Evaluating User Privacy in Bitcoin

E. Androulaki, G. Karame, M. Röschlin, T. Scherer, and S. Čapkun
Institute of Information Security, ETH Zürich
NEC Laboratories, Europe

Financial Cryptography & Data Security, April 2nd 2013

Bitcoin

- Anonymous & decentralized (p2p-based) payment system
- With its own digital currency (BTC)
- Emerging:
  - Integrated across multiple businesses
  - Several exchange markets
  - BTC-ATMs in schedule to be deployed

Bitcoin

- Anonymous & decentralized (p2p-based) payment system
- With its own digital currency (BTC)
- Emerging:
  - Integrated across multiple businesses
  - Several exchange markets
  - BTC-ATMs in schedule to be deployed

Payment confirmation requires

→ **public announcement** of each transaction

Privacy in payment systems

Unlinkability of transactions

→ two transactions of an individual cannot be linked together

Anonymity of transactions

→ a transaction cannot be linked to a specific identity with a better probability than to other identities

Our contributions: Privacy in Bitcoin

Contribution 1:

- Definition of Bitcoin privacy

Contribution 2:

- Investigation of privacy provisions of Bitcoin when used as a primary currency within a university

Bitcoin payments

Users represented by addresses

→ pseudonyms derived from public keys

Payments through transactions

→ signed transfers of BTCs from a sender address to a recipient address

Bitcoin transactions

- In real life:

  I am **Alice** and I transfer **10$** that I acquired from **Jessie** to **Bob**.

Alice *Jessie*

Bitcoin transactions

- In real life:

  I am **Alice** and I transfer **10$** that I acquired from **Jessie** to **Bob**.

  Alice *Jessie*

- In Bitcoin:
  - Transactions authenticated using PK signatures

I am **A** and I transfer **1 BTC** that I acquired from transaction **X** to **B**.

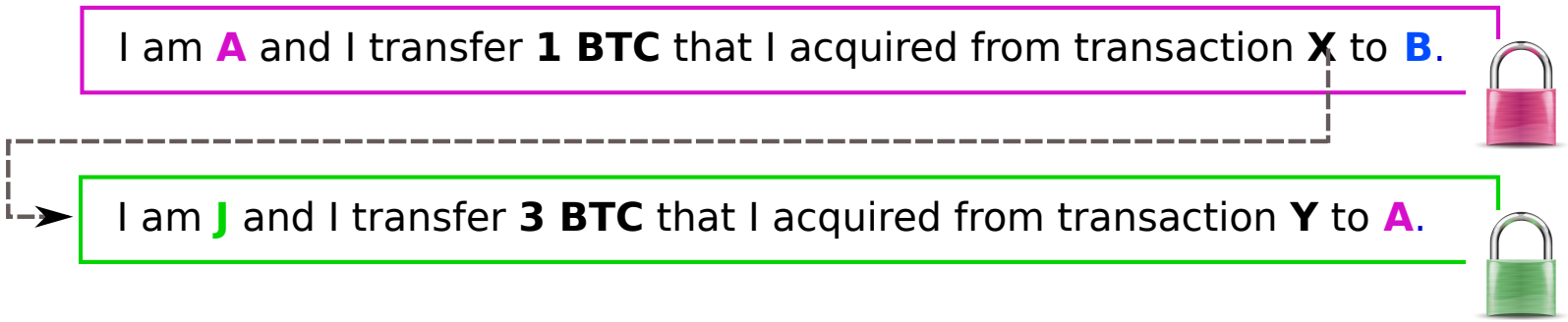
Bitcoin transactions

- In real life:

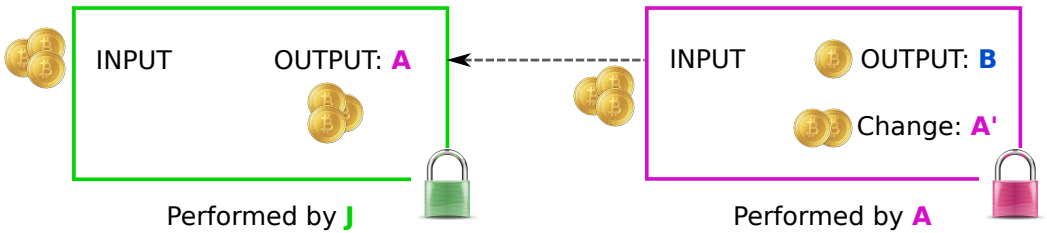
  I am **Alice** and I transfer **10$** that I acquired from **Jessie** to **Bob**.

