Privacy for Crypto

Ronghui Gu

Fall 2024

Columbia University

Course website: https://verigu.github.io/6998Fall2024/

1 What Information to Hide?

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 youLending

Anonymity

Strong Anonymity:

- **Pros**: Privacy
- **Cons**: No Reputation

4chan

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

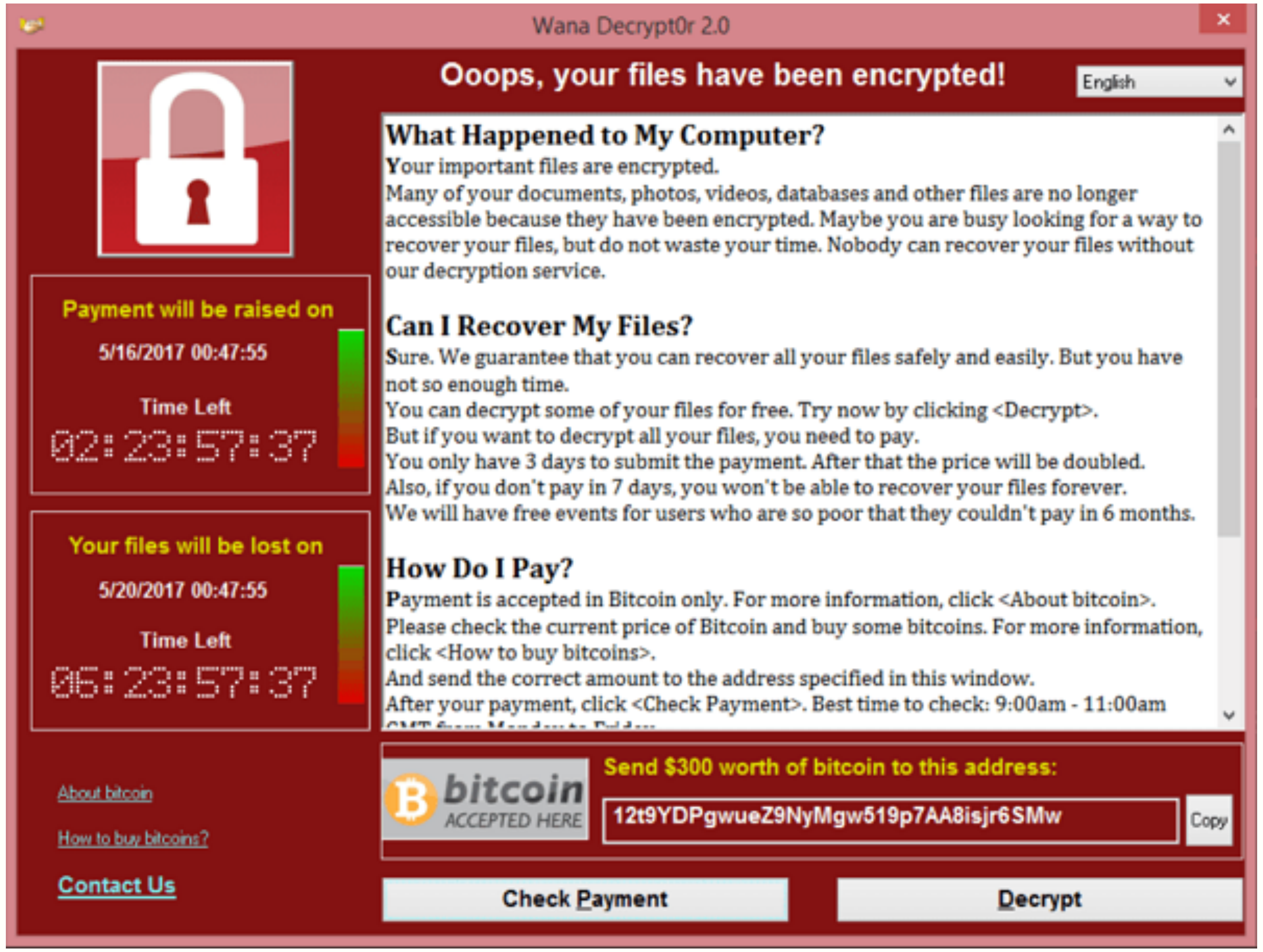
Consumers:

- Salary
- Rent
- Purchasing things online
- Donations

Who needs privacy for payments

Criminals (the followings are illegal!):

- Stealing funds (e.g., WannaCry ransomeware)
- Buying/selling drugs
- Tax evasion



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday

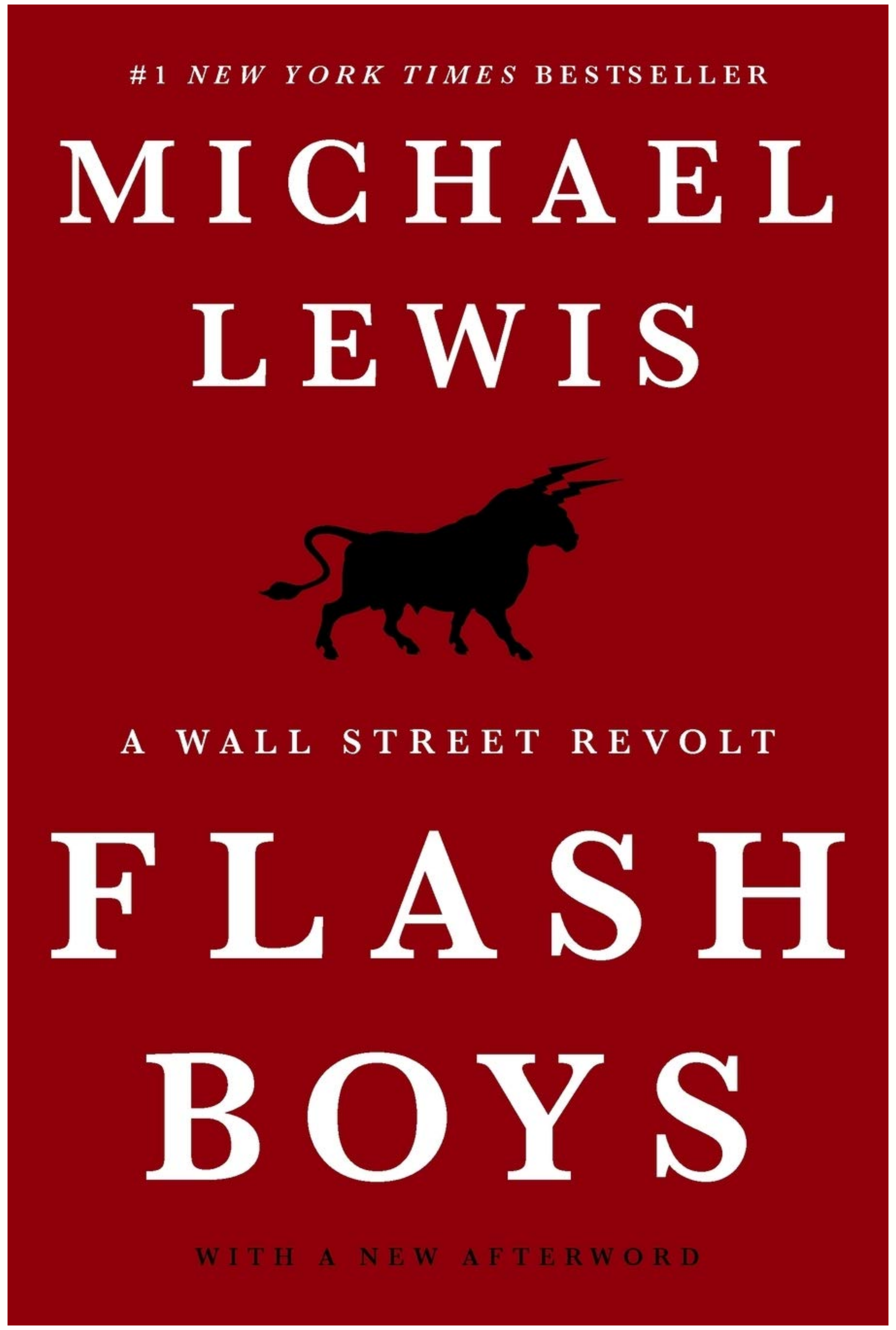
Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Who needs privacy for payments

