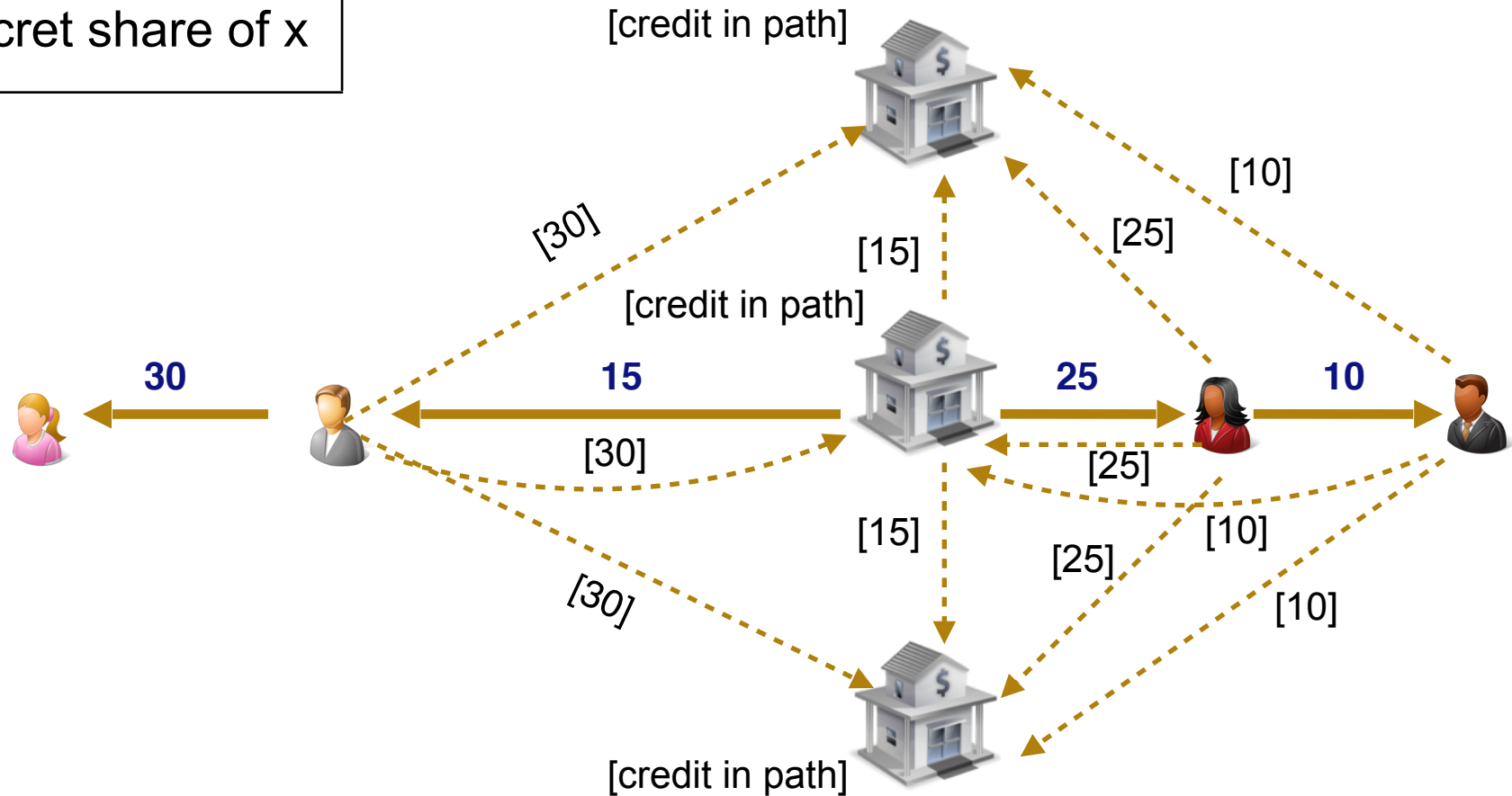
[x]: Secret share of x



- ◆ Given [x] it is not possible to know x

Credit in a Path: SMPC

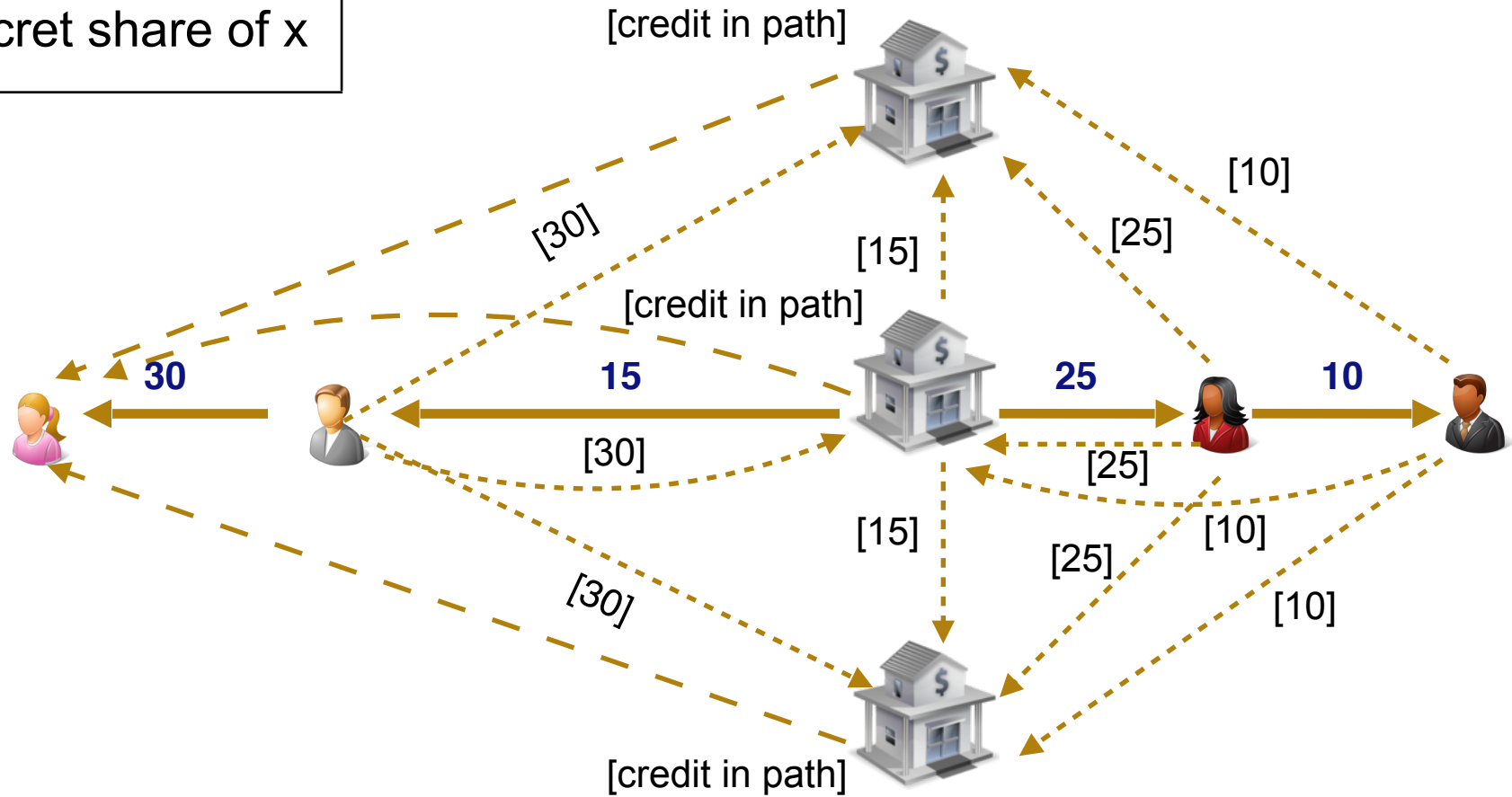
[x]: Secret share of x



- ◆ Given [x] it is not possible to know x

Credit in a Path: SMPC

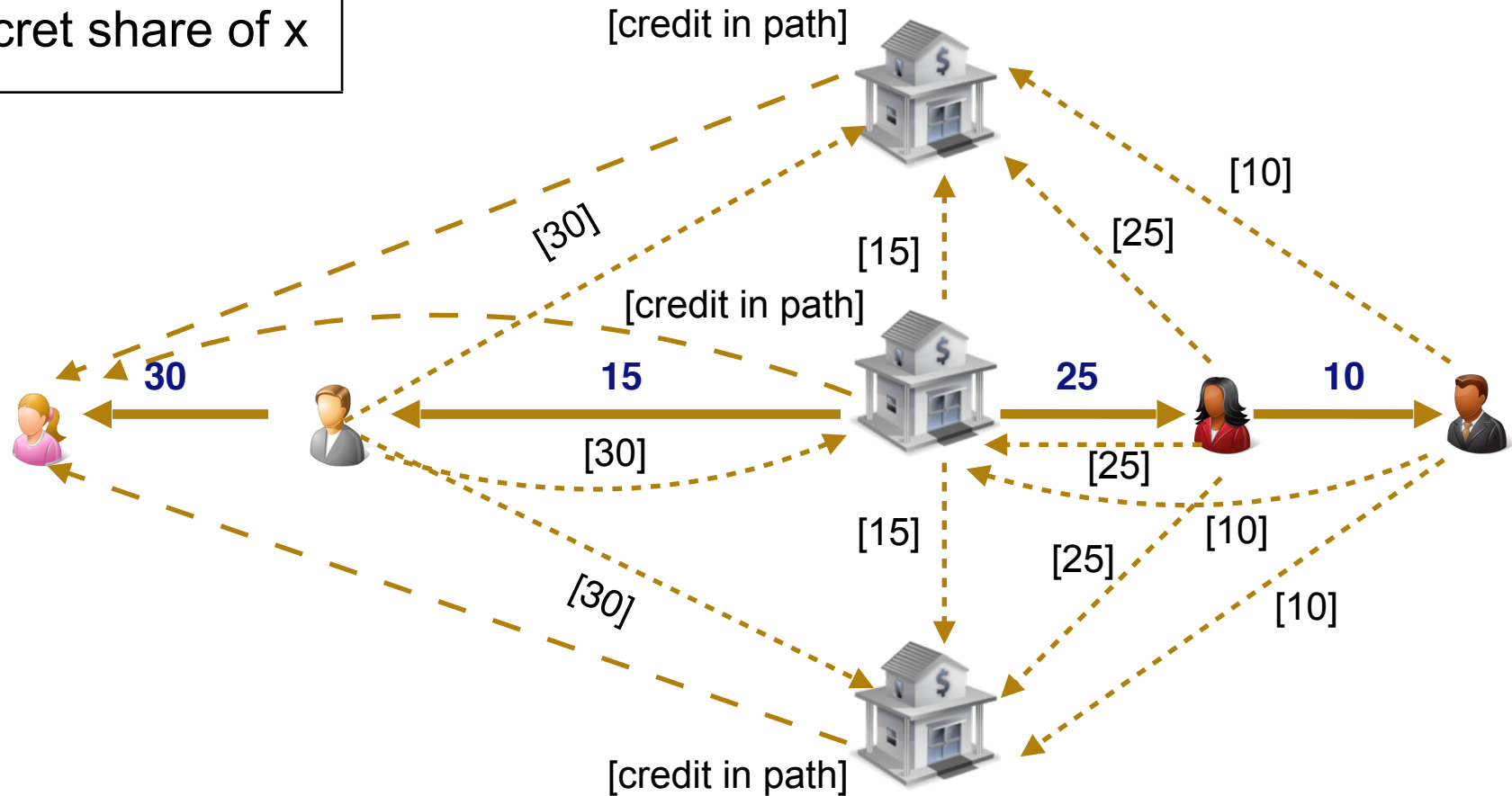