  Alice *Jessie*

- In Bitcoin:
  - Transactions authenticated using PK signatures

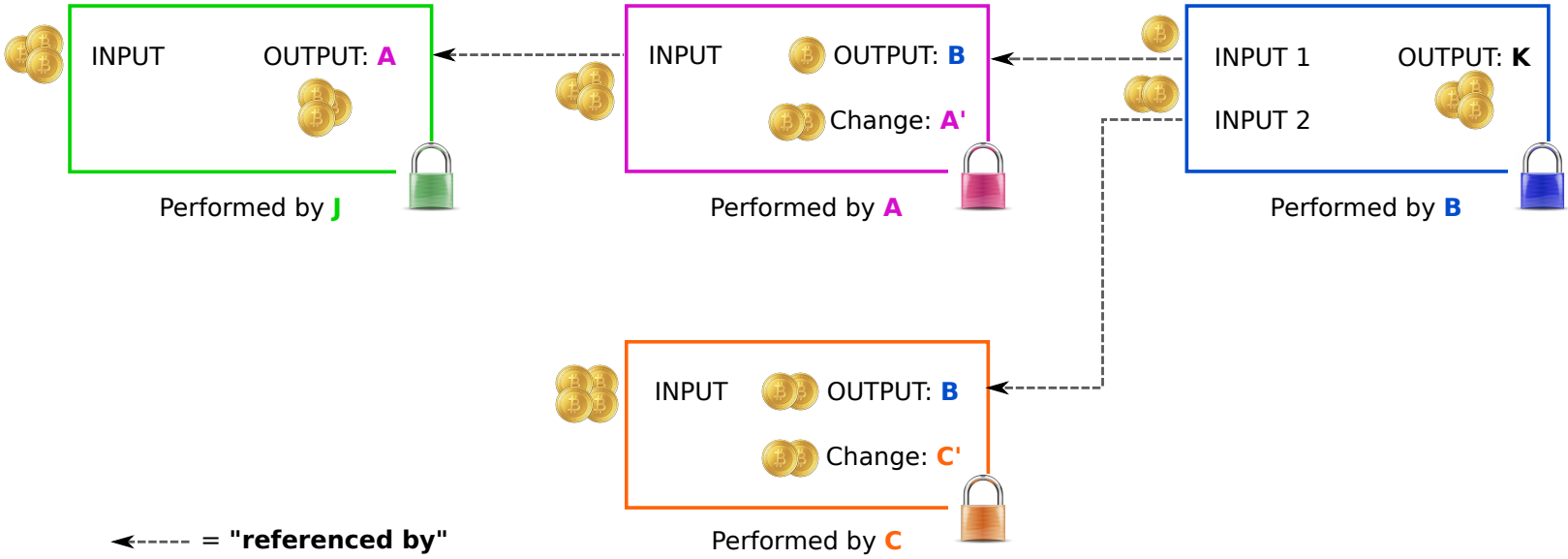


Bitcoin transactions

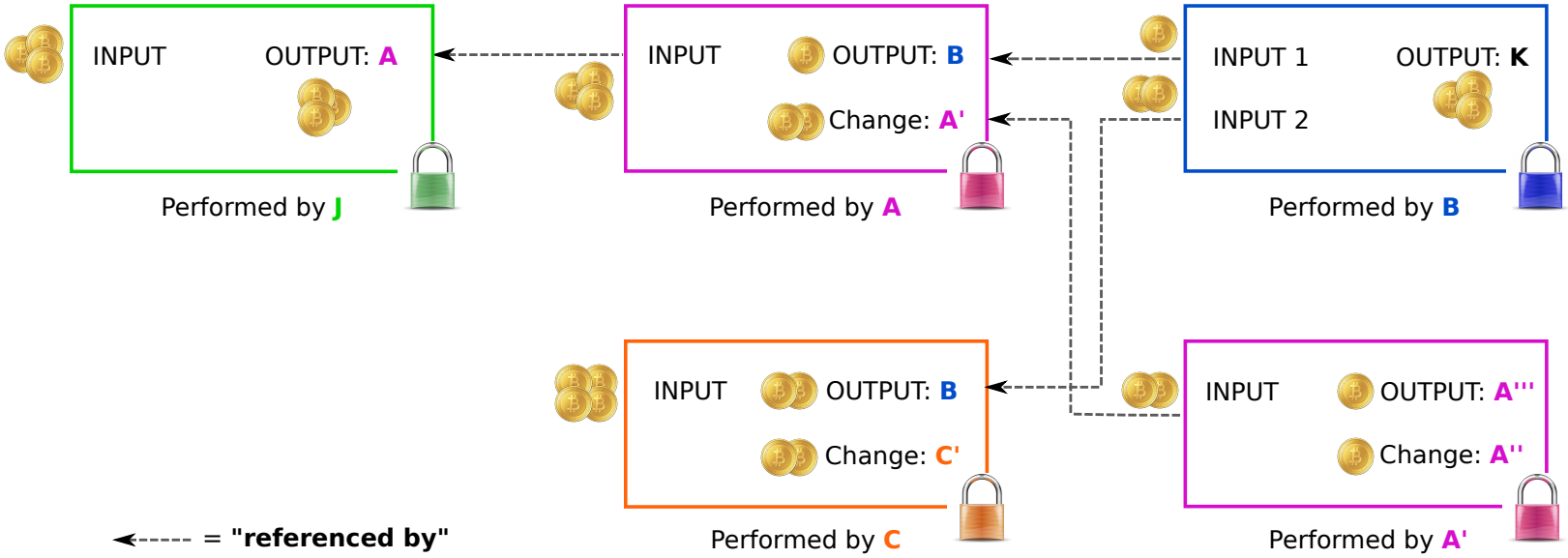


<----- = **"referenced by"**

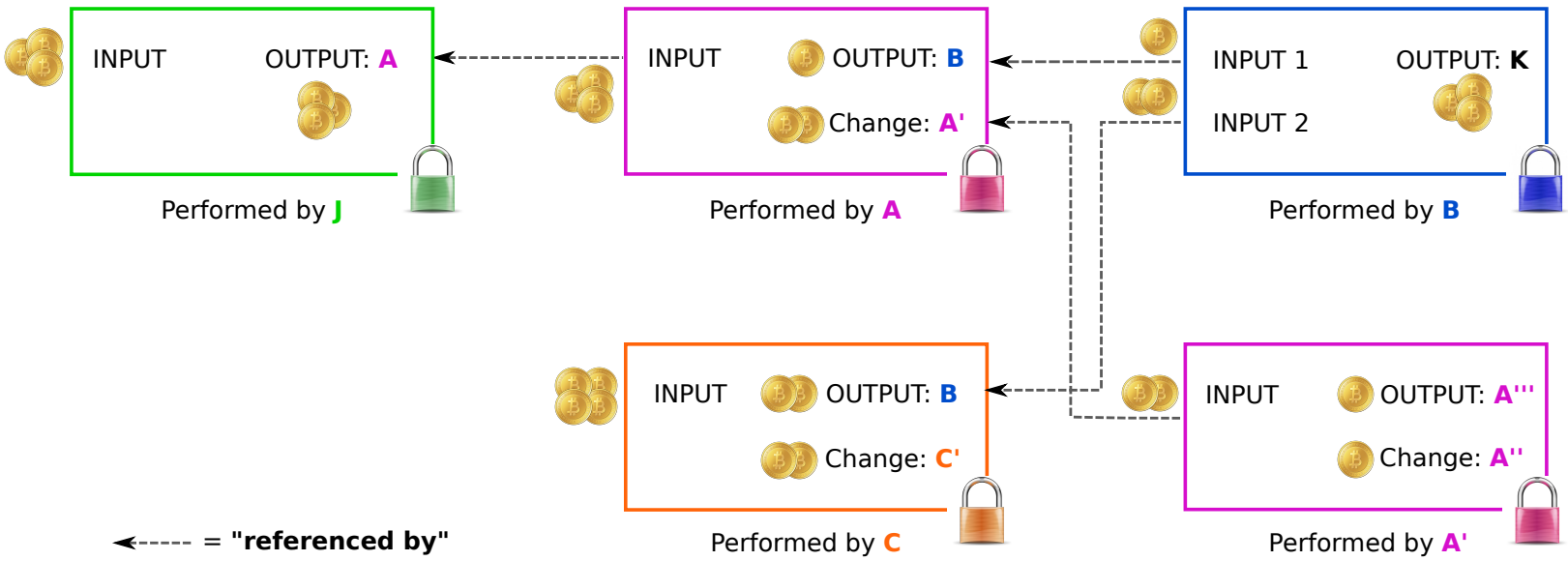
Bitcoin transactions



Bitcoin transactions



Bitcoin transactions



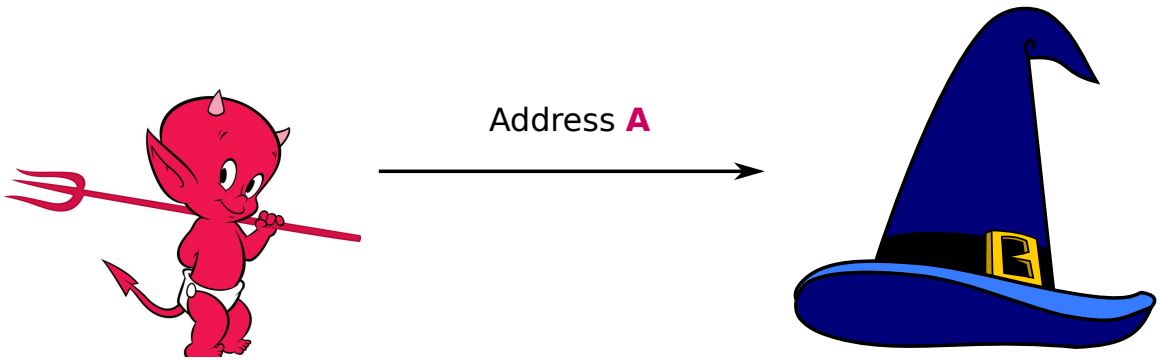
- Obfuscation mechanisms provided by Bitcoin **client**
  - Use of addresses/pseudonyms
  - Use of a **new** address for change!
- Recommendations to Bitcoin **users**
  - Transfer of BTCs to another address

