IOweYou Credit Networks

Applications and Privacy

Aniket Kate
Purdue University

CCS 2016 Tutorial

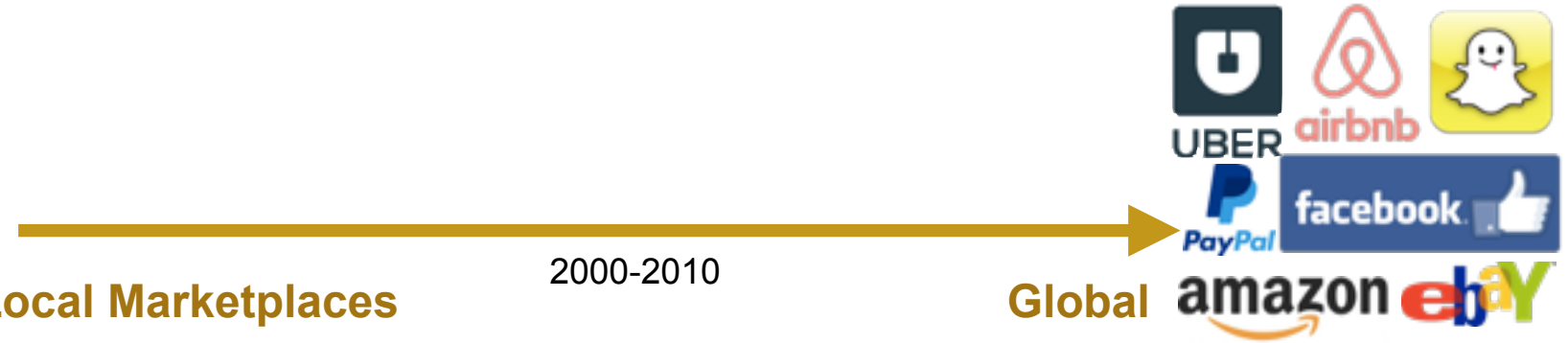
Ever Changing Landscape of Communication

PURDUE UNIVERSITY

Local Marketplaces

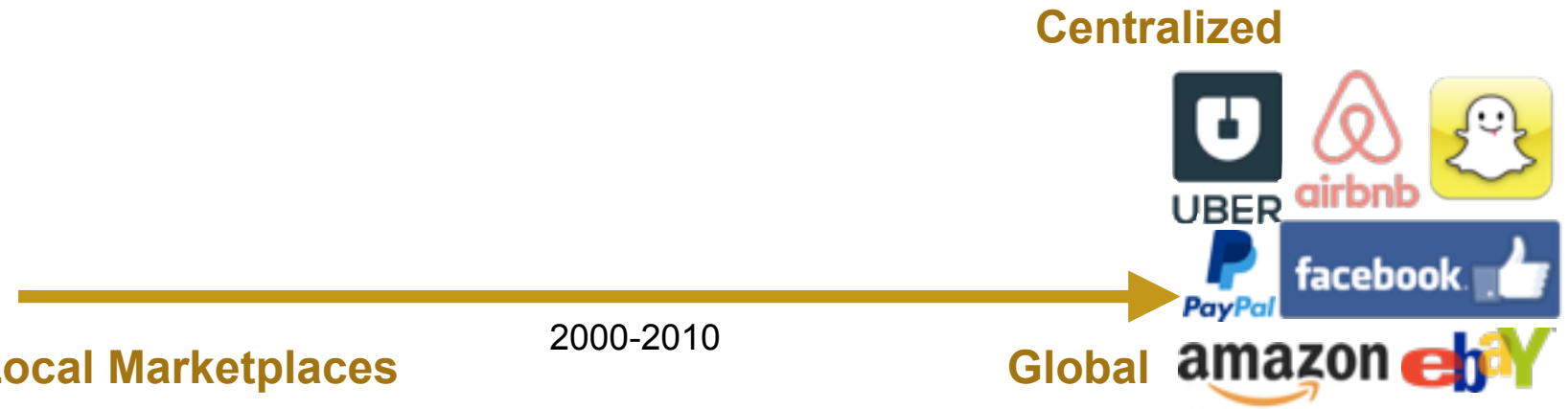
Ever Changing Landscape of Communication

PURDUE UNIVERSITY

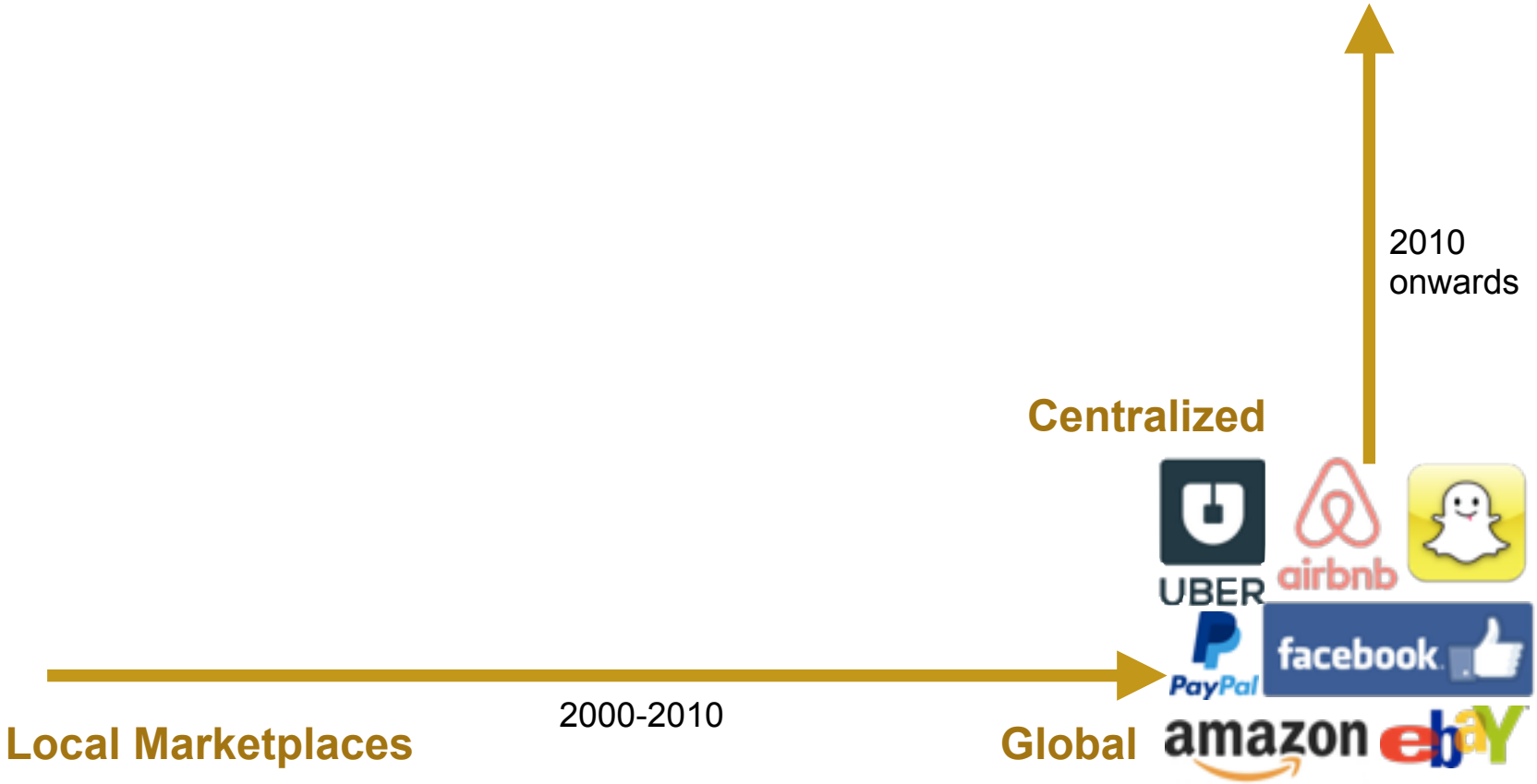


Ever Changing Landscape of Communication

PURDUE UNIVERSITY



Ever Changing Landscape of Communication



Ever Changing Landscape of Communication

PURDUE UNIVERSITY

Decentralized/
Distributed

2010
onwards

Centralized

UBER airbnb

PayPal facebook

amazon ebay

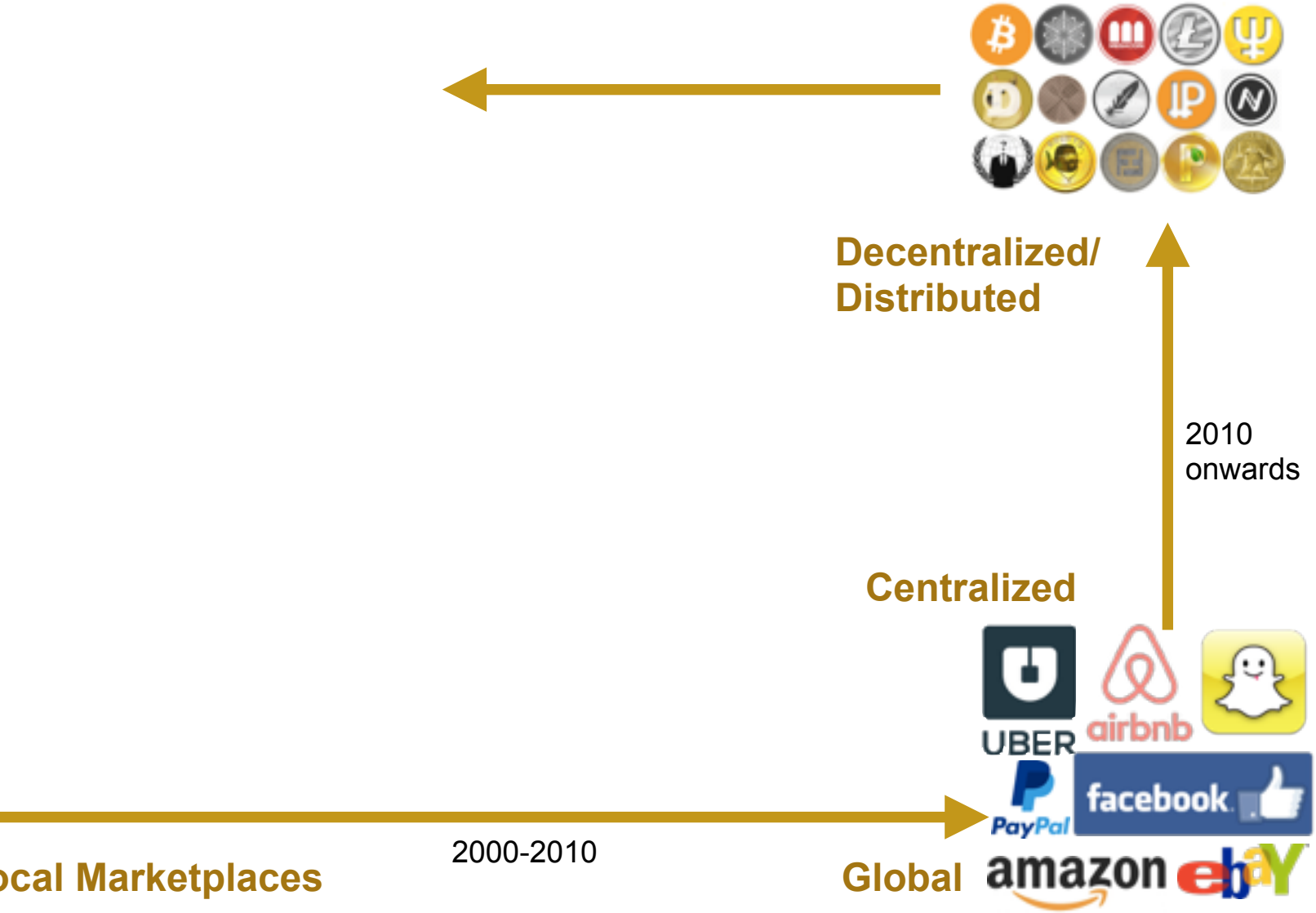
2000-2010

Local Marketplaces

Global

Ever Changing Landscape of Communication

PURDUE UNIVERSITY



Ever Changing Landscape of Communication

PURDUE UNIVERSITY

Blockchain for Everything!

Decentralized/ Distributed

2010 onwards

Centralized

2000-2010

Local Marketplaces

Global

Ever Changing Landscape of Communication

PURDUE UNIVERSITY

Blockchain for Everything!

Decentralized/ Distributed

Crypto-currencies may or may not survive, but the concept of distributed ledgers/blockchains is here to stay

2010 onwards

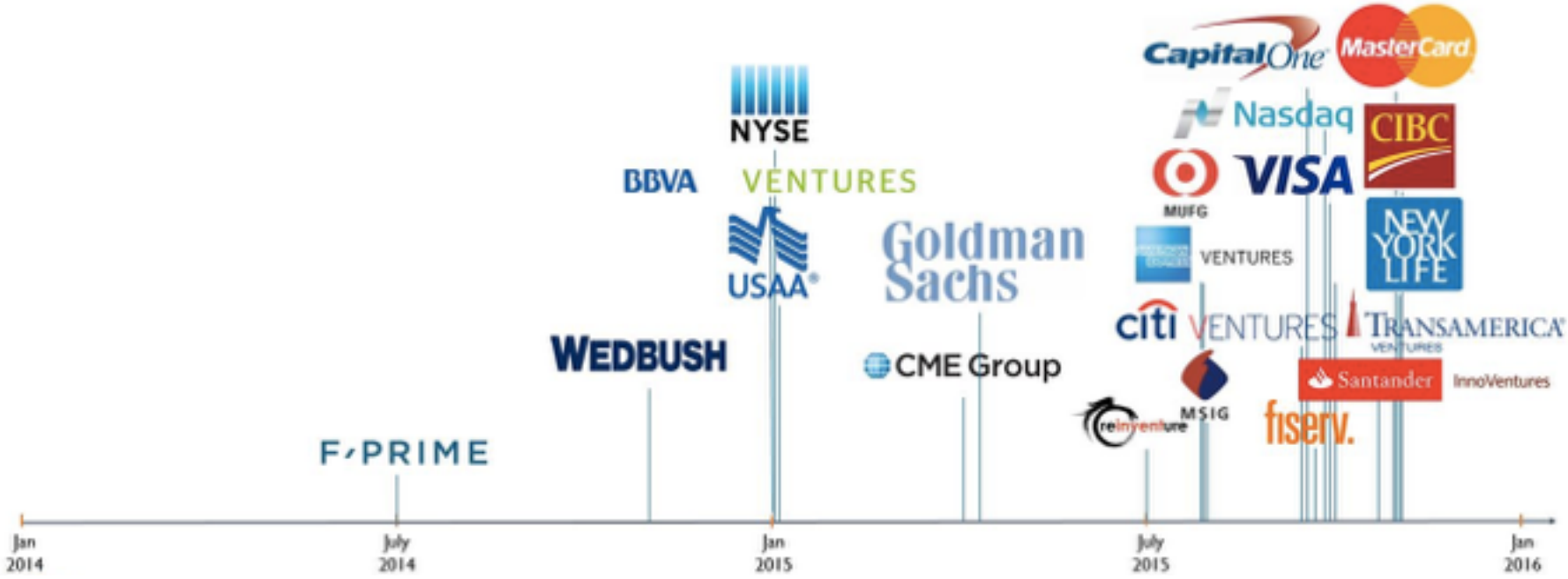
Centralized

2000-2010

Local Marketplaces

Global

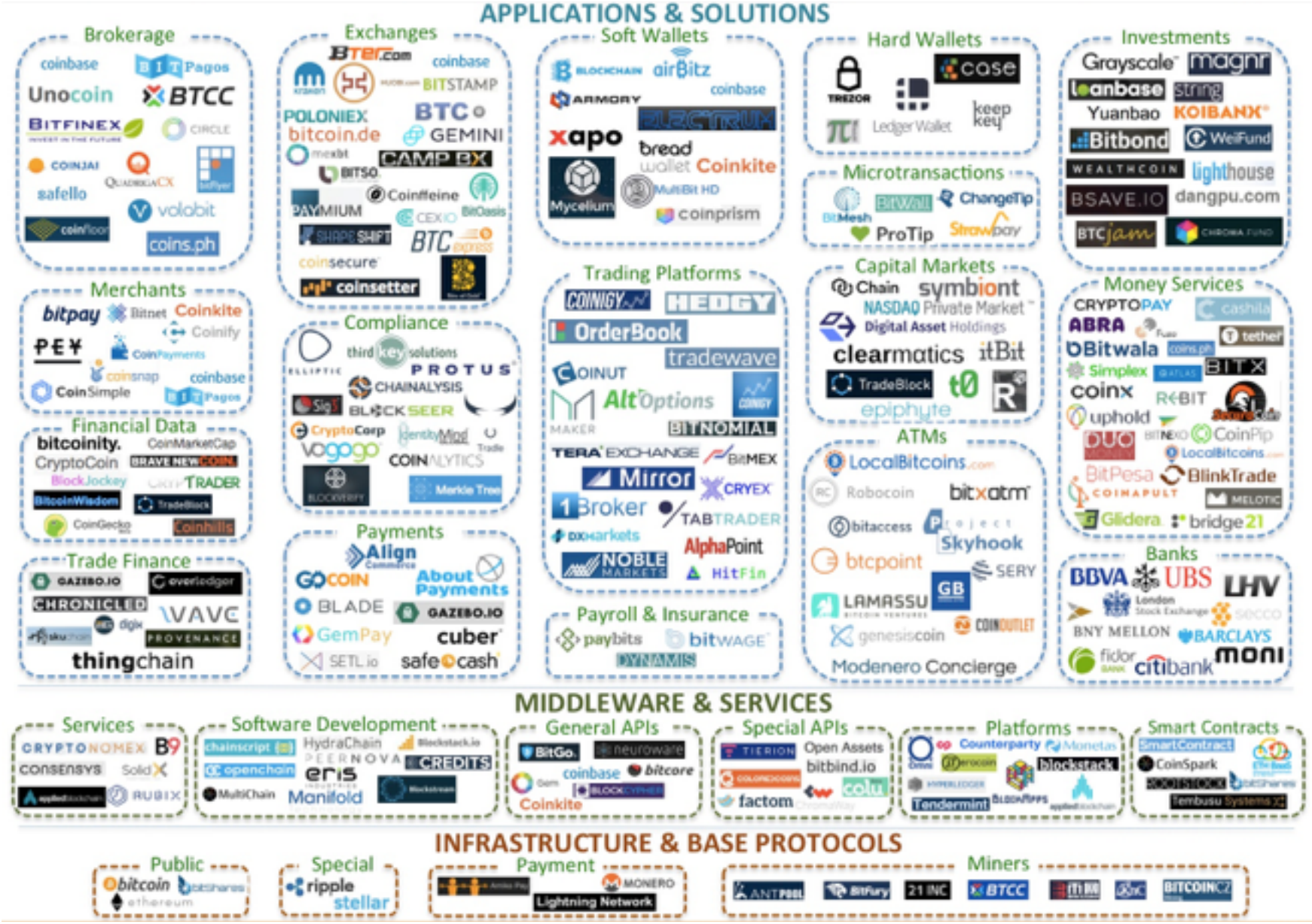
Blockchain can change ... well everything



Source: CB Insights

Blockchain can change ... well everything

PURDUE UNIVERSITY



Source: http://startupmanagement.org/blog

Blockchain can change ... well everything

PURDUE UNIVERSITY

Source: http://startupmanagement.org/blog

This talk proudly aims at leaving you with more interesting questions than mere answers regarding credit networks. :)

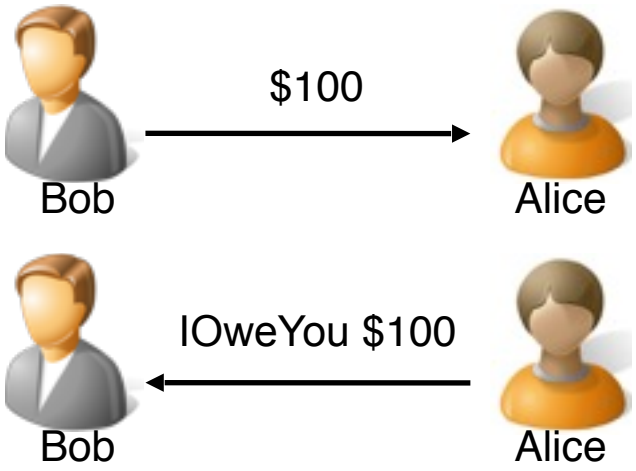
Credit (or IOU settlement) Networks: Basics

PURDUE UNIVERSITY

Credit (or IOU settlement) Networks: Basics

PURDUE UNIVERSITY

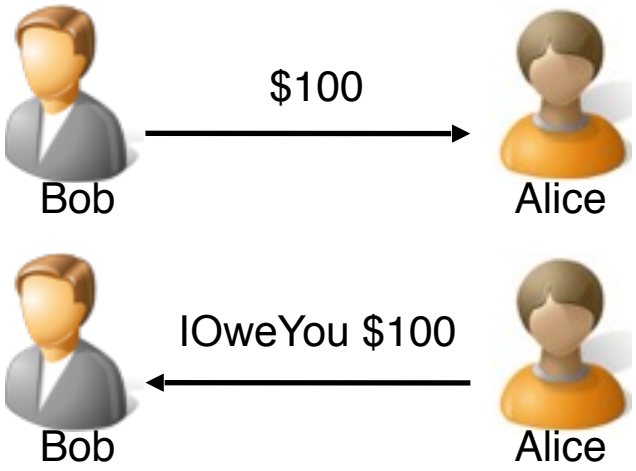
Transactions in the real world



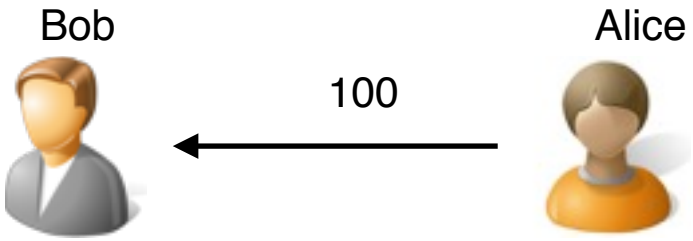
Credit (or IOU settlement) Networks: Basics

PURDUE UNIVERSITY

Transactions in the real world



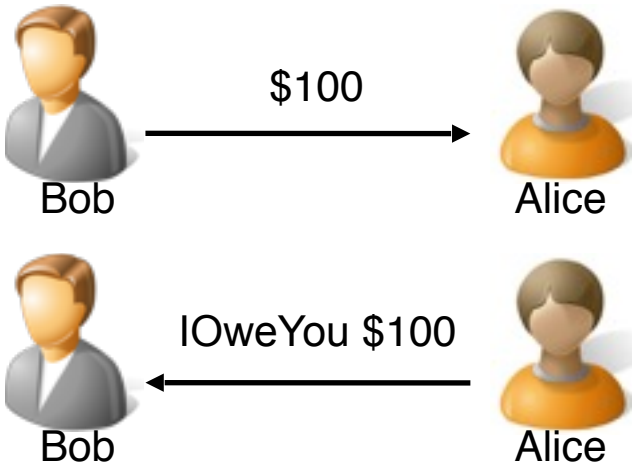
A credit network representation



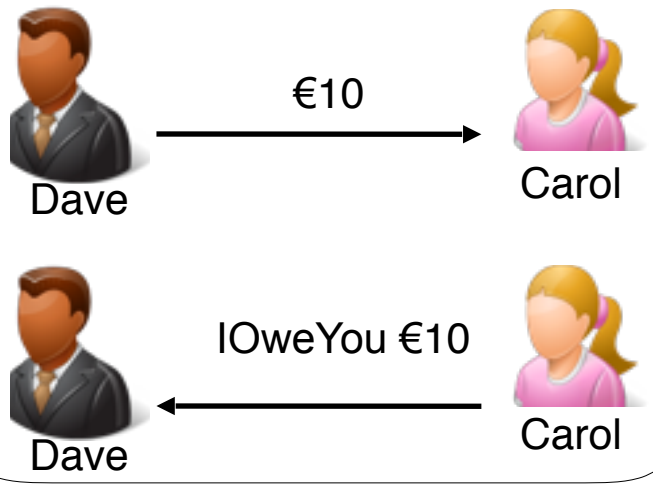
Credit (or IOU settlement) Networks: Basics

PURDUE UNIVERSITY

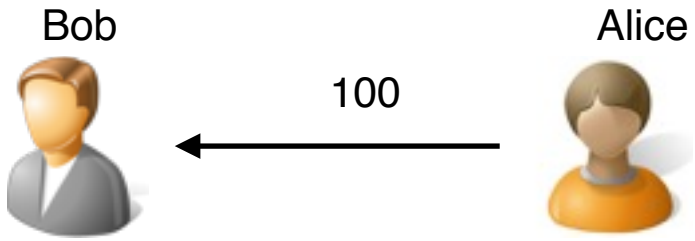
Transactions in the real world



During a hike with Alice & Bob



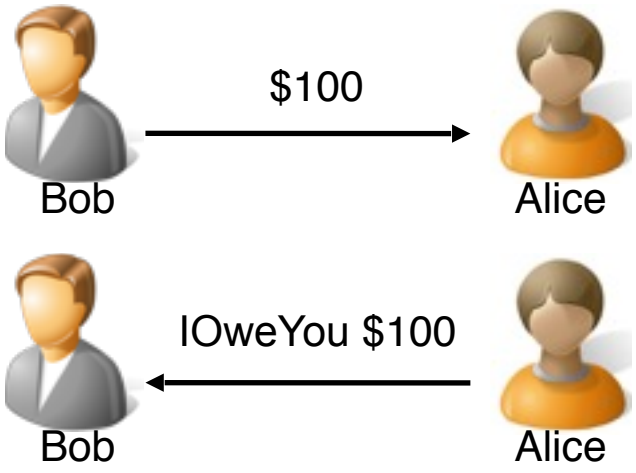
A credit network representation



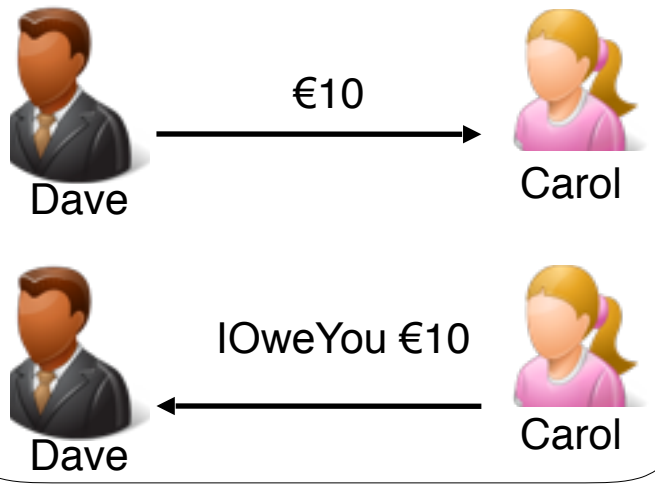
Credit (or IOU settlement) Networks: Basics

PURDUE UNIVERSITY

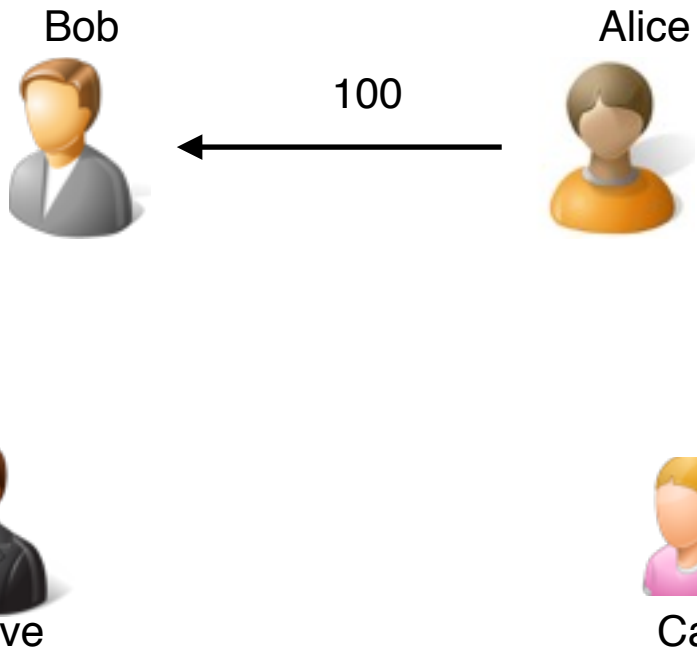
Transactions in the real world



During a hike with Alice & Bob



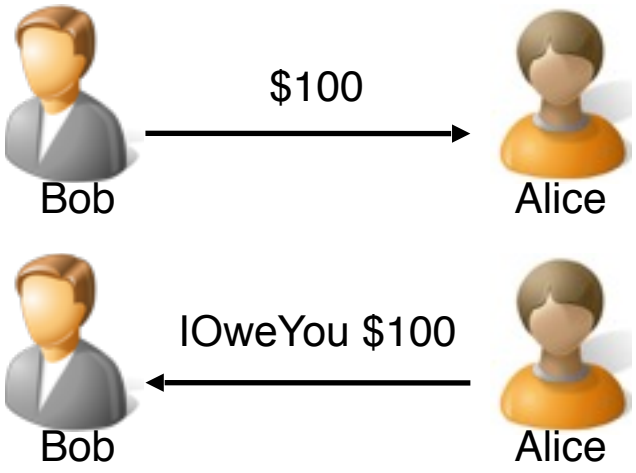
A credit network representation



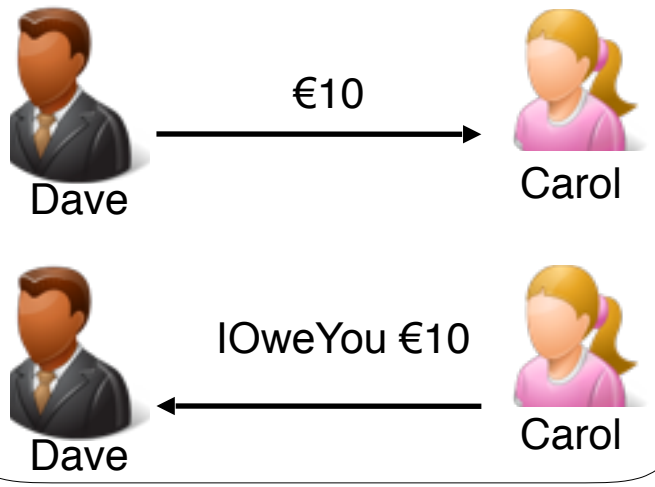
Credit (or IOU settlement) Networks: Basics

