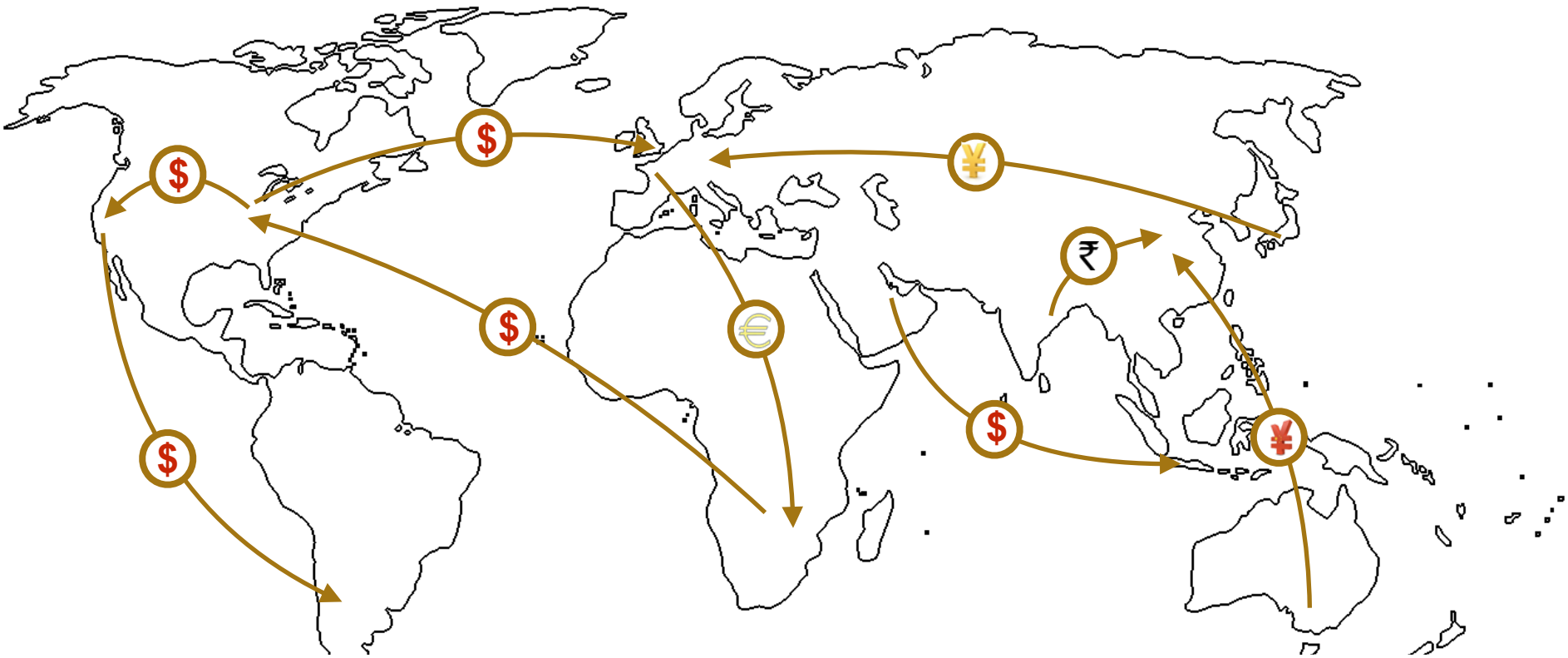
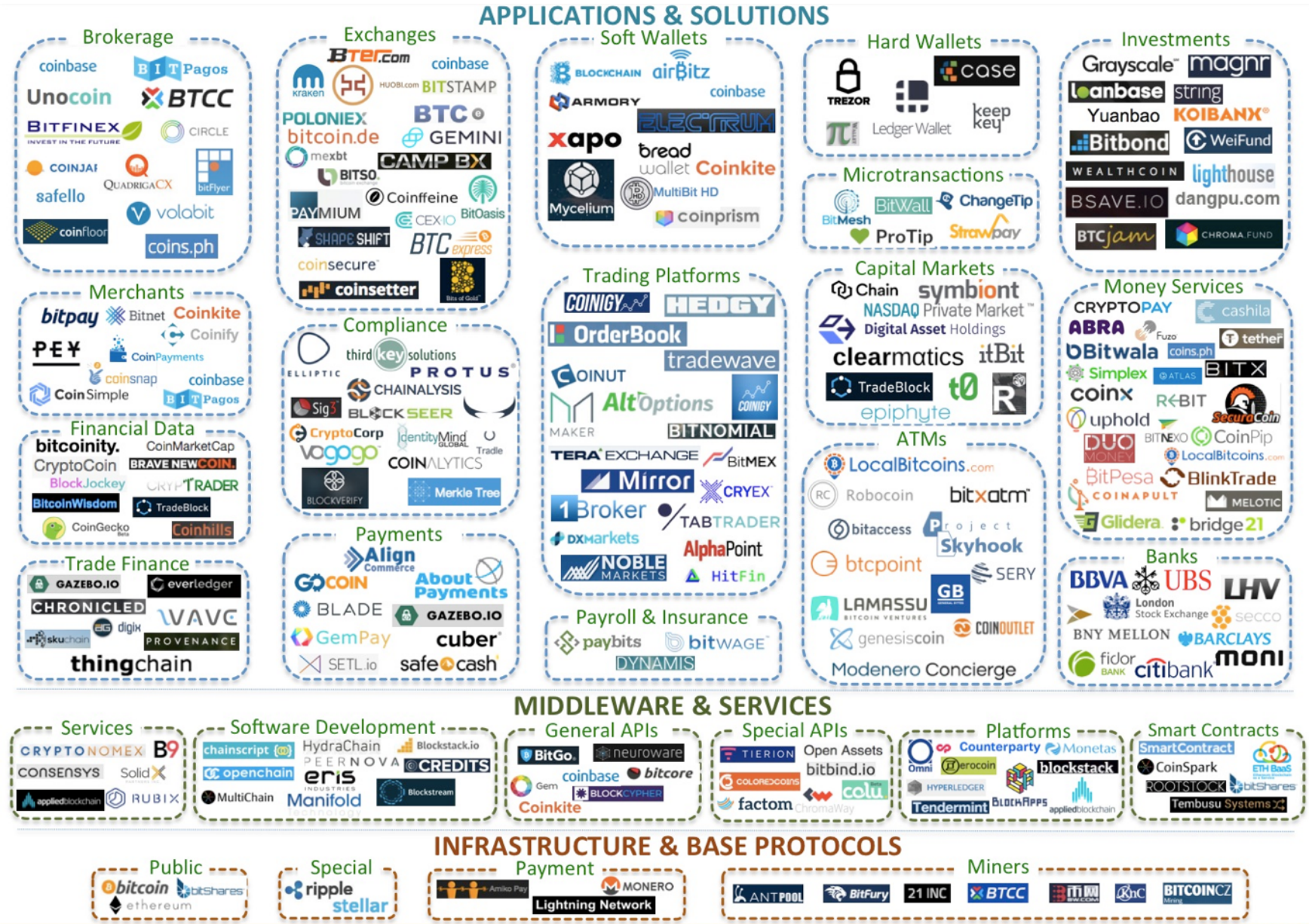
Distributed *IOweYou* Credit Networks



Aniket Kate
Purdue University

Blockchains can change a lot of things



Source: http://startupmanagement.org/blog

Issues with Global Blockchains

Issues with Global Blockchains

- 51% attack (or The tyranny of power)
  - If one controls more than half of the computation power in any permission-less cryptocurrency system, he/she can …

Issues with Global Blockchains

PURDUE UNIVERSITY

- 51% attack (or The tyranny of power)
  - If one controls more than half of the computation power in any permission-less cryptocurrency system, he/she can …
- Money Generation (or Proof of Work)
  - Bitcoin mining could consume as much electricity as Denmark by 2020!

Issues with Global Blockchains

PURDUE UNIVERSITY

- 51% attack (or The tyranny of power)
  - If one controls more than half of the computation power in any permission-less cryptocurrency system, he/she can …
- Money Generation (or Proof of Work)
  - Bitcoin mining could consume as much electricity as Denmark by 2020!
- Scalability and Speed
  - Bitcoin's 7 tps vs VISA's 2000 tps

Issues with Global Blockchains

PURDUE UNIVERSITY

- 51% attack (or The tyranny of power)
  - If one controls more than half of the computation power in any permission-less cryptocurrency system, he/she can …
- Money Generation (or Proof of Work)
  - Bitcoin mining could consume as much electricity as Denmark by 2020!
- Scalability and Speed
  - Bitcoin's 7 tps vs VISA's 2000 tps
- Money vs. Credit
  - Money: medium of exchange
  - Credit: exchange of present goods against future goods

Issues with Global Blockchains

PURDUE UNIVERSITY

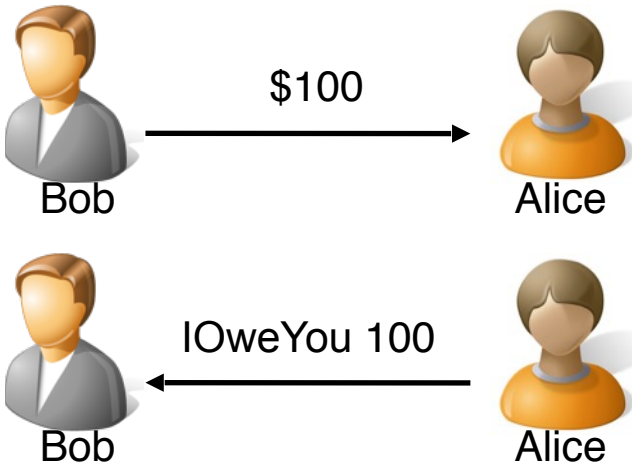
- 51% attack (or The tyranny of power)
  - If one controls more than half of the computation power in any permission-less cryptocurrency system, he/she can …
- Money Generation (or Proof of Work)
  - Bitcoin mining could consume as much electricity as Denmark by 2020!
- Scalability and Speed
  - Bitcoin's 7 tps vs VISA's 2000 tps
- Money vs. Credit
  - Money: medium of exchange
  - Credit: exchange of present goods against future goods
- IOU (or Credit) Networks
  - Combining credit and social trust (still not permissioned)

This talk aims at leaving you with *more questions* than answers regarding credit networks ;)

Credit (or IOU settlement) Networks: Basics

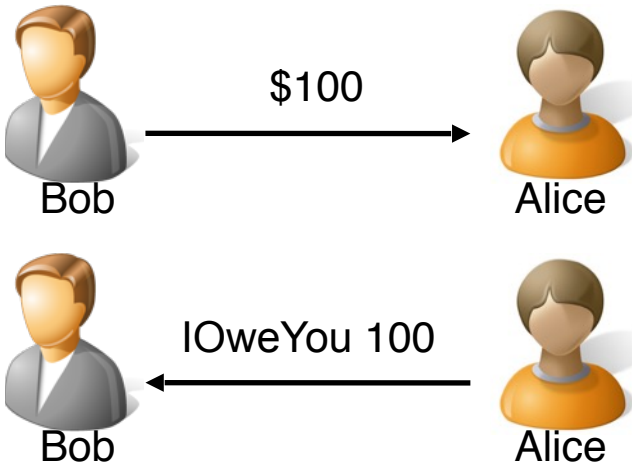
Credit (or IOU settlement) Networks: Basics

