CS251 Fall 2021

(cs251.stanford.edu)

Privacy, Mixers and Monero

Benedikt Bünz

Privacy for Cryptocurrencies

What information might a user want to hide?

Identity (anonymity):

- Who they are
- Who they pay
- Who pays them

Amounts:

- How much they are paying
- How much are they receiving
- E.g. salary

Metadata:

- Script Sig, e.g multisig threshold
- Smart contract

Anonymity

Weak Anonymity (Pseudonymity):
One consistent Pseudonym (e.g. reddit)
Pros: Reputation
Cons: Linkable posts, one post linked to you-> all posts linked to you
Writing style, topics of interest may link you

Strong Anonymity:
Cons: No Reputation

Who needs privacy for payments

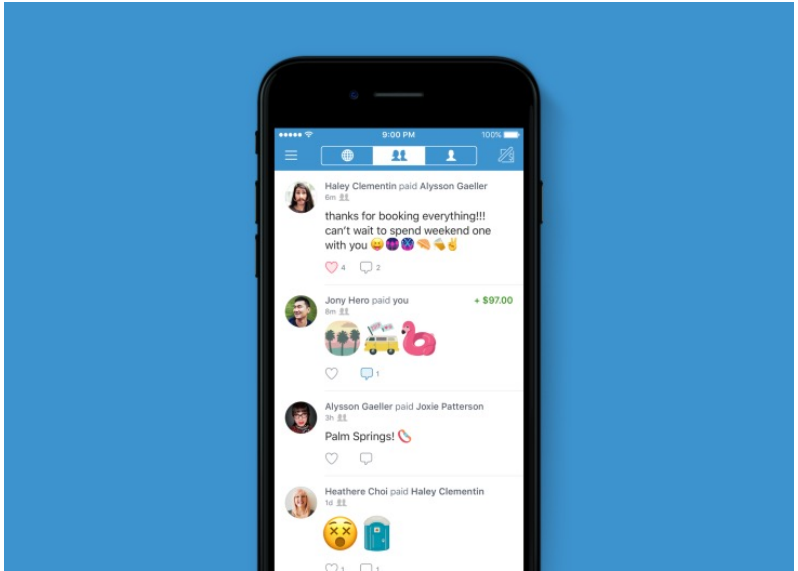
Companies:

- Ford does not want to reveal cost of tires
- Salaries of employees
- Investment funds want to keep strategies private

Who needs privacy for payments

Consumers

- Salary, Rent, Purchasing things online, Donations



Who needs privacy for payments

Criminals:

- Stolen funds (WannaCry), buying/selling drugs, tax evasion

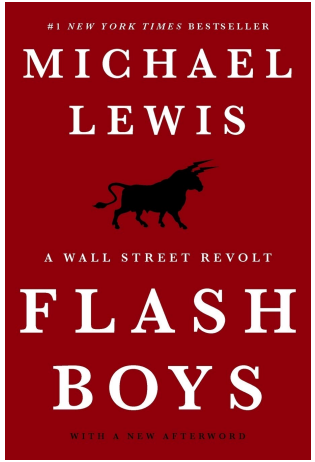
Silk Road

anonymous marketplace

Who needs privacy for payments

Applications:

- Privacy can prevent frontrunning
- Exchanges may want to keep orderbook private
- Sealed bid auction