Defining privacy in Bitcoin – (i) Address unlinkability

- Adversary $\mathcal{A}$(log, prior knowledge) $\leftrightarrow$ Challenger $\mathcal{C}$(log, truth)

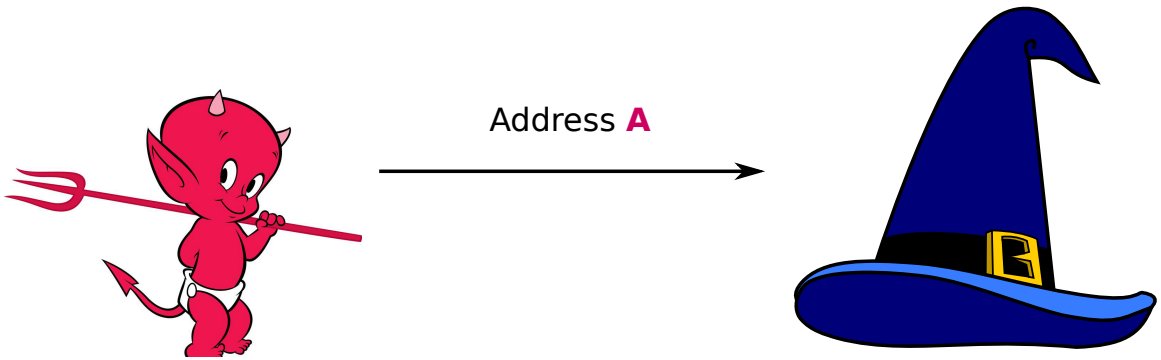
Defining privacy in Bitcoin – (i) Address unlinkability

- Adversary $\mathcal{A}$(log, prior knowledge) $\leftrightarrow$ Challenger $\mathcal{C}$(log, truth)



Defining privacy in Bitcoin – (i) Address unlinkability

- Adversary $\mathcal{A}$(log, prior knowledge) $\leftrightarrow$ Challenger $\mathcal{C}$(log, truth)

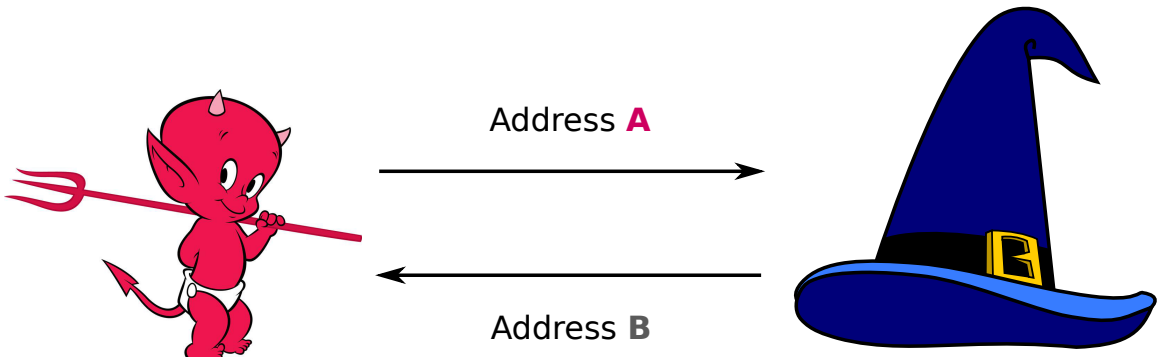


Bitcoin Addresses of the Owner of **A**

Bitcoin Addresses of other users

Defining privacy in Bitcoin – (i) Address unlinkability

- Adversary $\mathcal{A}$(log, prior knowledge) $\leftrightarrow$ Challenger $\mathcal{C}$(log, truth)

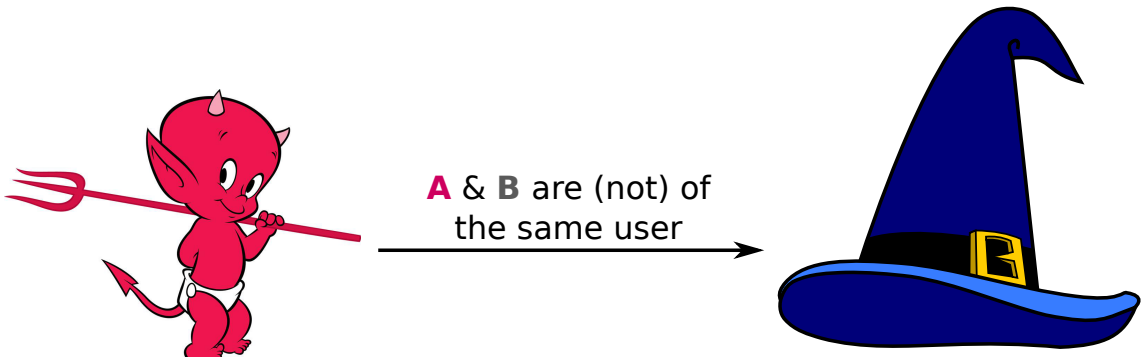


Bitcoin Addresses of the Owner of **A**

Bitcoin Addresses of other users

Defining privacy in Bitcoin – (i) Address unlinkability

- Adversary $\mathcal{A}$(log, prior knowledge) $\leftrightarrow$ Challenger $\mathcal{C}$(log, truth)
  $\rightarrow$ $\mathcal{A}$ wins if she answers **correctly**!



- **Ideally**, $\mathcal{A}$ should not outperform a **random adversary** $\mathcal{R}$ with **prior knowledge**.

Defining privacy in Bitcoin – (i) Address unlinkability

- **Ideally**, $\mathcal{A}$ should not outperform a **random adversary** $\mathcal{R}$ with **prior knowledge**.

Quantification → measuring address linkability

1. measure "success of $\mathcal{A}$"

	a_1	a_2					a_n
a_1	1	P_{21}					P_{1n}
a_2	P_{21}	1					P_{2n}
a_n	P_{n1}	P_{2n}					P_{nn}

$\mathbf{P}_{ij}$ = Probability that addresses a_i, a_j belong to the same user (adversarial estimate)

Defining privacy in Bitcoin – (i) Address unlinkability

- **Ideally**, $\mathcal{A}$ should not outperform a **random adversary** $\mathcal{R}$ with **prior knowledge**.

