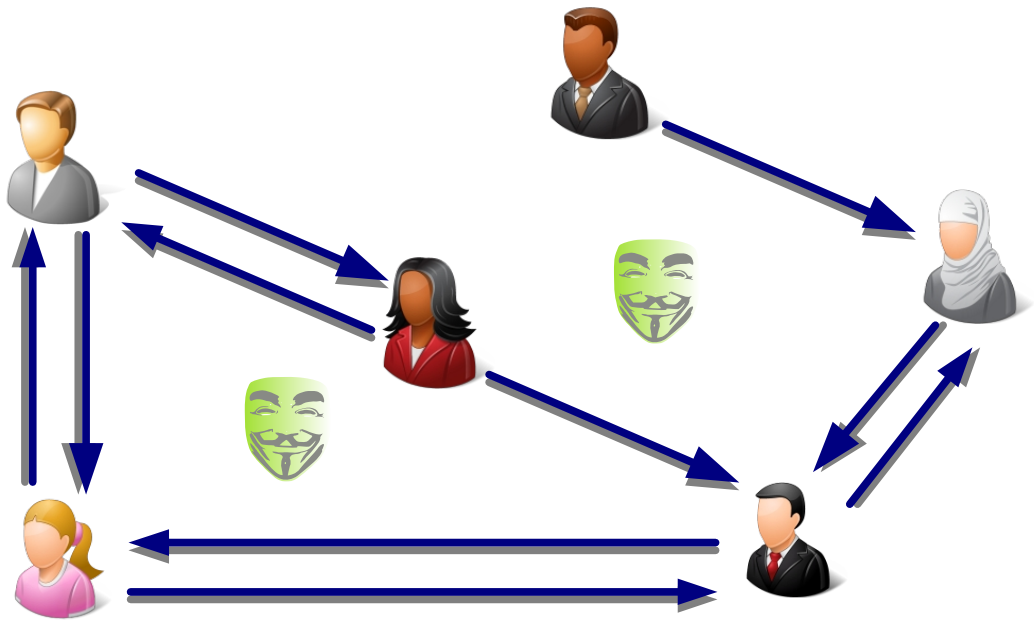
Privacy Preserving Payments in Credit Networks



Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei and Kim Pecina

CISPA, Saarland University

NDSS 2015

Credit Networks Introduction

Real World

Credit Network

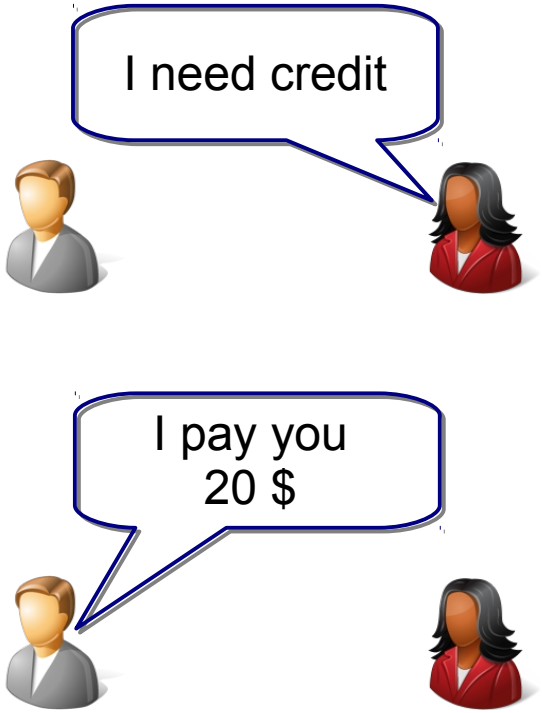
Credit Networks Introduction

Real World

Credit Network

Credit Networks Introduction

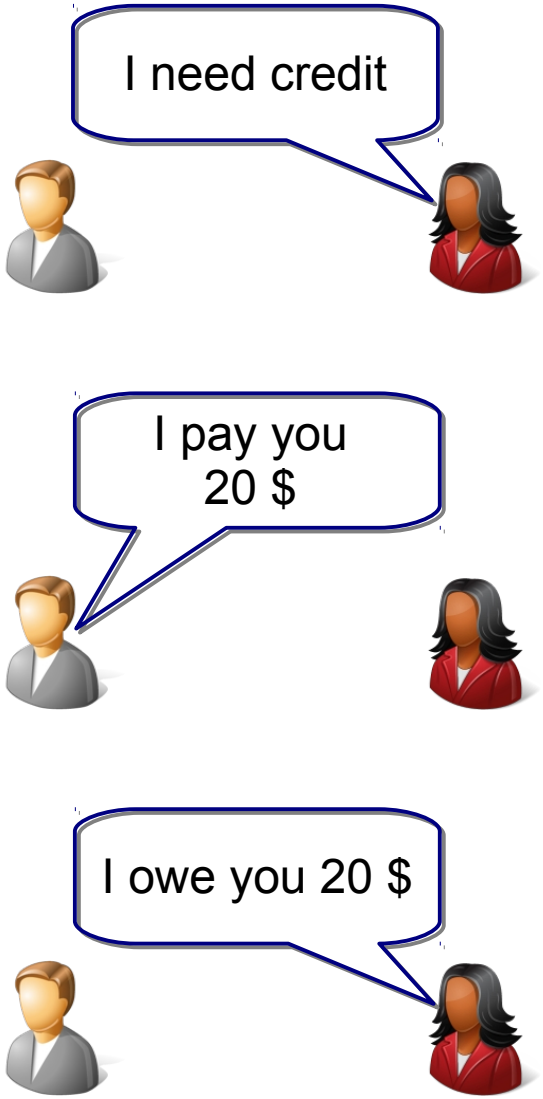
Real World



Credit Network

Credit Networks Introduction

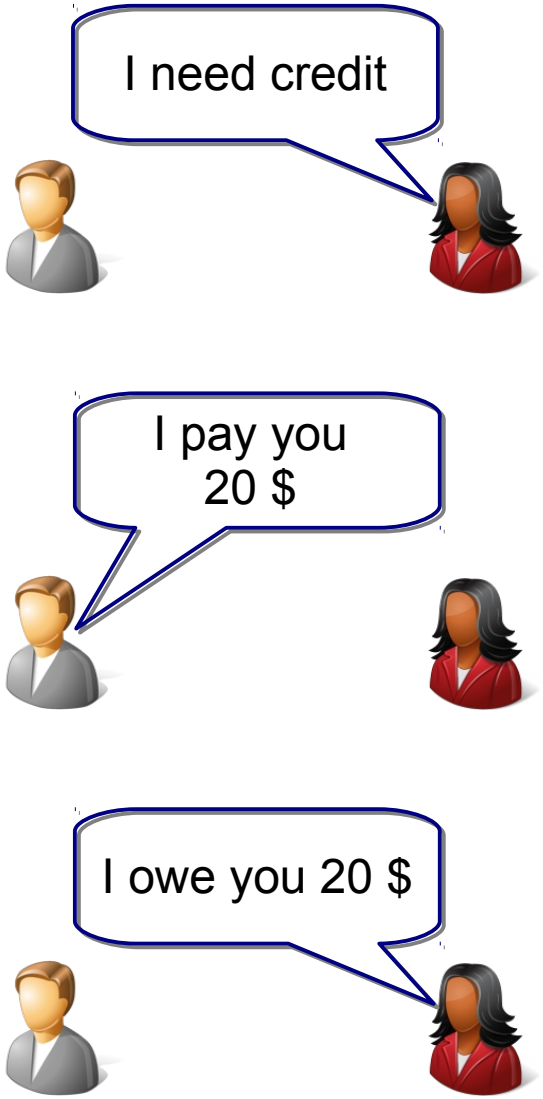
Real World



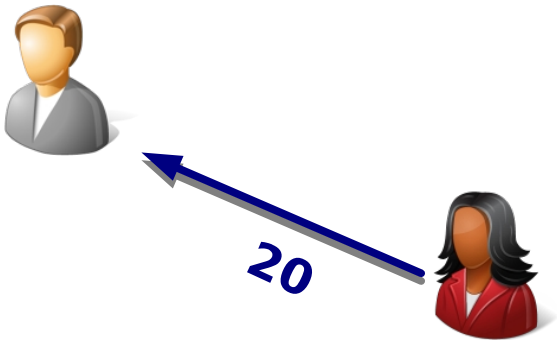
Credit Network

Credit Networks Introduction

Real World

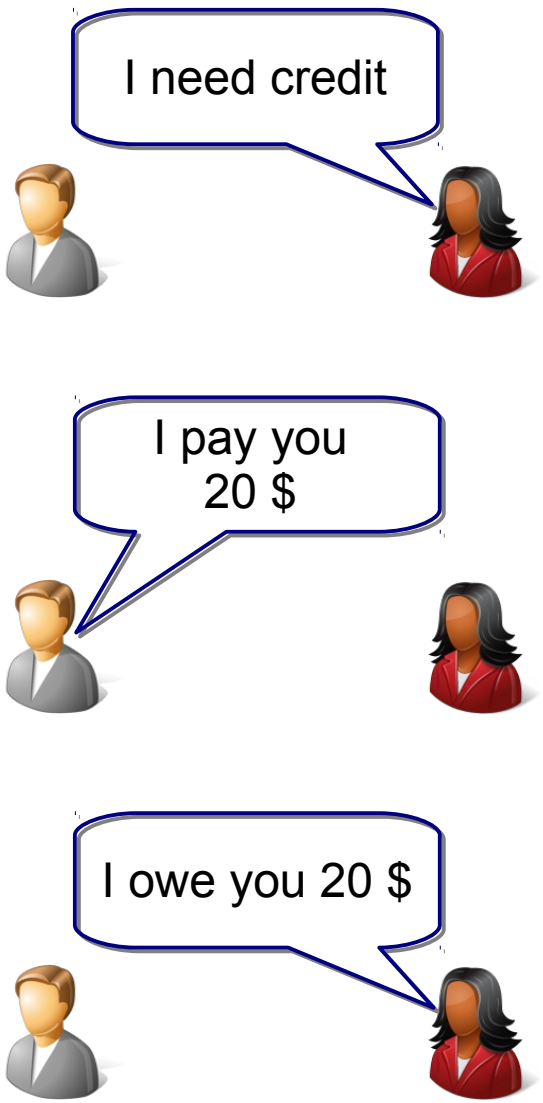


Credit Network

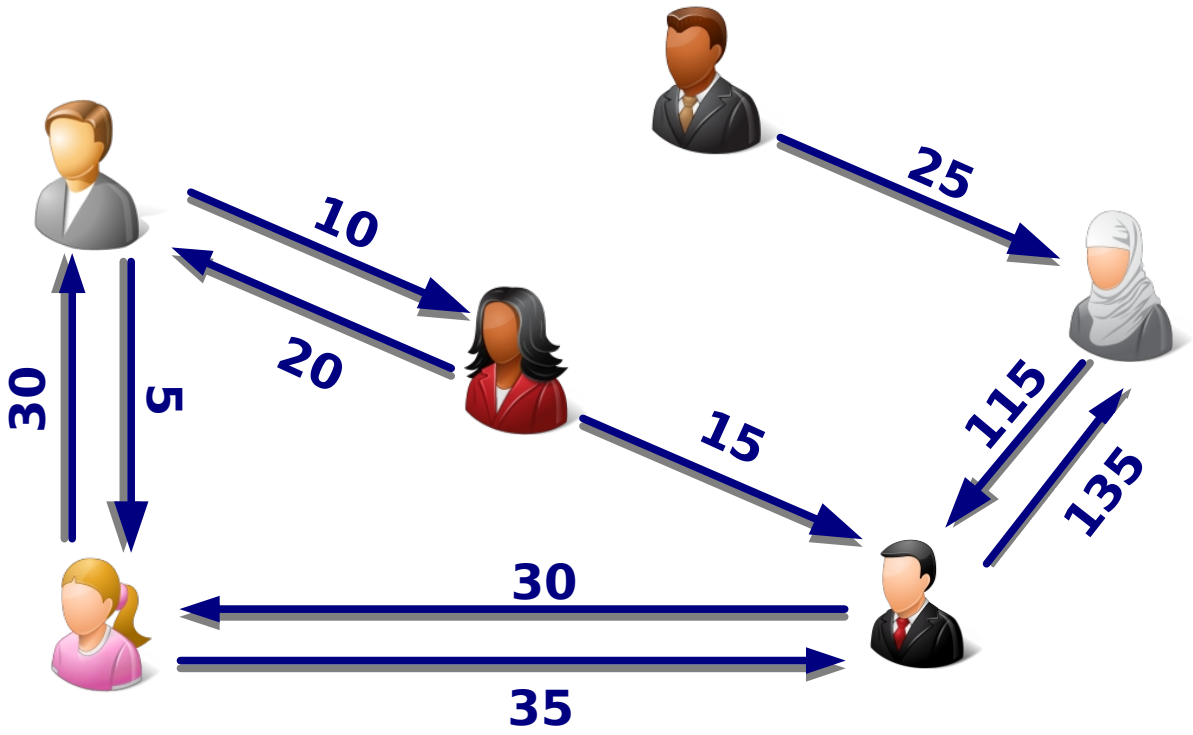


Credit Networks Introduction

Real World

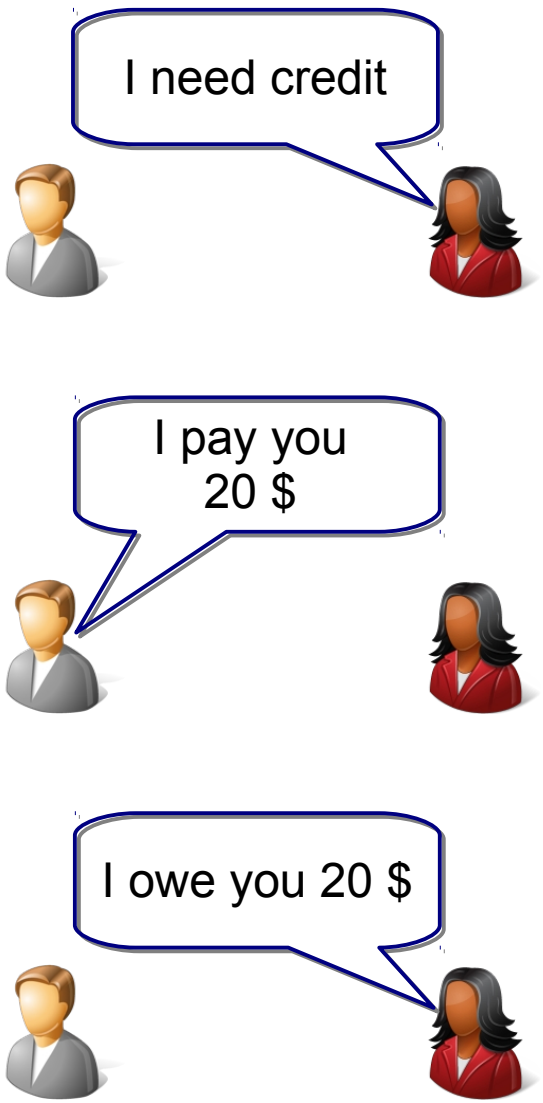


Credit Network

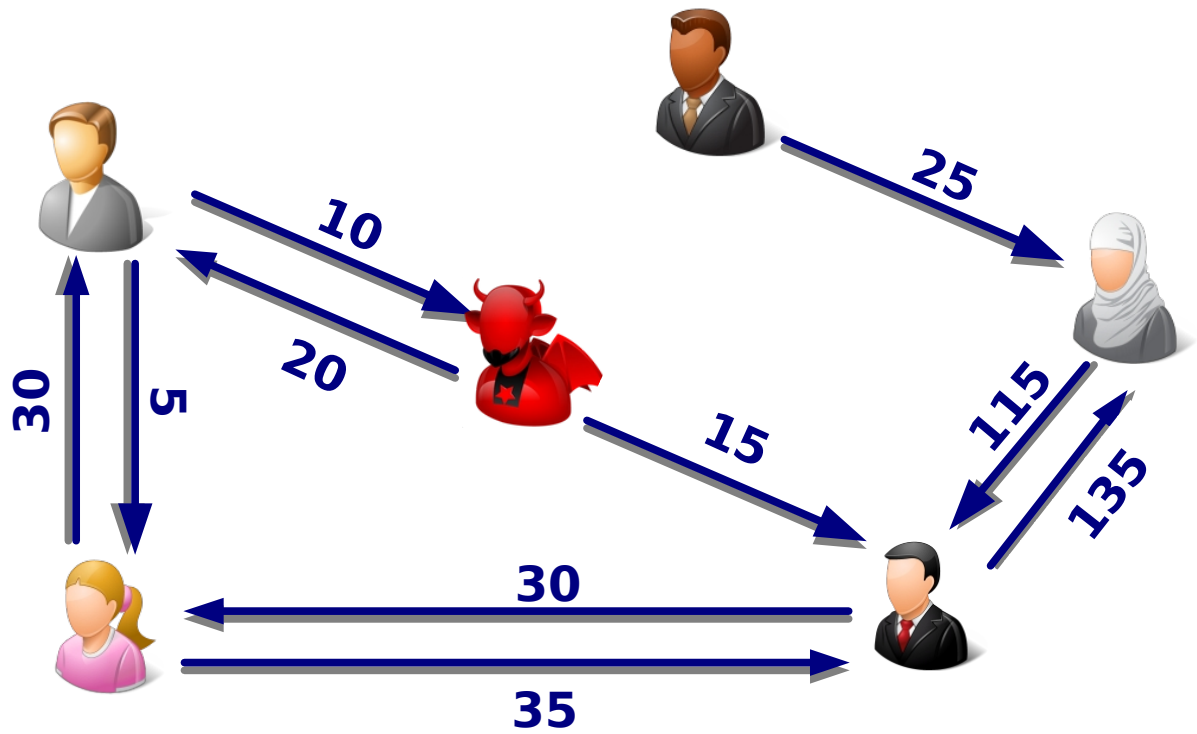


Credit Networks Introduction

Real World

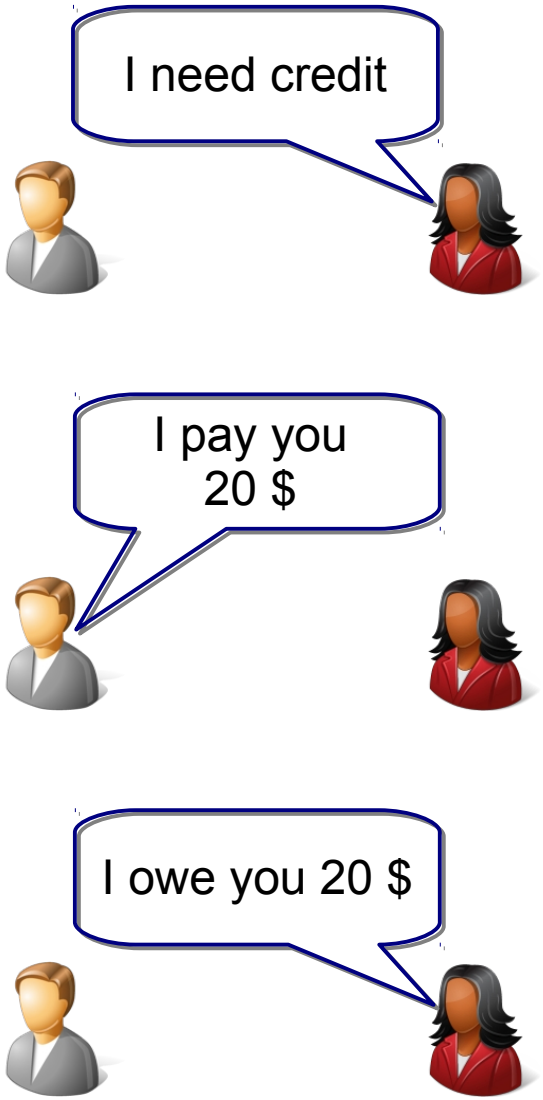


Credit Network

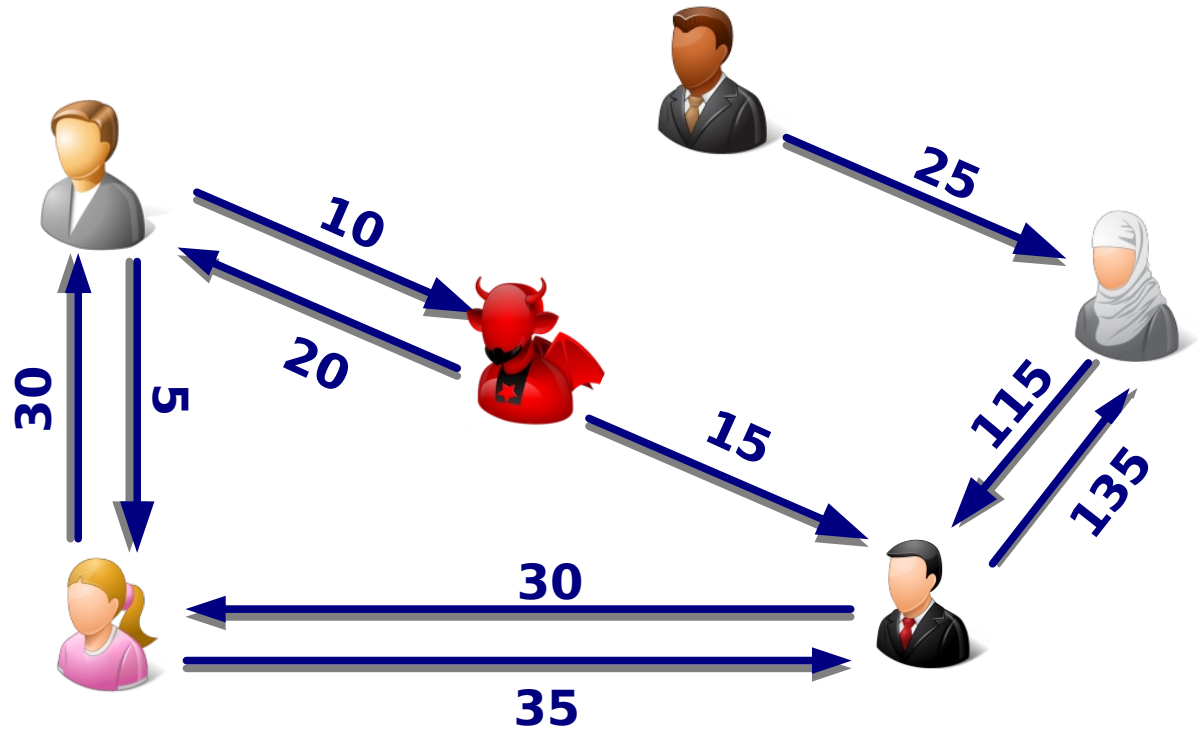


Credit Networks Introduction

Real World



Credit Network



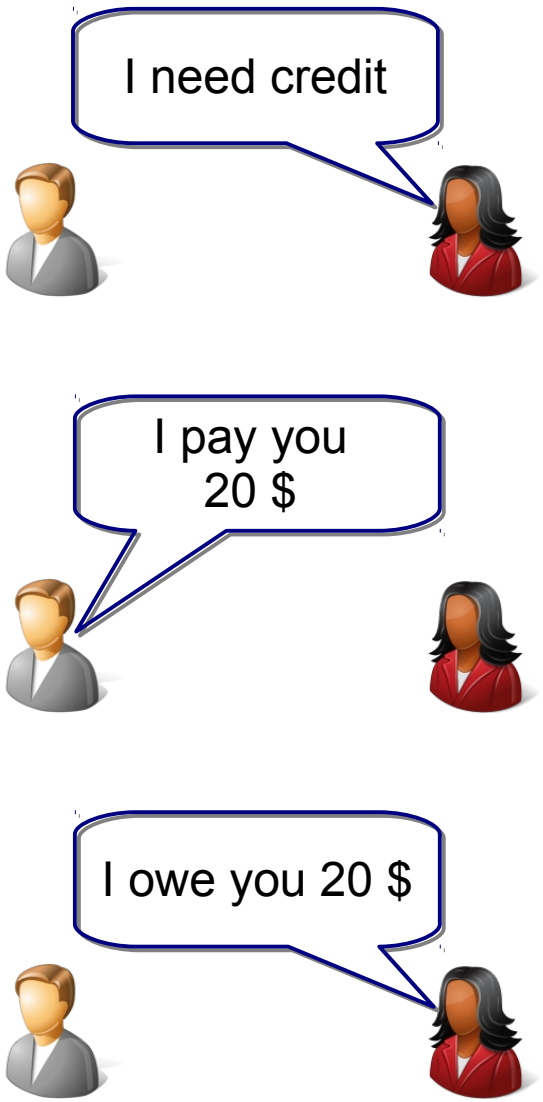
Misbehaving user's effect is:

Localized

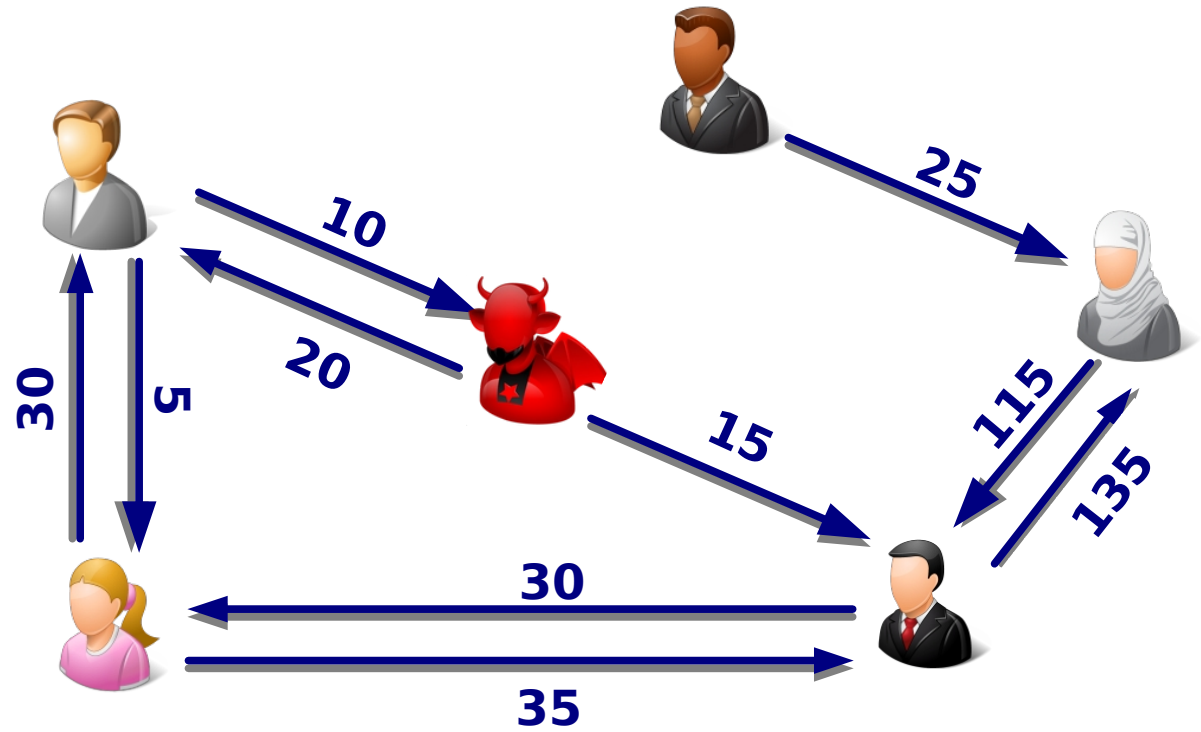
Bounded

Credit Networks Introduction

Real World



Credit Network



Misbehaving user's effect is:

Localized

Bounded

Multiple applications:

Ostra: mitigate spam in email system

Bazaar: strengthen online marketplaces, e.g., eBay

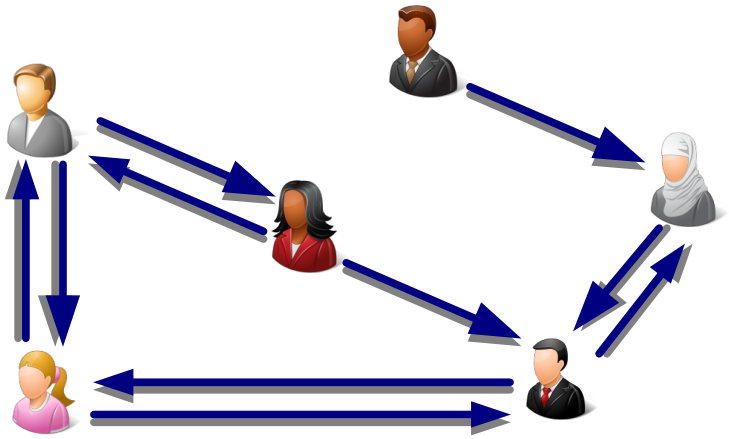
Etc.

Credit Networks Application: Payment Systems

- Payment systems: **Ripple [> 140,000 users, > $15M transaction volume]**

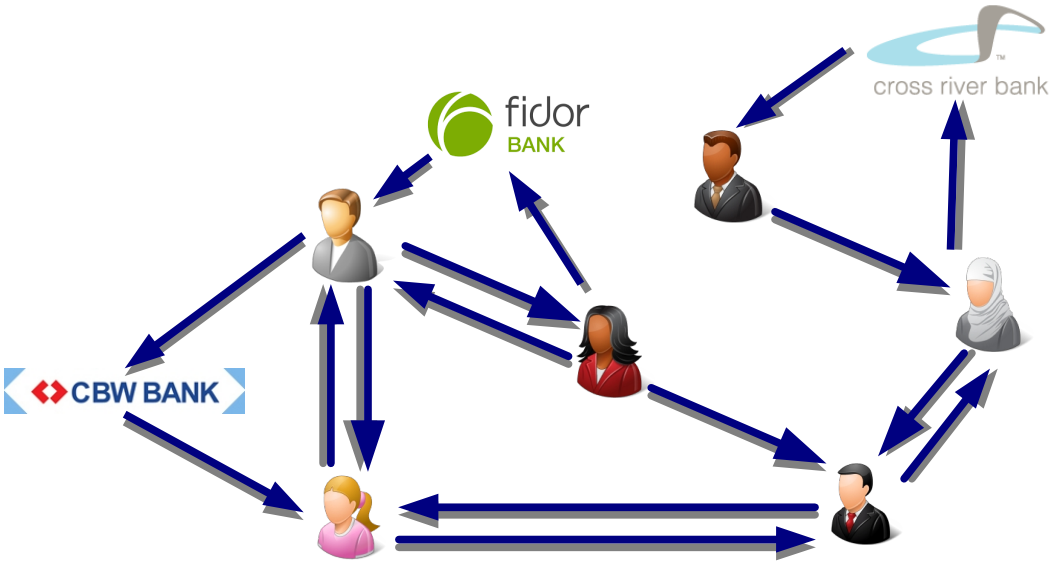
Credit Networks Application: Payment Systems

- Payment systems: **Ripple [> 140,000 users, > $15M transaction volume]**



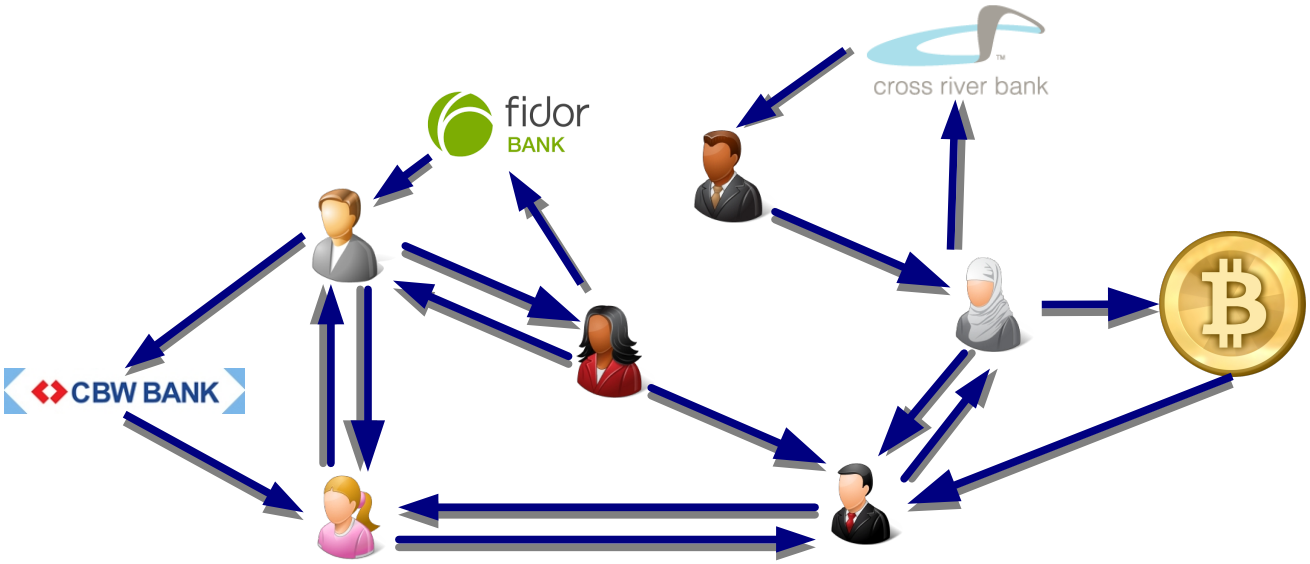
Credit Networks Application: Payment Systems

- Payment systems: **Ripple [> 140,000 users, > $15M transaction volume]**



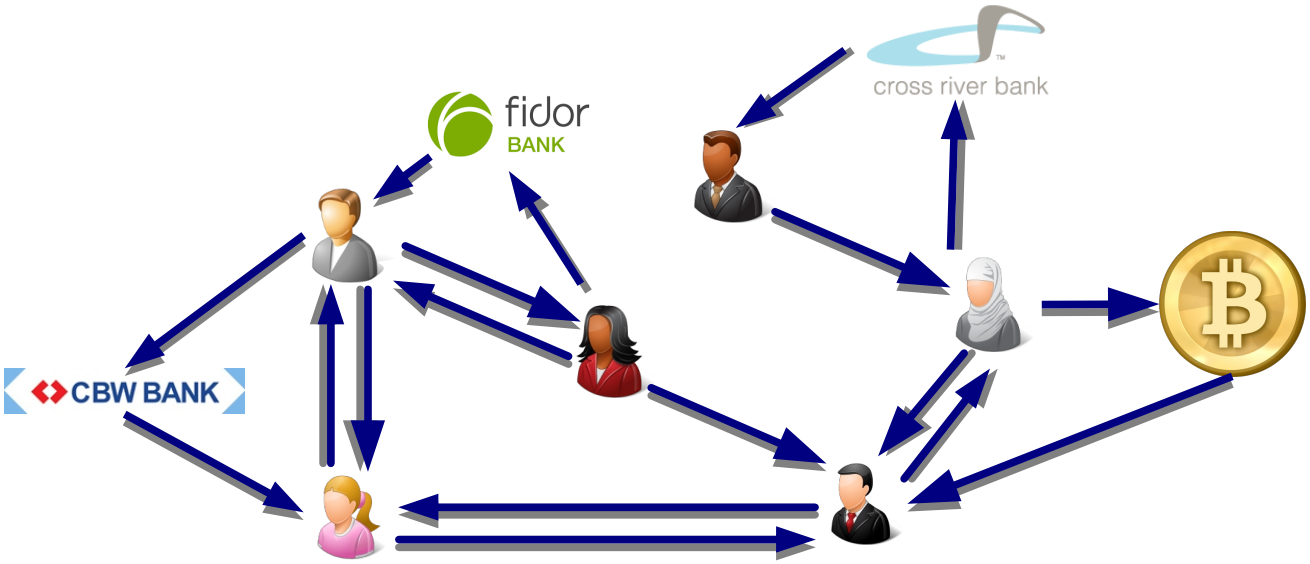
Credit Networks Application: Payment Systems

- Payment systems: **Ripple [> 140,000 users, > $15M transaction volume]**



Credit Networks Application: Payment Systems

- Payment systems: **Ripple [> 140,000 users, > $15M transaction volume]**



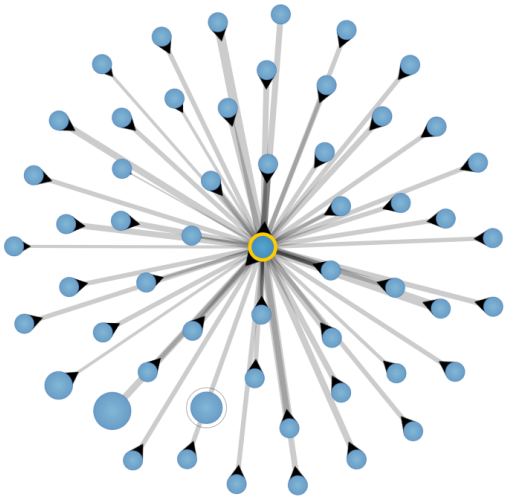
	Banking System	Ripple
Transaction	~ 1 day	~ 5 seconds
Multi-currency & worldwide transactions	High fees	Small fees
Integrity	Bank-only verifiable	Publicly verifiable

Public Verifiability & Privacy Problem

Ledger

	50
	30
fidor BANK	200
...	...

Credit links



Transaction details

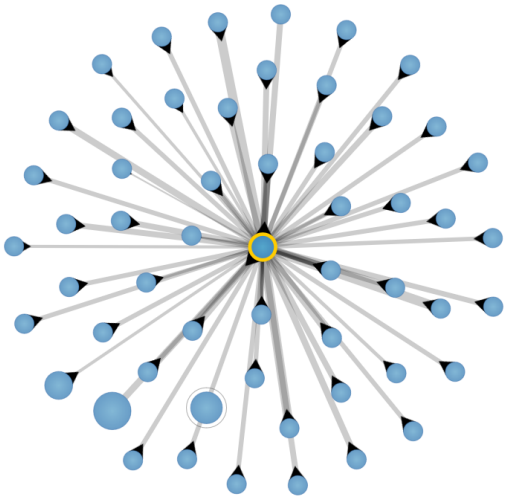
Account	Destination	Amount
rwvctTPLKZqK59f1fXpDkQ…	rMnVZ9maUWp5cAvmqBECZM…	300/XRP
rLSBpSquSHKbbfvcKt1c54…	rKoDt7VL83AKJZewLxVZEs…	75/XRP
r428G9fSSmD4SYmnDra16B…	rBeToNo4AwHaNbRX2n4BNC…	0.0693402709148/CCK/rB…
rhD759dbJMrzMNL4QbvQe9…	r95pWKA1K55fy7EJWrqJ9b…	300/XRP
r42WJGvV9MJa4t5QcF8Cnx…	rBeToNo4AwHaNbRX2n4BNC…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

Public Verifiability & Privacy Problem

Ledger

	50
	30
fidor BANK	200
...	...