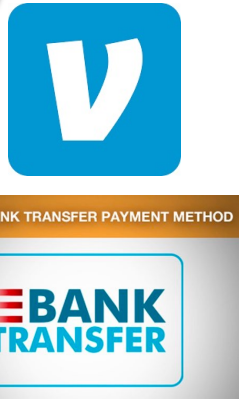


Privacy of Digital Payments

Payments publicly visible/linkable

Payments only visible to bank/venmo. Optionally sender/receiver public

Unlinkable private payments



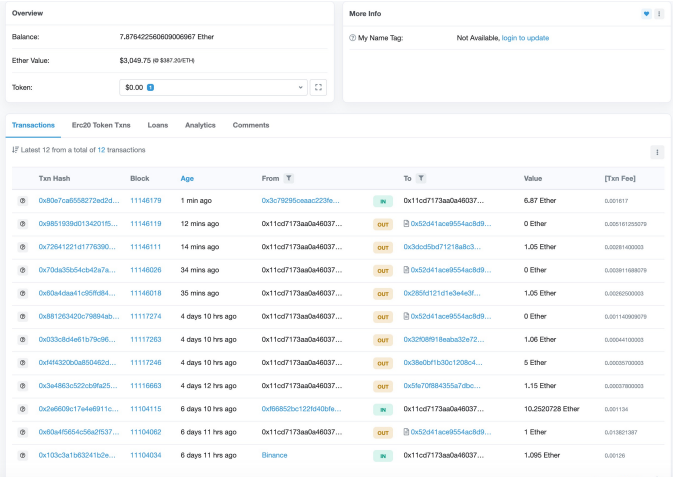
Less private ⟷ More private

Privacy in Ethereum

Overview | **State** | Comments

Advanced A set of information that represents the current **state** is updated when a transaction takes place on the network. The below is a summary of those changes :

Address	Before	After	State Difference
0x11cd7173aa0a46037…	1.006422560609006967 Eth	7.876422560609006967 Eth	▲ 6.87
0x3c79295ceaac223fe…	6.875943148 Eth Nonce: 20	0.004326148 Eth Nonce: 21	▼ 6.871617



Weak Pseudonymity:

- Account public
- Values public
- Mostly one account per user
- Some accounts known (Binance)

Privacy in Bitcoin

Summary

Size	1110 (bytes)
Fee Rate	0.0016173243243243244 BTC per kB
Received Time	Apr 10, 2017 12:38:00 AM
Mined Time	Apr 10, 2017 12:38:00 AM
Included in Block	0000000000000000001f0115cca585646832b337404032c88539ce2995e799e5c

Details

c2561b292ed4878bb28478a8cafd1f99a01faeb9c5a906715fa595cac0e8d1d8

mined Apr 10, 2017 12:38:00 AM

16k4365RzdeCPKGwJDNNBEkXj696MbChwx	0.53333328 BTC	>	1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA	0.01031593 BTC (U)
1Bsh4KD9ZJT4dJcoo7S5uS1jvtmtVmREb7	1.47877788 BTC		1AFLhD4EtG2uZmFxmfdXCyGUNqCqD5887u	2 BTC (S)