Applications:

- Privacy can prevent front-running
- Exchanges may want to keep order book private
- Sealed bid auction



2 Privacy in existing systems?

Privacy of Digital Payments

Payments publicly visible/linkable

ethereum

Payments only visible to Venmo unless sender/receiver makes public

Unlinkable private payments

Zcash

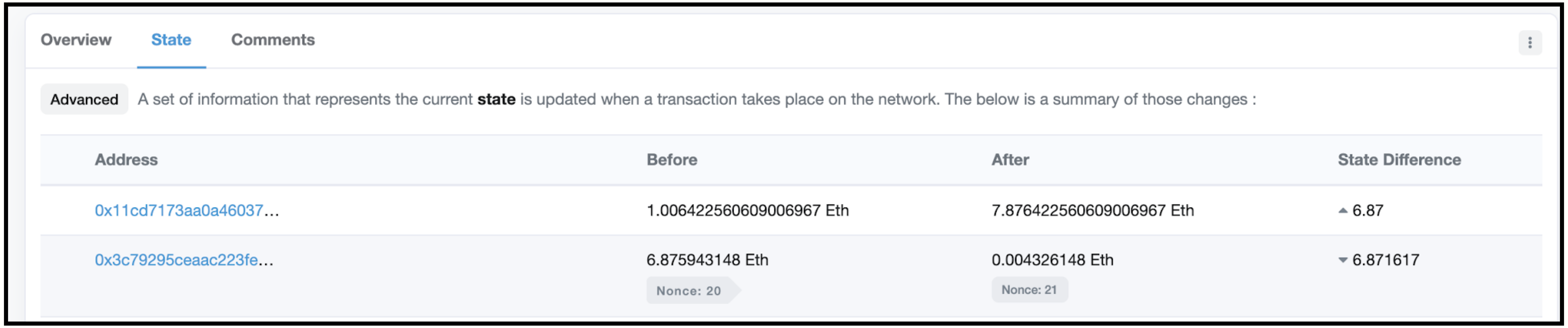
Less private

More private

Privacy in Ethereum

Weak Pseudonymity:

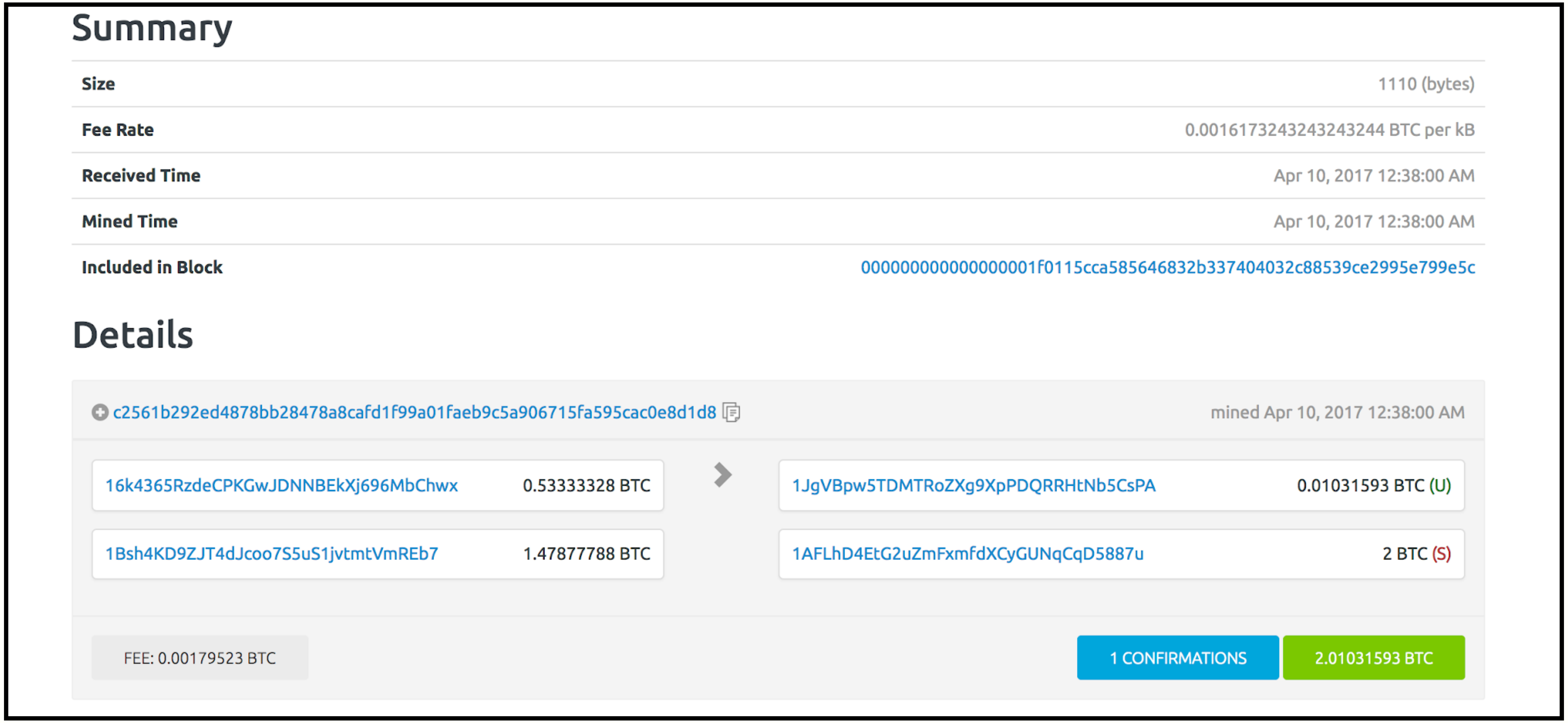
- Account public
- Values public
- Mostly one account per user
- Some accounts known (Binance)