Credit links



Transaction details

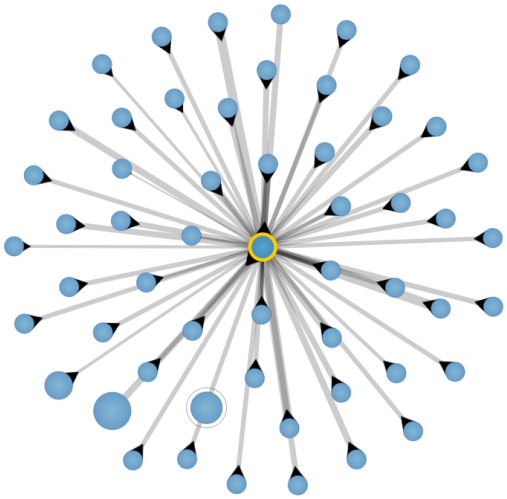
Account	Destination	Amount
rwvctTPLKZqK59f1fXpDkQ…	rMnVZ9maUWp5cAvmqBECZM…	300/XRP
rLSBpSquSHKbbfvcKt1c54…	rKoDt7VL83AKJZewLxVZEs…	75/XRP
r428G9fSSmD4SYmnDra16B…	rBeToNo4AwHaNbRX2n4BNC…	0.0693402709148/CCK/rB…
rhD759dbJMrzMNL4QbvQe9…	r95pWKA1K55fy7EJWrqJ9b…	300/XRP
r42WJGvV9MJa4t5QcF8Cnx…	rBeToNo4AwHaNbRX2n4BNC…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

Public Verifiability & Privacy Problem

Ledger

	30
	50
fidor BANK	200
...	...

Credit links



Transaction details

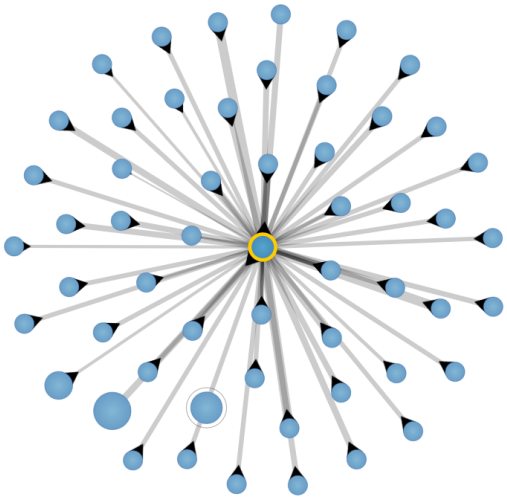
Account	Destination	Amount
rwvctTPLKZqK59f1fXpDkQ…	rMnVZ9maUWp5cAvmqBECZM…	300/XRP
rLSBpSquSHKbbfvcKt1c54…	rKoDt7VL83AKJZewLxVZEs…	75/XRP
r428G9fSSmD4SYmnDra16B…	rBeToNo4AwHaNbRX2n4BNC…	0.0693402709148/CCK/rB…
rhD759dbJMrzMNL4QbvQe9…	r95pWKA1K55fy7EJWrqJ9b…	300/XRP
r42WJGvV9MJa4t5QcF8Cnx…	rBeToNo4AwHaNbRX2n4BNC…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

Public Verifiability & Privacy Problem

Ledger

	30
	50
fidor BANK	200
...	...

Credit links



Transaction details

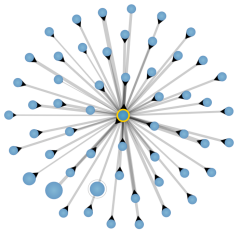
Account	Destination	Amount
rwvctTPLKZqK59f1fXpDkQ…	rMnVZ9maUWp5cAvmqBECZM…	300/XRP
rLSBpSquSHKbbfvcKt1c54…	rKoDt7VL83AKJZewLxVZEs…	75/XRP
r428G9fSSmD4SYmnDra16B…	rBeToNo4AwHaNbRX2n4BNC…	0.0693402709148/CCK/rB…
rhD759dbJMrzMNL4QbvQe9…	r95pWKA1K55fy7EJWrqJ9b…	300/XRP
r42WJGvV9MJa4t5QcF8Cnx…	rBeToNo4AwHaNbRX2n4BNC…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

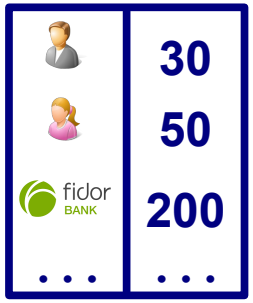
LINKABLE ANONYMITY

Contributions

- **Identify privacy problem** as an important issue in credit networks

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

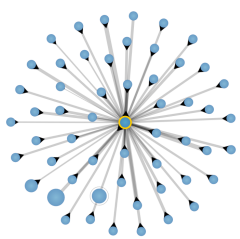


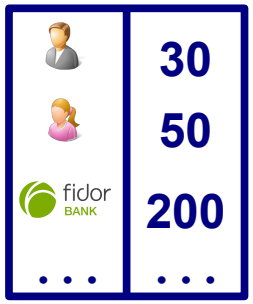


Contributions

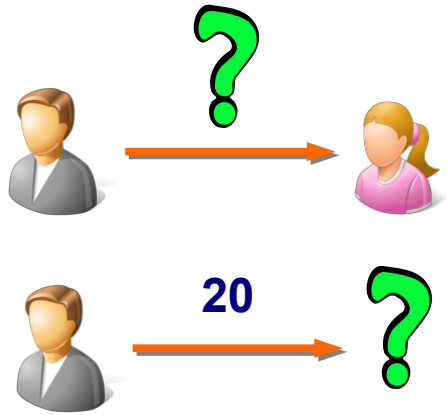
- **Identify privacy problem** as an important issue in credit networks

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





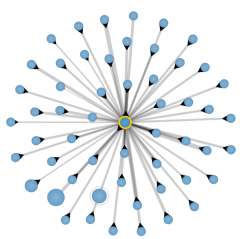
- **Define privacy properties** for credit networks: value and receiver privacy

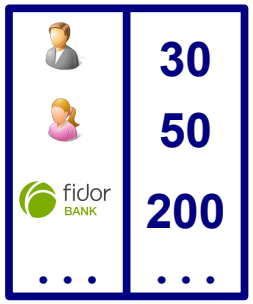


Contributions

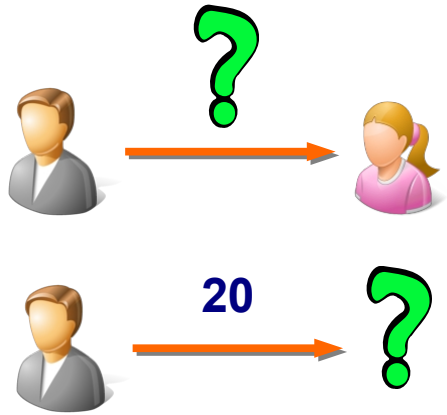
- **Identify privacy problem** as an important issue in credit networks

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

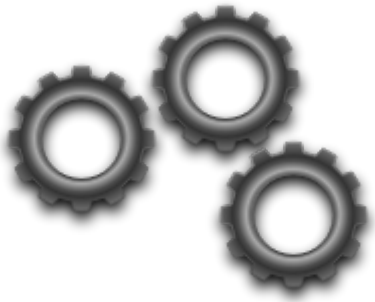




- **Define privacy properties** for credit networks: value and receiver privacy



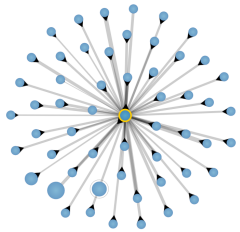
- **PrivPay: novel architecture** combining trusted hardware and oblivious algorithms

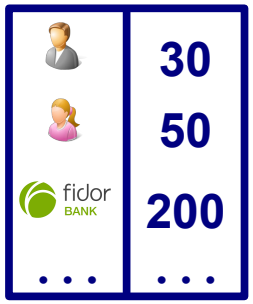


Contributions

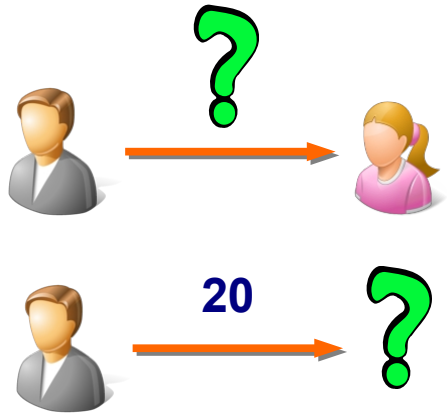
- **Identify privacy problem** as an important issue in credit networks

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

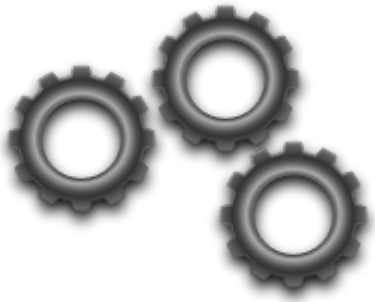




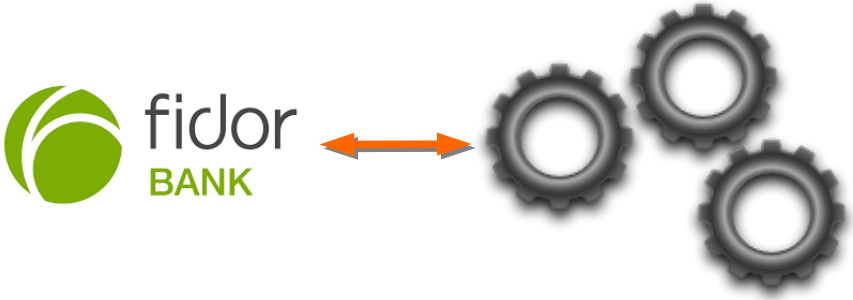
- **Define privacy properties** for credit networks: value and receiver privacy



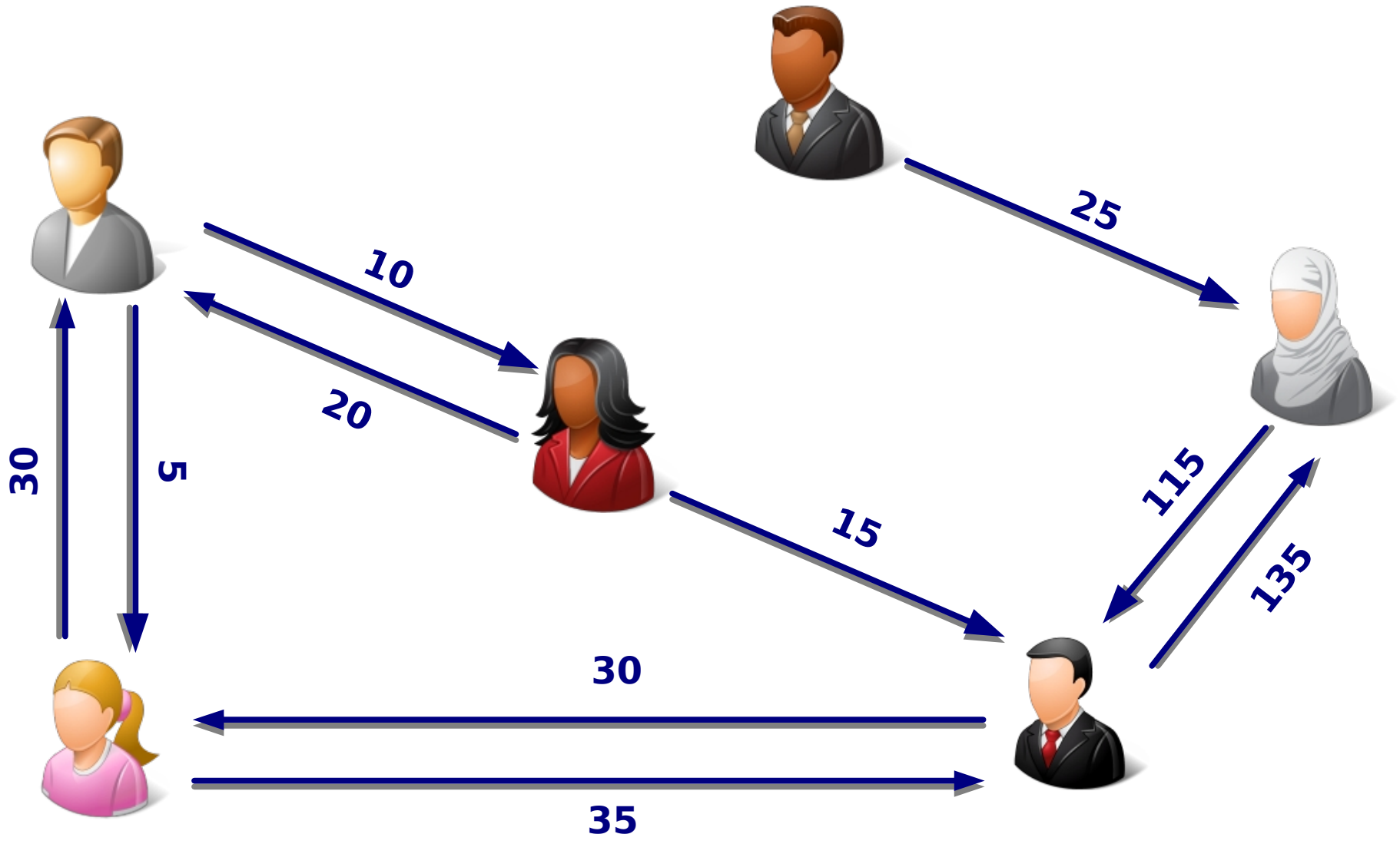
- **PrivPay: novel architecture** combining trusted hardware and oblivious algorithms



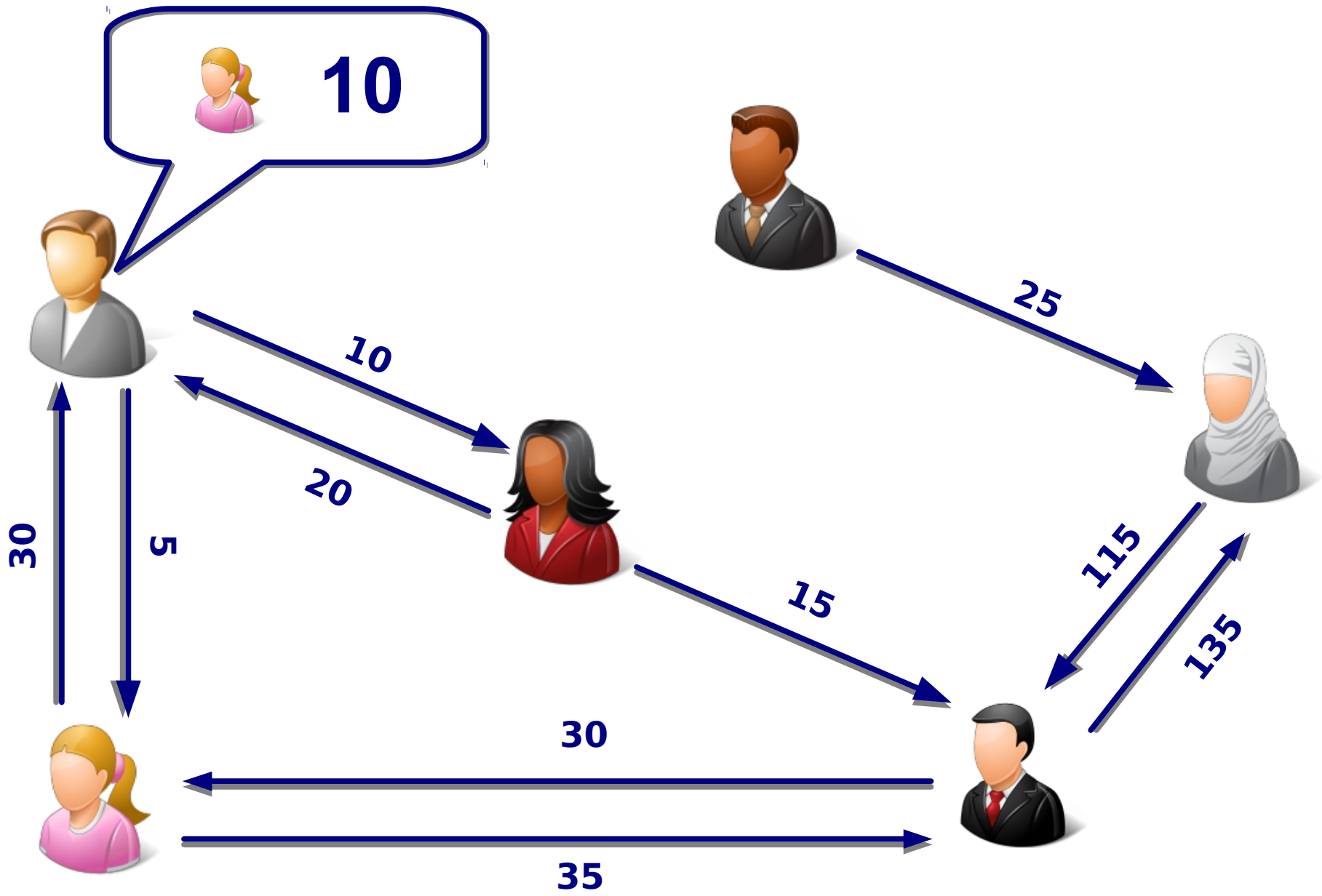
- Evaluation: **feasible to deploy** in practice