Quantification → measuring address linkability

1. measure "success of $\mathcal{A}$"

	a_1	a_2						a_n
a_1	1	P_{21}						P_{1n}
a_2	P_{21}	1						P_{2n}
a_n	P_{n1}	P_{2n}						P_{nn}

$\mathbf{P}_{ij}$ = Probability that addresses a_i, a_j belong to the same user (adversarial estimate)

	a_1	a_2						a_n
a_1	1	b_{21}						b_{1n}
a_2	b_{21}	1						b_{2n}
a_n	b_{n1}	b_{2n}						b_{nn}

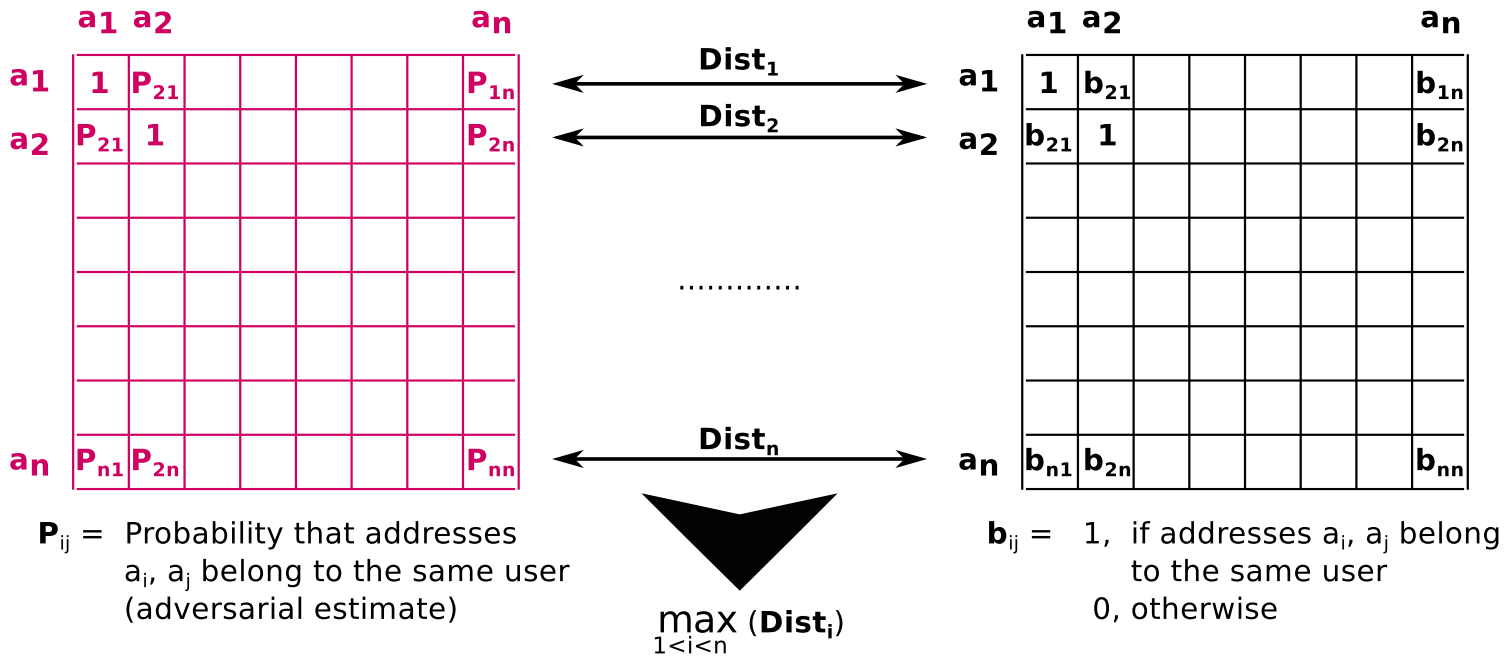
$\mathbf{b}_{ij}$ = 1, if addresses a_i, a_j belong to the same user
0, otherwise

Defining privacy in Bitcoin – (i) Address unlinkability

- **Ideally**, $\mathcal{A}$ should not outperform a **random adversary** $\mathcal{R}$ with **prior knowledge**.

Quantification → measuring address linkability

1. measure "success of $\mathcal{A}$"



$\mathbf{P}_{ij}$ = Probability that addresses a_i, a_j belong to the same user (adversarial estimate)

$\mathbf{b}_{ij}$ = 1, if addresses a_i, a_j belong to the same user
0, otherwise

Defining privacy in Bitcoin – (i) Address unlinkability

- **Ideally**, $\mathcal{A}$ should not outperform a **random adversary** $\mathcal{R}$ with **prior knowledge**.

Quantification $\rightarrow$ measuring address linkability

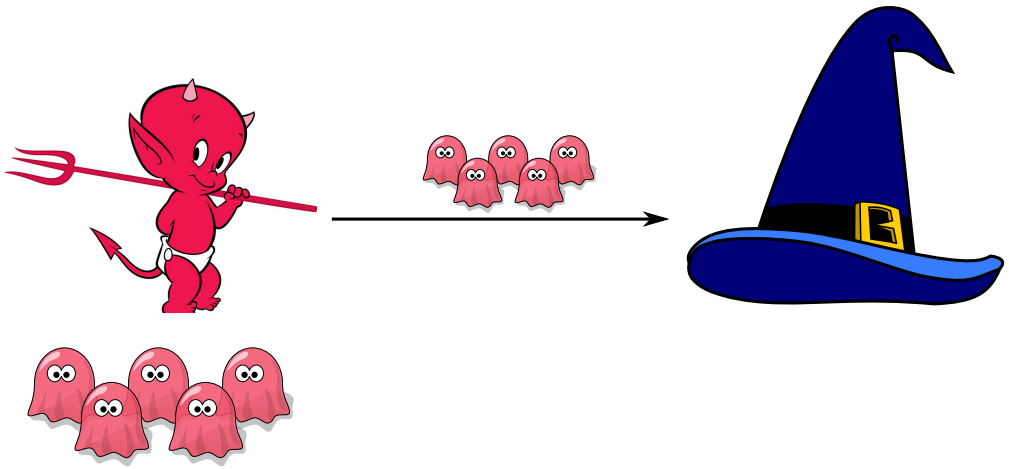
1. measure "success of $\mathcal{A}$"
2. measure "success of $\mathcal{R}$"
3. $=$ "success of $\mathcal{A}$" - "success of $\mathcal{R}$"

Defining privacy in Bitcoin – (ii) User indistinguishability

- User $\equiv$ set of transactions (addresses)
- Adversary $\mathcal{A}$(log, prior knowledge) $\leftrightarrow$ Challenger $\mathcal{C}$(log, truth)

Defining privacy in Bitcoin – (ii) User indistinguishability

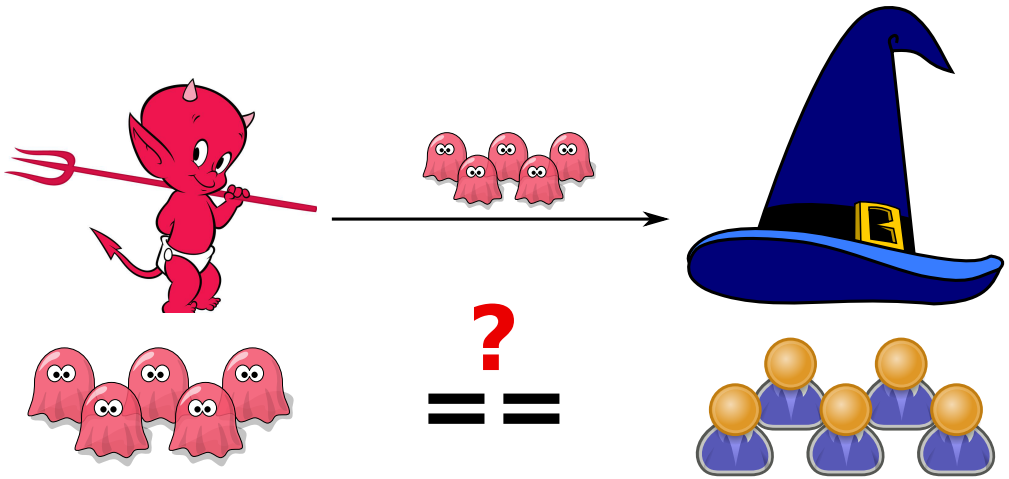
- User $\equiv$ set of transactions (addresses)
- Adversary $\mathcal{A}$(log, prior knowledge) $\leftrightarrow$ Challenger $\mathcal{C}$(log, truth)