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

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)

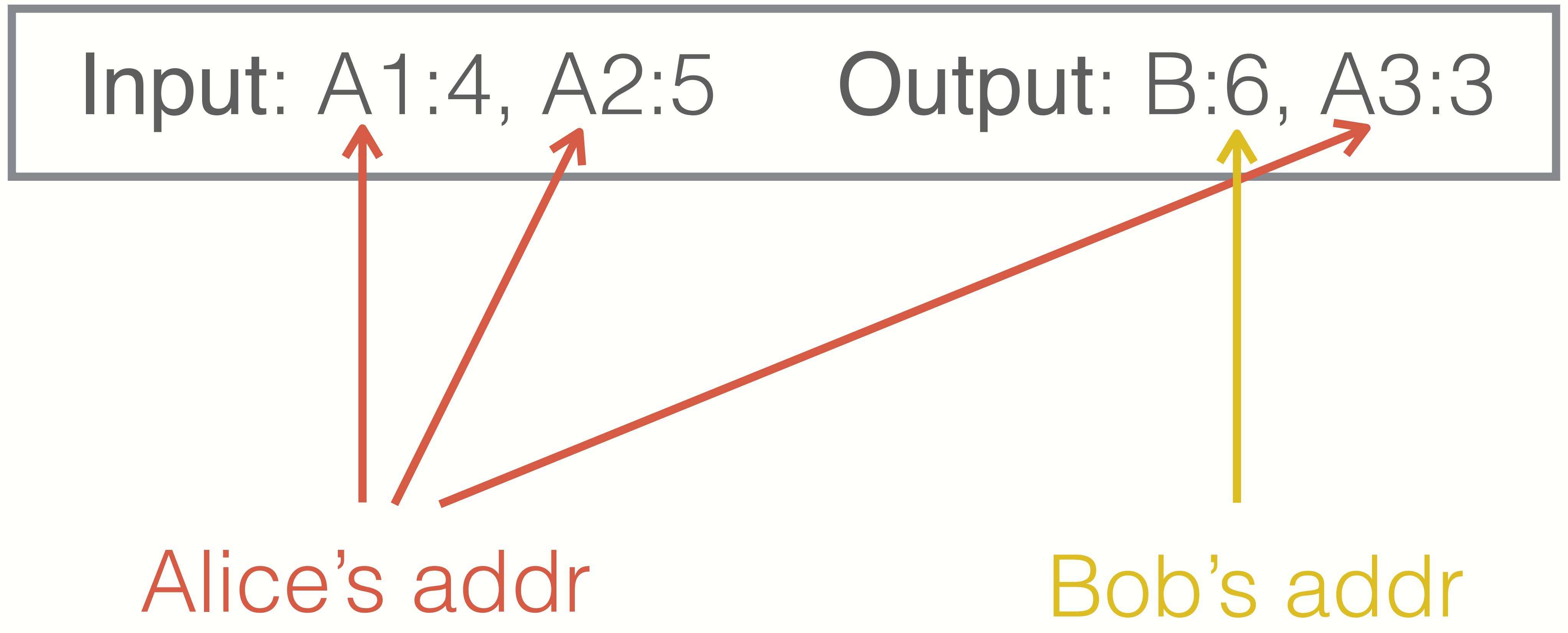
FEE: 0.00179523 BTC

1 CONFIRMATIONS

2.01031593 BTC

Privacy in Bitcoin

Alice can have many addresses (creating address is free)



Input: A1:4, A2:5 Output: B:6, A3:3

Alice's addr

Bob's addr

Privacy in Bitcoin

Input: A1:4, A2:5 **Output**: B:6, A3:3

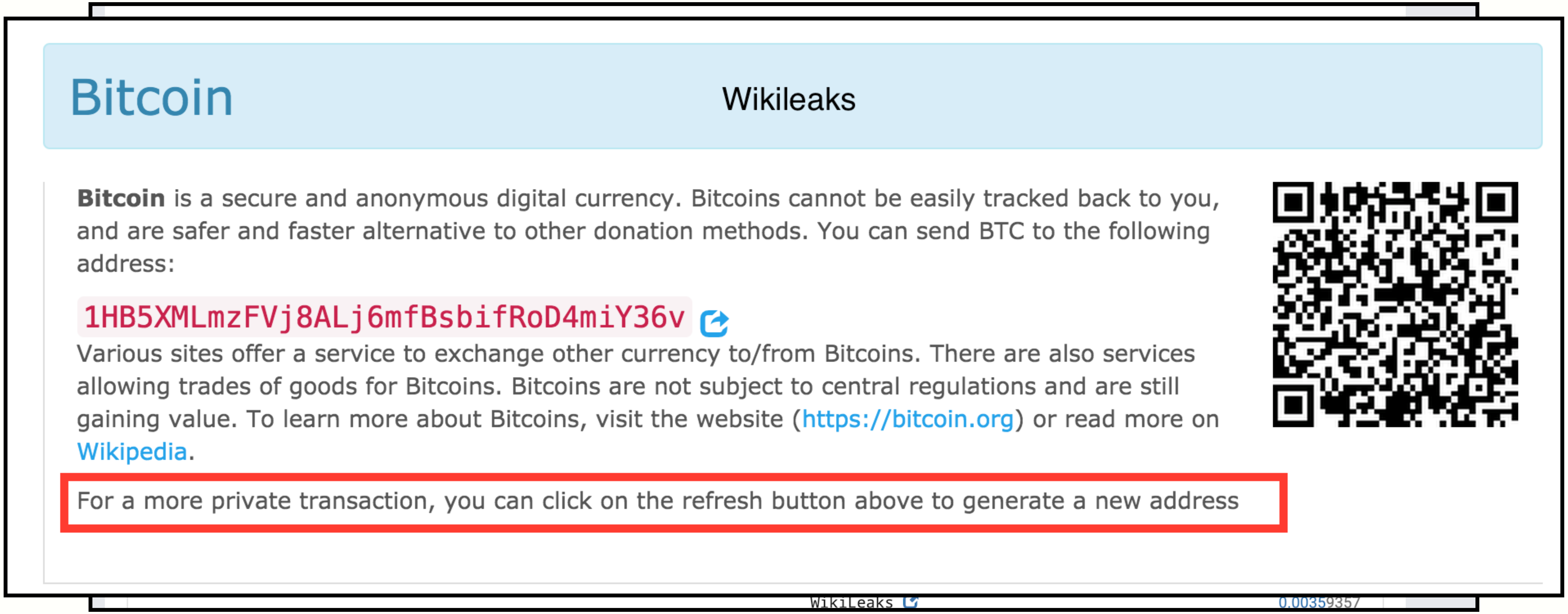
Buying book from merchant

- Alice learns one of merchant's addresses (B)
- Merchant learns three of Alice's addresses