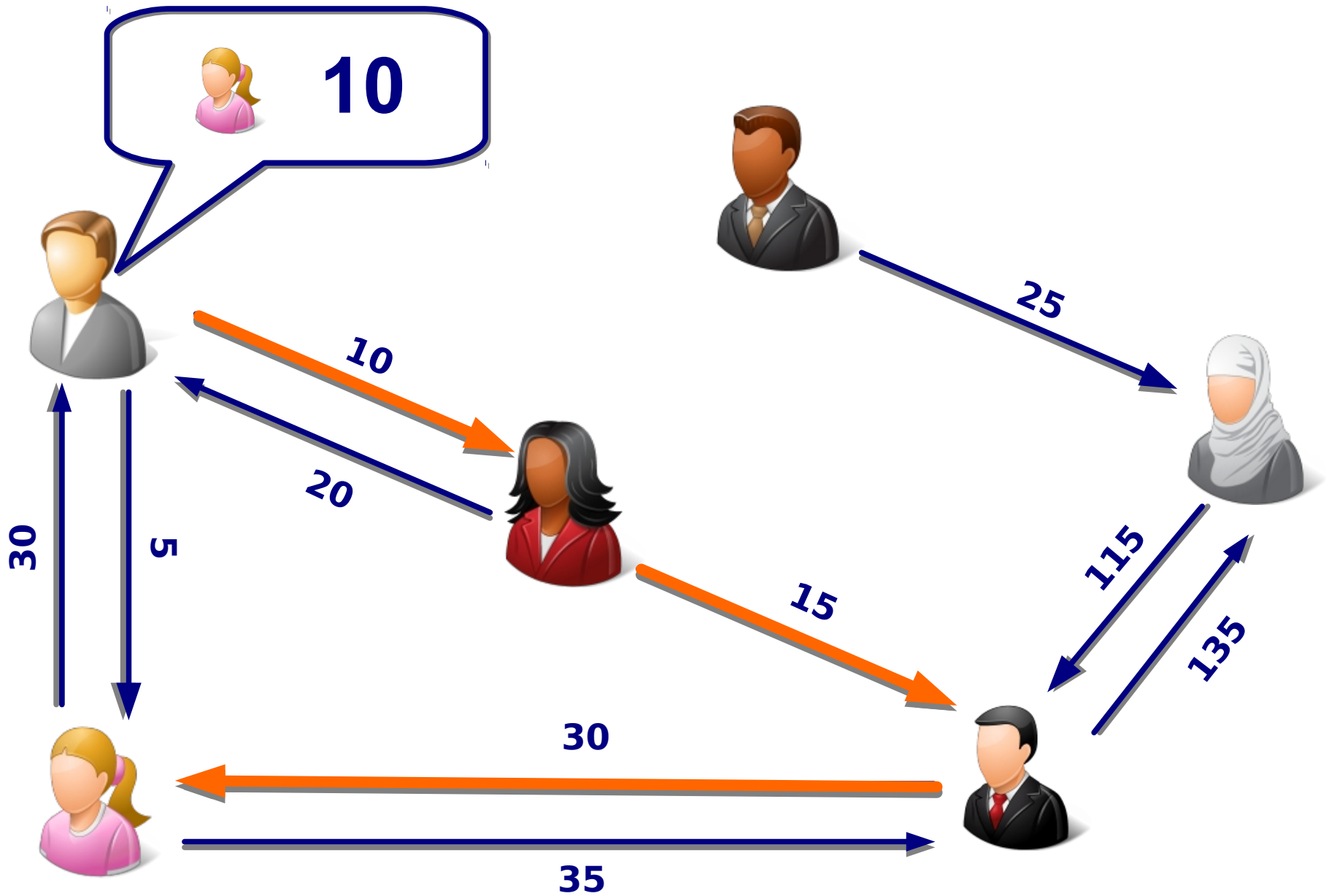
Credit Network Transaction



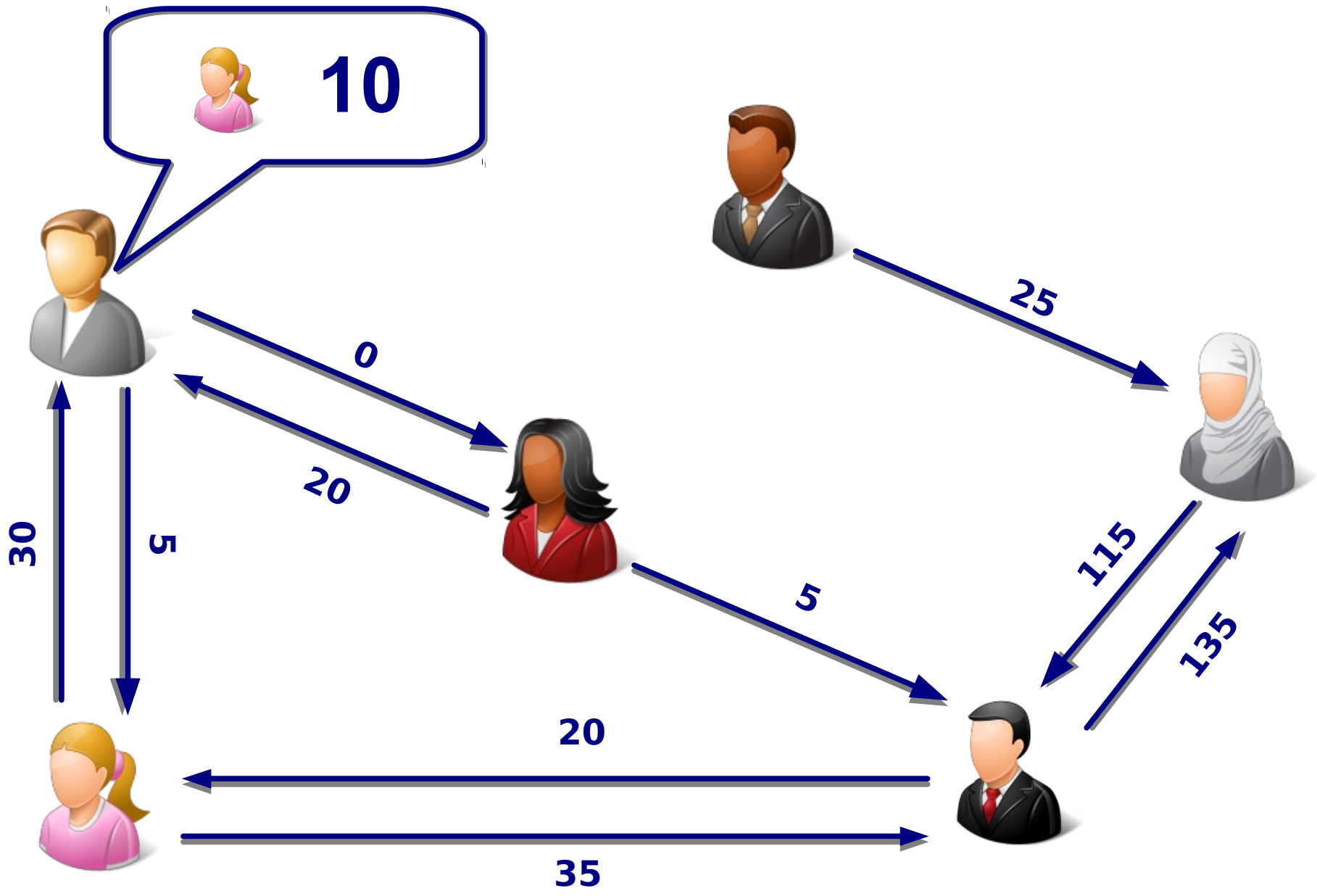
Credit Network Transaction



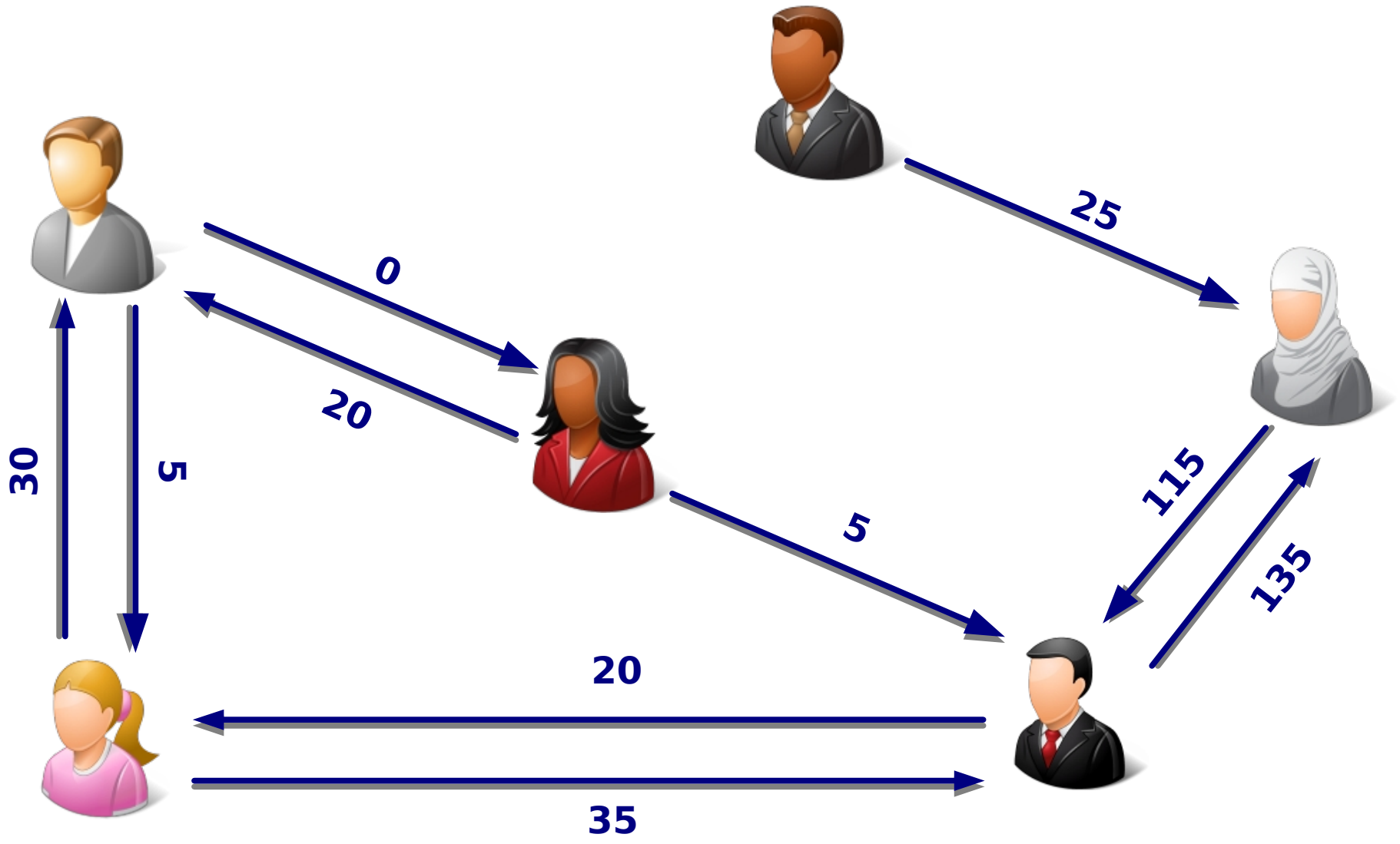
Credit Network Transaction



Credit Network Transaction



Credit Network Transaction



Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes

Credit Network: Routing challenge

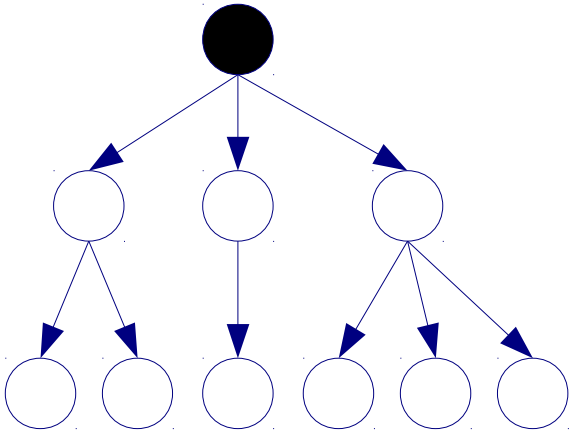
Routing: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes

Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

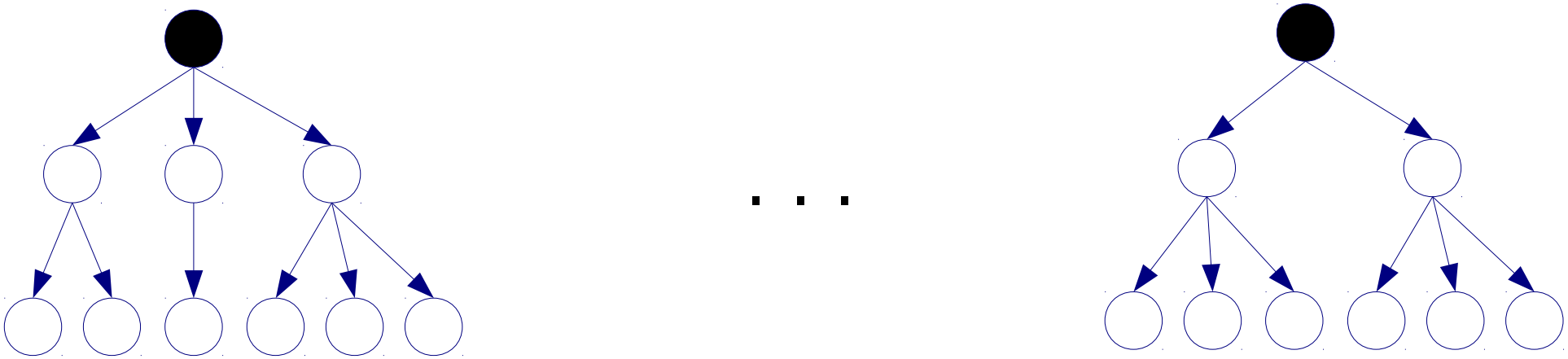
- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes



Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

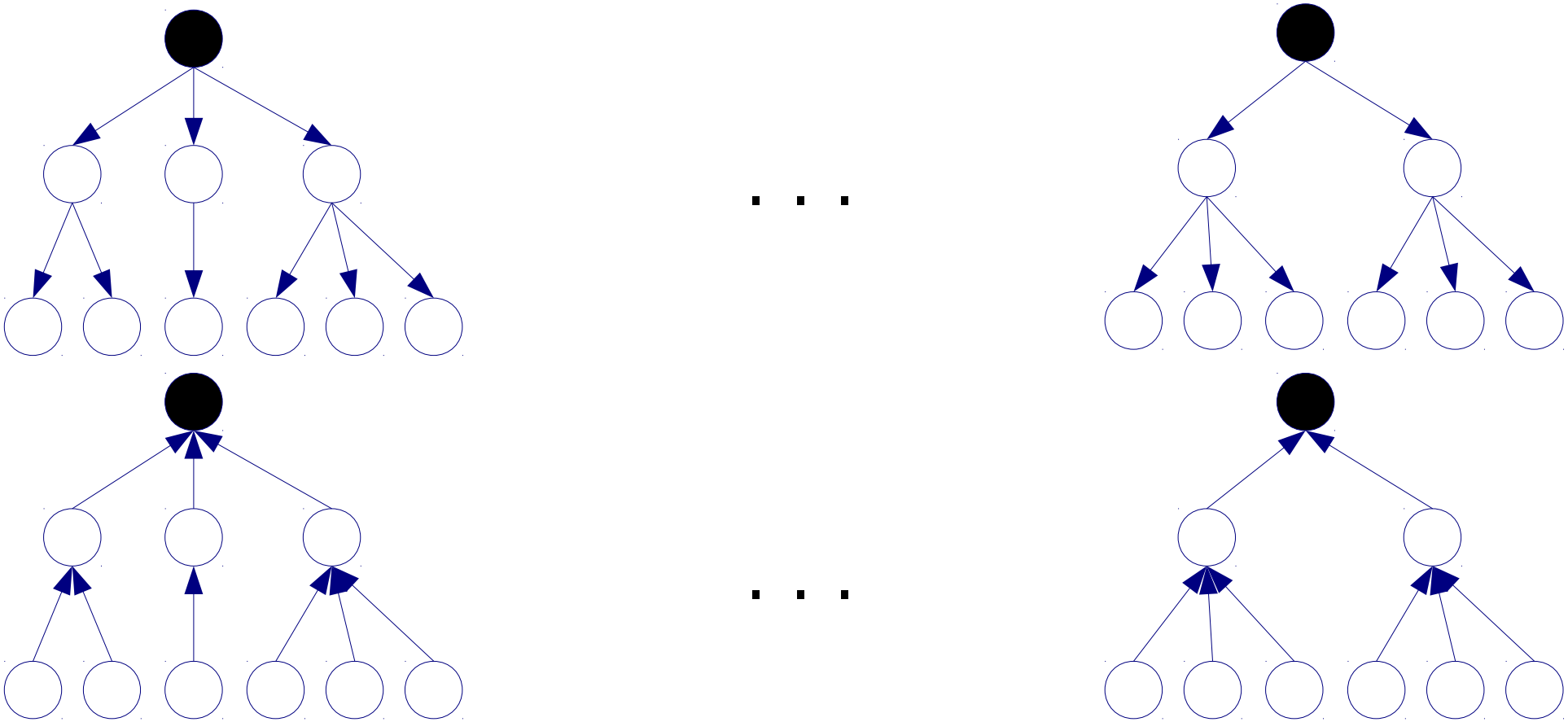
- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes



Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

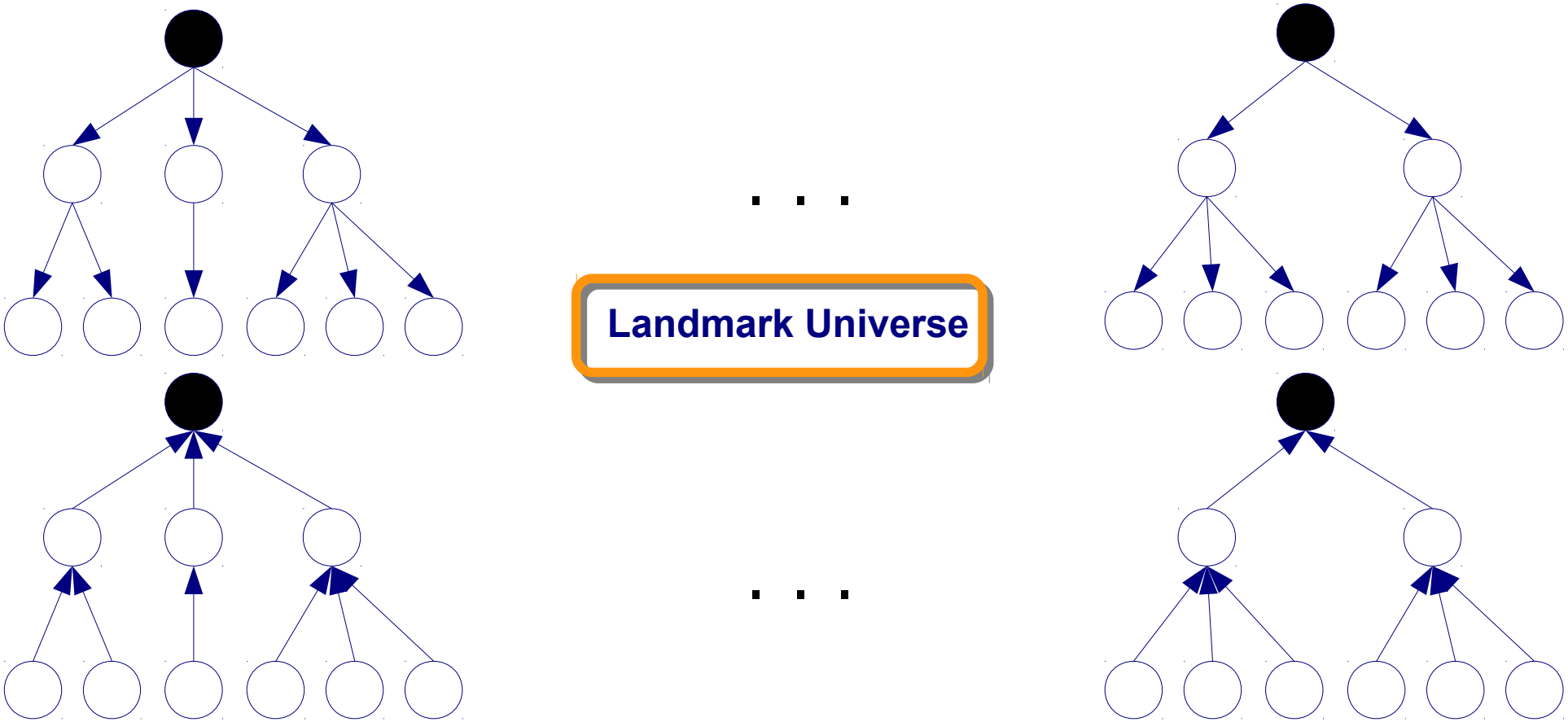
- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes



Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

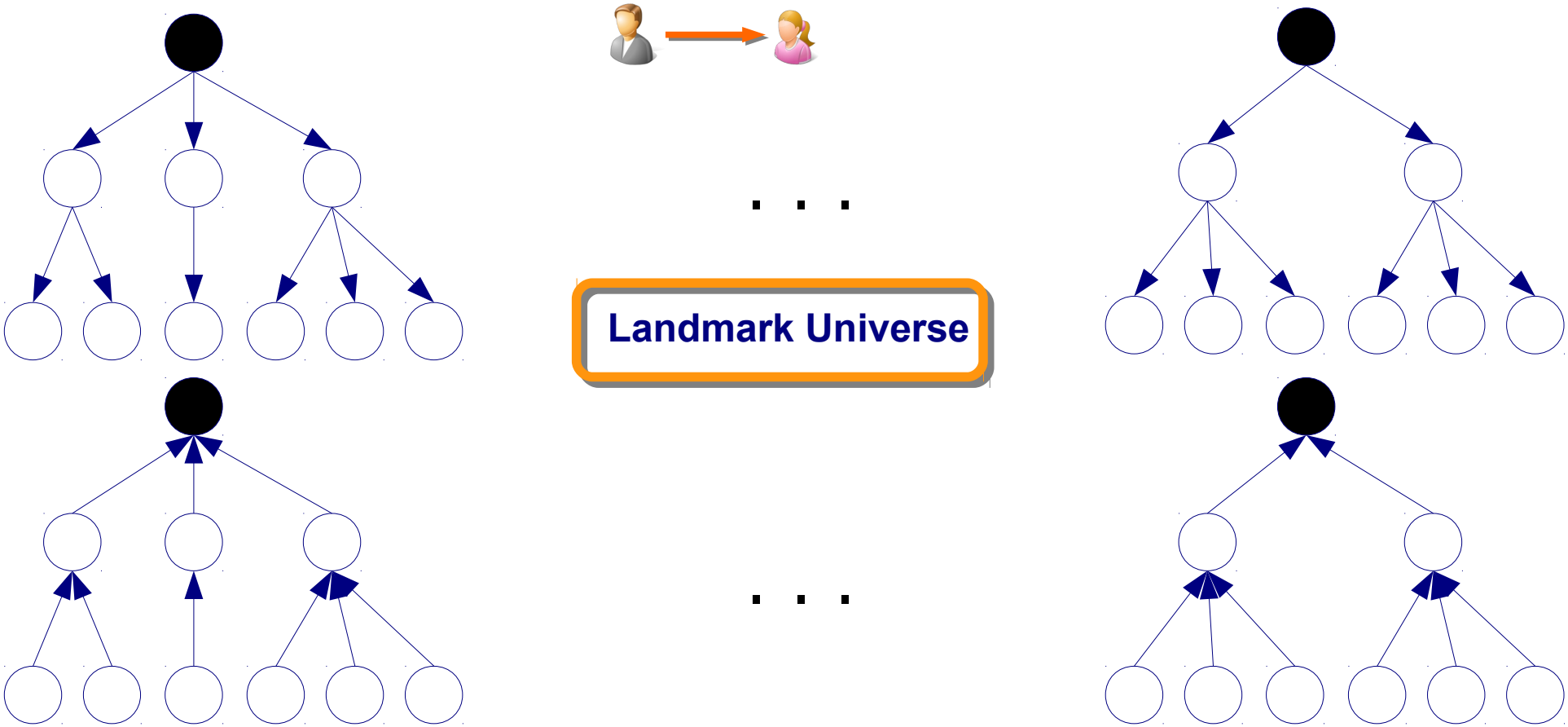
- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes



Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

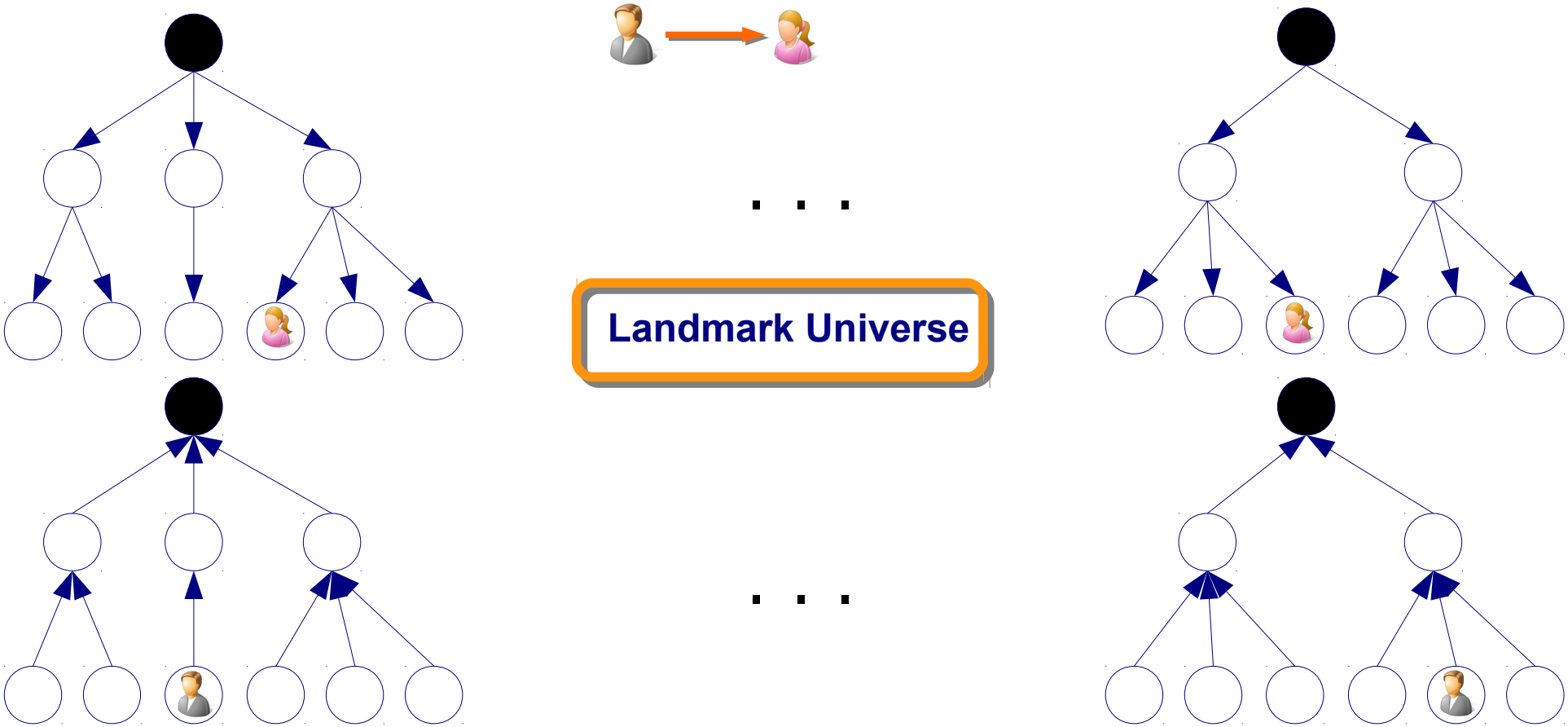
- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes



Credit Network: Routing challenge

Routing: determine credit route from a sender to a receiver

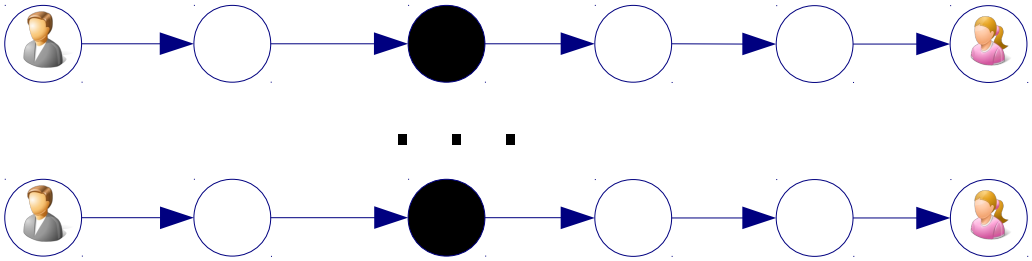
- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes



Credit Network: Routing challenge

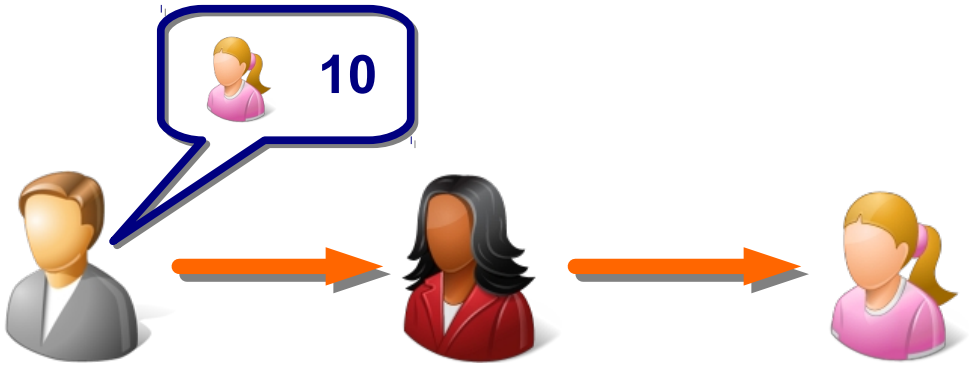
Routing: determine credit route from a sender to a receiver

- Existing systems use the max-flow approach:
  - **Inefficient** algorithms: $O(V^3)$ or $O(V^2 log(E))$
- Landmark routing [Tsuchiya, SIGCOMM'98]: calculate only a subset of all possible routes

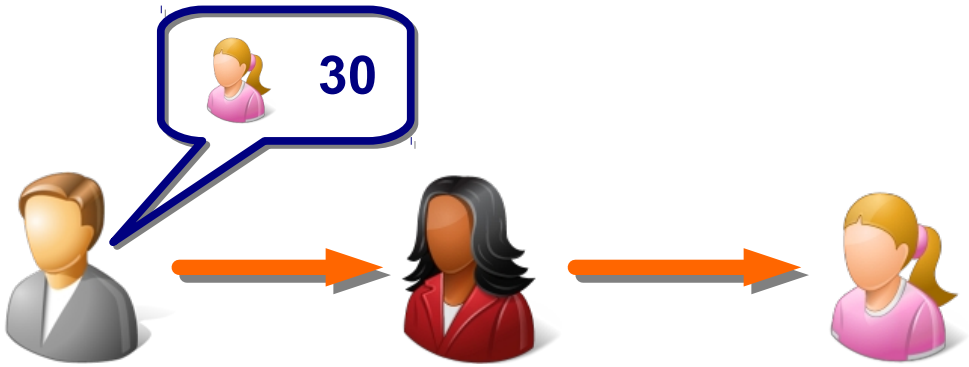


Credit Network: Privacy Definitions

Transaction Value Privacy

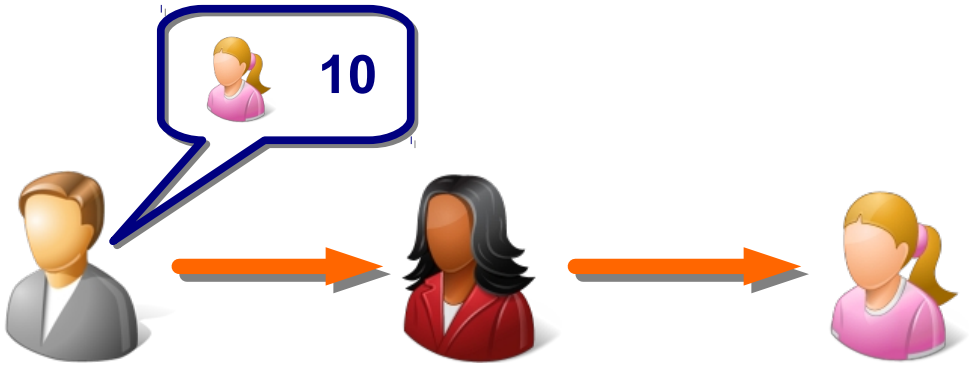


≈

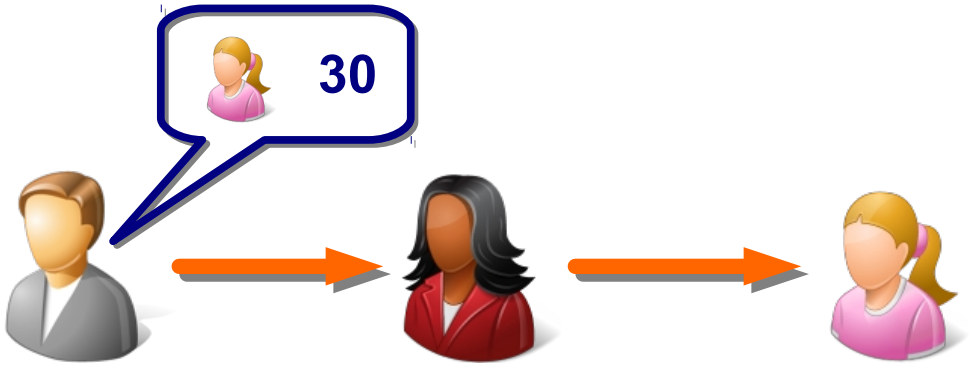


Credit Network: Privacy Definitions

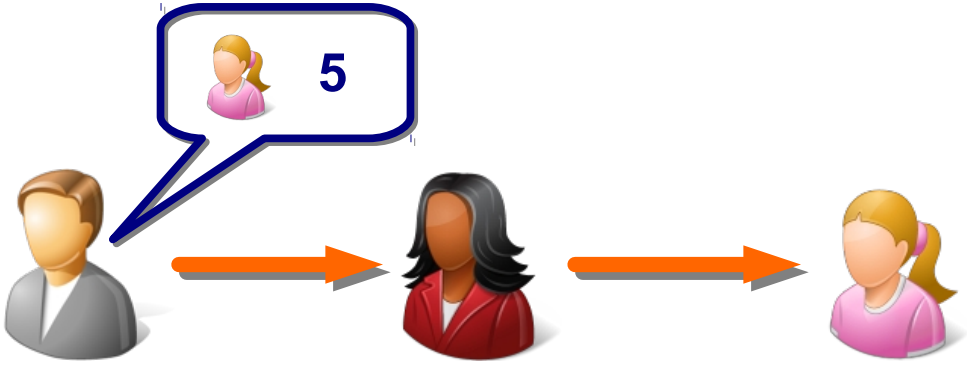
Transaction Value Privacy



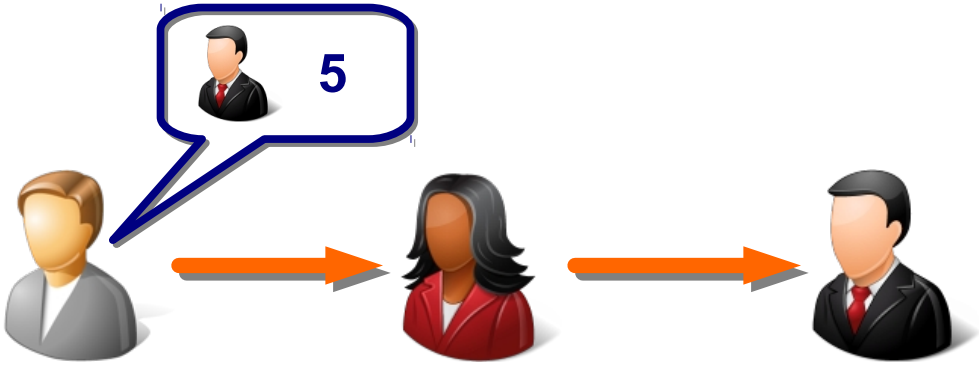
≈



Transaction Receiver Privacy



≈



Transaction Value Privacy: Definition (I)

Query phase

payment

change link

Challenger

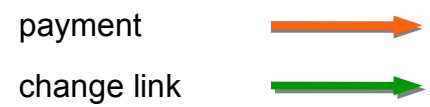
Attacker

Transaction Value Privacy: Definition (I)

Query phase

Transaction Value Privacy: Definition (I)

Query phase



Challenger

Attacker

Transaction Value Privacy: Definition (I)

Query phase

Challenger

Attacker

payment

change link

Transaction Value Privacy: Definition (I)

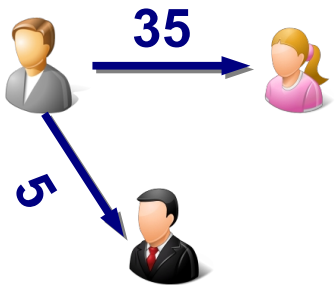
Query phase

Transaction Value Privacy: Definition (I)

Query phase

payment

change link



Challenger

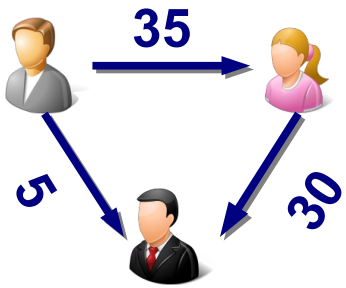
Attacker

Transaction Value Privacy: Definition (I)

Query phase

payment

change link



Challenger

Attacker

Transaction Value Privacy: Definition (I)

Query phase

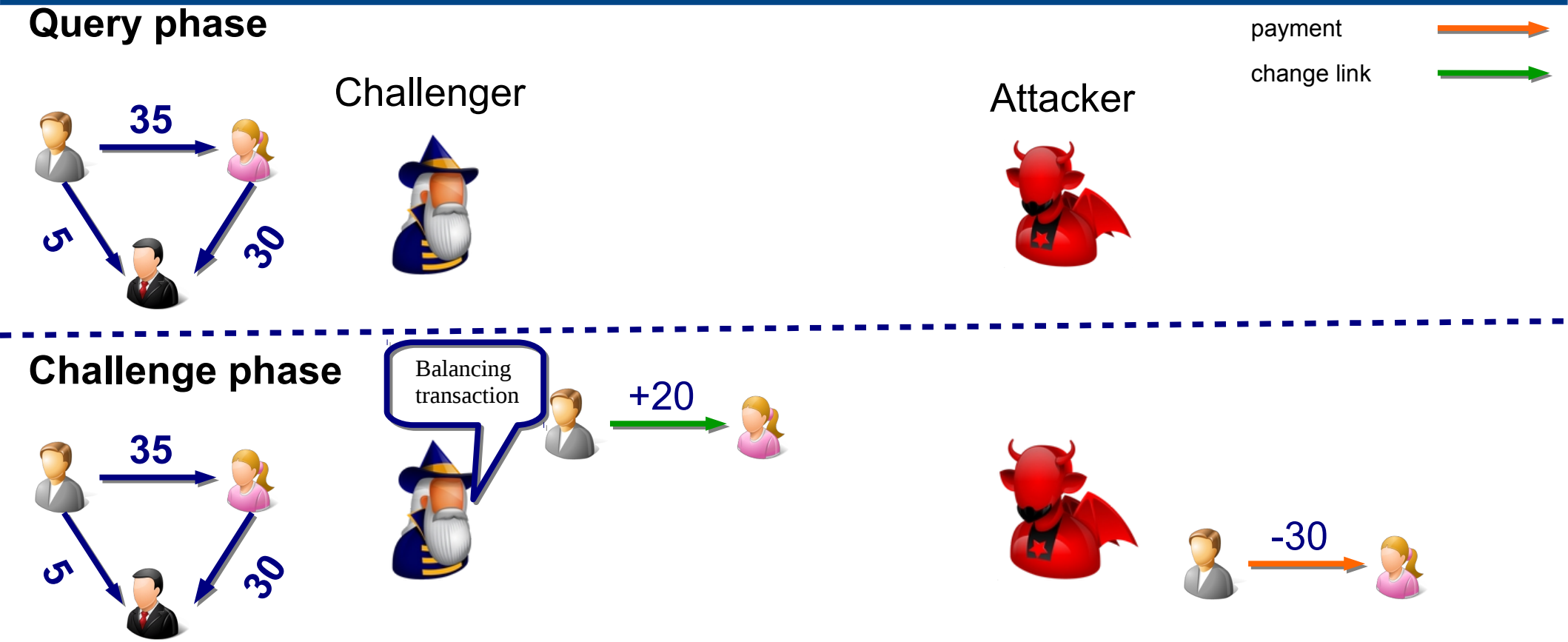
Challenge phase

Transaction Value Privacy: Definition (I)