= Set of addresses / transactions that represent one user
(adversarial estimate)

Defining privacy in Bitcoin – (ii) User indistinguishability

- User $\equiv$ set of transactions (addresses)
- Adversary $\mathcal{A}$(log, prior knowledge) $\leftrightarrow$ Challenger $\mathcal{C}$(log, truth)

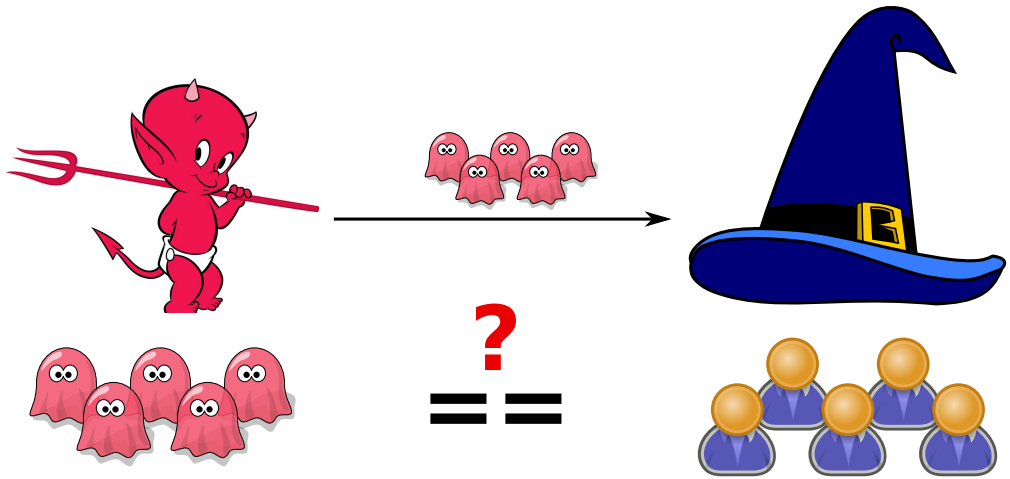


= Set of addresses / transactions that represent one user (adversarial estimate)

= Set of addresses / transactions that represent one user (truth)

Defining privacy in Bitcoin – (ii) User indistinguishability

- User $\equiv$ set of transactions (addresses)
- Adversary $\mathcal{A}$(log, prior knowledge) $\leftrightarrow$ Challenger $\mathcal{C}$(log, truth)
  $\rightarrow$ $\mathcal{A}$ wins if she answers **correctly**!



= Set of addresses / transactions that represent one user (adversarial estimate)

= Set of addresses / transactions that represent one user (truth)

Defining privacy in Bitcoin – (ii) User indistinguishability

- **Ideally**, $\mathcal{A}$ should not outperform $\mathcal{R}$.

Quantification $\rightarrow$ measuring user distinguishability

Defining privacy in Bitcoin – (ii) User indistinguishability

- **Ideally**, $\mathcal{A}$ should not outperform $\mathcal{R}$.

Quantification $\rightarrow$ measuring user distinguishability

- w.r.t transactions and addresses

Defining privacy in Bitcoin – (ii) User indistinguishability

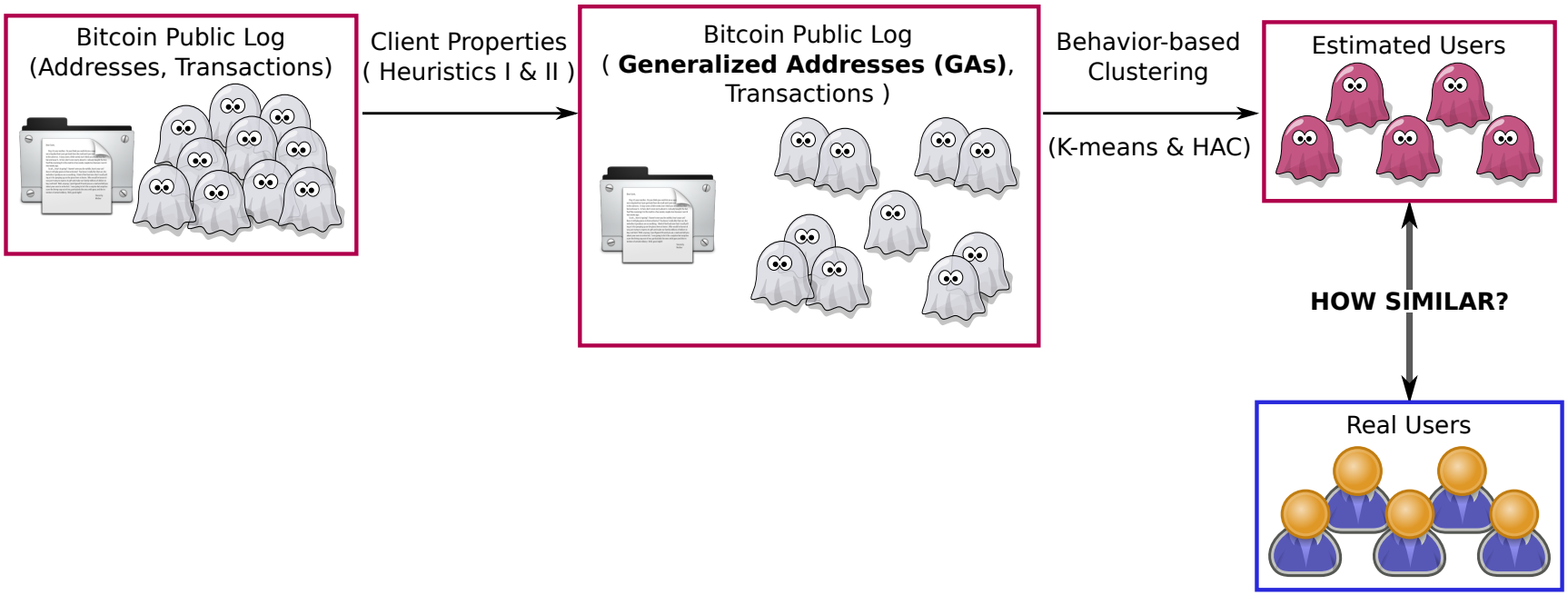
- **Ideally**, $\mathcal{A}$ should not outperform $\mathcal{R}$.