[x]: Secret share of x



- ◆ Given [x] it is not possible to know x

Credit in a Path: SMPC

[x]: Secret share of x



- ◆ Given [x] it is not possible to know x
 - ◆ Given “enough” copies of [x] one can reconstruct x

Integrity of the transactions

Transaction Integrity and Dispute Resolution

Transaction Integrity and Dispute Resolution

- ◆ 2-step transaction: **on hold** and **settle**

Transaction Integrity and Dispute Resolution

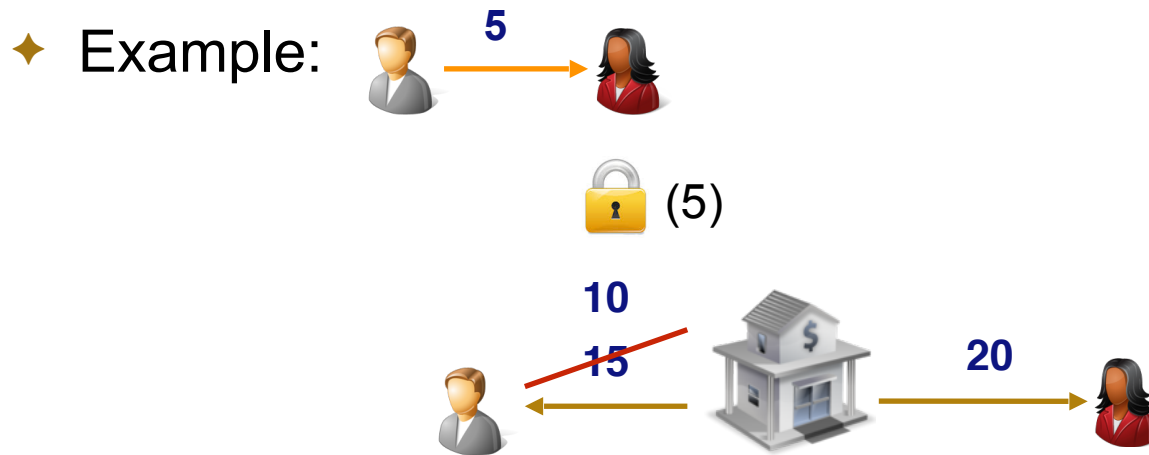
◆ 2-step transaction: **on hold** and **settle**

◆ Example:  $\xrightarrow{5}$ 



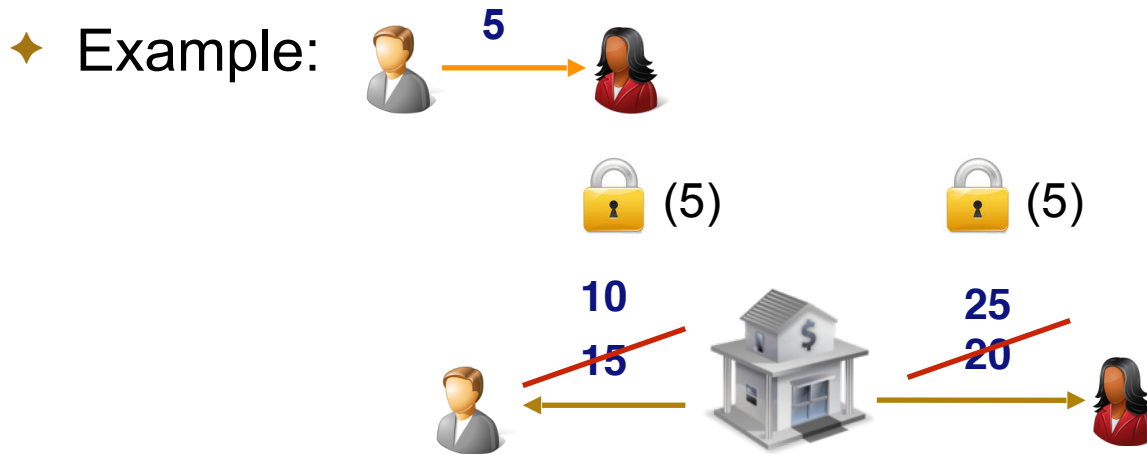
Transaction Integrity and Dispute Resolution