Query phase

Challenge phase

Transaction Value Privacy: Definition (I)



Transaction Value Privacy: Definition (I)

Query phase

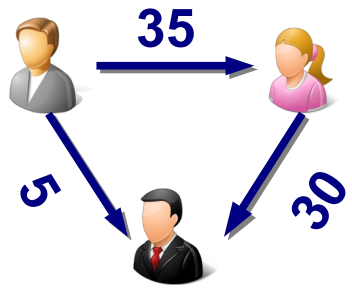
Challenge phase

Transaction Value Privacy: Definition (I)

Query phase

payment

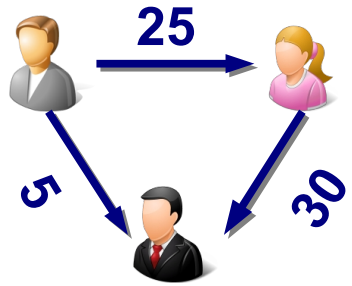
change link



Challenger

Attacker

Challenge phase

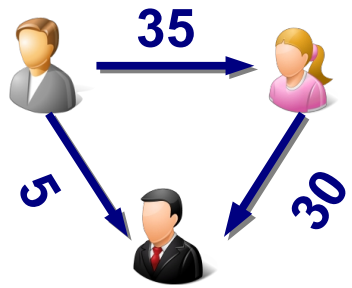


Transaction Value Privacy: Definition (I)

Query phase

payment

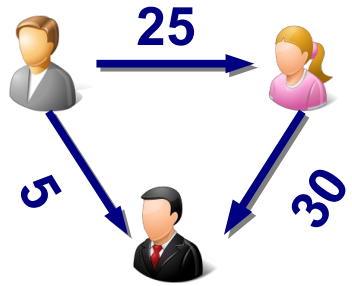
change link



Challenger

Attacker

Challenge phase

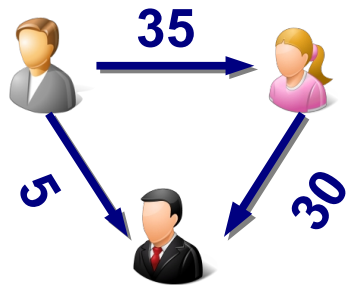


Transaction Value Privacy: Definition (I)

Query phase

payment

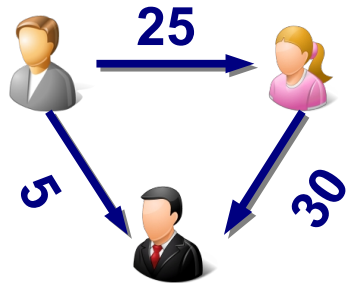
change link



Challenger

Attacker

Challenge phase



Query phase

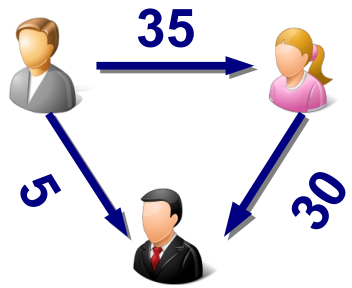
. . .

Transaction Value Privacy: Definition (I)

payment

change link

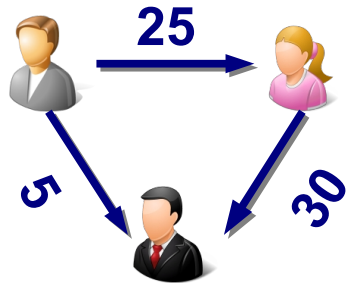
Query phase



Challenger

Attacker

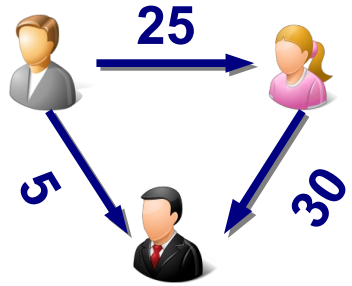
Challenge phase

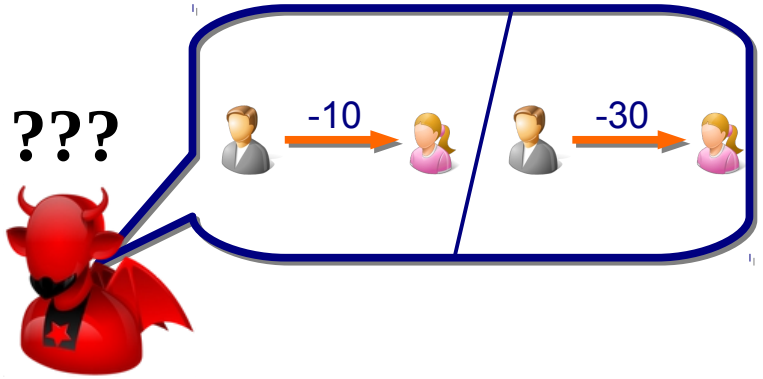


Query phase

. . .

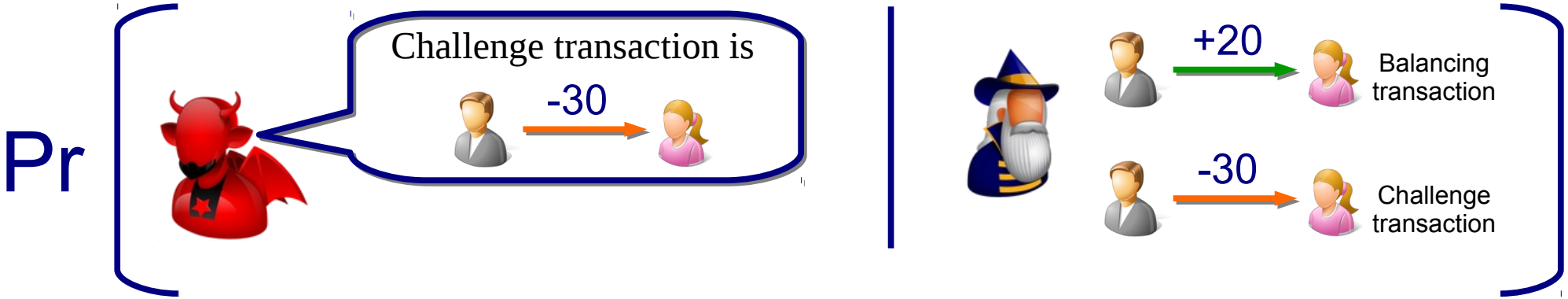
Guess phase



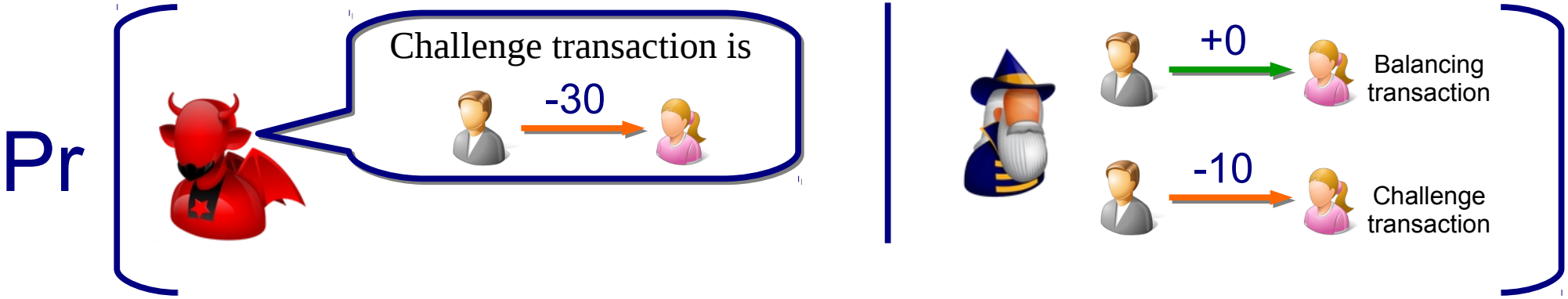


Transaction Value Privacy: Definition (II)

A credit network satisfies transaction value privacy if:



≈

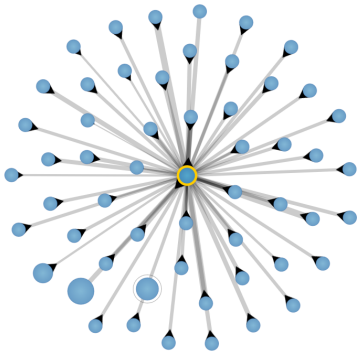


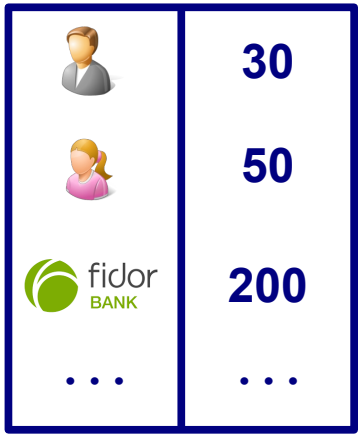
Credit Network: Privacy Challenge

Providing privacy is challenging:

- Hide transaction values → What is the paid amount?
- Hide transaction participants → Who are the sender and the receiver?

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



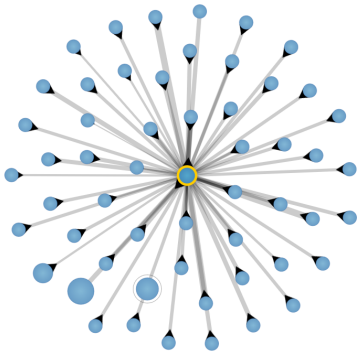


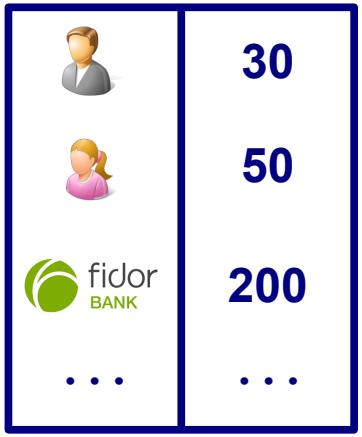
Credit Network: Privacy Challenge

Providing privacy is challenging:

- Hide transaction values → What is the paid amount?
- Hide transaction participants → Who are the sender and the receiver?

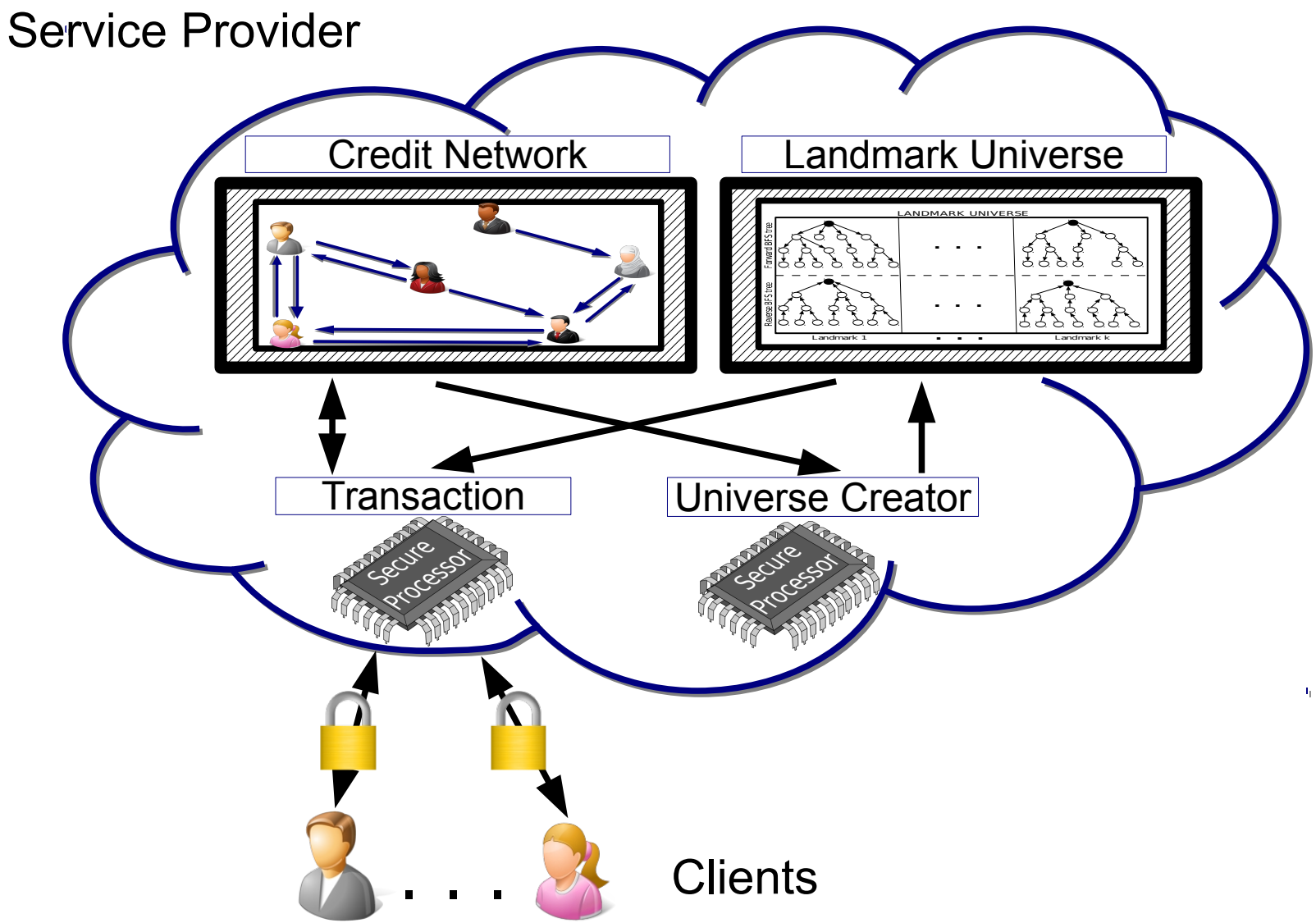
Account	Destination	Amount
rwvctTPLKZqK59f1fXpDkQ…	rMnVZ9maUWp5cAvmqBECZM…	300/XRP
rLSBpSquSHKbbfvcKt1c54…	rKoDt7VL83AKJZewLxVZEs…	75/XRP
r428G9fSSmD4SYmnDra16B…	rBeToNo4AwHaNbRX2n4BNC…	0.0693402709148/CCK/rB…
rhD759dbJMrzMNL4QbvQe9…	r95pWKA1K55fy7EJWrqJ9b…	300/XRP
r42WJGvV9MJa4t5QcF8Cnx…	rBeToNo4AwHaNbRX2n4BNC…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



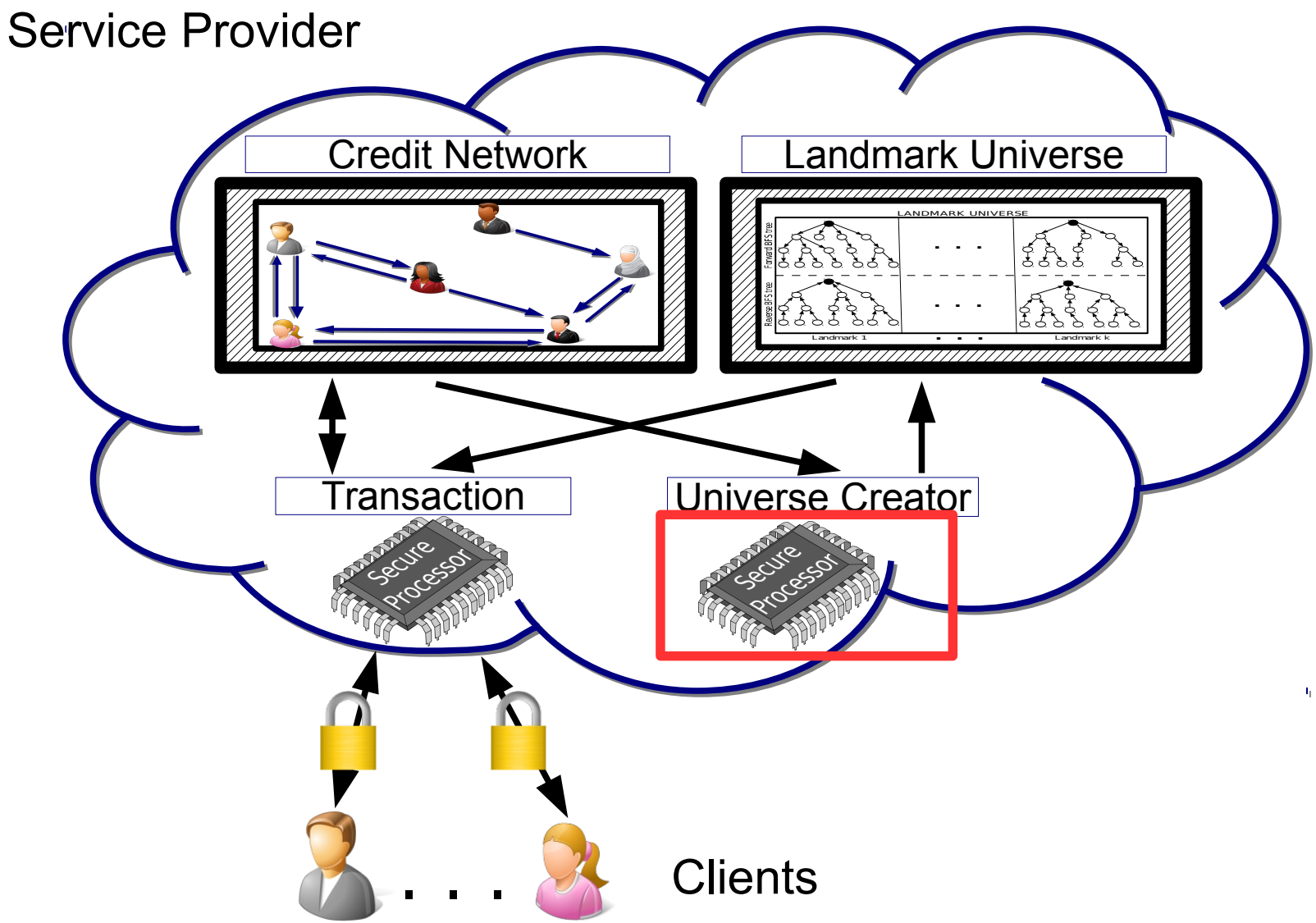


- In our approach, credit network information
  - stored on untrusted server,
  - accessed obliviously,
  - using trusted hardware