Quantification $\rightarrow$ measuring user distinguishability

- w.r.t transactions and addresses
- measure "success of $\mathcal{A}$"
  - e.g., via the **N**ormalized **M**utual **I**nformation (**NMI**)
- measure "advantage of success of $\mathcal{A}$ over the success of $\mathcal{R}$"
  - e.g., via the **A**djusted **M**utual **I**nformation (**AMI**)

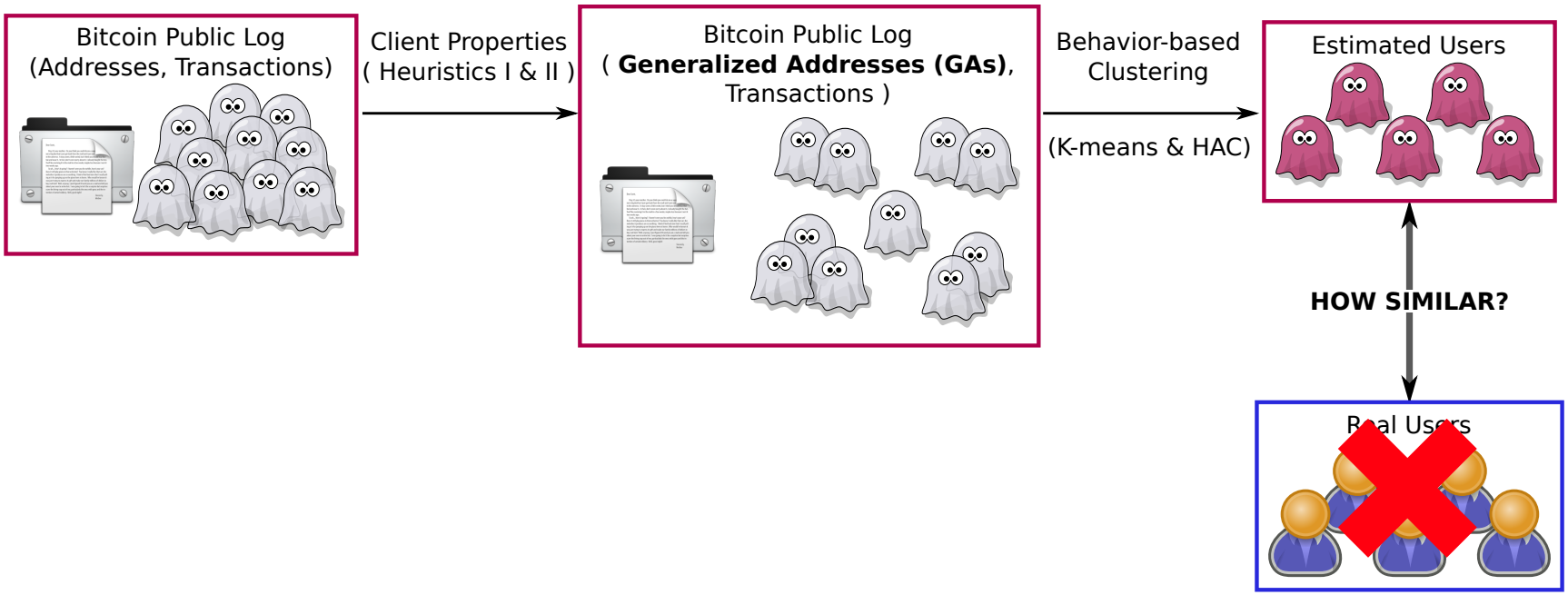
Evaluating Bitcoin privacy

- Not possible with the current Bitcoin log



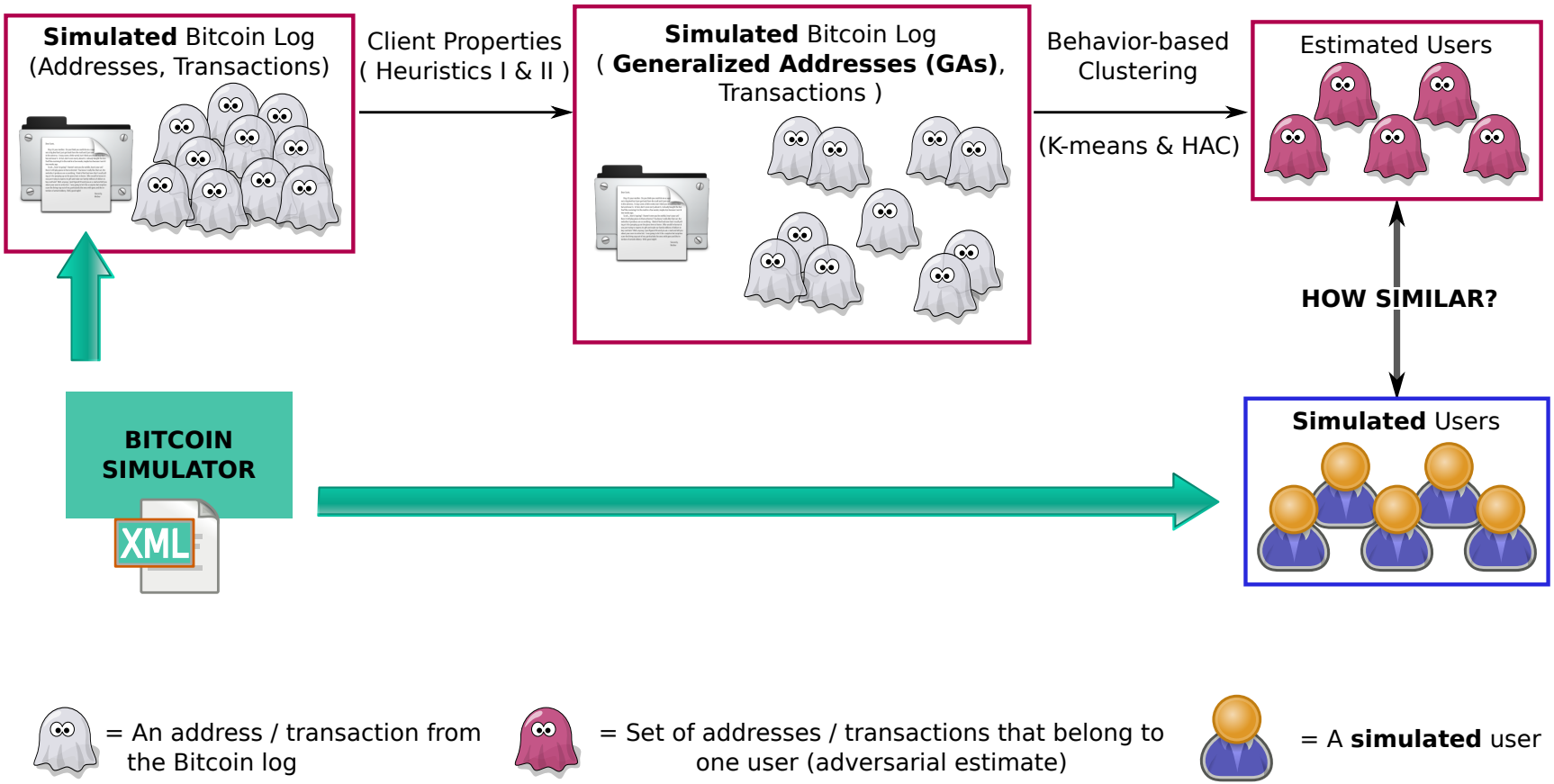
Evaluating Bitcoin privacy

- Not possible with the current Bitcoin log
  1. measuring adversarial success → **knowledge of real users**
  2. Bitcoin is not currently used for **daily payments**