Transactions in the real world

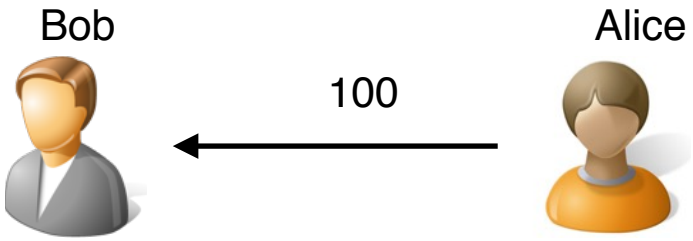


Credit (or IOU settlement) Networks: Basics

Transactions in the real world

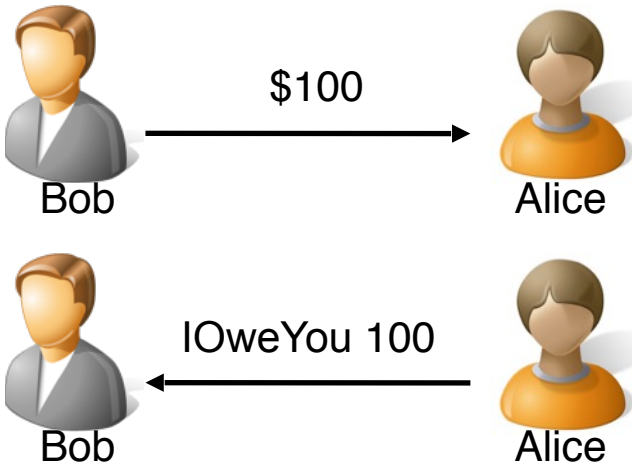


A credit network representation

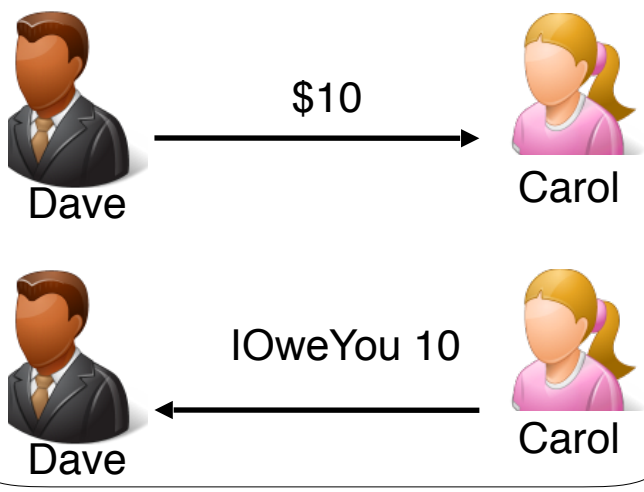


Credit (or IOU settlement) Networks: Basics

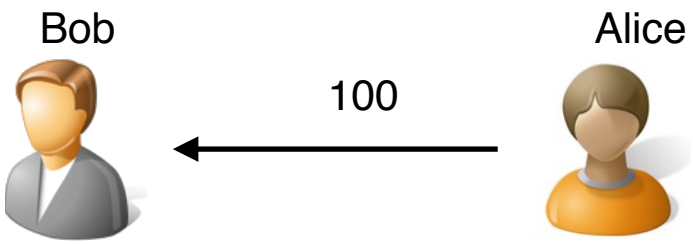
Transactions in the real world



During a hike with Alice & Bob

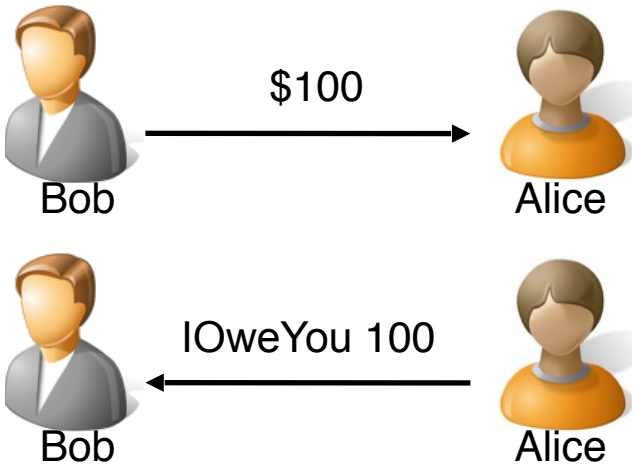


A credit network representation

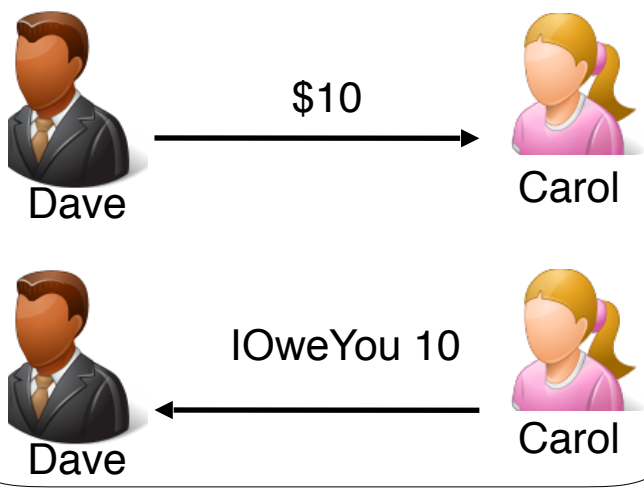


Credit (or IOU settlement) Networks: Basics

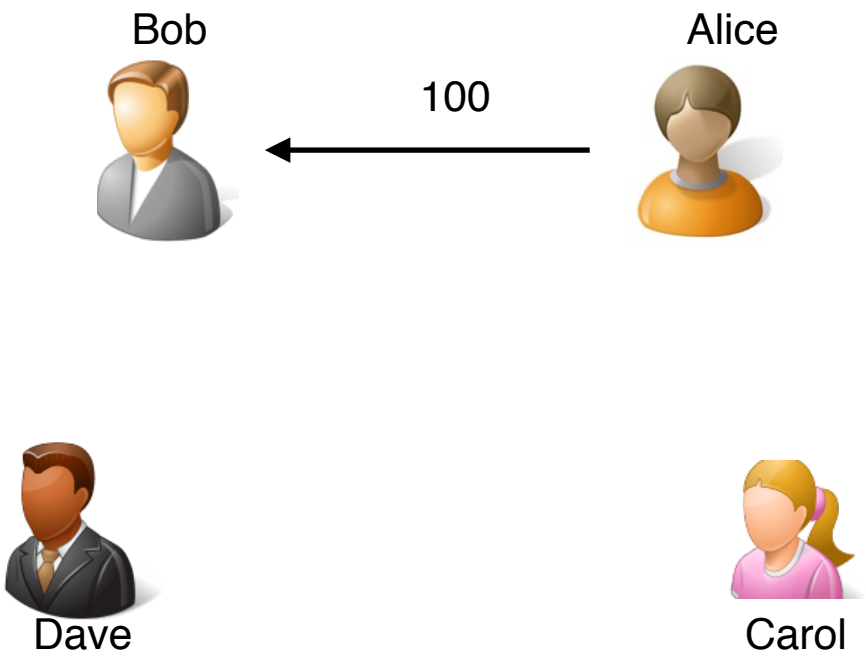
Transactions in the real world



During a hike with Alice & Bob

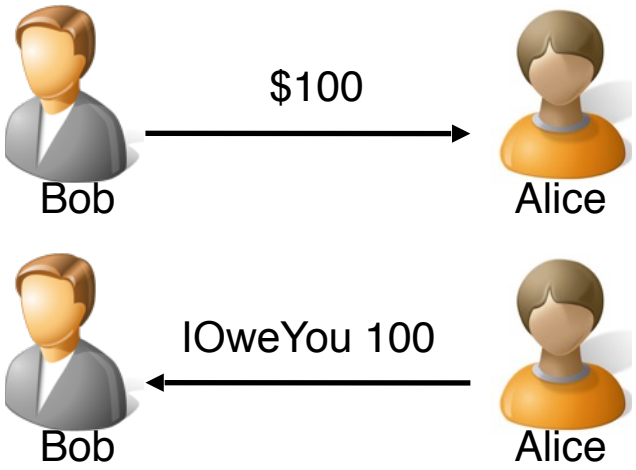


A credit network representation

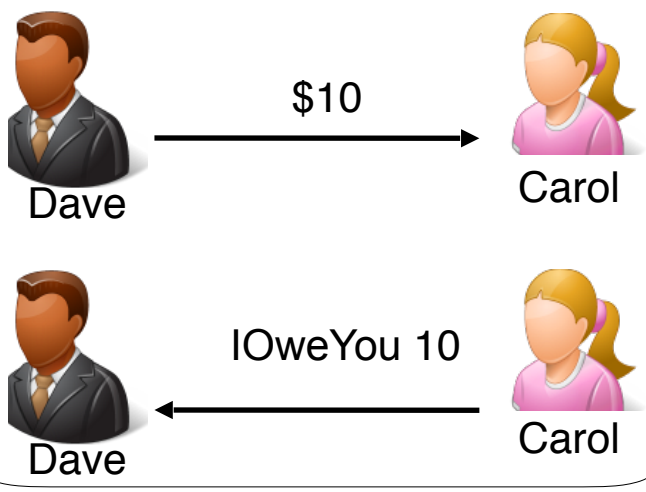


Credit (or IOU settlement) Networks: Basics

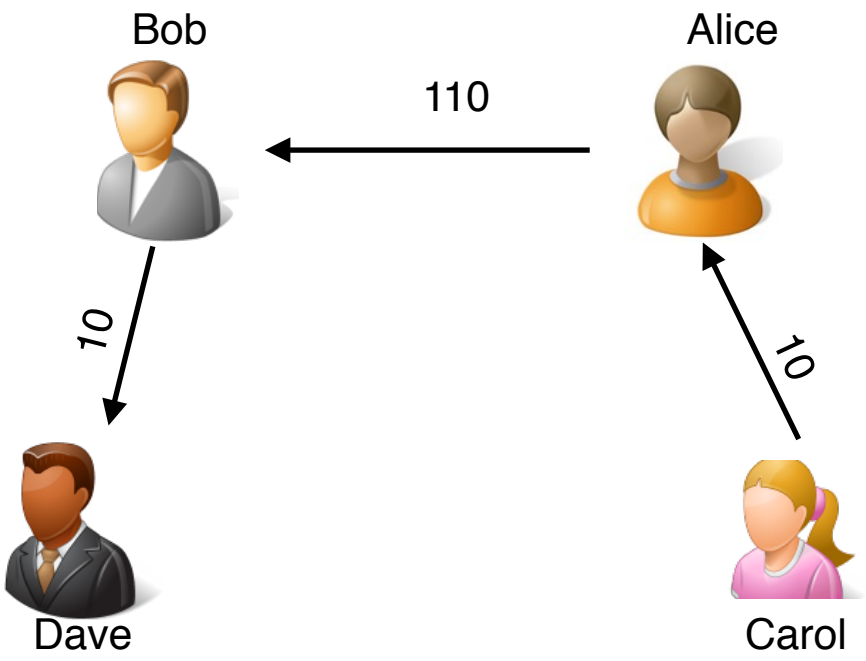
Transactions in the real world



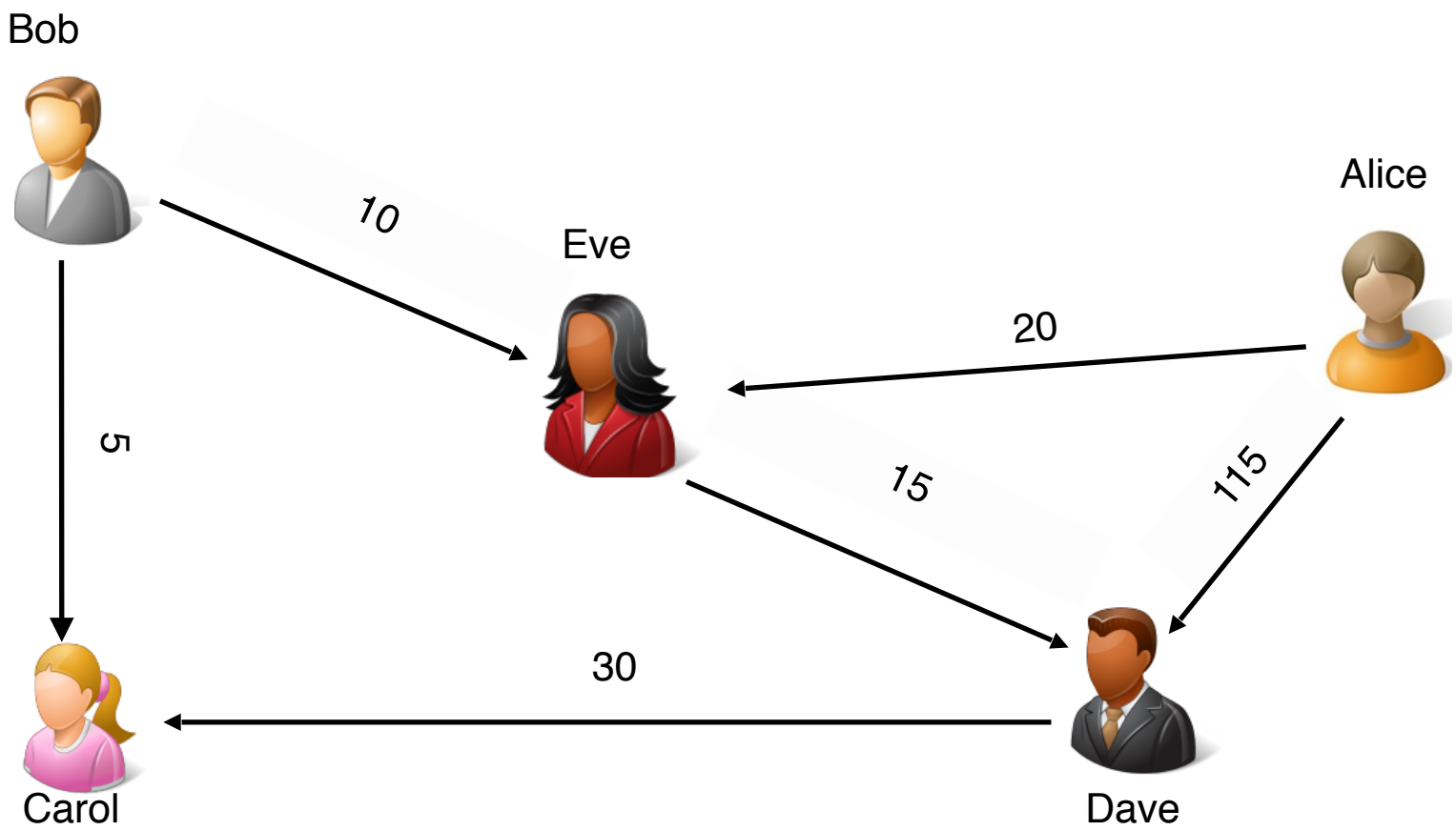
During a hike with Alice & Bob



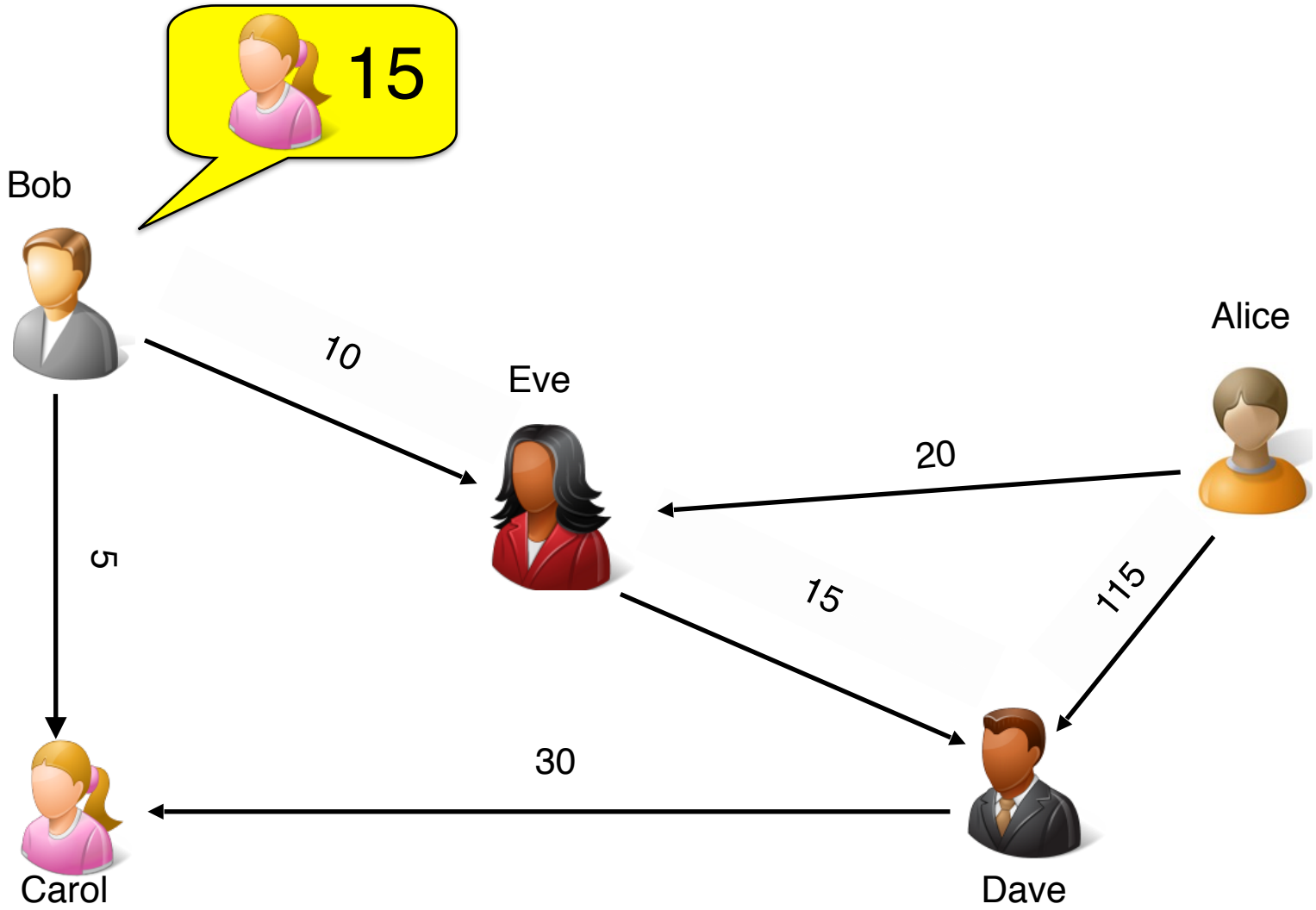
A credit network representation



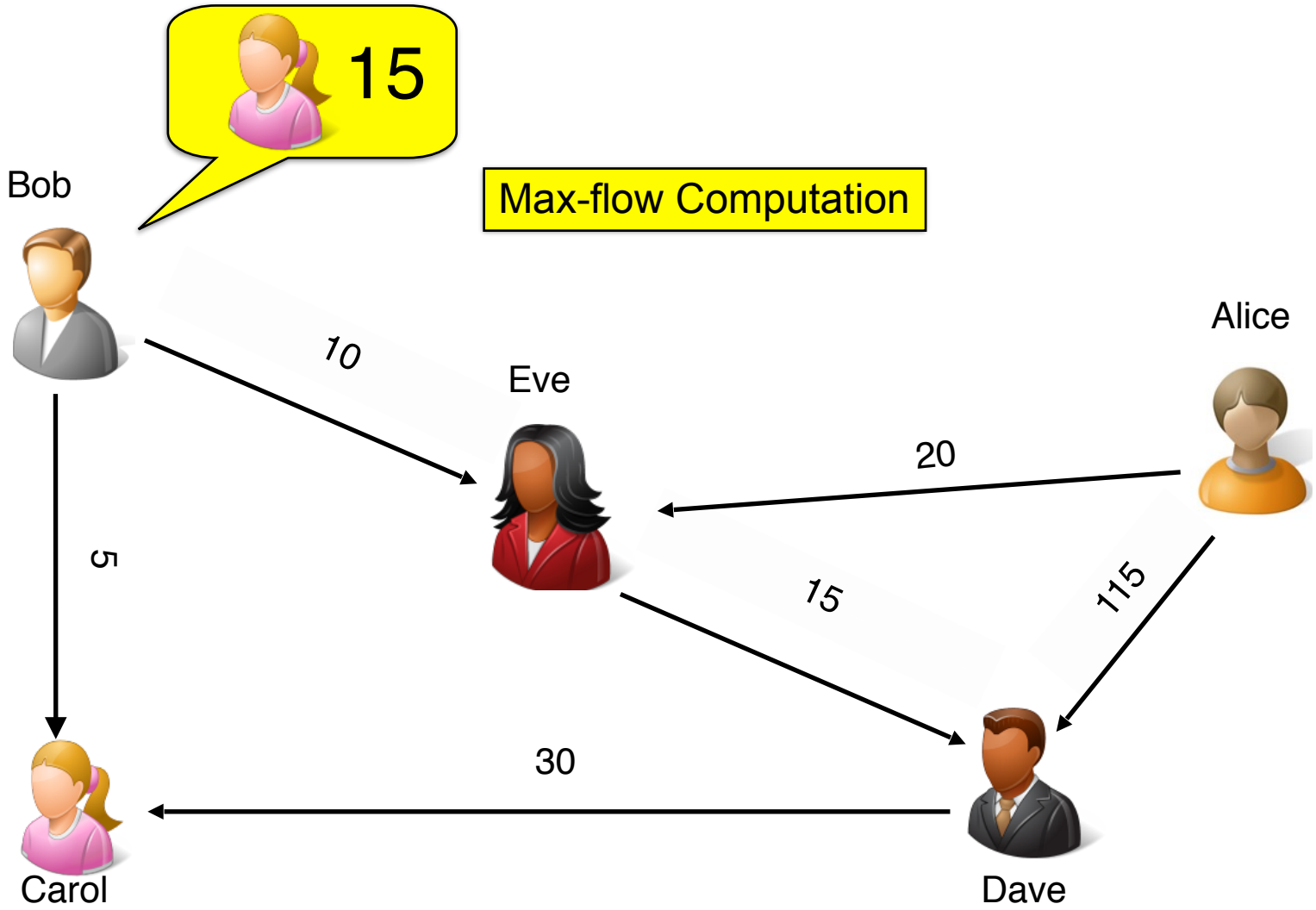
Payment (or credit) Network: an Example



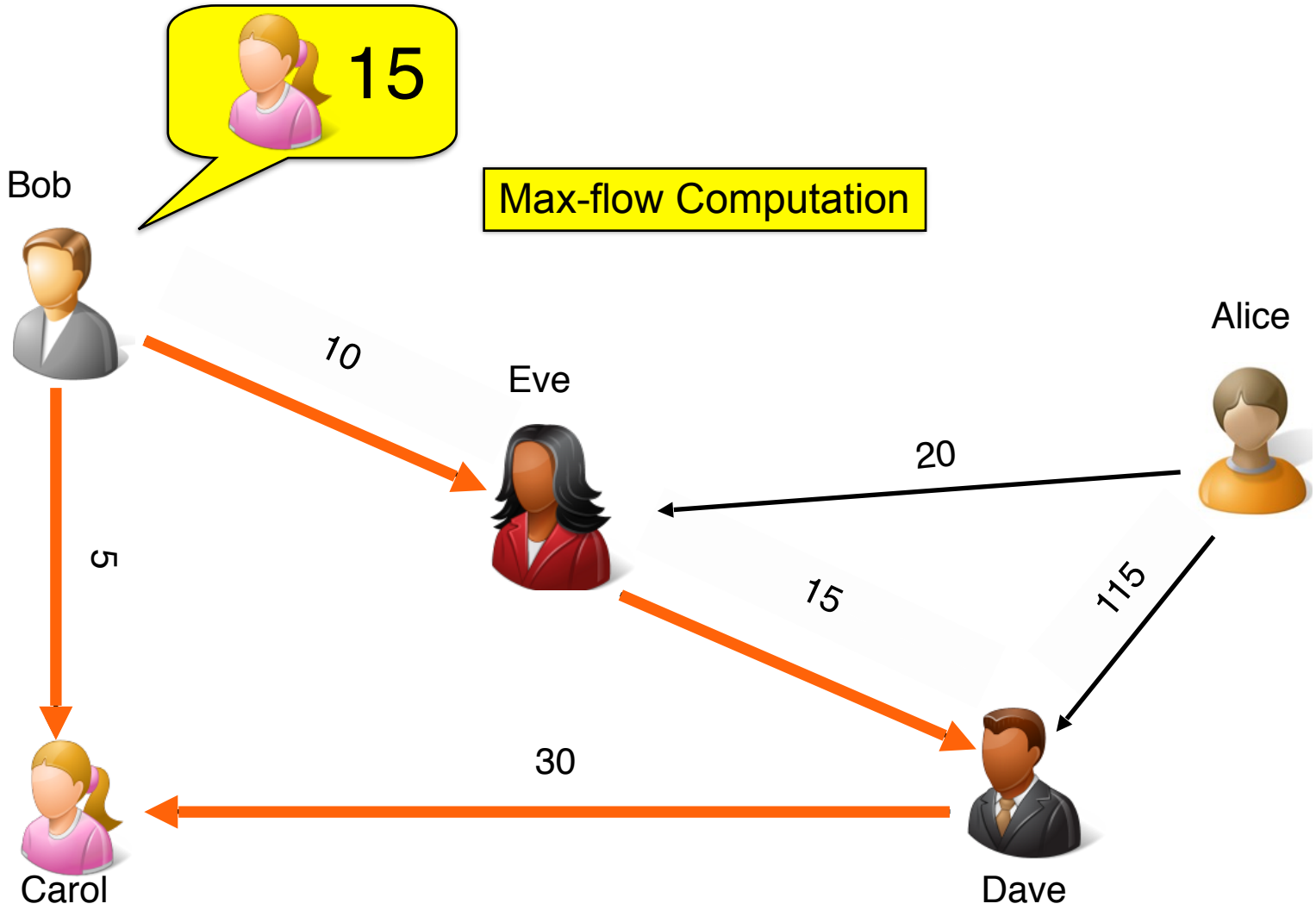
Payment (or credit) Network: an Example



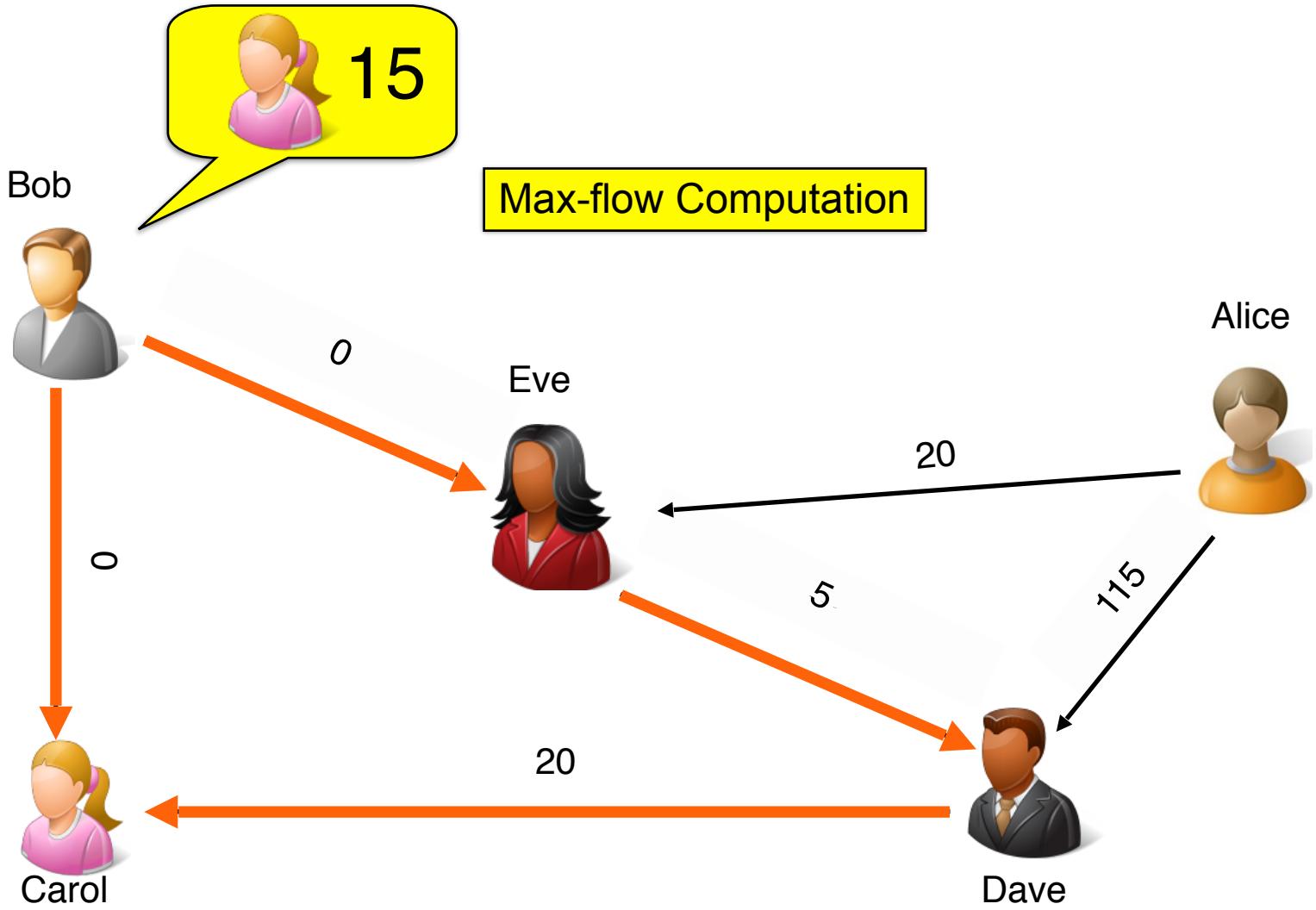
Payment (or credit) Network: an Example



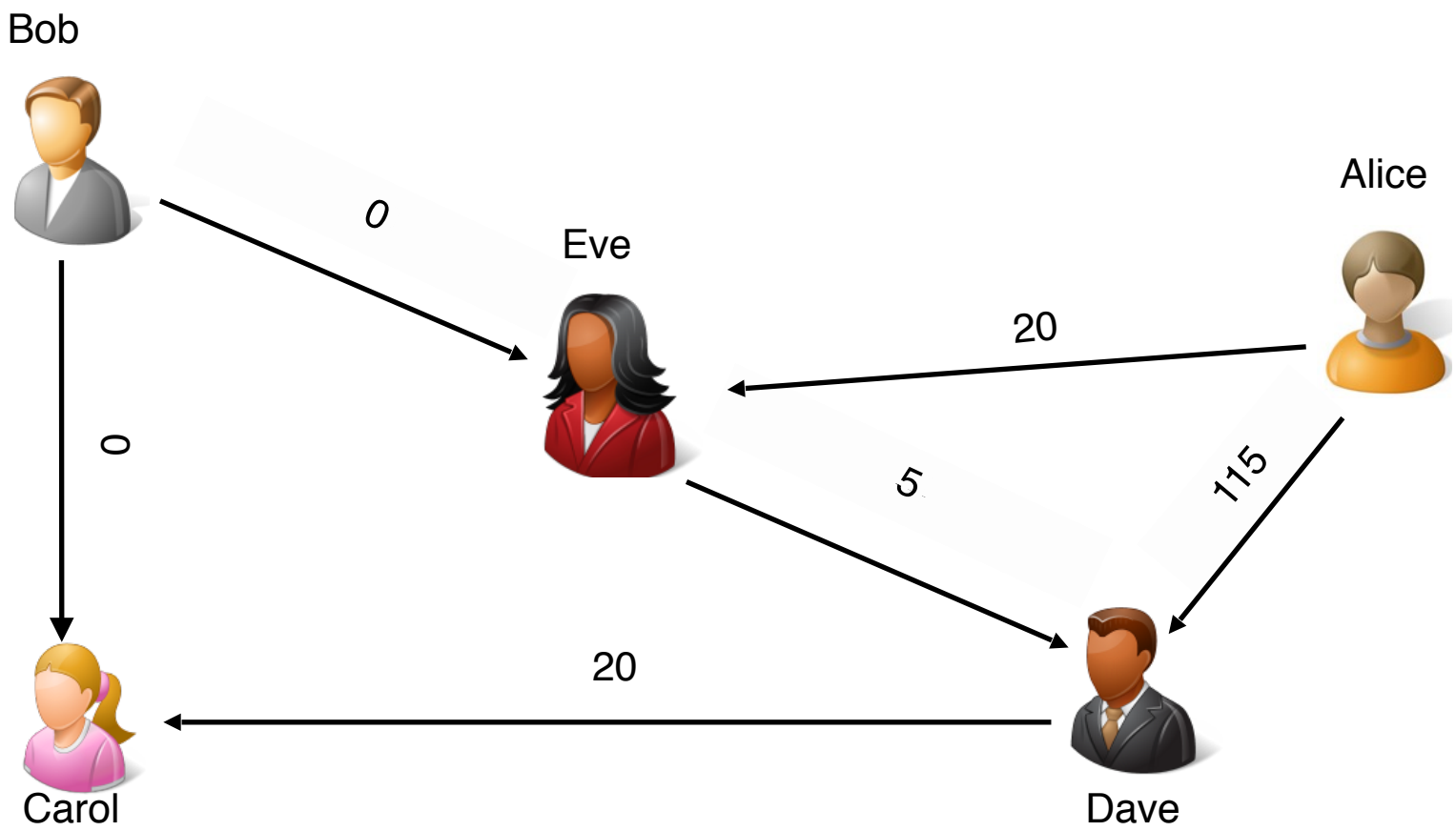
Payment (or credit) Network: an Example



Payment (or credit) Network: an Example



Payment (or credit) Network: an Example



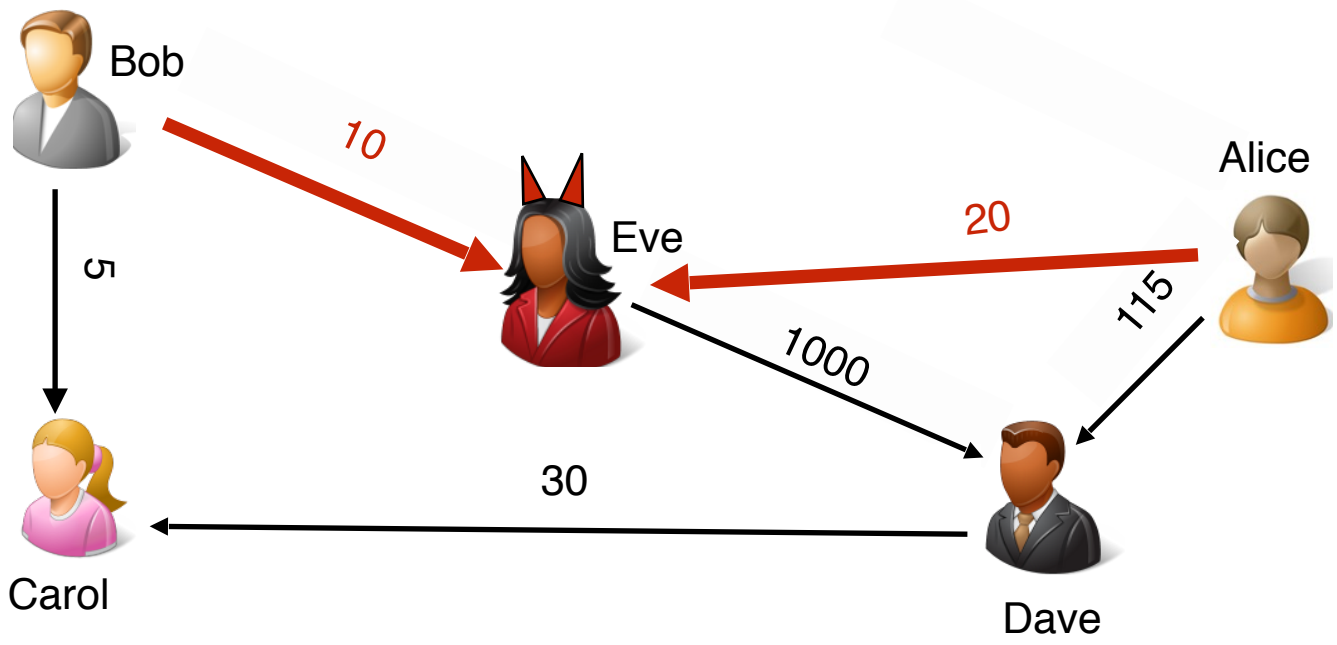
Why credit networks matter?

PURDUE UNIVERSITY

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

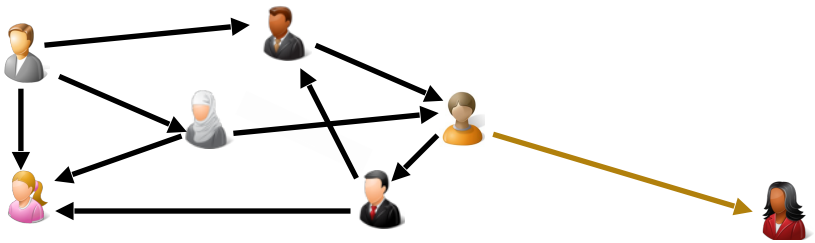
Why credit networks matter?