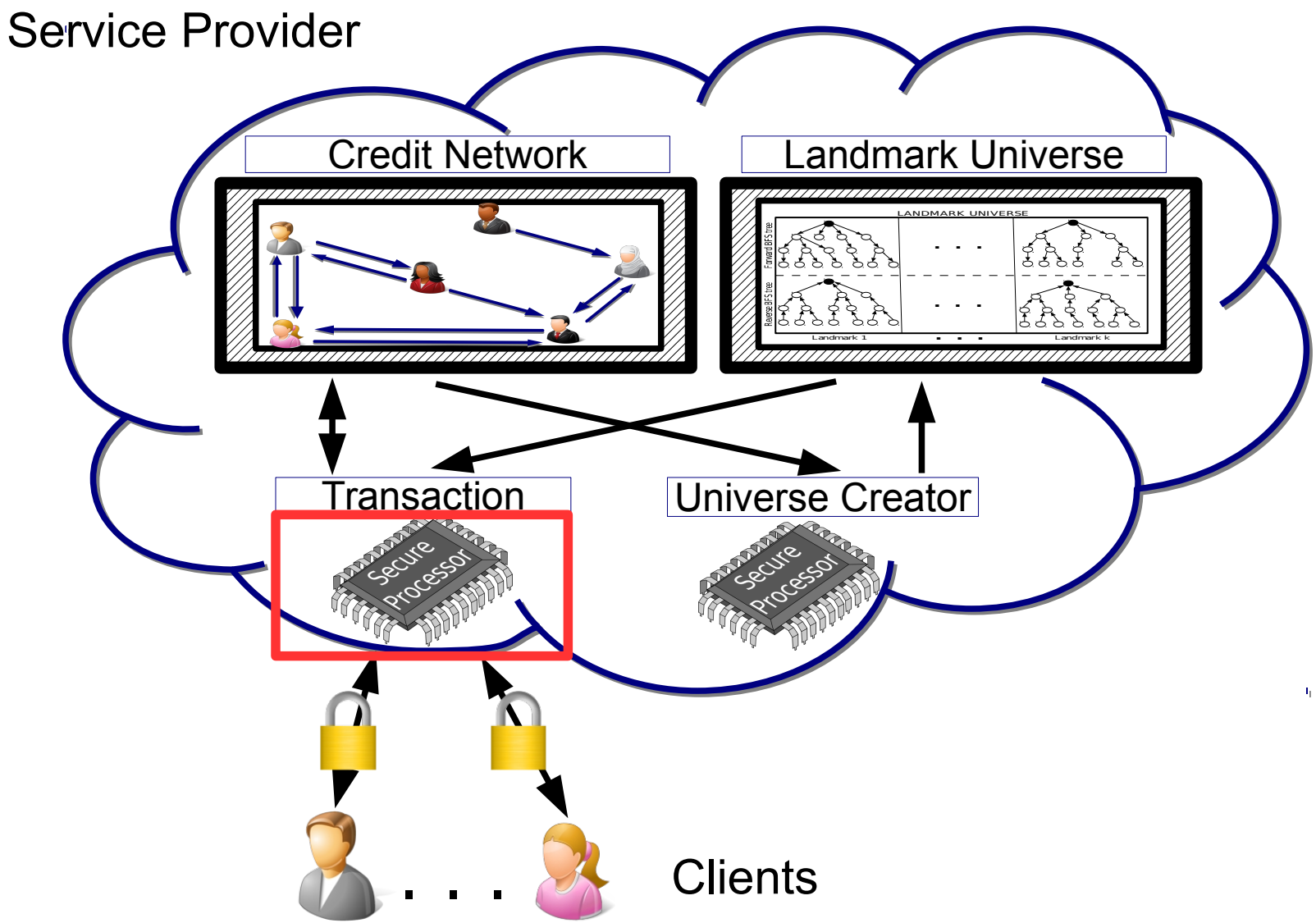
PrivPay: Overview



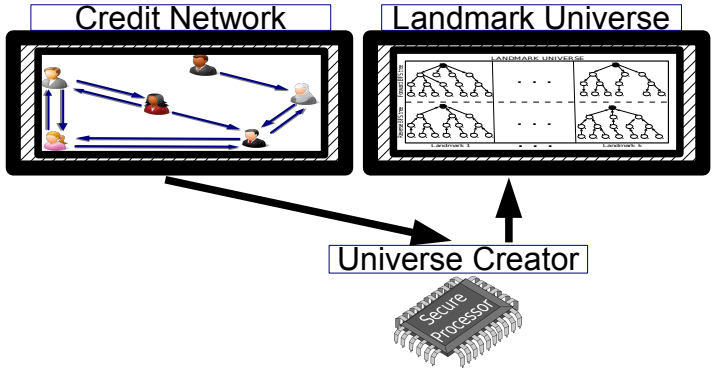
PrivPay: Overview



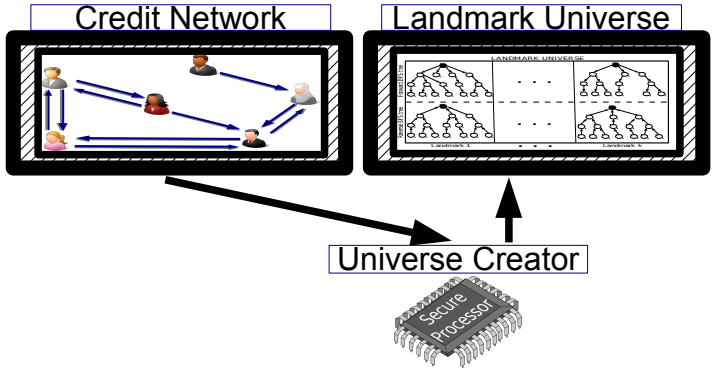
PrivPay: Overview

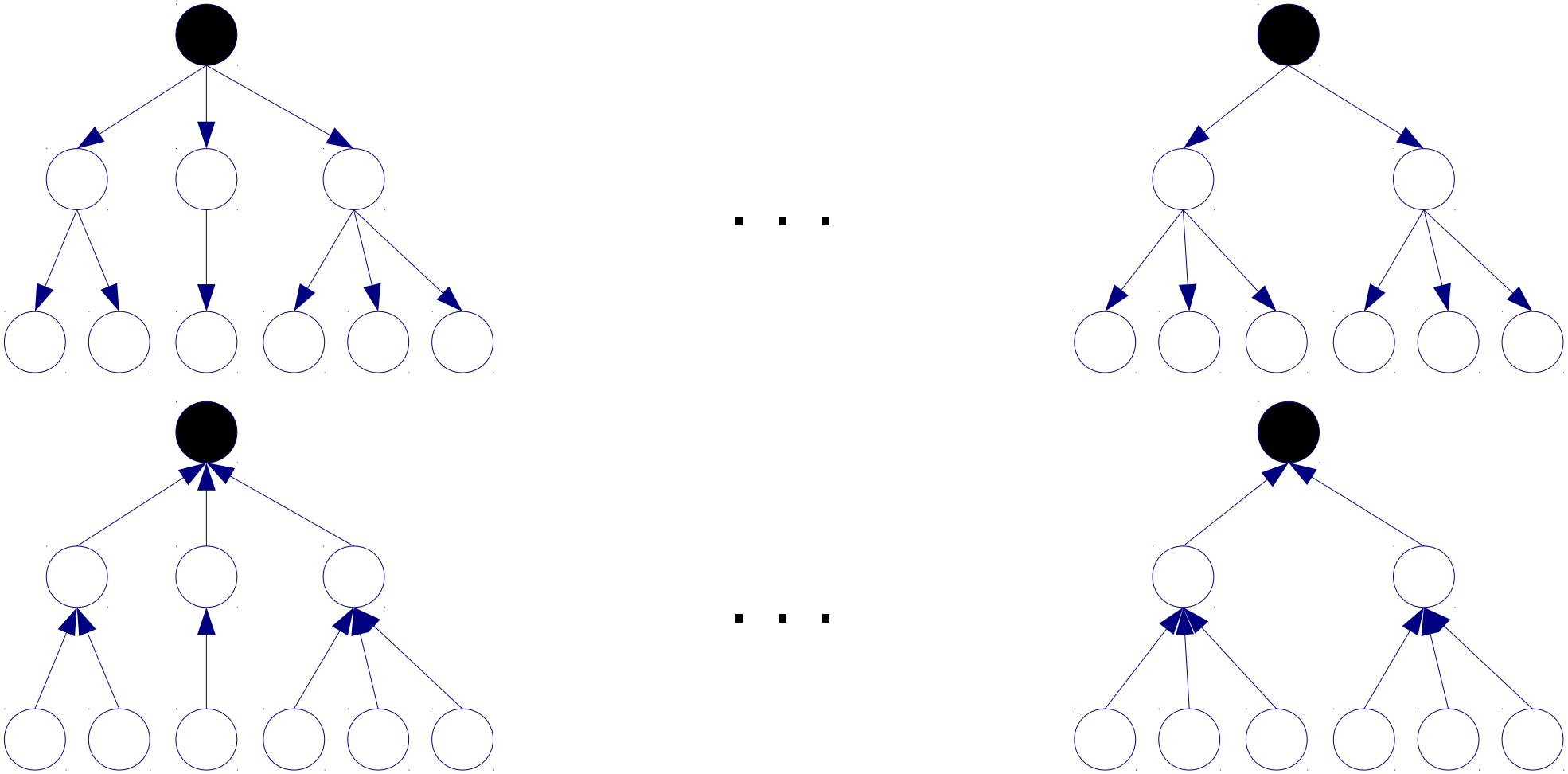


PrivPay: Universe Creator

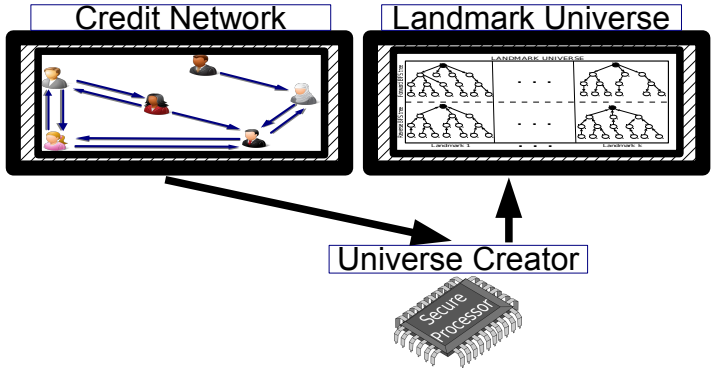


PrivPay: Universe Creator

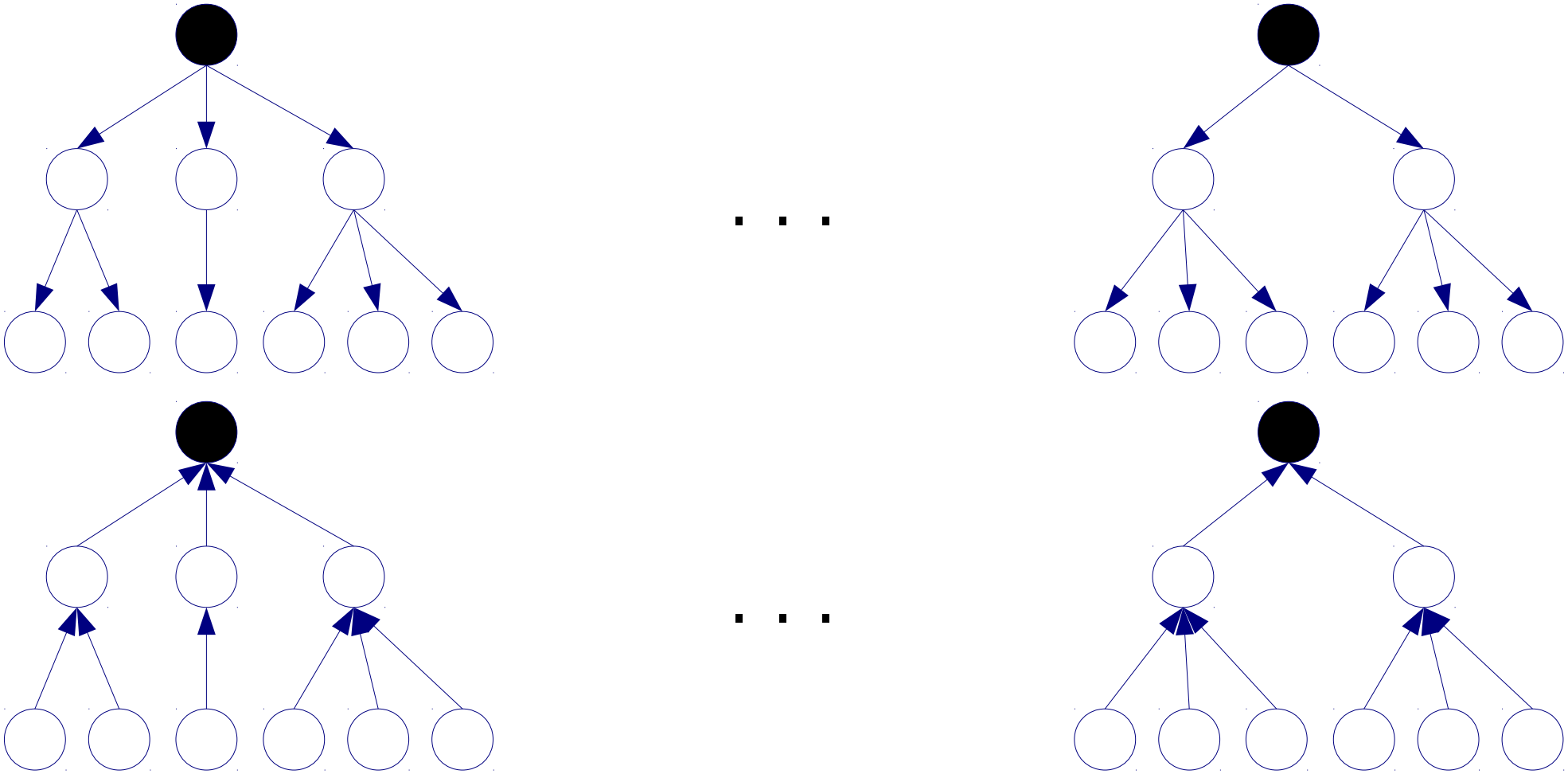




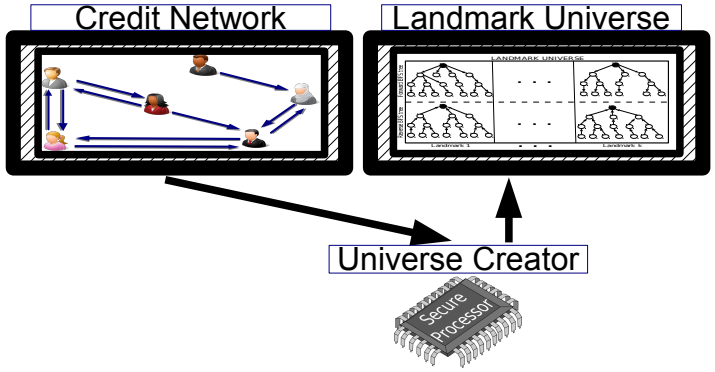
PrivPay: Universe Creator



ObliBFS: Standard BFS augmented with ORAM to ensure that "**no information is leaked**"



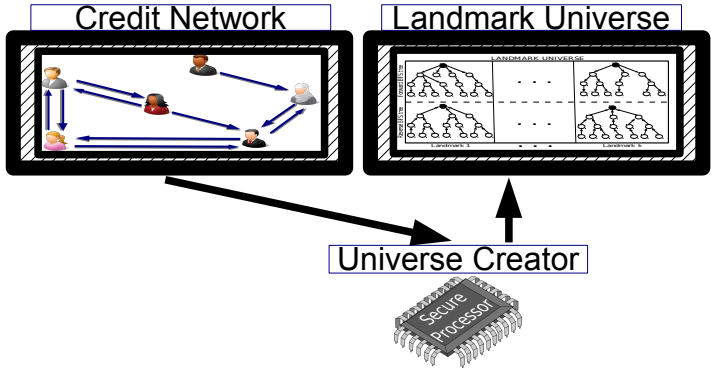
PrivPay: Universe Creator



ObliBFS: Standard BFS augmented with ORAM to ensure that "**no information is leaked**"

G, G': input graphs of the same size

PrivPay: Universe Creator

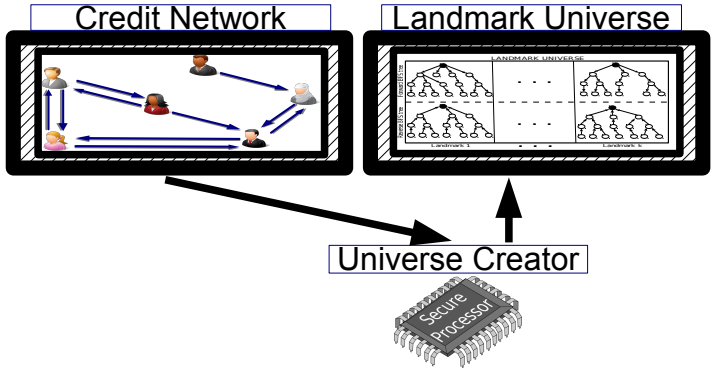


ObliBFS: Standard BFS augmented with ORAM to ensure that "**no information is leaked**"

G, G': input graphs of the same size

A(G): sequence of ObliBFS memory accesses

PrivPay: Universe Creator



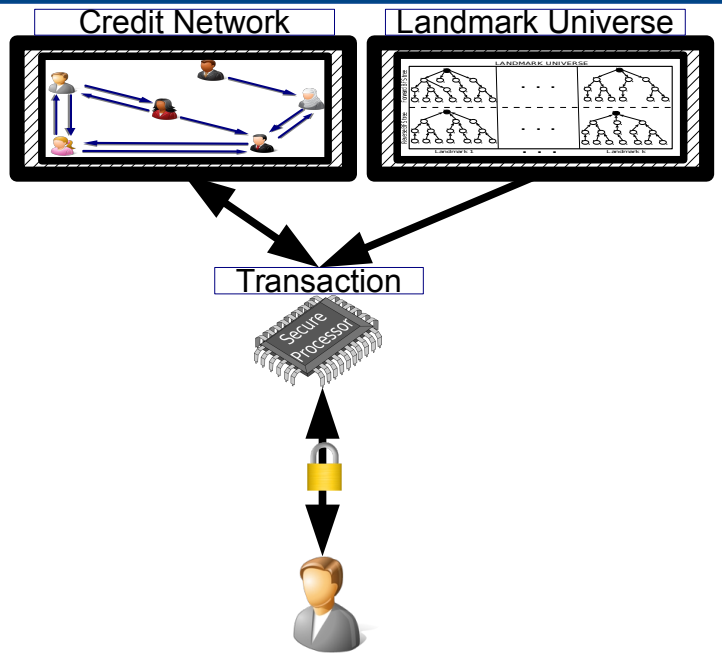
ObliBFS: Standard BFS augmented with ORAM to ensure that "**no information is leaked**"

