Privacy in Blockchain

Murat Osmanoglu

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk'

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- its roots traced back to the study of David Chaum on anonymous digital cash

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- its roots traced back to the study of David Chaum on anonymous digital cash

  'Blind Signatures for Untraceable Payments', 1982

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

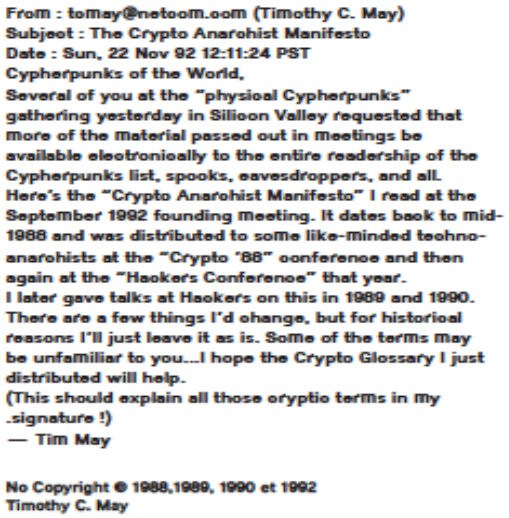
- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- in late 1992, three people: Eric Hughes (mathematicians from Berkeley), Tim May (businissman retired from Intel), and John Gilmore (computer scientist) were gathering to discuss some cryptographic and programing issues

Cypherpunk Manifesto

- they later initiated a mailing list (the number of subscribers reached 2000 in 1997) to reach out some other cypherpunks outside of Bay Area.

- Timothy May published 'the Crypto Anarchist Manifesto' in 1992



From : tcmay@netcom.com (Timothy C. May)
Subject : The Crypto Anarchist Manifesto
Date : Sun, 22 Nov 92 12:11:24 PST
Cypherpunks of the World,
Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990. There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you....I hope the Crypto Glossary I just distributed will help.
(This should explain all those cryptic terms in my .signature !)
— Tim May

No Copyright © 1988,1989, 1990 et 1992
Timothy C. May

THE CRYPTO-ANARCHIST MANIFESTO

Thimothy C.May

MANIFESTE CRYPTO-ANARCHISTE

Cypherpunk Manifesto

- They later initiated a mailing list (the number of subscribers reached 2000 in 1997) to reach out some other cypherpunks outside of Bay Area.

- Timothy May published 'the Crypto Anarchist Manifesto' in 1992

> "Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other."

Cypherpunk Manifesto

- Eric Hughes published *'A Cypherpunk's Manifesto'* in 1993, which can be considered as holy text of this movement.

> "When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. Therefore, privacy in an open society requires anonymous transaction systems."

Cypherpunk Manifesto

- Adam Back, inventor of Hashcash
- Nick Szabo, inventor of smart contracts, designer of bit gold
- Wei Dai, inventor of B-Money
- Hal Finney, the receiver of the first transaction made in Bitcoin
- Satoshi Nakamoto, inventor of Bitcoin
- Julian Assange, founder of wikileaks, author of 'Cypherpunks : Freedom and the Future of the Internet'

Privacy Issues

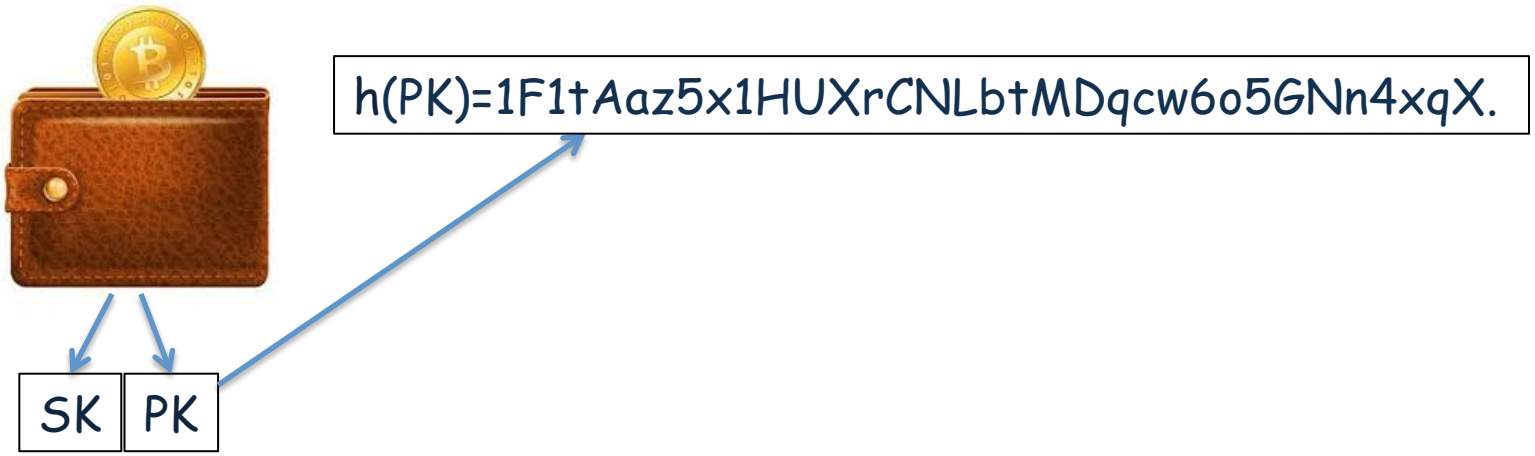
- each user can get all the transactions shared in the network
- it enables each user to validate integrity and authenticity of every transaction
- it also exposes all the transaction associated with an ID to everyone

Privacy Issues

- each user can get all the transactions shared in the network
- it enables each user to validate integrity and authenticity of every transaction
- it also exposes all the transaction associated with an ID to everyone
- Bitcoin uses pseudonymous addresses for users to provide privacy up to a certain degree

Privacy Issues

- each user can get all the transactions shared in the network
- it enables each user to validate integrity and authenticity of every transaction
- it also exposes all the transaction associated with an ID to everyone
- Bitcoin uses pseudonymous addresses for users to provide privacy up to a certain degree



Privacy Issues

- each user can get all the transactions shared in the network
- it enables each user to validate integrity and authenticity of every transaction
- it also exposes all the transaction associated with an ID to everyone
- Bitcoin uses pseudonymous addresses for users to provide privacy up to a certain degree

SK PK

h(PK)=1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX.

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX
sends 3 bitcoin received through tx to
13eBhR3oHFD5wkE4oGtrLdbdi2PvK3ijMC

Privacy Issues

- each user can get all the transactions shared in the network
- it enables each user to validate integrity and authenticity of every transaction
- it also exposes all the transaction associated with an ID to everyone
- Bitcoin uses pseudonymous addresses for users to provide privacy up to a certain degree

h(PK)=1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX.

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX
sends 3 bitcoin received through tx to
13eBhR3oHFD5wkE4oGtrLdbdi2PvK3ijMC

- Bitcoin even allows users to have more than one address and to use a new one for each transaction to improve privacy

Privacy Issues

- it is still possible to link pseudonyms to real identities by utilizing the blockchain data together with the external information obtained from different Internet sources such as twitter posts, forums etc.