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



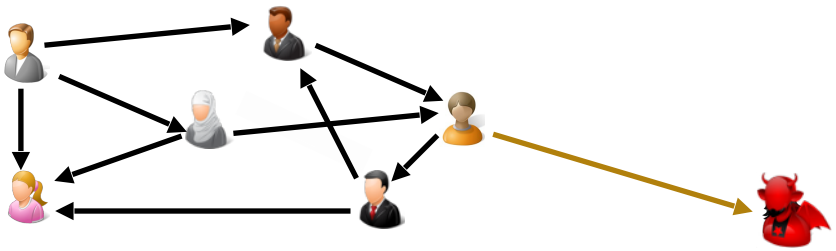
Building trust with credit networks

- Sybil-resistant applications



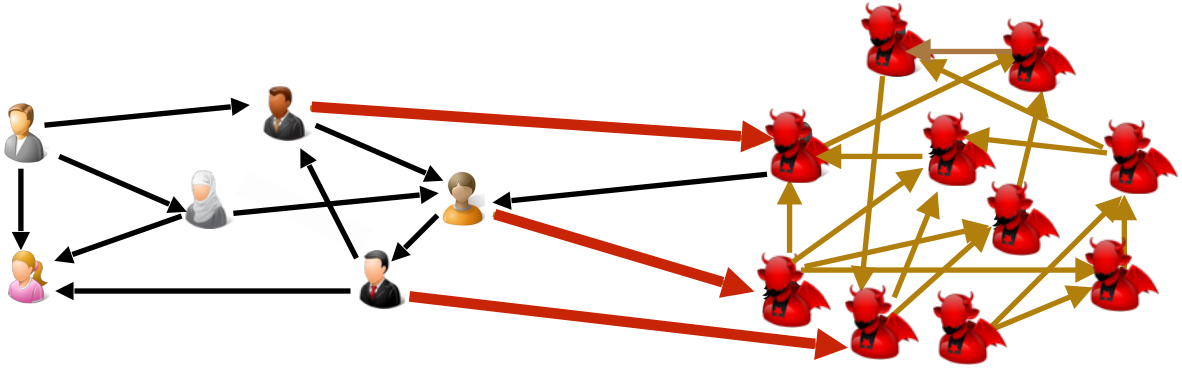
Building trust with credit networks

- Sybil-resistant applications



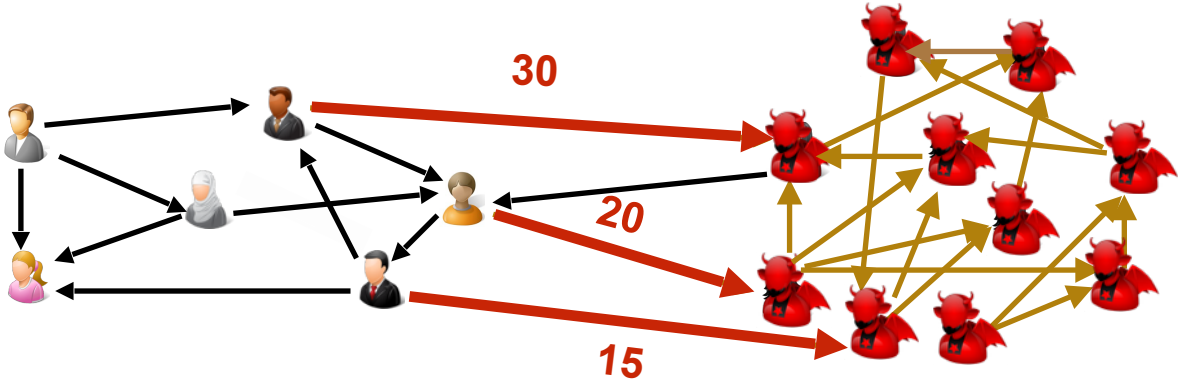
Building trust with credit networks

- Sybil-resistant applications



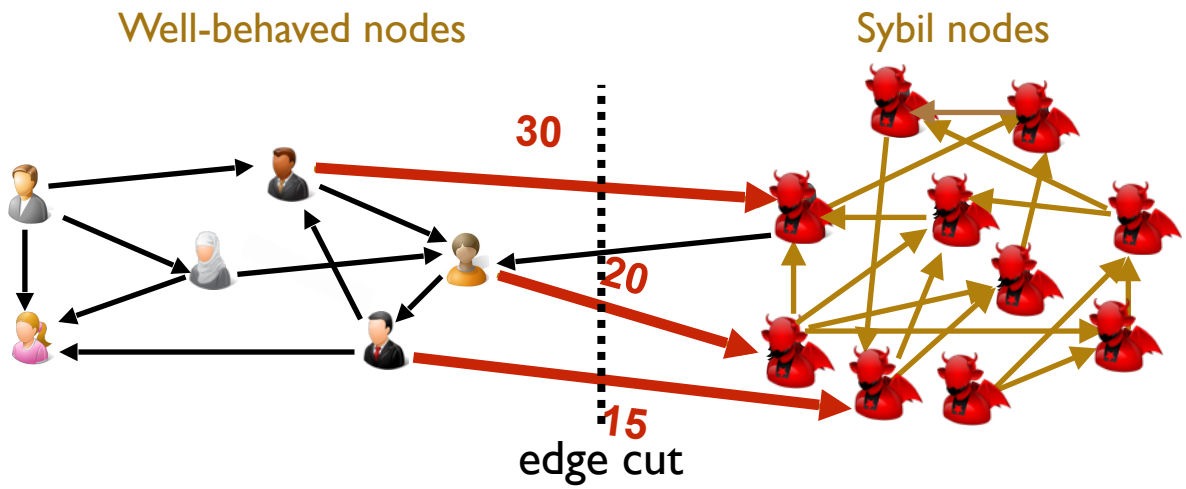
Building trust with credit networks

- Sybil-resistant applications



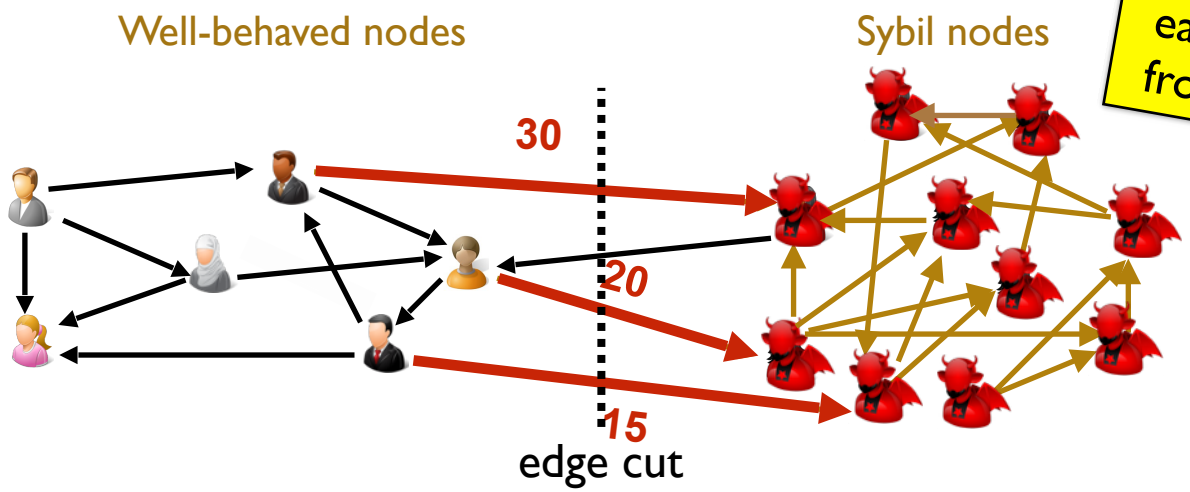
Building trust with credit networks

- Sybil-resistant applications



Building trust with credit networks

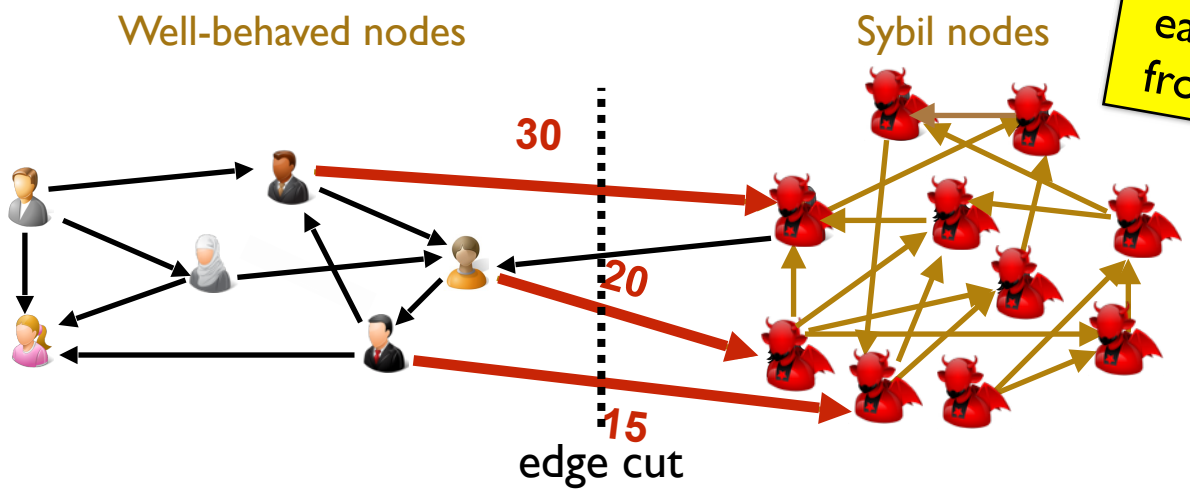
- Sybil-resistant applications



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

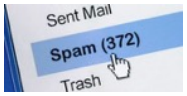
Building trust with credit networks

- Sybil-resistant applications



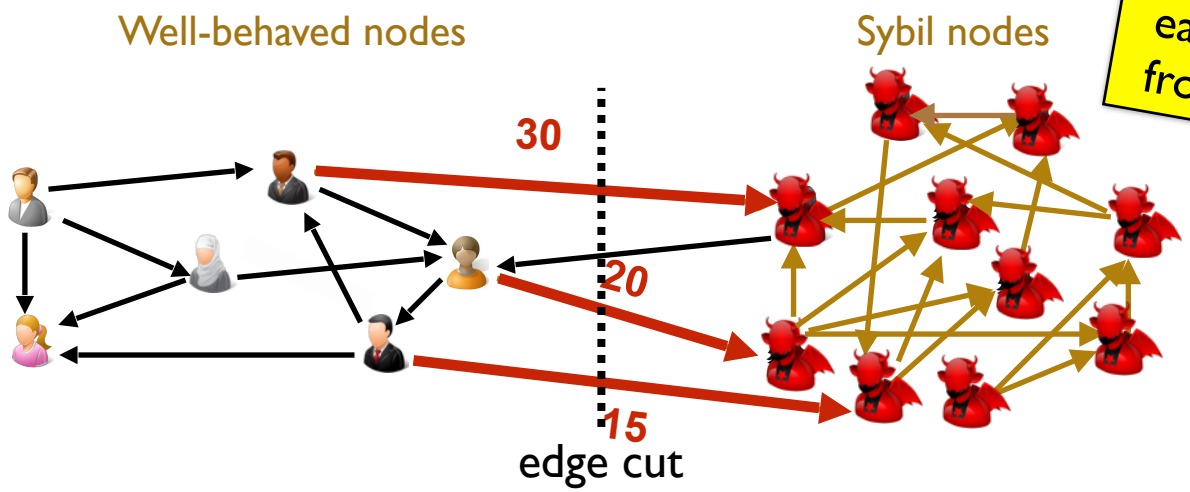
Introducing nodes is much easier than drawing trust from well-behaved nodes

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



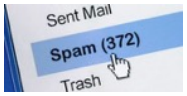
Building trust with credit networks

- Sybil-resistant applications



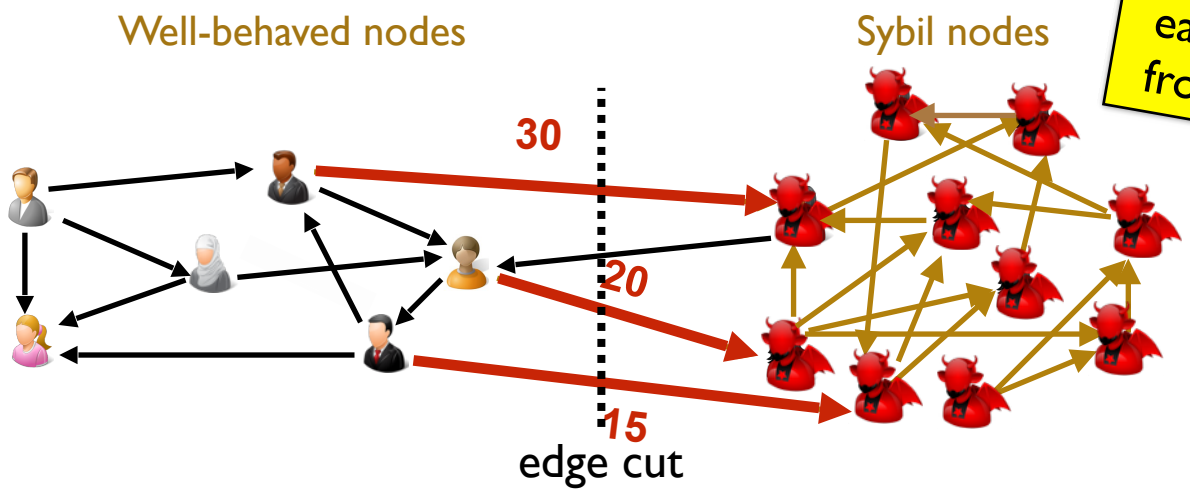
Introducing nodes is much easier than drawing trust from well-behaved nodes

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



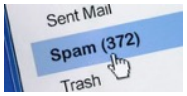
Building trust with credit networks

- Sybil-resistant applications



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

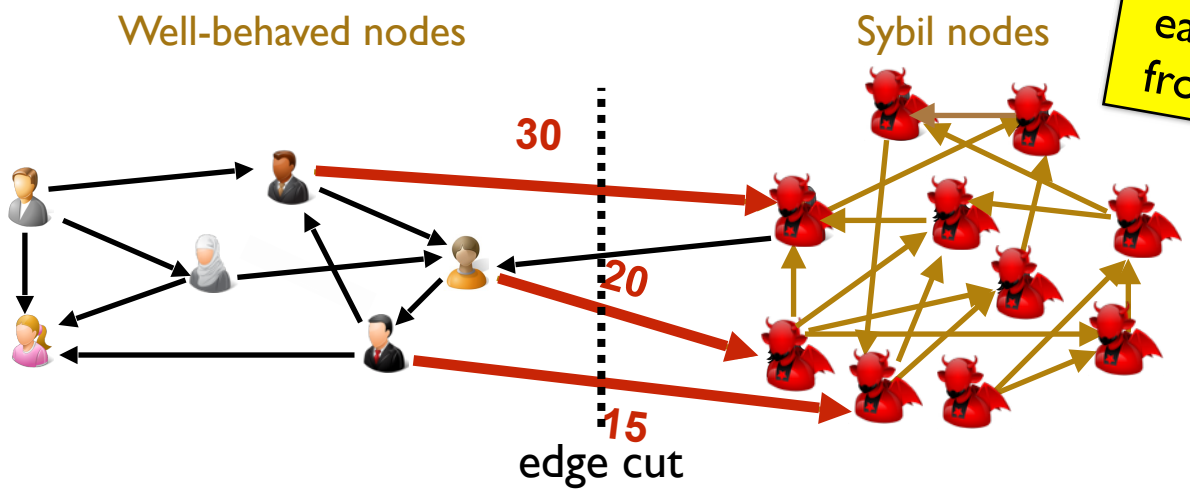
- Several Systems
  - Ostra: preventing e-mail spam [NSDI'08]
  - Bazaar: strengthening e-commerce [NSDI'11]
  - SumUp: Sybil-resilient content voting [NSDI'09]



Building trust with credit networks

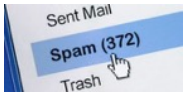
PURDUE UNIVERSITY

- Sybil-resistant applications

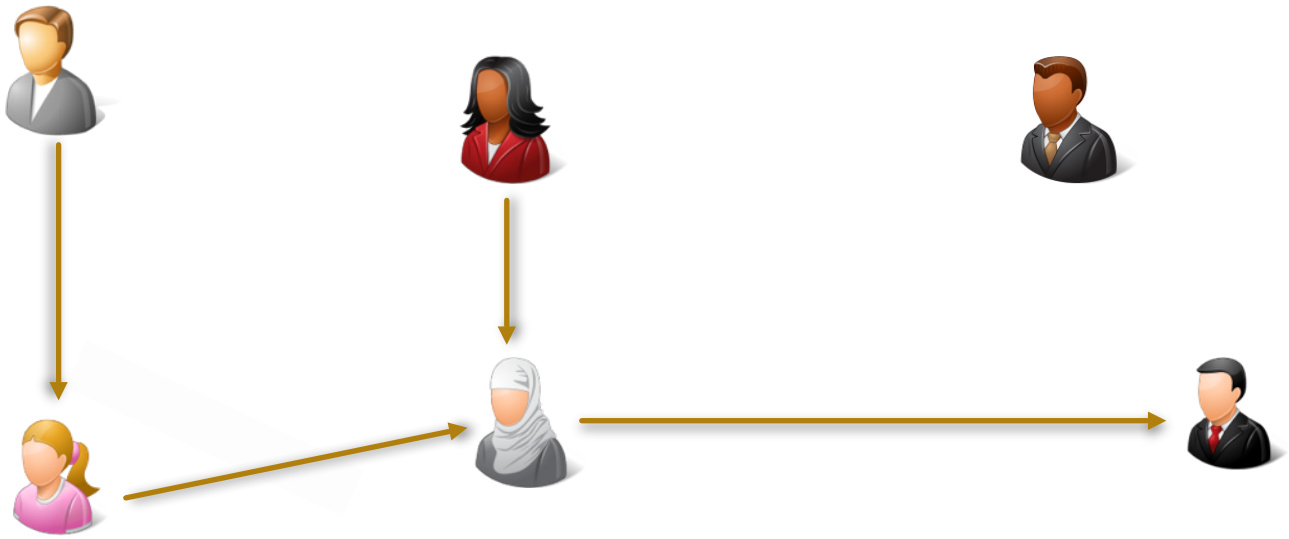


Introducing nodes is much easier than drawing trust from well-behaved nodes

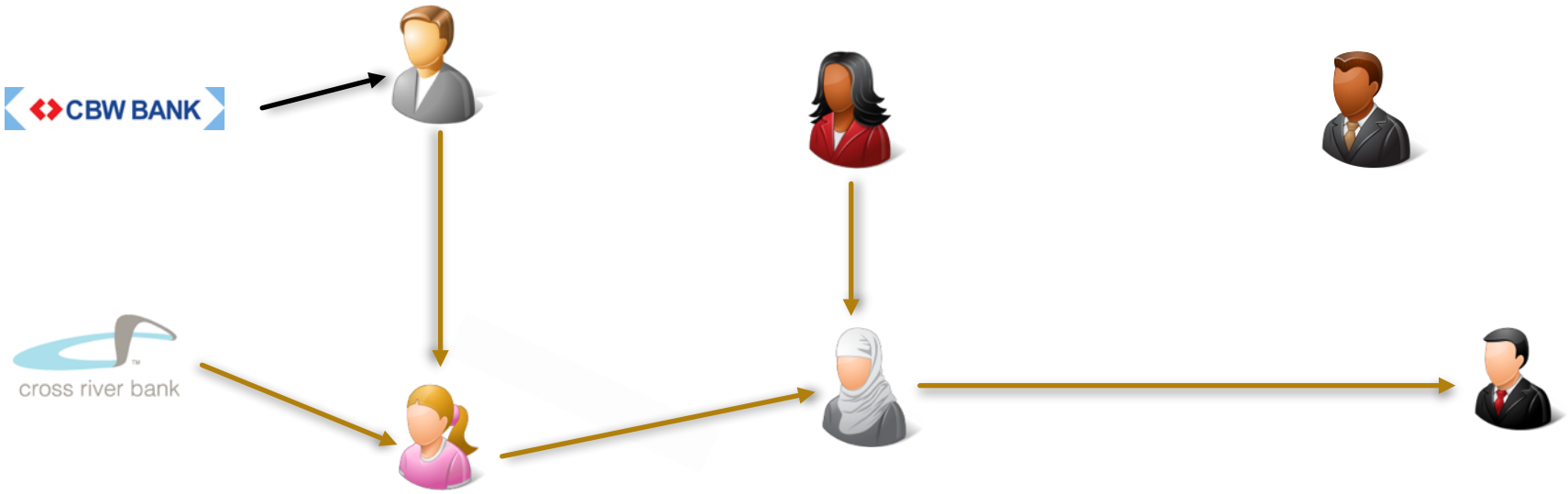
- Several Systems
  - Ostra: preventing e-mail spam [NSDI'08]
  - Bazaar: strengthening e-commerce [NSDI'11]
  - SumUp: Sybil-resilient content voting [NSDI'09]
  - Ripple: A real-life online settlement network



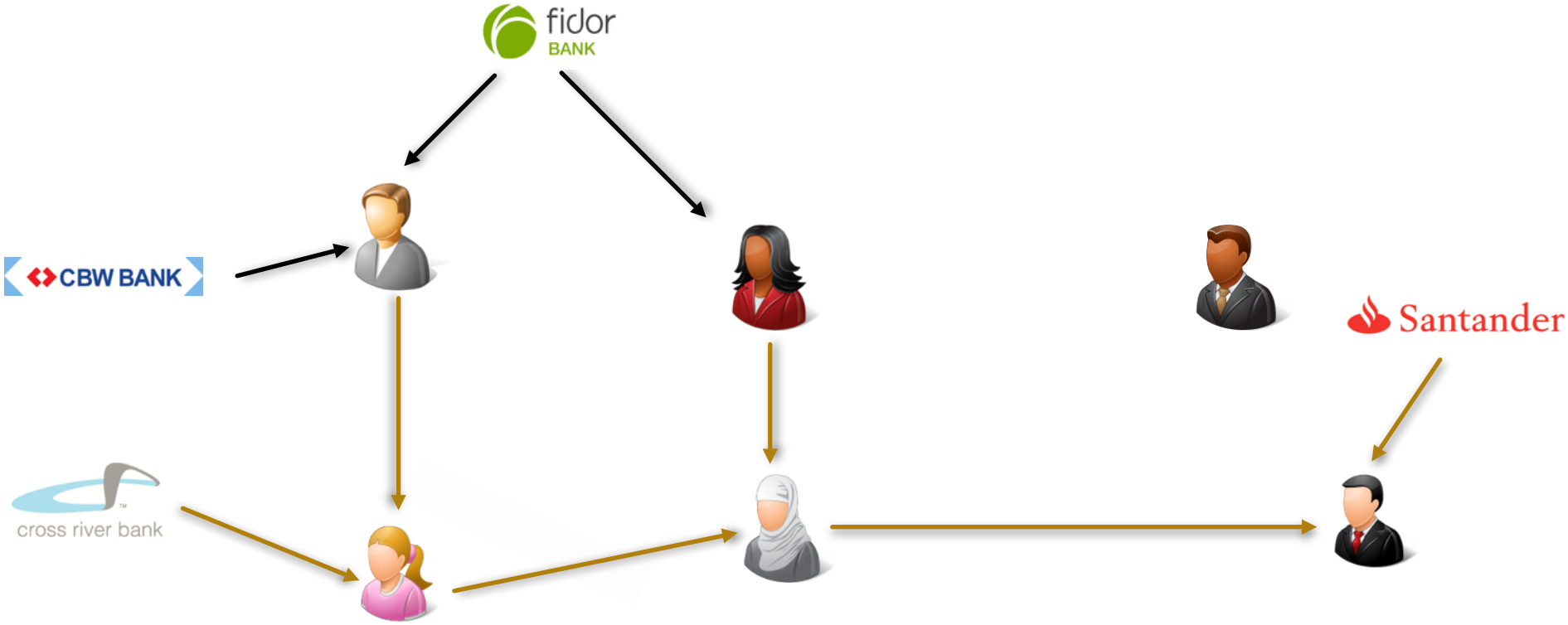
Ripple Credit (or Settlement) Network



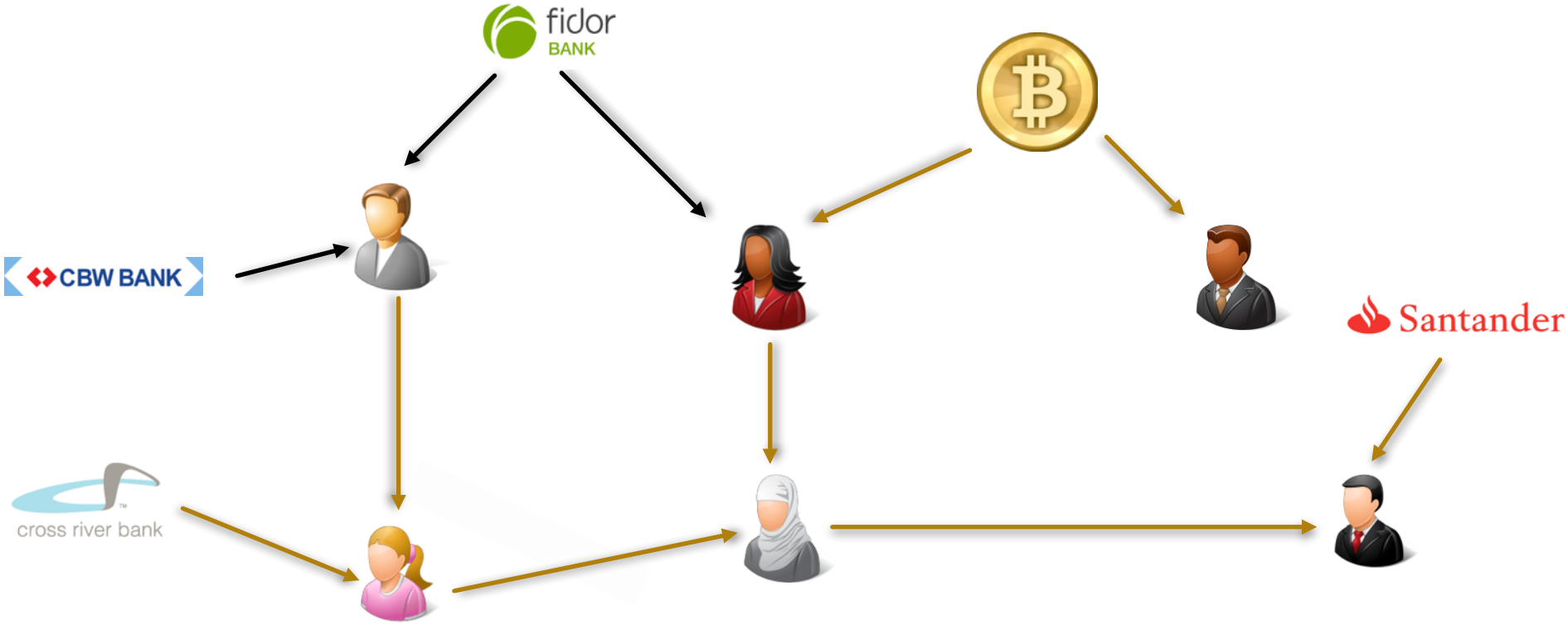
Ripple Credit (or Settlement) Network



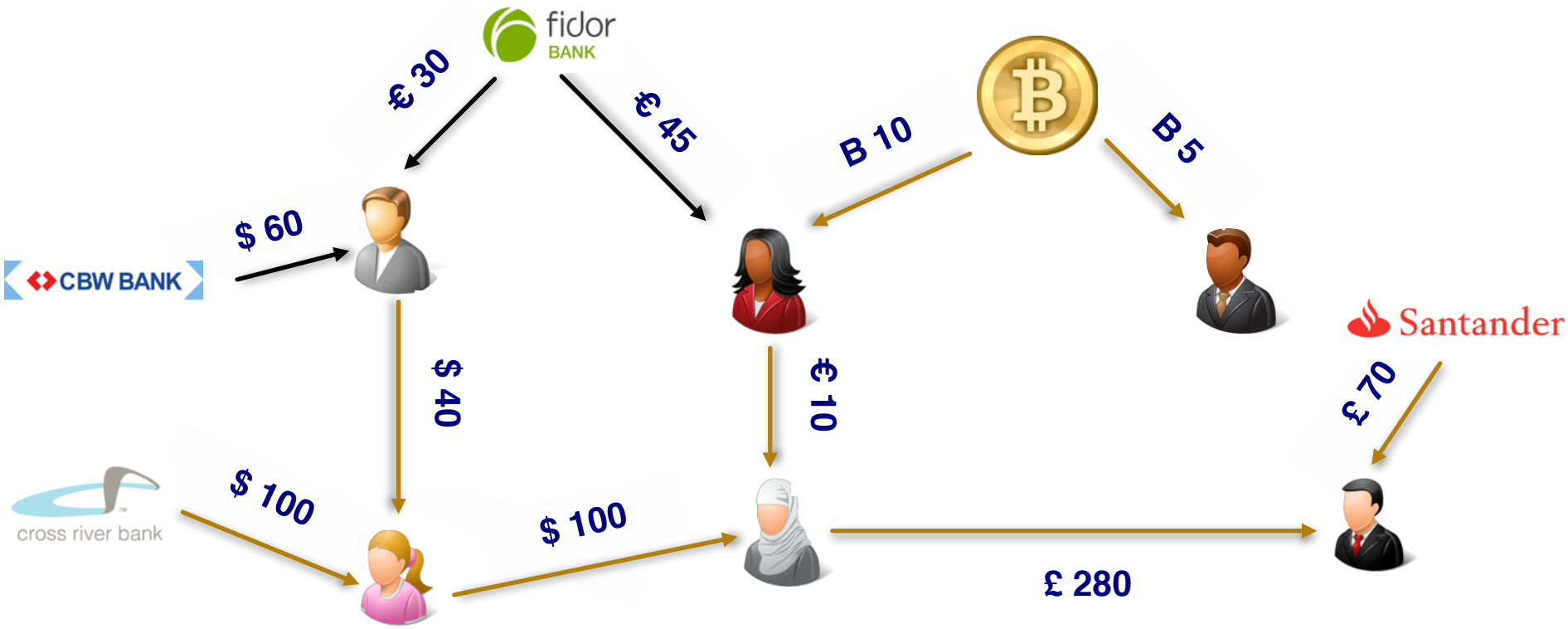
Ripple Credit (or Settlement) Network



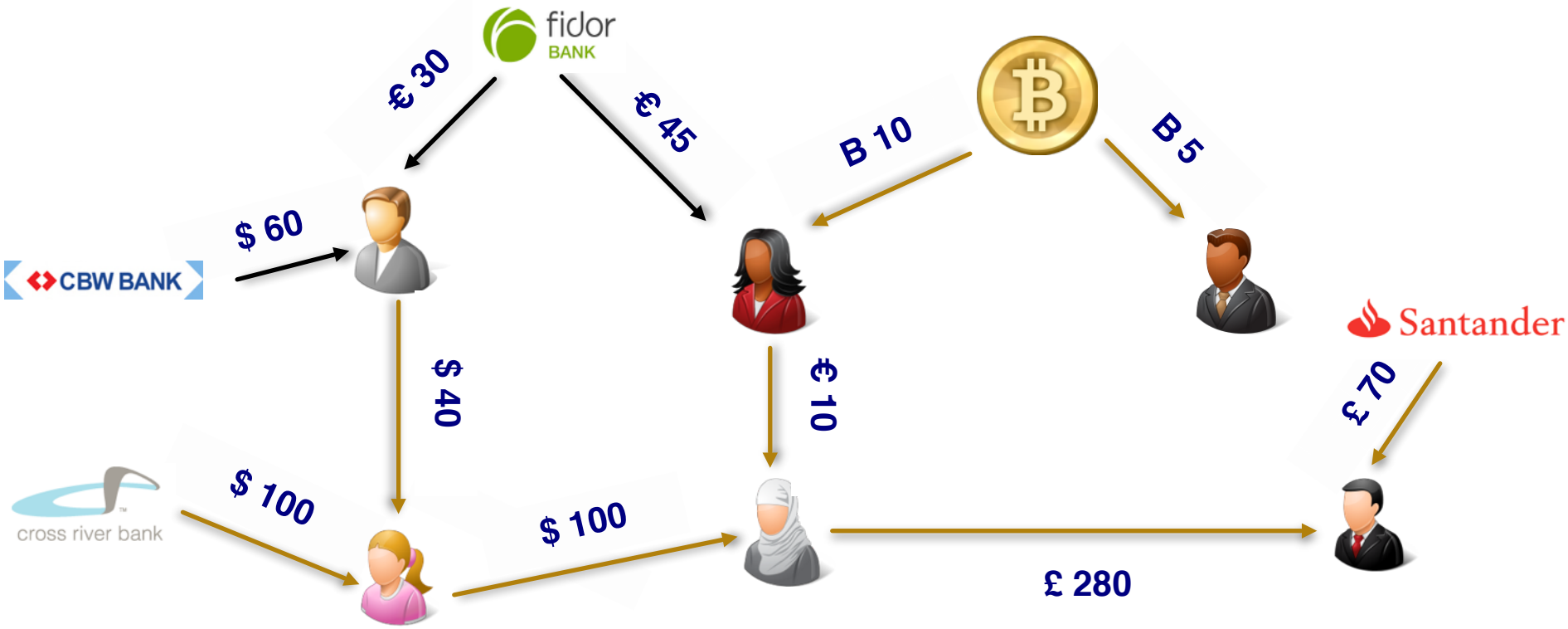
Ripple Credit (or Settlement) Network



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 vs Bitcoin

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

Ripple vs Bitcoin

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

Definition	Currency	Transaction network
Transfer of funds	Direct transactions between any two wallets	Transactions only via a path with enough credit
Scalability	Limited transaction rate (<100 tps)	Highly scalable

Ripple vs Bitcoin

PURDUE UNIVERSITY

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

Definition	Currency	Transaction network
Transfer of funds	Direct transactions between any two wallets	Transactions only via a path with enough credit
Scalability	Limited transaction rate (<100 tps)	Highly scalable