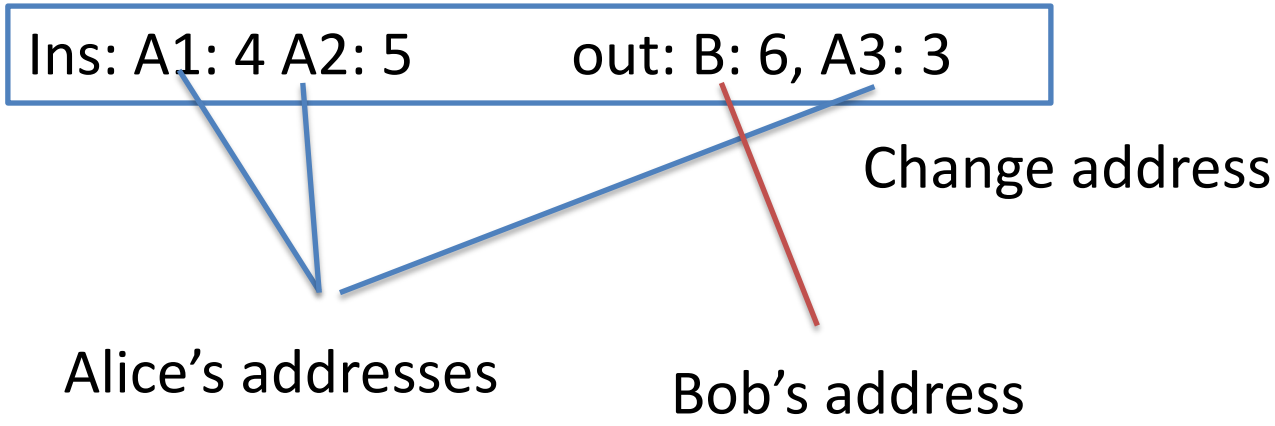
FEE: 0.00179523 BTC

1 CONFIRMATIONS

2.01031593 BTC

Privacy in Bitcoin

Alice can have many addresses (creating address is free)



Linking Addresses to Identities

Ins: A1: 4 A2: 5 out: B: 6, A3: 3

- Buying book from merchant
  - Alice learns one of merchant's addresses (B)
  - Merchant learns three of Alice's addresses
- Alice uses an exchange BTC ←→ $
  - KYC (Know your customer)
  - Money serving business collect and verify IDs

Linking Addresses to Identities

Ins: A1: 4 A2: 5 out: B: 6, A3: 3

- Buying book from merchant
  - Alice learns one of merchant's addresses (B)
  - Merchant learns three of Alice's addresses
- Alice uses an exchange BTC ←→ $
  - KYC (Know your customer)
  - Money serving business collect and verify IDs
  - Exchange learns real ID

Donating to Wikileaks

35cebb3fccb87014576cdc812a795149219bcc841add3bd5fde7df4ed6cfc86a | 118 Satoshis/vByte | 0.00039648 BTC | 643,240 | 2020-08-11 18:55:42

3KRN5kfK5CquqvXQSX8A9Tz8Ek7GRdYgpM	0.01651783	WikiLeaks	0.00010000
		3KRN5kfK5CquqvXQSX8A9Tz8Ek7GRdYgpM	0.01602135

+ 0.00010000 | 11,325 Confirmations

ed0a9b313673147e54e60f586e954866698d7d57172900e147c71dd6430d7a99 | 21 Satoshis/vByte | 0.00004663 BTC | 638,139 | 2020-07-07 13:49:18

WikiLeaks	0.00359357	33wvNiUkXJAJ85e4yXJxJVWtsKqWDsDFK4	0.00354694

Bitcoin

Wikileaks

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

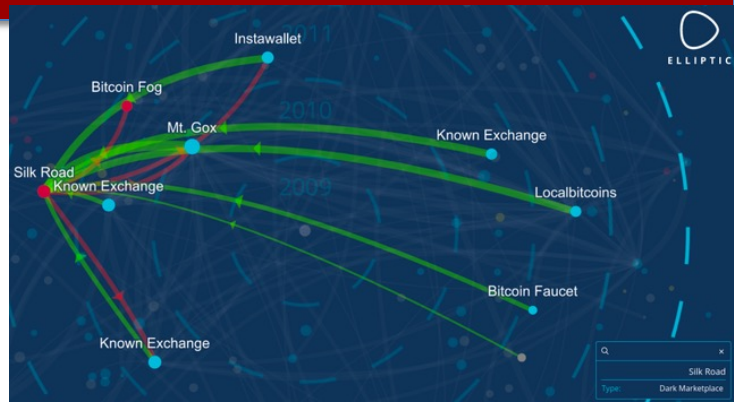
Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (https://bitcoin.org) or read more on Wikipedia.

For a more private transaction, you can click on the refresh button above to generate a new address

Wikileaks had one address -> Easy to see who donates

Is Bitcoin Anonymous?