◆ 2-step transaction: **on hold** and **settle**



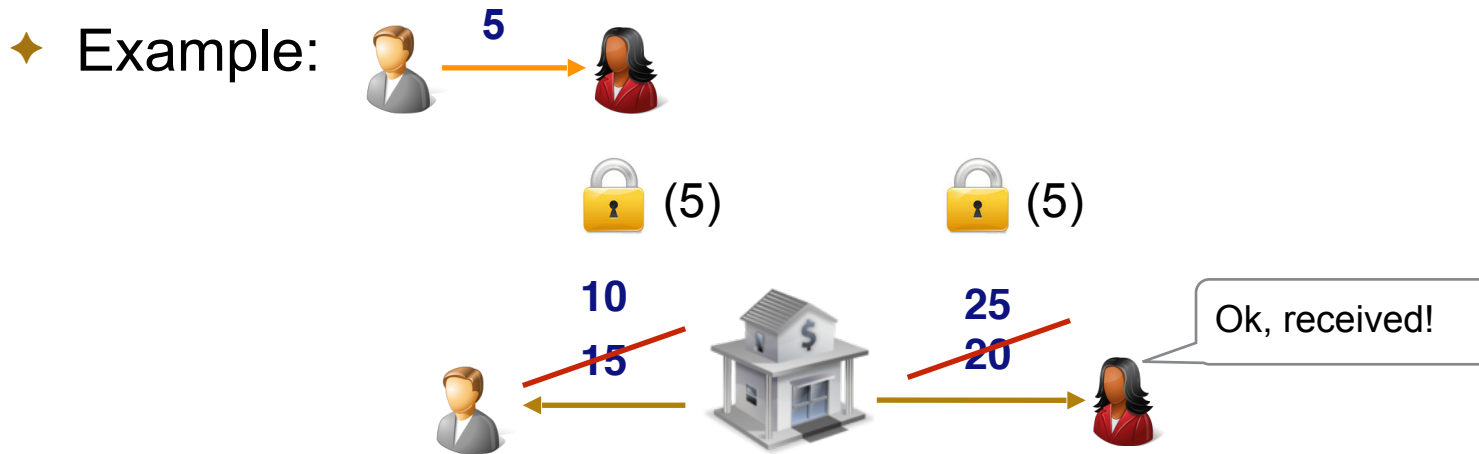
Transaction Integrity and Dispute Resolution

◆ 2-step transaction: **on hold** and **settle**



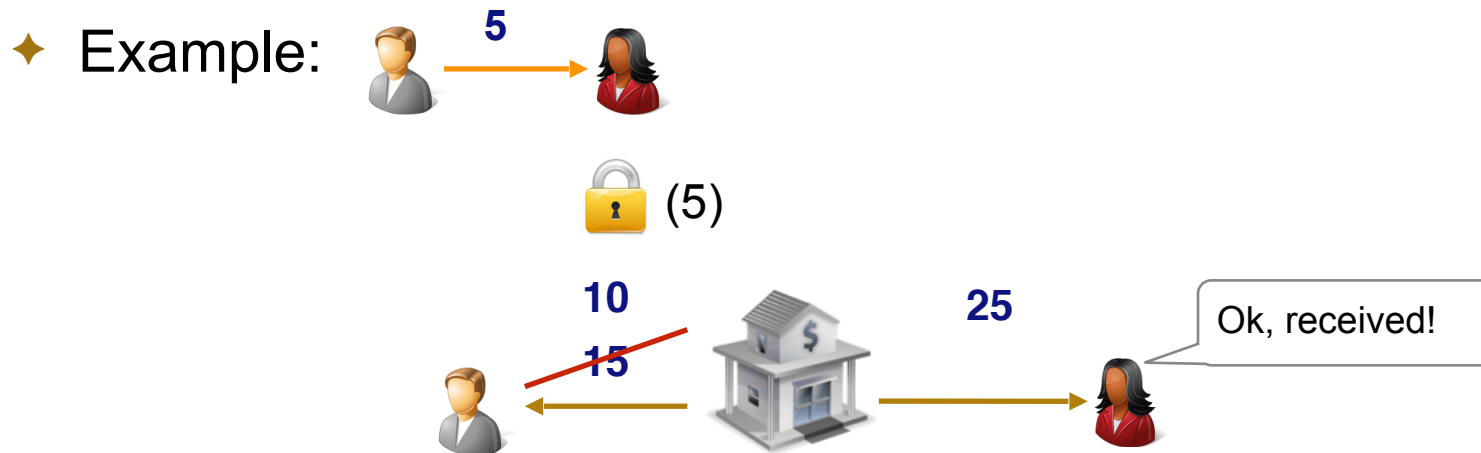
Transaction Integrity and Dispute Resolution