Public verifiability of transactions

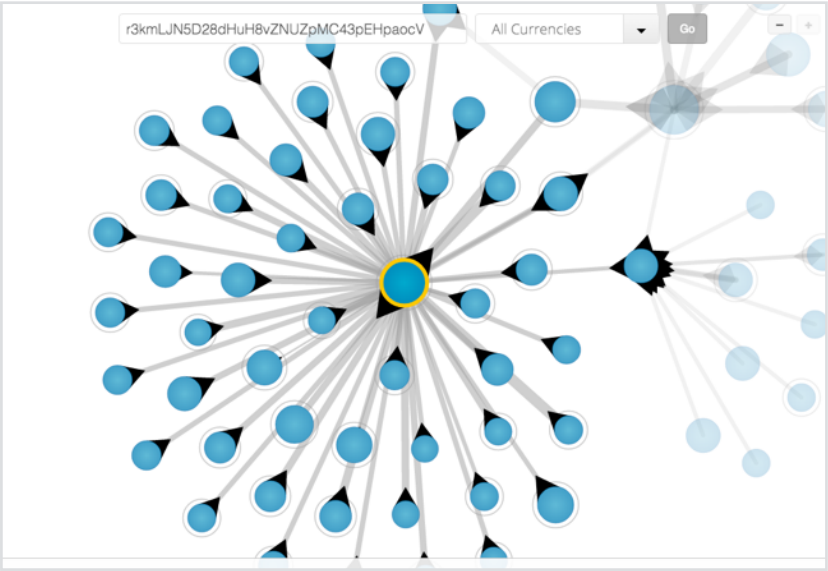
Attacks on privacy of Ripple links & transactions

PURDUE UNIVERSITY

Transaction Details

Account	Destination	Amount
rwvctTPLKZqK59f1fXpDkQ…	rMnVZ9maUWp5cAvmqBECZM…	300/XRP
rLSBpSquSHKbbfvcKt1c54…	rKoDt7VL83AKJZewLxVZEs…	75/XRP
r428G9fSSmD4SYmnDra16B…	rBeToNo4AwHaNbRX2n4BNC…	0.0693402709148/CCK/rB…
rhD759dbJMrzMNL4QbvQe9…	r95pWKA1K55fy7EJWrqJ9b…	300/XRP
r42WJGvV9MJa4t5QcF8Cnx…	rBeToNo4AwHaNbRX2n4BNC…	0.0821058028231/CCK/rB…
rUnr1p7xkuSBxyAqHEopZ5…	r3H4rynDShFMRKWuJcadLY…	1129.916679154465/EUR/…
rw7UfGvzCeZwJxxUEeZHLG…	rBwgTdzzMHnouLk5DJD3xd…	100/XRP
rpVVzfSTUJX9CrKBSS2Z5W…	rDCgaaSBAWYfsxUYhCk1n2…	999.99/XRP

Credit Graph



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

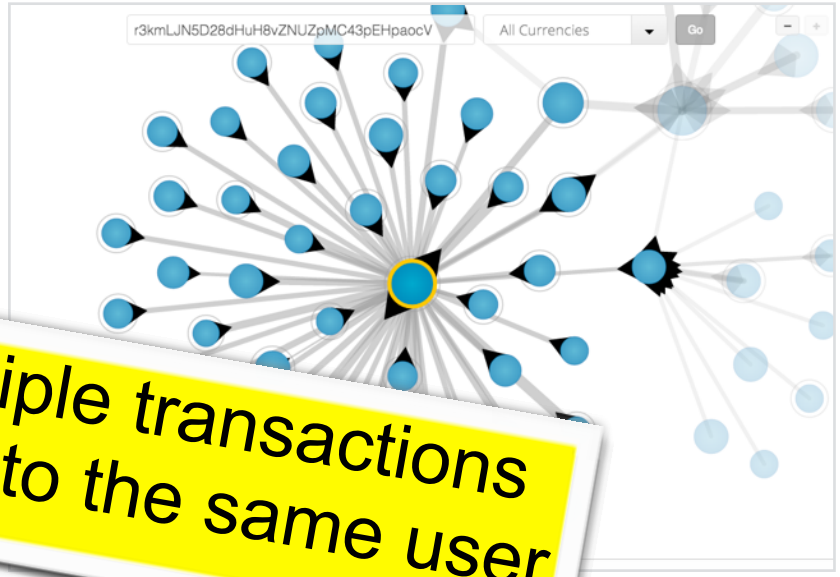
Attacks on privacy of Ripple links & transactions

PURDUE UNIVERSITY

Transaction Details

Account	Destination	Amount
rwvctTPLKZqK59f1fXpDkQ…	rMnVZ9maUWp5cAvmqBECZM…	300/XRP
rLSBpSquSHKbbfvcKt1c54…	rKoDt7VL83AKJZewLxVZEs…	75/XRP
r428G9fSSmD4	rBeToNo4AwHaNbRX2n4BNC…	0.0693402709148/CCK/rB…
rhD759dbJMr		300/XRP
r42WJGvV9M		231/CCK/rB…
rUnr1p7xku		
rw7UfGvzC		
rpVVzfST		

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/

Towards privacy-preserving transactions credit networks

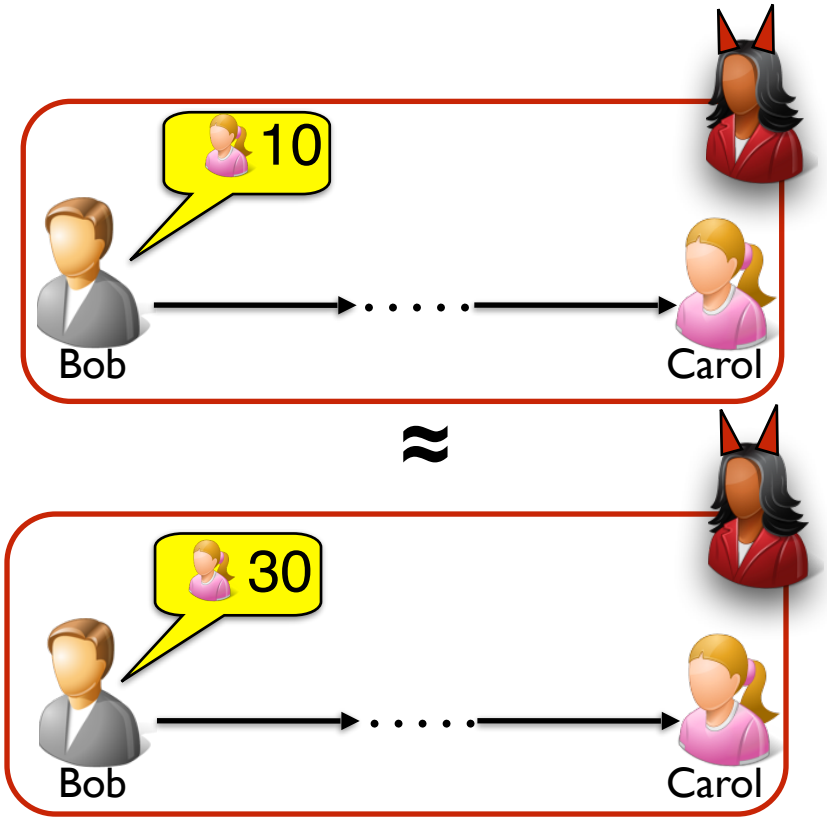
Towards privacy-preserving transactions credit networks

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

Defining privacy for a credit network

Defining privacy for a credit network

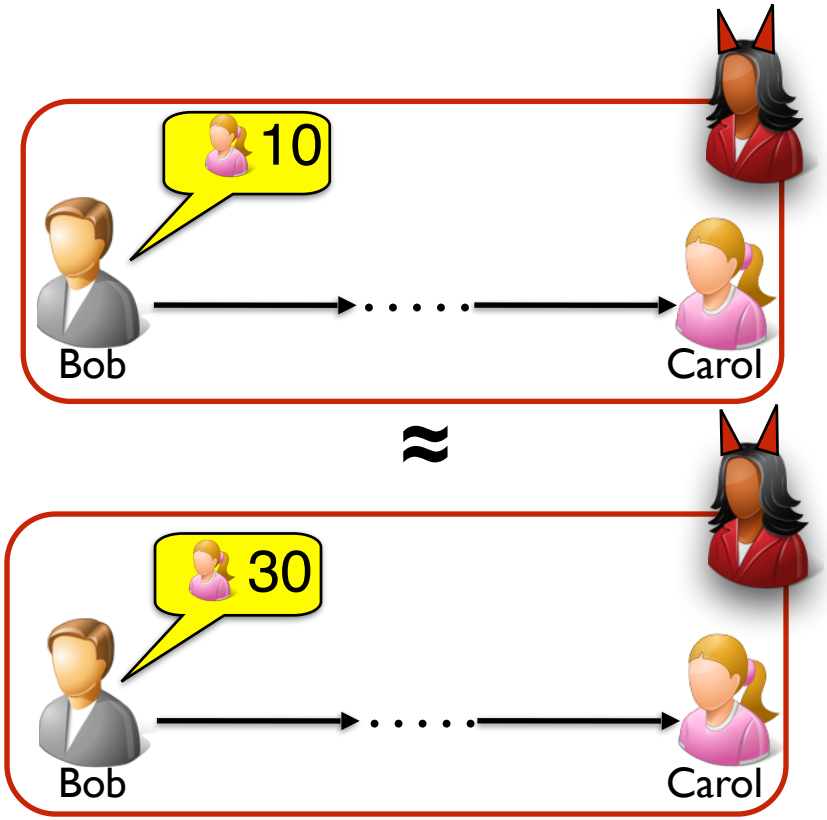
Transaction value privacy



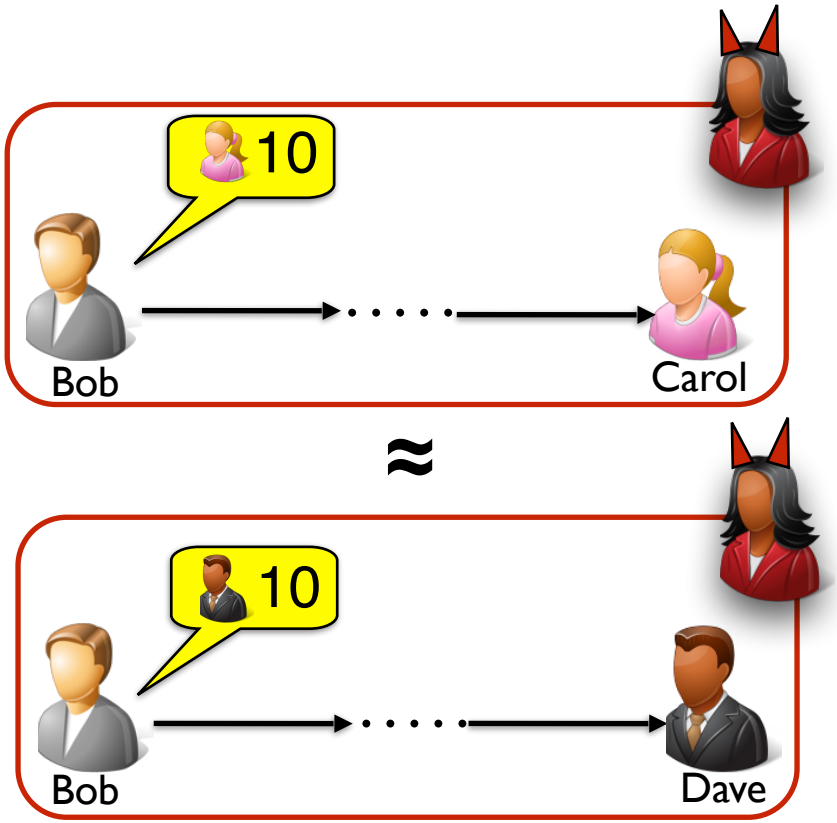
Defining privacy for a credit network

PURDUE UNIVERSITY

Transaction value privacy



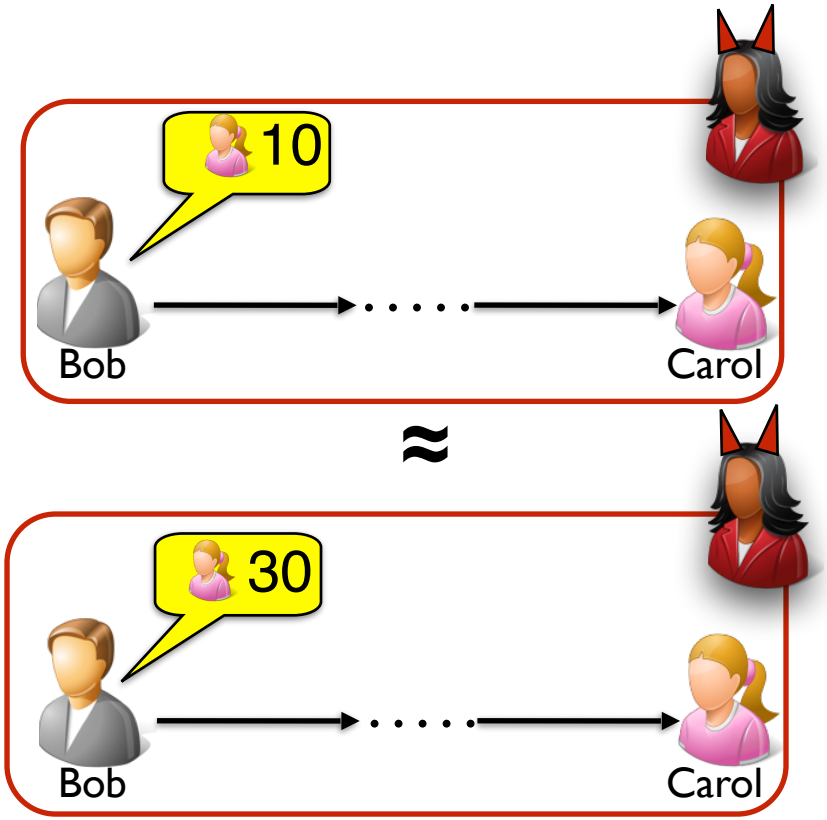
Transaction receiver privacy



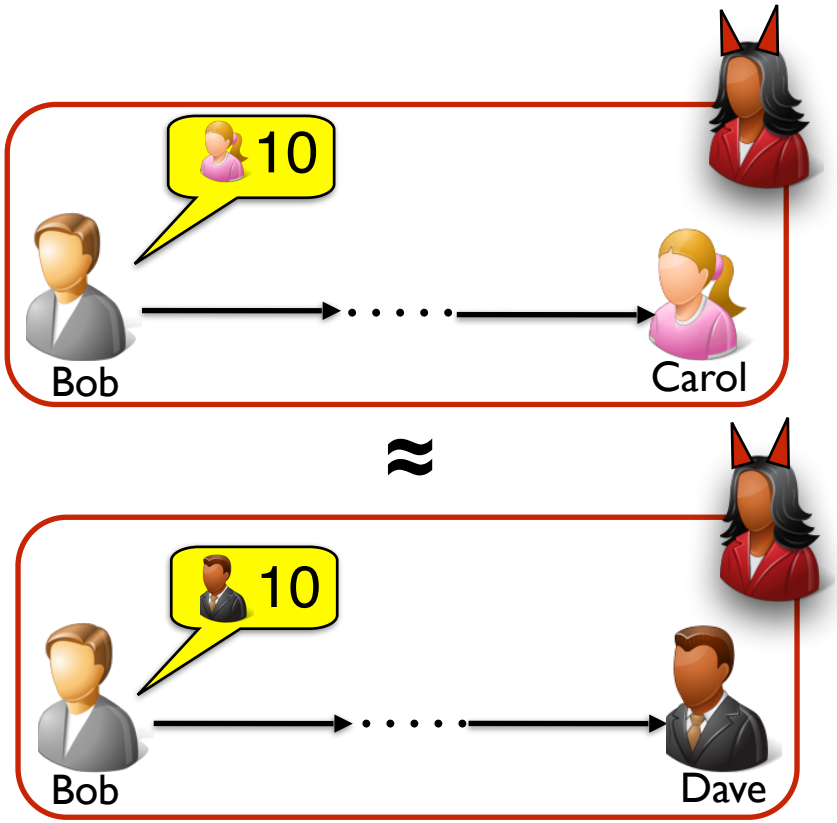
Defining privacy for a credit network

PURDUE UNIVERSITY

Transaction value privacy



Transaction receiver privacy



Transaction sender privacy can be defined similarly

Towards credit network privacy

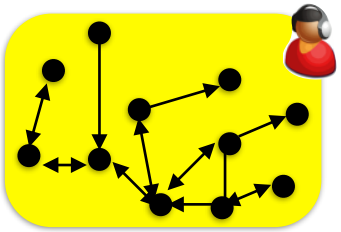
Towards credit network privacy

- A decentralized or centralized architecture?

Towards credit network privacy

- 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

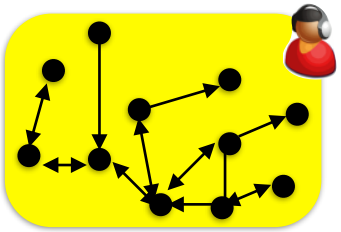


Towards credit network privacy

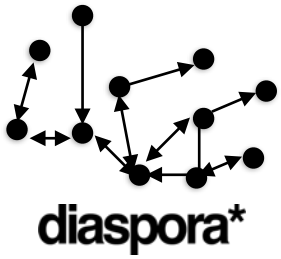
PURDUE UNIVERSITY

- 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

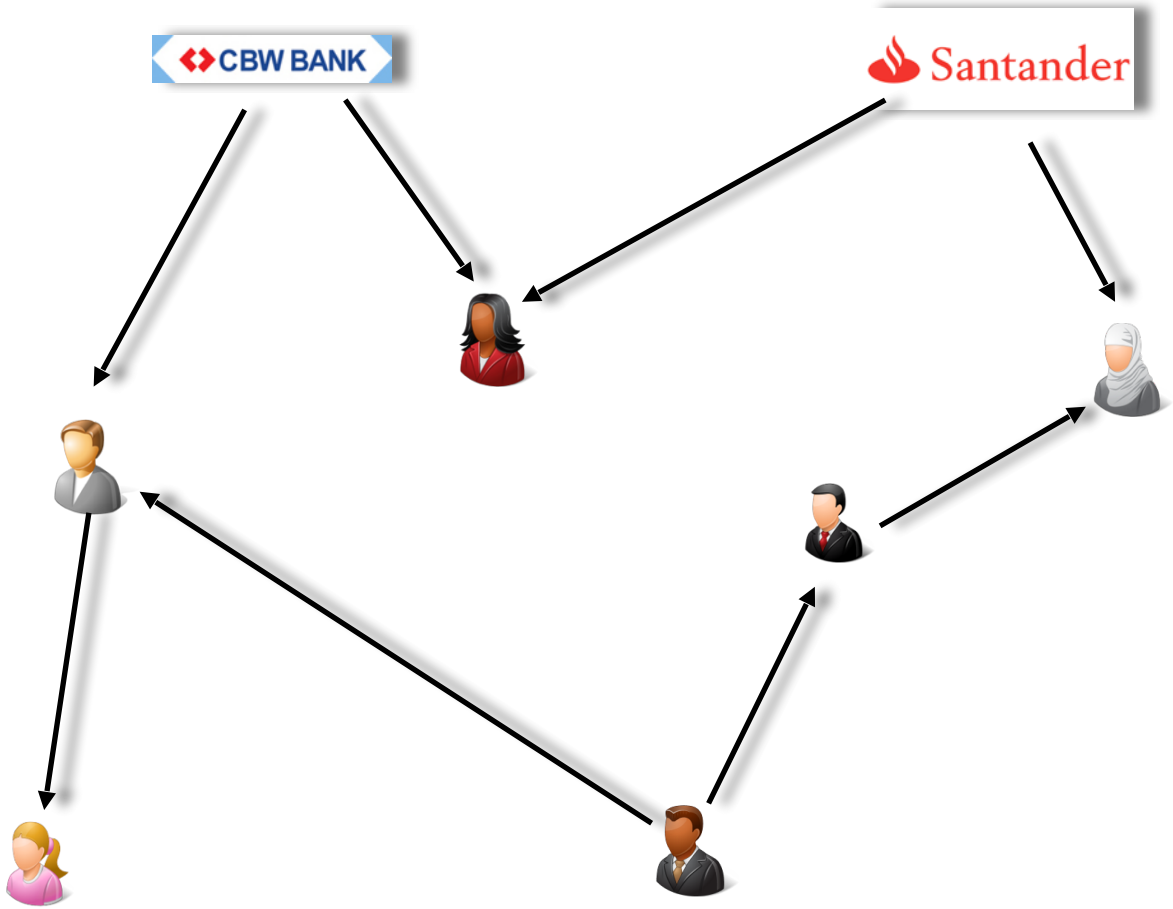


- Decentralized setting: edges are maintained locally
  - A transaction passing through a node requires its active involvement
  - We will focus on this solution in the rest of the talk



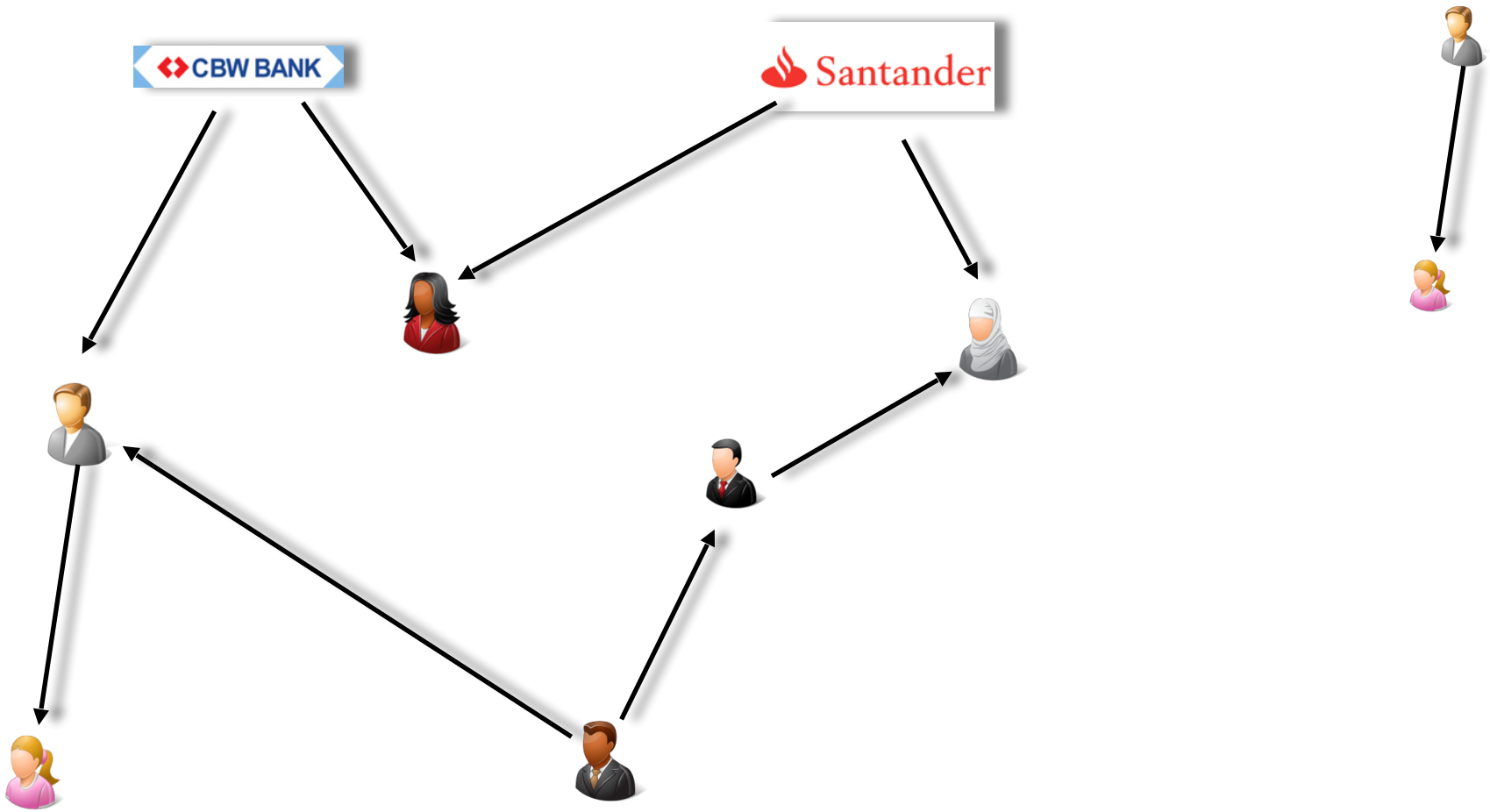
A Distributed Credit Network

- Each user maintains her own credit links



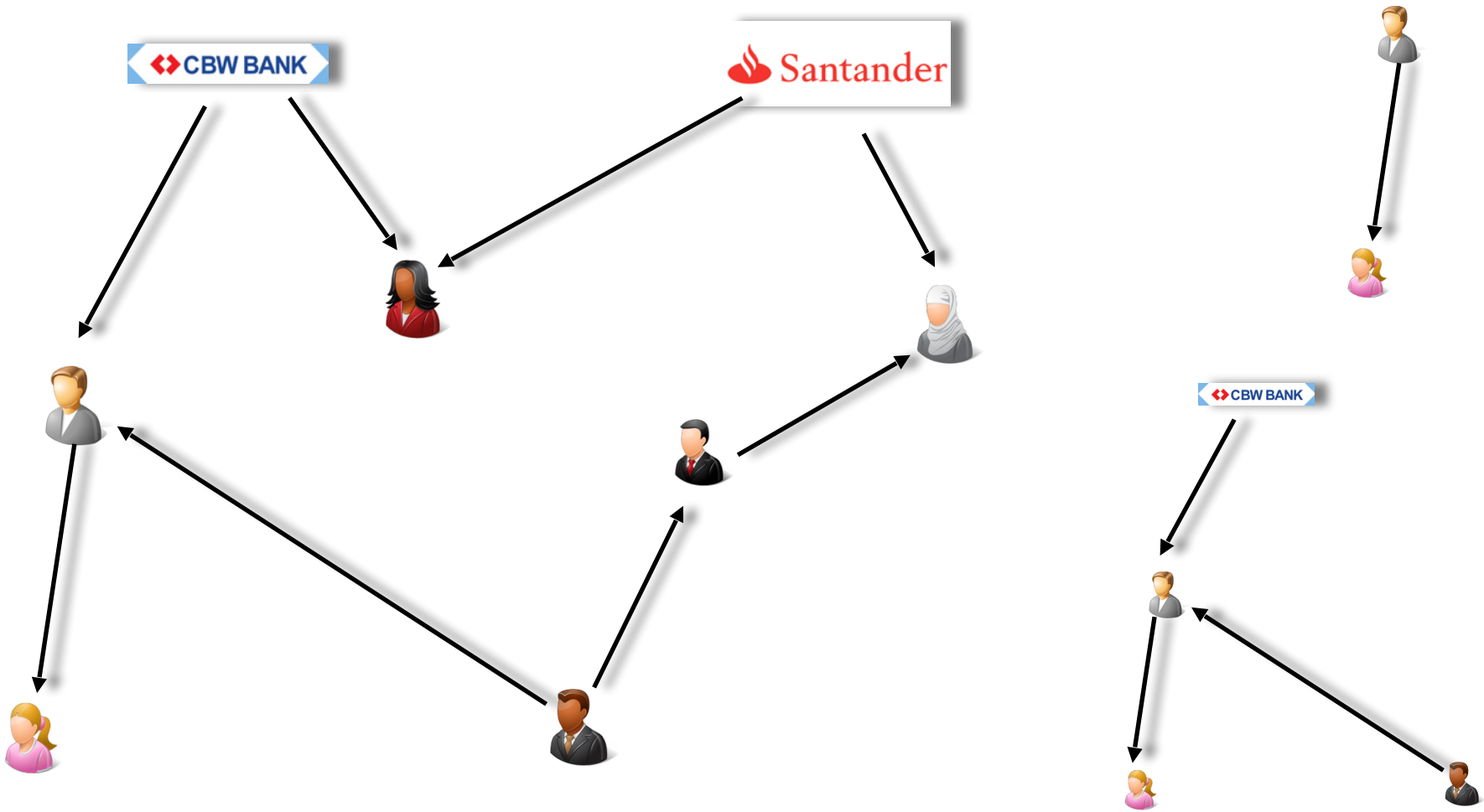
A Distributed Credit Network

- Each user maintains her own credit links



A Distributed Credit Network

- Each user maintains her own credit links

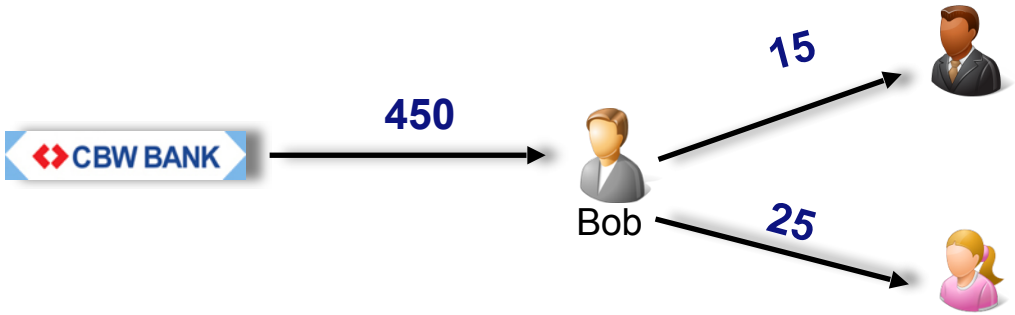


Local Knowledge is Sufficient!