PURDUE UNIVERSITY

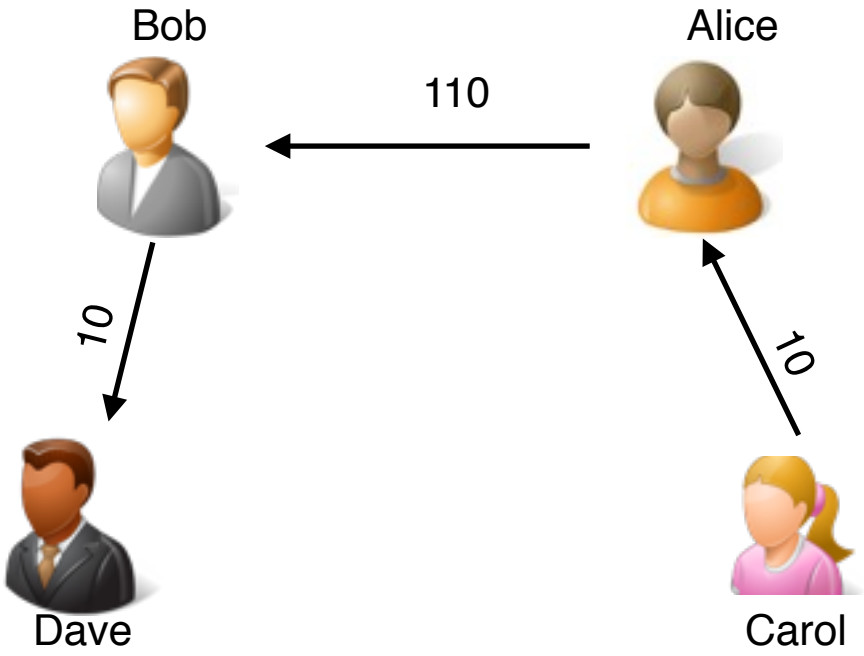
Transactions in the real world



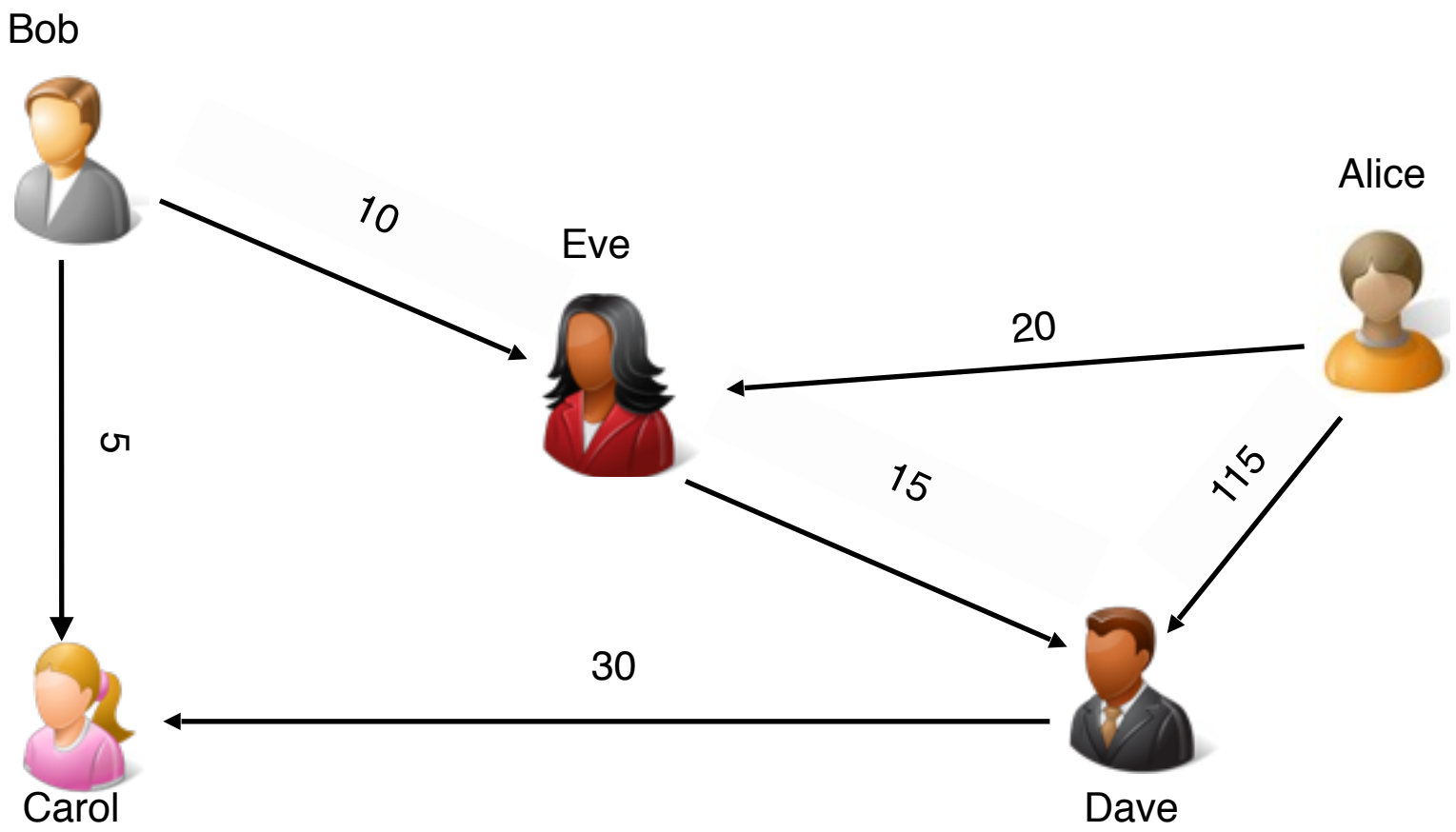
During a hike with Alice & Bob



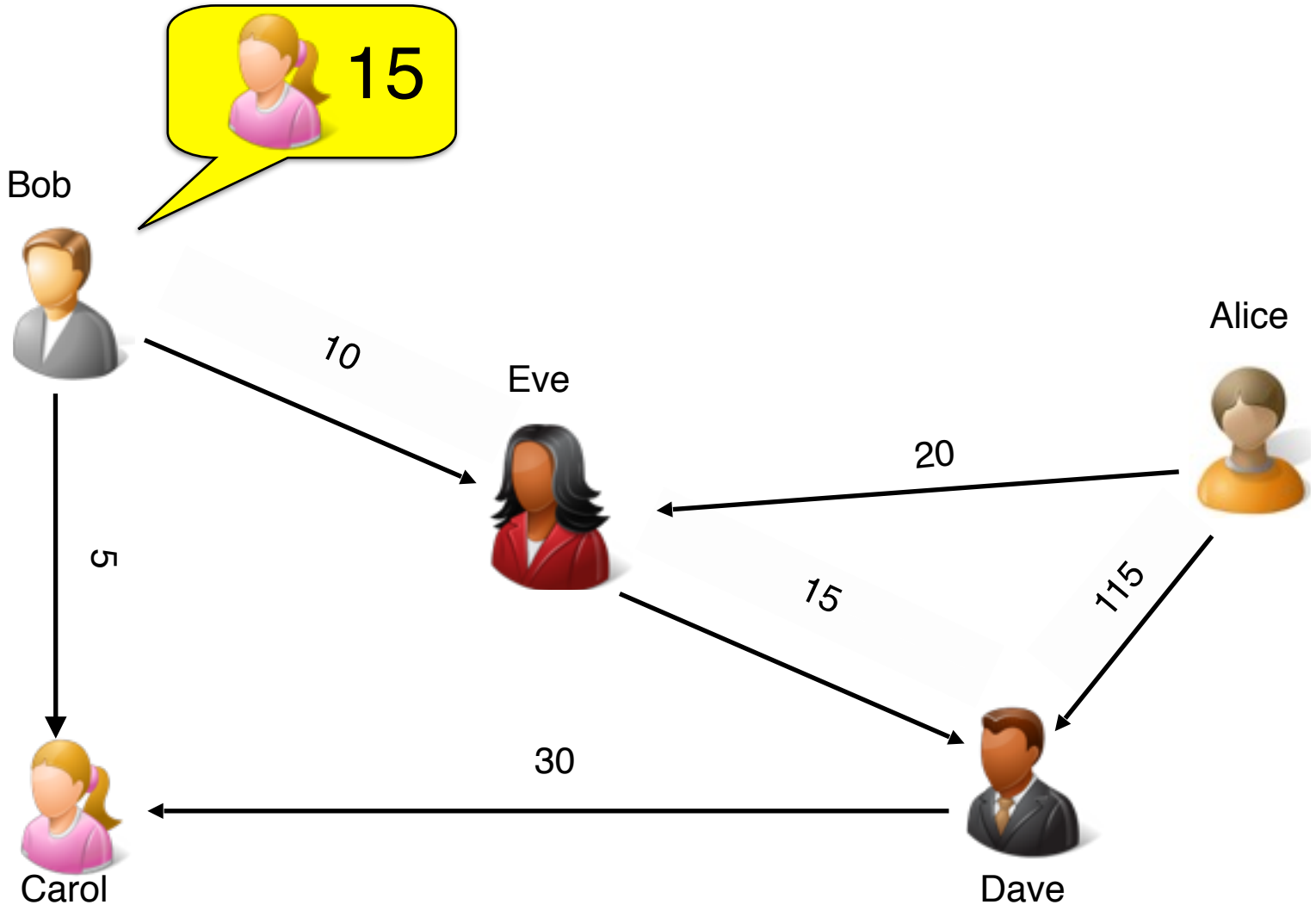
A credit network representation



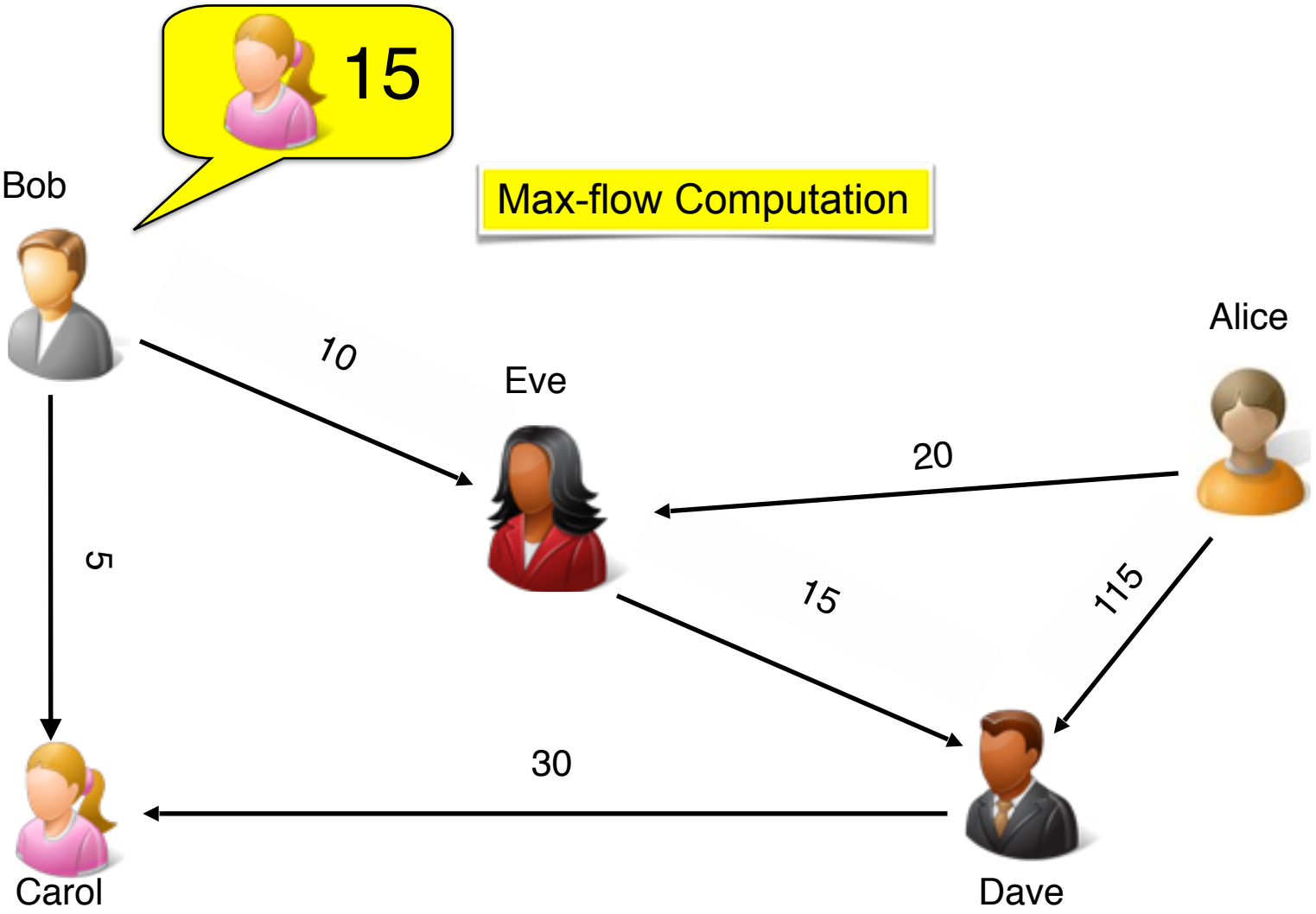
Payment (or credit) Network: an Example



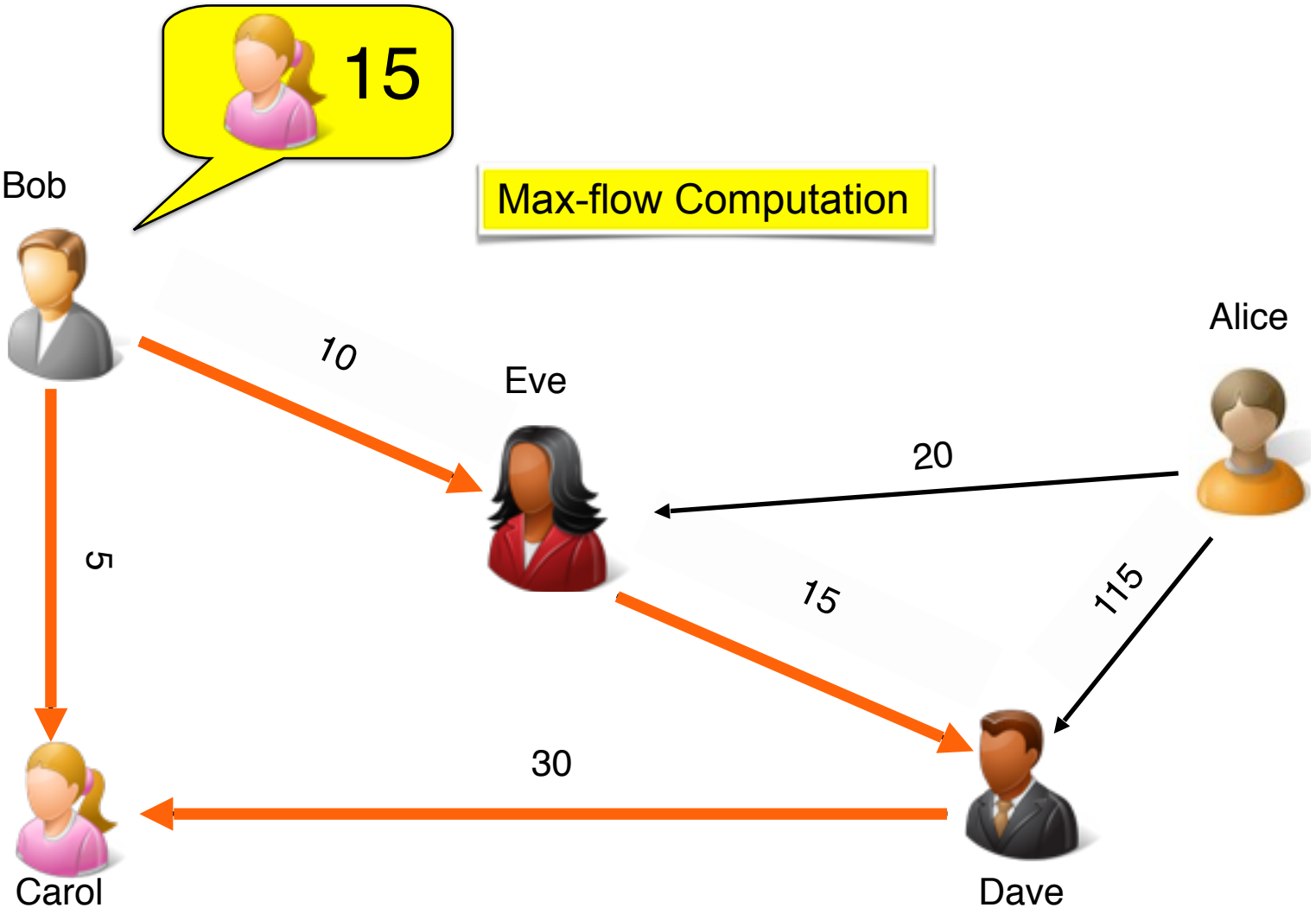
Payment (or credit) Network: an Example



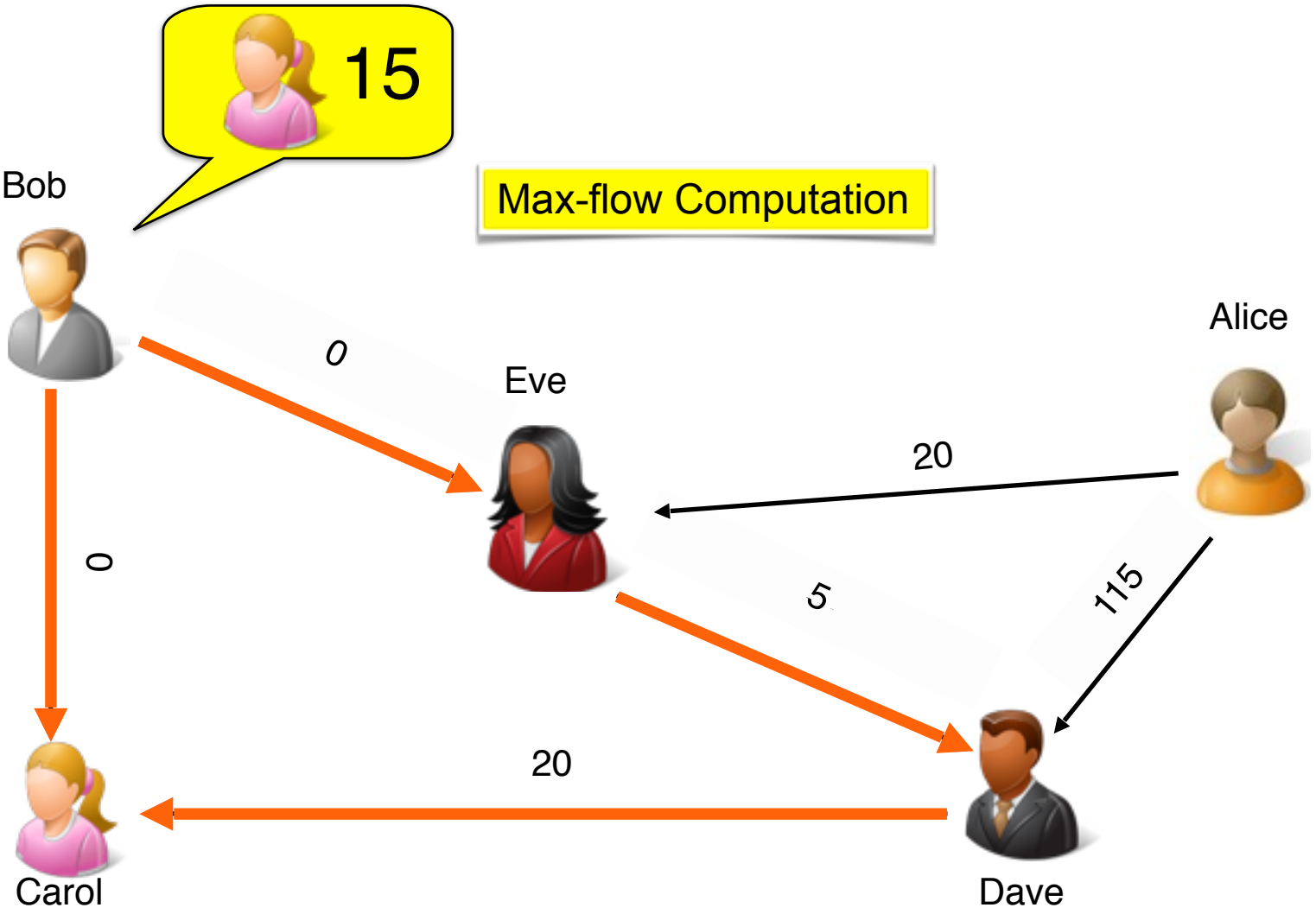
Payment (or credit) Network: an Example



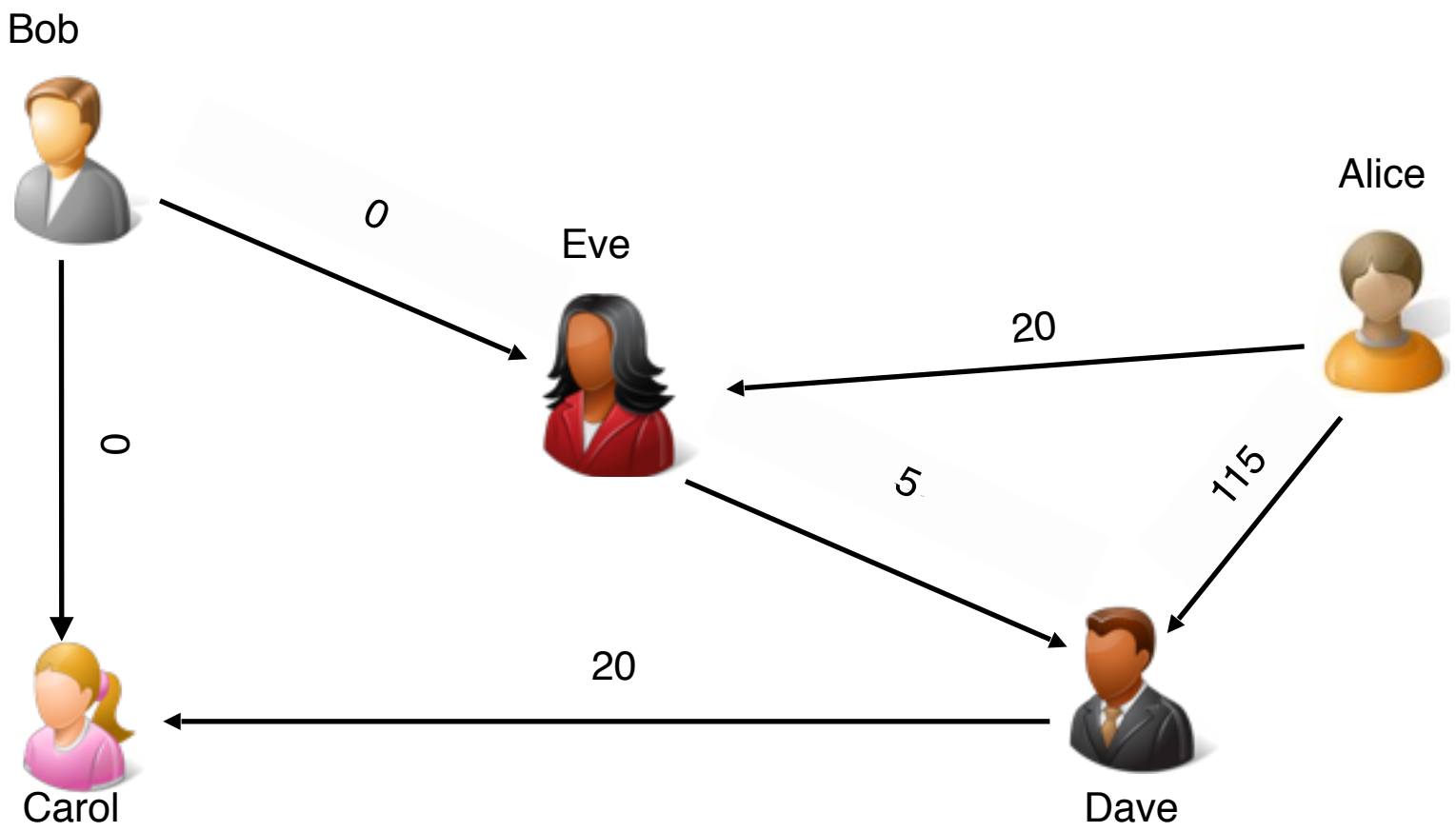
Payment (or credit) Network: an Example



Payment (or credit) Network: an Example



Payment (or credit) Network: an Example



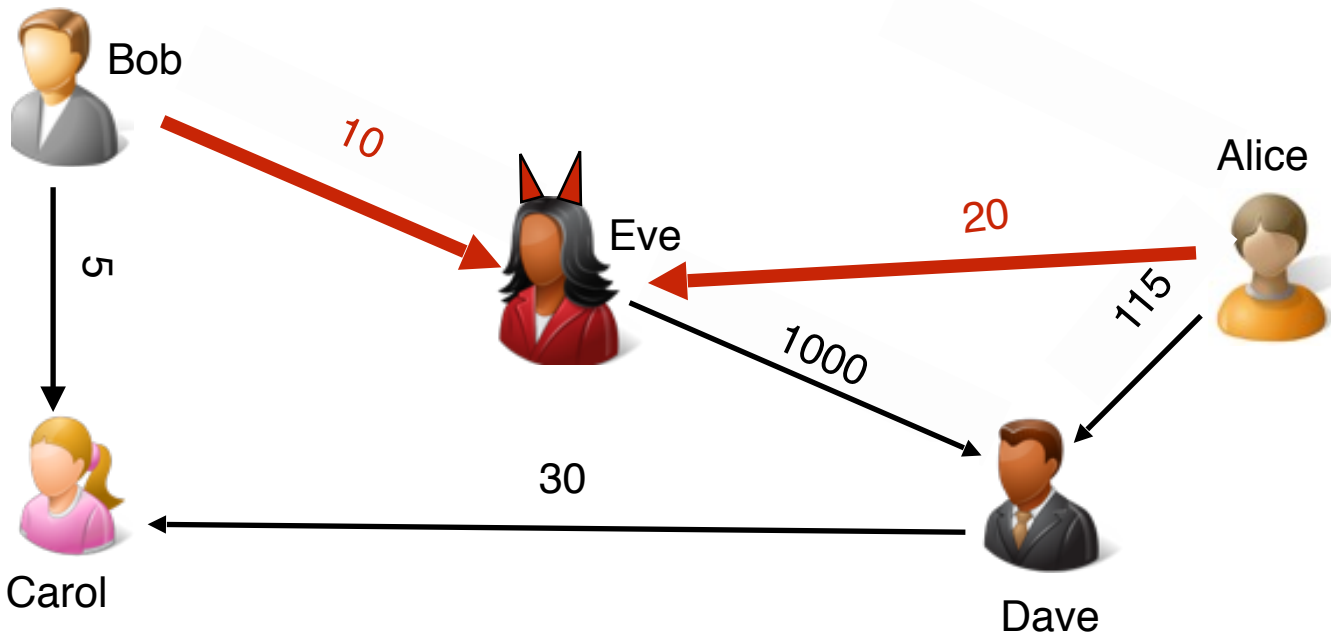
Key Questions for Credit Network Designs

PURDUE UNIVERSITY

- Roots in the very old Barter System or Havala
- Path Selection
  - How do we find paths?
    - Max flow algorithms may not scale
  - How do we select paths?
    - Social welfare; e.g., allowing many transactions to succeed
      - NP-hard problem
- Liquidity of the network
  - For randomly chosen pair of nodes, and transaction value, what is the probability that the transaction succeeds?
  - More and stronger links, better liquidity; Clique!?
- Sybil Tolerance
  - Number of sybil nodes should not matter
  - How much IOU credit can we allow the adversary to garner?
    - How many sybil links can we manage?
    - What kind topologies and links values?

Why credit networks matter?

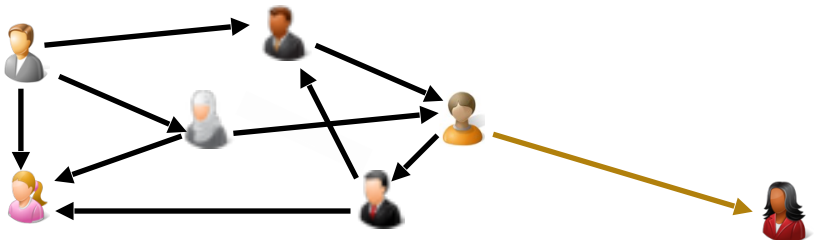
- A flexible-yet-robust design for distributed (transitive) trust
  - through pairwise credit allocations
- Loss incurred due to misbehaving identities is bounded and (sometimes) localized



Building trust with credit networks

PURDUE UNIVERSITY

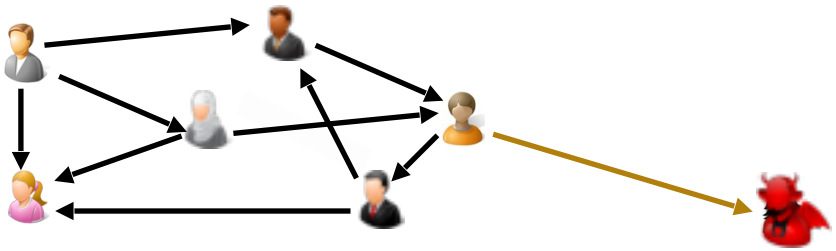
- Sybil-resistant applications



Building trust with credit networks

PURDUE UNIVERSITY

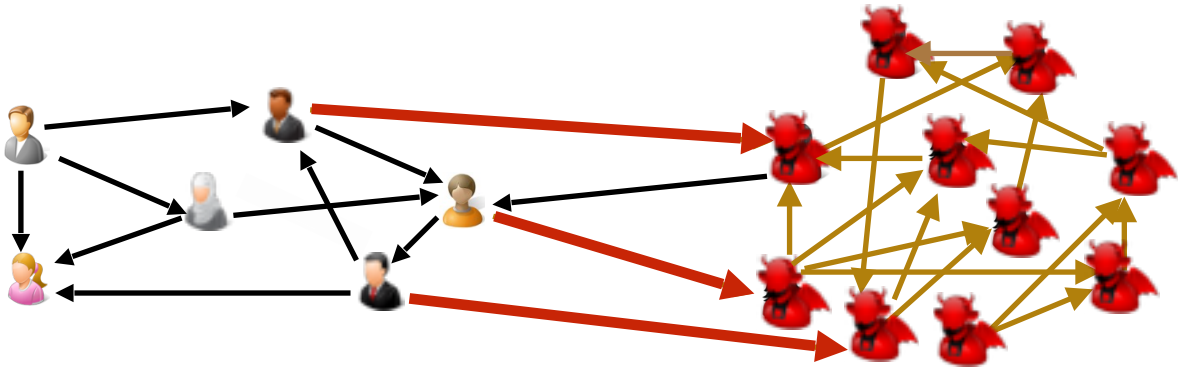
- Sybil-resistant applications



Building trust with credit networks

PURDUE UNIVERSITY

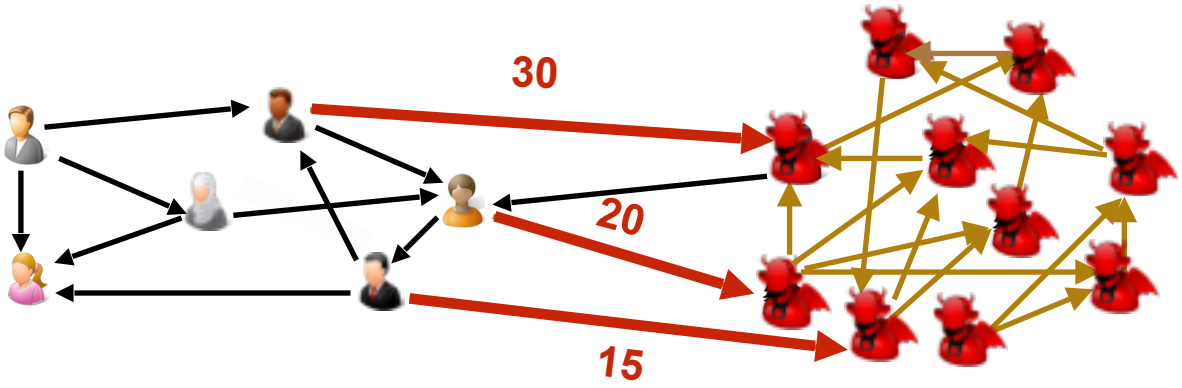
- Sybil-resistant applications



Building trust with credit networks

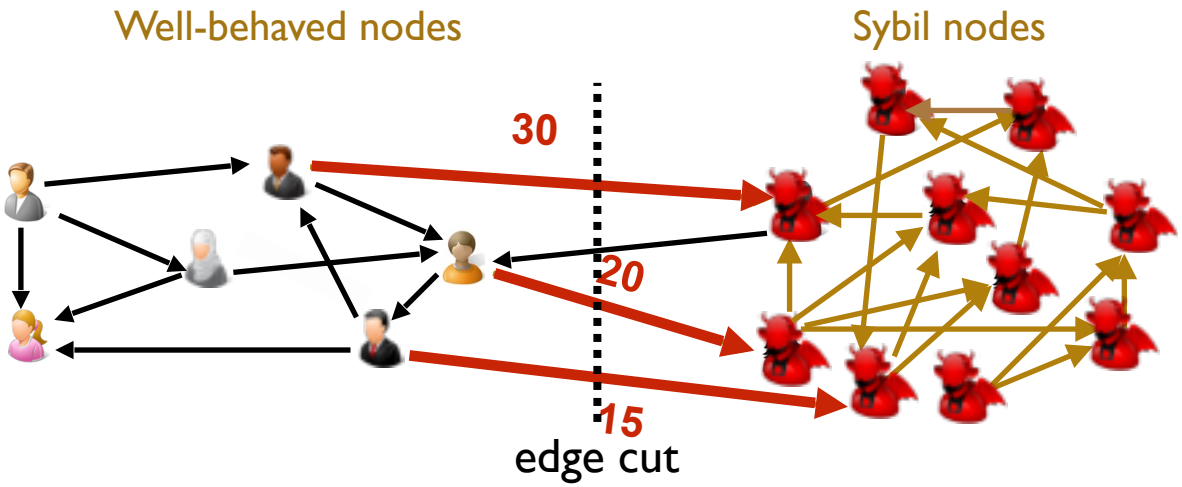
PURDUE UNIVERSITY

- Sybil-resistant applications



Building trust with credit networks

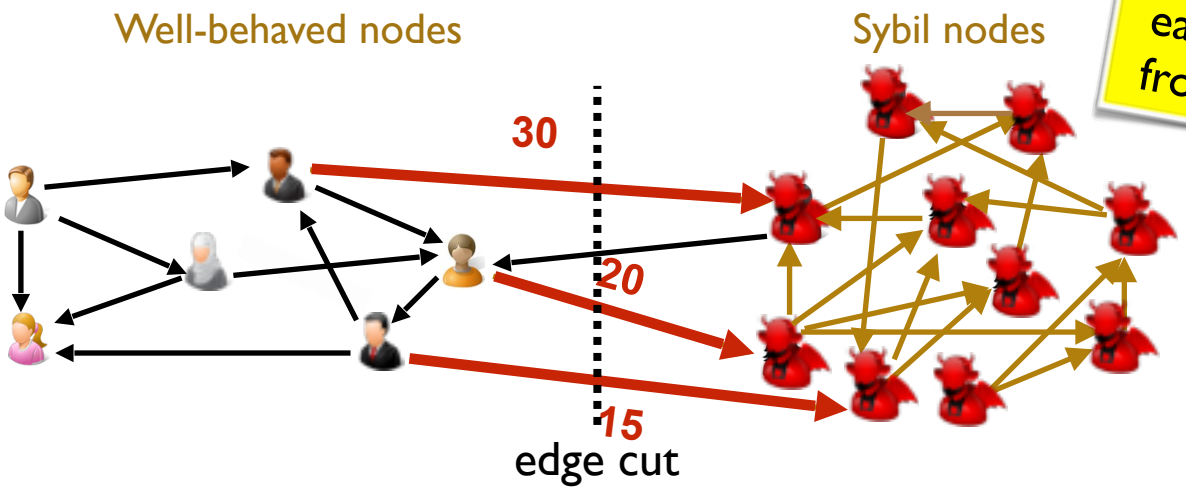
- Sybil-resistant applications



Building trust with credit networks

PURDUE UNIVERSITY

- Sybil-resistant applications

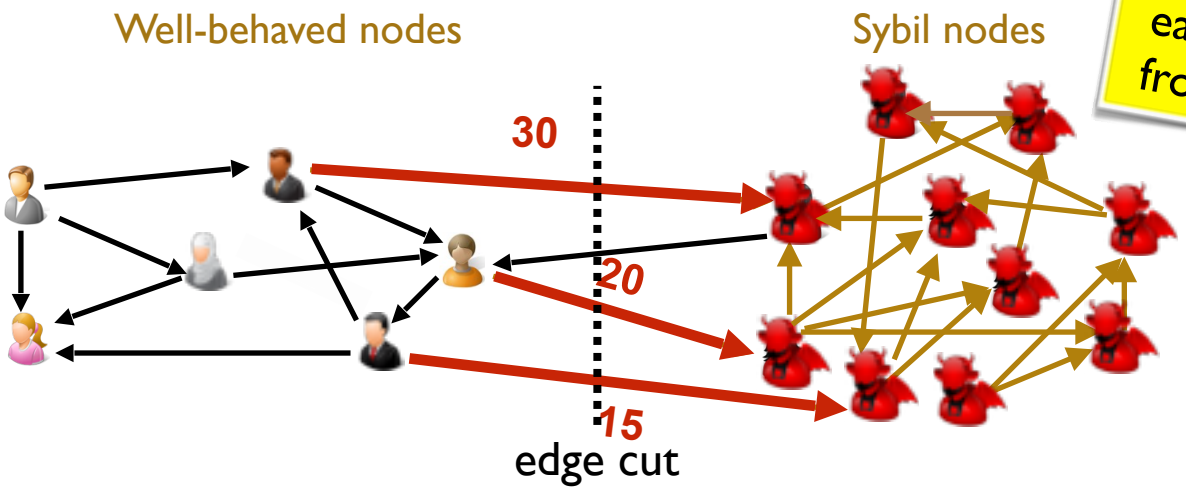


Introducing nodes is much easier than drawing trust from well-behaved nodes

Building trust with credit networks

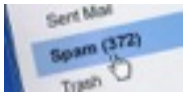
PURDUE UNIVERSITY

- Sybil-resistant applications



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

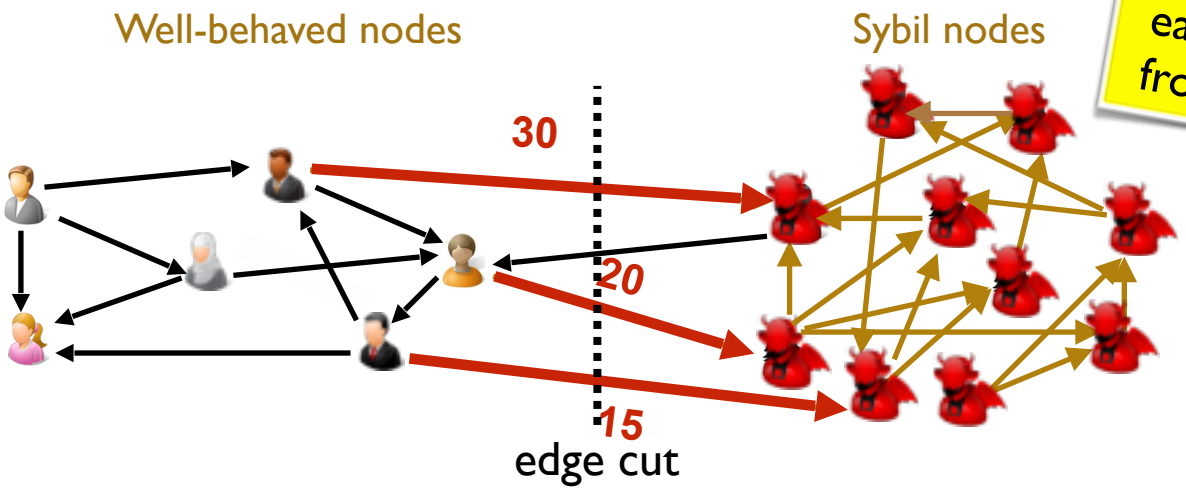
- Several Systems
  - Ostra: preventing e-mail spam [NSDI'08]



Building trust with credit networks

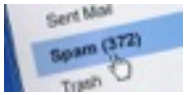
PURDUE UNIVERSITY

- Sybil-resistant applications



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

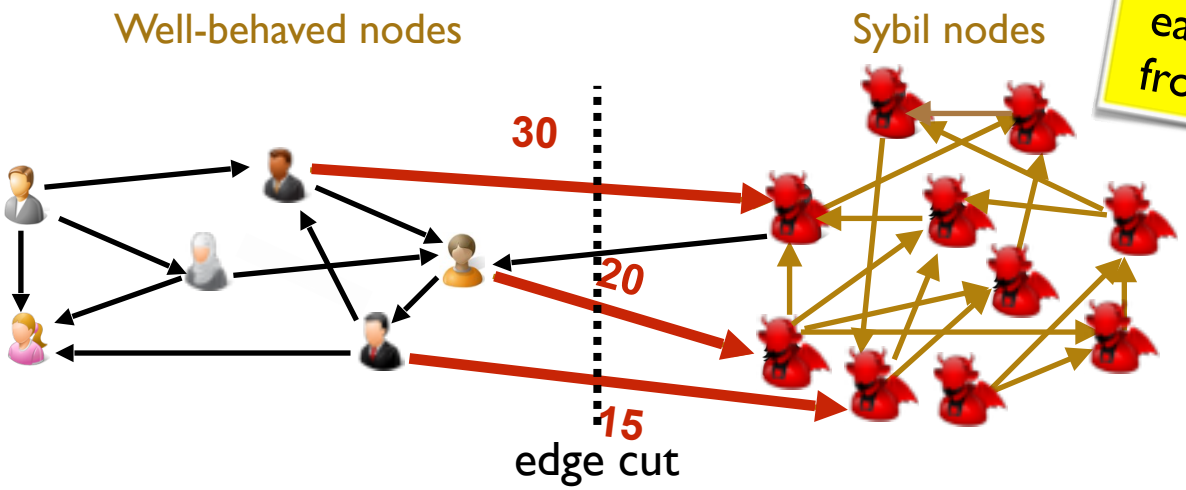
- Several Systems
  - Ostra: preventing e-mail spam [NSDI'08]
  - Bazaar: strengthening e-commerce [NSDI'11]



Building trust with credit networks

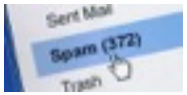
PURDUE UNIVERSITY

- Sybil-resistant applications



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

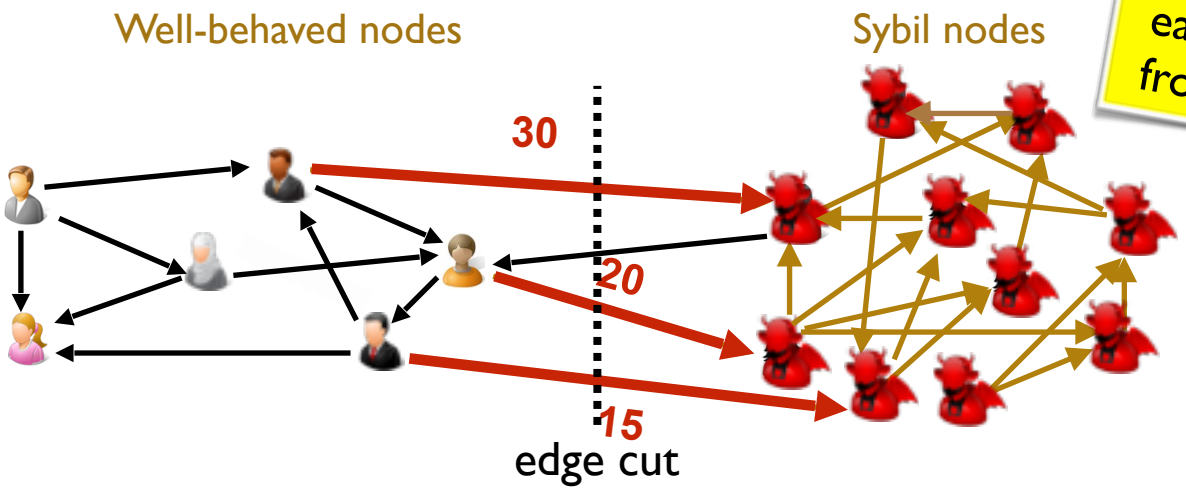
- Several Systems
  - Ostra: preventing e-mail spam [NSDI'08]
  - Bazaar: strengthening e-commerce [NSDI'11]
  - SumUp: Sybil-resilient content voting [NSDI'09]



Building trust with credit networks

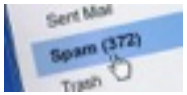
PURDUE UNIVERSITY

- Sybil-resistant applications



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

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



Bazaar: Strengthening Online Marketplaces

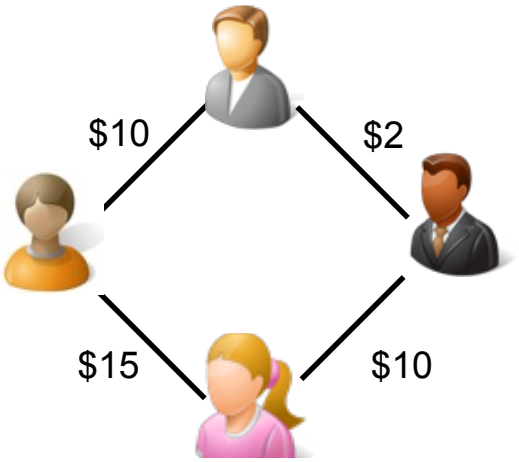
PURDUE UNIVERSITY

[NSDI'11]

Bazaar: Strengthening Online Marketplaces

PURDUE UNIVERSITY

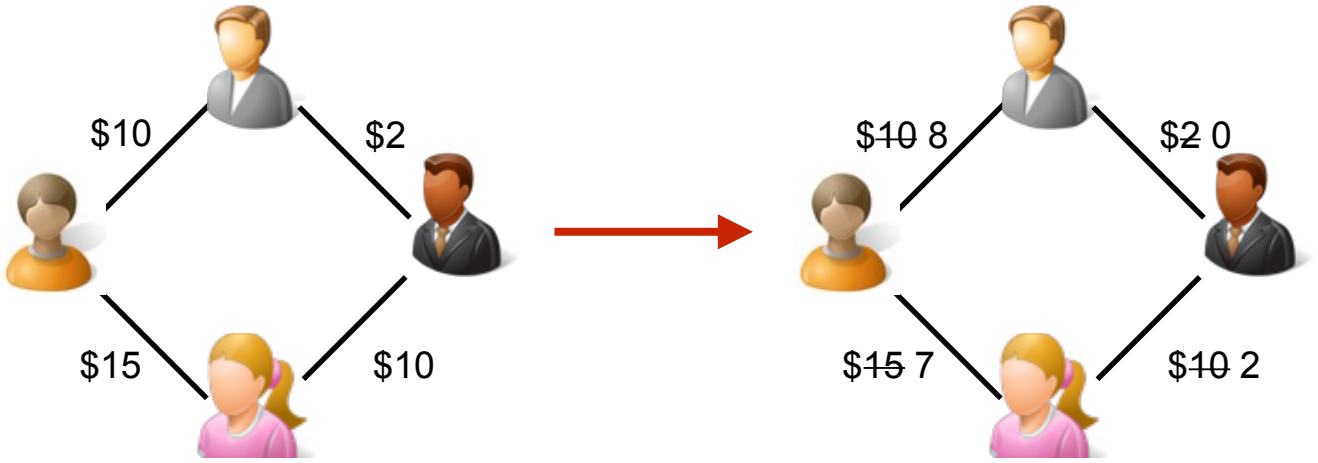
[NSDI'11]



Undirected reputations links!