Alice uses an exchange

- Money serving businesses often comply with KYC (Know Your Customer) standards
- So, they collect and verify real IDs
- Exchange learns real IDs

Donating to Wikileaks



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 0.00359357

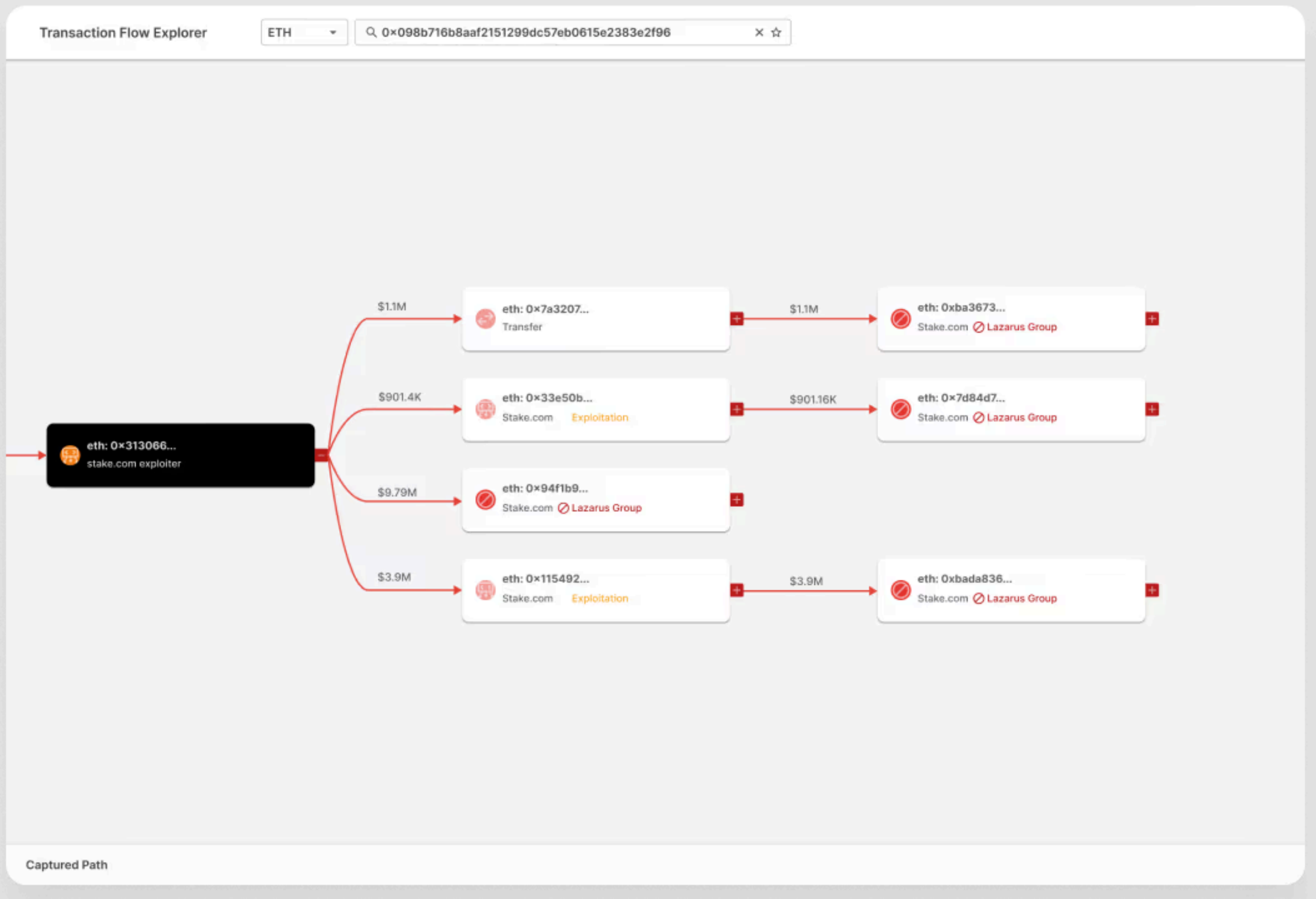
Is Bitcoin Anonymous?

NO!