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

Local Knowledge is Sufficient!

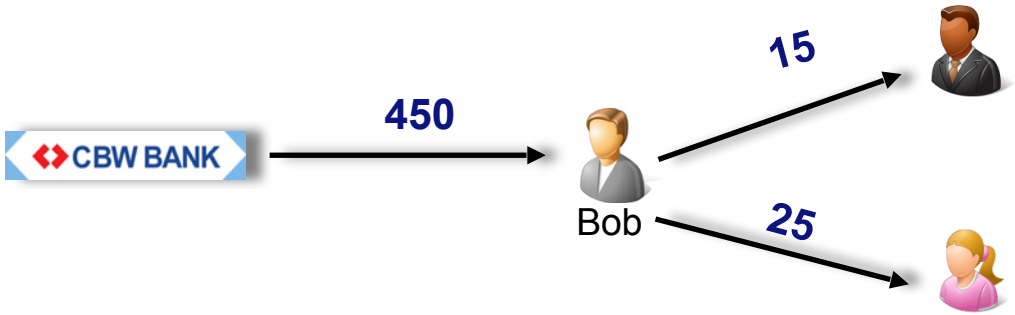
- Credit links of a user determine his credit in the network



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

Local Knowledge is Sufficient!

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

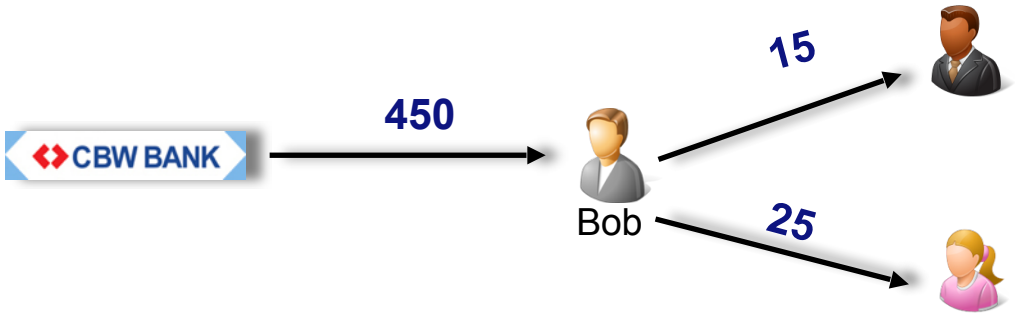


In-flow = 450
Out-flow = 40
Net-flow = 410

- A user checks net-flow does not change

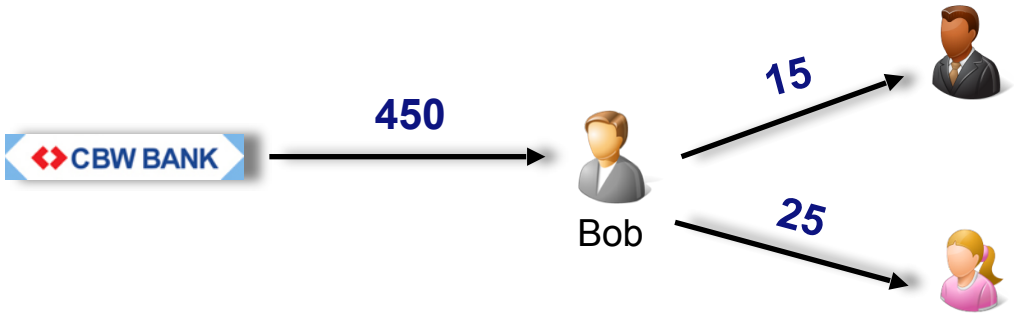
Local Knowledge is Sufficient!

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



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

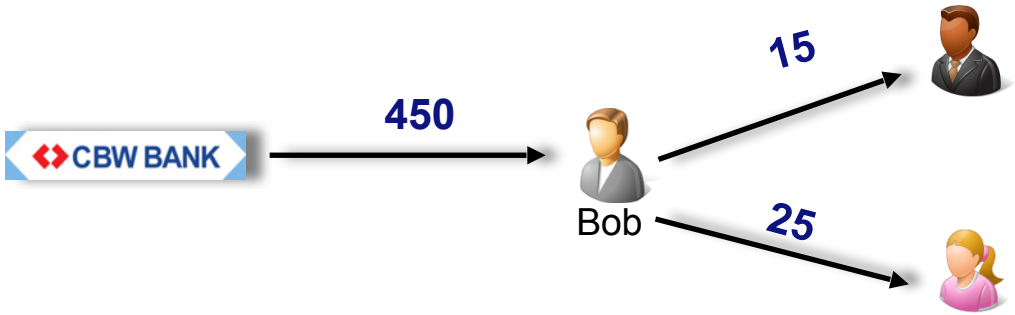
- A user checks net-flow does not change



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

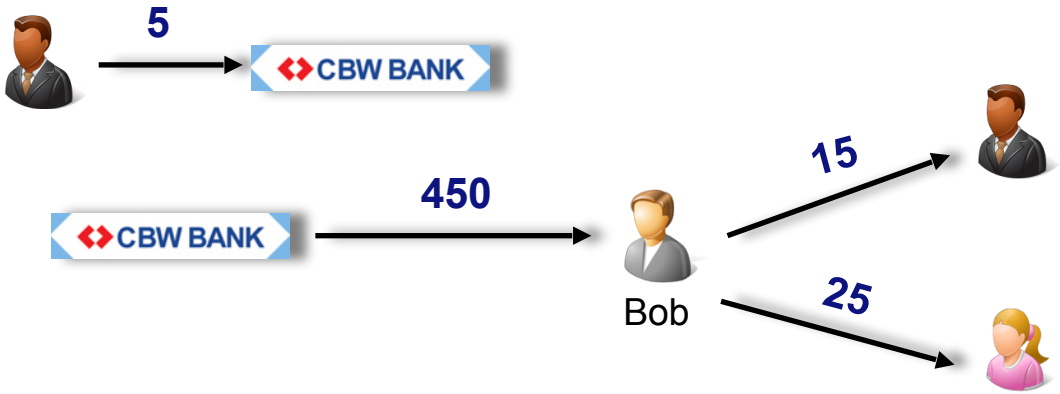
Local Knowledge is Sufficient!

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



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

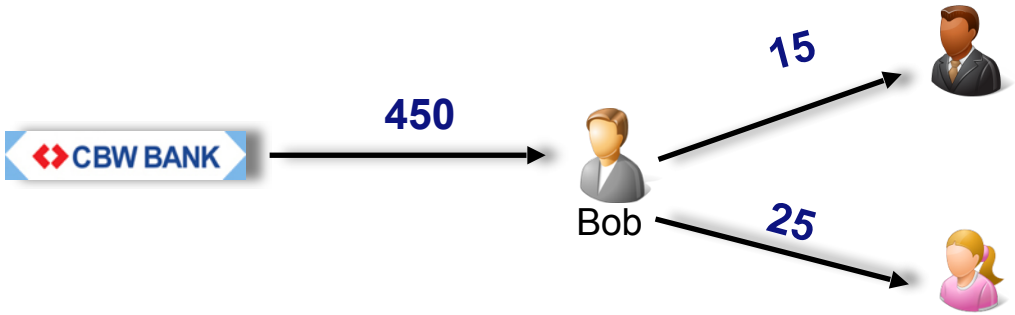
- A user checks net-flow does not change



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

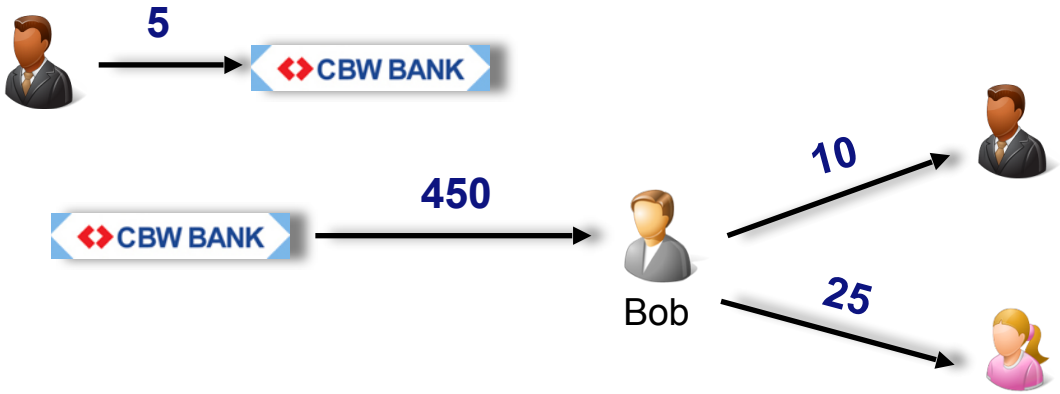
Local Knowledge is Sufficient!

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



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

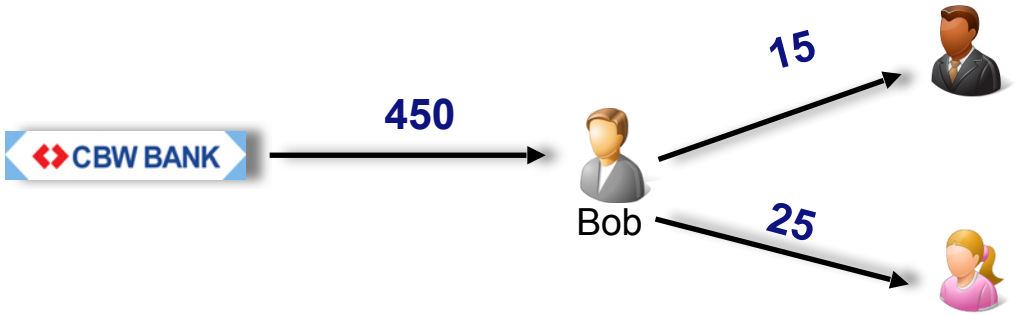
- A user checks net-flow does not change



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

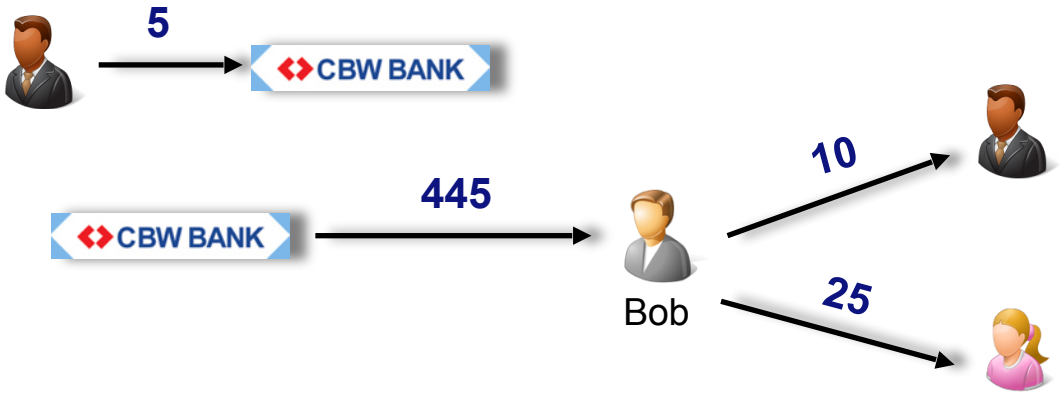
Local Knowledge is Sufficient!

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



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

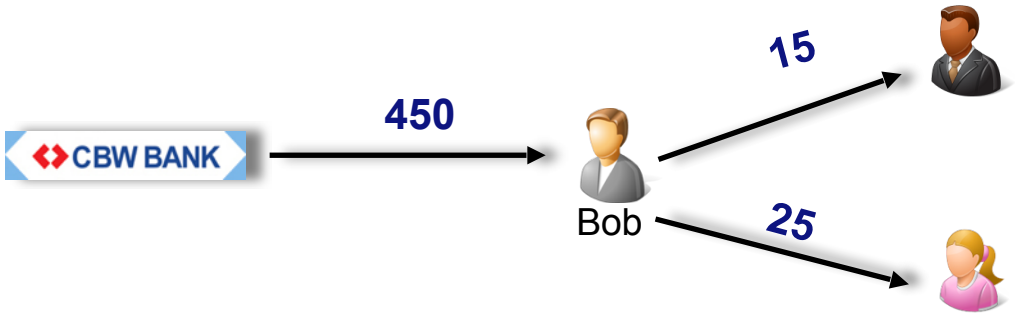
- A user checks net-flow does not change



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

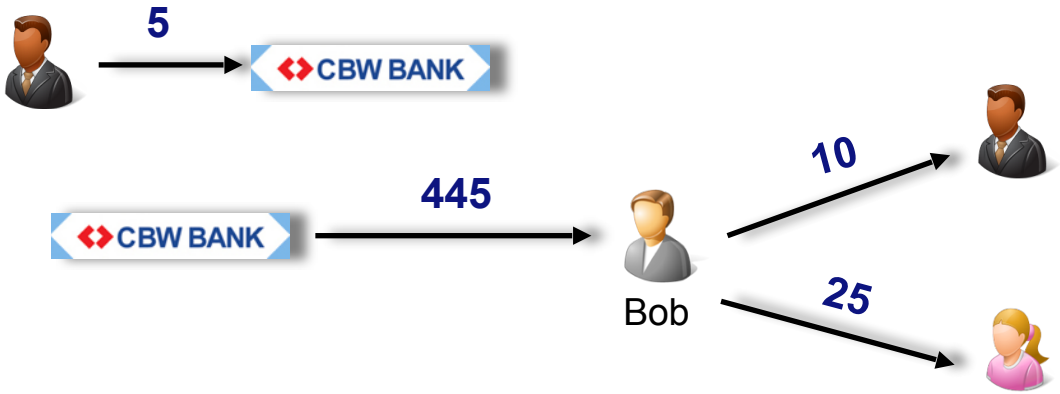
Local Knowledge is Sufficient!

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



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

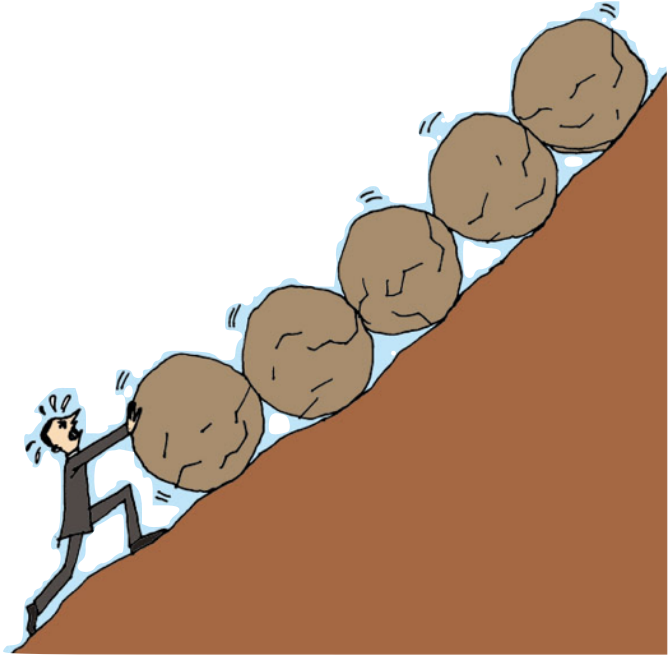
- A user checks net-flow does not change



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

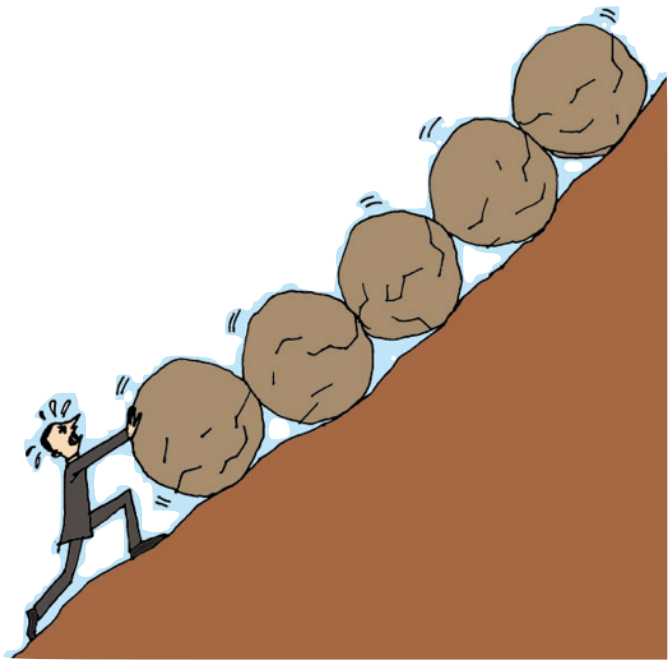
Challenges

- 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 and accountability guarantees…



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 and accountability guarantees…



A. Kate, M. Maffei, G. Malavolta, and P. Moreno-Sanchez:
Whispers: A Distributed Architecture for Enforcing Privacy in Credit Networks.
TechReport: http://crypsys.mmci.uni-saarland.de/projects/DecentralizedPrivPay/

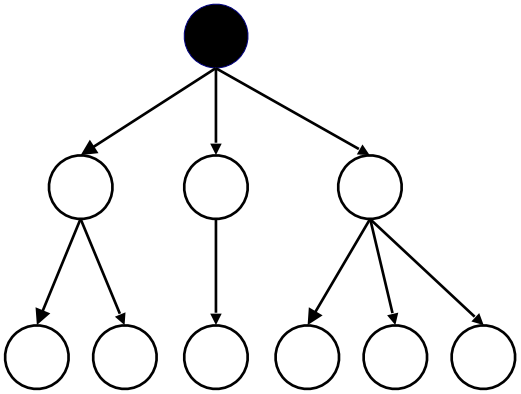
Routing: max-flow computation

- 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

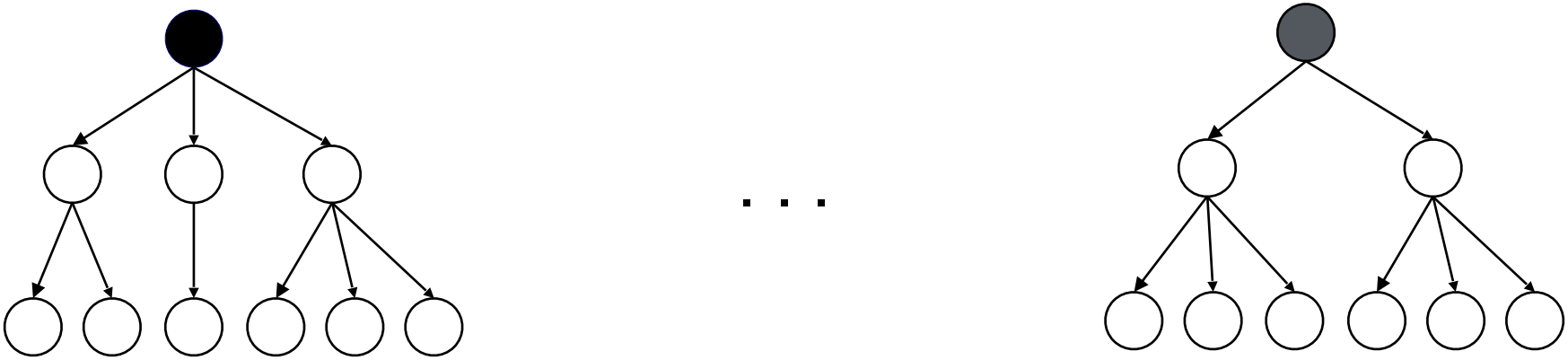
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



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

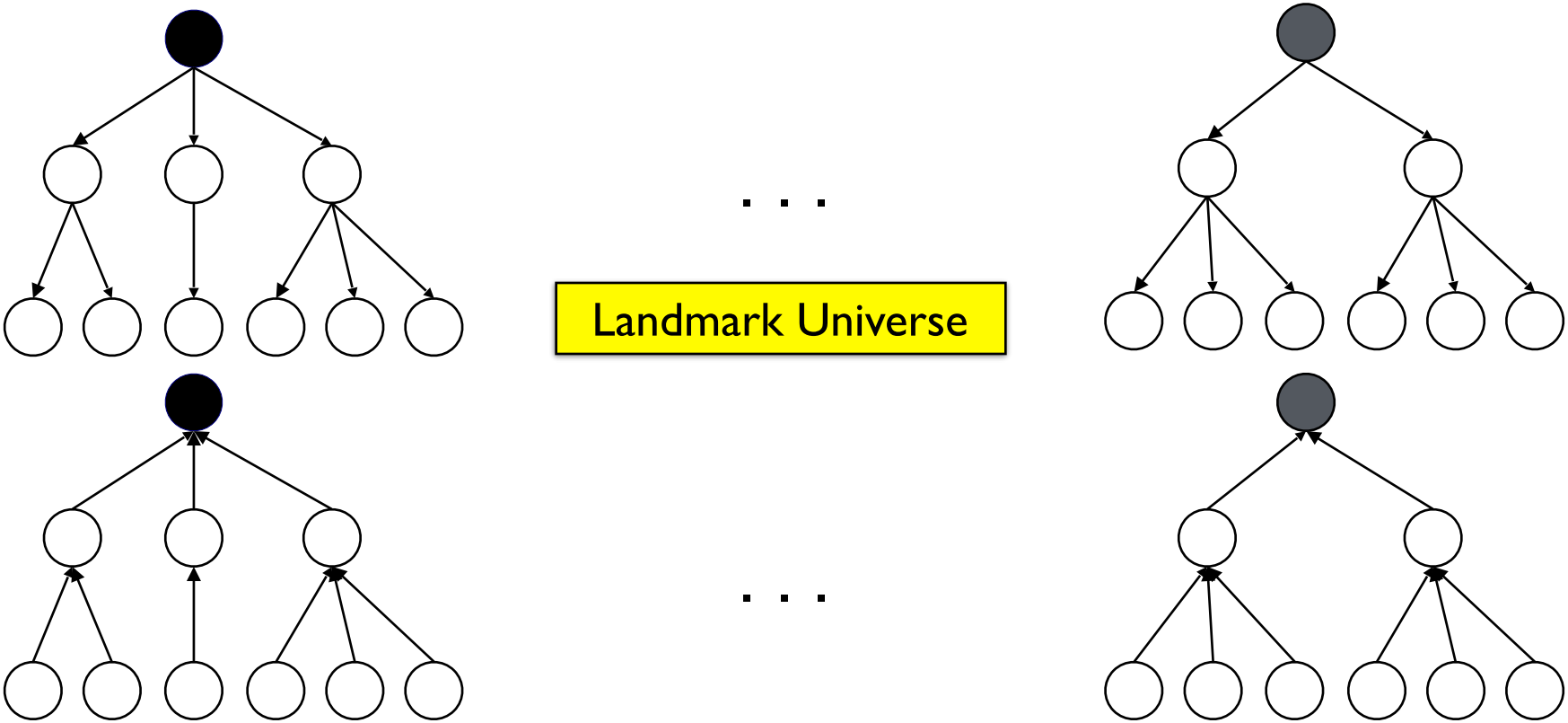
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



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

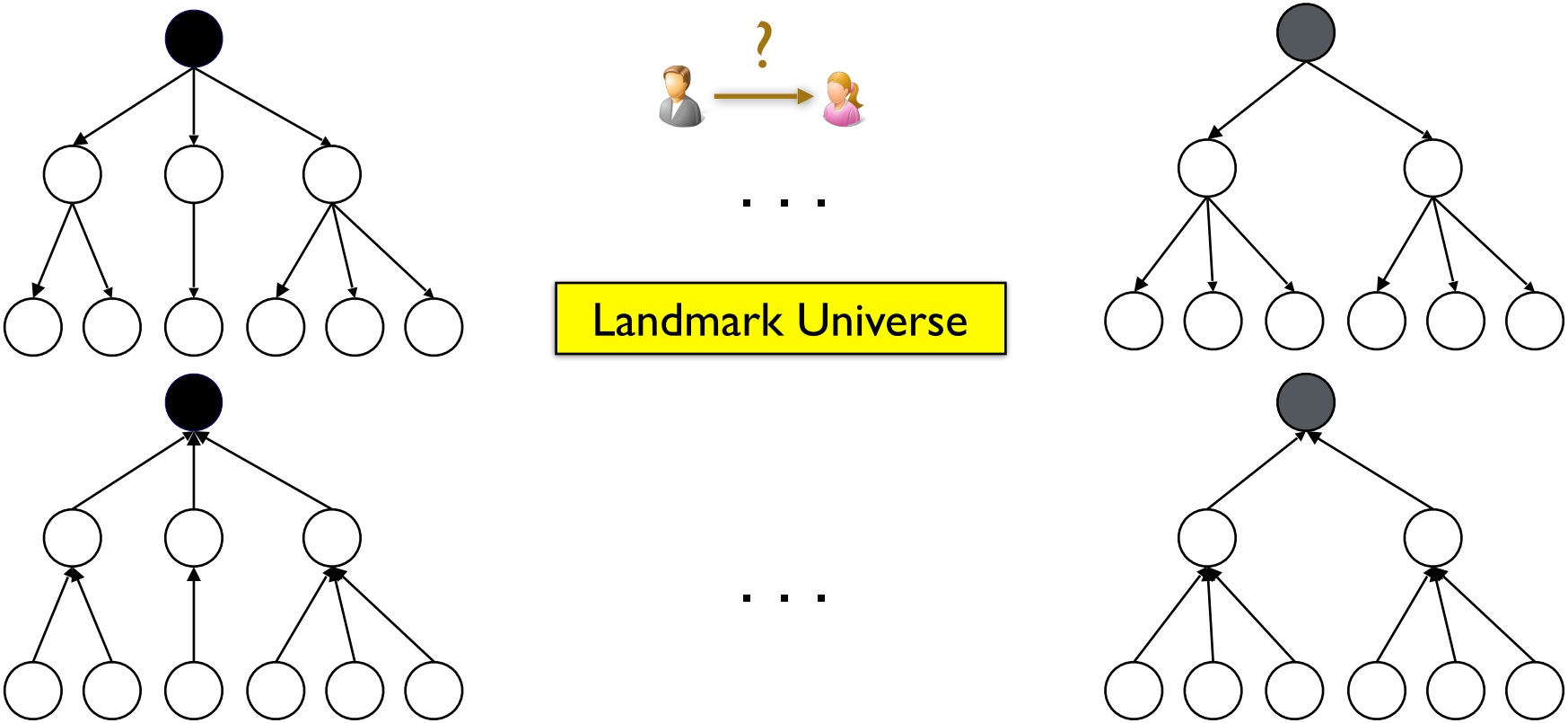
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