Bazaar: Strengthening Online Marketplaces

[NSDI'11]

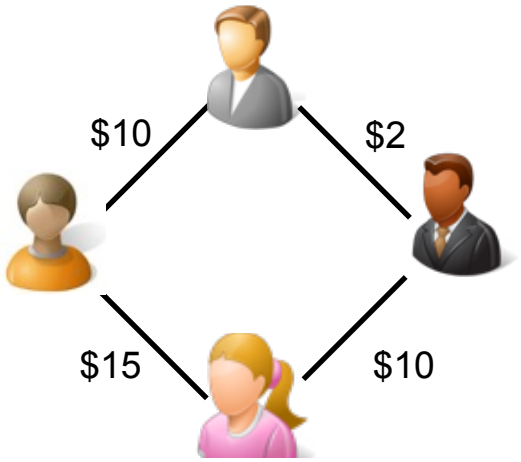


Undirected reputations links!

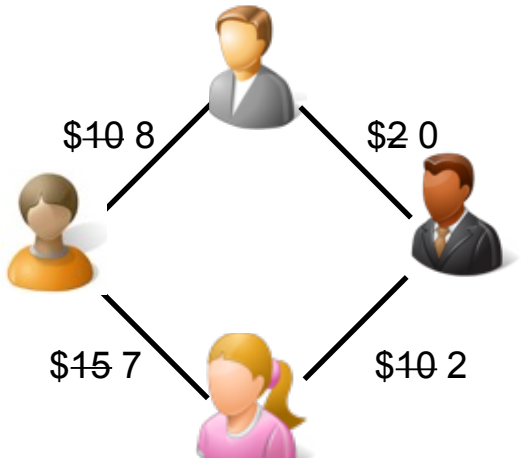
Consider a $10 transaction

Bazaar: Strengthening Online Marketplaces

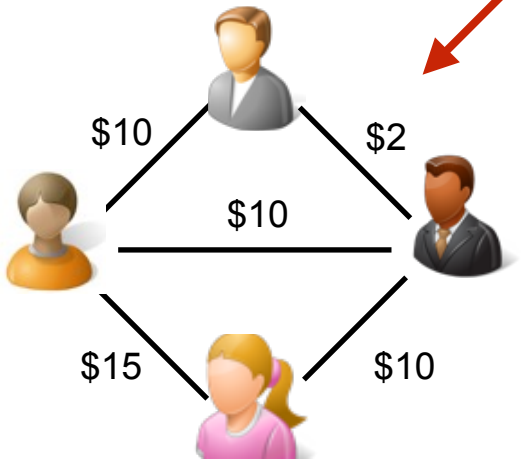
[NSDI'11]



Undirected reputations links!



Consider a $10 transaction

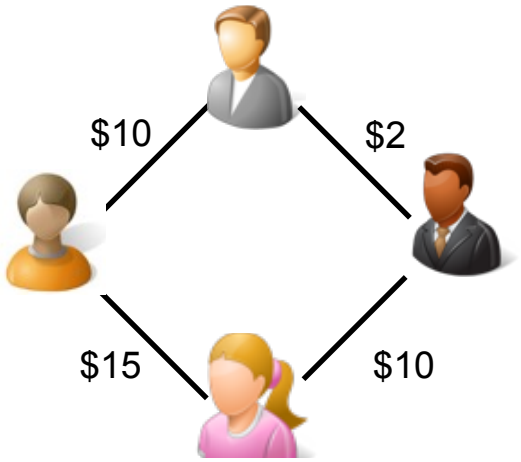


After a positive review

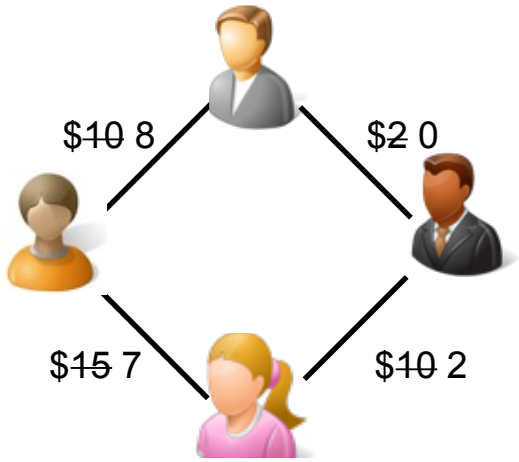
Bazaar: Strengthening Online Marketplaces

PURDUE UNIVERSITY

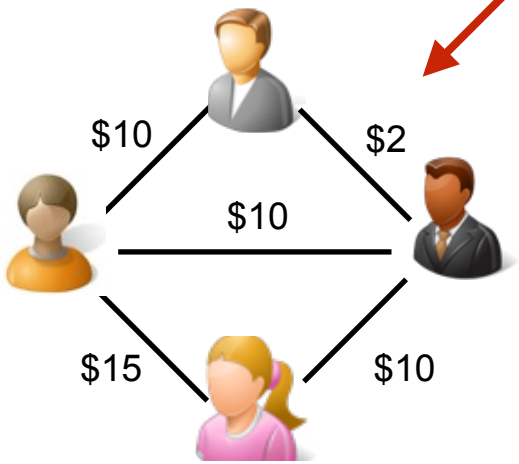
[NSDI'11]



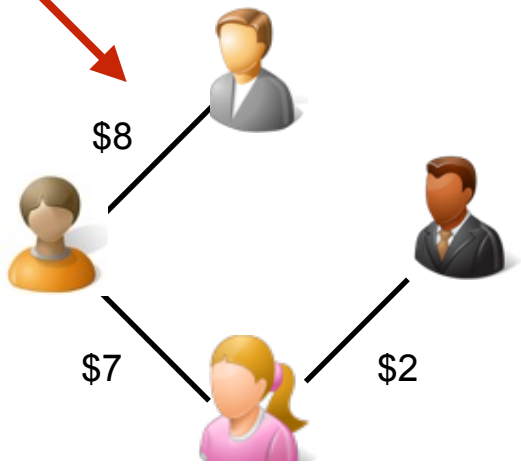
Undirected reputations links!



Consider a $10 transaction

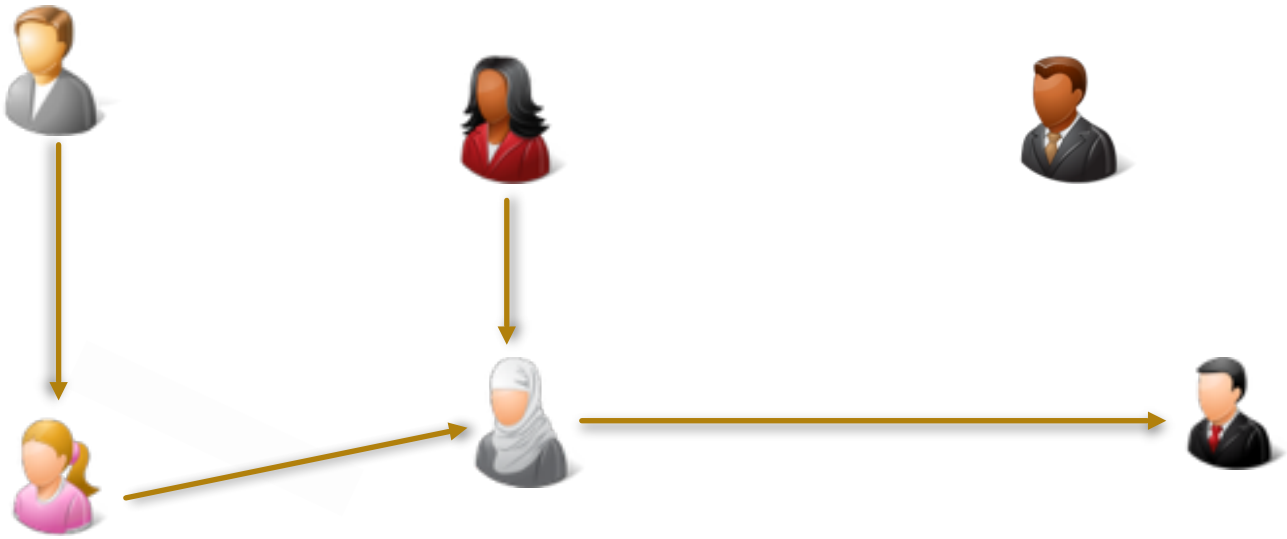


After a positive review

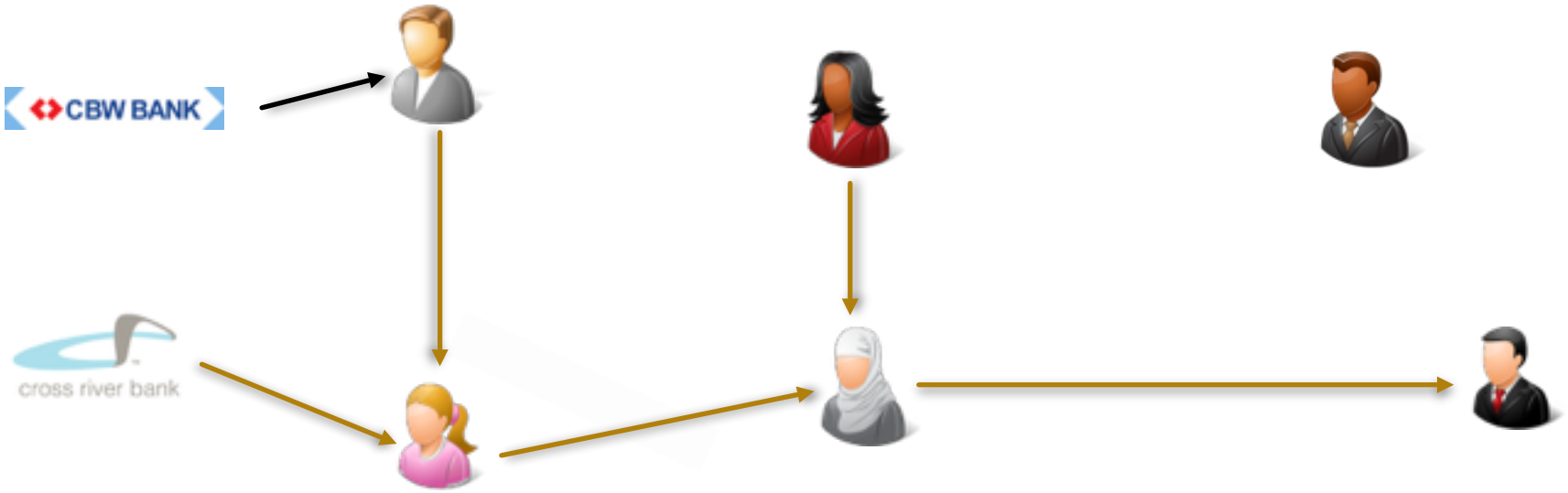


After a negative review

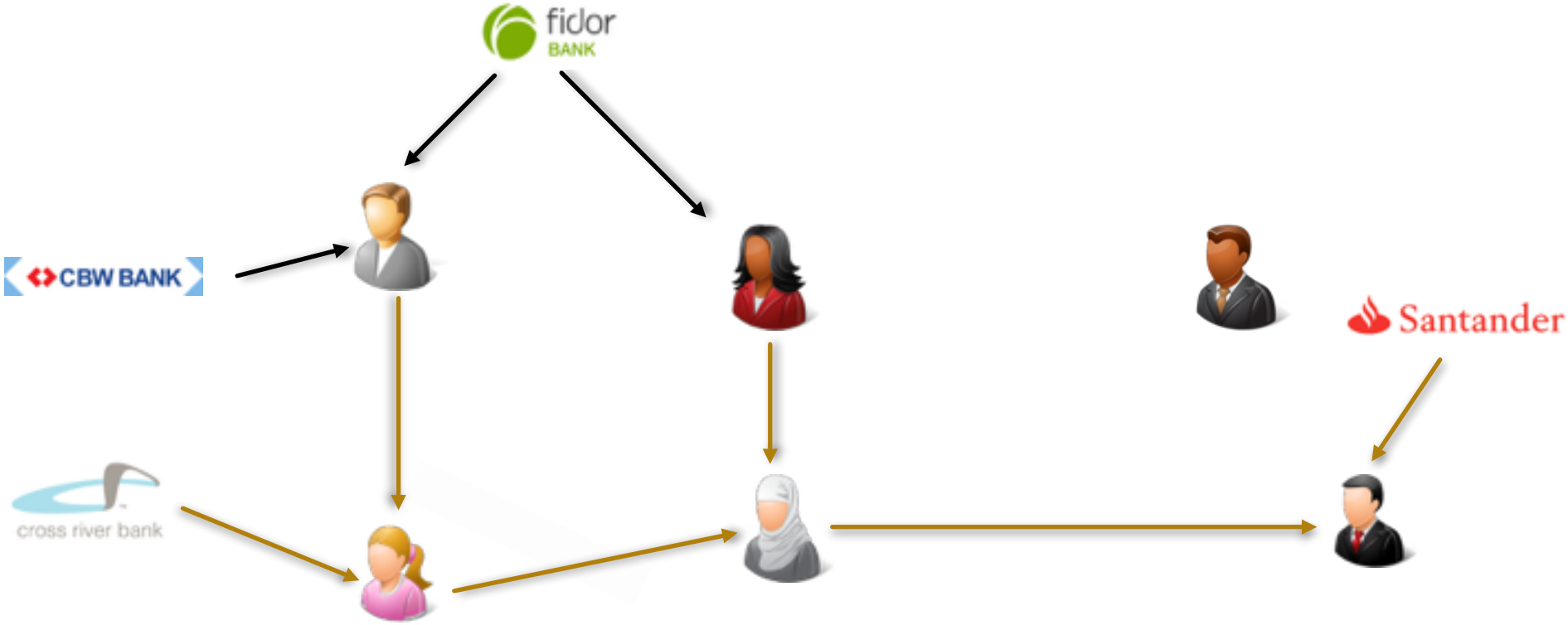
Ripple Credit (or Settlement) Network



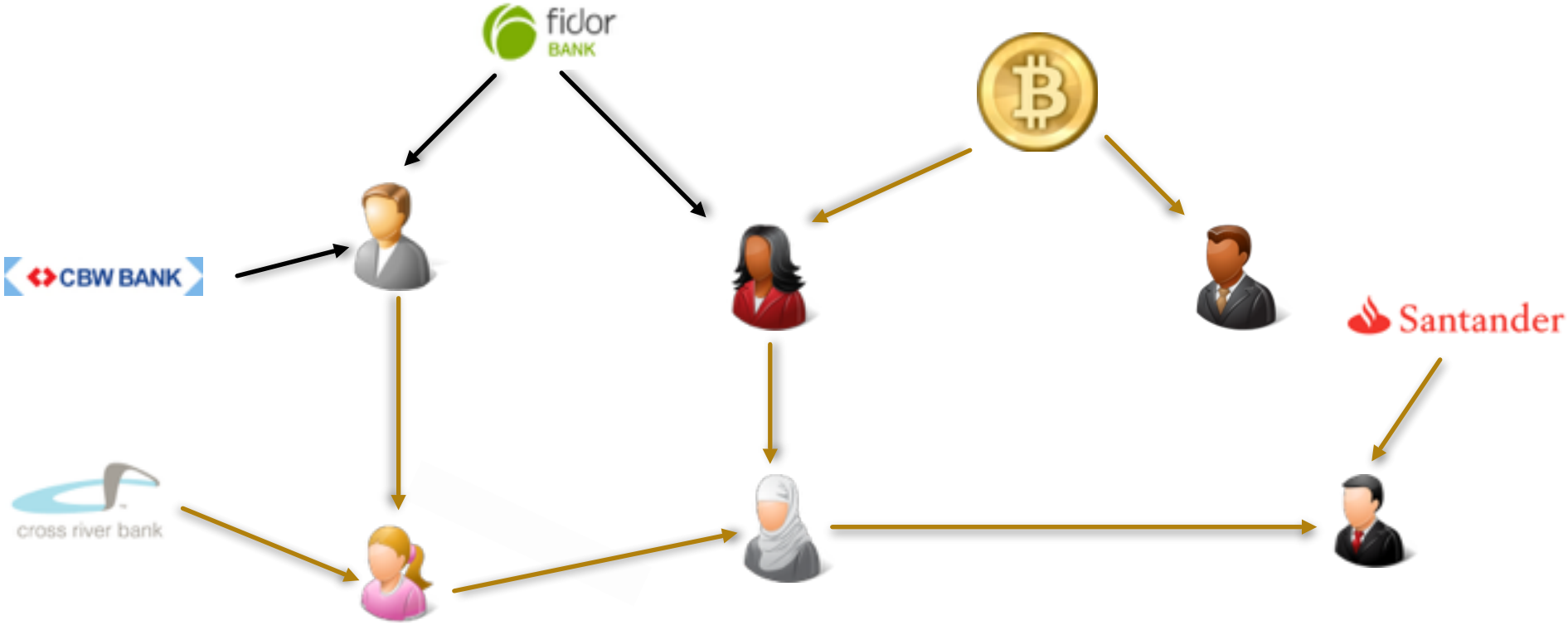
Ripple Credit (or Settlement) Network



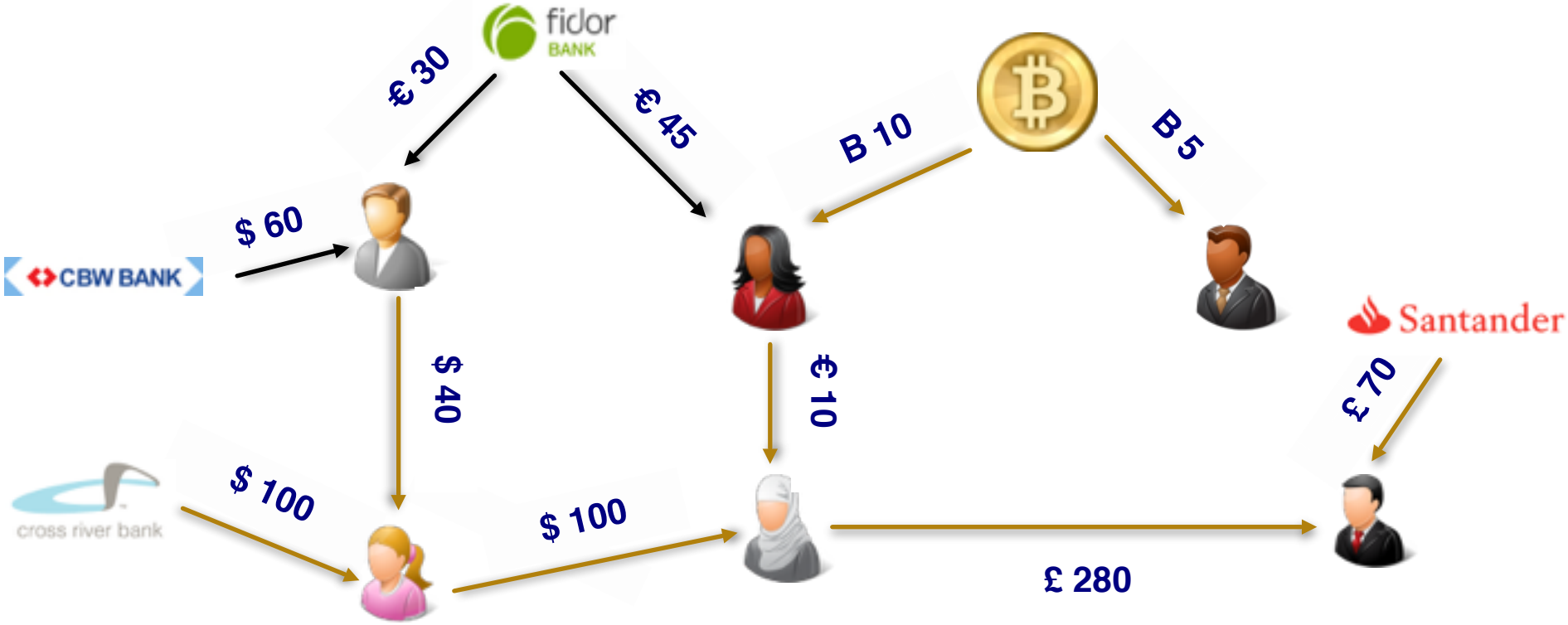
Ripple Credit (or Settlement) Network



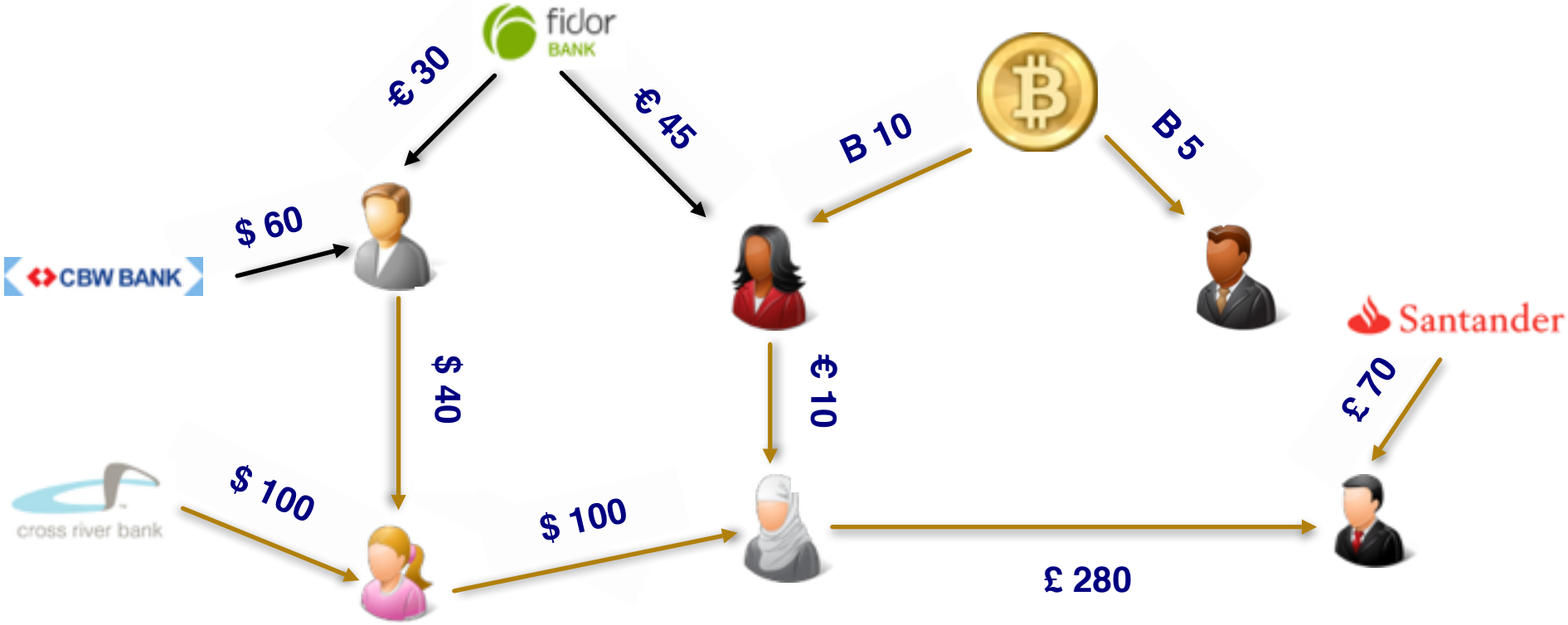
Ripple Credit (or Settlement) Network



Ripple Credit (or Settlement) Network

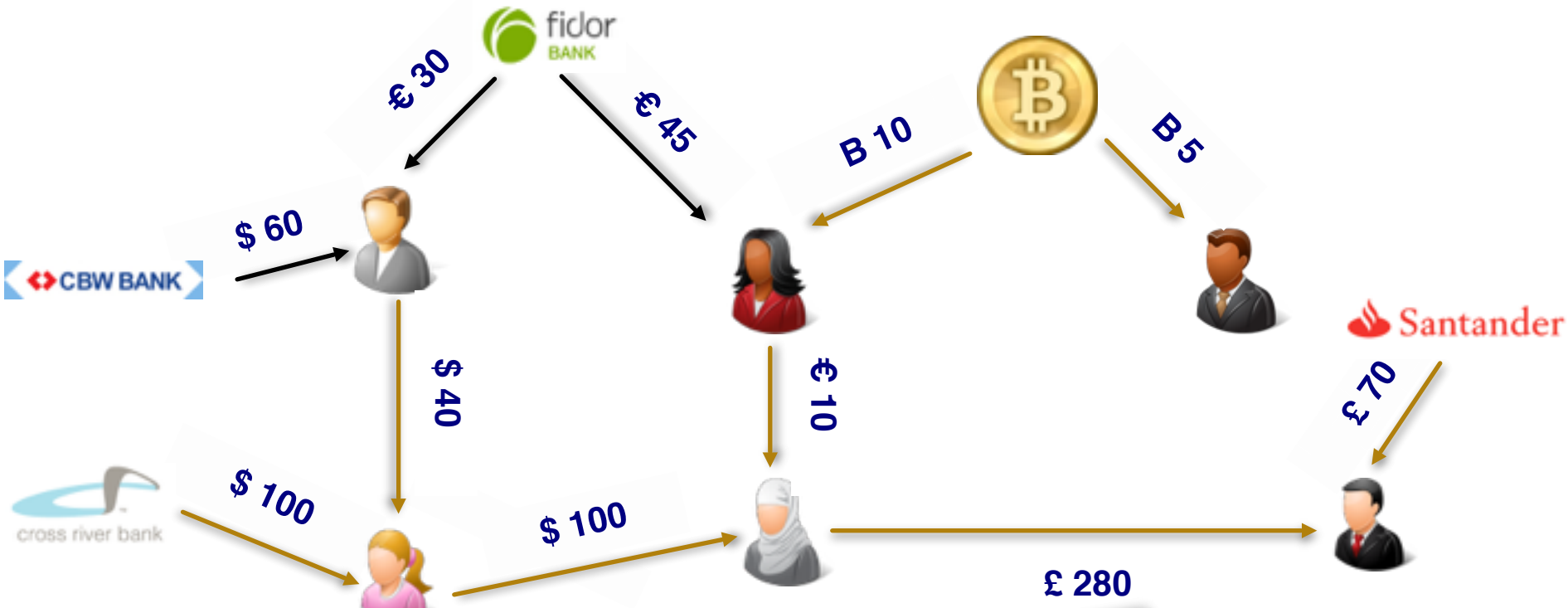


Ripple Credit (or Settlement) Network



	Tx time	Worldwide, inter-currency tx	Integrity
BANK	~ 1 day	High fees	Bank only
ripple	~ 5 seconds	Tiny fees	Public verifiability

Ripple Credit (or Settlement) Network



Ripple can significantly improve cross-currency remittance and settlements

	Tx tim		Integrity
BANK	~ 1 day	High fees	Bank only
ripple	~ 5 seconds	Tiny fees	Public verifiability

Cryptocurrencies vs Credit Networks

PURDUE UNIVERSITY

We already have cryptocurrencies, then why do we need Ripple?

	Cryptocurrencies	IOU Credit Networks
Definition	Medium of exchange; future productivity of the public	Credit settlement network: future productivity of a specific borrower
Transfer of funds	Direct transactions between any two wallets	Transactions only via a path with enough credit
Fungibility	Good	Restricted by path availability
Scalability	Limited transaction rate (<100 tps)	Highly scalable

Cryptocurrencies vs Credit Networks

PURDUE UNIVERSITY

- IOU (or Credit) Networks
  - Combining credit and social trust (still *not* permissioned)

Cryptocurrencies vs Credit Networks

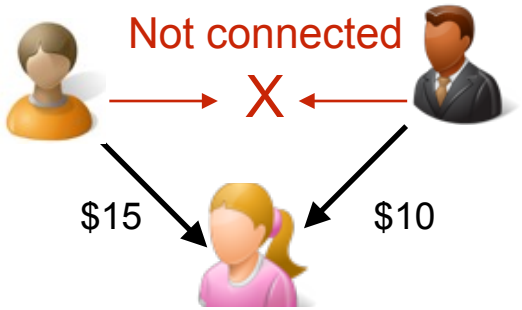
PURDUE UNIVERSITY

- IOU (or Credit) Networks
  - Combining credit and social trust (still *not* permissioned)
- Restricted Fungibility of Credit Networks

Cryptocurrencies vs Credit Networks

PURDUE UNIVERSITY

- IOU (or Credit) Networks
  - Combining credit and social trust (still *not* permissioned)
- Restricted Fungibility of Credit Networks

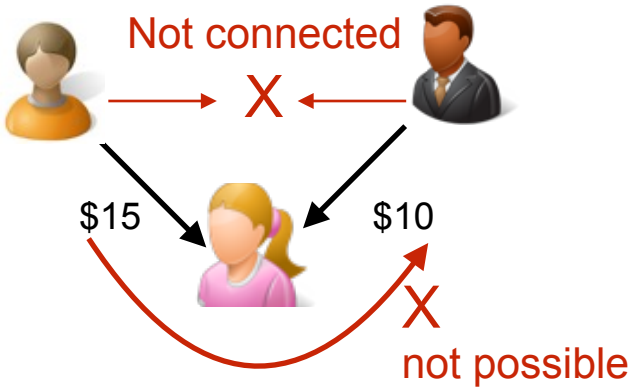


Cryptocurrencies vs Credit Networks

PURDUE UNIVERSITY

- IOU (or Credit) Networks
  - Combining credit and social trust (still *not* permissioned)

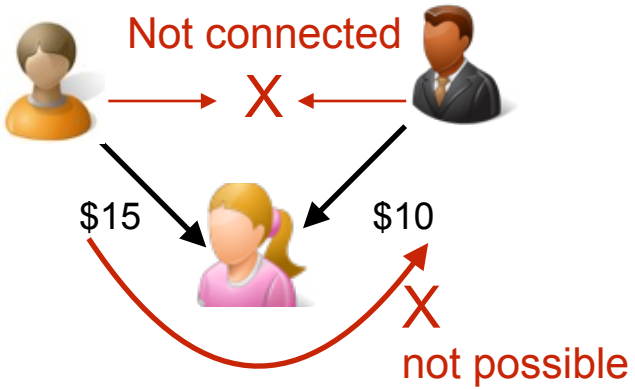
- Restricted Fungibility of Credit Networks



Cryptocurrencies vs Credit Networks

PURDUE UNIVERSITY

- IOU (or Credit) Networks
  - Combining credit and social trust (still *not* permissioned)
- Restricted Fungibility of Credit Networks



- The Tyranny of Proof of Work
  - Bitcoin mining could consume as much electricity as Denmark by 2020!
  - (Distributed) credit networks may not require global consensus!
    - I care only about my links to my friends
    - I do not even care about links between friends and friends-of-friends
    - Formalization coming soon …

Credit Networks: State of the Art

PURDUE UNIVERSITY

- Examples: Ripple, Stellar Settlement Networks
  - For Ripple,
    Trade volume: $800K Payment volume: $400K per day
  - Several banking systems across the world (US, Canada, Germany, China, Japan, Singapore,…) are getting involved
- Global (Federated!) Consensus
  - Non-standard atomic broadcast protocol
    - An interesting problem to study/improve it
  - Choice to consensus parties is not convincing
    - A major criticism against Ripple in academics and P2P communities
- Public verifiability of transactions
  - Motivated from the Bitcoin success
  - Same privacy problem!

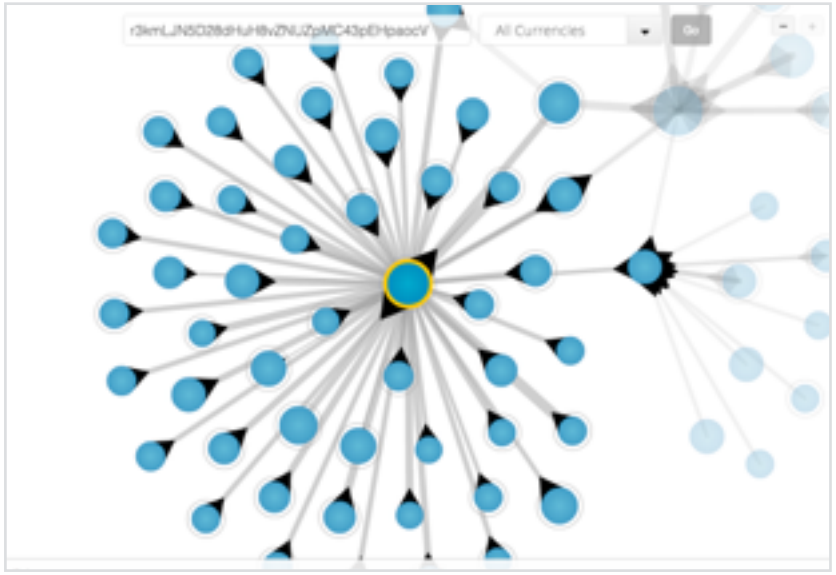
Attacks on privacy of Ripple links & transactions

PURDUE UNIVERSITY

Transaction Details

Account	Destination	Amount
rwvctTPLKZqK59f1fXpDkQ…	rMnVZ9maUWp5cAvmqBECZM…	300/XRP
rLSBpSquSHKbbfvcKt1c54…	rKoDt7VL83AKJZewLxVZEs…	75/XRP
r428G9fSSmD45YmnDra16B…	rBeToNo4AwHaNbRX2n4BNC…	0.0693402709148/CCK/rB…
rhD759dbJMrzMNL4QbvQe9…	r95pWKA1K55fy7EJWrqJ9b…	300/XRP
r42WJGvV9MJa4t5QcF8Cnx…	rBeToNo4AwHaNbRX2n4BNC…	0.0821058028231/CCK/rB…
rUnr1p7xkuSBxyAqHEopZ5…	r3H4rynDShFMRKWuJcadLY…	1129.916679154465/EUR/…
rw7UfGvzCeZwJxxUEeZHLG…	rBwgTdzzMHnouLk5DJD3xd…	100/XRP
rpVVzfSTUJX9CrKBS52Z5W…	rDCgaaSBAWYfsxUYhCk1n2…	999.99/XRP

Credit Graph



Ripple provides pseudonymity to its users by employing public-key hashes as identities

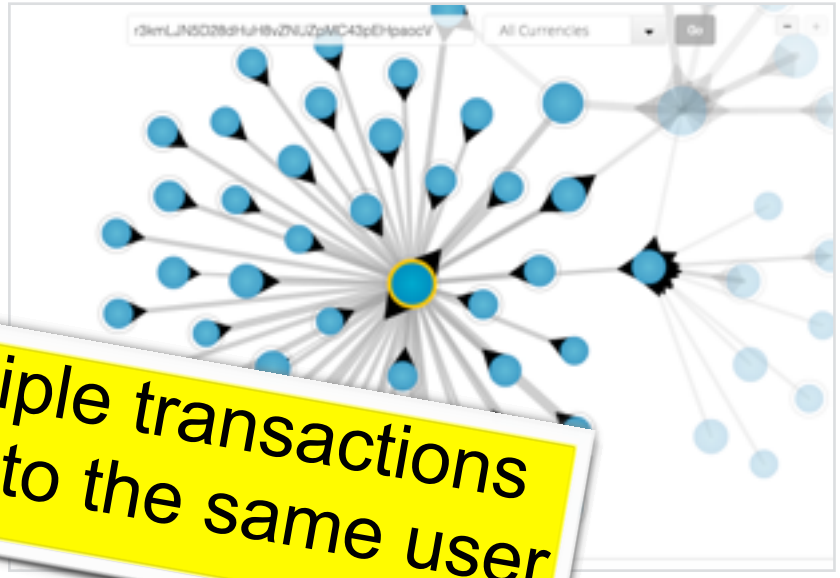
Attacks on privacy of Ripple links & transactions

PURDUE UNIVERSITY

Transaction Details

Account	Destination	Amount
rwvctTPLKZqK59f1fXpDkQ…	rMnVZ9maUWp5cAvmqBECZM…	300/XRP
rLSBpSquSHKbbfvcKt1c54…	rKoDt7VL83AKJZewLxVZEs…	75/XRP
r428G9fSSmD4…	rBeToNo4AwHaNbRX2n4BNC…	0.0693402709148/CCK/rB…
rhD759dbJMr…		300/XRP
r42WJGvV9MJ…		…8231/CCK/rB…
rUnr1p7xku…		
rw7UfGvzC…		
rpVVzfSTU…		

Credit Graph



It is possible to link multiple transactions and identities belonging to the same user

Ripple provides pseudonymity to its users by employing public-key hashes as identities

Is privacy a real problem in Ripple?

Privacy Attacks: Innocent until Proven Guilty

Is privacy a real problem in Ripple?

Privacy Attacks: Innocent until Proven Guilty

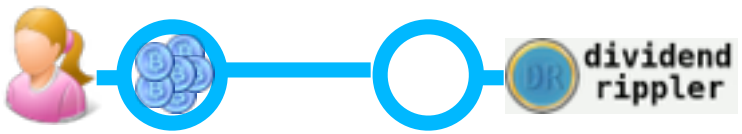
P. Moreno-Sanchez, M. B. Zafar, A. Kate:
Linking Wallets and Deanonymizing Transactions in the Ripple Network.
Privacy Enhancing Technologies Symposium (PETS) 2016.