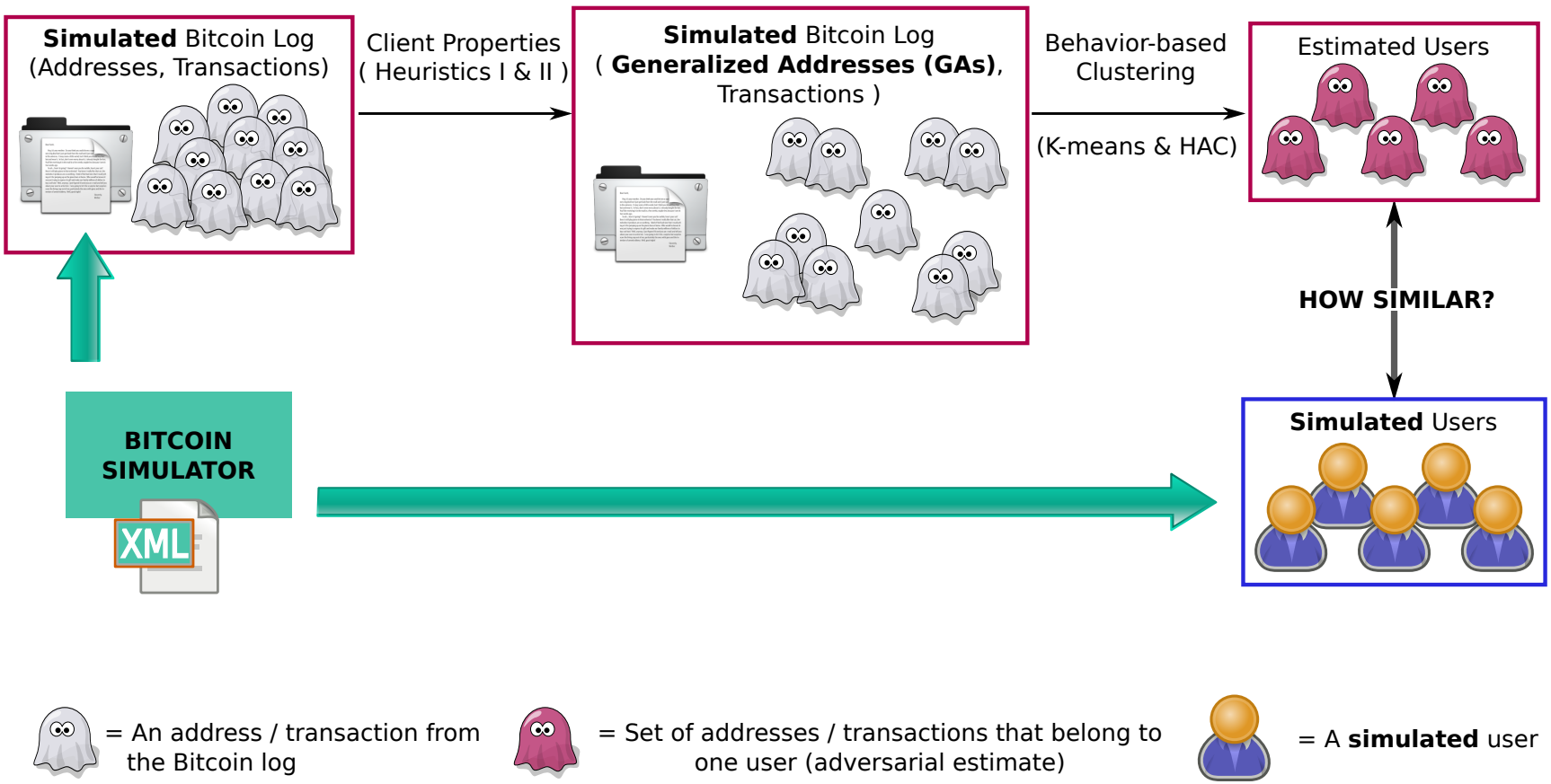
Evaluating Bitcoin privacy

- Not possible with the current Bitcoin log
  1. measuring adversarial success → **knowledge of real users**
  2. Bitcoin is not currently used for **daily payments**



Evaluating Bitcoin privacy

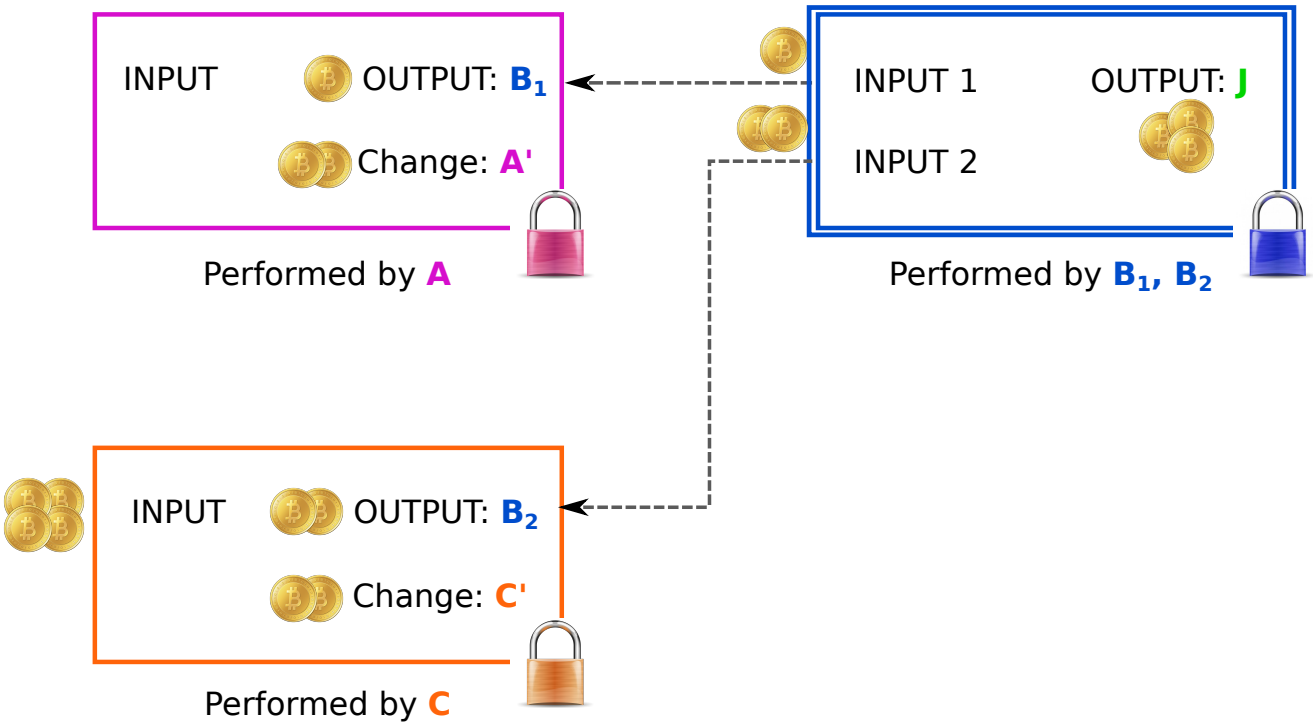
- At first glance, **addresses** can be linked together by
  1. Leveraging Bitcoin client properties
  2. Leveraging behavior-based clustering