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

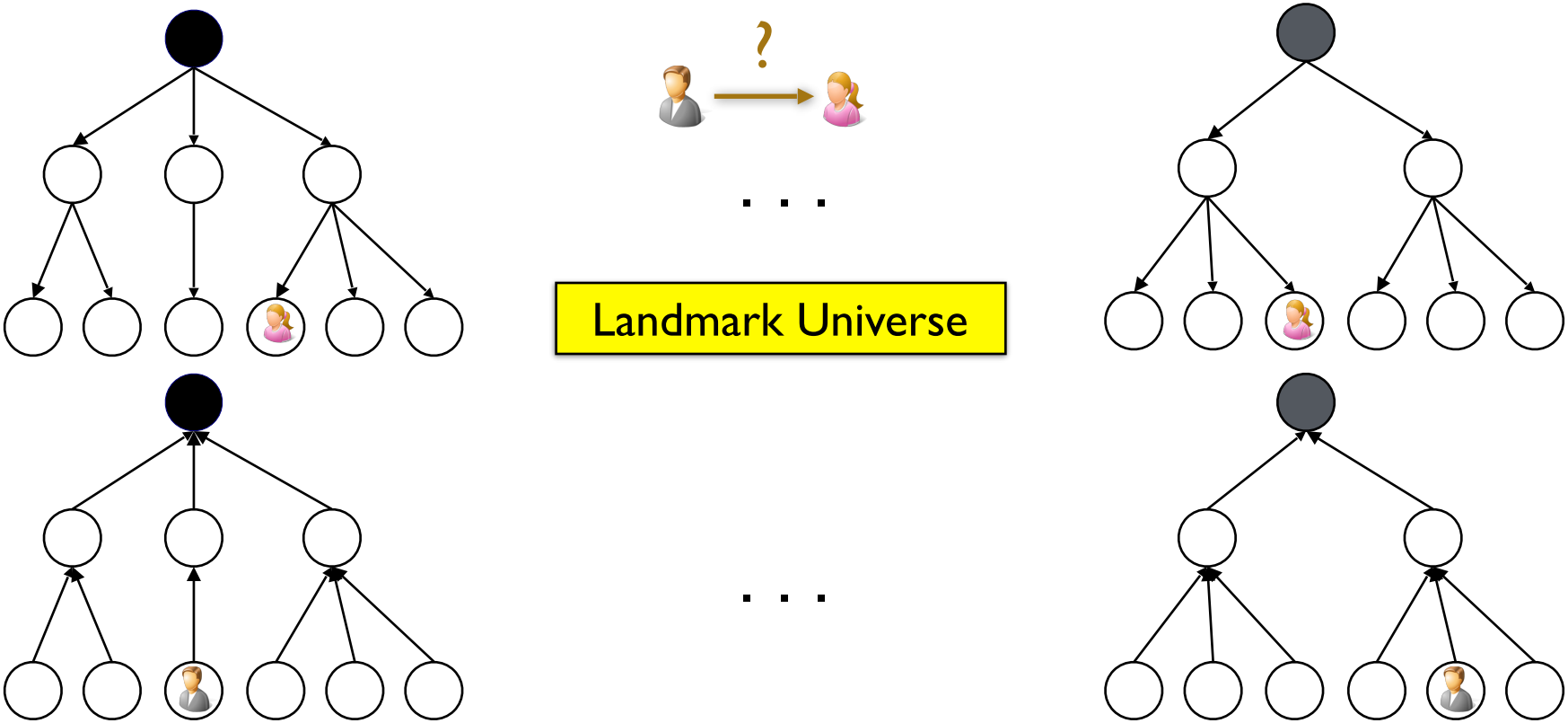
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



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

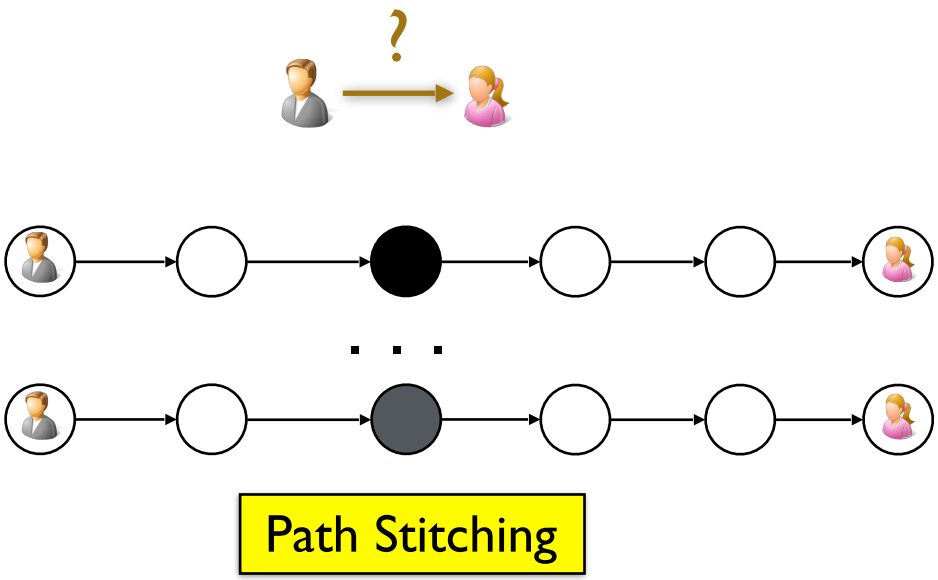
[Tsuchiya SigComm'88] [Vishanath et al. Eurosys'12]



Routing: max-flow computation

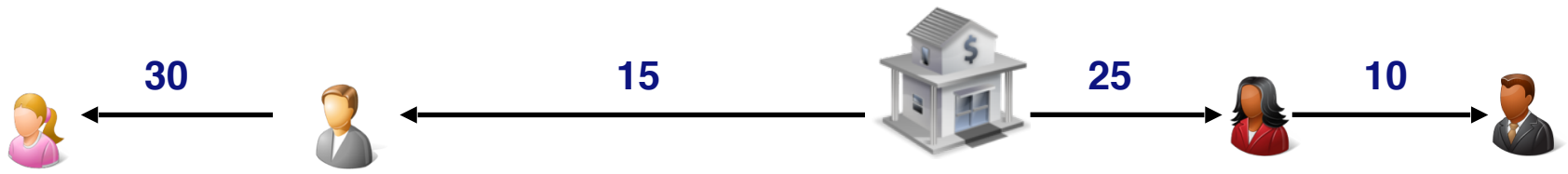
- Routing challenge:
  Known max-flow algorithms are not scalable: $O(V^3)$ or $O(V^2 \log(E))$
- We employ landmark routing:
  Calculate only a subset of all possible routes through intermediary nodes called landmarks

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



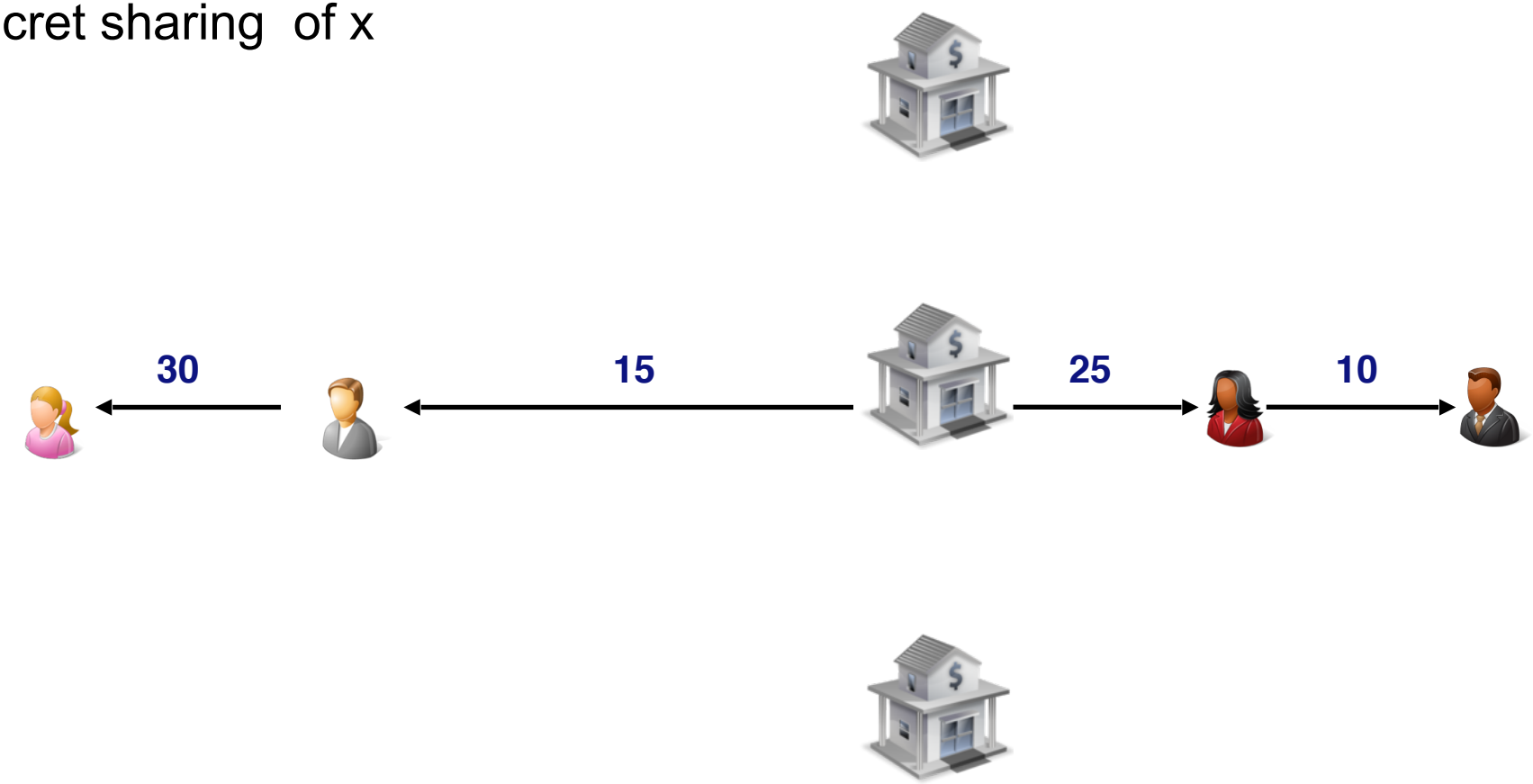
Credit in a Path

[x]: Secret sharing of x



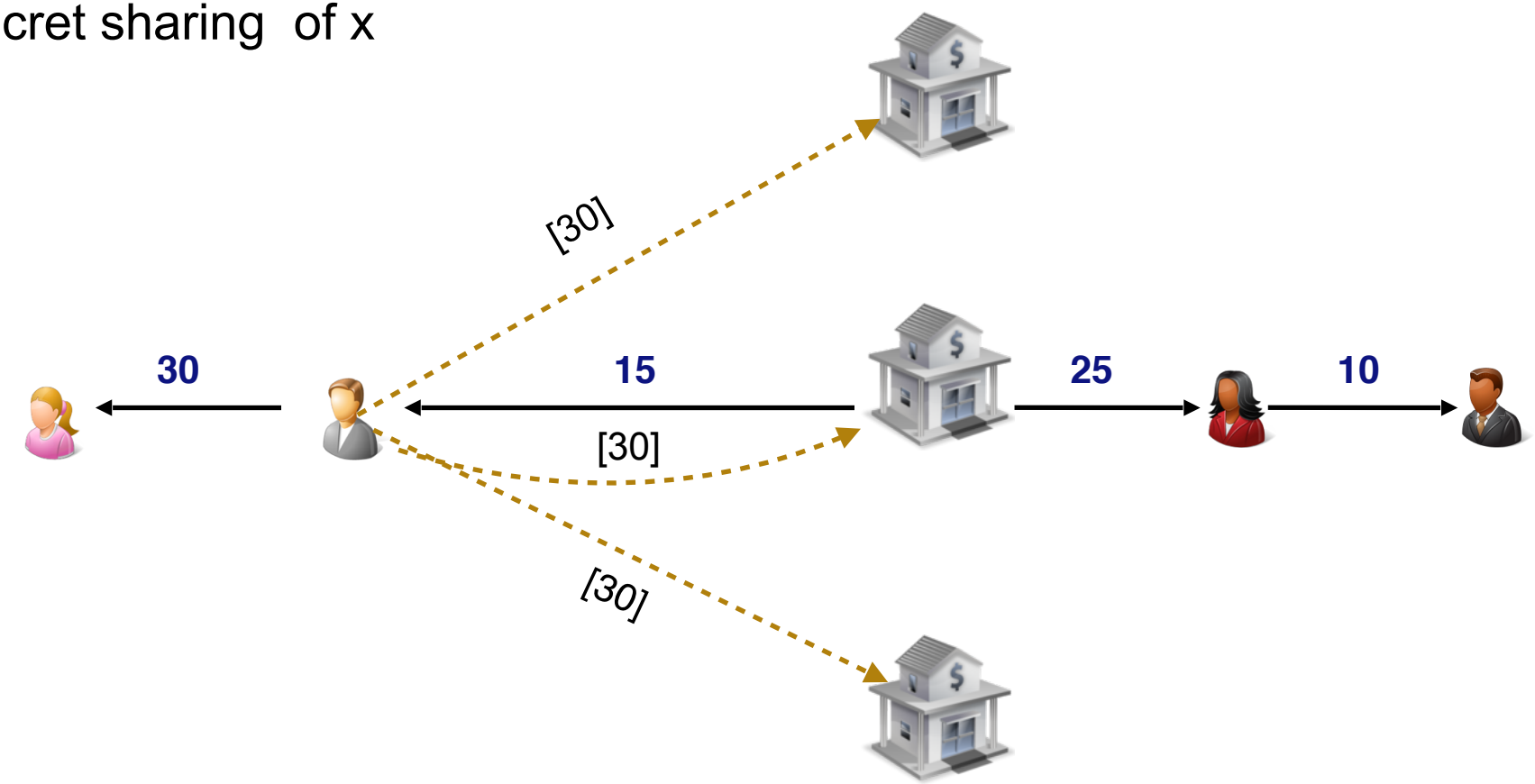
Credit in a Path

[x]: Secret sharing of x



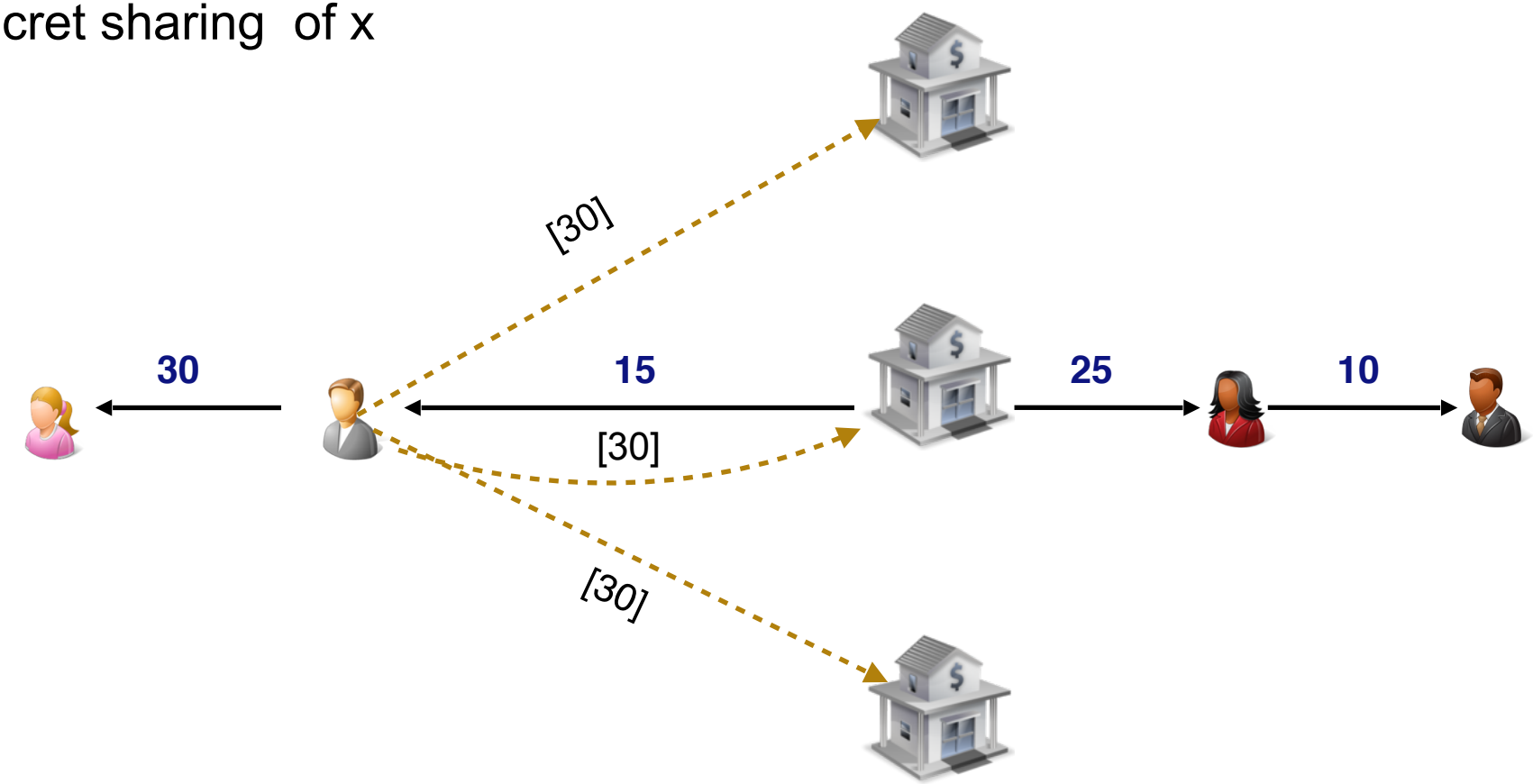
Credit in a Path

[x]: Secret sharing of x



Credit in a Path

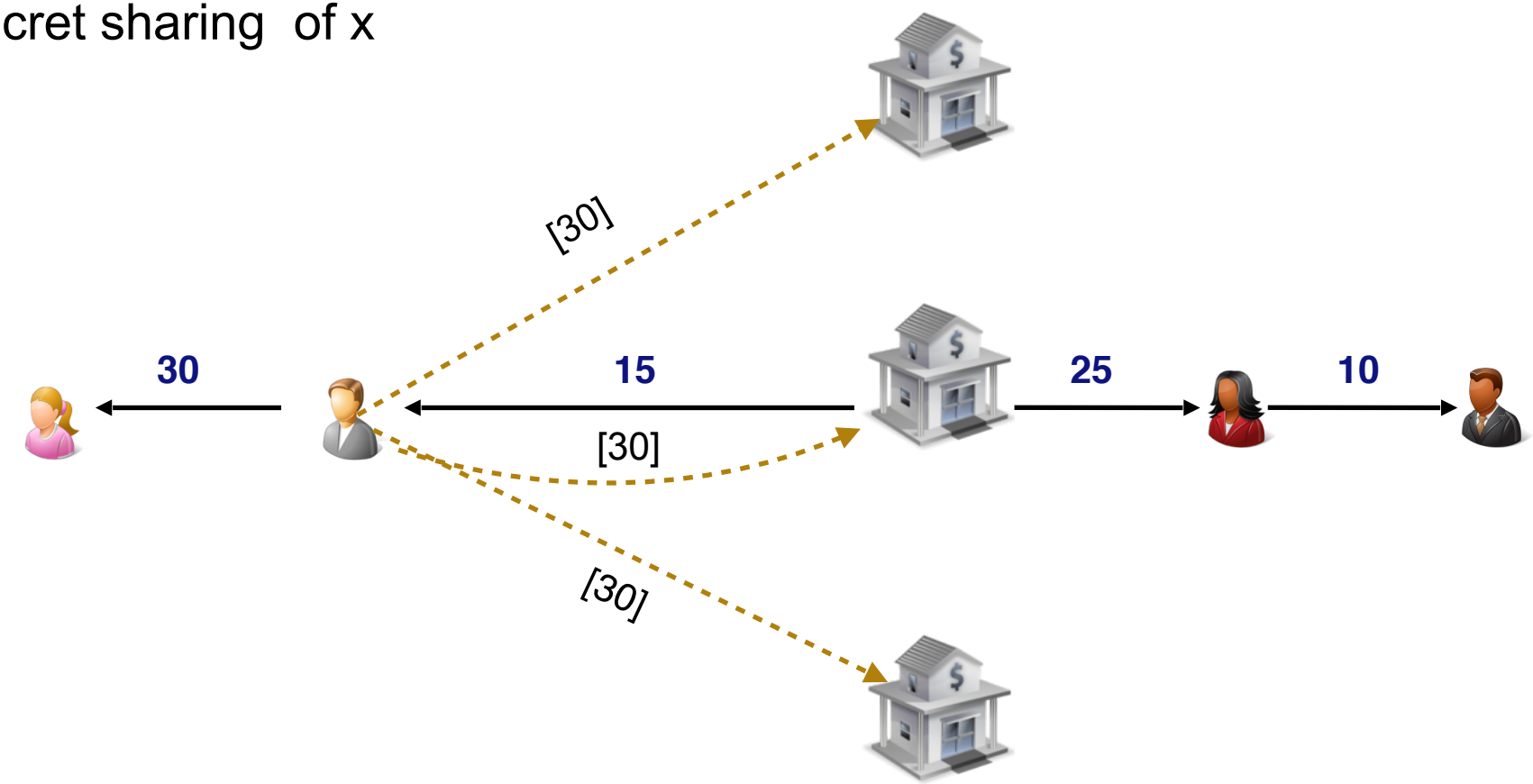
[x]: Secret sharing of x



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

Credit in a Path

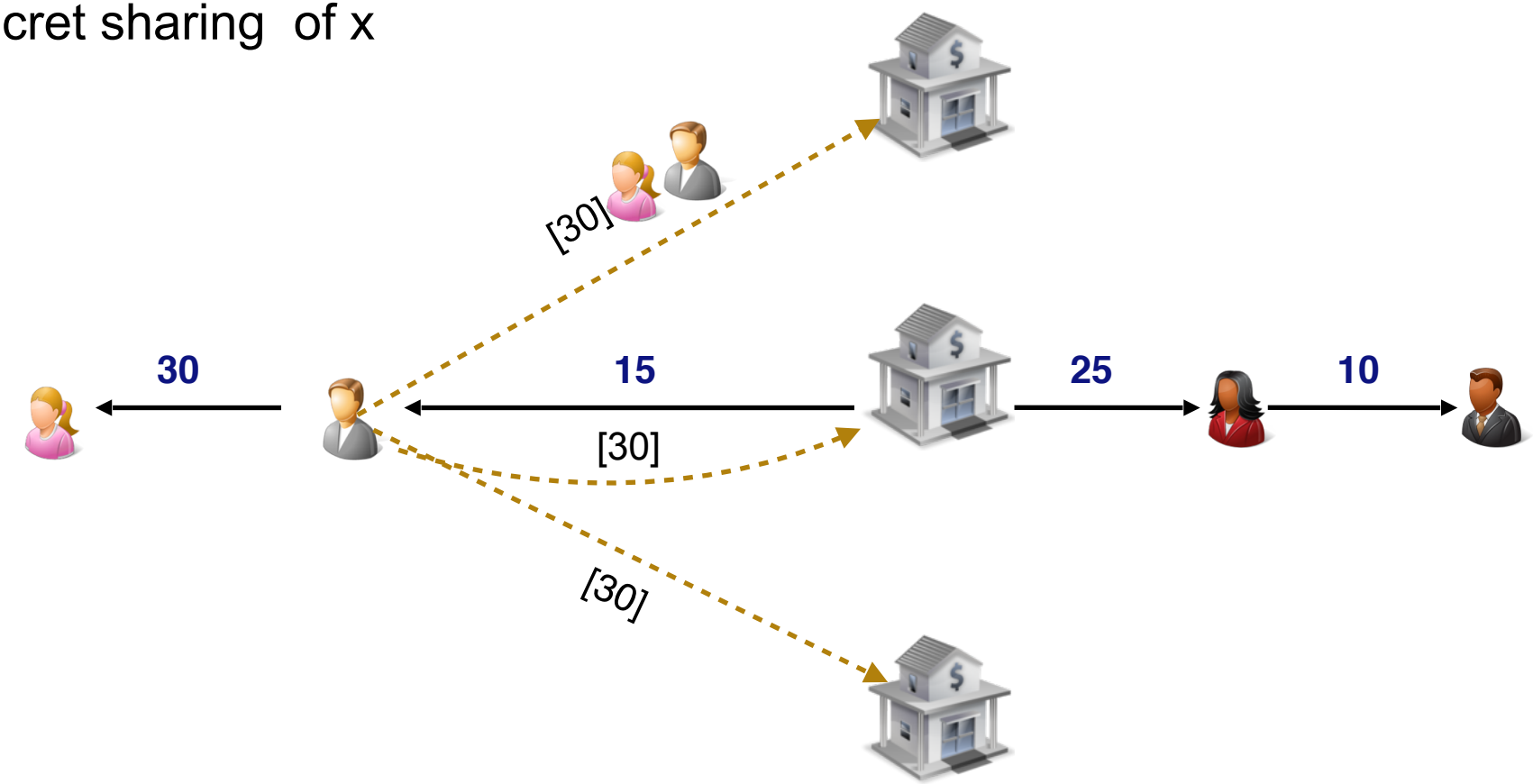
[x]: Secret sharing of x



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

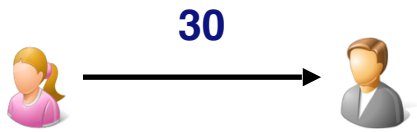
Credit in a Path

[x]: Secret sharing of x

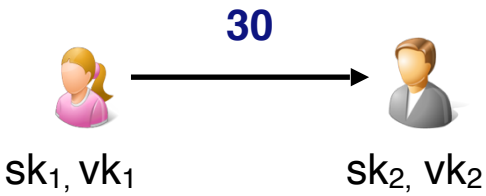


- Given [x] it is not possible to know x
- How to ensure that [x] comes from a user in a path?