Ripple Forum Discussion:
www.xrpchat.com/topic/1721-linking-wallets-and-deanonymizing-transactions-in-ripple/

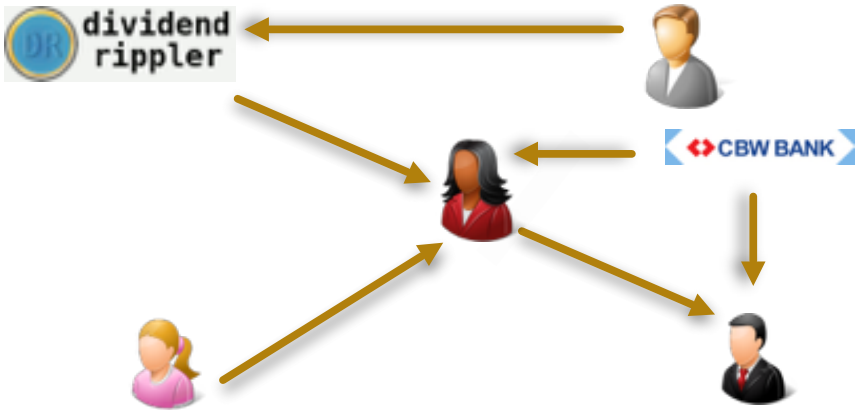
Heuristic 1: The Tale of two Public Logs

PURDUE UNIVERSITY

Bitcoin



Ripple

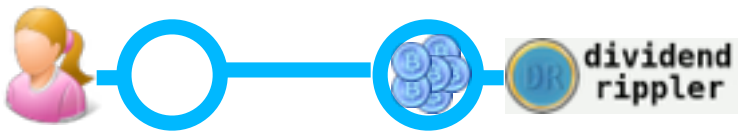


Heuristic 1: The Tale of two Public Logs

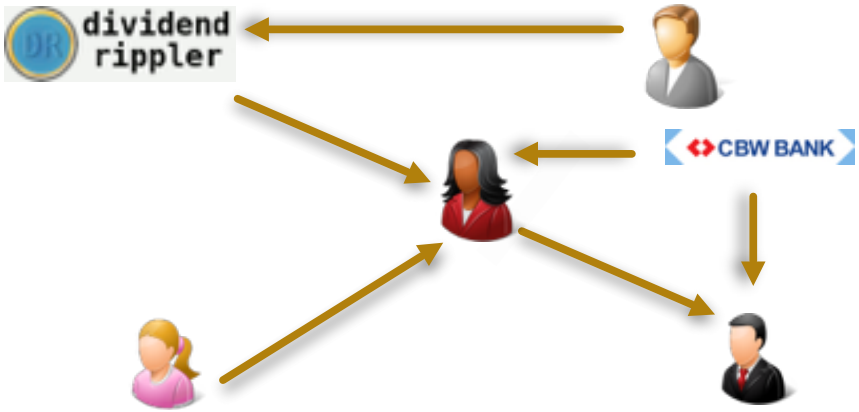
PURDUE UNIVERSITY

Bitcoin

Input	Output
Alice-Bitcoin: 6 BTC	DR-Bitcoin: 6 BTC
Alice	



Ripple

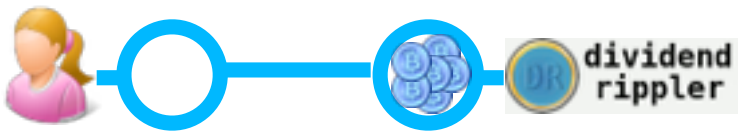


Heuristic 1: The Tale of two Public Logs

PURDUE UNIVERSITY

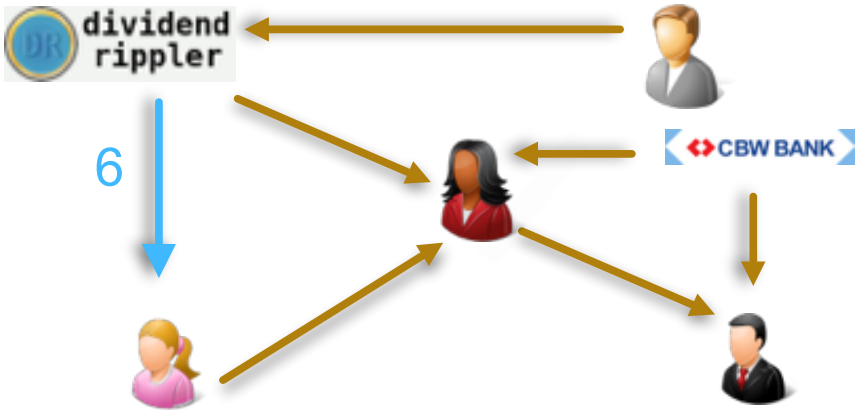
Bitcoin

Input	Output
Alice-Bitcoin: 6 BTC	DR-Bitcoin: 6 BTC
Alice	



Ripple

Sender	DR-Ripple
Receiver	Alice-Ripple
Value	6 BTC IOU
Path	Bob —> Alice
Bob	

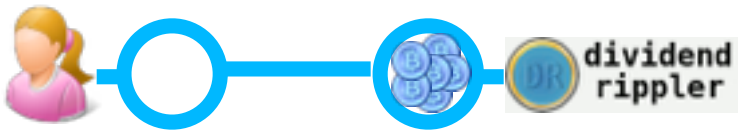


Heuristic 1: The Tale of two Public Logs

PURDUE UNIVERSITY

Bitcoin

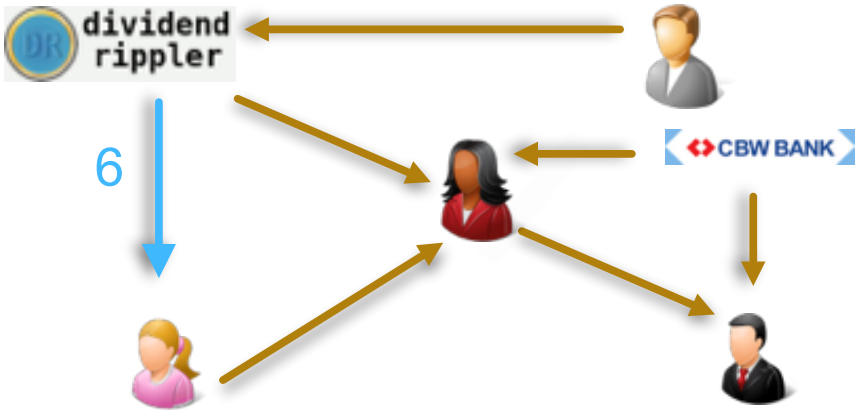
Input	Output
Alice-Bitcoin: 6 BTC	DR-Bitcoin: 6 BTC
Alice	



Alice-Bitcoin
Alice-Ripple

Ripple

Sender	DR-Ripple
Receiver	Alice-Ripple
Value	6 BTC IOU
Path	Bob —> Alice
Bob	



Heuristic 1: The Tale of two Public Logs

PURDUE UNIVERSITY

Bitcoin

Input	Output
Alice-Bitcoin: 6 BTC	DR-Bitcoin: 6 BTC
Alice	

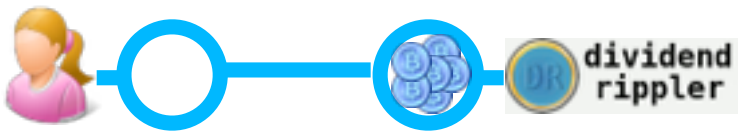
Alice-Bitcoin
Alice-Ripple

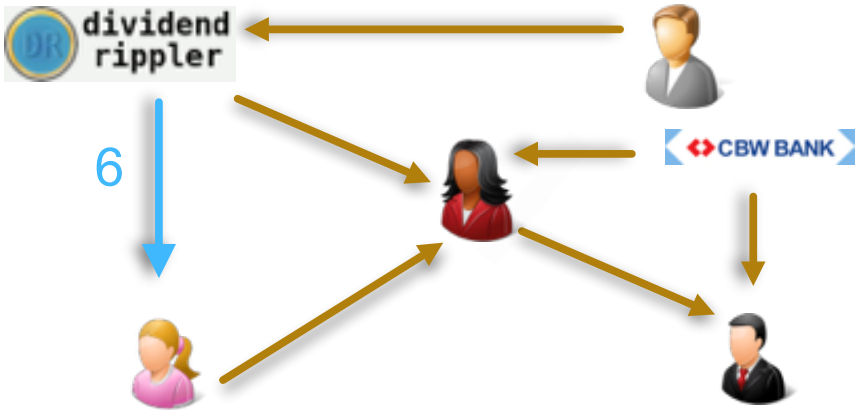
dividend rippler

DR-Bitcoin
DR-Ripple

Ripple

Sender	DR-Ripple
Receiver	Alice-Ripple
Value	6 BTC IOU
Path	Bob —> Alice
Bob	





Heuristic 1: The Tale of two Public Logs

PURDUE UNIVERSITY

Bitcoin

Input	Output
Alice-Bitcoin: 6 BTC	DR-Bitcoin: 6 BTC
Alice	

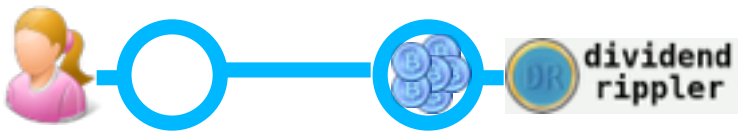
Alice-Bitcoin
Alice-Ripple

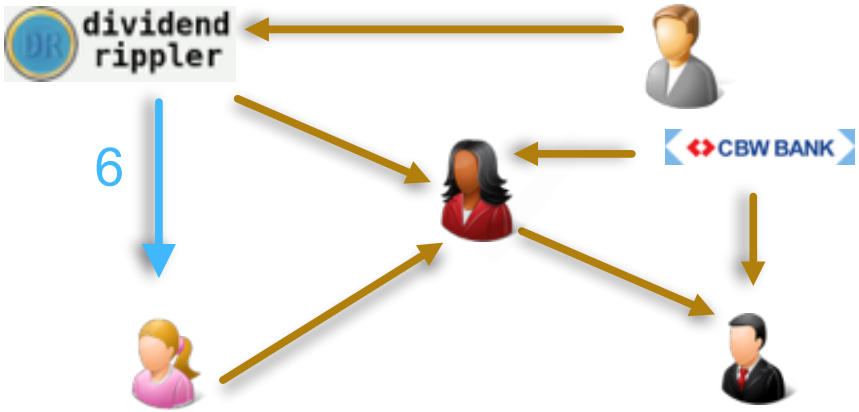
dividend rippler

DR-Bitcoin
DR-Ripple

Ripple

Sender	DR-Ripple
Receiver	Alice-Ripple
Value	6 BTC IOU
Path	Bob —> Alice
Bob	





- How to link these two events?

Heuristic 1: The Tale of two Public Logs

PURDUE UNIVERSITY

- Some gateways/exchanges keep public logs of their businesses

Recently Issued

timestamp	recipient		amount	status
2016-01-19 21:38	rBxdQqyJqxJV...	BTC	0.0020	done
2015-10-30 08:09	randomHTp7bl...	BTC	4.9990	done
2015-10-29 22:30	randomHTp7bl...	BTC	2.0000	done
2015-10-26 01:18	ramEbQX5Y7Jw...	LTC	1.7132	done
2015-10-25 16:36	rUgCBSD6SSox...	BTC	0.0010	done

Recently Redeemed

timestamp	recipient		amount	status
2016-02-16 16:41	1DmjJWLHKKPV...	BTC	0.2000	done
2016-02-08 08:36	raMn8PEs3TvM...	XRP	20.0000	done
2016-02-05 14:46	rJQFhLdAFaTB...	XRP	22.0000	done
2016-02-05 14:02	rJQFhLdAFaTB...	XRP	0.0000	processing
2016-01-30 08:39	LMYam6Akq5E3...	LTC	1.0000	done

- This interlog linkability attack possible without public log
  - timestamps and transaction amounts

Heuristic 2: Hot-Cold Wallets

€ 100,000

Heuristic 2: Hot-Cold Wallets

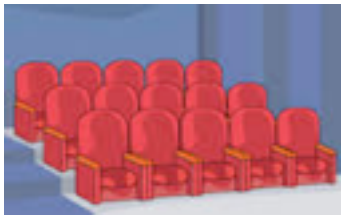
€ 100,~~000~~

Heuristic 2: Hot-Cold Wallets

€ 40

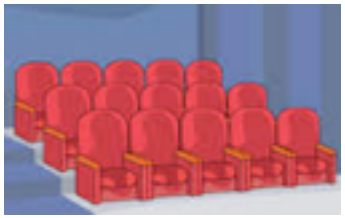
Heuristic 2: Hot-Cold Wallets

€ 20



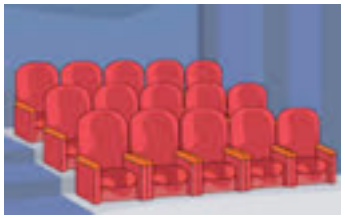
Heuristic 2: Hot-Cold Wallets

€ 20



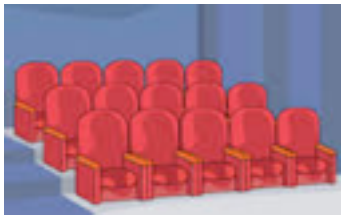
Heuristic 2: Hot-Cold Wallets

€ 150

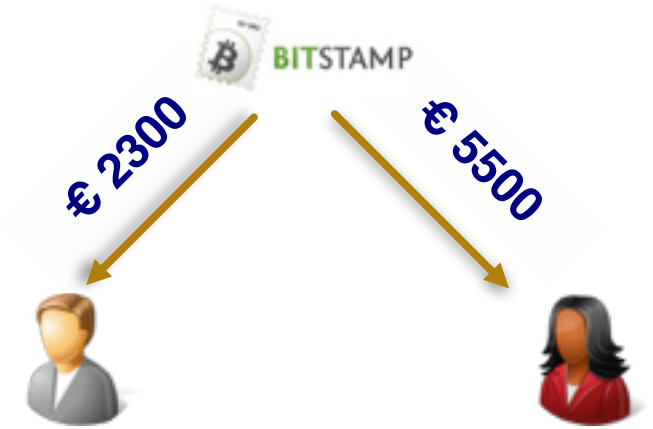


Heuristic 2: Hot-Cold Wallets

€ 150

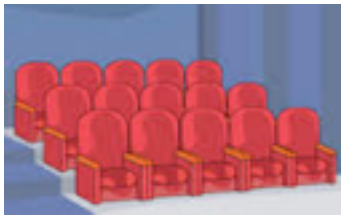


Ripple Users

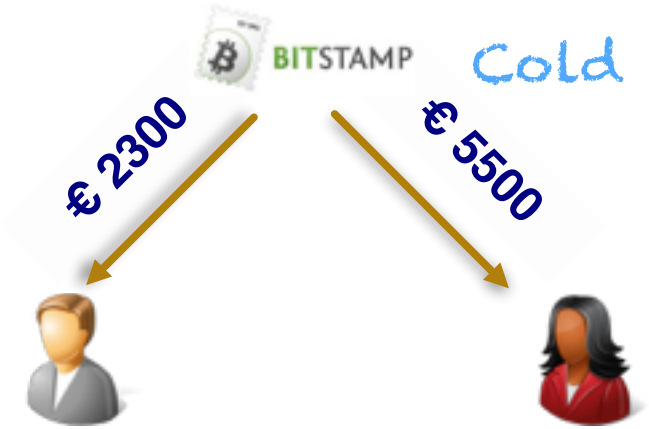


Heuristic 2: Hot-Cold Wallets

€ 150

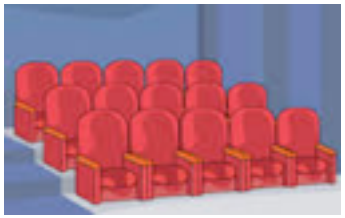


Ripple Users

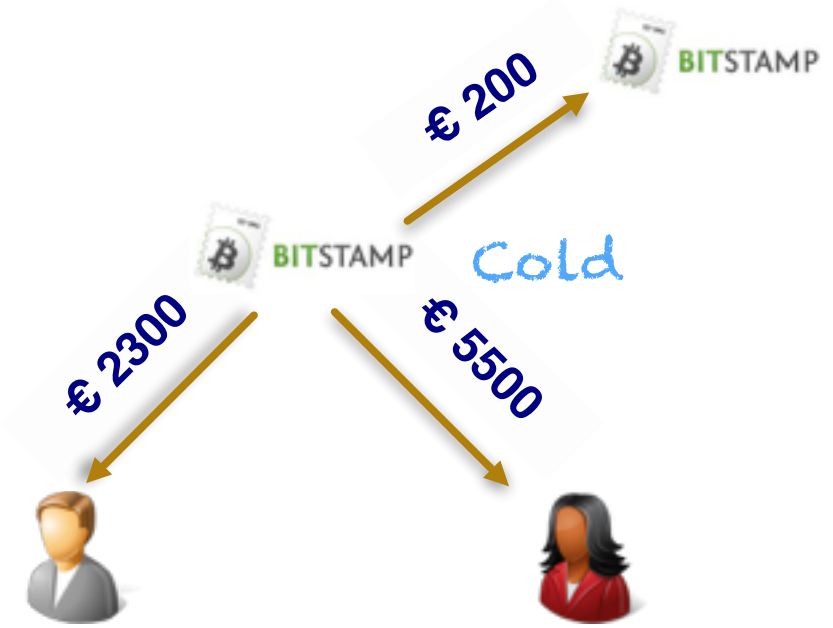


Heuristic 2: Hot-Cold Wallets

€ 150

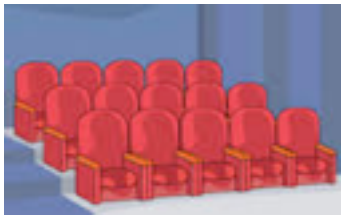


Ripple Users

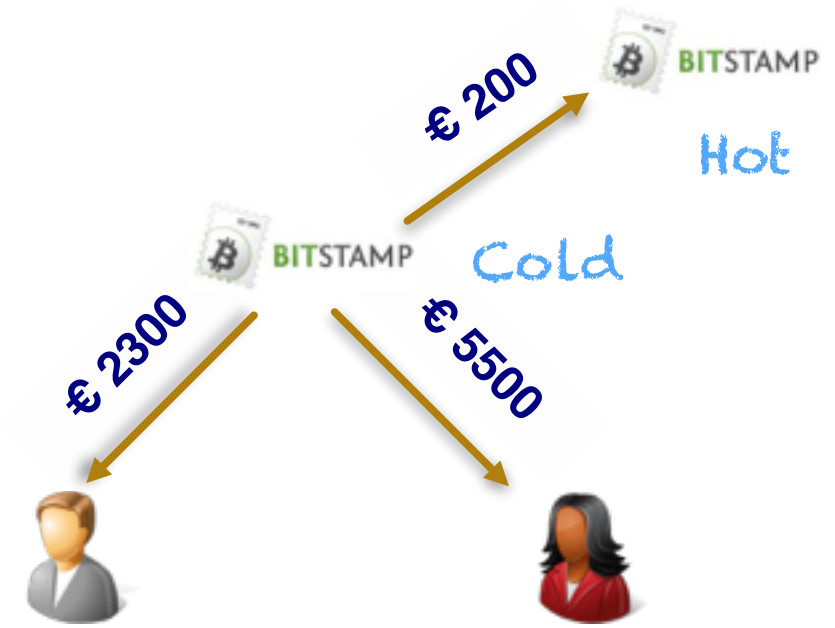


Heuristic 2: Hot-Cold Wallets

€ 150

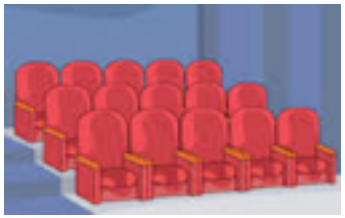


Ripple Users

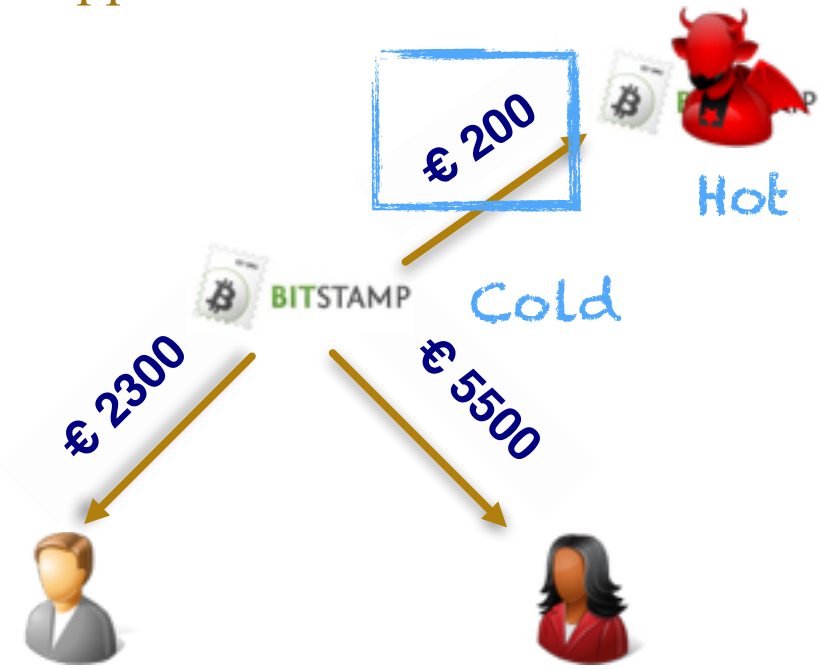


Heuristic 2: Hot-Cold Wallets

€ 150

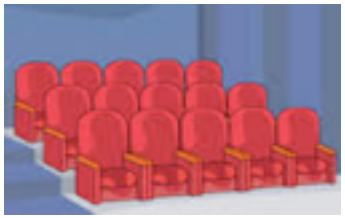


Ripple Users

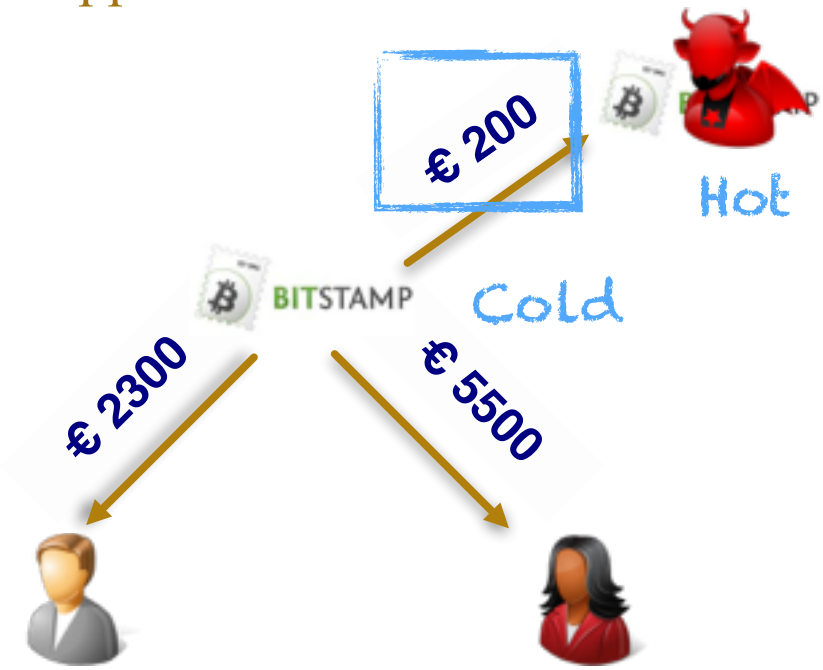


Heuristic 2: Hot-Cold Wallets

€ 150



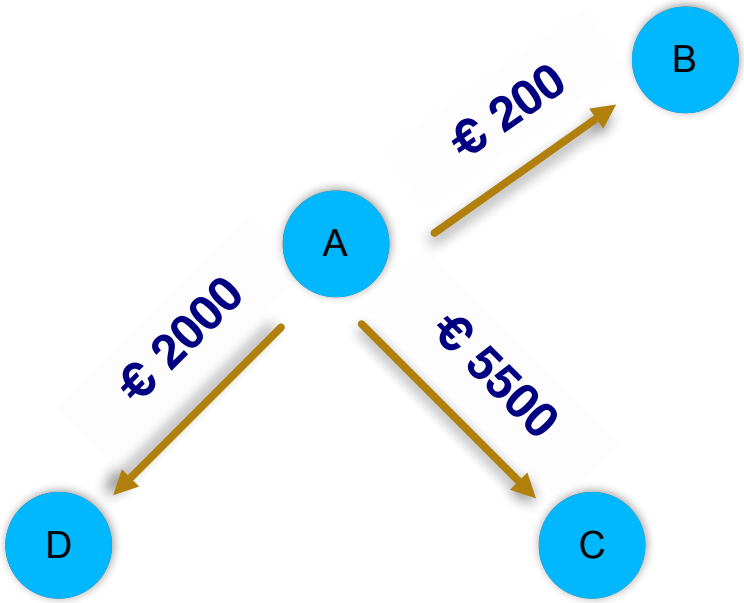
Ripple Users



Link hot and cold wallets!!

Heuristic 2: Hot-Cold Wallets

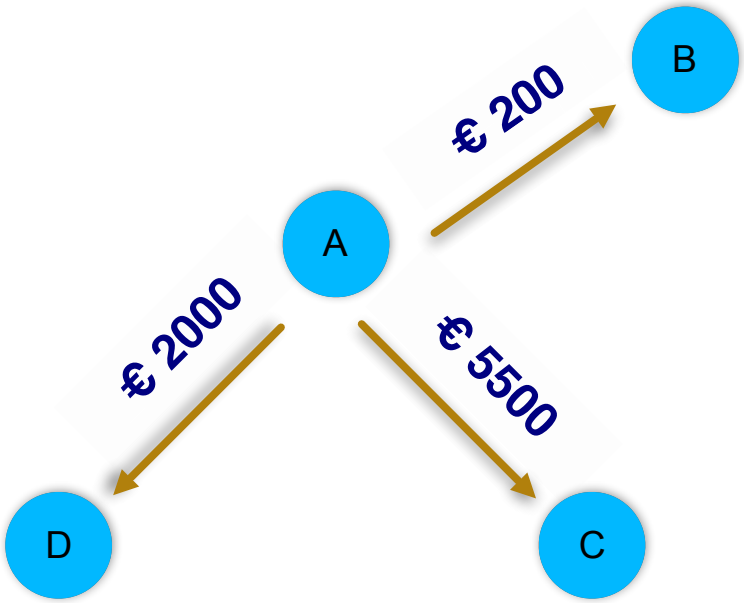
- Correlation between network topology and transactions



Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

Heuristic 2: Hot-Cold Wallets

- Correlation between network topology and transactions

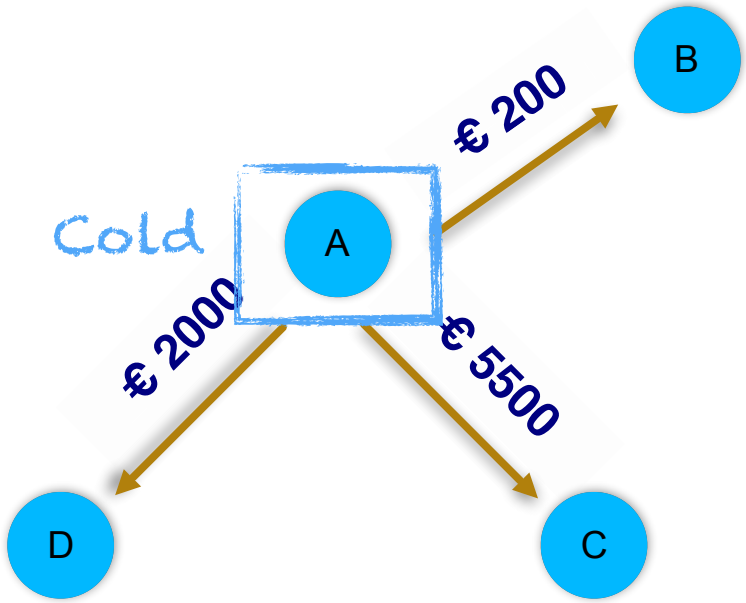


Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

- Cold wallet only issues credit

Heuristic 2: Hot-Cold Wallets

- Correlation between network topology and transactions

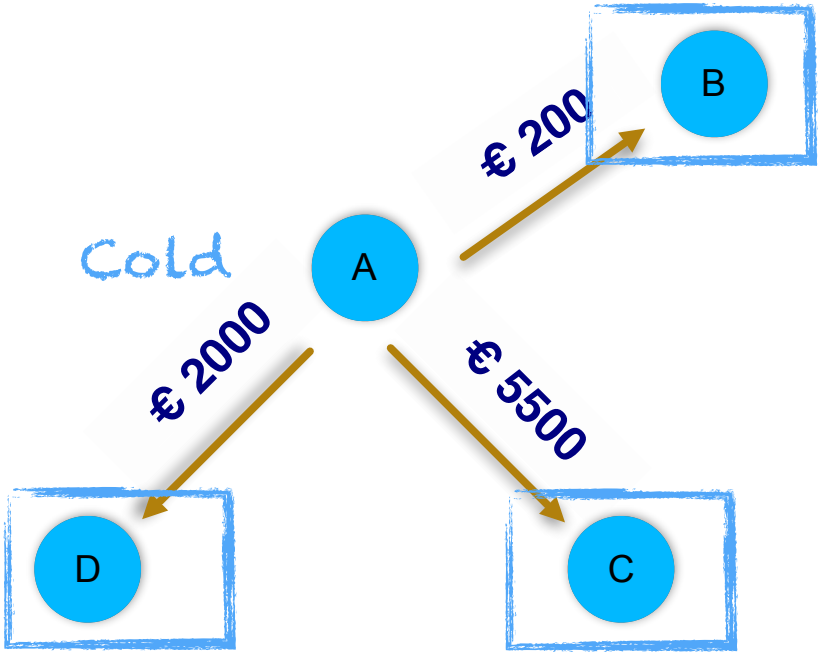


Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

- Cold wallet only issues credit

Heuristic 2: Hot-Cold Wallets

- Correlation between network topology and transactions

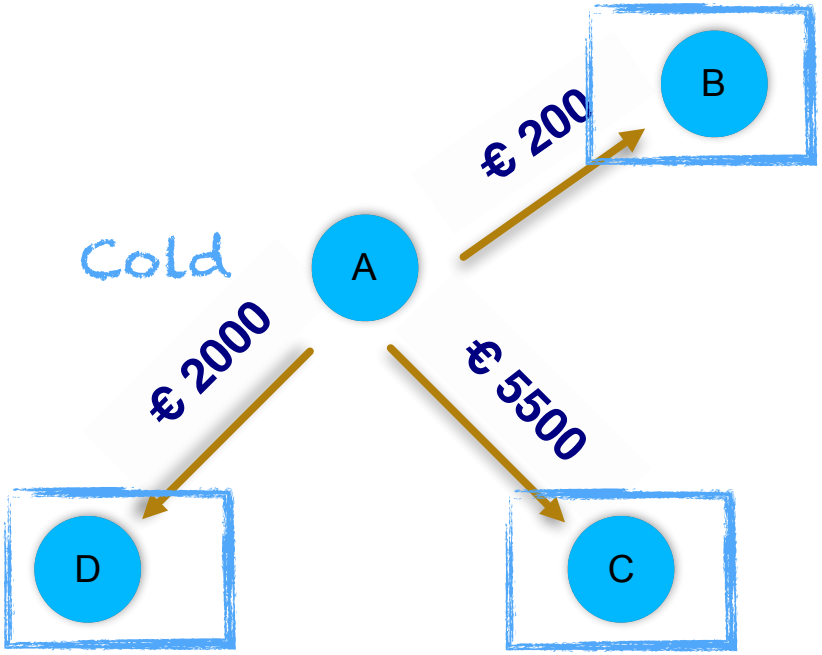


Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

- Cold wallet only issues credit

Heuristic 2: Hot-Cold Wallets

- Correlation between network topology and transactions

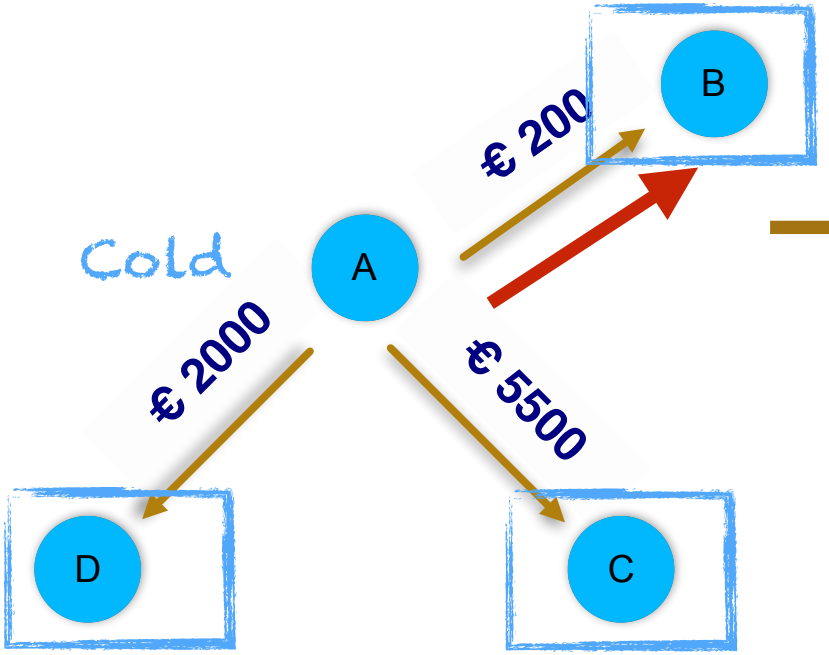


Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

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

Heuristic 2: Hot-Cold Wallets

- Correlation between network topology and transactions

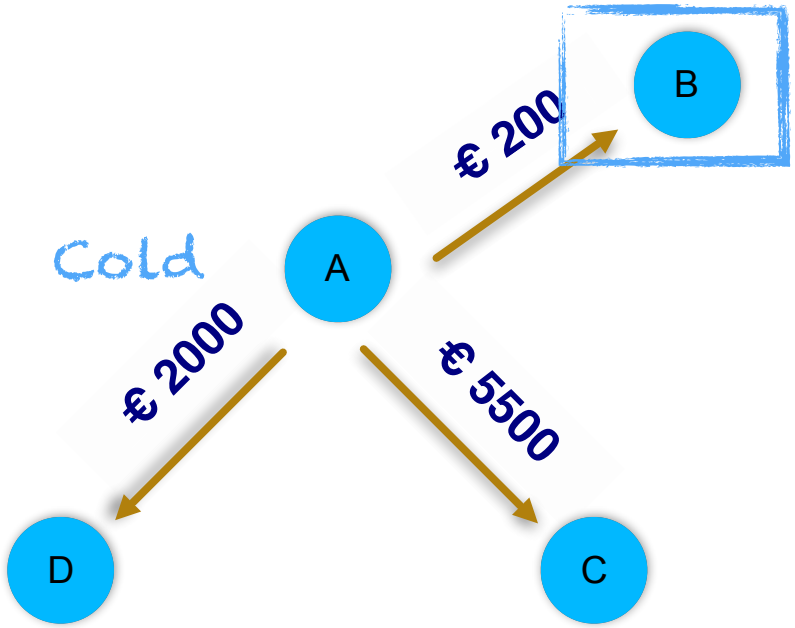


Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

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

Heuristic 2: Hot-Cold Wallets

- Correlation between network topology and transactions

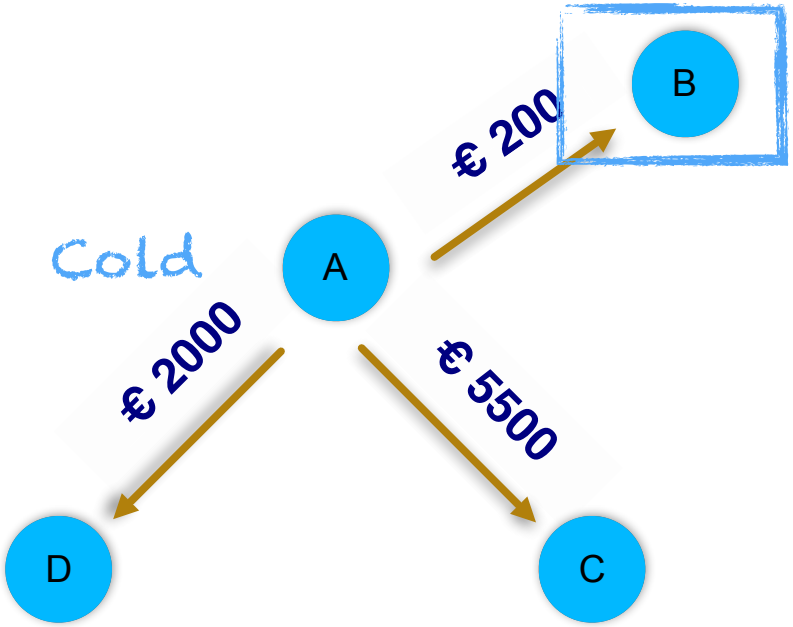


Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

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

Heuristic 2: Hot-Cold Wallets

- Correlation between network topology and transactions

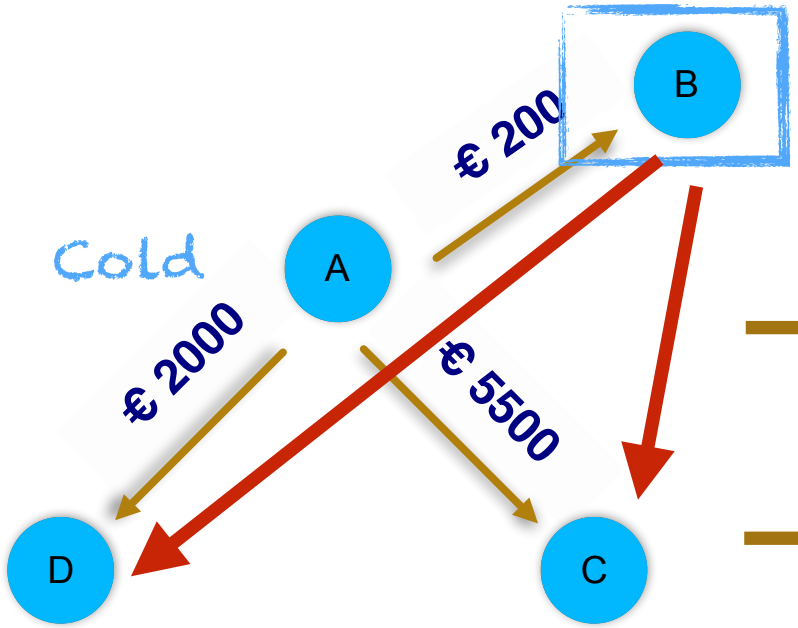


Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

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

Heuristic 2: Hot-Cold Wallets

- Correlation between network topology and transactions

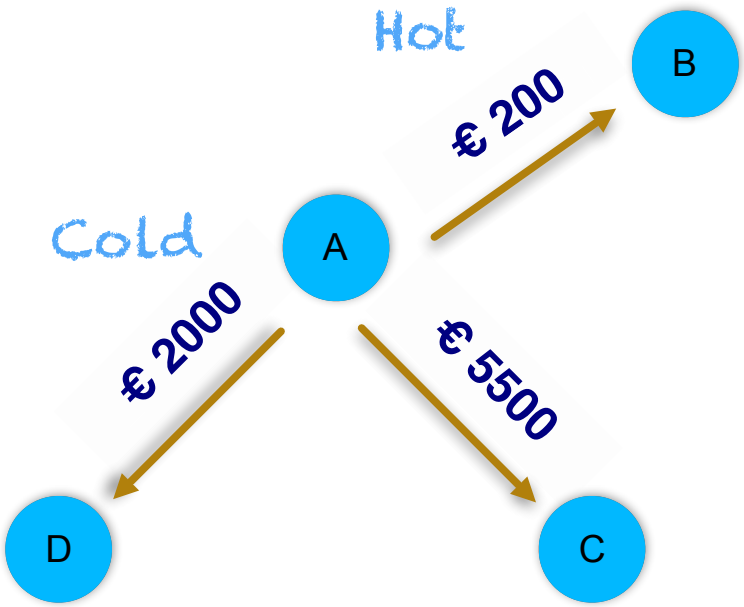


Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

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

Heuristic 2: Hot-Cold Wallets

- Correlation between network topology and transactions



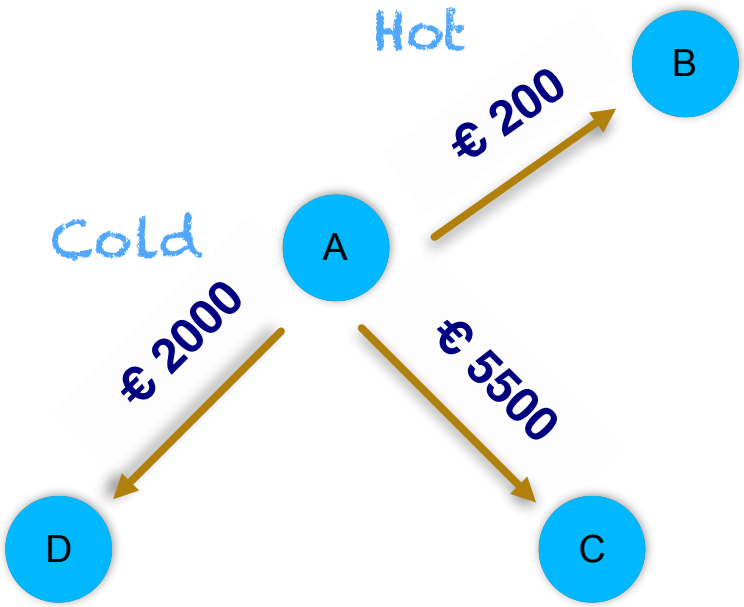
Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