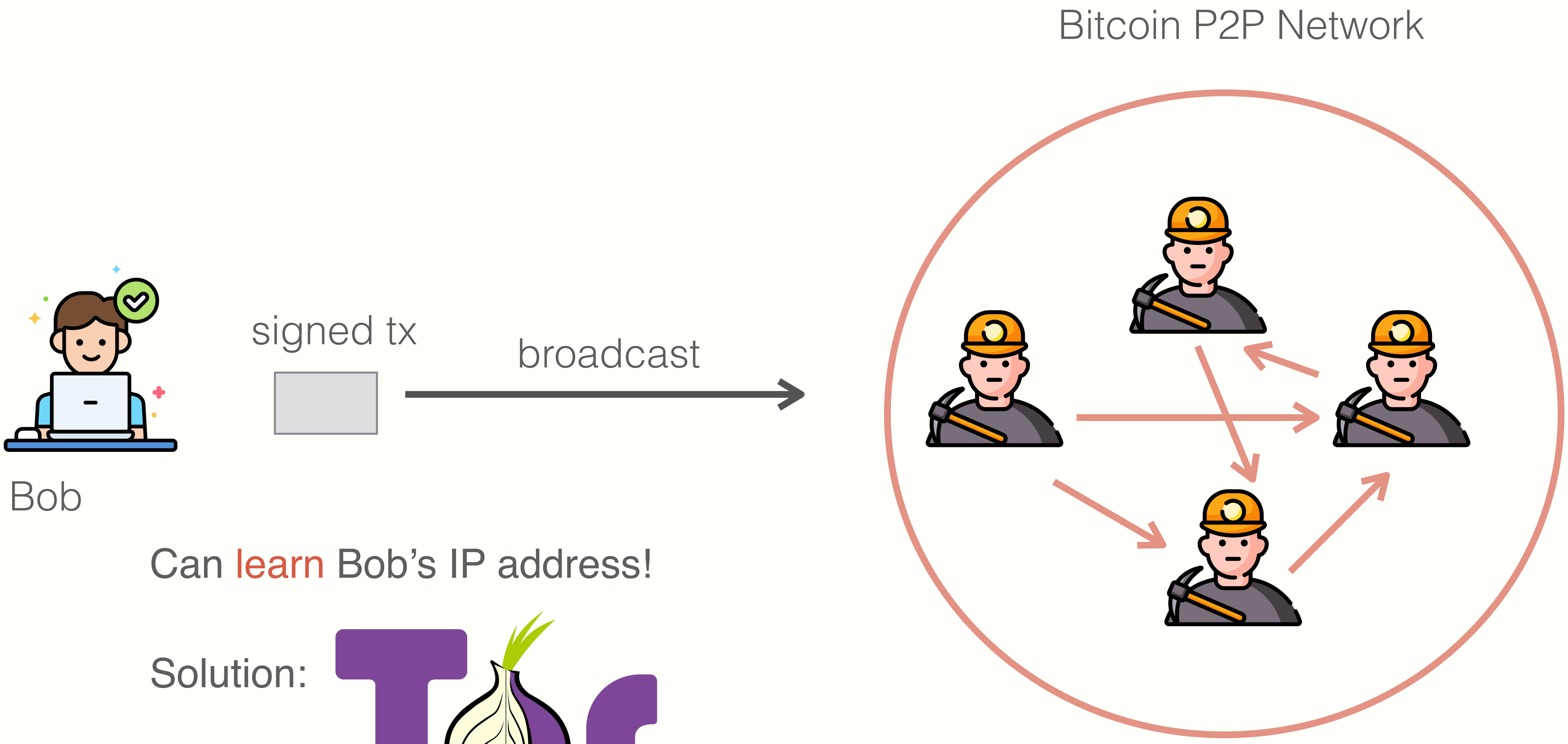
It is pos

- Link all
    - Can
- Given t
    - If D k
    - Can
    - Oppr
- Test if A

CertiK SkyInsights!



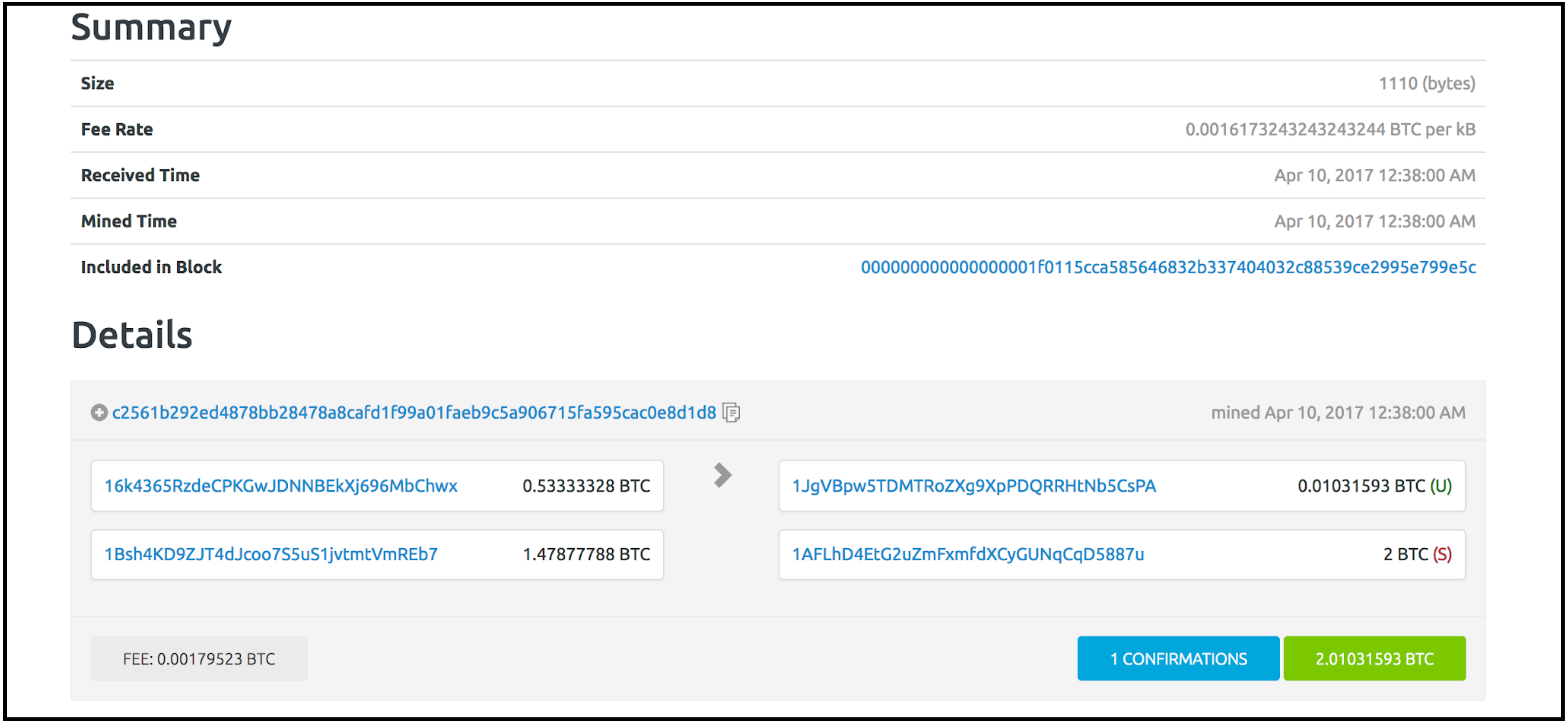
Network Anonymity



Can learn Bob’s IP address!

Solution: Tor

Idioms of use



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	000000000000000001f0115cca585646832b337404032c88539ce2995e799e5c