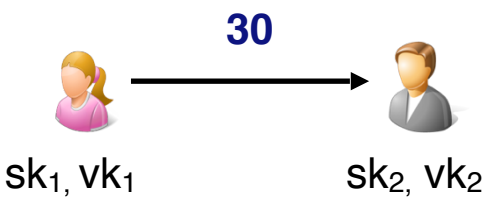
Proof of Credit Links in a Path



Proof of Credit Links in a Path

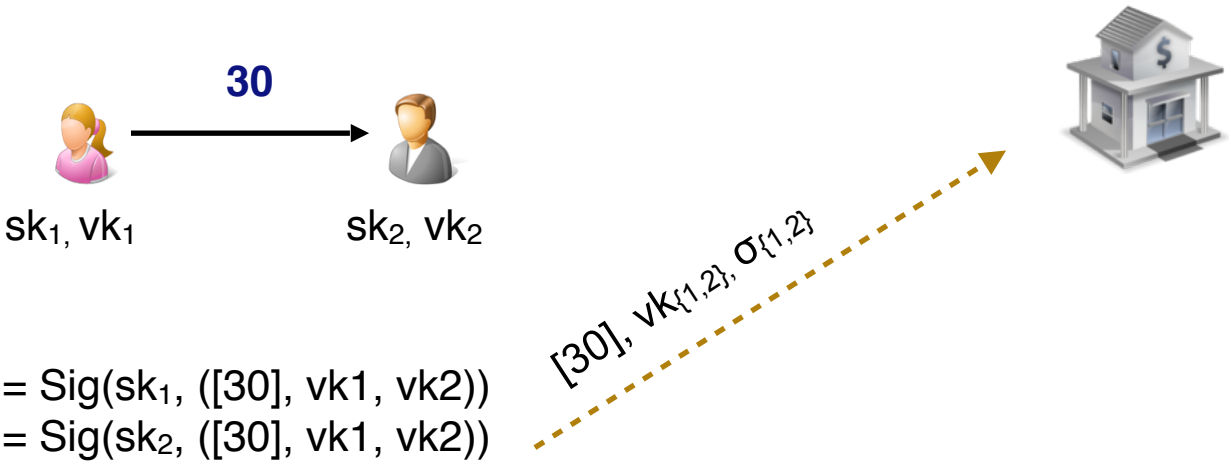


Proof of Credit Links in a Path



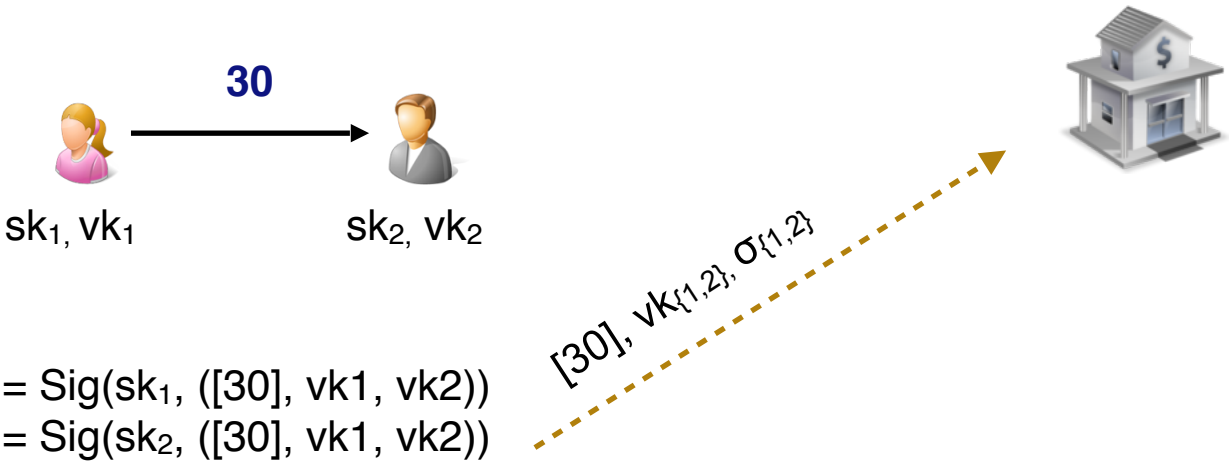
$\sigma_1 := \mathrm{Sig}(sk_1, ([30], vk1, vk2))$
$\sigma_2 := \mathrm{Sig}(sk_2, ([30], vk1, vk2))$

Proof of Credit Links in a Path



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

Proof of Credit Links in a Path

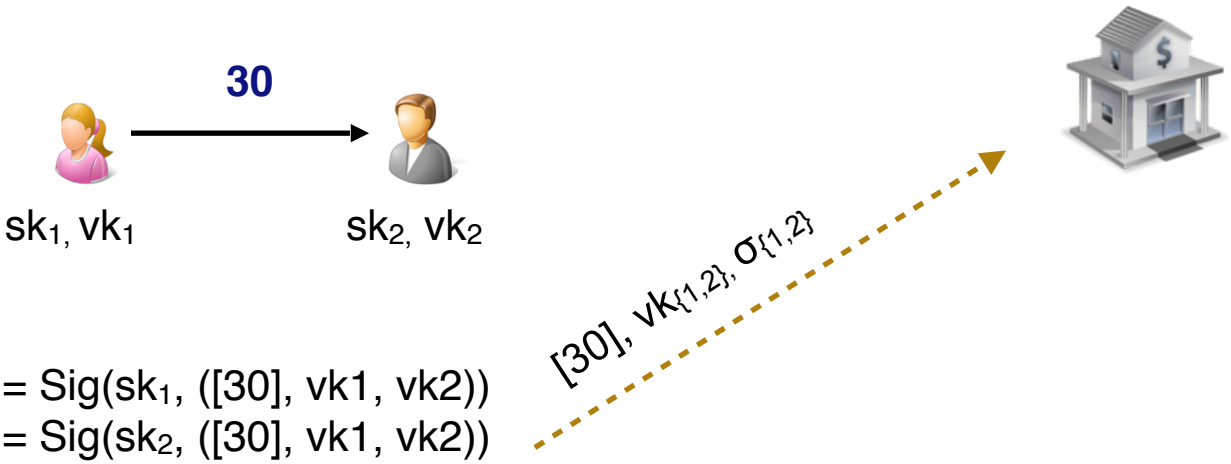


$\sigma_1 := Sig(sk_1, ([30], vk1, vk2))$
$\sigma_2 := Sig(sk_2, ([30], vk1, vk2))$

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

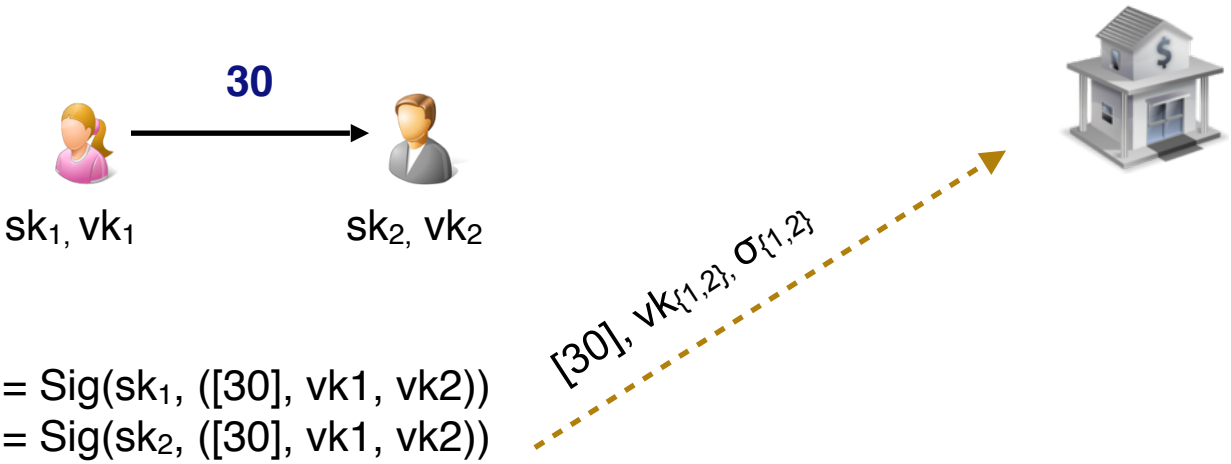


$\sigma_1 := Sig(sk_1, ([30], vk1, vk2))$
$\sigma_2 := Sig(sk_2, ([30], vk1, vk2))$

Correct proof for a path

$(vk_1, \boxed{vk_2}), (vk_2, vk_3), (vk_3, vk_4), \ldots$

Proof of Credit Links in a Path

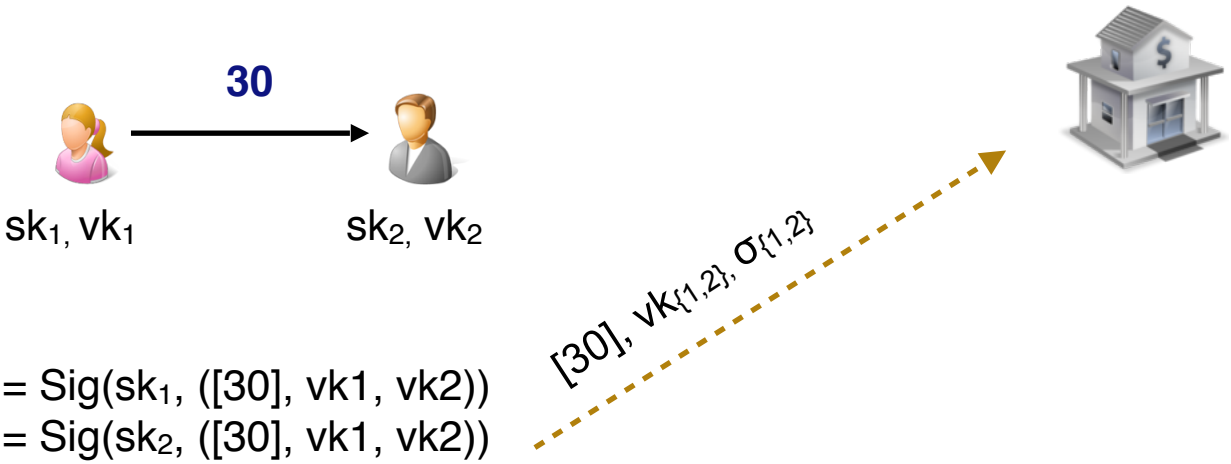


$\sigma_1 := Sig(sk_1, ([30], vk1, vk2))$
$\sigma_2 := Sig(sk_2, ([30], vk1, vk2))$

Correct proof for a path

$(vk_1, \boxed{vk_2}), (\boxed{vk_2}, vk_3), (vk_3, vk_4), \ldots$

Proof of Credit Links in a Path



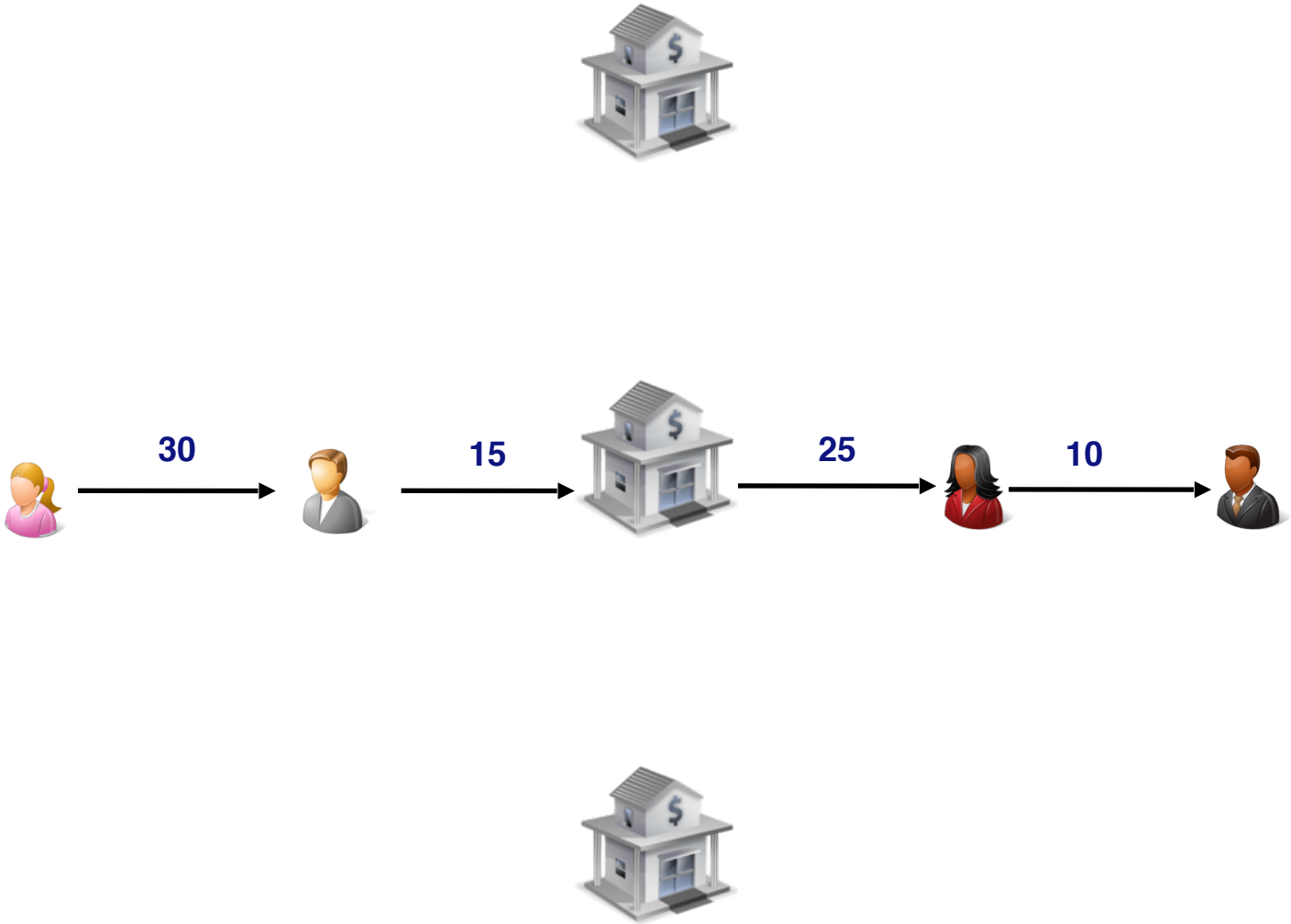
$\sigma_1 := Sig(sk_1, ([30], vk1, vk2))$
$\sigma_2 := Sig(sk_2, ([30], vk1, vk2))$

Correct proof for a path

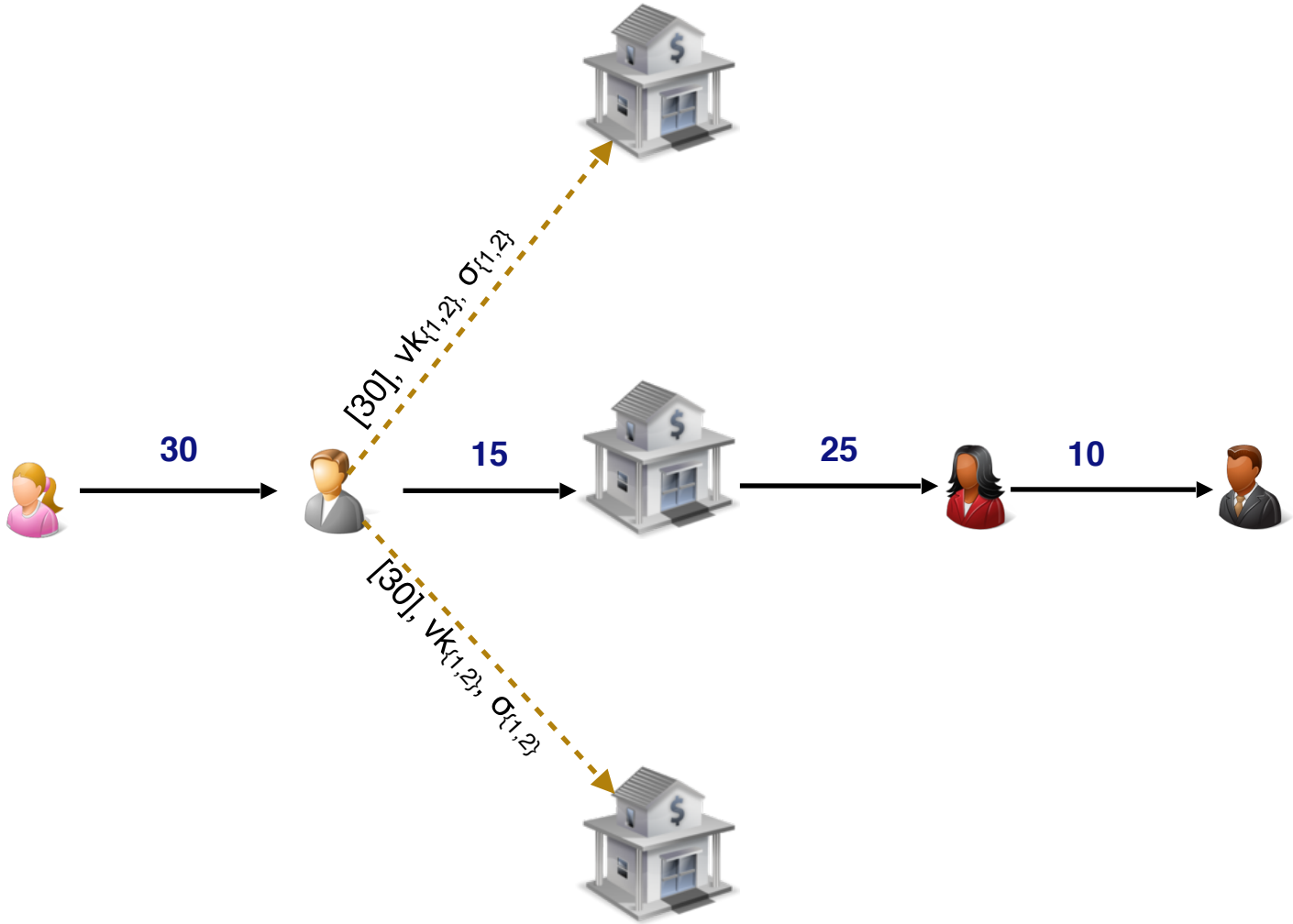
$(vk_1, \boxed{vk_2}), \boxed{(vk_2,} vk_3), (vk_3, vk_4), \ldots$