Privacy Issues

- it is still possible to link pseudonyms to real identities by utilizing the blockchain data together with the external information obtained from different Internet sources such as twitter posts, forums etc.
- since bitcoin enables users to create more than one address, the first goal here is to cluster all addresses belonging to the same user

Privacy Issues

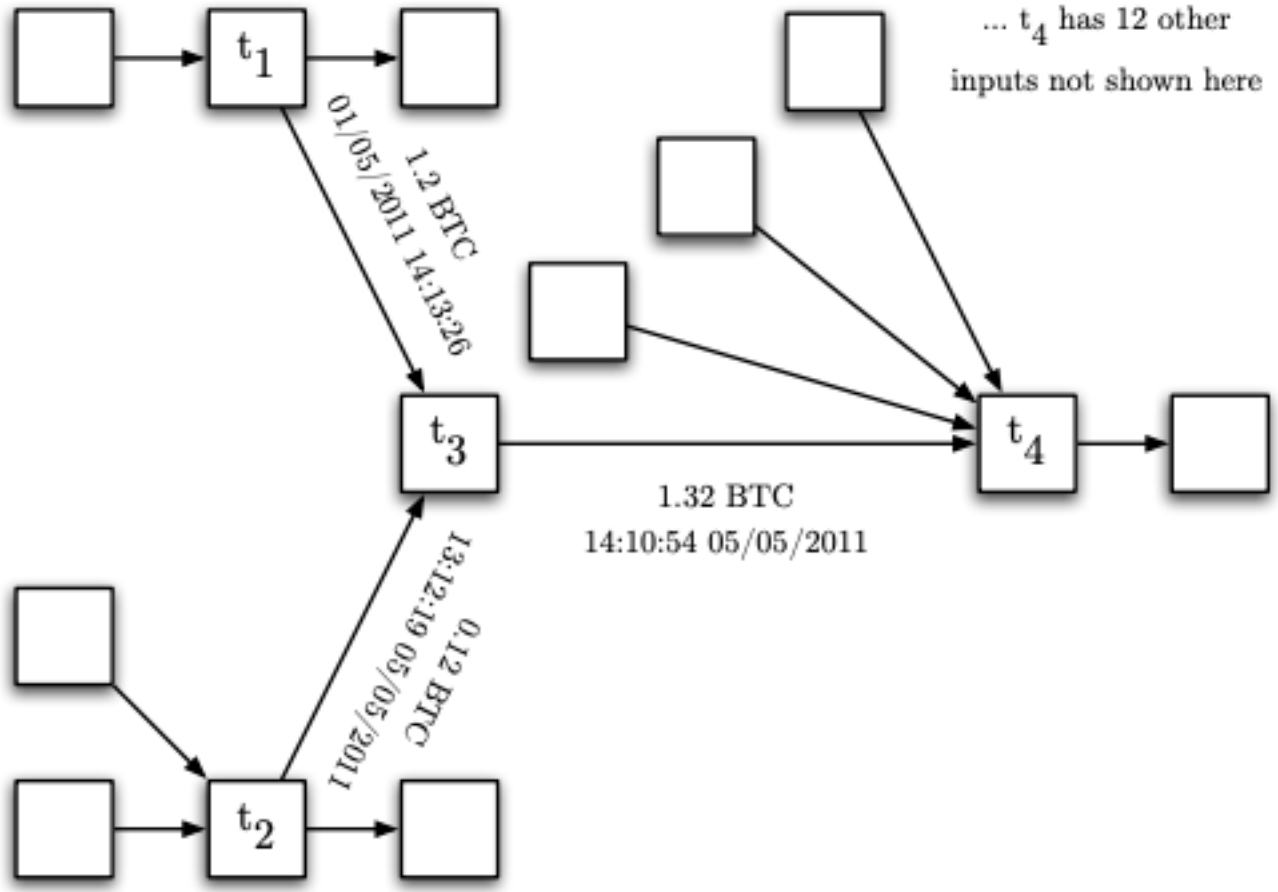
- it is still possible to link pseudonyms to real identities by utilizing the blockchain data together with the external information obtained from different Internet sources such as twitter posts, forums etc.
- since bitcoin enables users to create more than one address, the first goal here is to cluster all addresses belonging to the same user
- analyze the study proposed Reid and Harrigan [1]

Privacy Issues

- it is still possible to link pseudonyms to real identities by utilizing the blockchain data together with the external information obtained from different Internet sources such as twitter posts, forums etc.
- since bitcoin enables users to create more than one address, the first goal here is to cluster all addresses belonging to the same user
- analyze the study proposed Reid and Harrigan [1]
  - they obtained all the transactions recorded in bitcoin from January 2009 to July 2011 (1019486 txs between 1253054 addresses)
  - they built two networks (transaction and user) based on the input-output relationship between transactions and re-use and co-use of the addresses

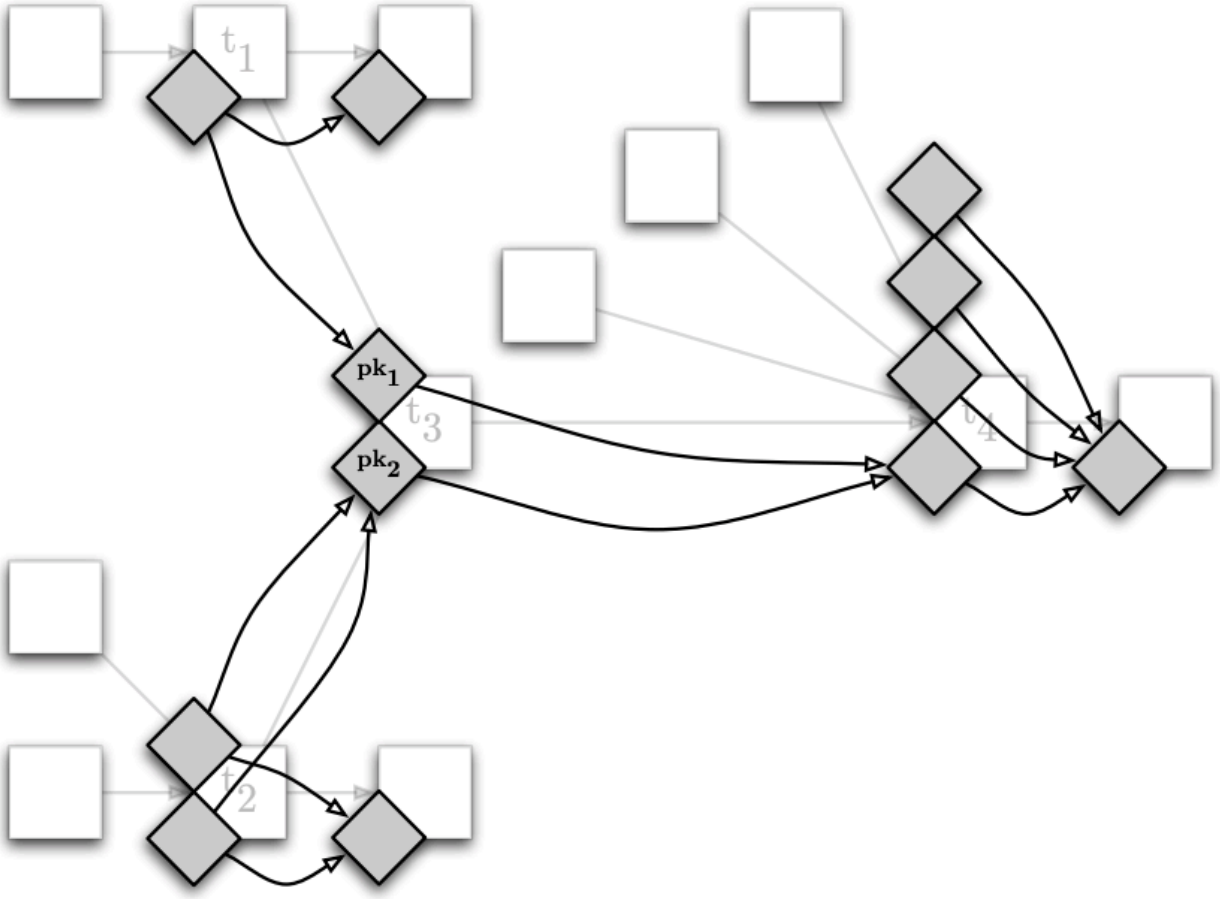
Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- a sub-network of transaction network



Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- a sub-network of user network



Privacy Issues

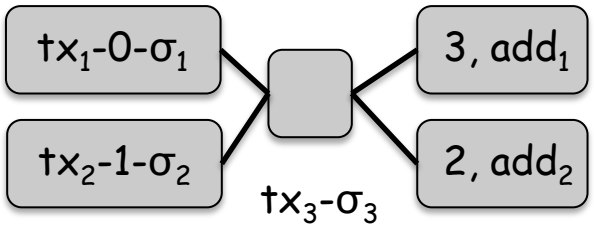
- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)

Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid

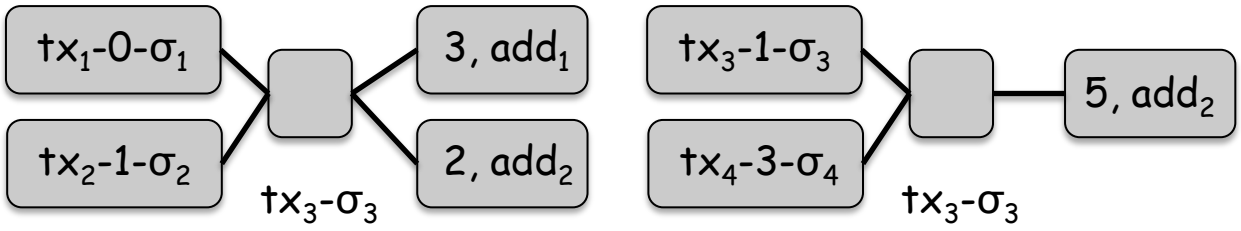
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



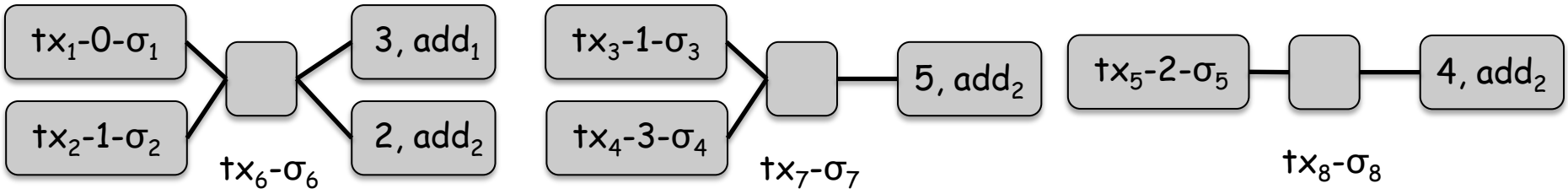
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



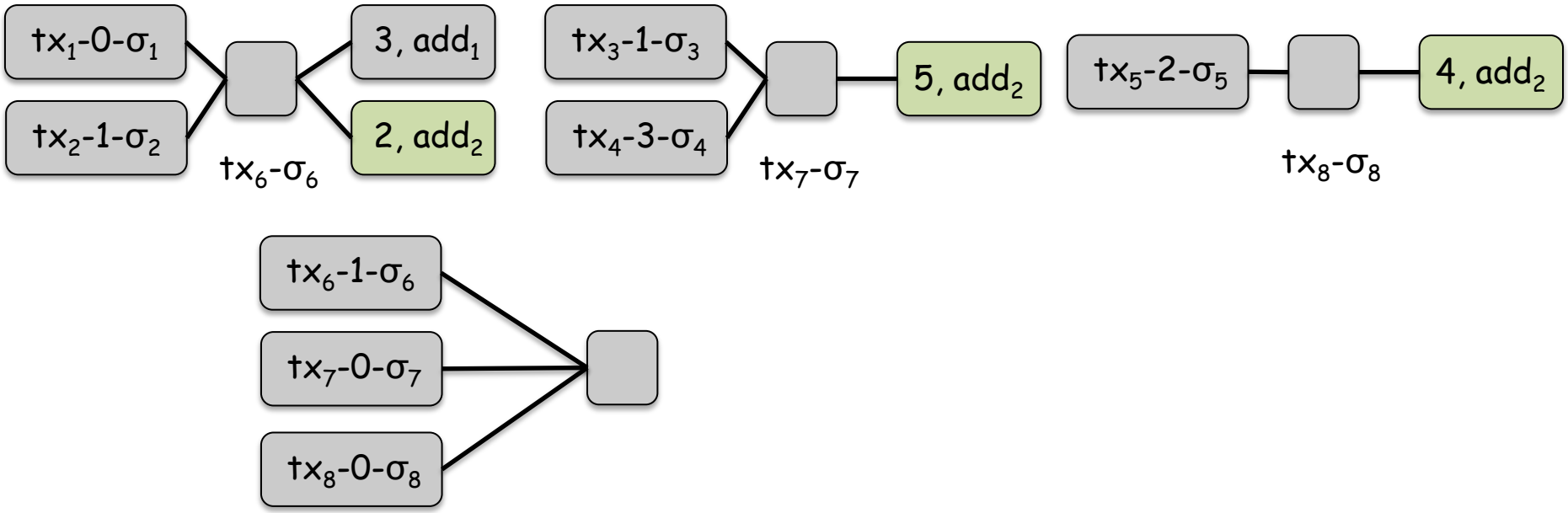
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



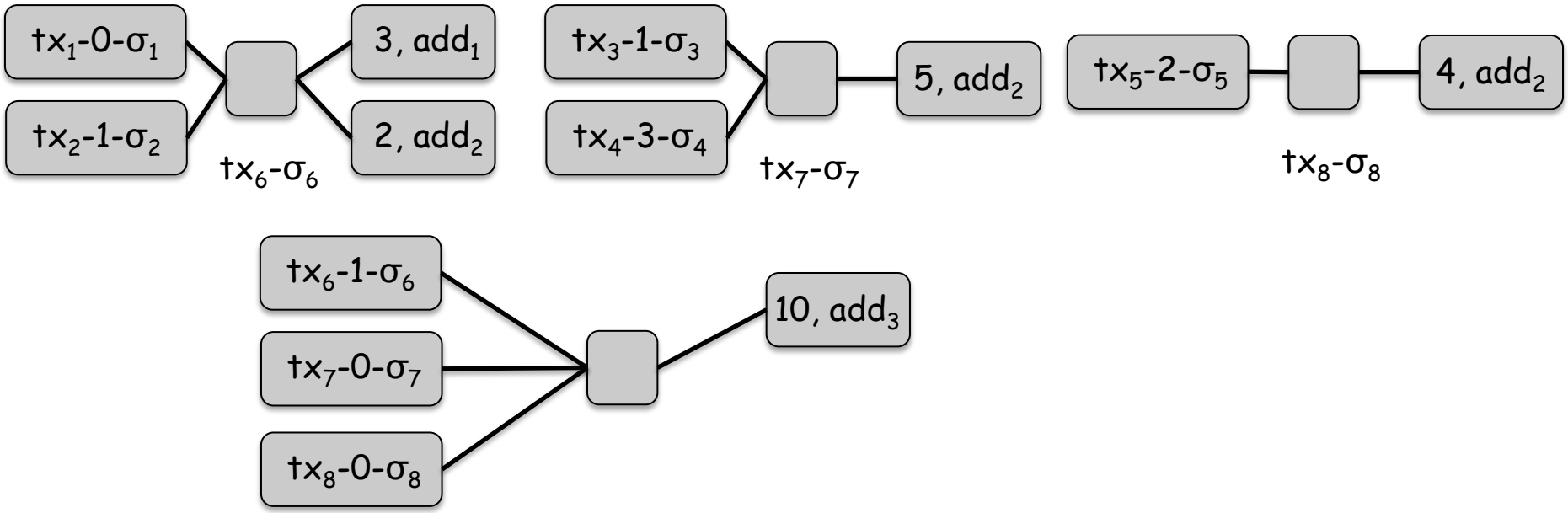
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