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

Heuristic 2: Hot-Cold Wallets

PURDUE UNIVERSITY

- Correlation between network topology and transactions

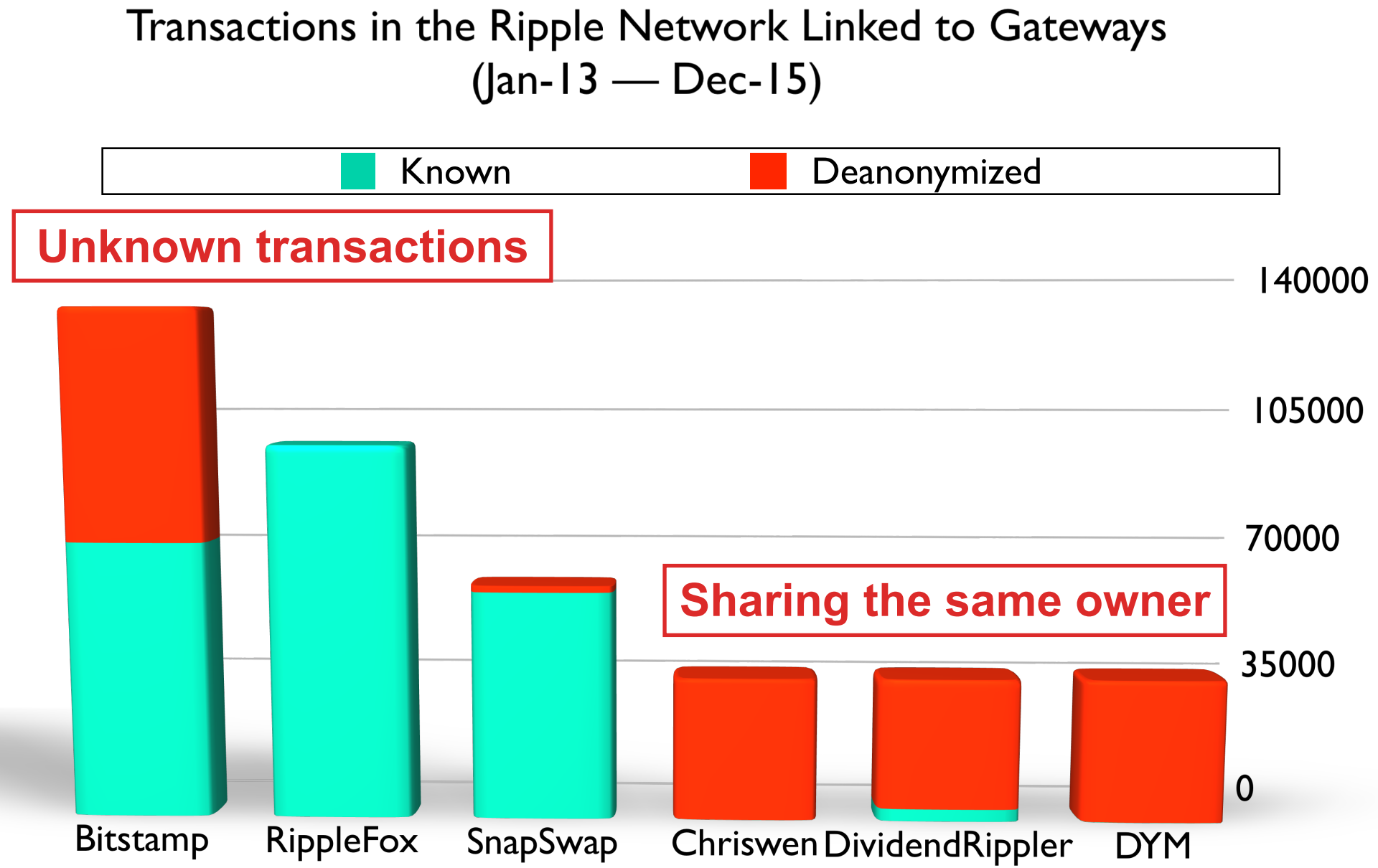


Sender	Receiver	Amount
A	B	€275
B	D	€30
D	C	€10
B	C	€45

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

A, B belong to the same user

Deanonymization of several gateways



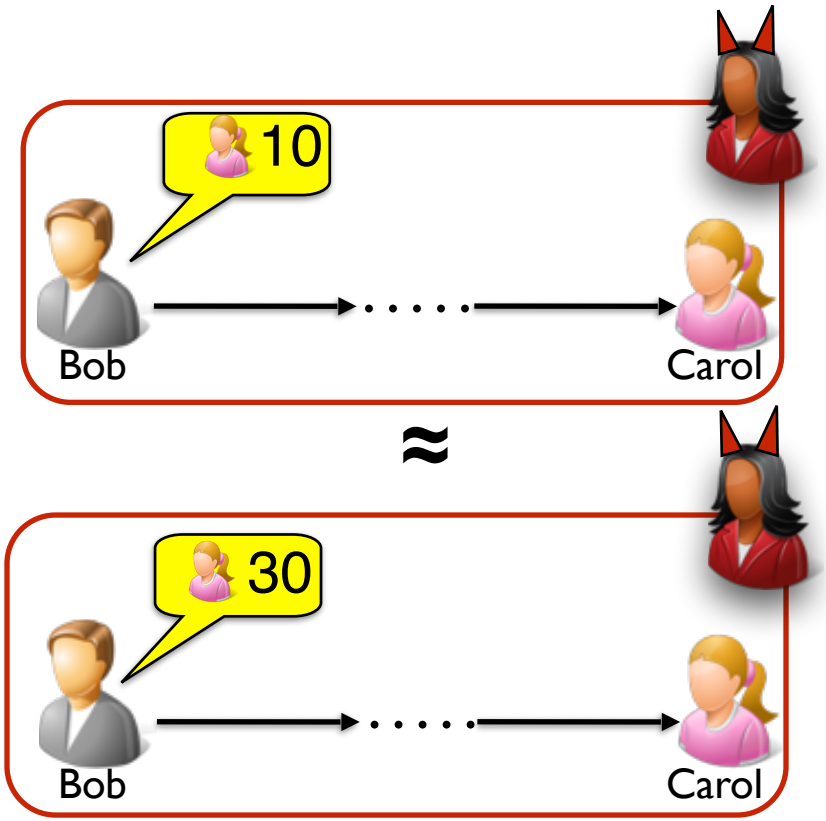
Towards privacy-preserving transactions credit networks

P. Moreno-Sanchez, A. Kate, M. Maffei, and K. Pecina:
Privacy Preserving Payments in Credit Networks.
NDSS 2015

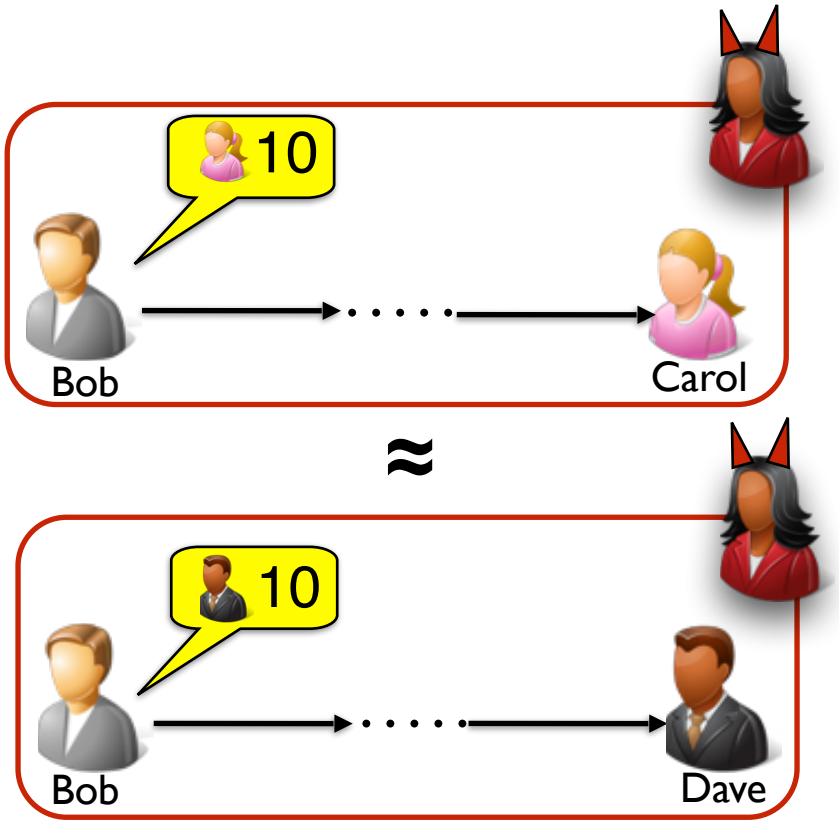
Defining privacy for a credit network

PURDUE UNIVERSITY

Transaction value privacy



Transaction receiver privacy

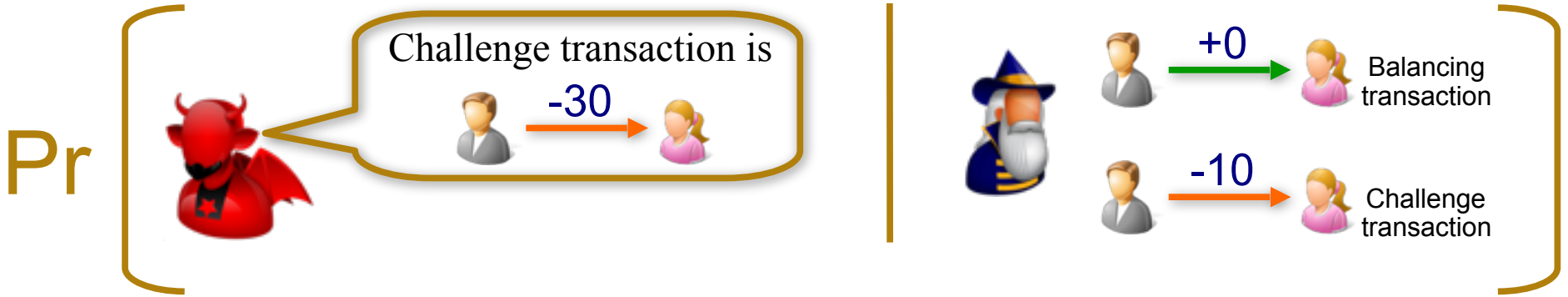


Transaction sender privacy can be defined similarly

Transaction Value Privacy: Definition (II)

- A credit network satisfies value privacy if:

≈



Towards credit network privacy

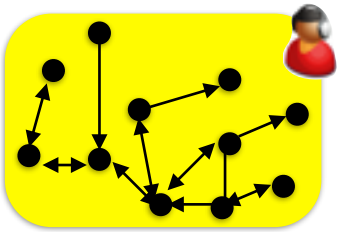
Towards credit network privacy

- A decentralized or centralized architecture?

Towards credit network privacy

PURDUE UNIVERSITY

- A decentralized or centralized architecture?
- Centralized setting: the network is maintained by a server
  - The service provider can trivially break the privacy
    - The routing computation can be performed privately, but any modifications to the edges not
    - Use of pseudonyms and anonymous channels (e.g, Tor) is not sufficient
  - In our NDSS'15 paper, we resolve this issue using minimally trusted hardware and oblivious algorithms

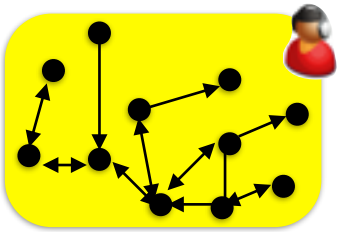


Towards credit network privacy

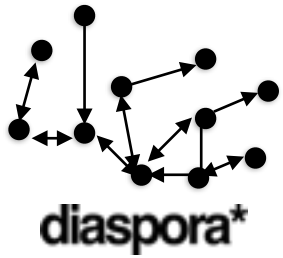
PURDUE UNIVERSITY

- A decentralized or centralized architecture?

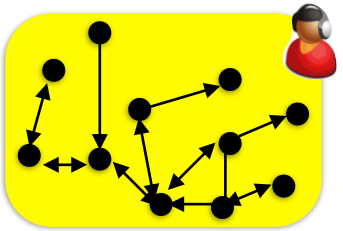
- Centralized setting: the network is maintained by a server
  - The service provider can trivially break the privacy
    - The routing computation can be performed privately, but any modifications to the edges not
    - Use of pseudonyms and anonymous channels (e.g, Tor) is not sufficient
  - In our NDSS'15 paper, we resolve this issue using minimally trusted hardware and oblivious algorithms



- Decentralized setting: edges are maintained locally
  - A transaction passing through a node requires its active involvement
  - We will consider this later during the talk



Towards credit network privacy



- Centralized setting
  - The network is maintained by a service provider

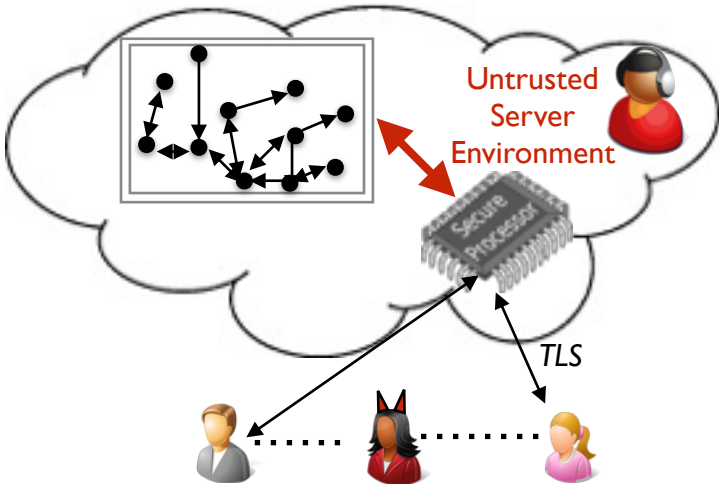
- Threat Model
  - The service provider is honest-but-curious
  - Some users are controlled by the service provider

- The service provider can trivially break the privacy
  - The routing computation can be performed privately, but any modifications to the edges cannot

- We resolve this feasibility issue using minimally trusted hardware

Our centralized approach: PrivPay

- Threat Model
  - The service provider is honest-but-curious
  - Some users are controlled by the service provider



- A service-side trusted hardware module maintains the network graph in the untrusted server memory
- Correctness of the hardware module can be verified using remote code attestation
- Encryption by itself prevents an attacker from learning the database entry but monitoring memory accesses is still possible
- We develop oblivious algorithms for routing to solve this problem

Routing: max-flow computation

PURDUE UNIVERSITY

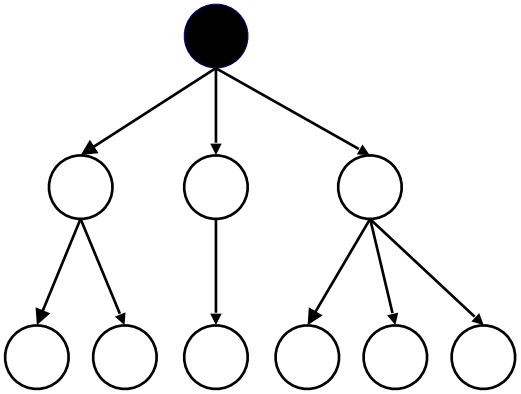
- Routing challenge:
  Known max-flow algorithms are not scalable: $O(V^3)$ or $O(V^2 \log(E))$
- We employ landmark routing:
  Calculate only a subset of all possible routes through intermediary nodes called landmarks [Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]

Routing: max-flow computation

PURDUE UNIVERSITY

- Routing challenge:
  Known max-flow algorithms are not scalable: $O(V^3)$ or $O(V^2 \log(E))$
- We employ landmark routing:
  Calculate only a subset of all possible routes through intermediary nodes called landmarks

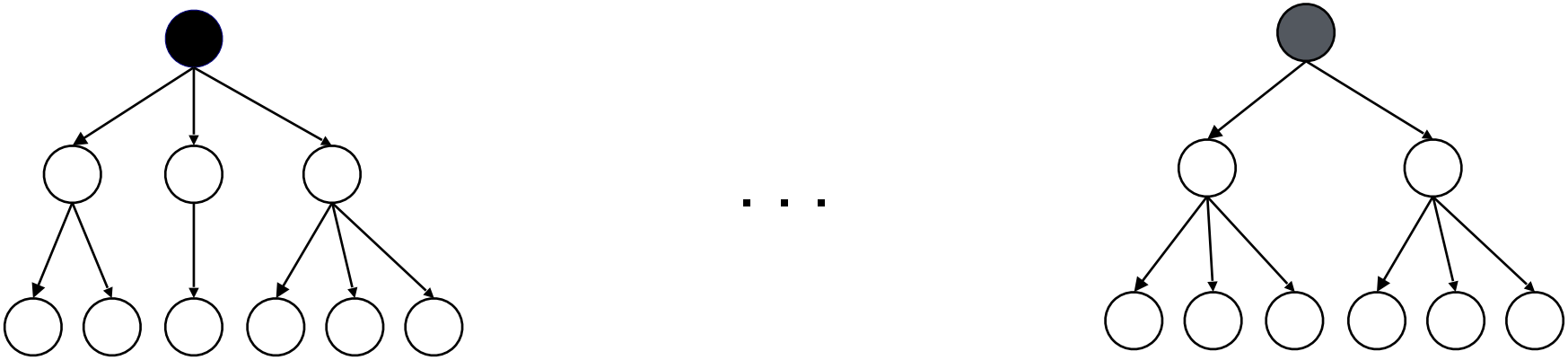
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



Routing: max-flow computation

- Routing challenge:
  Known max-flow algorithms are not scalable: $O(V^3)$ or $O(V^2 \log(E))$
- We employ landmark routing:
  Calculate only a subset of all possible routes through intermediary nodes called landmarks

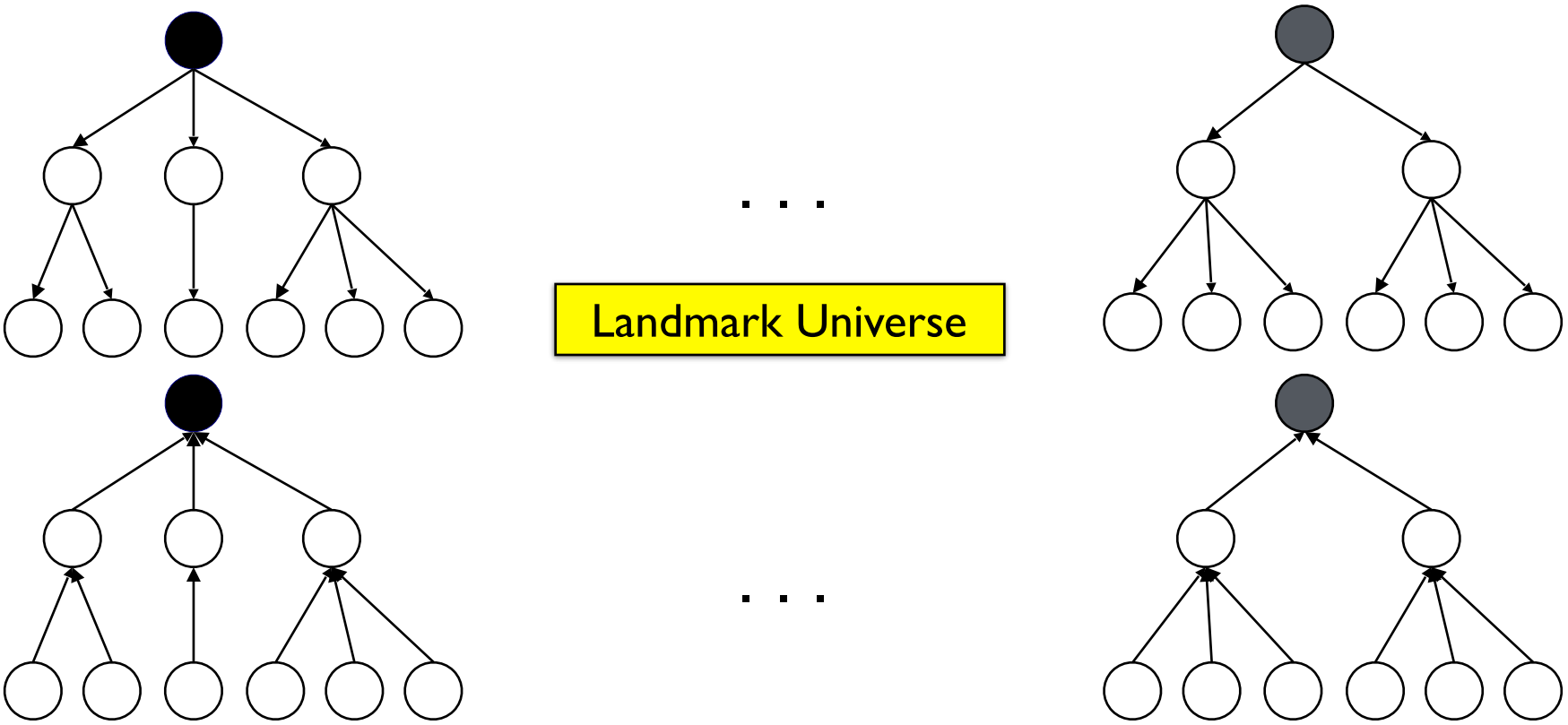
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



Routing: max-flow computation

- Routing challenge:
  Known max-flow algorithms are not scalable: $O(V^3)$ or $O(V^2 \log(E))$
- We employ landmark routing:
  Calculate only a subset of all possible routes through intermediary nodes called landmarks

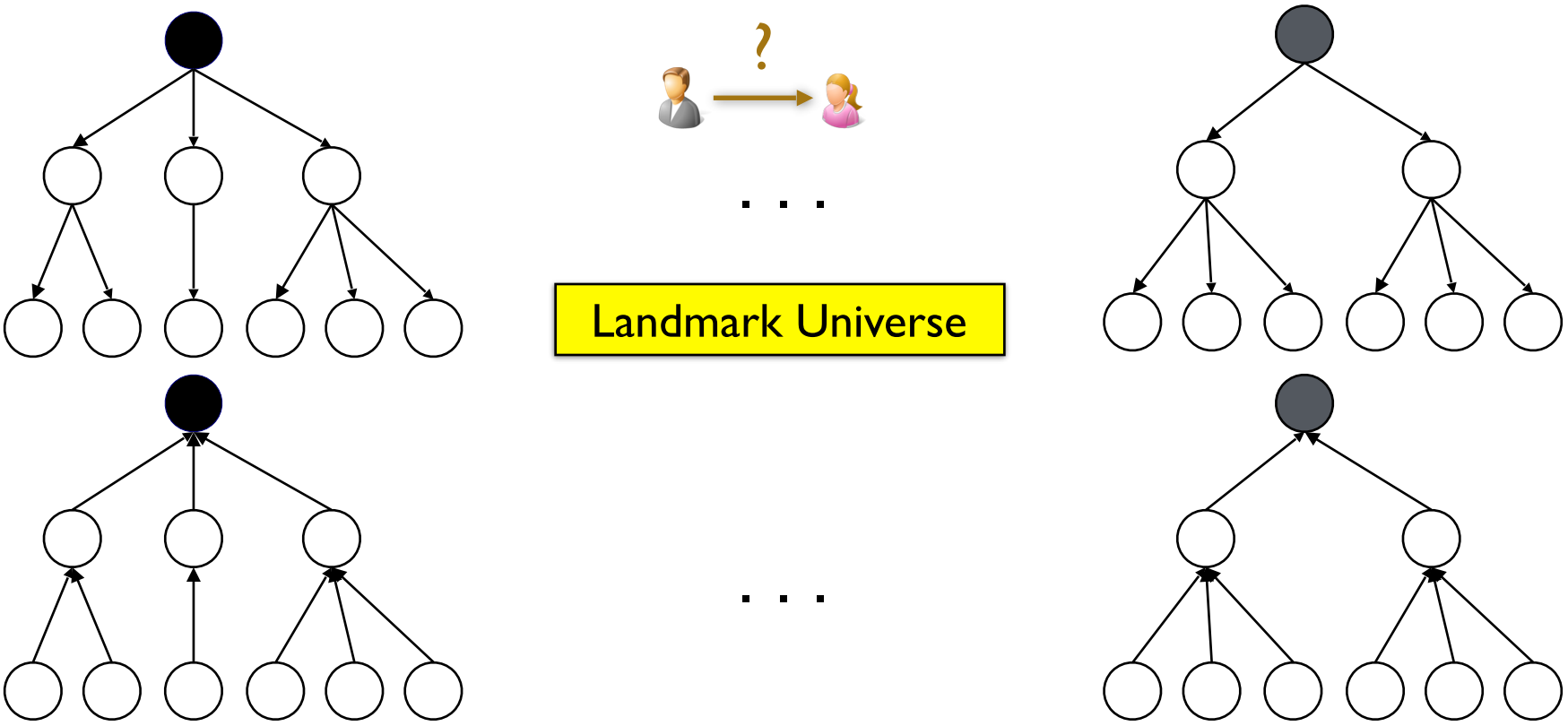
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



Routing: max-flow computation

- Routing challenge:
  Known max-flow algorithms are not scalable: $O(V^3)$ or $O(V^2 \log(E))$
- We employ landmark routing:
  Calculate only a subset of all possible routes through intermediary nodes called landmarks

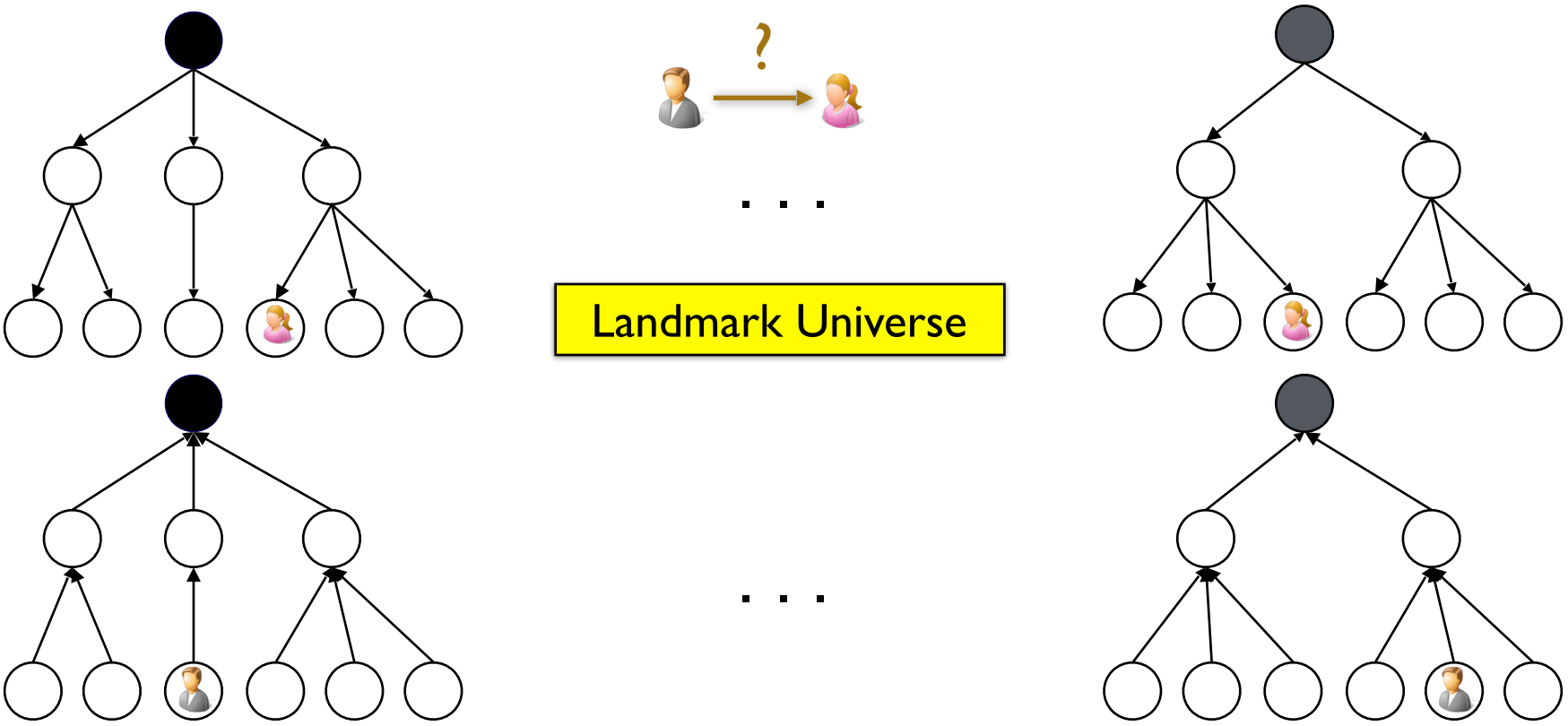
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



Routing: max-flow computation

- Routing challenge:
  Known max-flow algorithms are not scalable: $O(V^3)$ or $O(V^2 \log(E))$
- We employ landmark routing:
  Calculate only a subset of all possible routes through intermediary nodes called landmarks

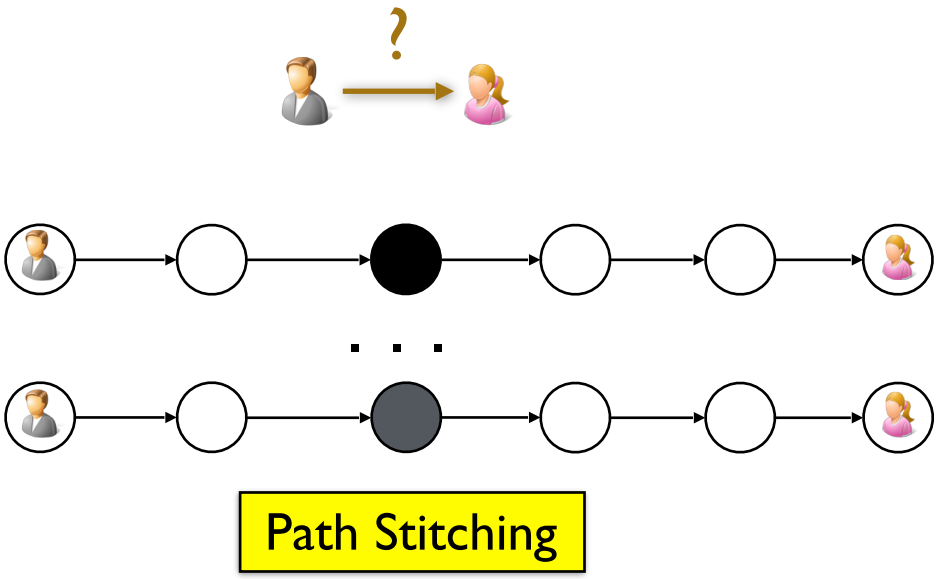
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



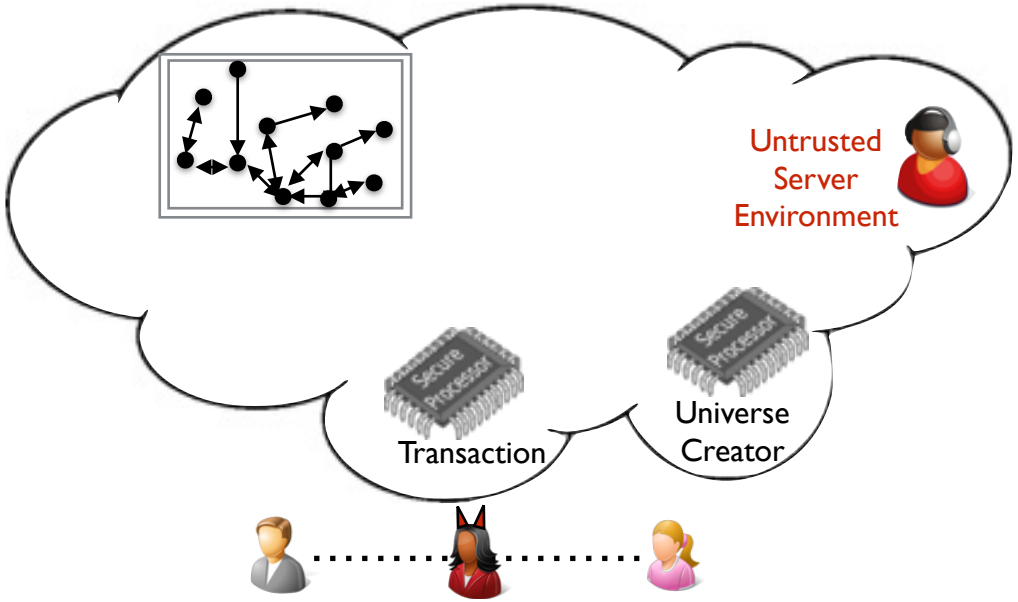
Routing: max-flow computation

- Routing challenge:
  Known max-flow algorithms are not scalable: $O(V^3)$ or $O(V^2 \log(E))$
- We employ landmark routing:
  Calculate only a subset of all possible routes through intermediary nodes called landmarks

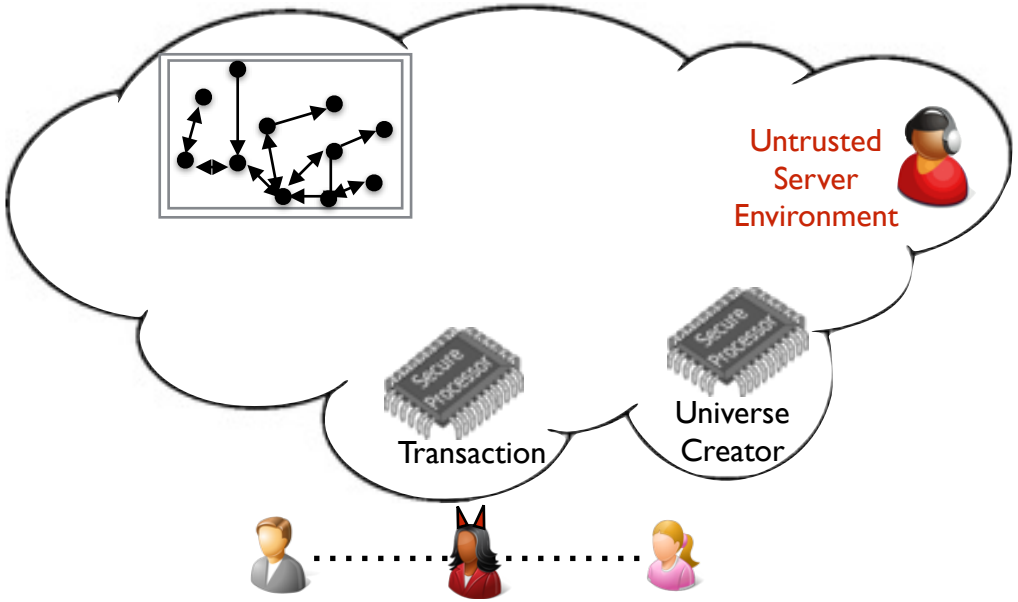
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