Now commercialized:



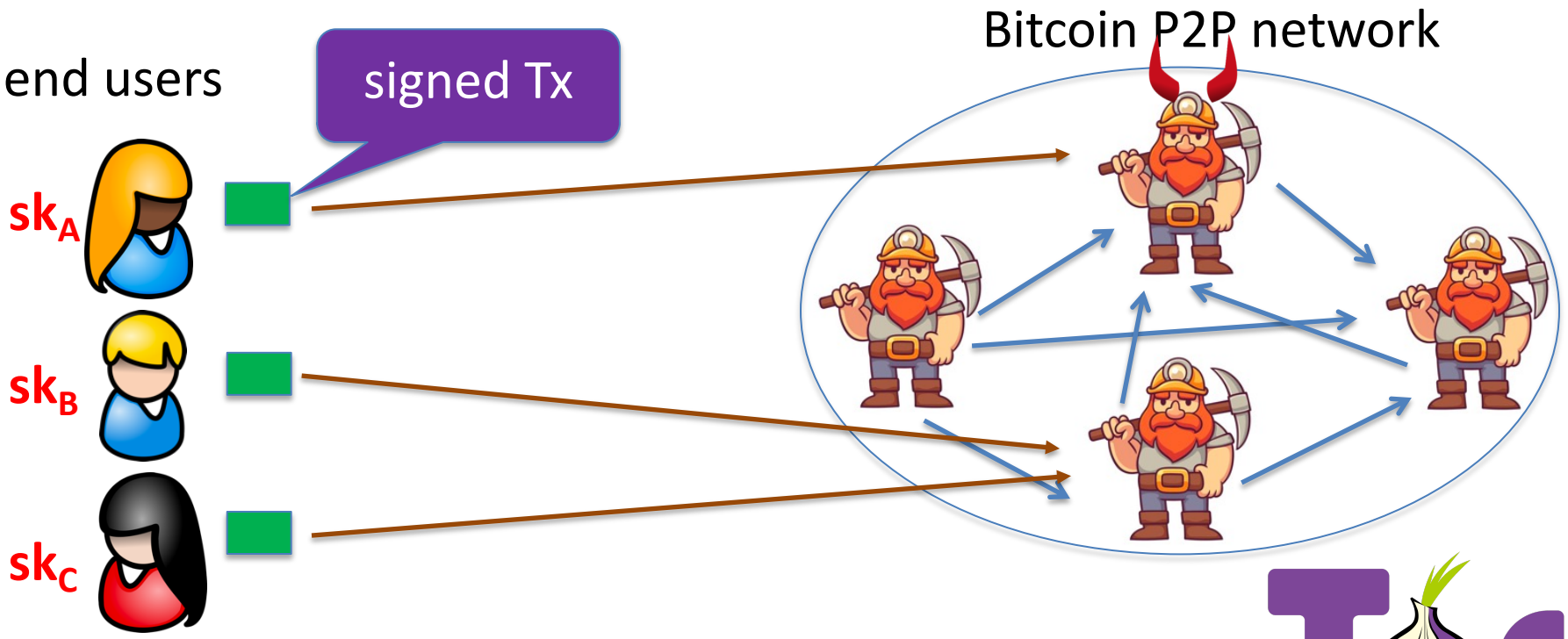
No!

It is possible to:

- Link all addresses of a single entity:
  - Determine total assets
- Given two TX A->B, C->D, Are B&C the same
  - If D knows C, can unmask B
  - Trace stolen funds, find tax evasion
  - Oppressive governments (Venezuela, North Korea)
- Test if Alice ever paid Bob (Wikileaks)

Often answer is yes for all 3. How?