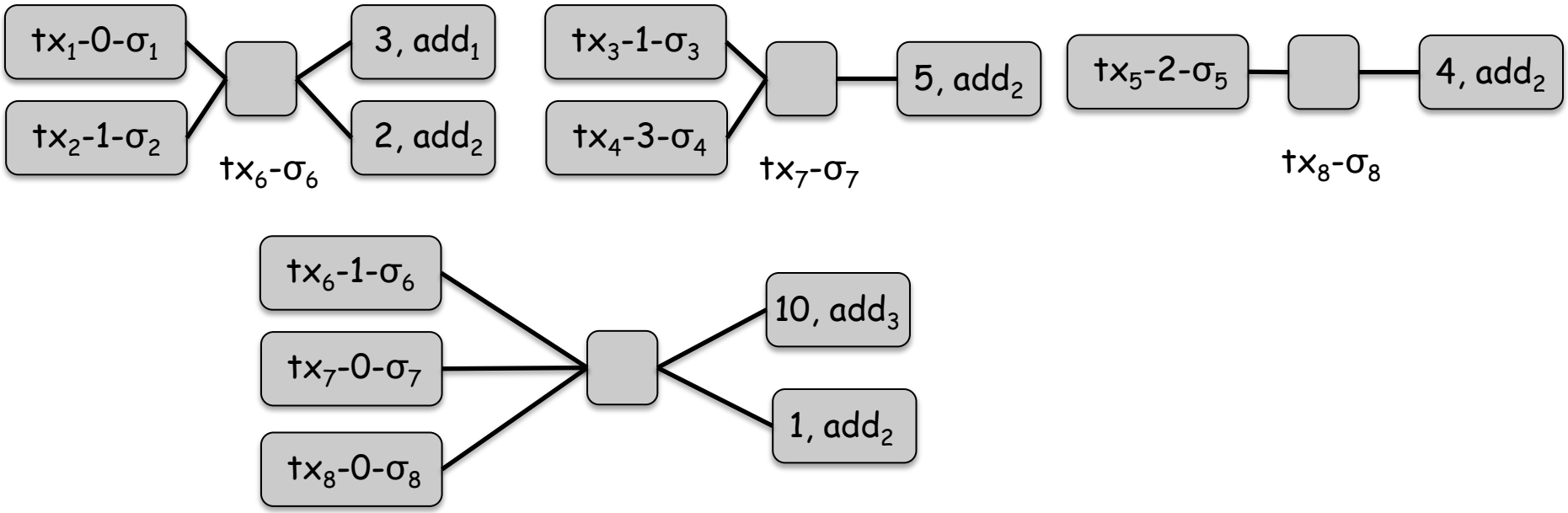
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



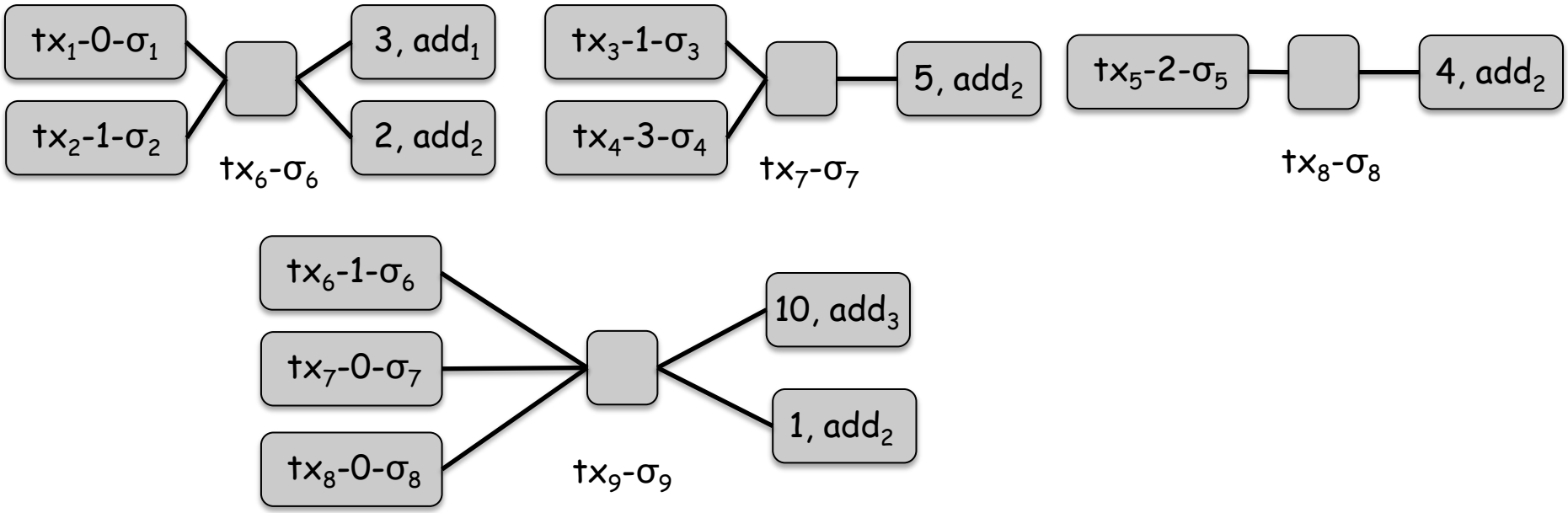
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