PrivPay architecture

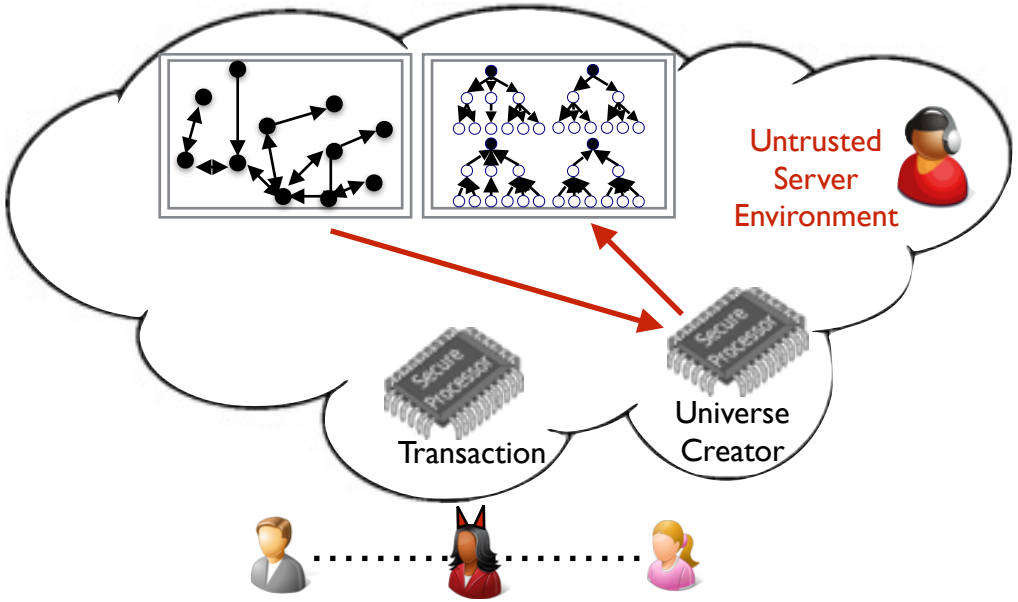


PrivPay architecture



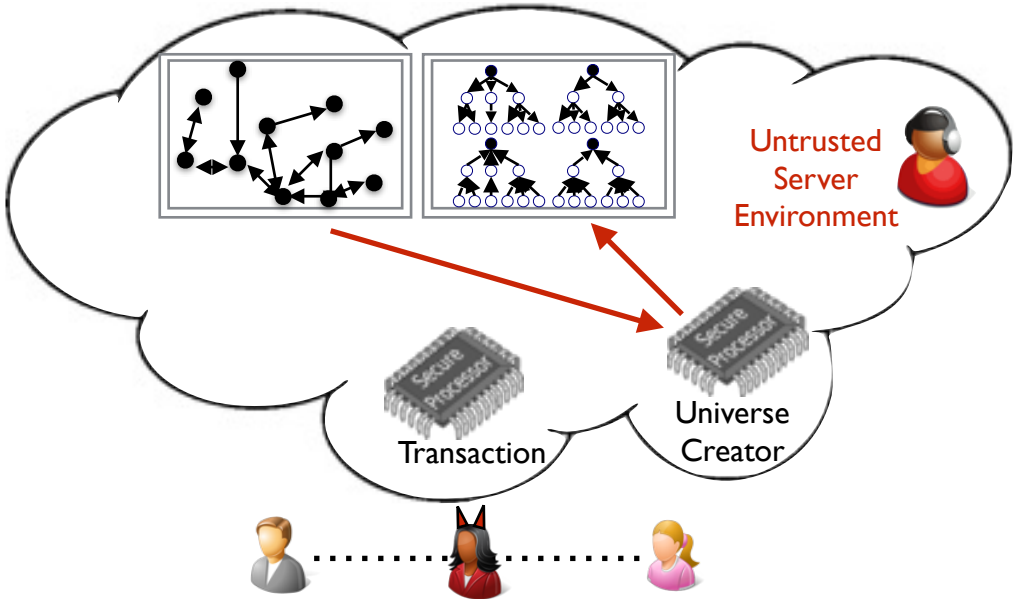
- Landmark universe creator module
  - Oblivious BFS computation for selected landmark nodes

PrivPay architecture



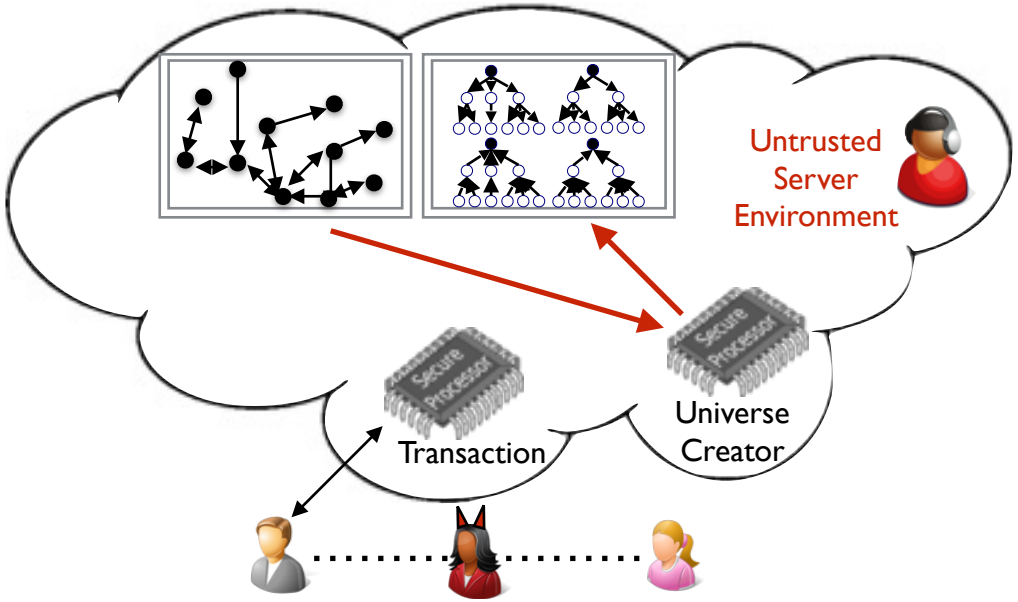
- Landmark universe creator module
  - Oblivious BFS computation for selected landmark nodes

PrivPay architecture



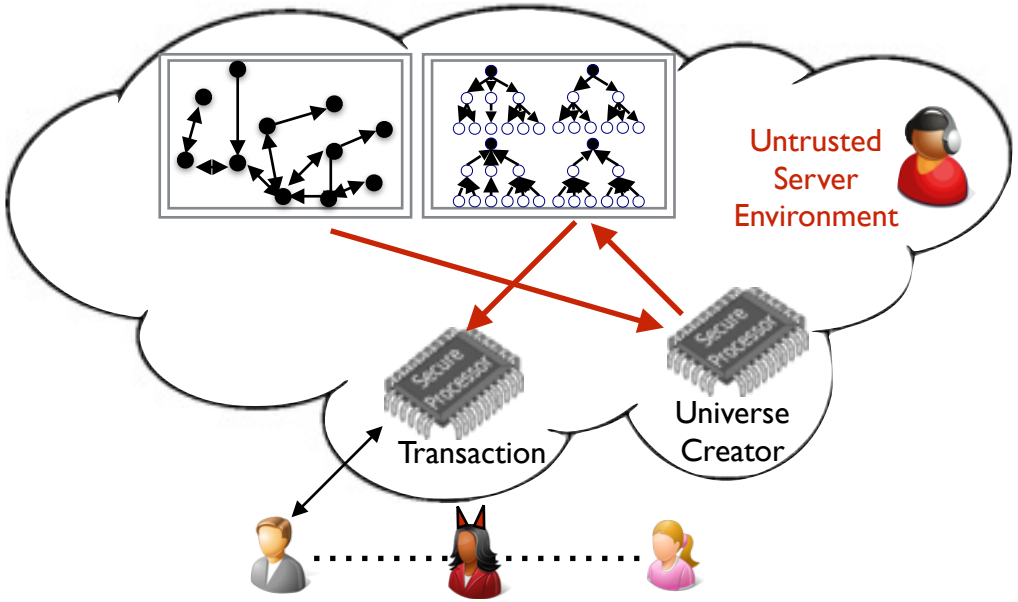
- Landmark universe creator module
  - Oblivious BFS computation for selected landmark nodes
- Transaction (path stitcher) module
  - Given a sender and a receiver, traverse the BFS trees in an oblivious manner for the overlapping landmark nodes

PrivPay architecture



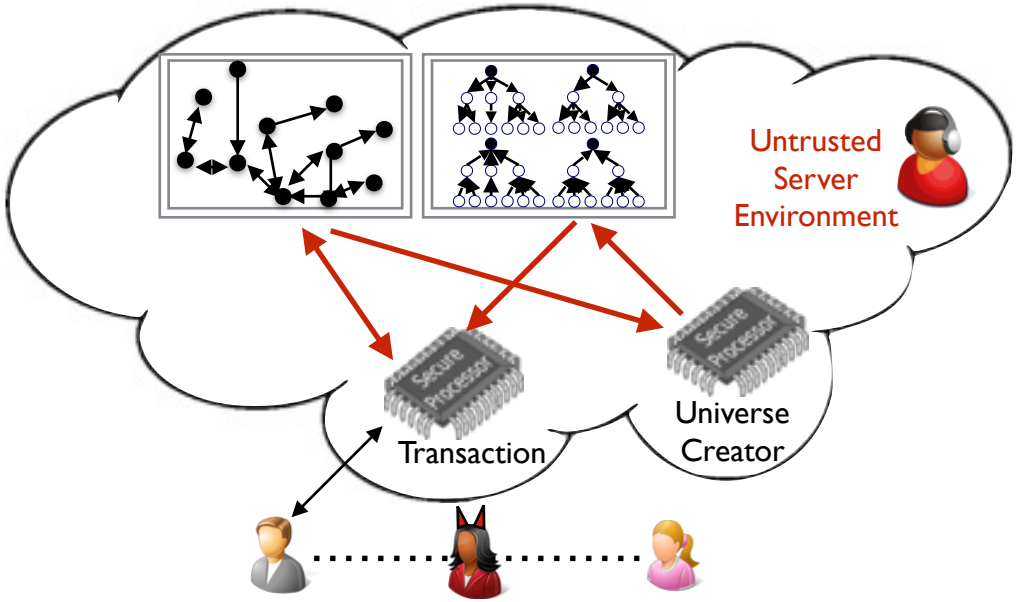
- Landmark universe creator module
  - Oblivious BFS computation for selected landmark nodes
- Transaction (path stitcher) module
  - Given a sender and a receiver, traverse the BFS trees in an oblivious manner for the overlapping landmark nodes
- Privacy properties are formally proven

PrivPay architecture



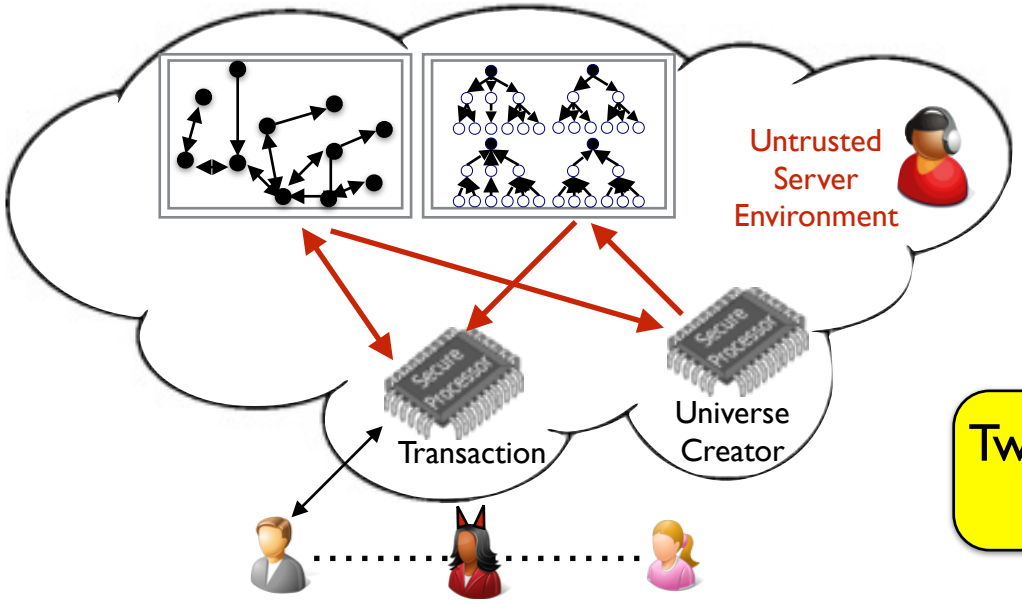
- Landmark universe creator module
  - Oblivious BFS computation for selected landmark nodes
- Transaction (path stitcher) module
  - Given a sender and a receiver, traverse the BFS trees in an oblivious manner for the overlapping landmark nodes
- Privacy properties are formally proven

PrivPay architecture



- Landmark universe creator module
  - Oblivious BFS computation for selected landmark nodes
- Transaction (path stitcher) module
  - Given a sender and a receiver, traverse the BFS trees in an oblivious manner for the overlapping landmark nodes
- Privacy properties are formally proven

PrivPay architecture



Two modules are not synchronized

- Landmark universe creator module
  - Oblivious BFS computation for selected landmark nodes
- Transaction (path stitcher) module
  - Given a sender and a receiver, traverse the BFS trees in an oblivious manner for the overlapping landmark nodes
- Privacy properties are formally proven

Applying PrivPay to the Ripple network

PURDUE UNIVERSITY

- We have implemented PrivPay as a C++ library
- We employed real-world Ripple transactions over a period of four months (Oct'13 – Jan'14)

Time in *msec*	Non-Private [Eurosys'12]	PrivPay
Payment	0.078	1510
Change link	0.005	95
Oblivious BFS	50	22000
Coverage	97%	95%

Ripple takes 5 sec. to confirm a transaction

Background Process

No false positive, only false negative

PrivPay: Deployment Challenges

PURDUE UNIVERSITY

- Ripple is currently focusing on their business growth
  - The privacy concerns was secondary to them
  - Trusted hardware-based solutions require investment
    - Ripple is not ready for the challenge yet!
- Scalability of (background) Oblivious BFS algorithm as number of users have increased ten holds
  - the coverage will reduces
- Question: Can we find some solution that is compatible with the current Ripple architecture?
  - Yes! but with a caveat

PathShuffle

PURDUE UNIVERSITY

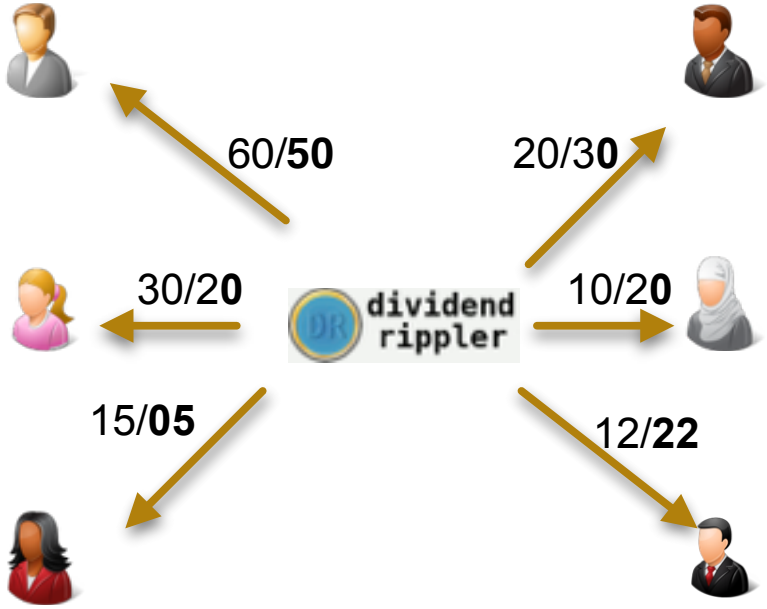
[In Submission]

PathShuffle

PURDUE UNIVERSITY

[In Submission]

- Idea: Perform several transactions simultaneously enables privacy-preserving transactions
  - Similar to Conjoin or CoinShuffle for Bitcoin

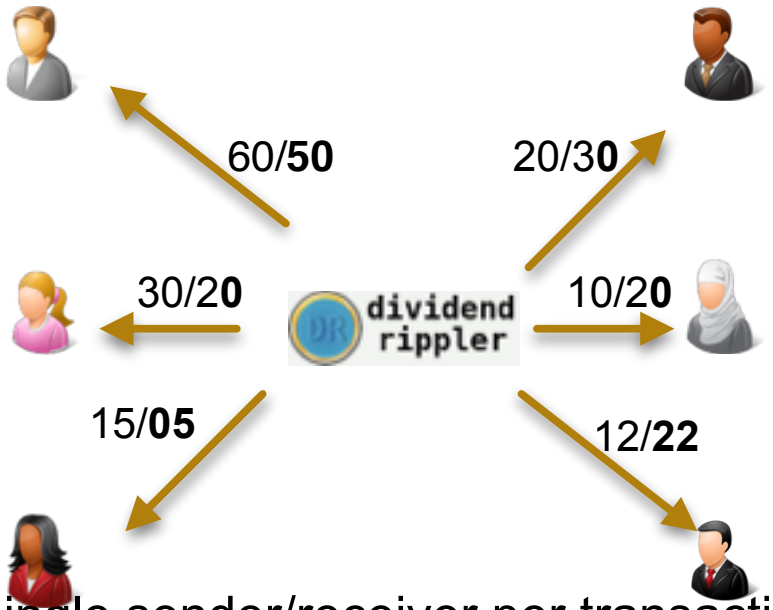


PathShuffle

PURDUE UNIVERSITY

[In Submission]

- Idea: Perform several transactions simultaneously enables privacy-preserving transactions
  - Similar to Conjoin or CoinShuffle for Bitcoin



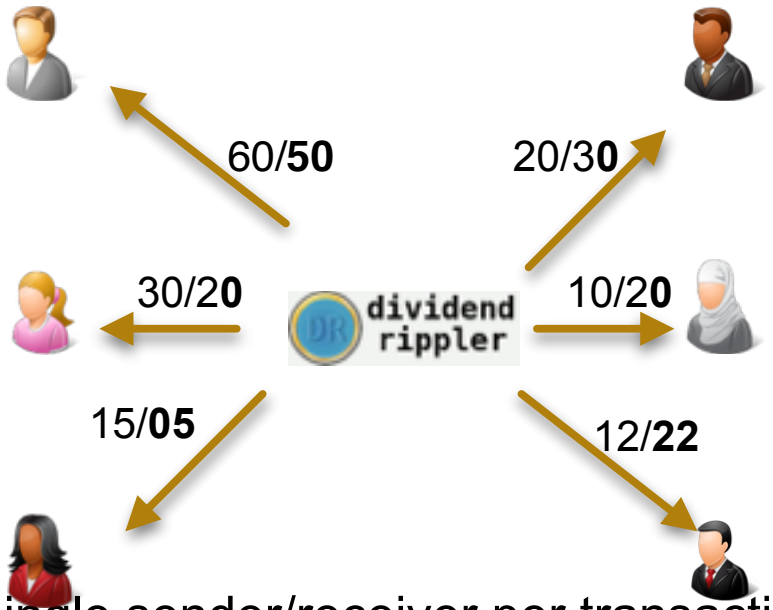
- Ripple only allows single sender/receiver per transaction
  - Employ threshold signature techniques overcome the problem
  - Pathjoin!

PathShuffle

PURDUE UNIVERSITY

[In Submission]

- Idea: Perform several transactions simultaneously enables privacy-preserving transactions
  - Similar to Conjoin or CoinShuffle for Bitcoin



- Ripple only allows single sender/receiver per transaction
  - Employ threshold signature techniques overcome the problem
  - Pathjoin!

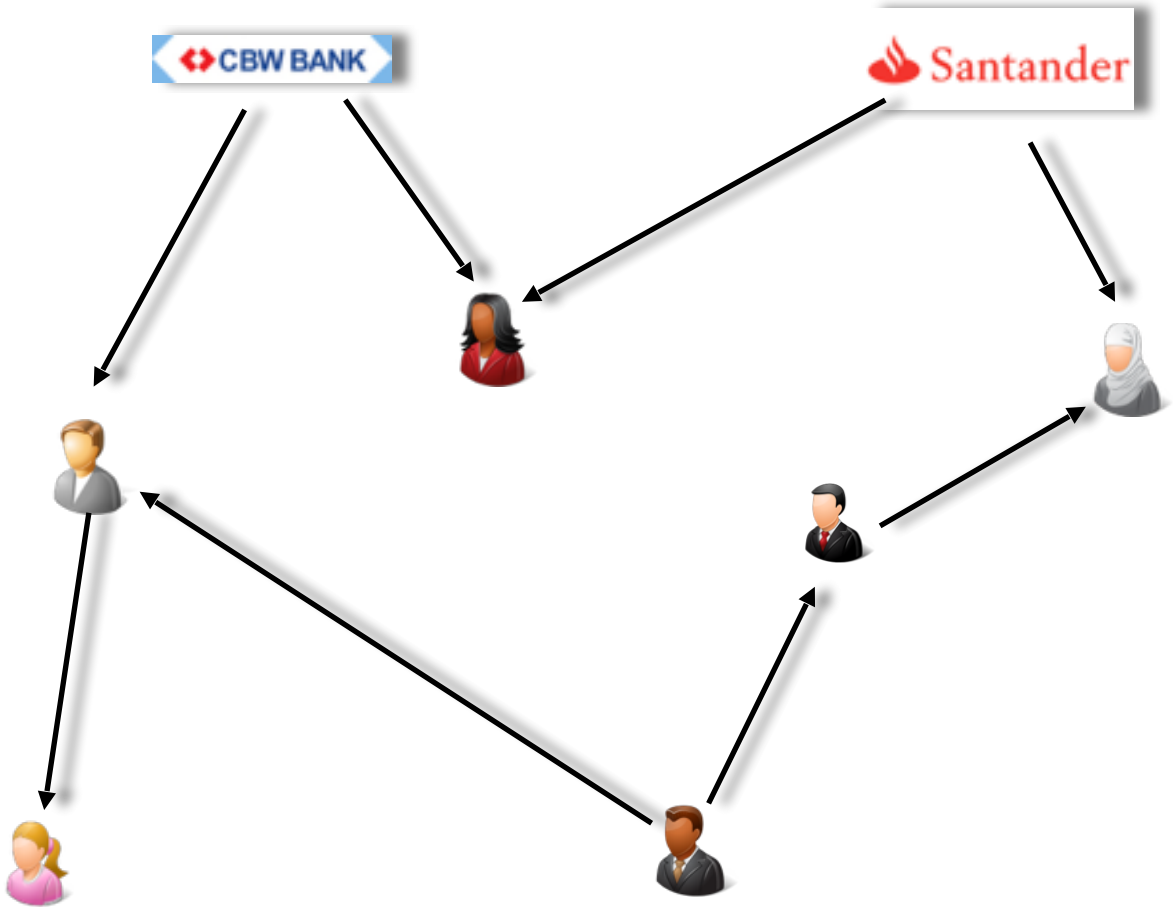
- 100% Compatible with Ripple. We tested it on the real Ripple network!

Towards Secure Distributed Credit Networks

A. Kate, M. Maffei, G. Malavolta, and P. Moreno-Sanchez:
SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks
To appar at **NDSS 2017**
TechReport: http://crypsys.mmci.uni-saarland.de/projects/DecentralizedPrivPay/

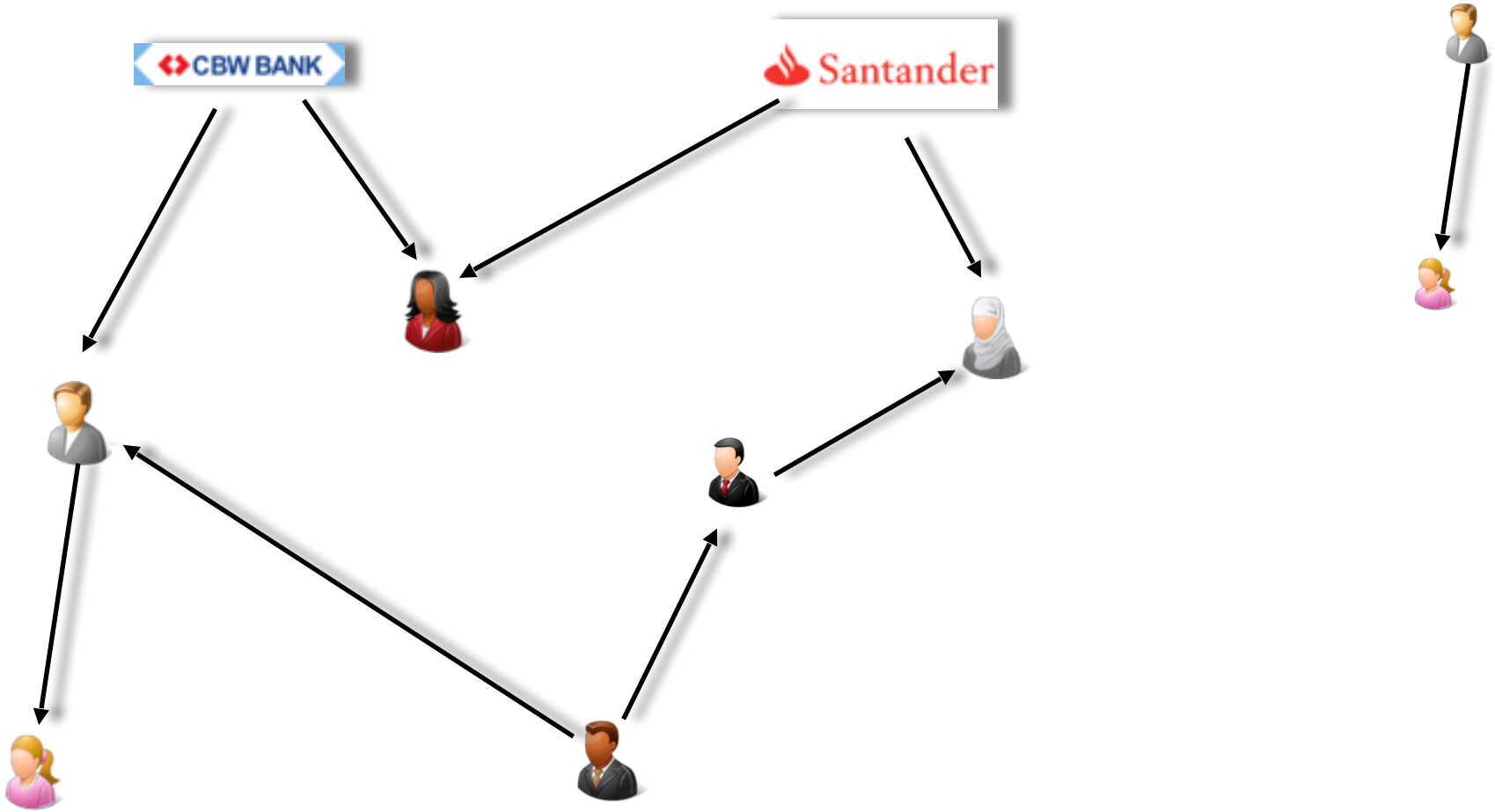
A Distributed Credit Network

- Each user maintains her own credit links



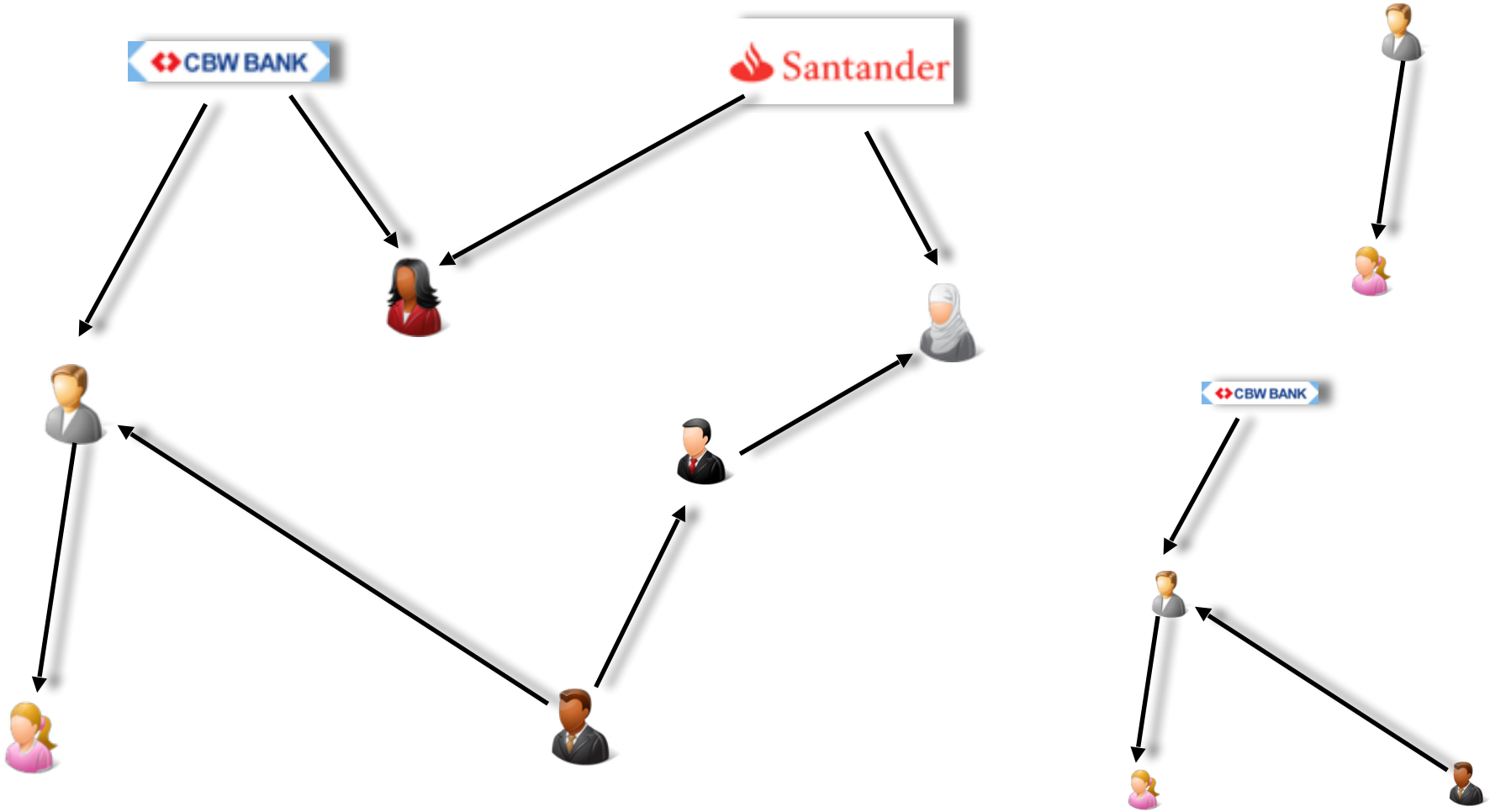
A Distributed Credit Network

- Each user maintains her own credit links



A Distributed Credit Network

- Each user maintains her own credit links

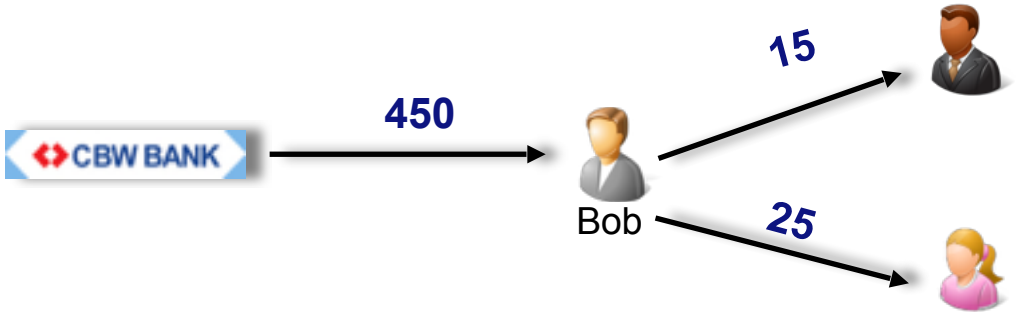


Local Knowledge is Sufficient!

- Credit links of a user determine his credit in the network

Local Knowledge is Sufficient!

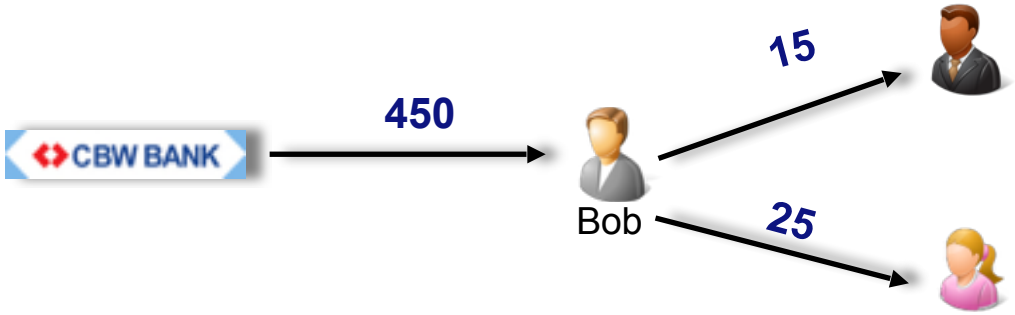
- Credit links of a user determine his credit in the network



In-flow = 450
Out-flow = 40
Net-flow = 410

Local Knowledge is Sufficient!

- Credit links of a user determine his credit in the network

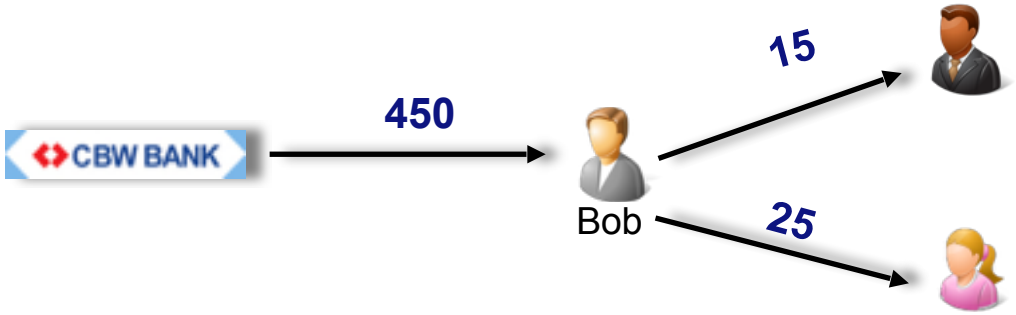


In-flow = 450
Out-flow = 40
Net-flow = 410

- A user checks net-flow does not change

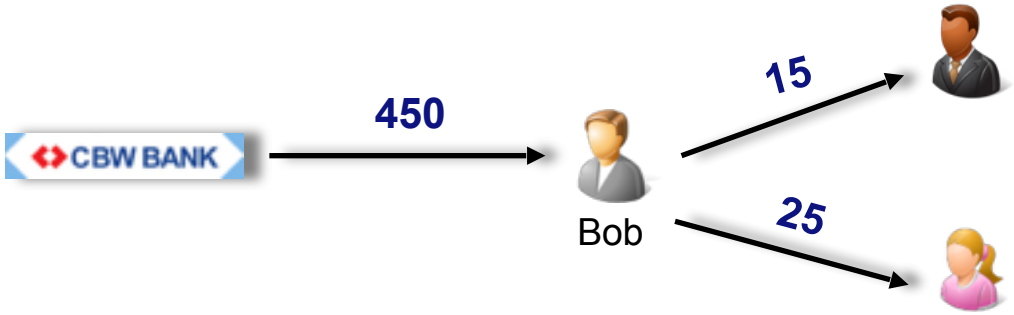
Local Knowledge is Sufficient!

- Credit links of a user determine his credit in the network



In-flow = 450
Out-flow = 40
Net-flow = 410

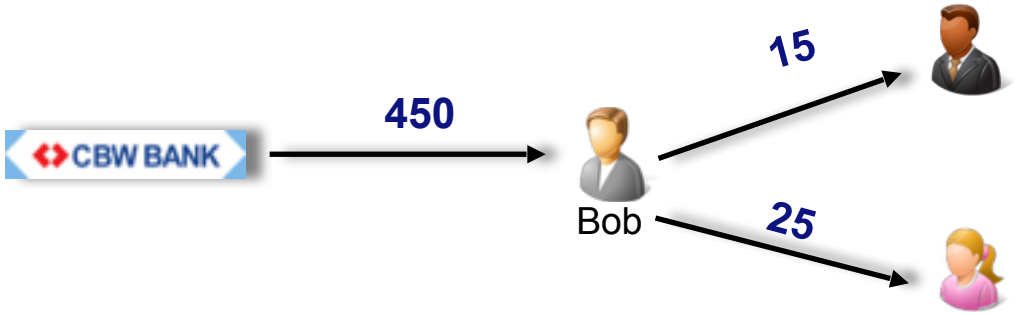
- A user checks net-flow does not change



In-flow = 450
Out-flow = 40
Net-flow = 410

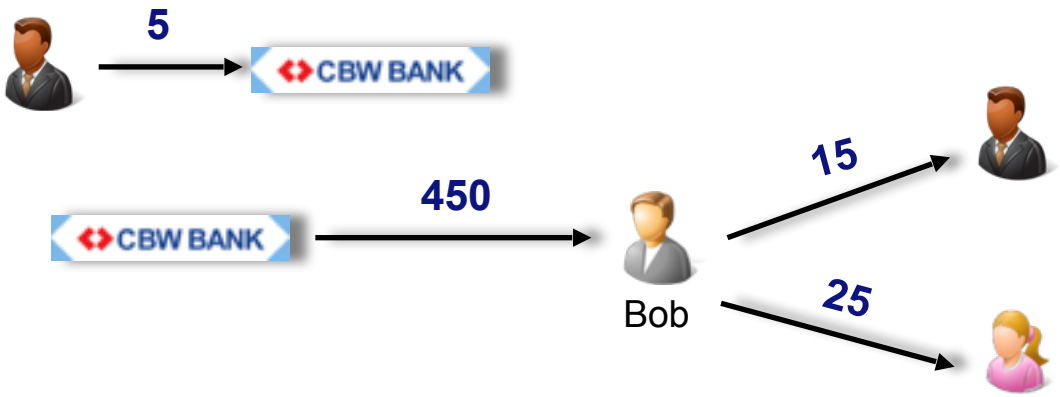
Local Knowledge is Sufficient!

- Credit links of a user determine his credit in the network



In-flow = 450
Out-flow = 40
Net-flow = 410

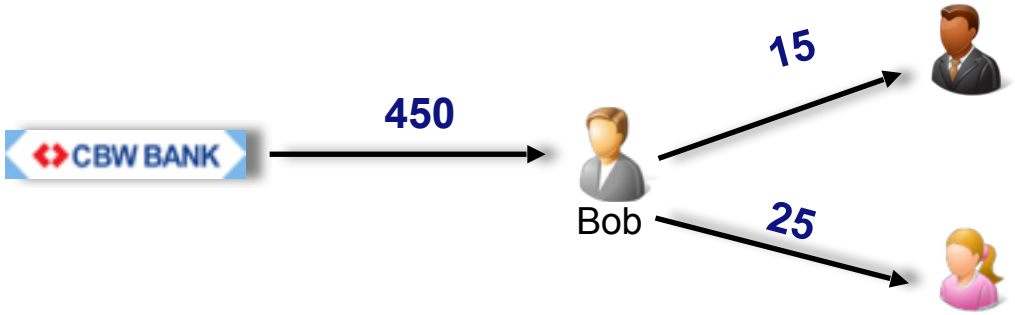
- A user checks net-flow does not change



In-flow = 450
Out-flow = 40
Net-flow = 410

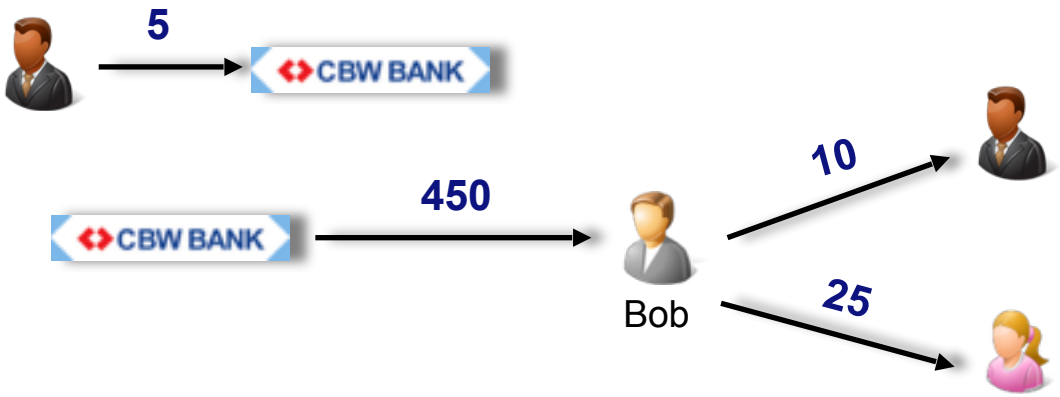
Local Knowledge is Sufficient!