Network Anonymity

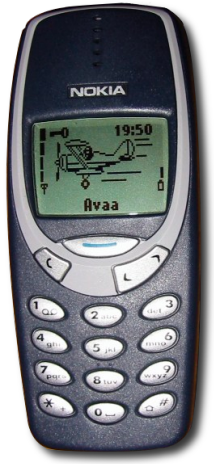


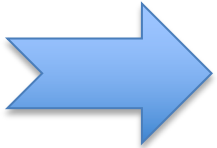
Can learn Alice's IP address

Solution:

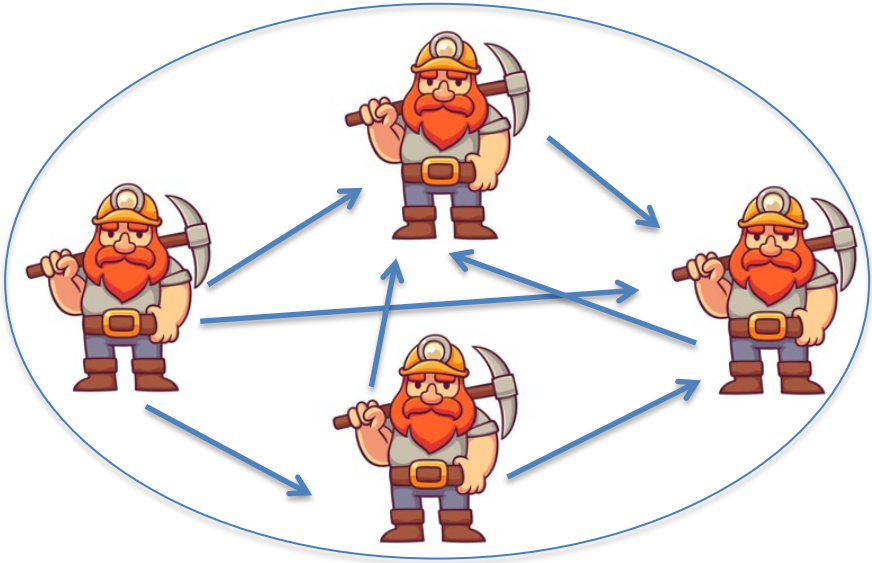
Light client network anonymity

SPV client





Full node



All addresses and transactions

Fully linkable!

Idioms of use

Heuristic 1:

Two addresses are input to same TX (and not multisig script)

-> both addresses are controlled by same entity

c2561b292ed4878bb28478a8cafd1f99a01faeb9c5a906715fa595cac0e8d1d8 mined Apr 10, 2017 12:38:00 AM

16k4365RzdeCPKGwJDNNBEkXj696MbChwx	0.53333328 BTC	1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA	0.01031593 BTC (U)
1Bsh4KD9ZJT4dJcoo7S5uS1jvtmtVmREb7	1.47877788 BTC	1AFLhD4EtG2uZmFxmfdXCyGUNqCqD5887u	2 BTC (S)

FEE: 0.00179523 BTC

1 CONFIRMATIONS 2.01031593 BTC

Idioms of use

Heuristic 2:

Change address is controlled by same user as input address

Which is change address: Used to be first address

Heuristic: Only new address, Non round, Less than inputs

c2561b292ed4878bb28478a8cafd1f99a01faeb9c5a906715fa595cac0e8d1d8

mined Apr 10, 2017 12:38:00 AM

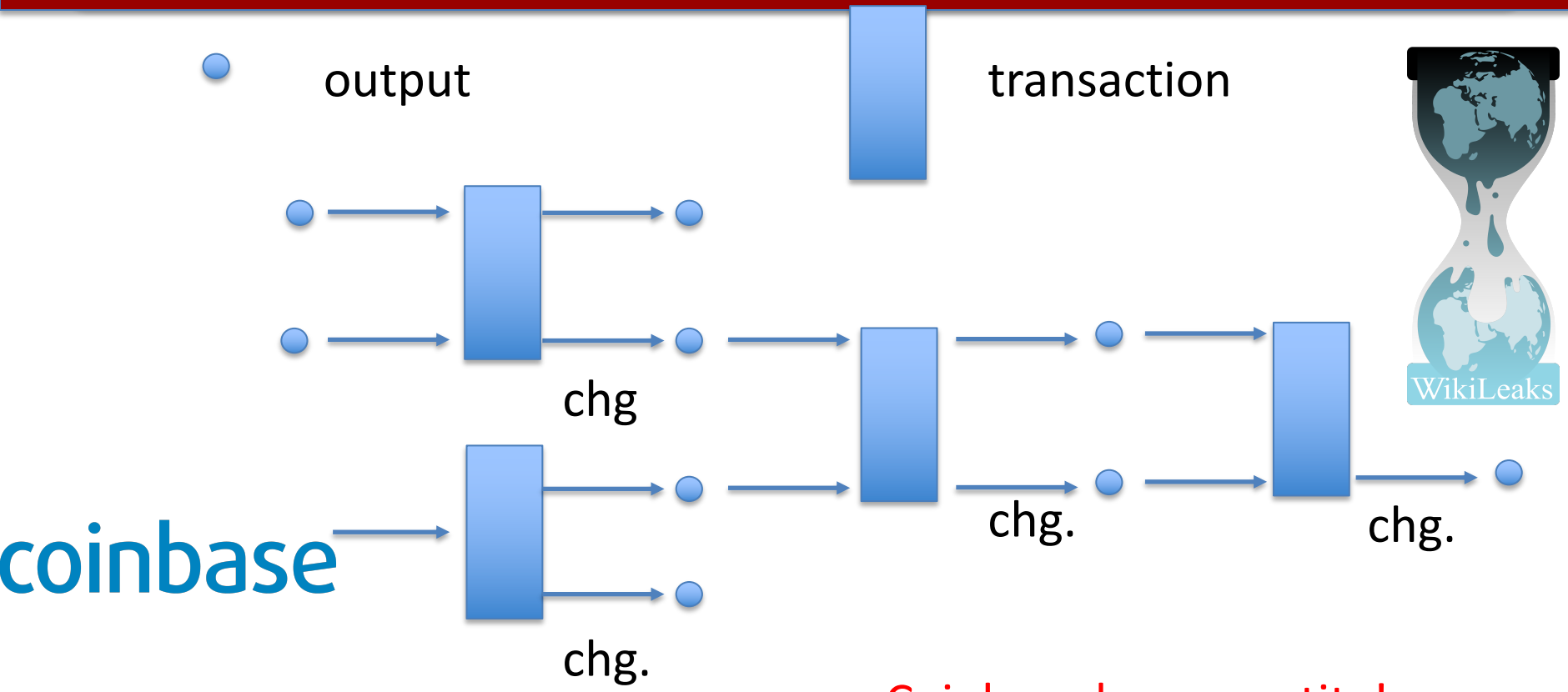
16k4365RzdeCPKGwJDNNBEkXj696MbChwx	0.53333328 BTC	1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA	0.01031593 BTC (U)
1Bsh4KD9ZJT4dJcoo7S5uS1jvtmtVmREb7	1.47877788 BTC	1AFLhD4EtG2uZmFxmfdXCyGUNqCqD5887u	2 BTC (S)

FEE: 0.00179523 BTC

1 CONFIRMATIONS

2.01031593 BTC

Example tracing



Coinbase knows entity!

Experiment (2013)

- Use Heuristic 1 and 2 -> 3.3M clusters
- ID 1070 addreses by interacting with merchants
  - Coinbase, Bitpay, …
- Learn ID of 2200 clusters
  - 1.8M address
  - 15% of total value
  - Track multiple thefts
  - Learn total assets for each cluster

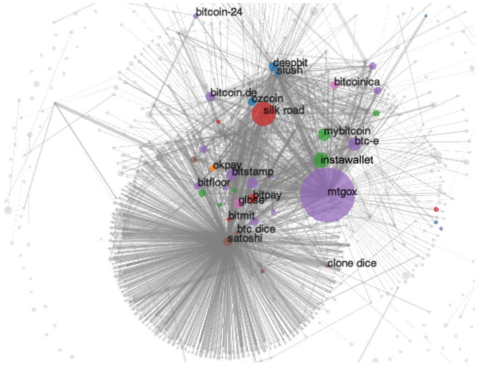


Figure 6: A visualization of the user network. The area of the cluster represents the external incoming value; i.e., the bitcoins received from