◆ 2-step transaction: **on hold** and **settle**



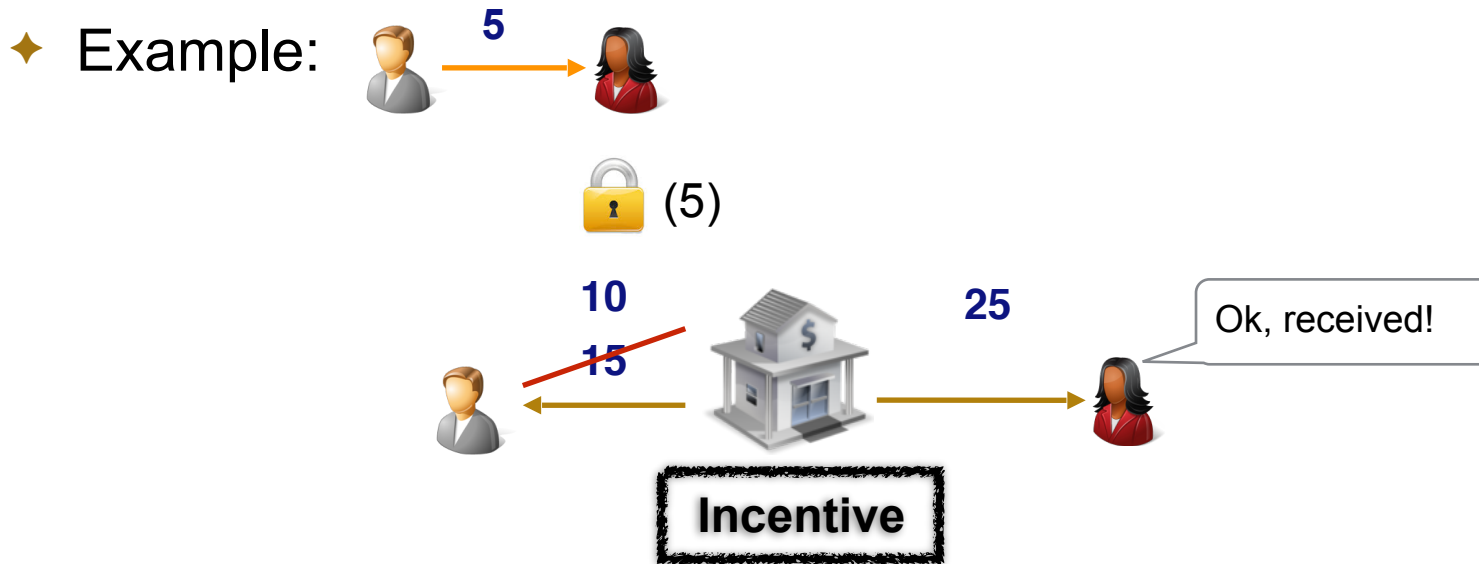
Transaction Integrity and Dispute Resolution

◆ 2-step transaction: **on hold** and **settle**



Transaction Integrity and Dispute Resolution

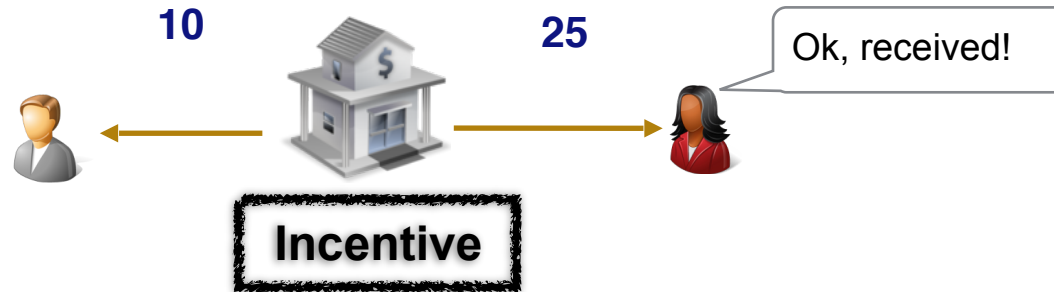
◆ 2-step transaction: **on hold** and **settle**