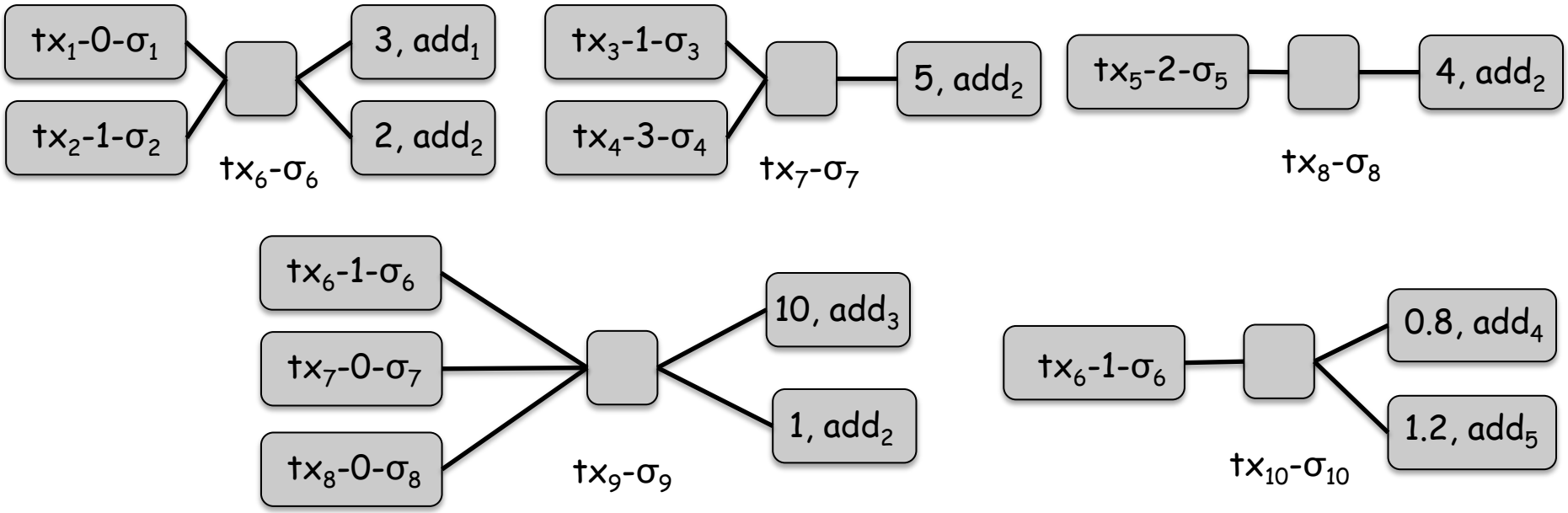
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



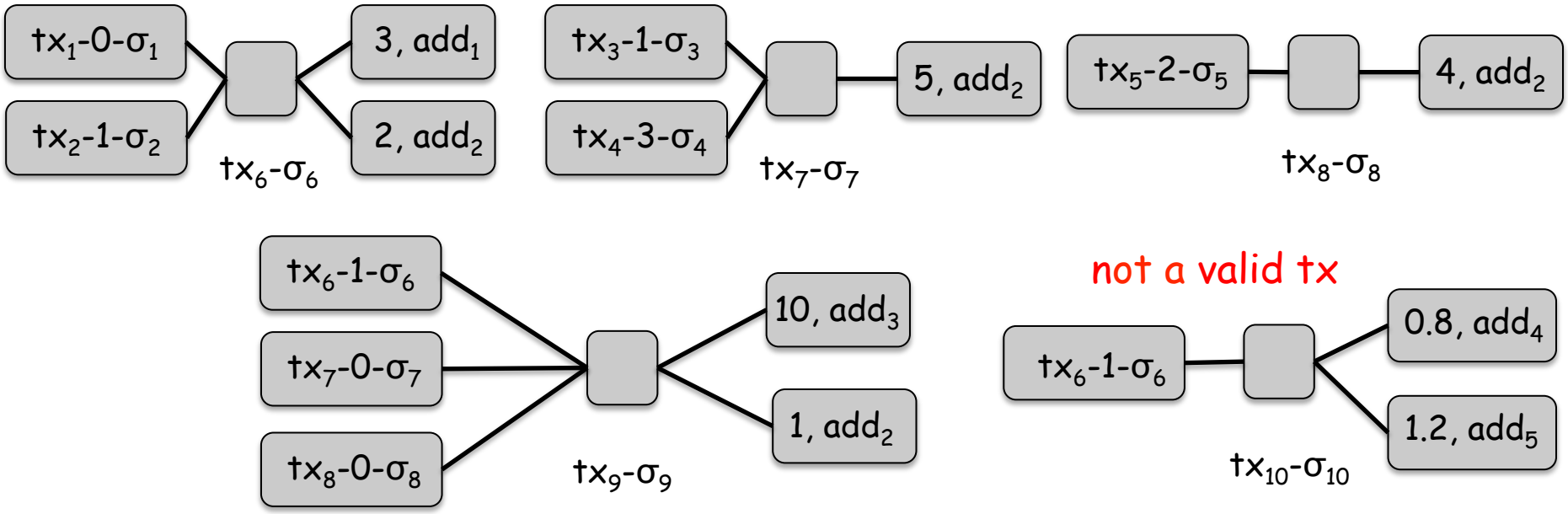
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- some findings:
  - user network has cyclic structure (it is expected to just contain Bitcoin flows between one-time addresses keys that were not connected to other addresses)
  - a tx frequently has single input from a larger tx, or multiple inputs from smaller txs
  - a tx frequently has two outputs: one for payment, one directing to user's other address

Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- some findings:
  - user network has cyclic structure (it is expected to just contain Bitcoin flows between one-time addresses keys that were not connected to other addresses)
  - a tx frequently has single input from a larger tx, or multiple inputs from smaller txs
  - a tx frequently has two outputs: one for payment, one directing to user's other address
- data obtained from different Internet sources such as twitter posts, bitcoin forums etc. (they usually post one of their addresses) used to link an address to a real identity
  - utilizing user network, they can even link public addresses to some other address belonging to same users

Privacy Issues

- analyze the study proposed Reid and Harrigan [1]