Details

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

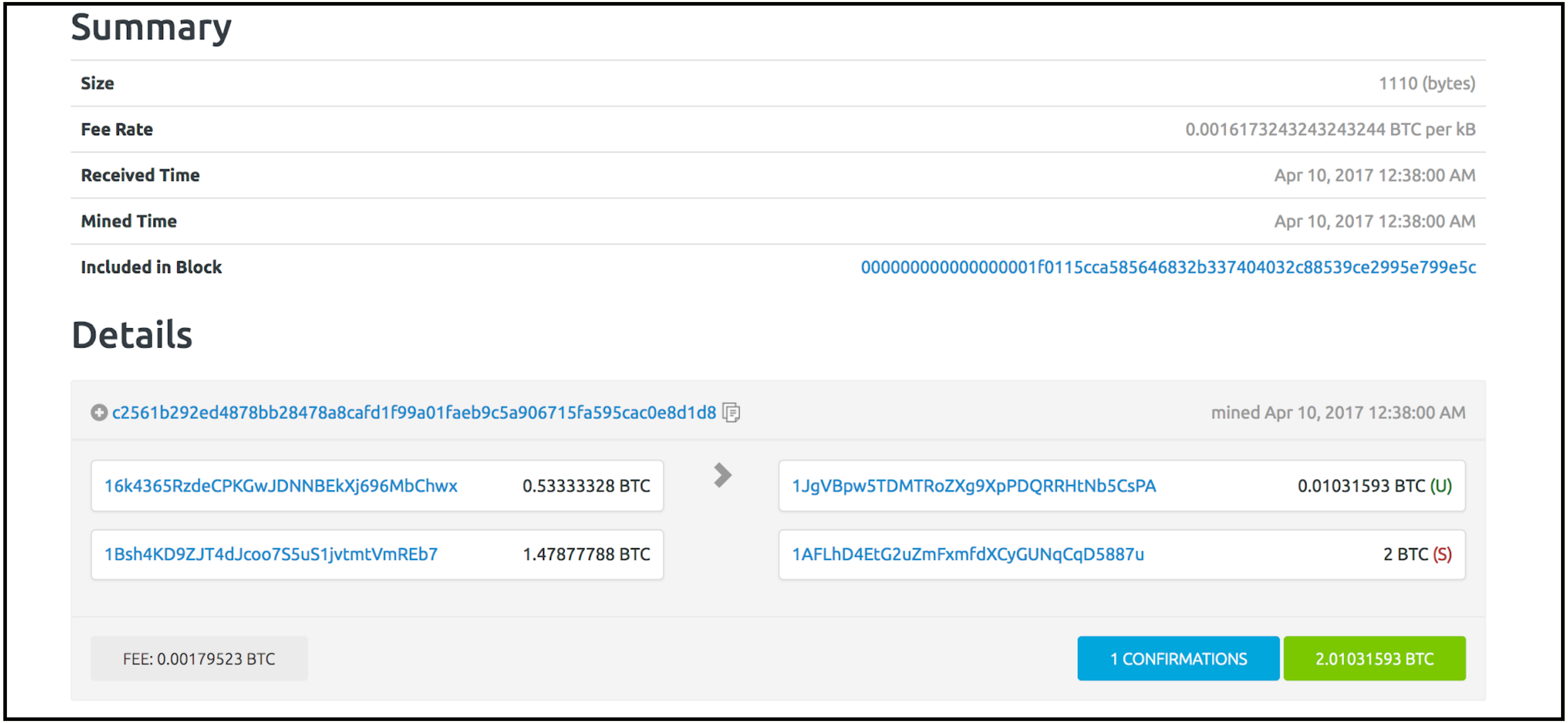
16k4365RzdeCPKGwJDNNBEkXj696MbChwx	0.53333328 BTC	›	1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA	0.01031593 BTC (U)
1Bsh4KD9ZJT4dJcoo7S5uS1jvtmtVmREb7	1.47877788 BTC		1AFLhD4EtG2uZmFxmfdXCyGUNqCqD5887u	2 BTC (S)

FEE: 0.00179523 BTC

1 CONFIRMATIONS

2.01031593 BTC

Idioms of use



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	00000000000000001f0115cca585646832b337404032c88539ce2995e799e5c

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

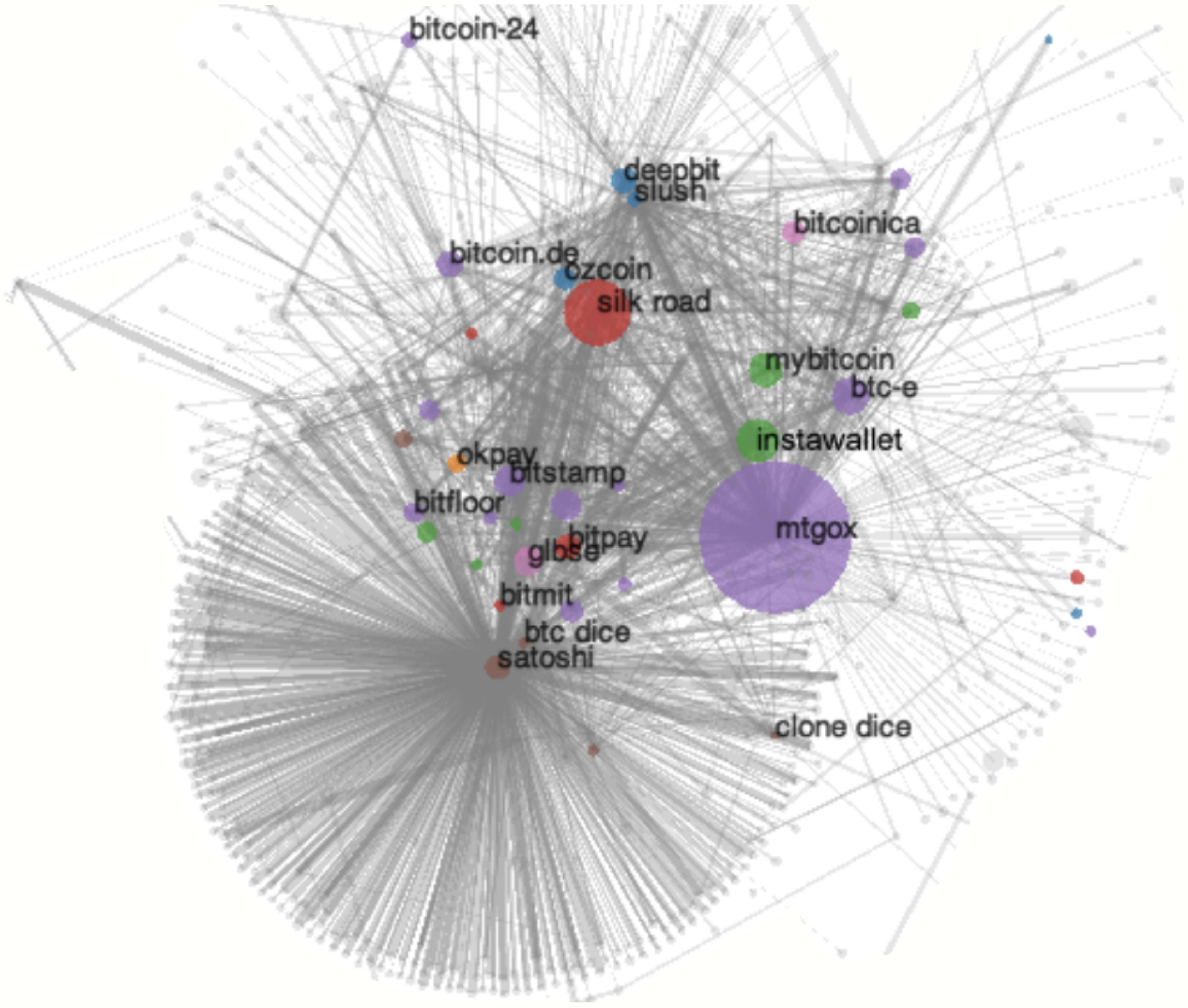
2.01031593 BTC

Experiment (2013)