Transaction Integrity and Dispute Resolution

◆ 2-step transaction: **on hold** and **settle**

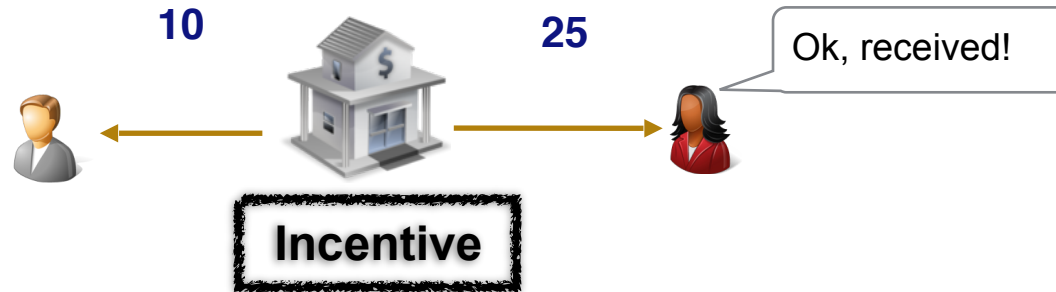
◆ Example:  $\xrightarrow{5}$ 



Transaction Integrity and Dispute Resolution

◆ 2-step transaction: **on hold** and **settle**

◆ Example:  $\xrightarrow{5}$ 



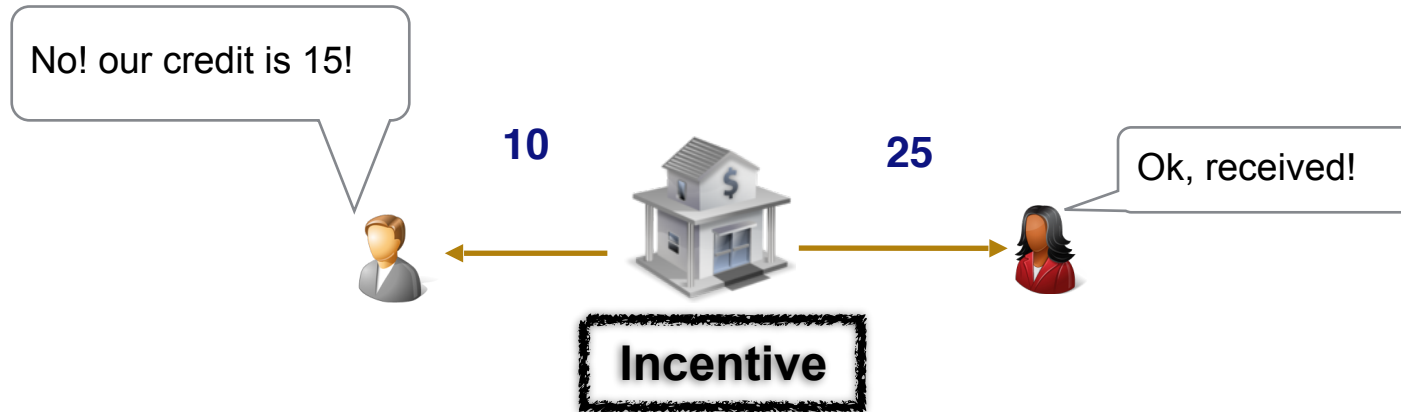
◆ **Integrity:**

◆ All landmarks cannot make the user lose credit

Transaction Integrity and Dispute Resolution

- ◆ 2-step transaction: **on hold** and **settle**

- ◆ Example:  $\xrightarrow{5}$ 

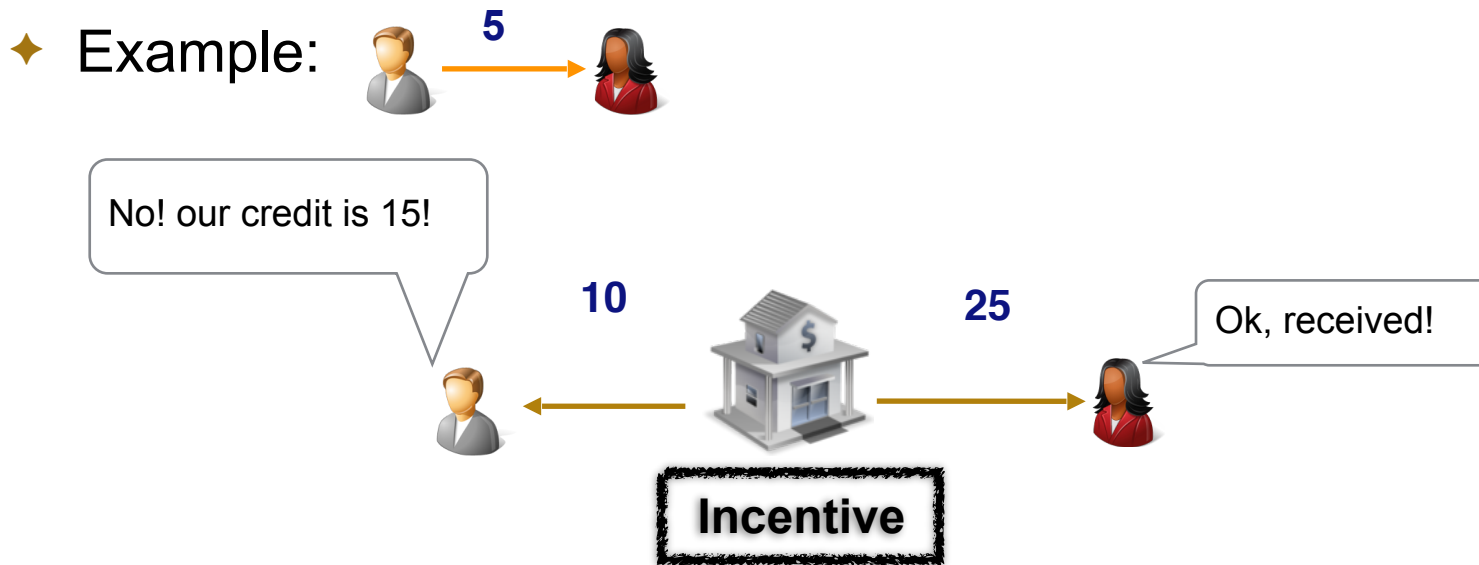


- ◆ **Integrity:**

- ◆ All landmarks cannot make the user lose credit

Transaction Integrity and Dispute Resolution

- ◆ 2-step transaction: **on hold** and **settle**



- ◆ **Integrity:**

- ◆ All landmarks cannot make the user lose credit

- ◆ **Accountability:**

- ◆ In case of dispute, users must prove the link value
- ◆ Local logs suffice to determine the valid current value
- ◆ The disputed value is bounded