- they also examined the theft of 25k BTC reported in the bitcoin forums

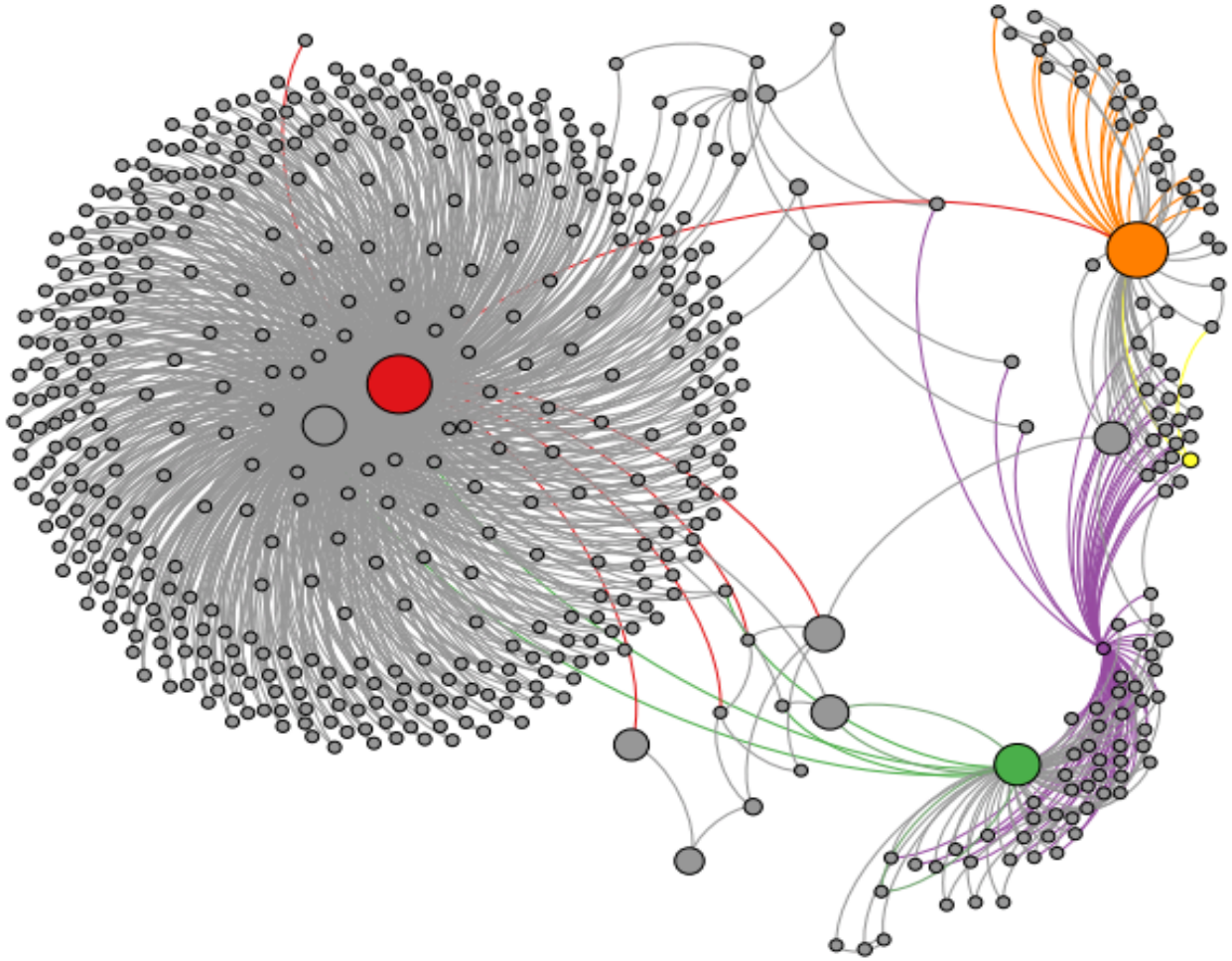
Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- they also examined the theft of 25k BTC reported in the bitcoin forums

- attacker broke into allinvain's Slush pool account and changed the payout address as his address

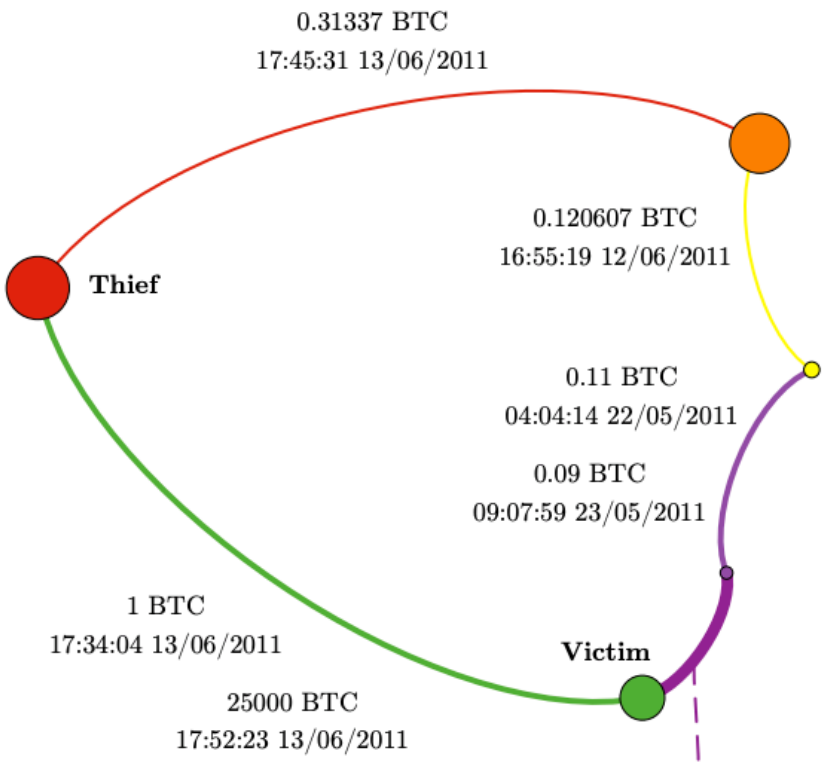
Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- they also examined the theft of 25k BTC reported in the bitcoin forums



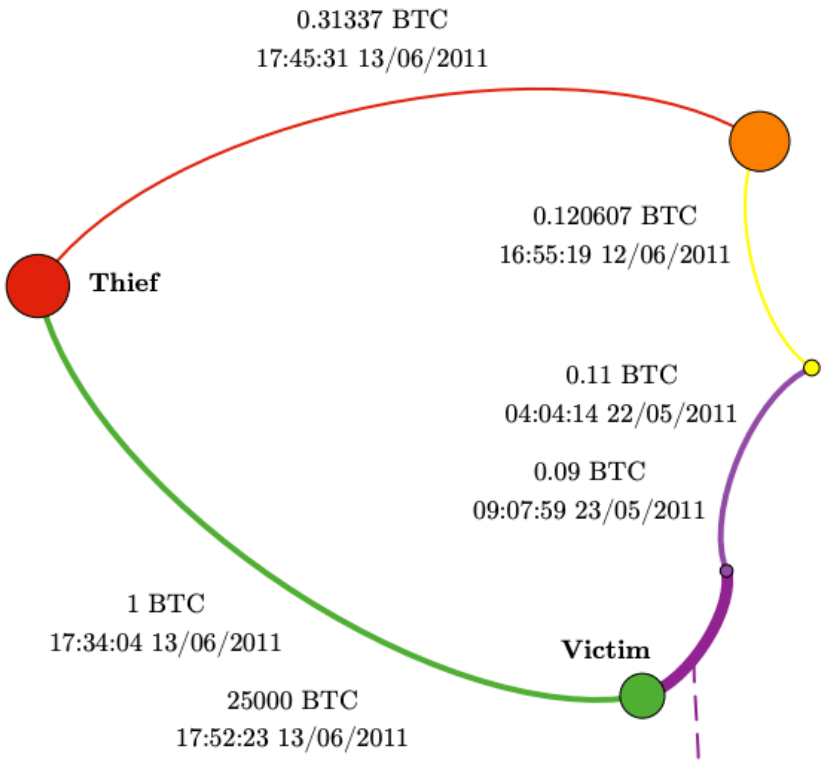
Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- they also examined the theft of 25k BTC reported in the bitcoin forums
- they deduced that thief address belongs to allinvain



Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- they also examined the theft of 25k BTC reported in the bitcoin forums
- they deduced that thief address belongs to allinvain