- Credit links of a user determine his credit in the network



In-flow = 450
Out-flow = 40
Net-flow = 410

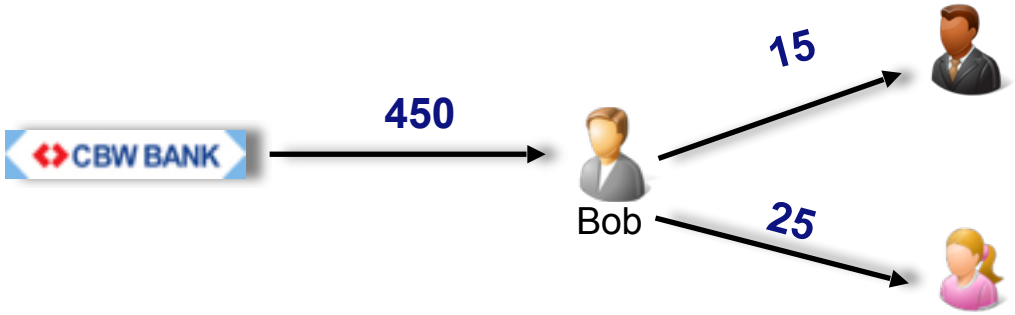
- A user checks net-flow does not change



In-flow = 450
Out-flow = 40
Net-flow = 410

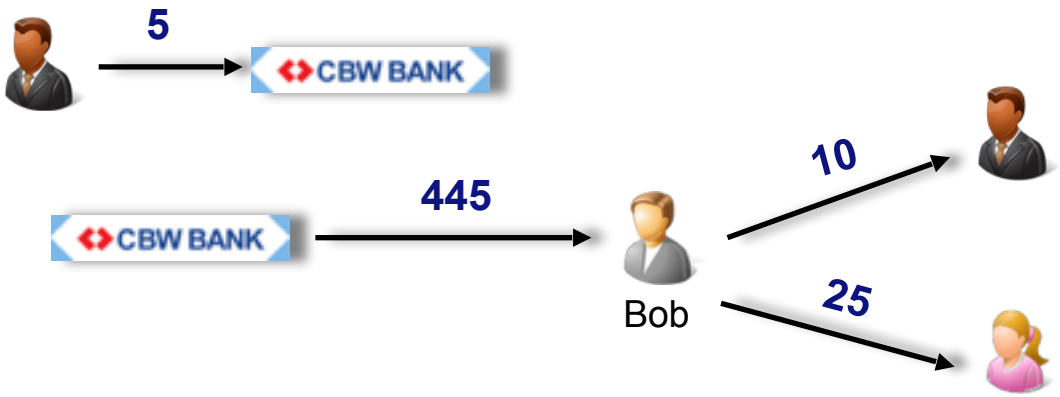
Local Knowledge is Sufficient!

- Credit links of a user determine his credit in the network



In-flow = 450
Out-flow = 40
Net-flow = 410

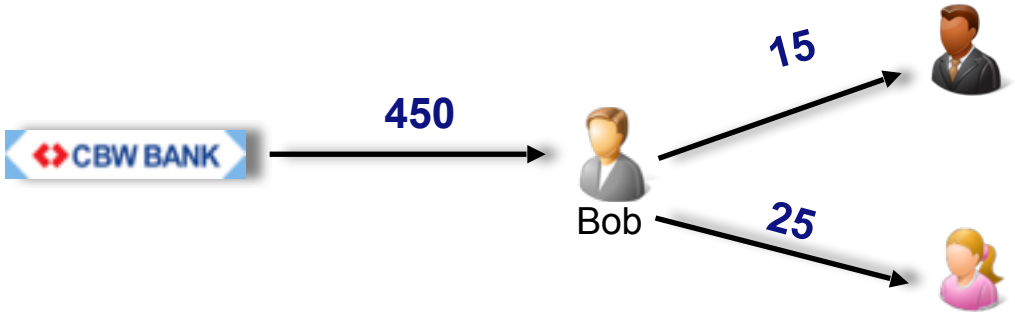
- A user checks net-flow does not change



In-flow = 450
Out-flow = 40
Net-flow = 410

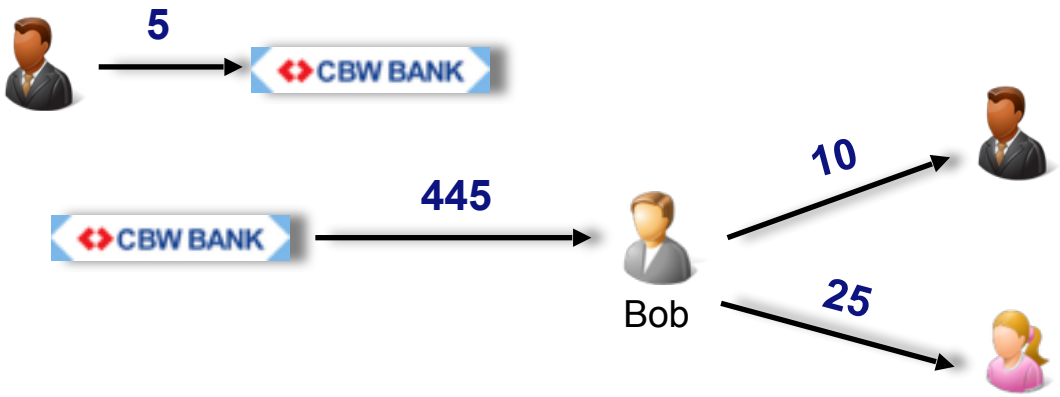
Local Knowledge is Sufficient!

- Credit links of a user determine his credit in the network



In-flow = 450
Out-flow = 40
Net-flow = 410

- A user checks net-flow does not change



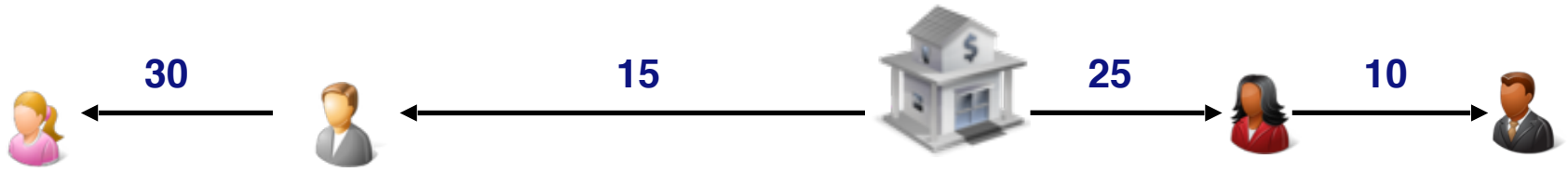
In-flow = ~~450~~ 445
Out-flow = ~~40~~ 35
Net-flow = 410

Challenges

- How to find paths between a sender and a receiver?
- How to find the IOU credit available in the path?
- How to ensure credit links form a path?
- And maintaining strong privacy, availability, and accountability guarantees…

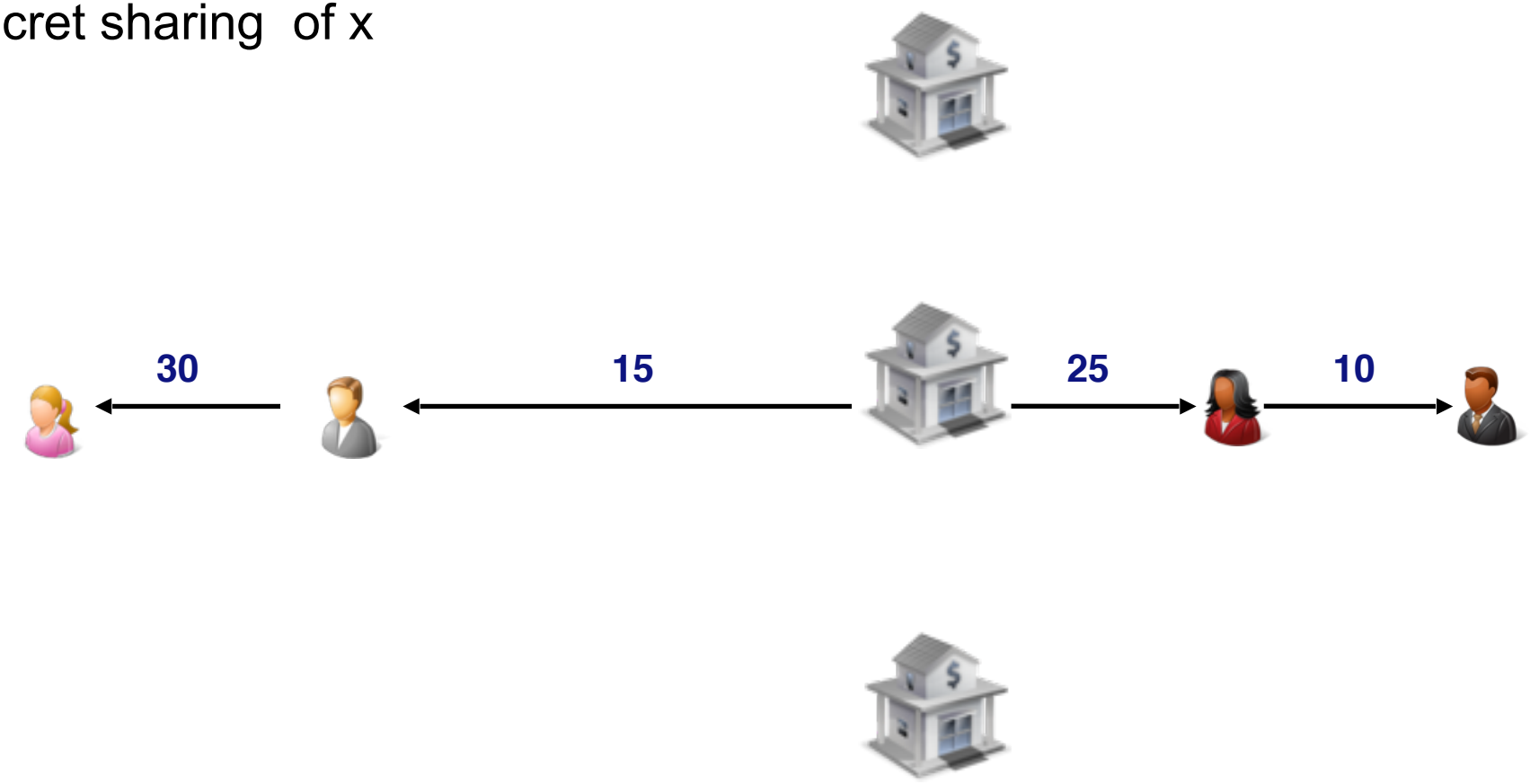
Credit in a Path

[x]: Secret sharing of x



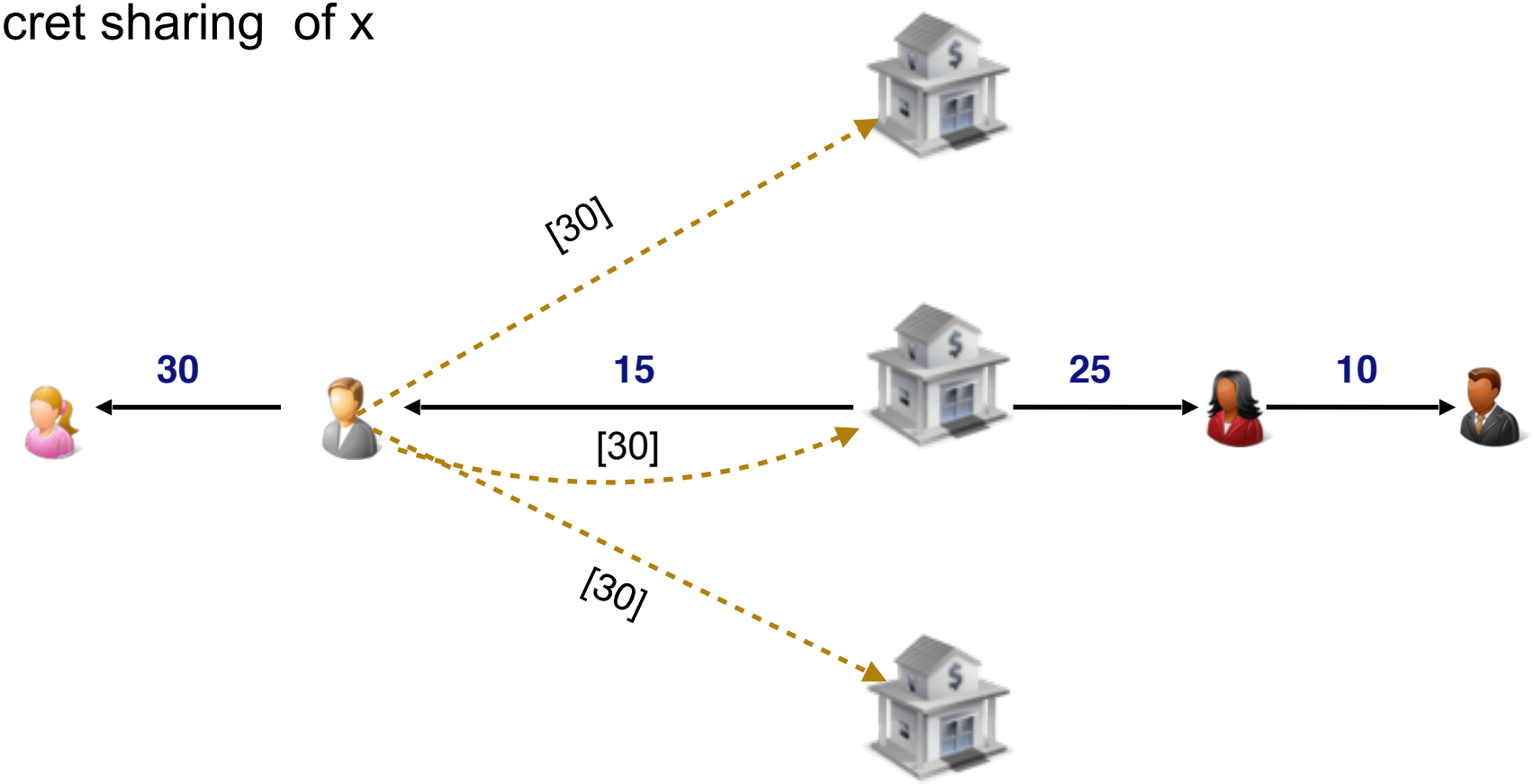
Credit in a Path

[x]: Secret sharing of x



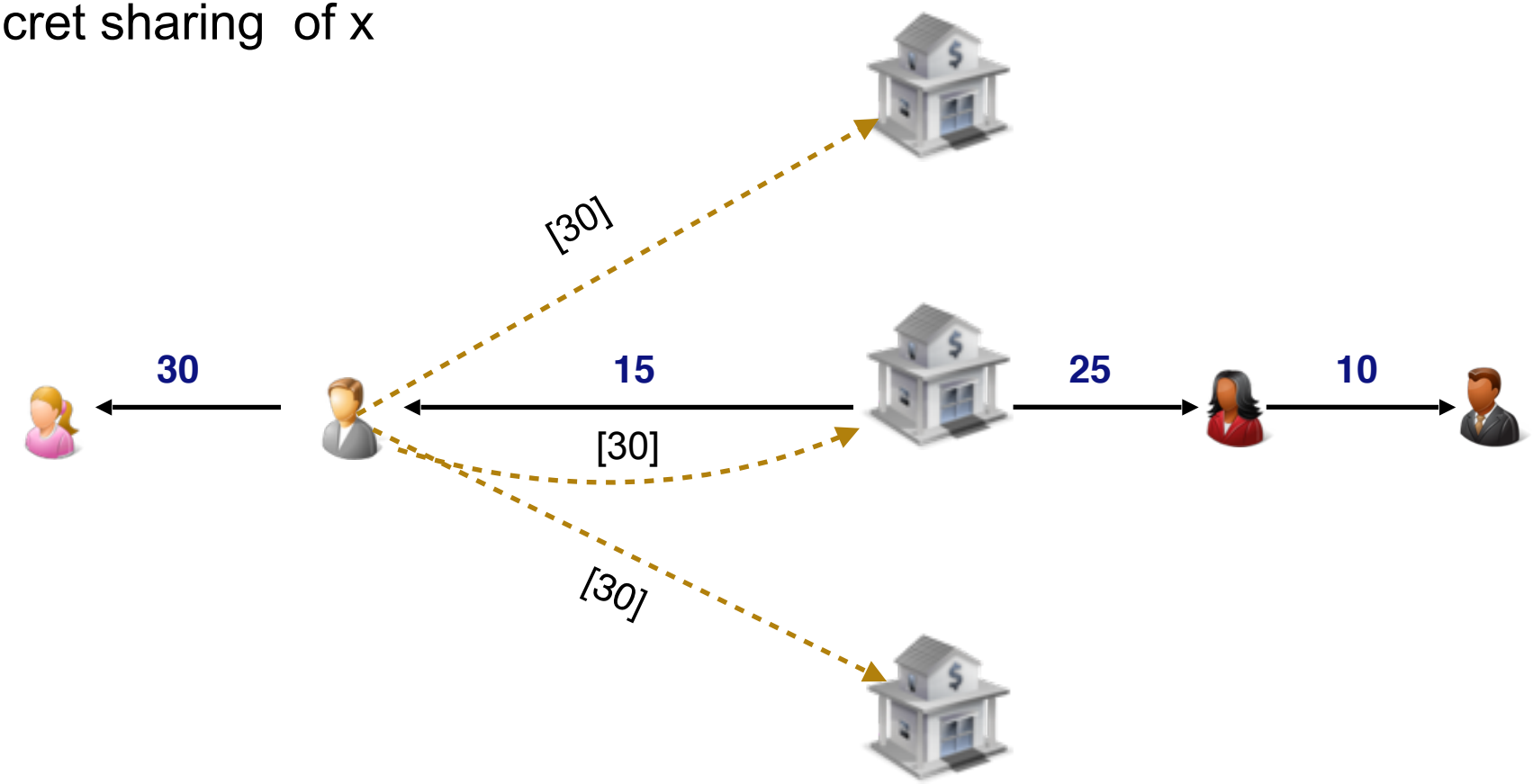
Credit in a Path

[x]: Secret sharing of x



Credit in a Path

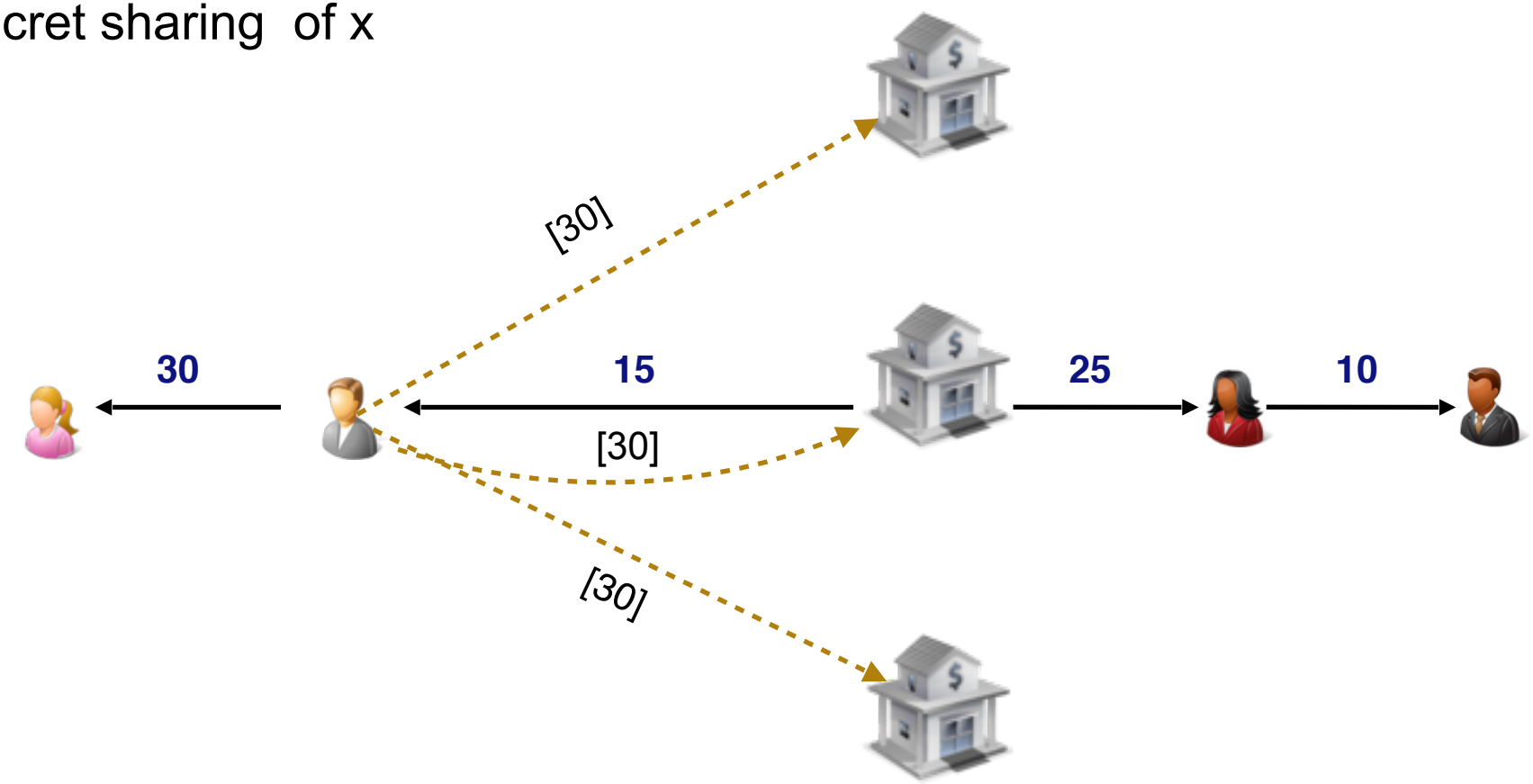
[x]: Secret sharing of x



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

Credit in a Path

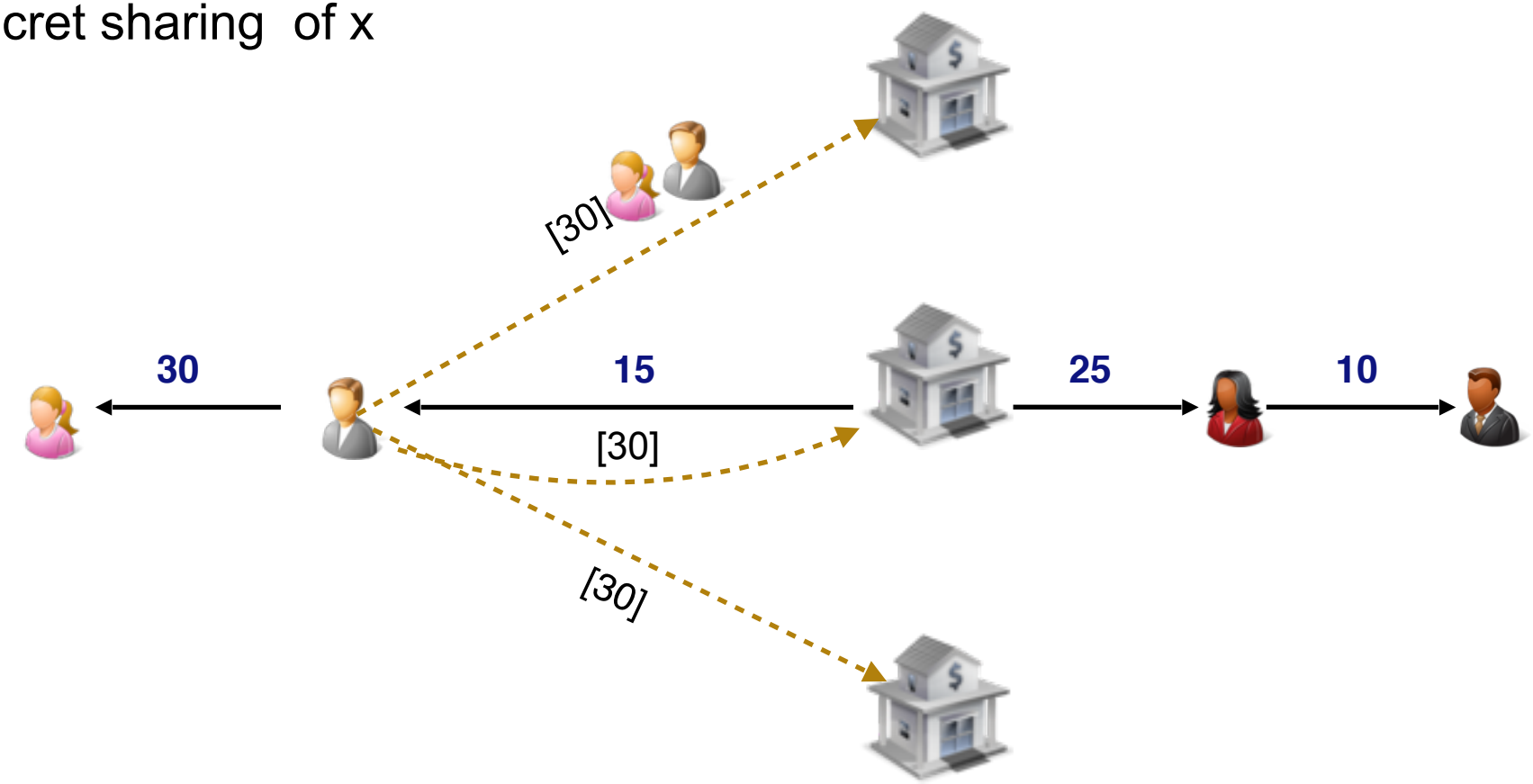
[x]: Secret sharing of x



- Given [x] it is not possible to know x
- How to ensure that [x] comes from a user in a path?

Credit in a Path

[x]: Secret sharing of x



- Given [x] it is not possible to know x
- How to ensure that [x] comes from a user in a path?

Proof of Credit Links in a Path

Proof of Credit Links in a Path

sk_1, vk_1 sk_2, vk_2

Proof of Credit Links in a Path

sk_1, vk_1 sk_2, vk_2

$\sigma_1 := Sig(sk_1, ([30], vk1, vk2))$
$\sigma_2 := Sig(sk_2, ([30], vk1, vk2))$

Proof of Credit Links in a Path

sk_1, vk_1 sk_2, vk_2

$[30], vk_{\{1,2\}}, \sigma_{\{1,2\}}$

$\sigma_1 := Sig(sk_1, ([30], vk1, vk2))$
$\sigma_2 := Sig(sk_2, ([30], vk1, vk2))$

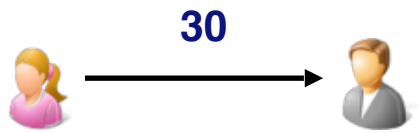
Proof of Credit Links in a Path

$\sigma_1 := Sig(sk_1, ([30], vk1, vk2))$
$\sigma_2 := Sig(sk_2, ([30], vk1, vk2))$

Correct proof for a path

$(vk_1, vk_2), (vk_2, vk_3), (vk_3, vk_4), \ldots$

Proof of Credit Links in a Path



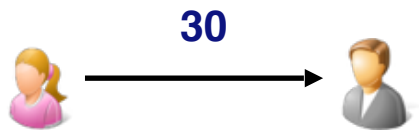
$\sigma_1 := Sig(sk_1, ([30], vk1, vk2))$
$\sigma_2 := Sig(sk_2, ([30], vk1, vk2))$

$[30], vk_{\{1,2\}}, \sigma_{\{1,2\}}$

Correct proof for a path

(vk_1, vk_2) (vk_2, vk_3), (vk_3, vk_4), …

Proof of Credit Links in a Path



$\sigma_1 := Sig(sk_1, ([30], vk1, vk2))$
$\sigma_2 := Sig(sk_2, ([30], vk1, vk2))$

$[30], vk_{\{1,2\}}, \sigma_{\{1,2\}}$

Correct proof for a path

$(vk_1, vk_2), (vk_2, vk_3), (vk_3, vk_4), \ldots$

Proof of Credit Links in a Path

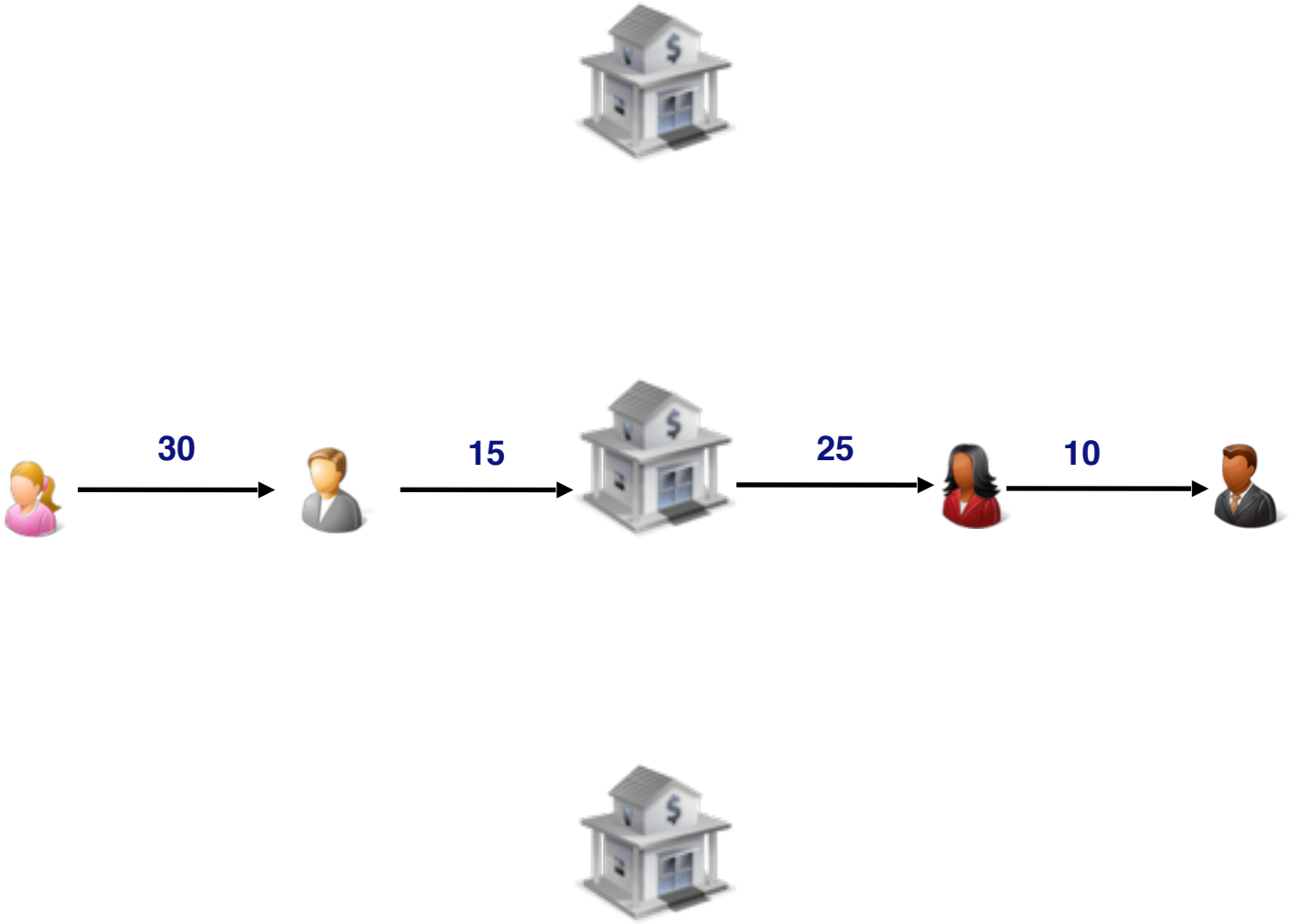
$\sigma_1 := Sig(sk_1, ([30], vk1, vk2))$
$\sigma_2 := Sig(sk_2, ([30], vk1, vk2))$

Correct proof for a path

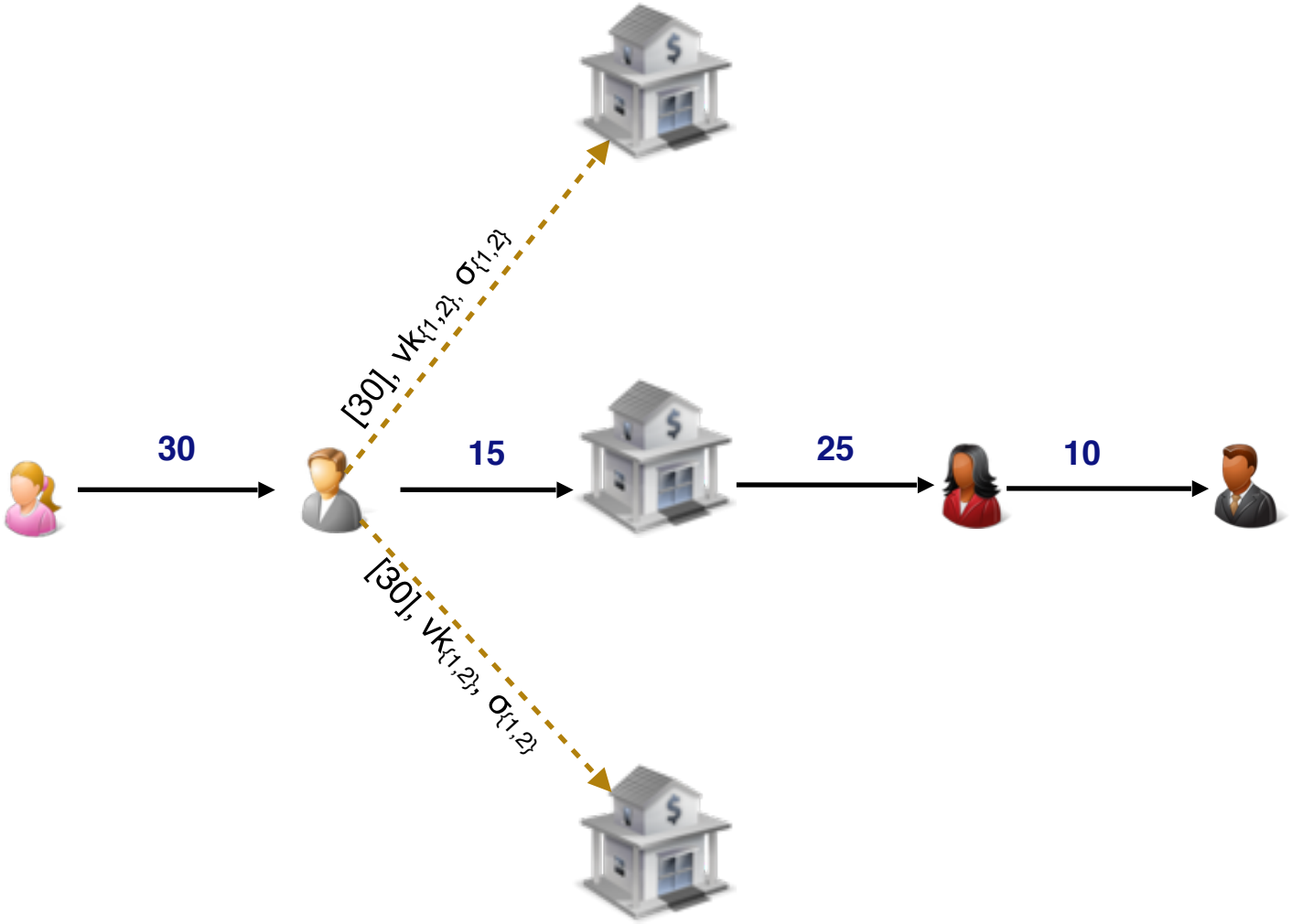
$(vk_1, vk_2), (vk_2, vk_3), (vk_3, vk_4), \ldots$