Evaluation

Evaluation and Discussion

Evaluation and Discussion

- ◆ C++ prototype implementation
 - ◆ Secret Sharing-based MPC library: <https://github.com/Zayat/MPC-Shared>

Evaluation and Discussion

- ◆ C++ prototype implementation
 - ◆ Secret Sharing-based MPC library: <https://github.com/Zayat/MPC-Shared>
- ◆ Setup using Ripple transactions:
 - ◆ Maximum path length: 10 links
 - ◆ Maximum number of paths: 7 landmarks (Ripple Gateways)

Evaluation and Discussion

- ◆ C++ prototype implementation
 - ◆ Secret Sharing-based MPC library: <https://github.com/Zayat/MPC-Shared>
- ◆ Setup using Ripple transactions:
 - ◆ Maximum path length: 10 links
 - ◆ Maximum number of paths: 7 landmarks (Ripple Gateways)
- ◆ Computing available credit on a path in ~1.3 seconds
 - ◆ Different paths in parallel

Evaluation and Discussion

- ◆ C++ prototype implementation
 - ◆ Secret Sharing-based MPC library: <https://github.com/Zayat/MPC-Shared>
- ◆ Setup using Ripple transactions:
 - ◆ Maximum path length: 10 links
 - ◆ Maximum number of paths: 7 landmarks (Ripple Gateways)
- ◆ Computing available credit on a path in ~1.3 seconds
 - ◆ Different paths in parallel

Feasible to run in practice current Ripple transactions

Evaluation and Discussion

- ◆ C++ prototype implementation
 - ◆ Secret Sharing-based MPC library: <https://github.com/Zayat/MPC-Shared>
- ◆ Setup using Ripple transactions:
 - ◆ Maximum path length: 10 links
 - ◆ Maximum number of paths: 7 landmarks (Ripple Gateways)
- ◆ Computing available credit on a path in ~1.3 seconds
 - ◆ Different paths in parallel

Feasible to run in practice current Ripple transactions

- ◆ SilentWhispers has attracted attention from industry:
 - ◆ KOINA: <https://koina.cc/>



The Landscape of Emerging Payment Systems

The Landscape of Emerging Payment Systems

	Cryptocurrencies	Ripple	SilentWhispers
Transfer of funds	Direct transactions between any two wallets	Transactions <i>only</i> via a <i>path</i> with enough credit	

The Landscape of Emerging Payment Systems

	Cryptocurrencies	Ripple	SilentWhispers
Transfer of funds	Direct transactions between any two wallets	Transactions only via a path with enough credit	
Transaction flexibility	Fixed currency agreed between sender and receiver	Support for cross-currency transactions	

The Landscape of Emerging Payment Systems

	Cryptocurrencies	Ripple	SilentWhispers
Transfer of funds	Direct transactions between any two wallets	Transactions only via a path with enough credit	
Transaction flexibility	Fixed currency agreed between sender and receiver	Support for cross-currency transactions	
Transaction verification	Globally verified		Locally verified by users in the path

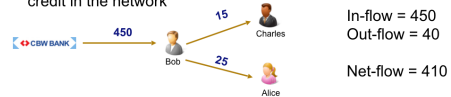
Take Home Message

Take Home Message

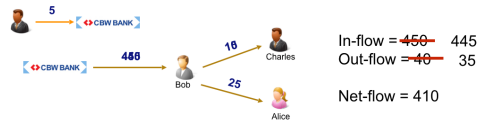
- ◆ A credit network does not require a global ledger or global consensus

SilentWhispers: A Decentralized Credit Network

- ◆ Local Information suffices: Credit links of a user determine his credit in the network



- ◆ Net-flow is what matters: Net-flow of a user must not change without the user's consent



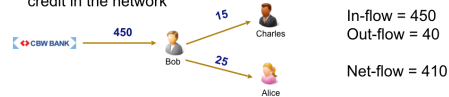
8

Take Home Message

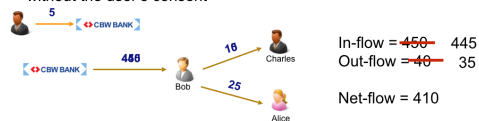
- ◆ A credit network does not require a global ledger or global consensus

SilentWhispers: A Decentralized Credit Network

- ◆ Local Information suffices: Credit links of a user determine his credit in the network



- ◆ Net-flow is what matters: Net-flow of a user must not change without the user's consent



8

- ◆ SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges

Challenges

- ◆ Find paths between users?
- ◆ Credit available in the path?
- ◆ Integrity of transactions?
- ◆ And more ...