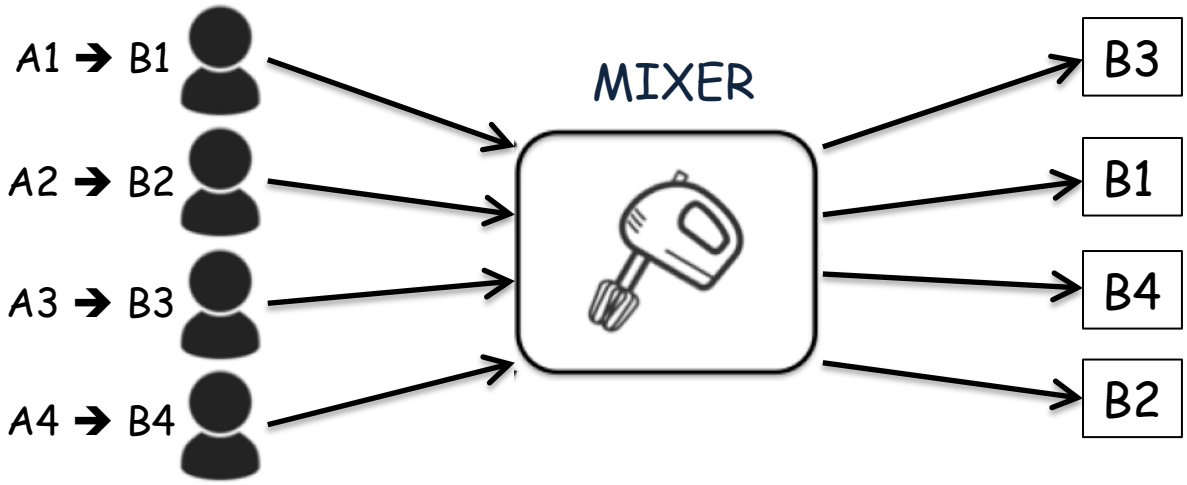
he even tried to associate the thief with the hacker group LulcSec by creating a transaction from hacker to that group

Privacy Enhancing Techniques

- break the link between source and destination address

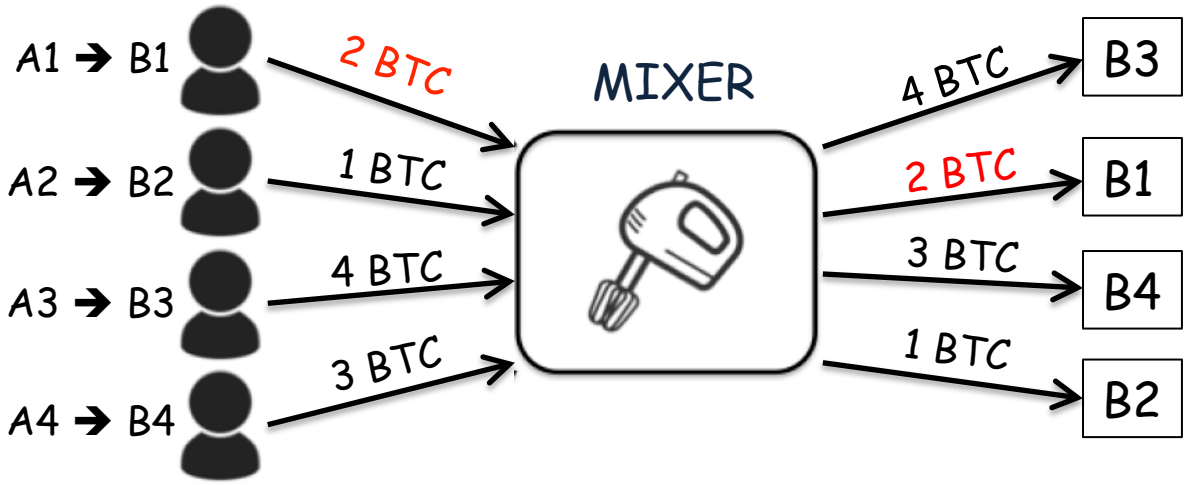
Privacy Enhancing Techniques - Mixing

- break the link between source and destination address



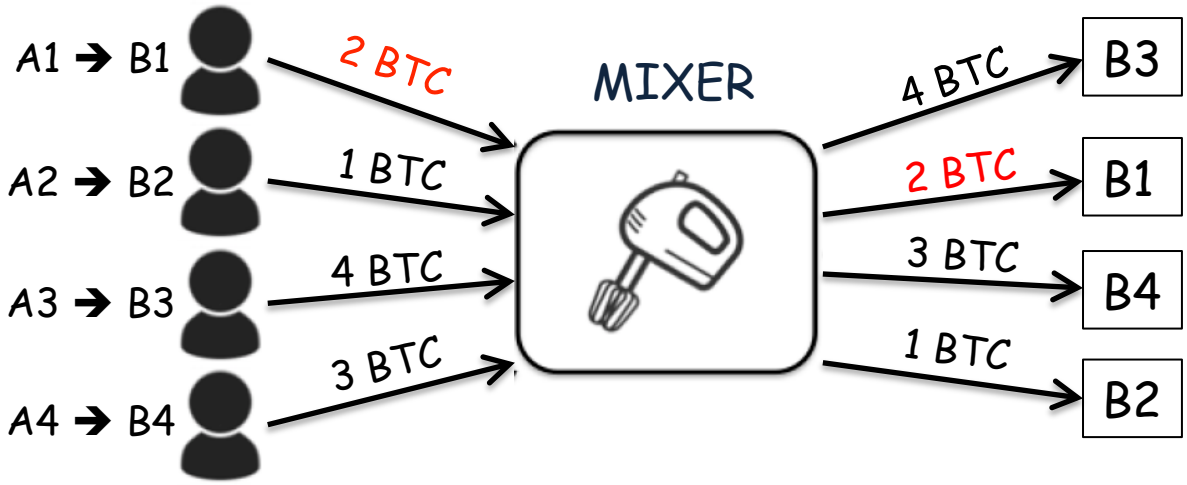
Privacy Enhancing Techniques - Mixing

- break the link between source and destination address



Privacy Enhancing Techniques - Mixing

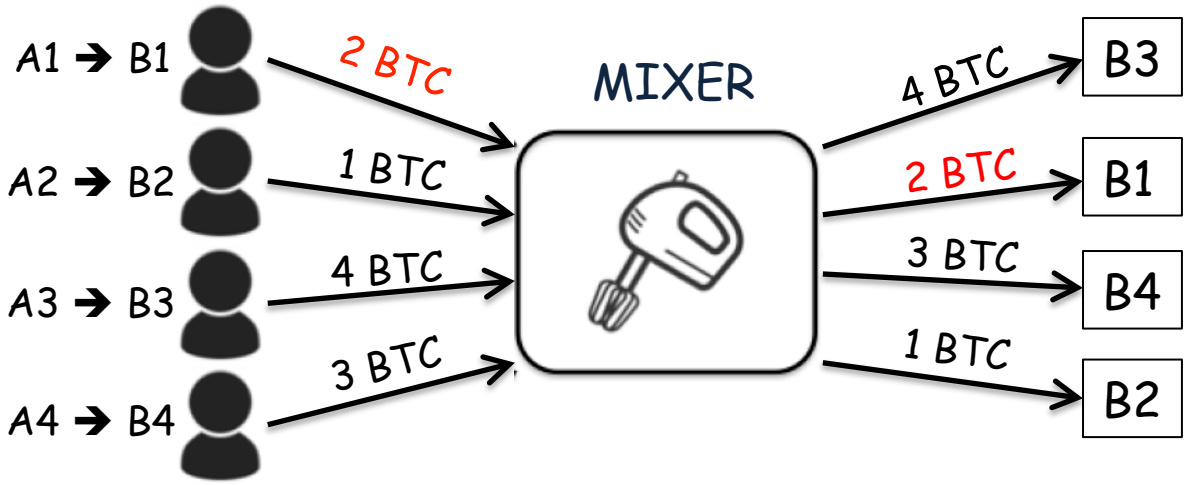
- break the link between source and destination address



- transaction amount should be same to be indistinguishable

Privacy Enhancing Techniques - Mixing

- break the link between source and destination address



- transaction amount should be same to be indistinguishable
- mixer should be trusted
  - it can steal the money
  - it knows all the senders and receivers addresses, it can reveal that information