Fresh keys per transaction

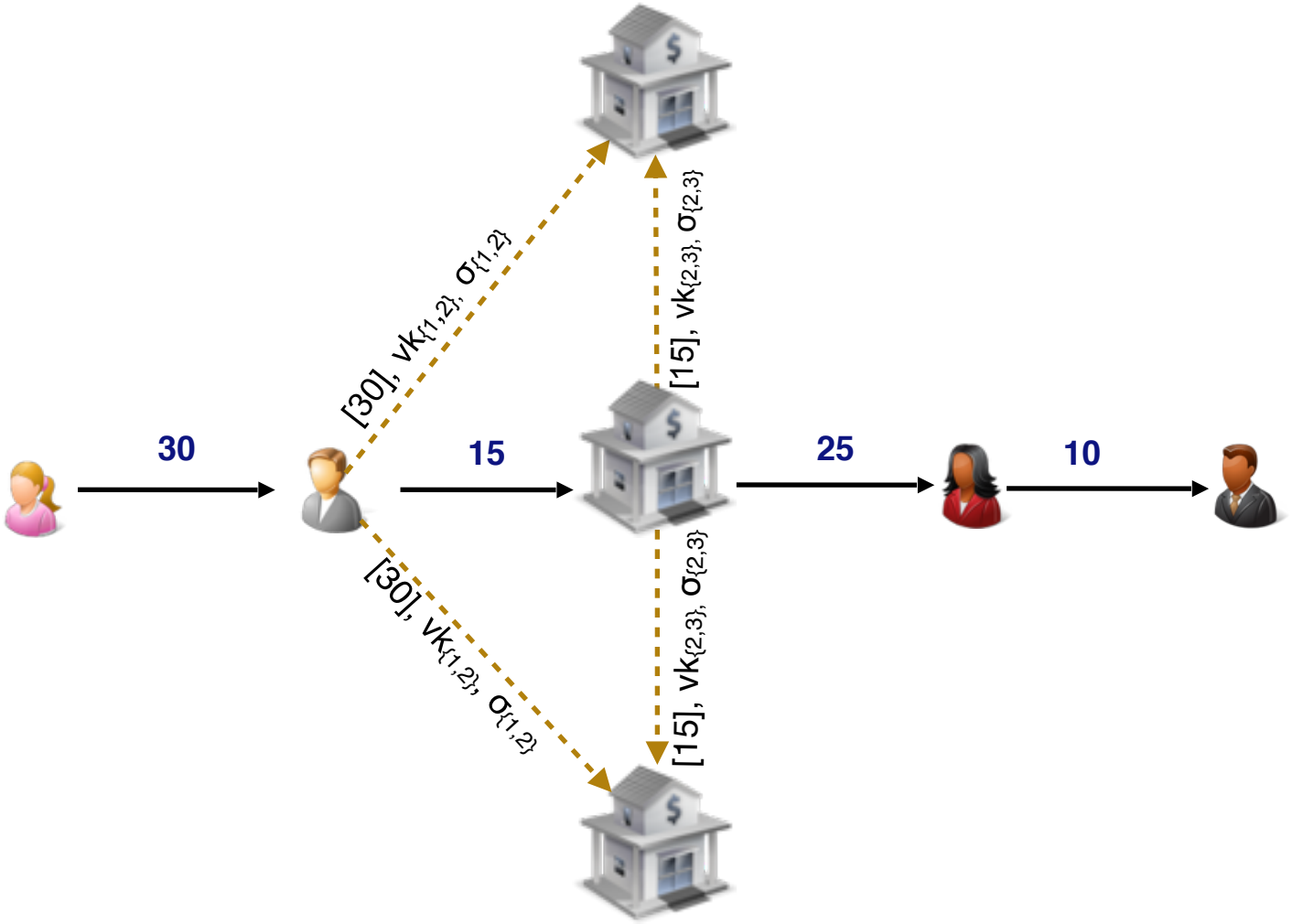
Privacy-preserving Credit in a Path



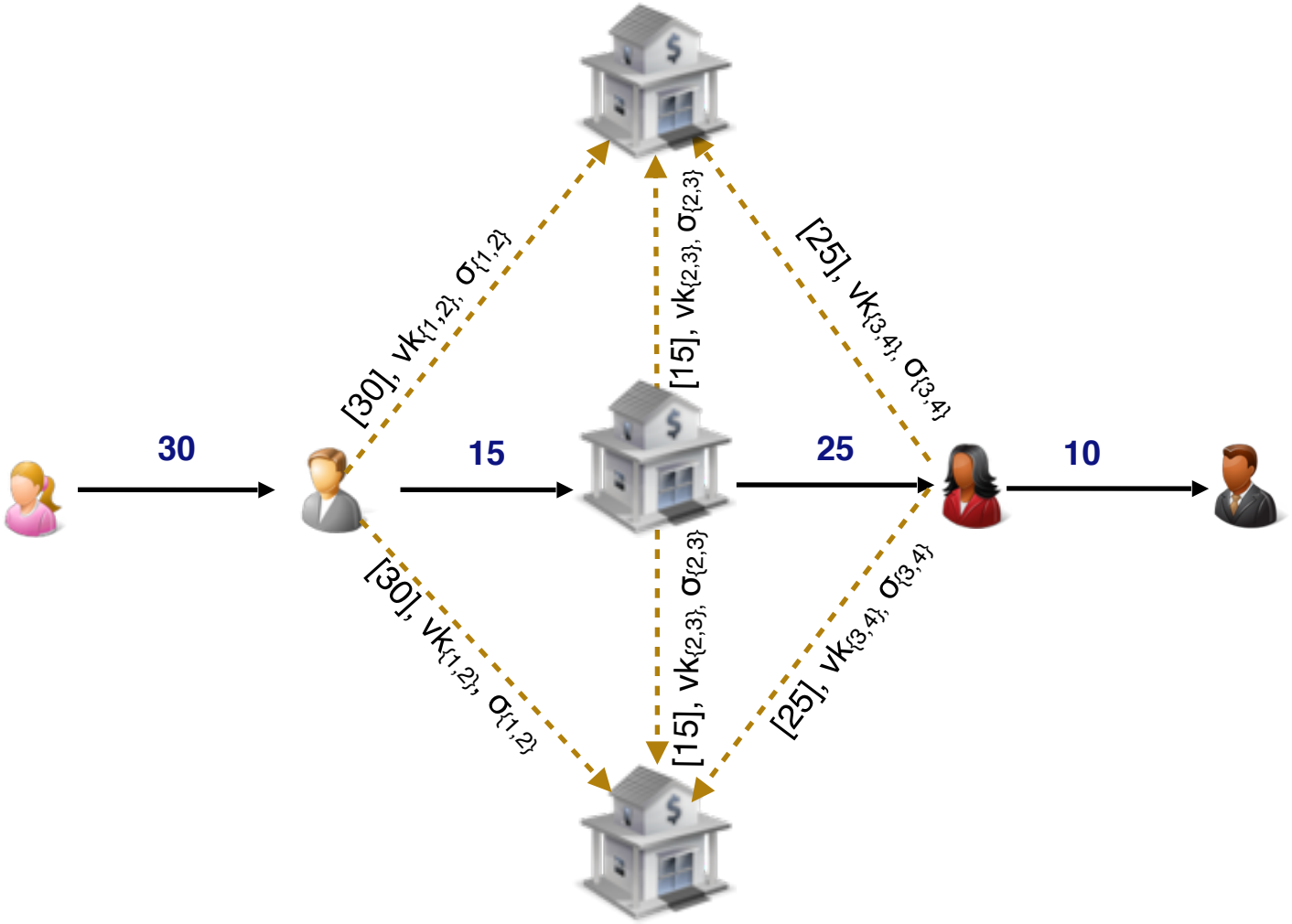
Privacy-preserving Credit in a Path



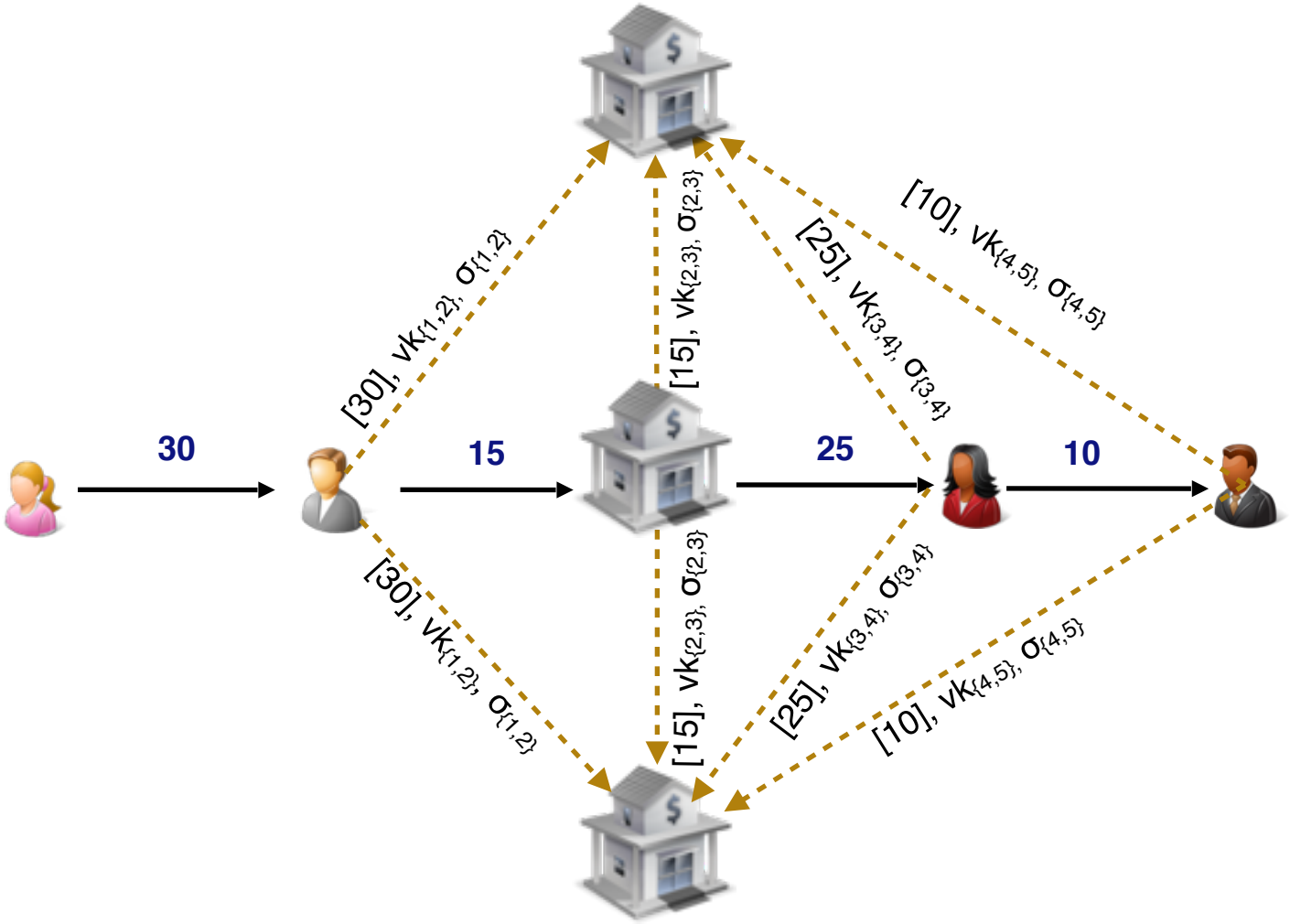
Privacy-preserving Credit in a Path



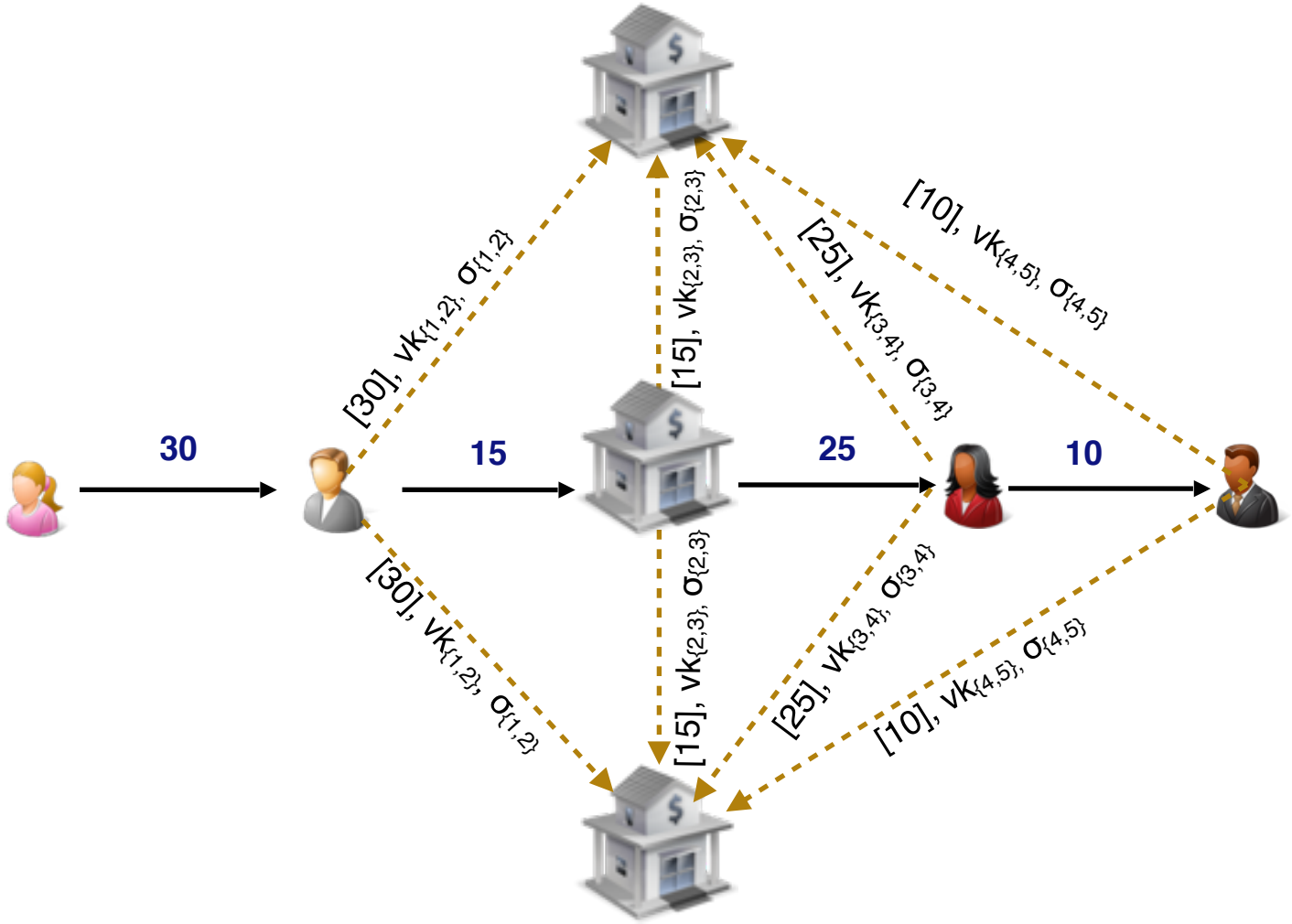
Privacy-preserving Credit in a Path



Privacy-preserving Credit in a Path

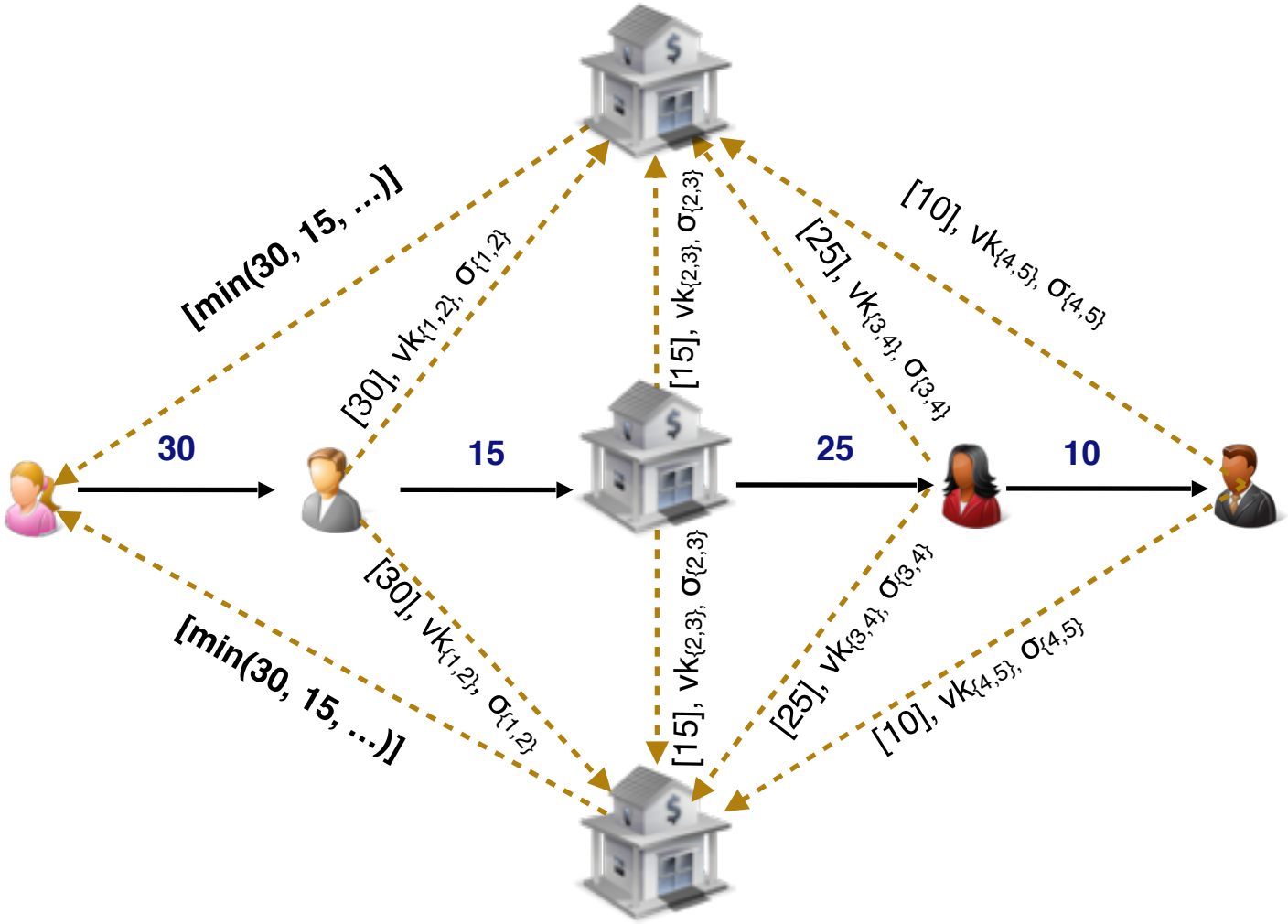


Privacy-preserving Credit in a Path



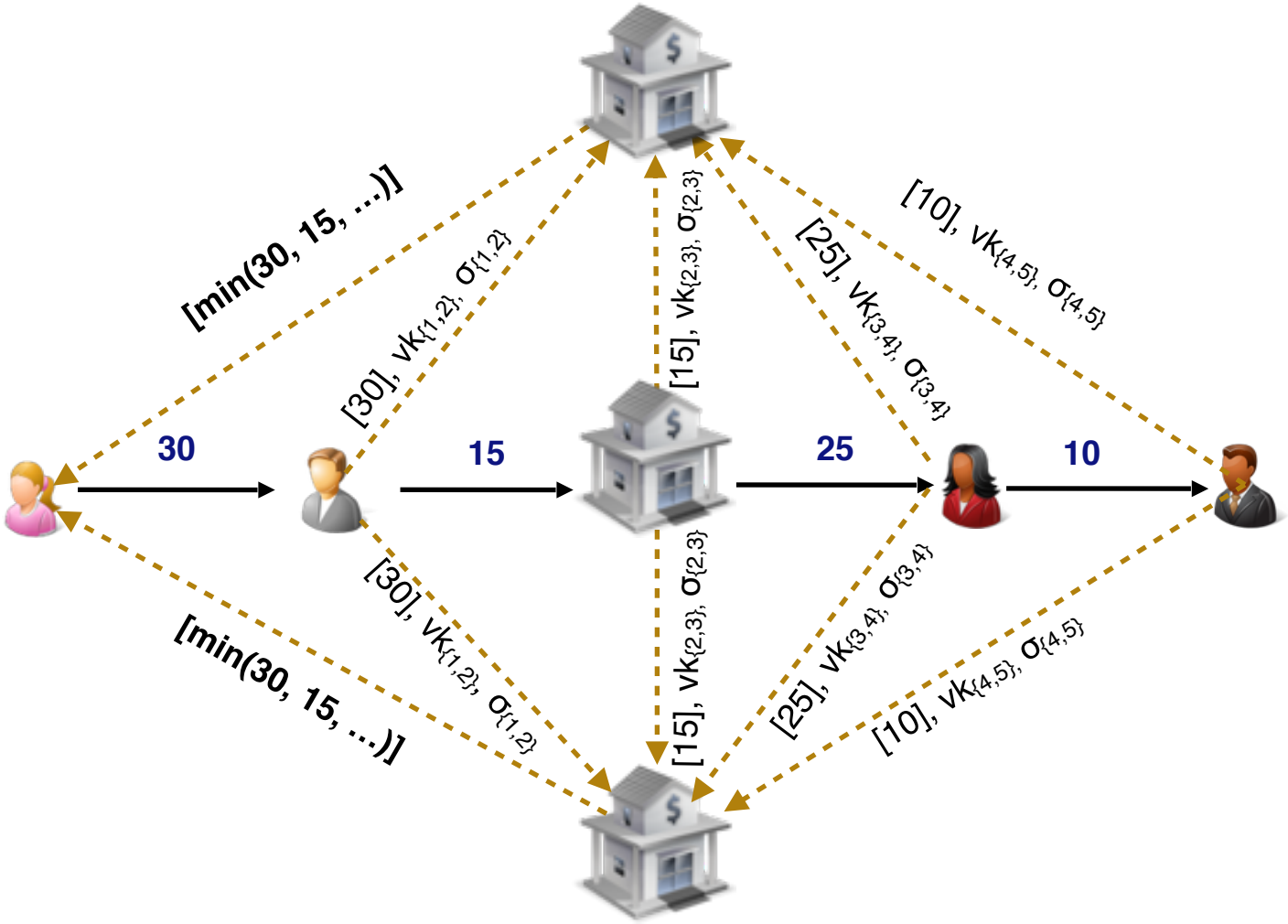
- Landmarks perform SMPC min computation over the shared link values

Privacy-preserving Credit in a Path



- Landmarks perform SMPC min computation over the shared link values

Privacy-preserving Credit in a Path



- Landmarks perform SMPC min computation over the shared link values
- Given enough “copies” of [x] it is possible to recover x for Alice

Transaction Execution

PURDUE UNIVERSITY

Transaction Execution

- Sequential friend-to-friend communication

Transaction Execution

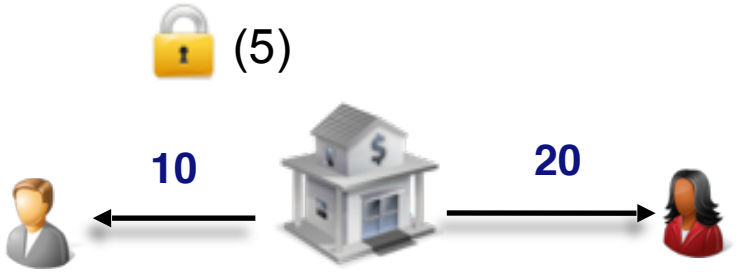
- Sequential friend-to-friend communication
- Two-step transaction: on hold (or block) and settle

Transaction Execution

- Sequential friend-to-friend communication
- Two-step transaction: on hold (or block) and settle
- Example:

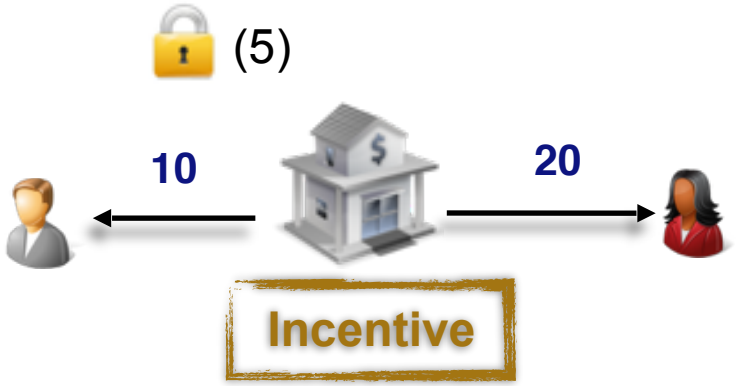
Transaction Execution

- Sequential friend-to-friend communication
- Two-step transaction: on hold (or block) and settle
- Example:



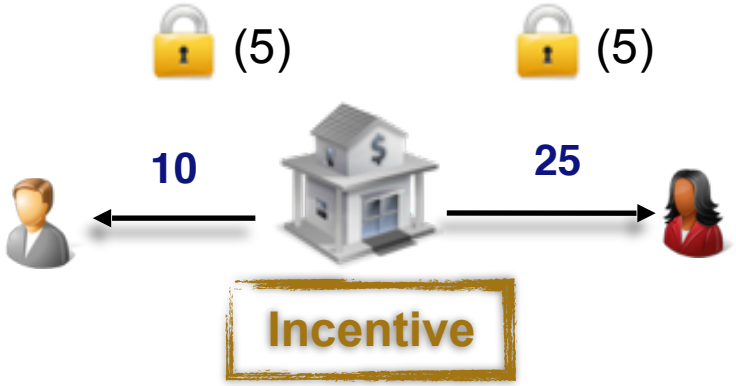
Transaction Execution

- Sequential friend-to-friend communication
- Two-step transaction: on hold (or block) and settle
- Example:



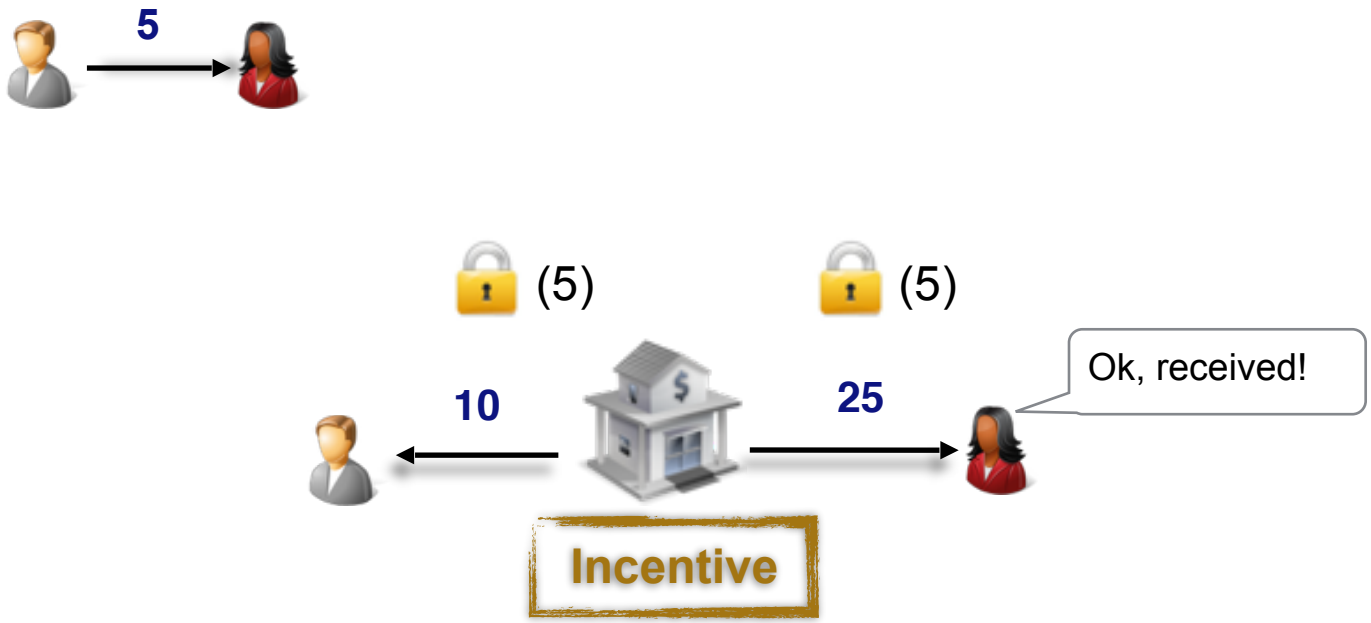
Transaction Execution

- Sequential friend-to-friend communication
- Two-step transaction: on hold (or block) and settle
- Example:



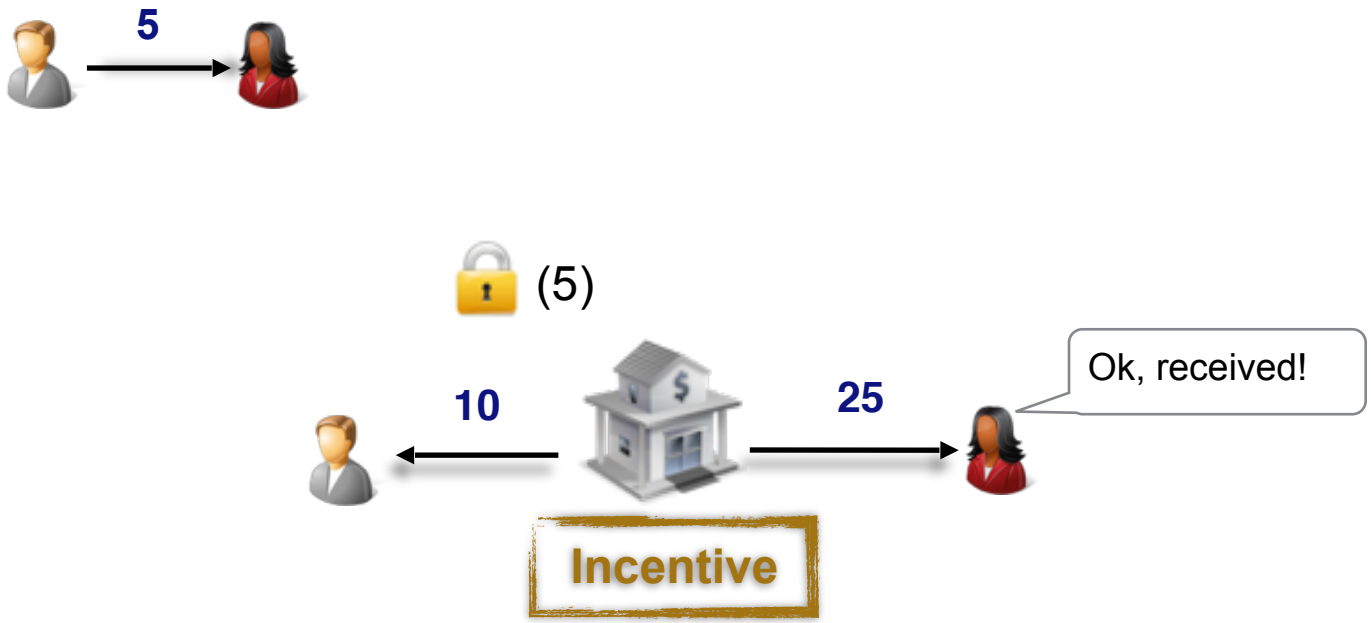
Transaction Execution

- Sequential friend-to-friend communication
- Two-step transaction: on hold (or block) and settle
- Example:



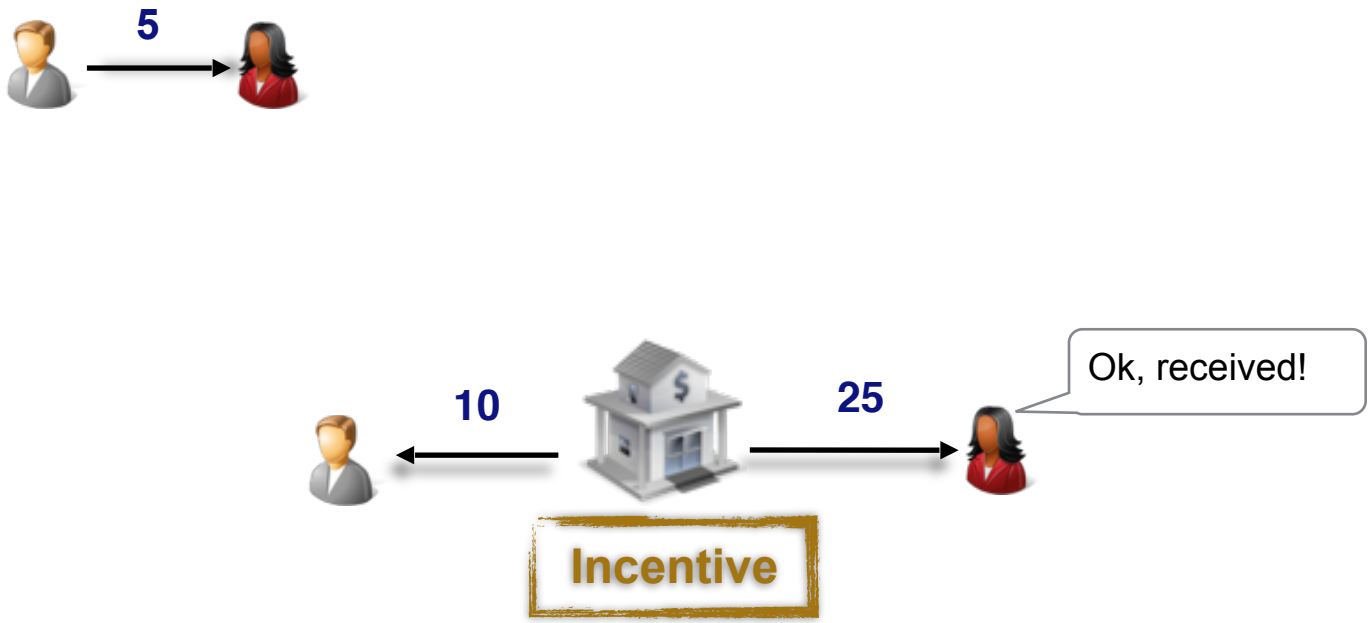
Transaction Execution

- Sequential friend-to-friend communication
- Two-step transaction: on hold (or block) and settle
- Example:



Transaction Execution

- Sequential friend-to-friend communication
- Two-step transaction: on hold (or block) and settle
- Example:



SilentWhispers: Characteristics/Limitations

PURDUE UNIVERSITY

- Distributed credit network transactions are possible without requiring
  - a blockchain ledger
  - a proof-of-work
- SilentWhispers can be modified by using landmarks as distributed stores

[more details in the paper]

- In case of disputes, this leaves task of proving links to the users
- It is blocking solution, and deadlocks are possibles
  - Problem: designing non-blocking solutions in the asynchronous communication setting
    - distributed max-flow computation and atomic broadcast

In the Future

- Payment Channels and lighting network

  https://lightning.network

  - Designing distributed solutions for lighting network

- The Interledger Protocol

  https://www.w3.org/community/interledger

  - Several distributed/decentralized/centralized ledger solutions are coming up
  - Performing transactions across different ledgers

Thanks to My Collaborators

PURDUE UNIVERSITY

Pedro Moreno-Sanchez

Matteo Maffei

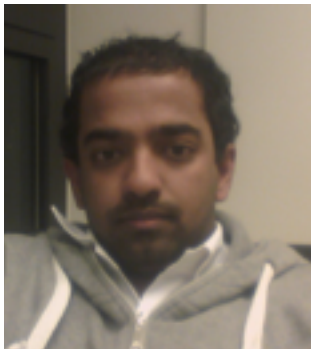
Muhammad Bilal Zafar

Sonia Fahmy

Tim Ruffing

Kim Pecina

Giulio Malavolta



Srivatsan Ravi

Thanks to My Collaborators

PURDUE UNIVERSITY

Pedro Moreno-Sanchez

Matteo Maffei

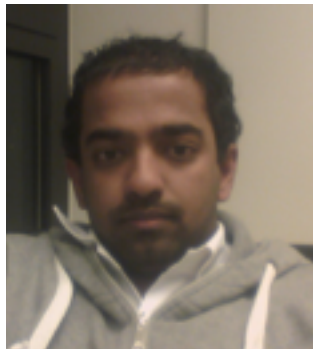
Muhammad Bilal Zafar

Sonia Fahmy

Tim Ruffing

Kim Pecina

Giulio Malavolta



Srivatsan Ravi

Thanks to My Collaborators

PURDUE UNIVERSITY

Pedro Moreno-Sanchez

Matteo Maffei

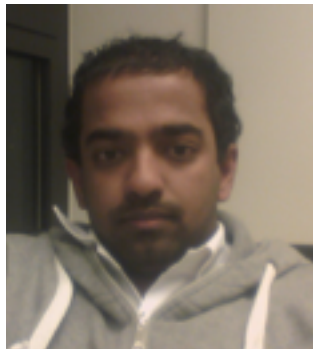
Muhammad Bilal Zafar

Sonia Fahmy

Tim Ruffing

Kim Pecina

Giulio Malavolta

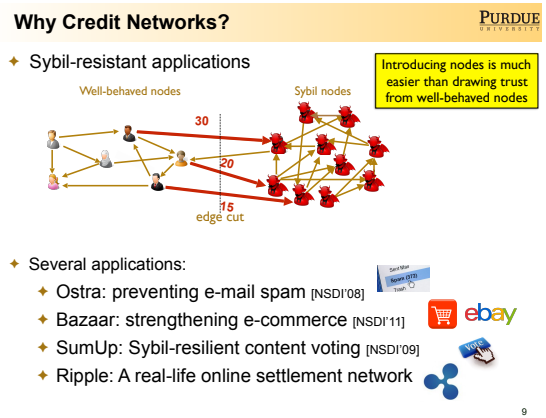


Srivatsan Ravi

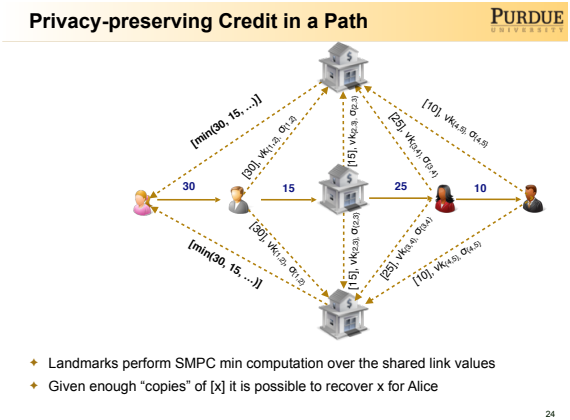
To make credit networks great again!

Take home message

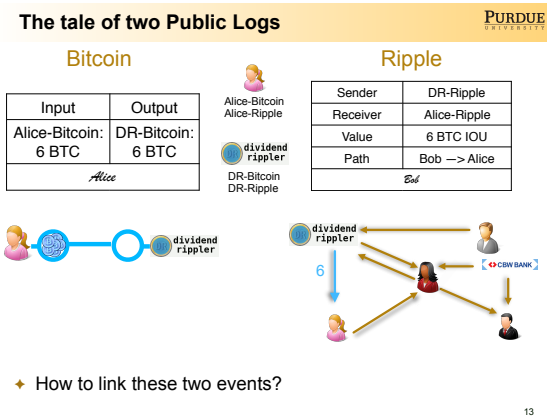
- Credit networks have interesting properties and can be used in multiple scenarios



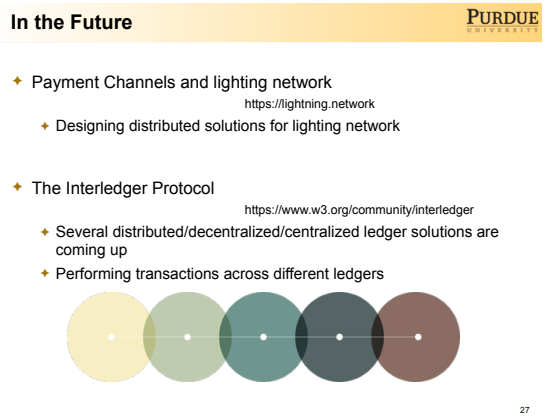
- SlientWhispers: a decentralized architecture for providing accountability and privacy for credit networks



- Ledgers although provide accountability, it makes privacy a real problem in credit networks



- Several questions remain unanswered leaving lots of open problems



Thanks!