Making Cryptocurrencies anonymous

Mixing

Anonymous cryptocurrencies

Another example

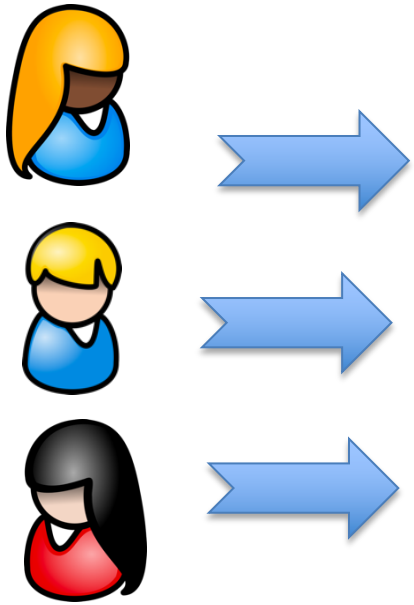
Ins: A1: 1. out: EC1 1

Ins: EC1: 1 out: S: 0.8, EC2: 0.2

Alice and Subcontractor learn EC's profit margin.

How can we prevent this?

Another example



Ins: A1: 1. out: EC1 1

Ins: EC1: 1 out: S: 0.8, EC2: 0.2

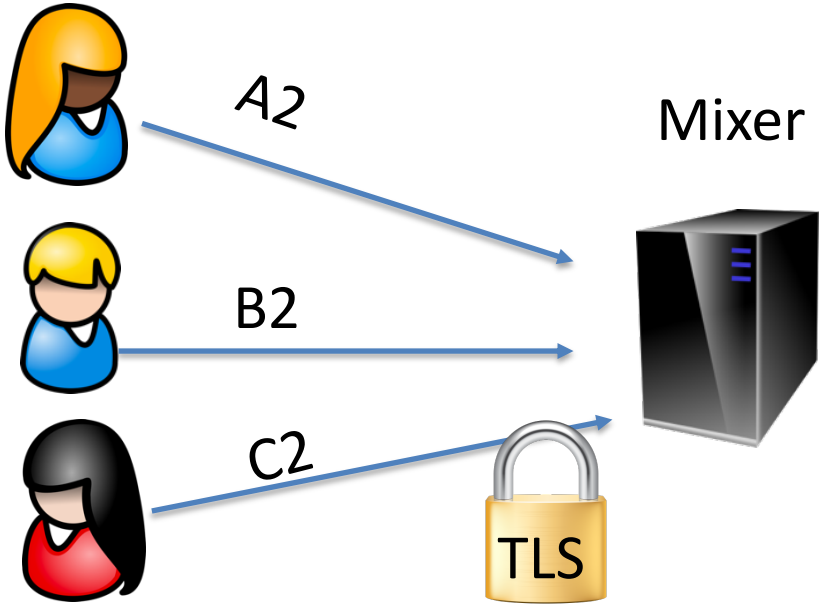
EC has many customers. Mix payments -> use some to pay sub

Mixing

A1 -> M: 1

B1 -> M: 1

C1 -> M: 1



Ins: M: 3 Outs: B2: 1, A2: 1, C2: 1

Mixing Analysis

- Outside observer who is A2?
  - A2 $\in \{Alice, Bob, Carol\}$
- For Bob
  - A2 $\in \{Alice, \cancel{Bob}, Carol\}$
- The more the better mixing

Mixer Problems

- Mixer can deanonymize
- All outputs MUST have same value
  - If not you can match inputs and outputs
- Mixer takes transaction fees
- Mixer can steal funds
- ScriptPK for all outputs must be the same
  - Otherwise linkable on spend

CoinJoin (Mixing without Mixer)