Use Heuristic 1 and 2 —> discover 3.3M clusters

Learn ID of 2200 clusters

- 1.8M addresses
- 15% of total value
- Track multiple thefts
- Learn total assets for each cluster



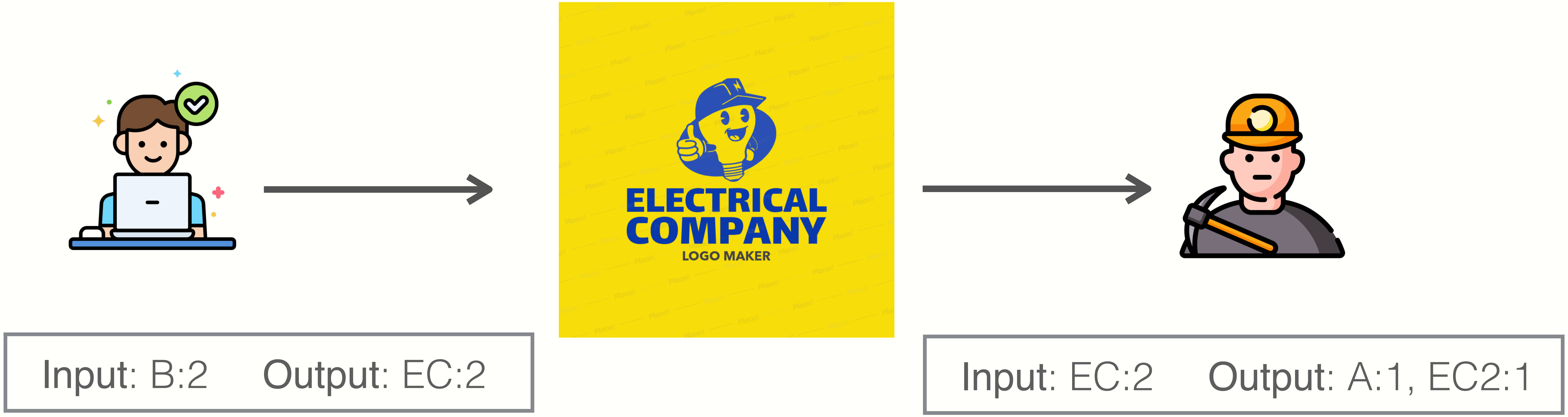
3 Anonymous Crypto?

Making Cryptocurrencies anonymous

Mixing

Anonymous
cryptocurrencies

Another example

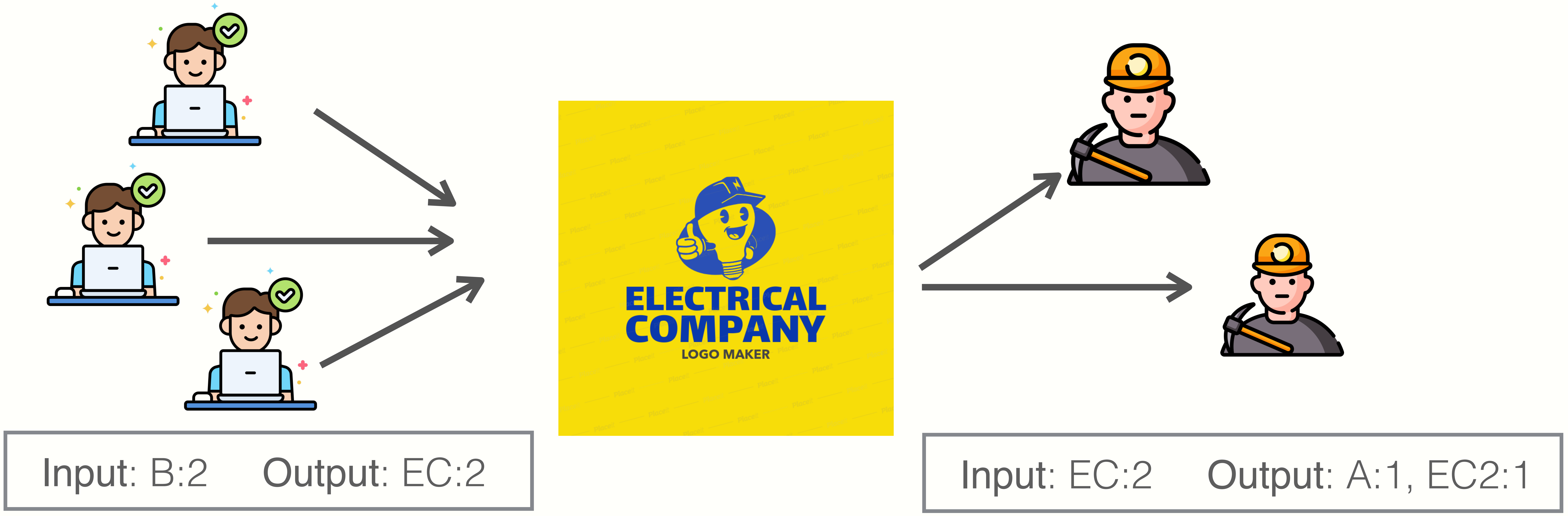


Input: B:2 **Output**: EC:2

Input: EC:2 **Output**: A:1, EC2:1

Bob and Subcontractor learn EC’s profit margin.
How can we prevent this?