Privacy Enhancing Techniques - Mixing

Mixcoin

- introduced by Bonneau et al. [2] in 2014

Mixcoin

- introduced by Bonneau et al. [2] in 2014

- before sending bitcoin, sender takes a signed warrant from the mixer stating that

  if the mixer gets x bitcoin from A by time t, it will send x′ bitcoin to B by time t′

Mixcoin

- introduced by Bonneau et al. [2] in 2014

- before sending bitcoin, sender takes a signed warrant from the mixer stating that

  if the mixer gets x bitcoin from A by time t, it will send x' bitcoin to B by time t'

- if mixer steals the money, A publishes the warrant to ruin mixer's reputation

Mixcoin

- introduced by Bonneau et al. [2] in 2014

- before sending bitcoin, sender takes a signed warrant from the mixer stating that

  if the mixer gets x bitcoin from A by time t, it will send x' bitcoin to B by time t'

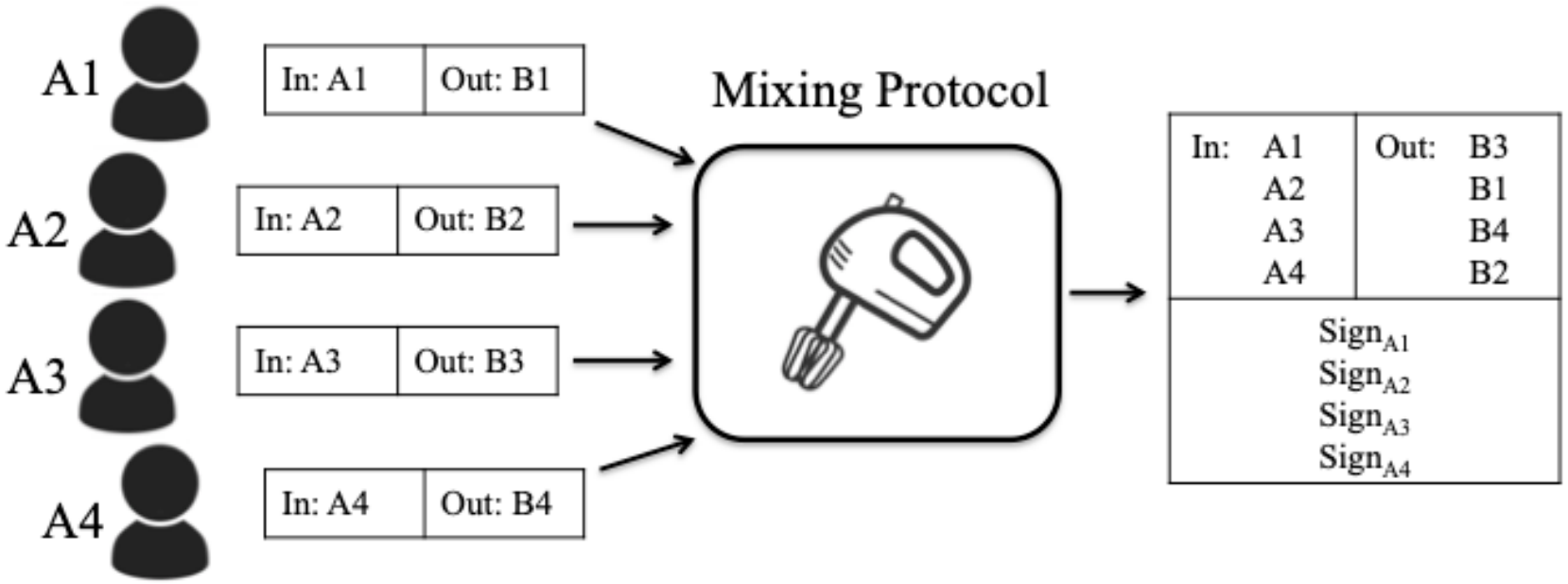
- if mixer steals the money, A publishes the warrant to ruin mixer's reputation

- mixer may reveal the sender's and receiver's address

Privacy Enhancing Techniques - Mixing

CoinJoin

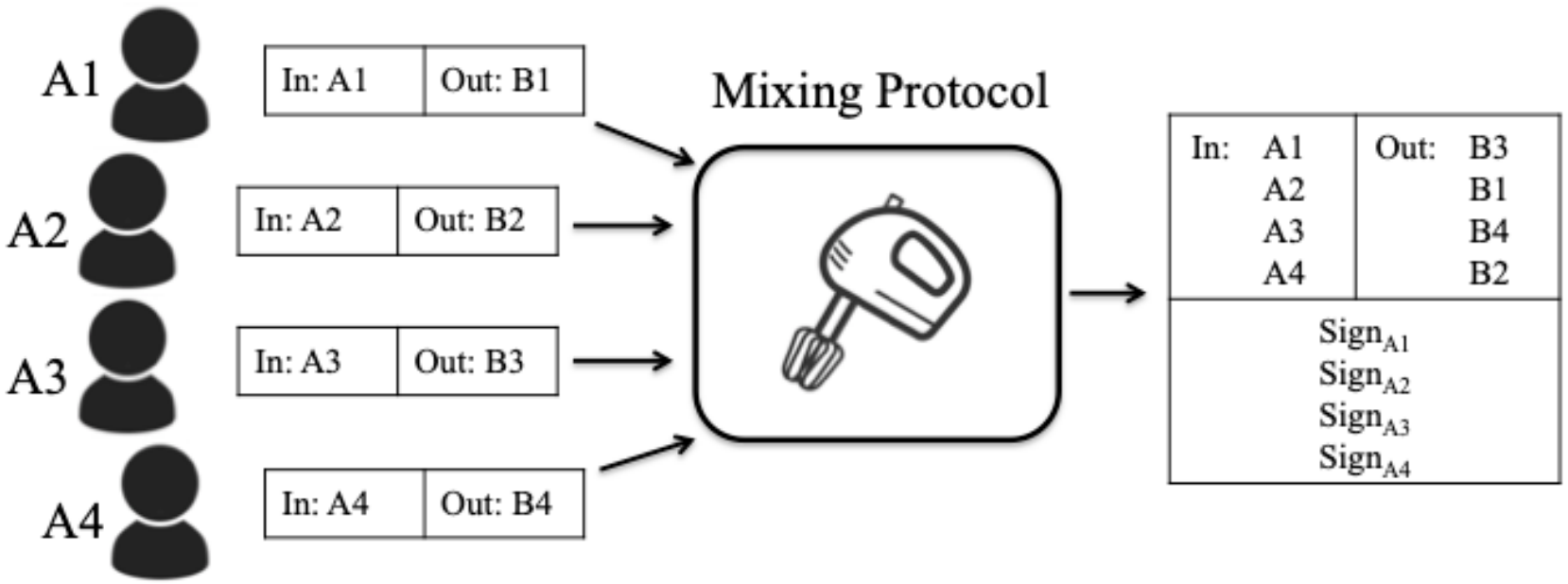
- introduced by Maxwell [3] in 2013
- utilized in practice by different systems



Privacy Enhancing Techniques - Mixing

CoinJoin

- introduced by Maxwell [3] in 2013
- utilized in practice by different systems



- insiders can reveal the link of each transaction

CoinShuffle

- introduced by Ruffing et al. [4] in 2014