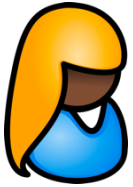
CoinJoin TX

Ins: :A1: 5, B1: 3, C1: 2
Outs: B2: 2, A2: 2, C2: 2
Change (not private): A3: 3, B3: 1
Signed: Multisig A1, B1, C1

Out value = min of inputs

Usually ~40 inputs

CoinJoin



A1: 5, A3 (change)

A2 (over Tor)

Add Signatures

Online Forum

PASTEBIN

A1: 5, A3
B1: 3, B3
C1: 2, C3

B2,A2,C2

Publish Transaction

What if A1 is spent?

Coinjoin drawbacks

Coinjoin still has drawbacks:

- Interaction required
- Any party can disrupt the process
- Anonymity set determined by who is using the service
- Transaction amounts public

Cryptonote (Monero)

- Cryptonote protocol, proposed in 2012
- Enables non interactive coinjoin
- Sender can choose anonymity set
- Hides amounts
- Basis of Monero, Mobile coin, others

Recap Signatures

Def: a signature scheme is a triple of algorithms:

- **Gen**(): outputs a key pair (pk, sk)
- **Sign**(sk, msg) outputs sig. σ
- **Verify**(pk, msg, σ) outputs 'accept' or 'reject'

Secure signatures: (informal)

Adversary who sees signatures on many messages of his choice, cannot forge a signature on a new message.

Linkable Ring Signatures

Def: a signature scheme is a triple of algorithms:

- **Gen**(): outputs a key pair (pk, sk)
- **RingSign**(sk,PKs, msg) outputs sig. σ
- **Verify**(~~pk,~~ PKs, msg, σ) outputs 'accept' or 'reject'
- **Link**(PKs, msg, σ, PKs', msg', σ') outputs 0 or 1

PKs=$\{pk_1, pk_2, \ldots, pk_n\}$
pk∈PKs

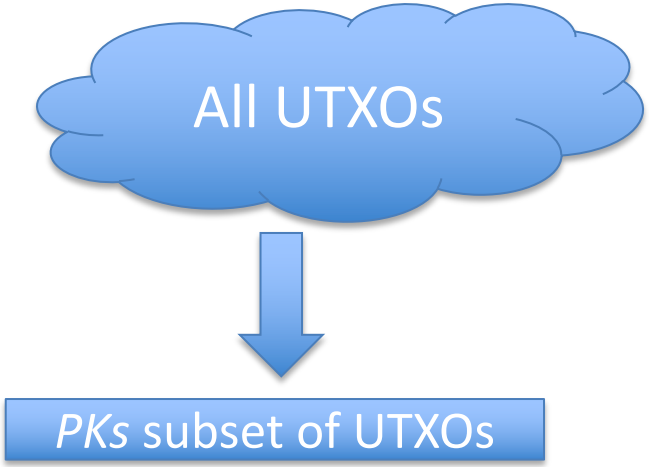
Secure signatures: (informal)

Unforgeability: Adversary who sees signatures on many messages of his choice, cannot forge a signature on a new message.

Anonymity: **Sign**(sk_i,PKs, msg) ≈ **Sign**(sk_j,PKs, msg) for $pk_i, pk_j \in PKs$

Linkability: If a secret key signs two messages, then the signatures can be linked

CryptoNote



Additional Pieces:

- Generate PK_S without interaction
- Make amounts private (next lecture)

Fresh PK_R

TX: Inputs *PKs* , Output: PK_R, Signature: Sign(sk, *PKs* ,TX)

CryptoNote analysis

- Sender picks anonymity set
  - Ring signature provides anonymity in set
  - The larger the set the better
  - Still not perfect (e.g. if I know all other PKs in set)
- Linkability of ring signatures prevents double spends
- Keys can only be used once
- Hides amounts (unlike coinjoin)
- Fully non interactive

END OF LECTURE

Next lecture:

Zero-knowledge SNARKs