Another example

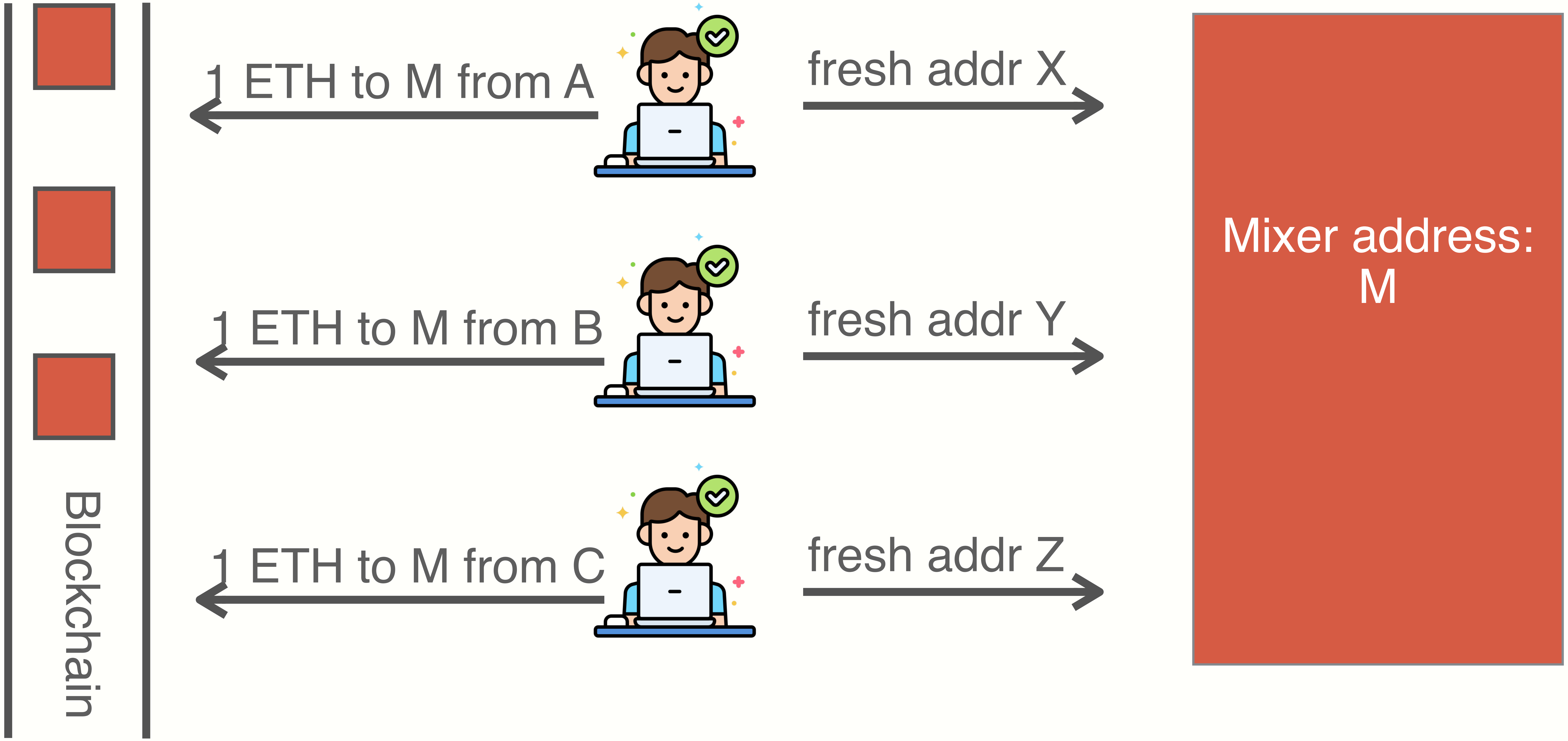


Input: B:2 Output: EC:2

Input: EC:2 Output: A:1, EC2:1

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

Simple blockchain anonymity via mixing



1 ETH to M from A

1 ETH to M from B

1 ETH to M from C

fresh addr X

fresh addr Y

fresh addr Z

Mixer address:
M

Blockchain

Input: M:3 Output: X:1, Y:1, Z:1

Mixing Analysis

Outside observer who is X?

- X must be A or B or C

For B?

- X must be A or C

The more participants the better mixing

Mixer Problems

- Mixer can deanonymize
- Mixer can steal funds
- Mixer takes transaction fees
- All outputs MUST have same value
  - If not you can match inputs and outputs

CoinJoin (Mixing without Mixer)

Input: A1: 5, B1: 3, C1:2
Output: B2: 2, A2: 2, C2: 2
Change: A3: 3, B3: 1

Signed: Multisig A1, B1, C1

CoinJoin (Mixing without Mixer)

- 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

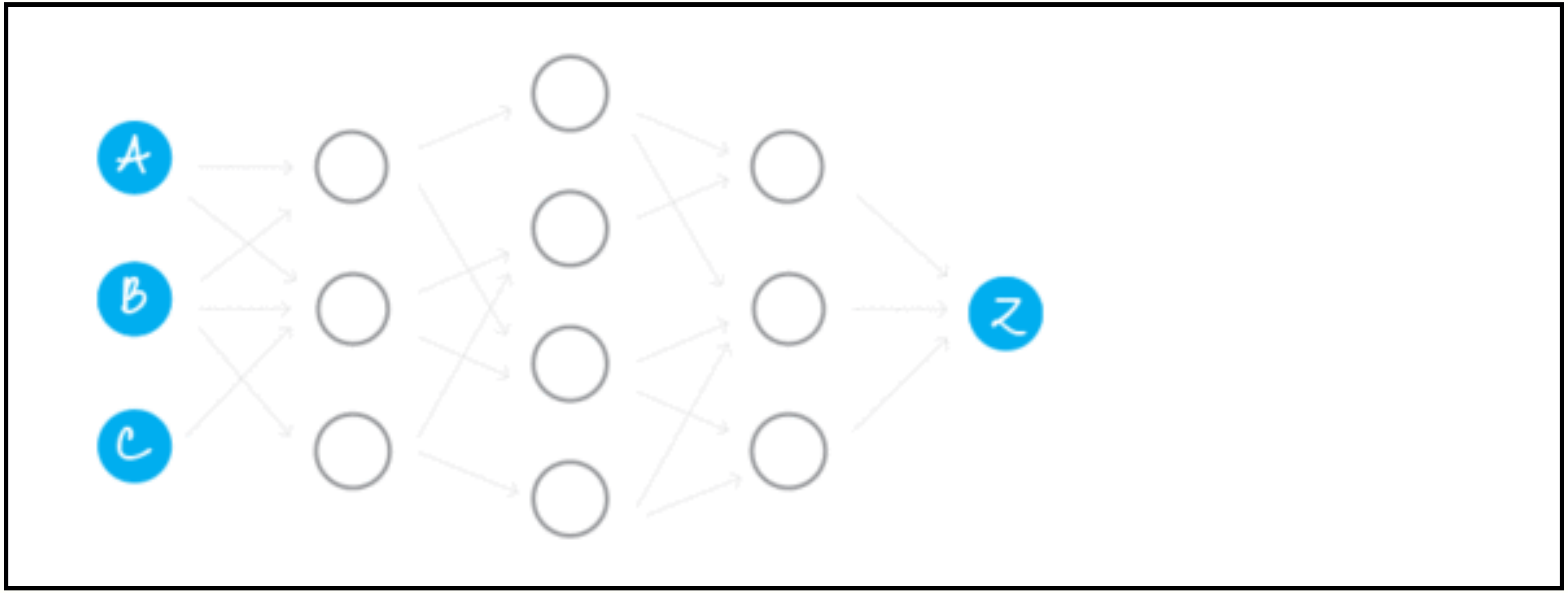
Def: a linkable ring signature scheme contains:

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

Secure signatures: (informal)

- Unforgettability, Anonymity, Linkability

Linkable Ring Signatures



Cryptonote (Monero)

- 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
  - That is, keys can only be used once
- Hides amounts (unlike coinjoin)
- Fully non interactive

4

Discussion Session

How to deal with failures?