Exploiting Bitcoin-client Properties

Heuristic I

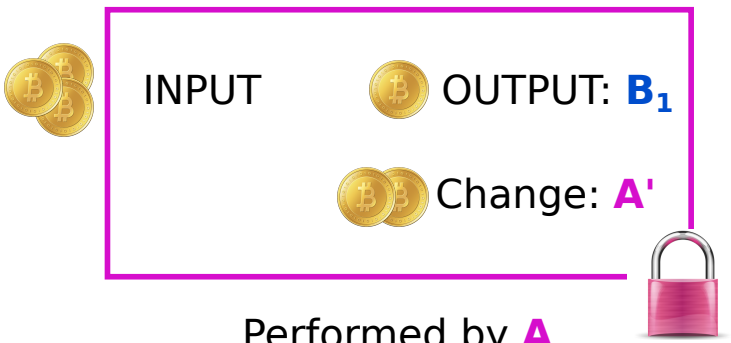
- *Addresses contributing to a multiple input transaction belong to the same user*
  E.g., Addresses $\mathbf{B_1}$ and $\mathbf{B_2}$ belong to the same user



Exploiting Bitcoin-client Properties

Heuristic II

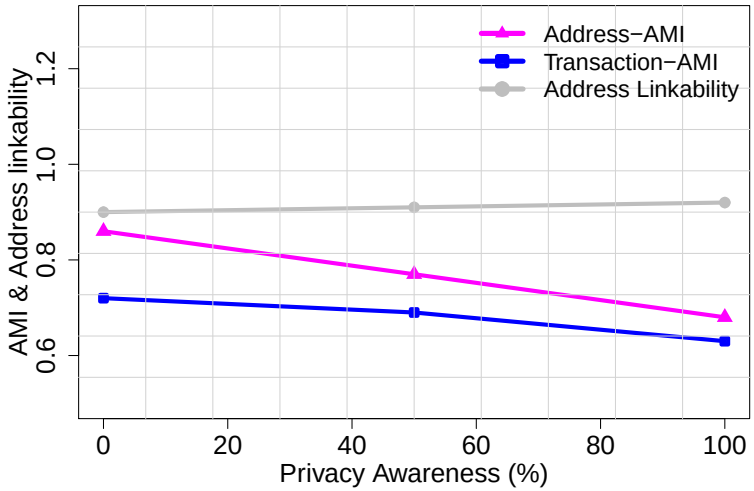
- *If a transaction has two outputs* **exactly one of which** *is to a new address, the new address and the sender address belong to the same user.*
  E.g., if **B_1** has appeared before, **A** and **A'** are of the same user



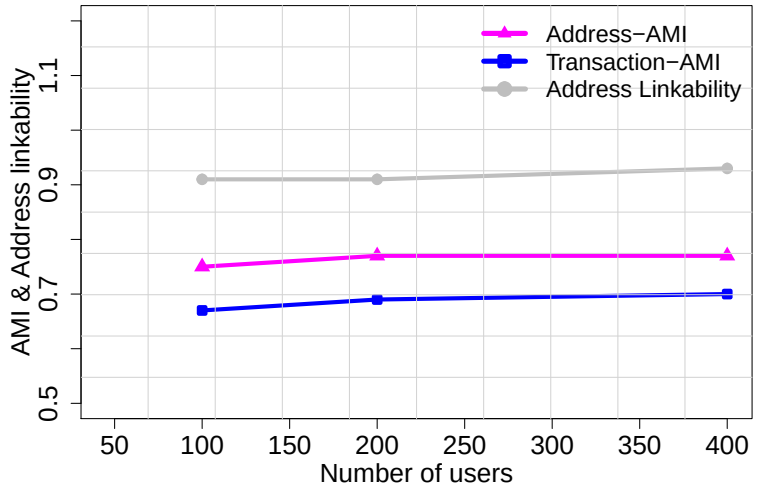
Our simulation environment

- Emulates the use of Bitcoin in a university setting
- **Randomly** generated **purchase habits** per user (profiles)
- Accounts for **privacy-aware** users

Our results: Address linkability & User distinguishability



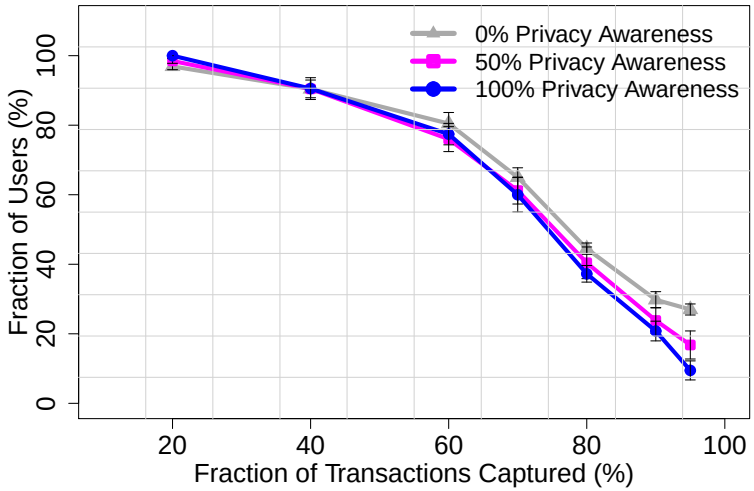
(for 200 users)



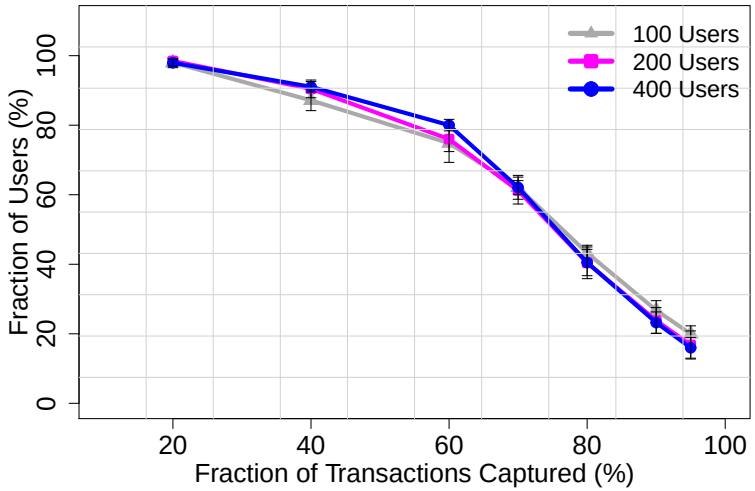
(for 50% privacy awareness)

- Address linkability $\approx$ $\frac{\text{“Success of } \mathcal{A}\text{”} - \text{“Success of } \mathcal{R}\text{”}}{\text{“Success of } \mathcal{A}\text{”}}$
- User distinguishability $\approx$ AMI:
  - i) 1: correct clustering,
  - ii) 0: random clustering,
  - iii) -1 worse than random

Our results: User profile capturing



(for 200 users)



(for 50% privacy awareness)

Over **40% of the users** have their profiles **compromised** by at least **80%**!

Suggestions for enhancing Bitcoin privacy

Getting around Heuristic I & Heuristic II

- Transfer of BTCs to single-use addresses before or after the payment
- Results in scalability and performance issues

Mixers!

- Centralized entity that handles multiple accounts
- **Against Bitcoin de-centralized nature**

Conclusions

1. Bitcoin privacy definitions
2. Investigated Bitcoin privacy provisions in a simulated setting, where Bitcoin is used for **daily payments**
3. Current version of Bitcoin **would** enable the recovery of user transaction profiles to a large extend!

Thank you for your attention!