Fresh keys per transaction

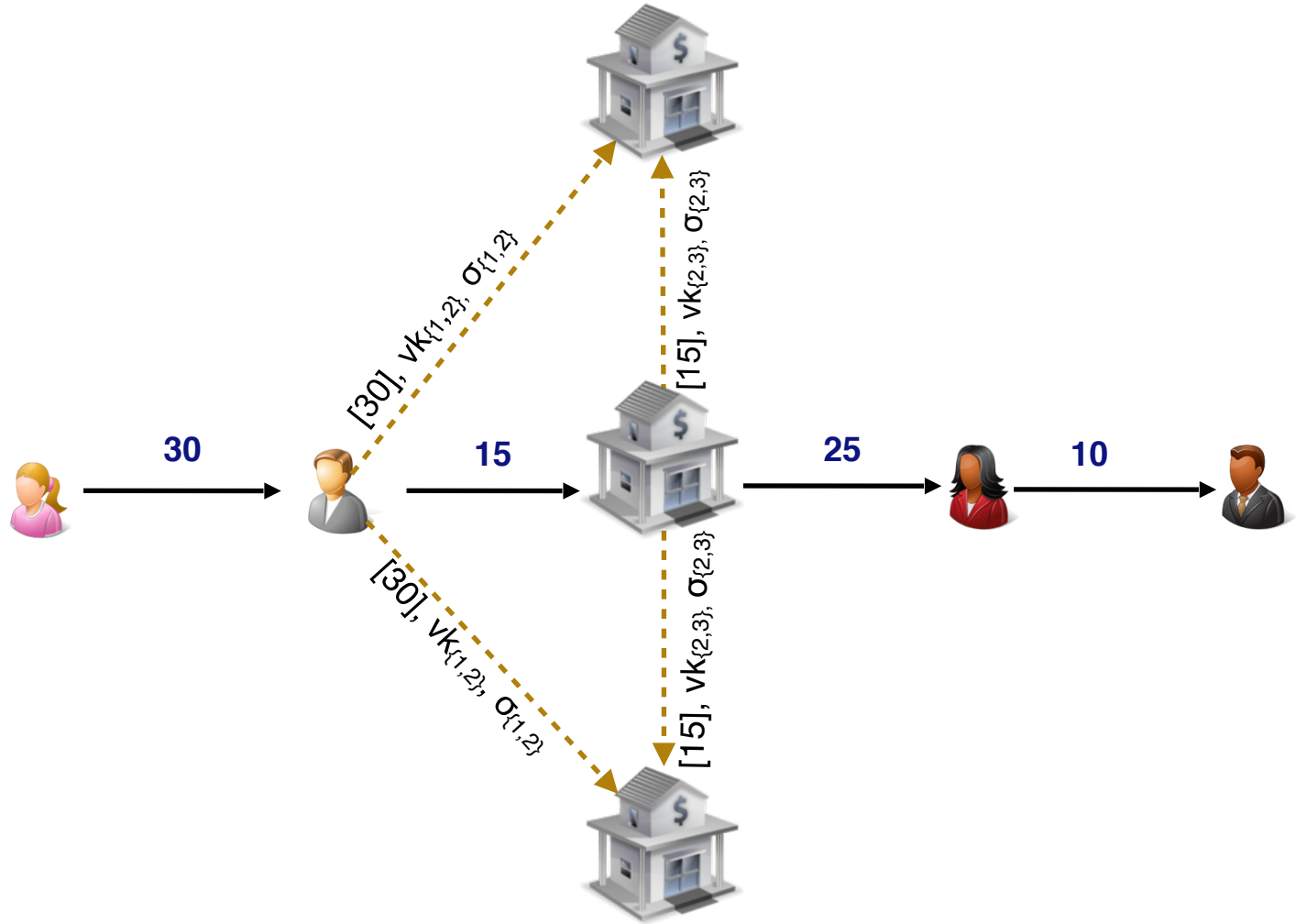
Privacy-preserving Credit in a Path



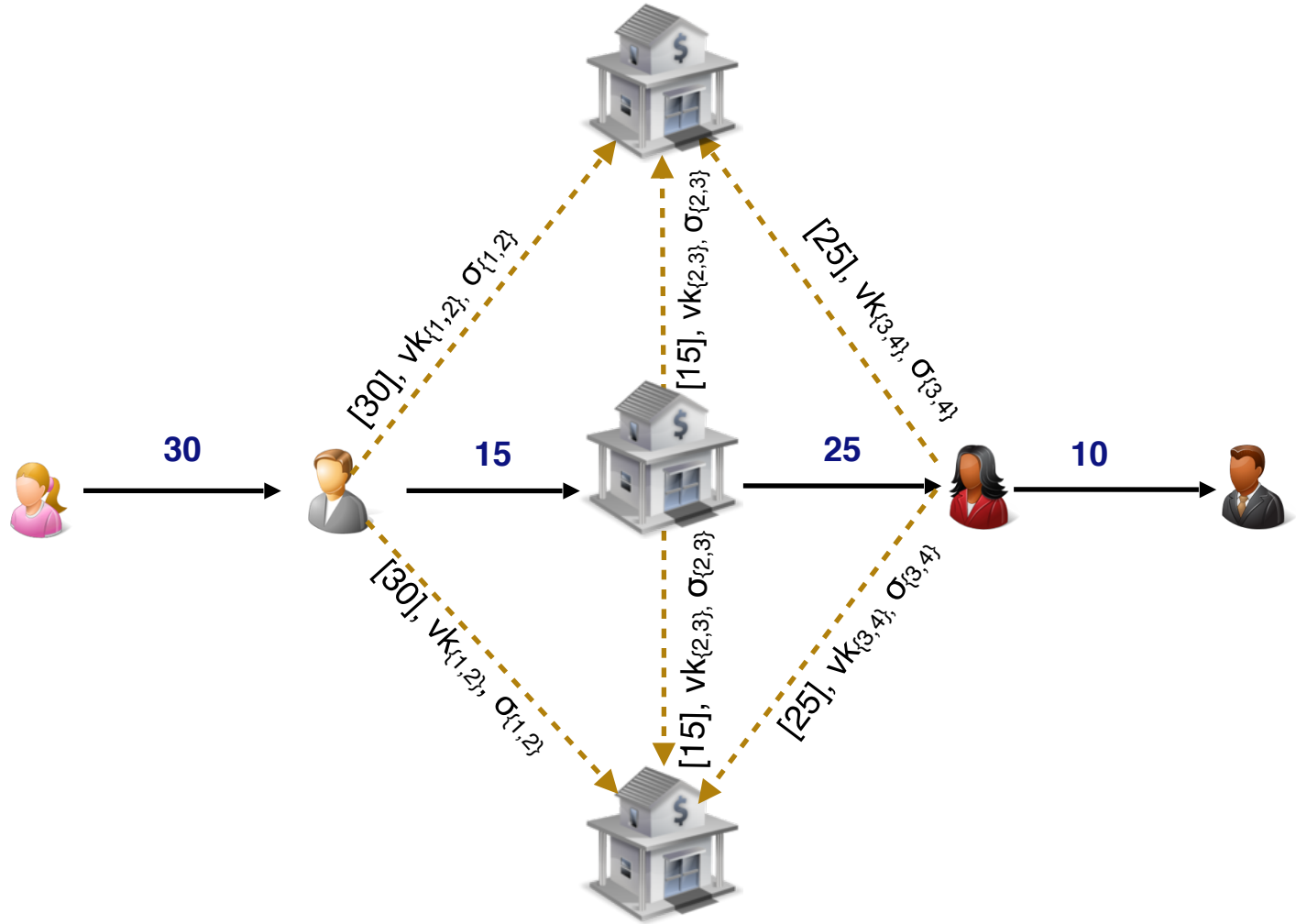
Privacy-preserving Credit in a Path



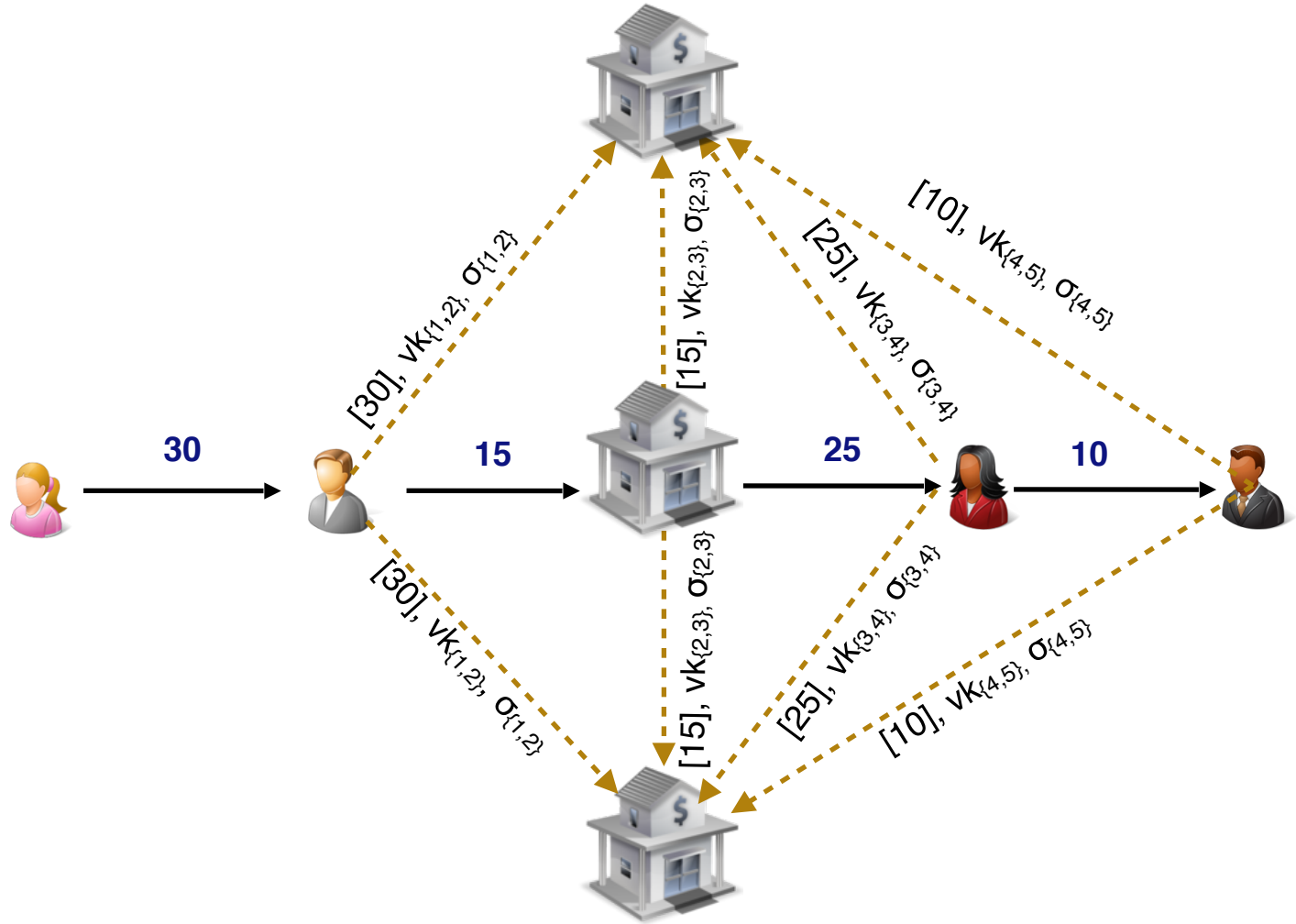
Privacy-preserving Credit in a Path



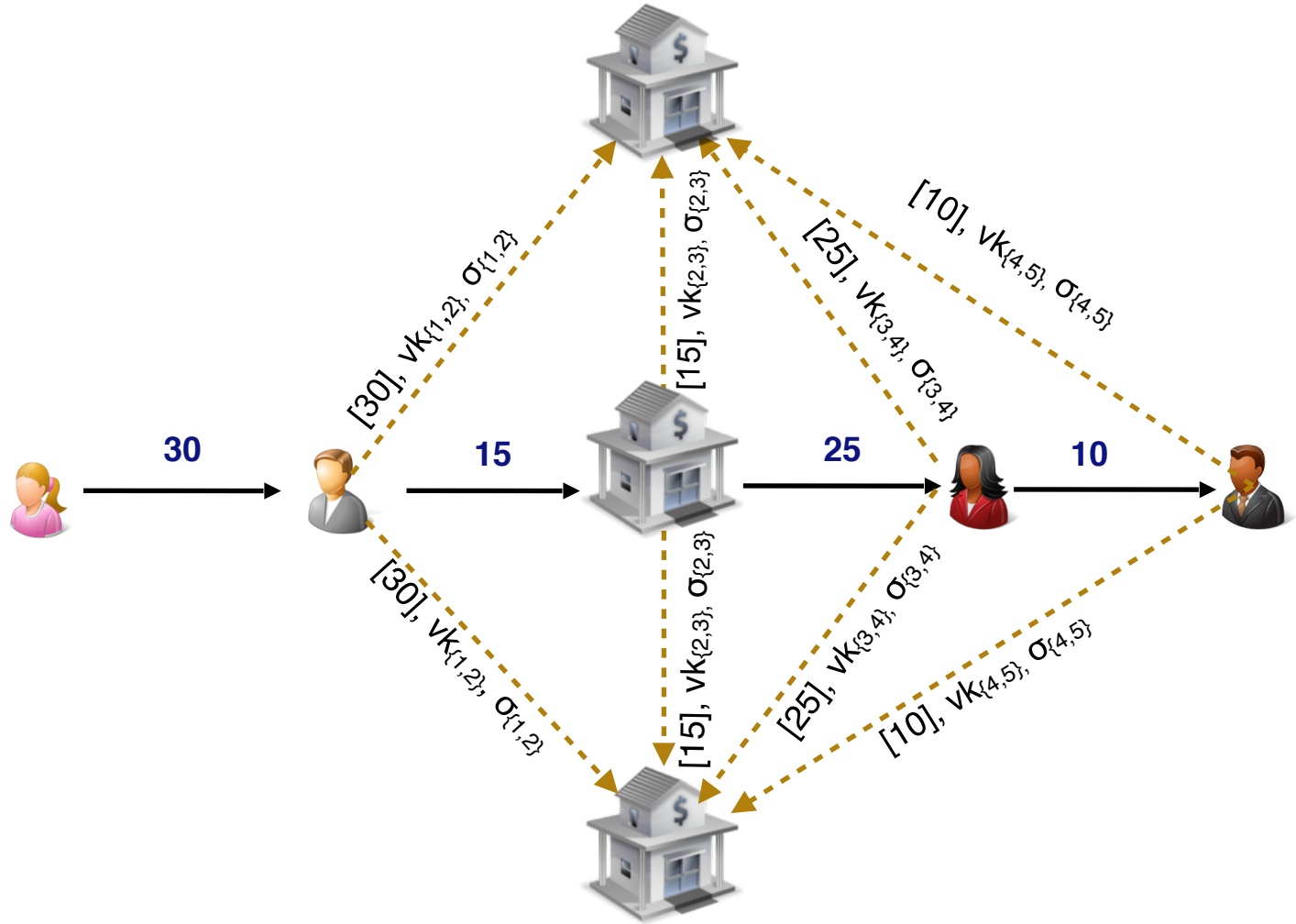
Privacy-preserving Credit in a Path



Privacy-preserving Credit in a Path

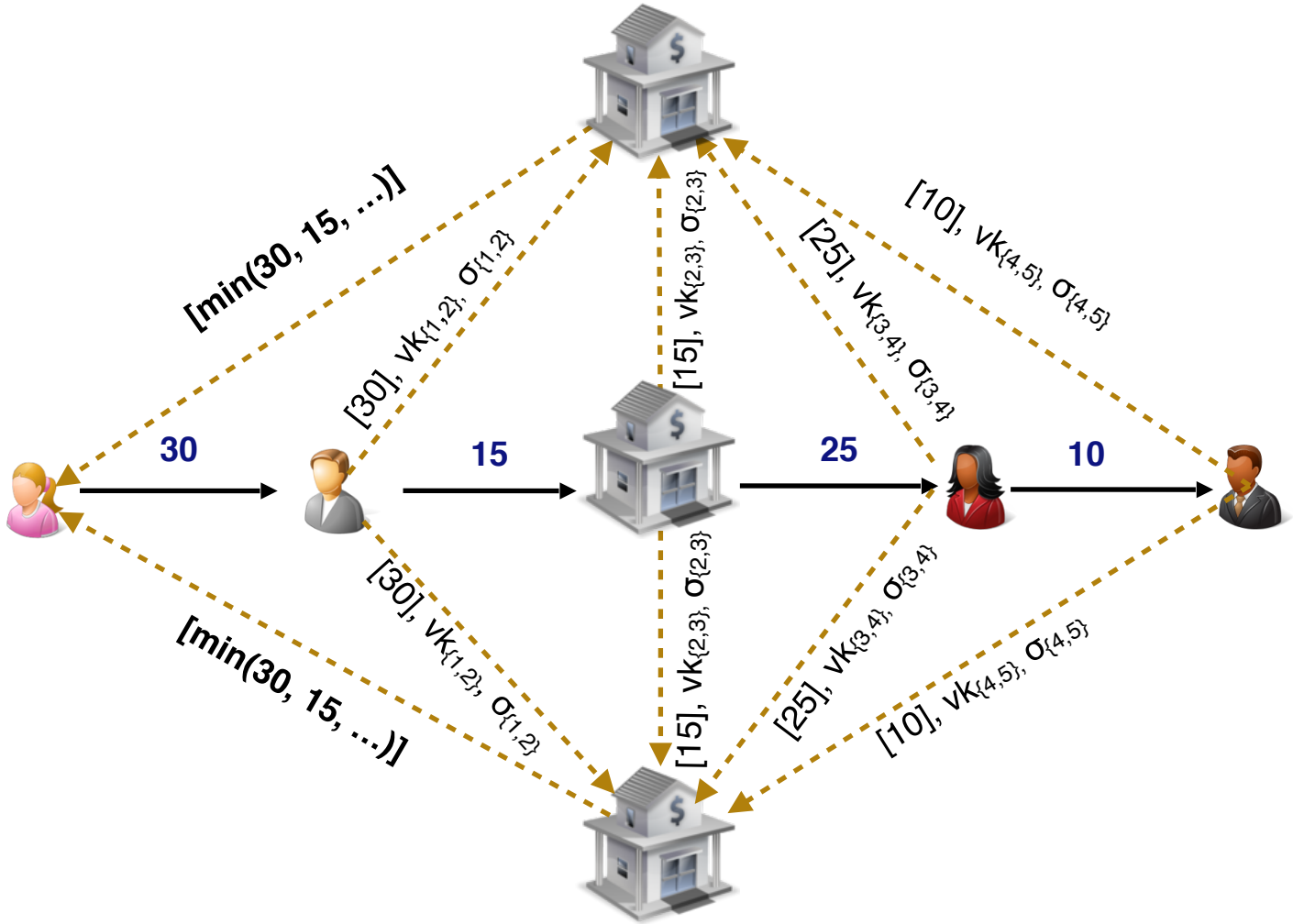


Privacy-preserving Credit in a Path



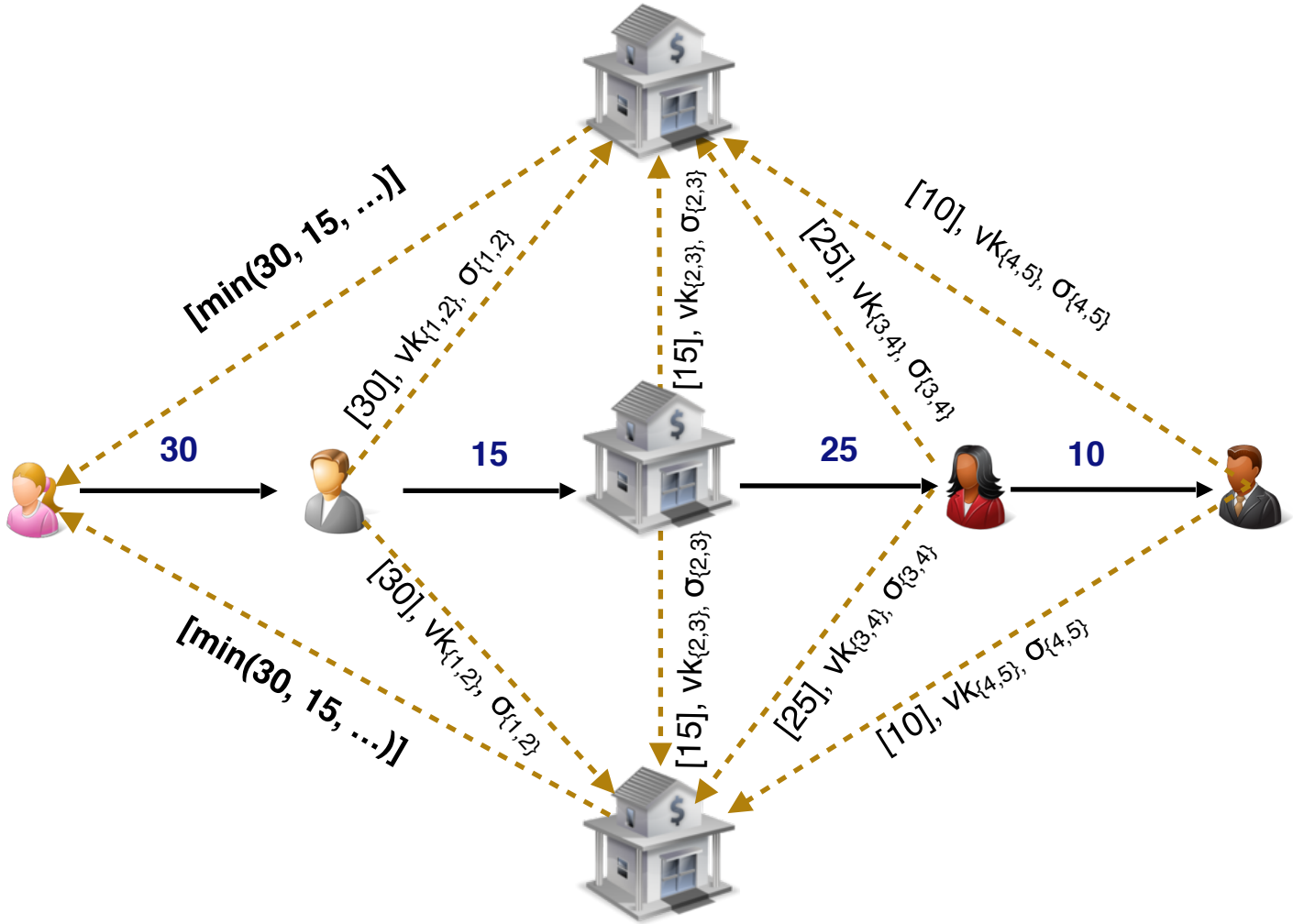
- Landmarks perform SMPC min computation over the shared link values

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

Transaction Execution

- Sequential friend-to-friend communication

Transaction Execution

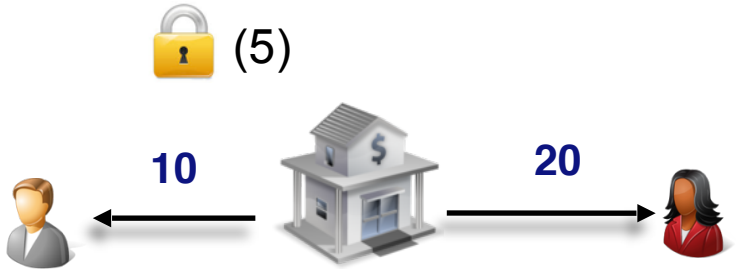
- Sequential friend-to-friend communication
- Two-step transaction: on hold (or block) and settle

Transaction Execution

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

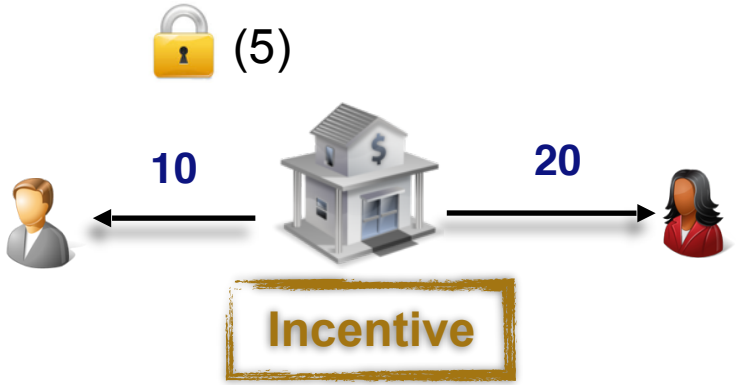
Transaction Execution

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



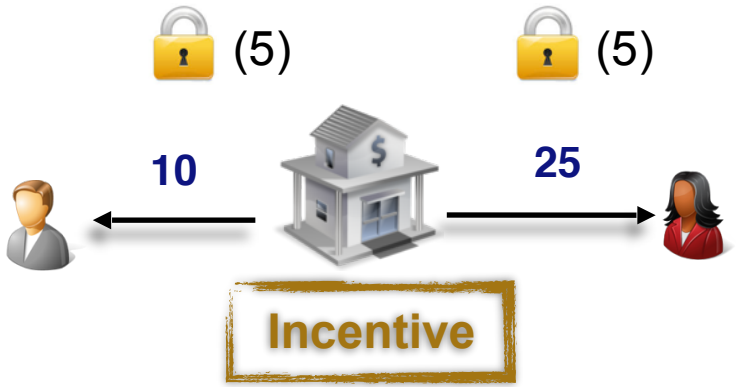
Transaction Execution

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



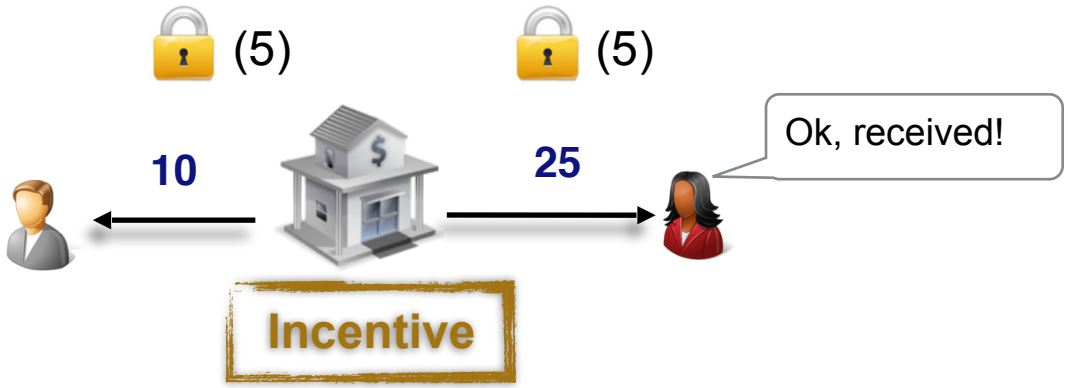
Transaction Execution

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



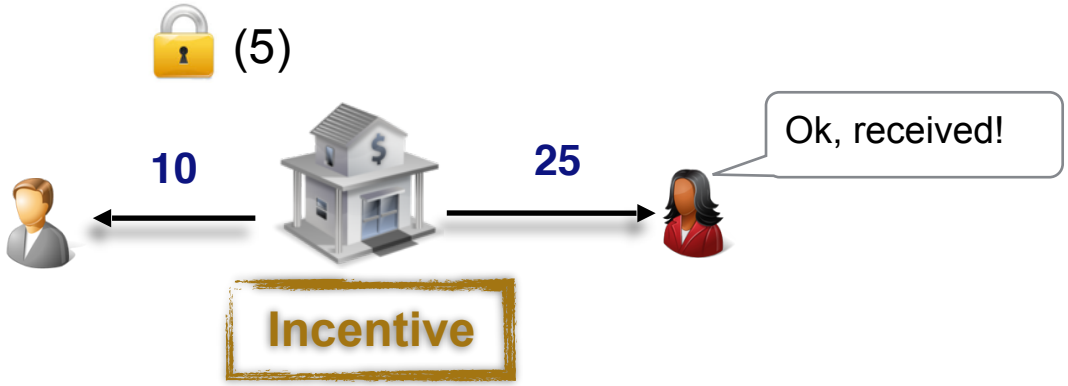
Transaction Execution

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



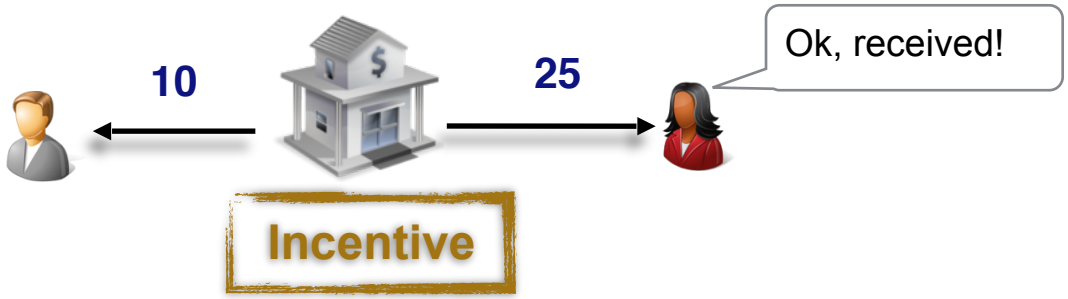
Transaction Execution

- 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:



Whispers: Characteristics/Limitations

PURDUE UNIVERSITY

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

  [more details in the techreport]
- In case of disputes, this leaves task of proving links to the users
- It is blocking solution, and deadlocks are possibles
- In the near future
  - design non-blocking solutions in the asynchronous communication setting
    - distributed max-flow computation and atomic broadcast

In the Future

In the Future

- Payment Channels and lighting network

https://lightning.network

  - Designing distributed solutions for lighting network

In the Future

- Payment Channels and lighting network

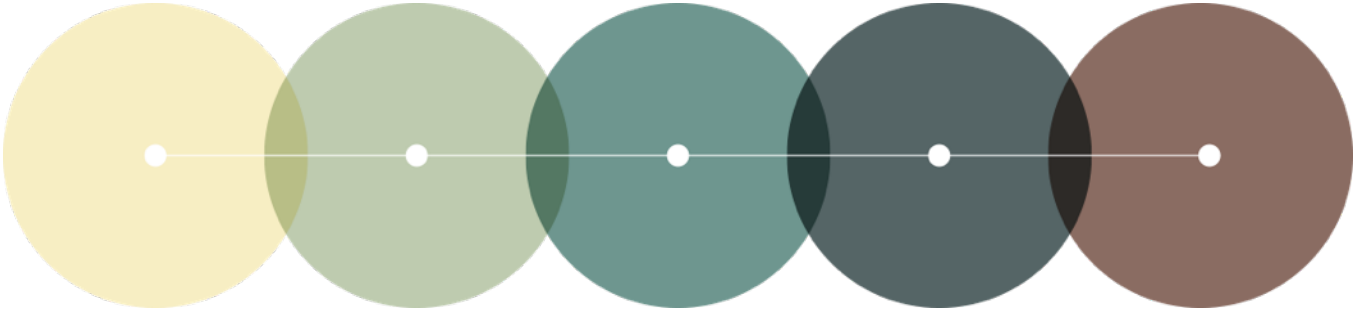
  https://lightning.network

  - Designing distributed solutions for lighting network

- The Interledger Protocol

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

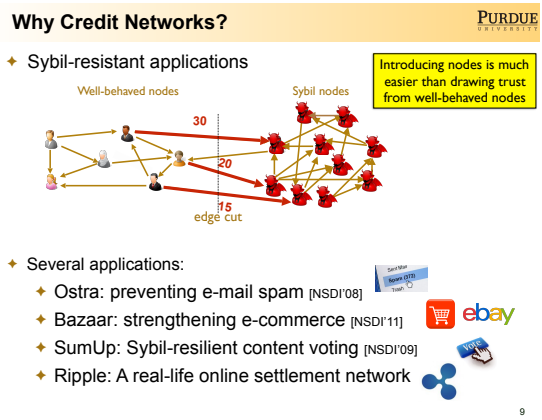
  - Several distributed/decentralized/centralized ledger solutions are coming up
  - Performing transactions across different ledgers



Take home message

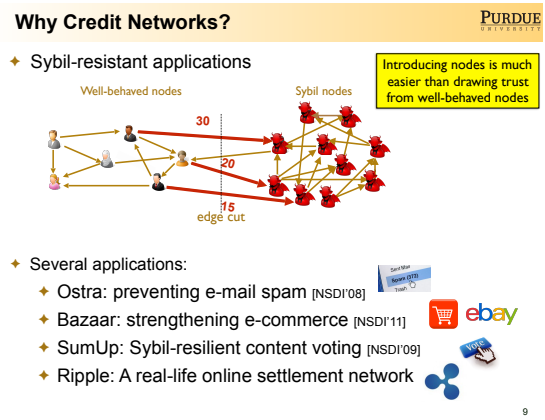
Take home message

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

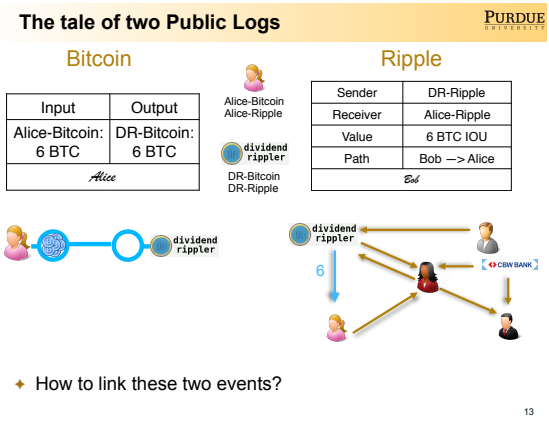


Take home message

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

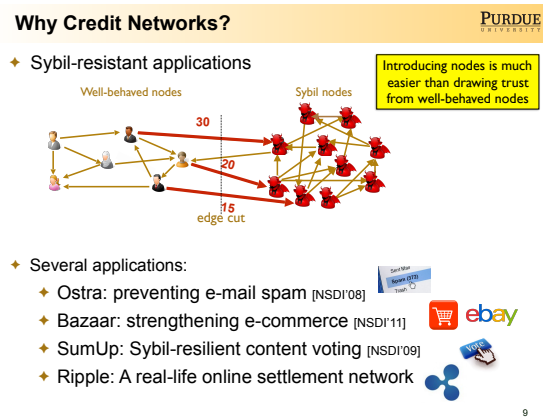


- Ledgers although provide accountability, it makes privacy a real problem in credit networks

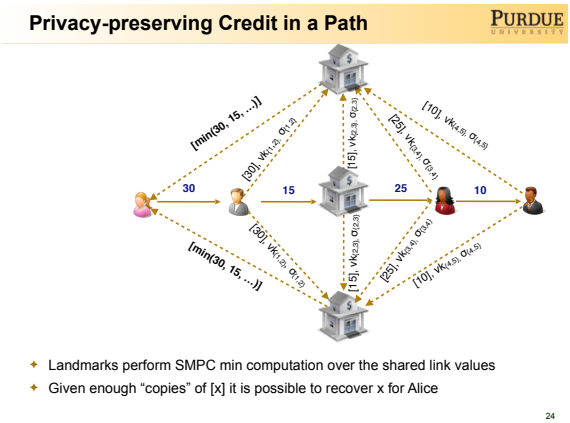


Take home message

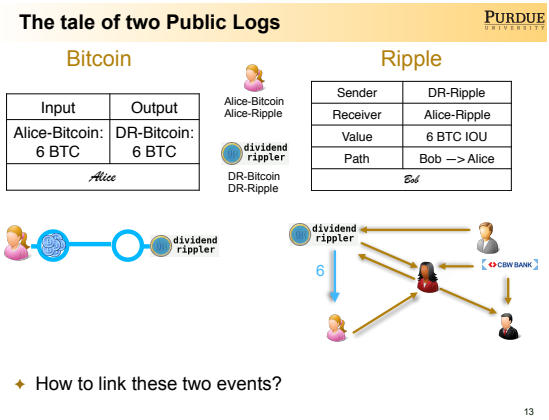
- Credit networks have interesting properties and can be used in multiple scenarios



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

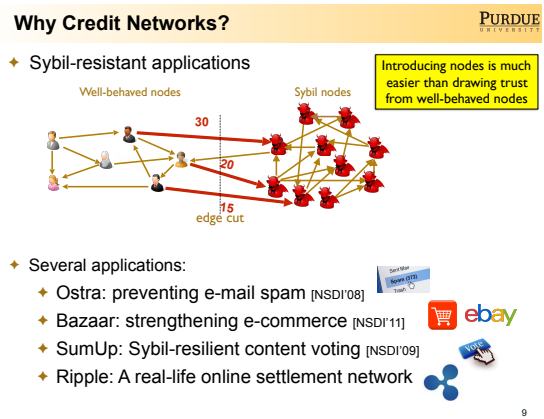


- Ledgers although provide accountability, it makes privacy a real problem in credit networks

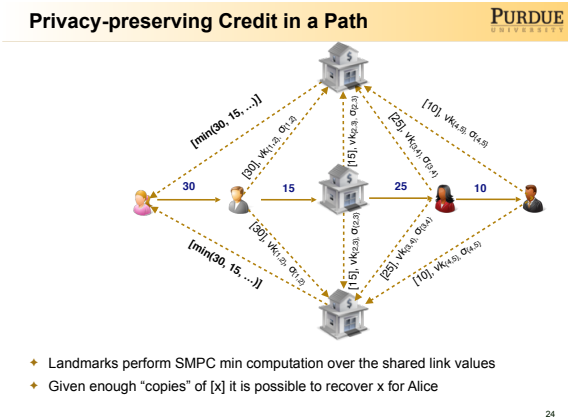


Take home message

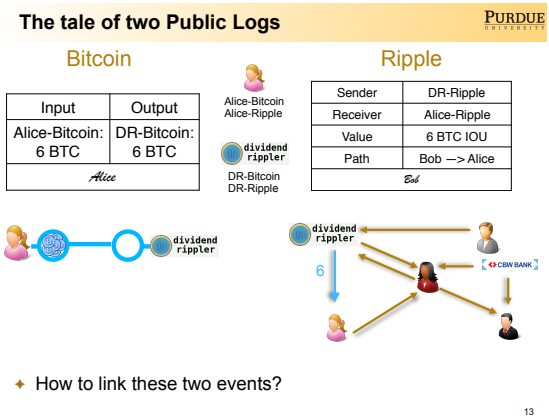
- Credit networks have interesting properties and can be used in multiple scenarios



- Whispers: 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