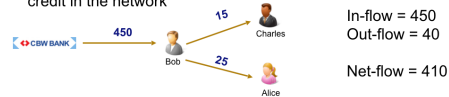
9

Take Home Message

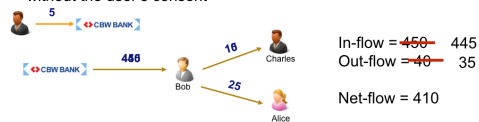
- ◆ A credit network does not require a global ledger or global consensus

SilentWhispers: A Decentralized Credit Network

- ◆ Local Information suffices: Credit links of a user determine his credit in the network



- ◆ Net-flow is what matters: Net-flow of a user must not change without the user's consent



8

- ◆ SilentWhispers is feasible in practice and it has attracted attention from industry

Evaluation

- ◆ C++ prototype implementation
 - ◆ MPC-Shared library: <https://github.com/Zayat/MPC-Shared>
- ◆ Setup using Ripple transactions:
 - ◆ Maximum path length: 10 links
 - ◆ Maximum number of paths: 7 landmarks (Ripple Gateways)
- ◆ Computing available credit on a path in ~1.3 seconds
 - ◆ Different paths in parallel
- ◆ SilentWhispers has attracted the attention from industry:
 - ◆ KOINA: A credit network with market-specific currencies <https://koina.cc/>

Feasible to run in practice current Ripple transactions



17

- ◆ SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges

Challenges

- ◆ Find paths between users?
- ◆ Credit available in the path?
- ◆ Integrity of transactions?
- ◆ And more ...



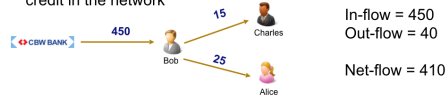
9

Take Home Message

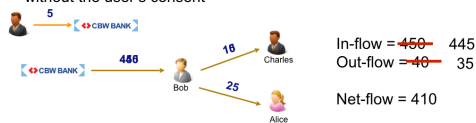
- ◆ A credit network does not require a global ledger or global consensus

SilentWhispers: A Decentralized Credit Network

- ◆ Local Information suffices: Credit links of a user determine his credit in the network



- ◆ Net-flow is what matters: Net-flow of a user must not change without the user's consent



- ◆ SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges

Challenges

- ◆ Find paths between users?
- ◆ Credit available in the path?
- ◆ Integrity of transactions?
- ◆ And more ...



- ◆ SilentWhispers is feasible in practice and it has attracted attention from industry

Evaluation

- ◆ C++ prototype implementation
 - ◆ MPC-Shared library: <https://github.com/Zayat/MPC-Shared>
- ◆ Setup using Ripple transactions:
 - ◆ Maximum path length: 10 links
 - ◆ Maximum number of paths: 7 landmarks (Ripple Gateways)
- ◆ Computing available credit on a path in ~1.3 seconds
 - ◆ Different paths in parallel

Feasible to run in practice current Ripple transactions

- ◆ SilentWhispers has attracted the attention from industry:
 - ◆ KOINA: A credit network with market-specific currencies <https://koina.cc/>



- ◆ SilentWhispers is an interesting alternative in the landscape of emerging payment systems

The Landscape of Emerging Payment Systems

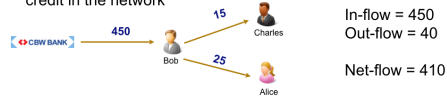
	Cryptocurrencies	Ripple	SilentWhispers
Transfer of funds	Direct transactions between any two wallets	Transactions only via a path with enough credit	
Transaction flexibility	Fixed currency agreed between sender and receiver	Support for cross-currency transactions	
Transaction verification	Globally verified		Locally verified by users in the path

Take Home Message

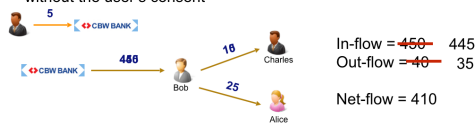
- ◆ A credit network does not require a global ledger or global consensus

SilentWhispers: A Decentralized Credit Network

- ◆ Local Information suffices: Credit links of a user determine his credit in the network



- ◆ Net-flow is what matters: Net-flow of a user must not change without the user's consent



8

- ◆ SilentWhispers is feasible in practice and it has attracted attention from industry

Evaluation

- ◆ C++ prototype implementation
 - ◆ MPC-Shared library: <https://github.com/Zayat/MPC-Shared>
- ◆ Setup using Ripple transactions:
 - ◆ Maximum path length: 10 links
 - ◆ Maximum number of paths: 7 landmarks (Ripple Gateways)
- ◆ Computing available credit on a path in ~1.3 seconds
 - ◆ Different paths in parallel

Feasible to run in practice current Ripple transactions

- ◆ SilentWhispers has attracted the attention from industry:
 - ◆ KOINA: A credit network with market-specific currencies <https://koina.cc/>



17

- ◆ SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges

- ◆ SilentWhispers is an interesting alternative in the landscape of emerging payment systems

Challenges

- ◆ Find paths between users?
- ◆ Credit available in the path?
- ◆ Integrity of transactions?
- ◆ And more ...



9

The Landscape of Emerging Payment Systems

	Cryptocurrencies	Ripple	SilentWhispers
Transfer of funds	Direct transactions between any two wallets	Transactions only via a path with enough credit	
Transaction flexibility	Fixed currency agreed between sender and receiver	Support for cross-currency transactions	
Transaction verification	Globally verified		Locally verified by users in the path

Thanks!
@pedrorechez

18