G, G': input graphs of the same size

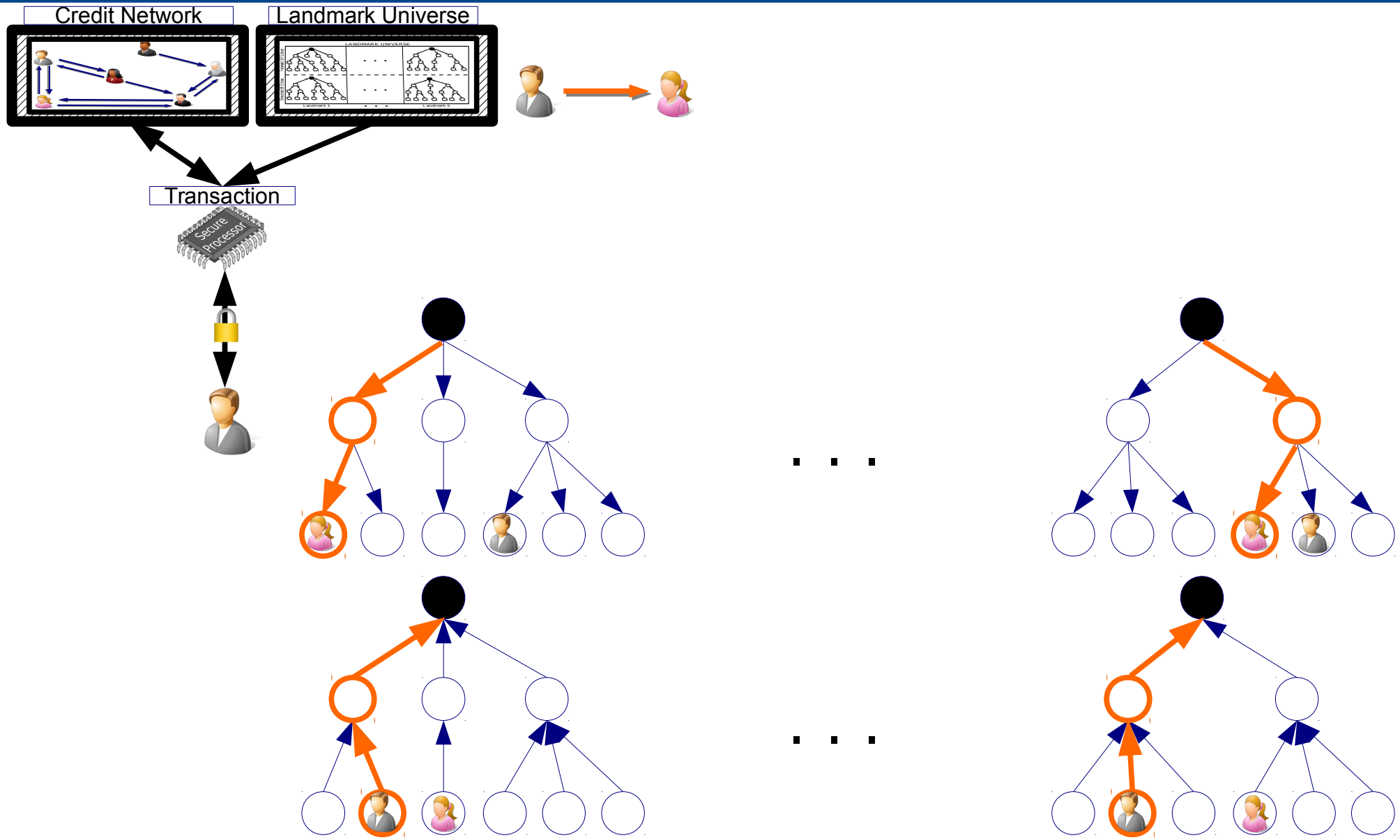
A(G): sequence of ObliBFS memory accesses

$$\mathbf{A}(G) \approx \mathbf{A}(G')$$

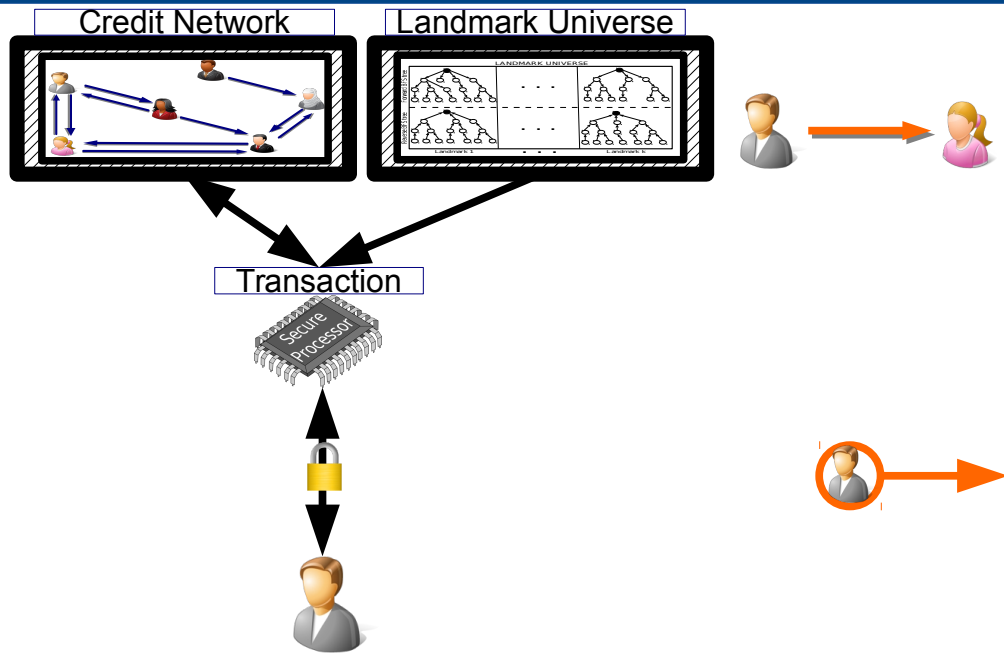
PrivPay: Transaction

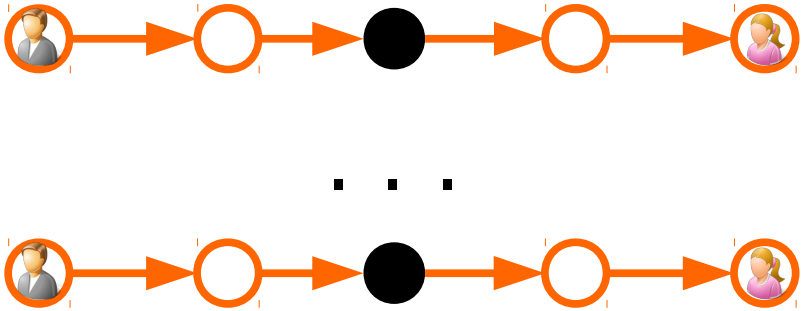


PrivPay: Transaction

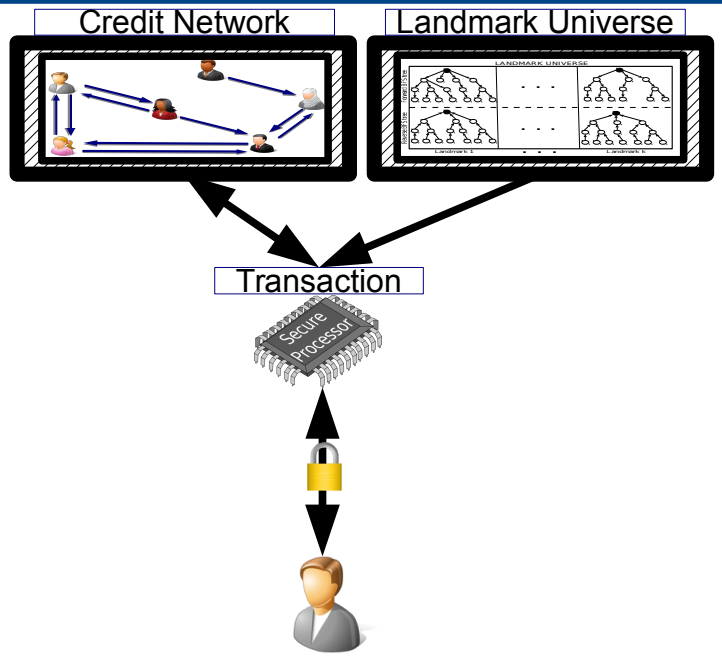


PrivPay: Transaction

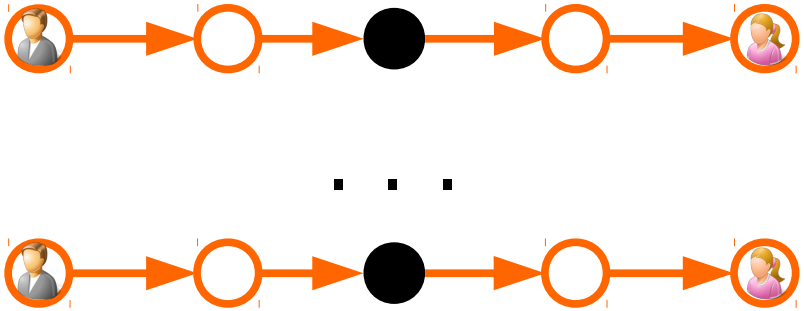




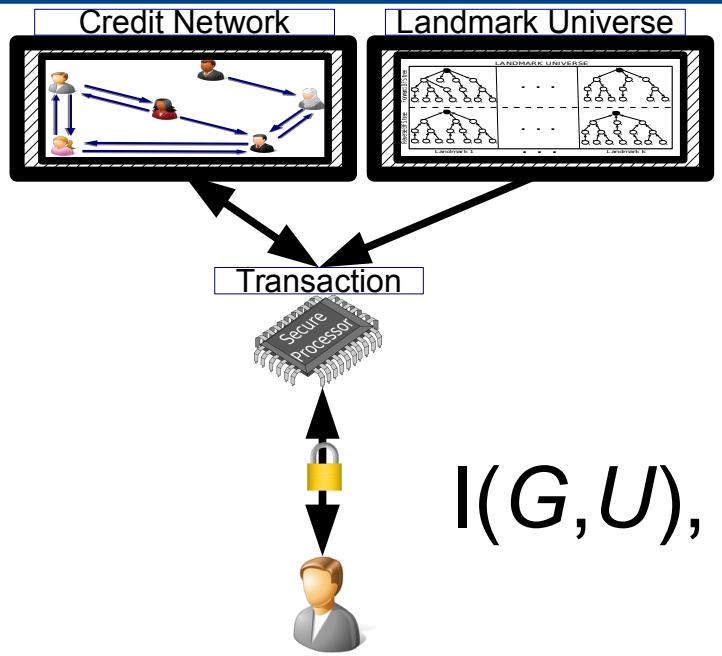
PrivPay: Transaction



Oblivious transactions: Transaction algorithm augmented with ORAM to ensure that "**no information about input is leaked**"



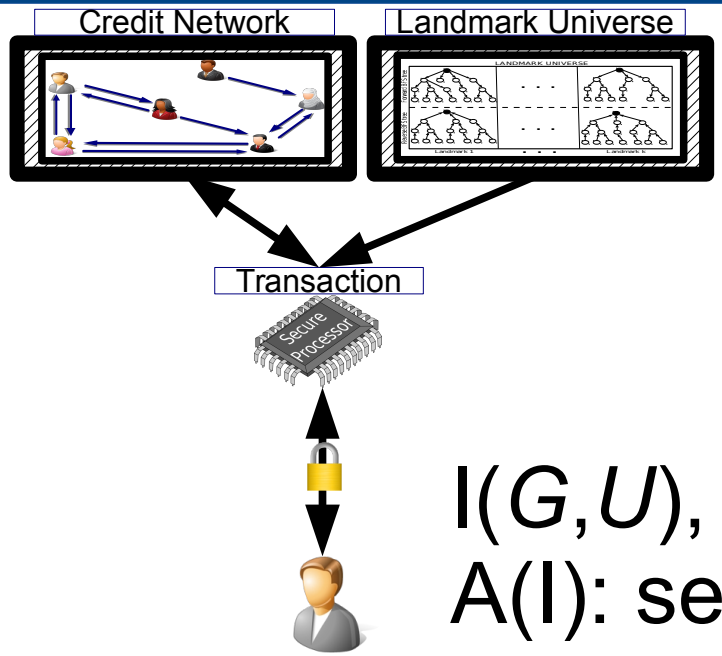
PrivPay: Transaction



Oblivious transactions: Transaction algorithm augmented with ORAM to ensure that "**no information about input is leaked**"

I(G,U), I'(G',U'): input information

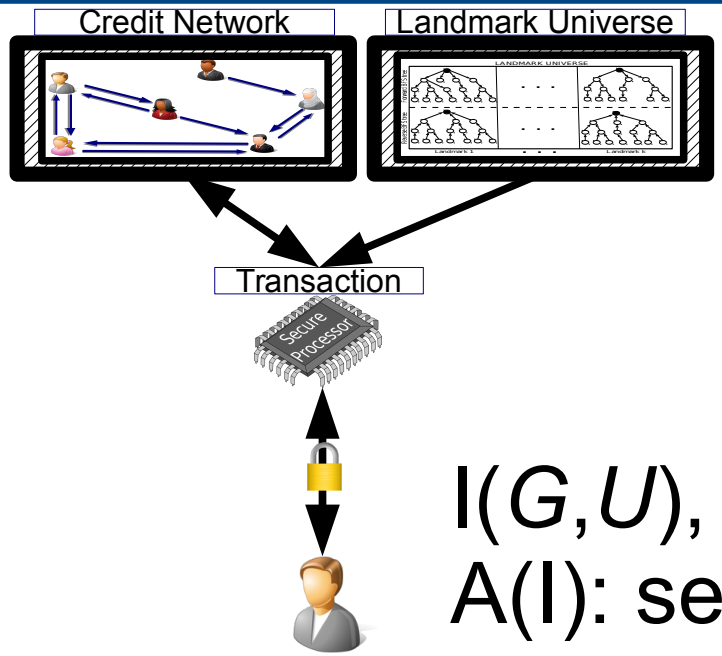
PrivPay: Transaction



Oblivious transactions: Transaction algorithm augmented with ORAM to ensure that "**no information about input is leaked**"

I(G,U), I'(G',U'): input information
A(I): sequence of oblivious transactions memory accesses

PrivPay: Transaction



Oblivious transactions: Transaction algorithm augmented with ORAM to ensure that "**no information about input is leaked**"

I(G,U), I'(G',U'): input information
A(I): sequence of oblivious transactions memory accesses

$$\mathbf{A(I) \approx A(I')}$$

PrivPay: Evaluation

- We have implemented PrivPay as a multithreaded C++ library
- We use Ripple transactions over a period of four months (Oct'13 – Jan'14)
  - network: 14,317 nodes and 14,176 links

	Non-Private setting [1]	PrivPay
Payment (ms)	0.078	1510
Change link (ms)	0.005	95
Oblivious BFS (ms) [Background process]	50	22000
Coverage	97%	95%

[1] B. Viswanath, M. Mondal, K. P. Gummadi, A. Mislove, and A. Post. Canal: Scaling Social Networks-based Sybil Tolerance Schemes. *Eurosys'12.*

PrivPay: Evaluation

- We have implemented PrivPay as a multithreaded C++ library
- We use Ripple transactions over a period of four months (Oct'13 – Jan'14)
  - network: 14,317 nodes and 14,176 links

	Non-Private setting [1]	PrivPay
Payment (ms)	0.078	1510
Change link (ms)	0.005	95
Oblivious BFS (ms) [Background process]	50	22000
Coverage	97%	95%

Deployable in practice (Ripple ~5 sec)

[1] B. Viswanath, M. Mondal, K. P. Gummadi, A. Mislove, and A. Post. Canal: Scaling Social Networks-based Sybil Tolerance Schemes. *Eurosys'12.*

PrivPay: Evaluation

- We have implemented PrivPay as a multithreaded C++ library
- We use Ripple transactions over a period of four months (Oct'13 – Jan'14)
  - network: 14,317 nodes and 14,176 links

	Non-Private setting [1]	PrivPay
Payment (ms)	0.078	1510
Change link (ms)	0.005	95
Oblivious BFS (ms) [Background process]	50	22000
Coverage	97%	95%

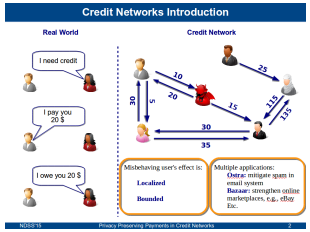
Deployable in practice (Ripple ~5 sec)

No false positives

[1] B. Viswanath, M. Mondal, K. P. Gummadi, A. Mislove, and A. Post. Canal: Scaling Social Networks-based Sybil Tolerance Schemes. *Eurosys'12.*

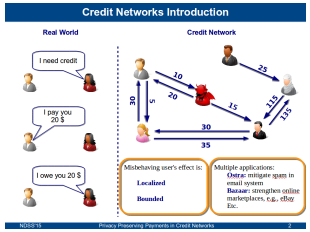
Take Home Message

- Credit networks have **interesting properties** and are used in **multiple application scenarios**

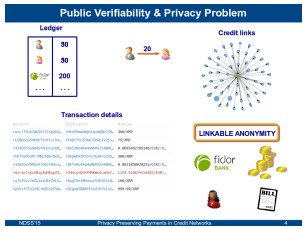


Take Home Message

- Credit networks have **interesting properties** and are used in **multiple application scenarios**

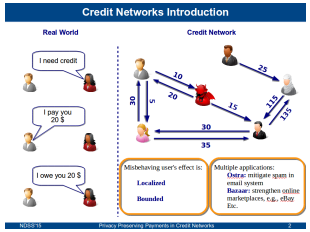


- **Privacy** is an **important** and **challenging** problem in credit networks

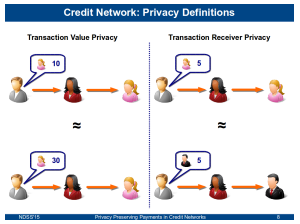


Take Home Message

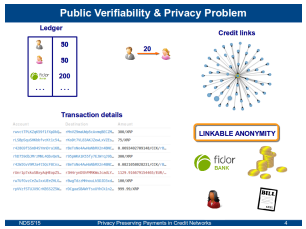
- Credit networks have **interesting properties** and are used in **multiple application scenarios**



- **Define privacy properties** for credit networks

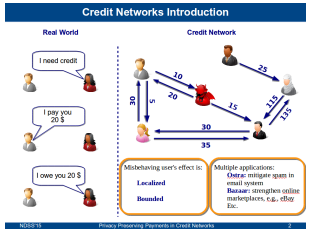


- **Privacy** is an **important** and **challenging** problem in credit networks

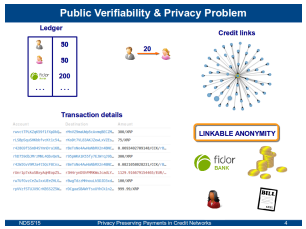


Take Home Message

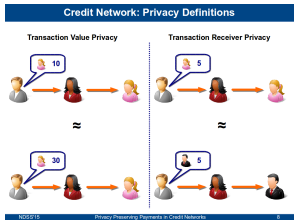
- Credit networks have **interesting properties** and are used in **multiple application scenarios**



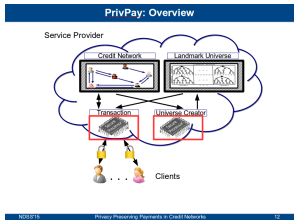
- **Privacy** is an **important** and **challenging** problem in credit networks



- **Define privacy properties** for credit networks

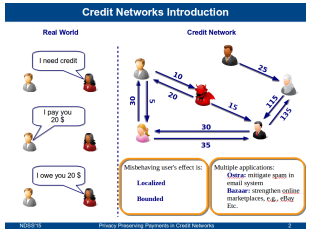


- **PrivPay: novel architecture** combining trusted hardware and oblivious algorithms

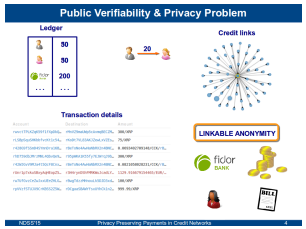


Take Home Message

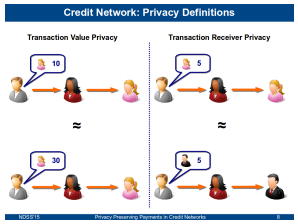
- Credit networks have **interesting properties** and are used in **multiple application scenarios**



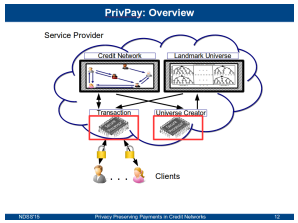
- **Privacy** is an **important** and **challenging** problem in credit networks



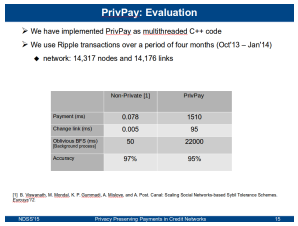
- **Define privacy properties** for credit networks



- **PrivPay: novel architecture** combining trusted hardware and oblivious algorithms



- PrivPay is **feasible to deploy** in practice



	Non-Private [1]	PrivPay
Payment (ms)	0.078	1510
Change link (ms)	0.005	95
Oblivious BFS (ms) (Background process)	50	22000
Accuracy	97%	95%