

CS251 Fall 2020
(cs251.stanford.edu)

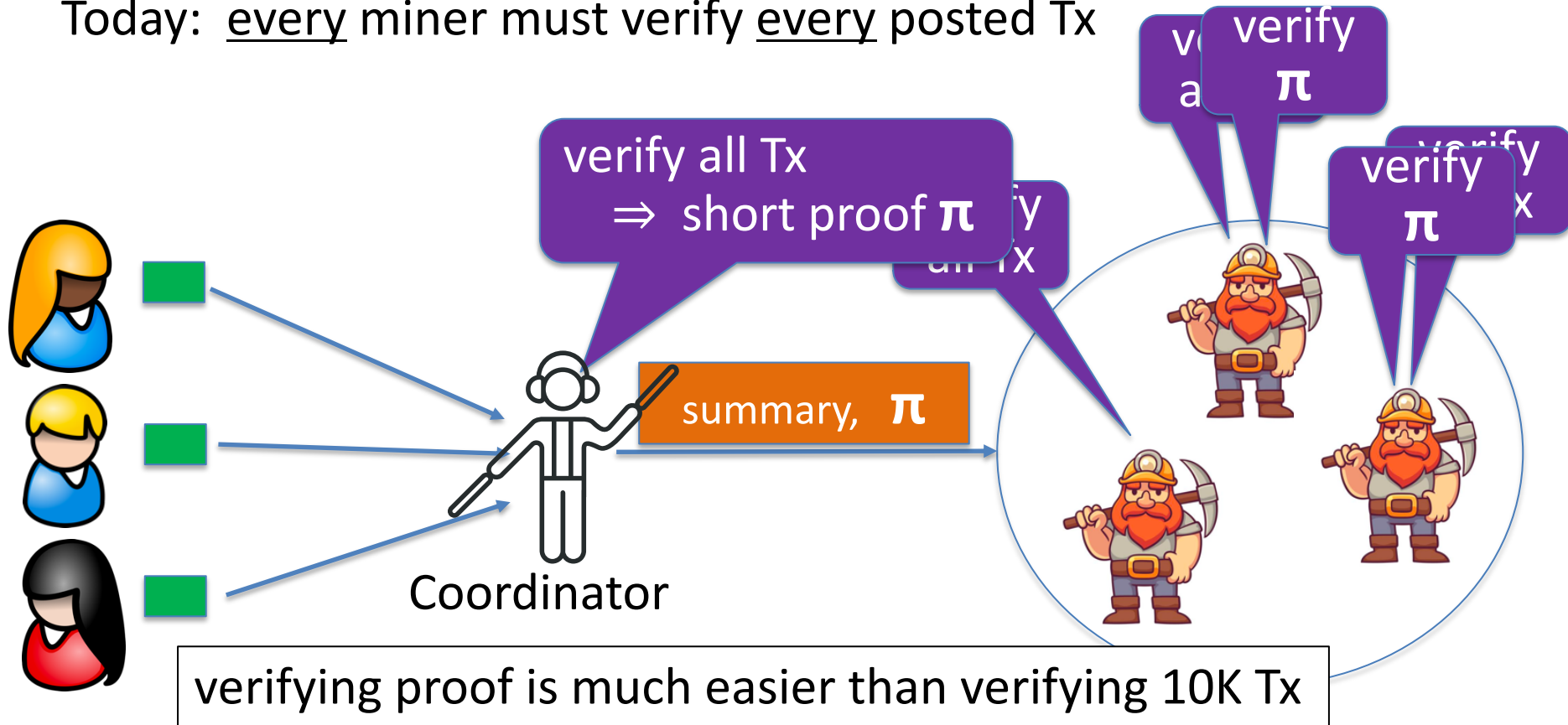


Rollup, Privacy and Mixers

Benedikt Bünz

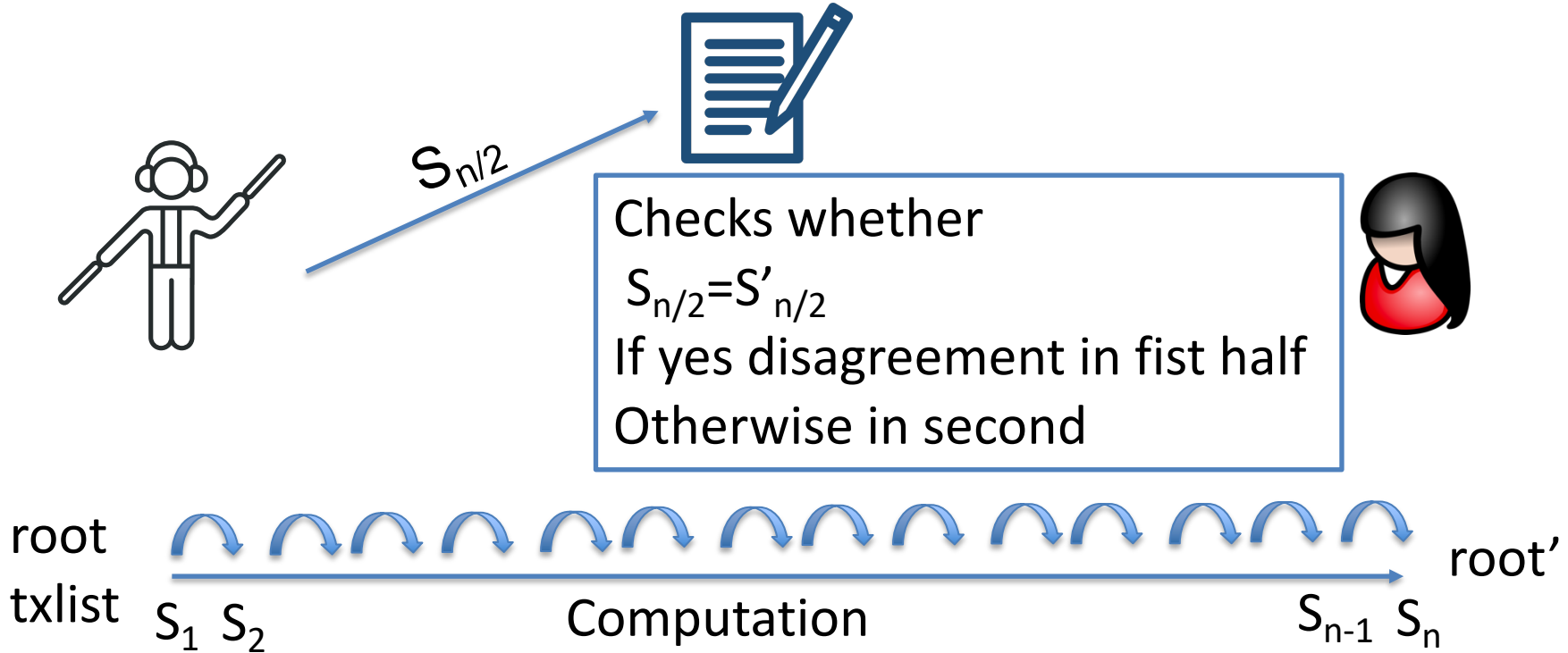
Recap: Rollup

Today: every miner must verify every posted Tx



Referee Delegation

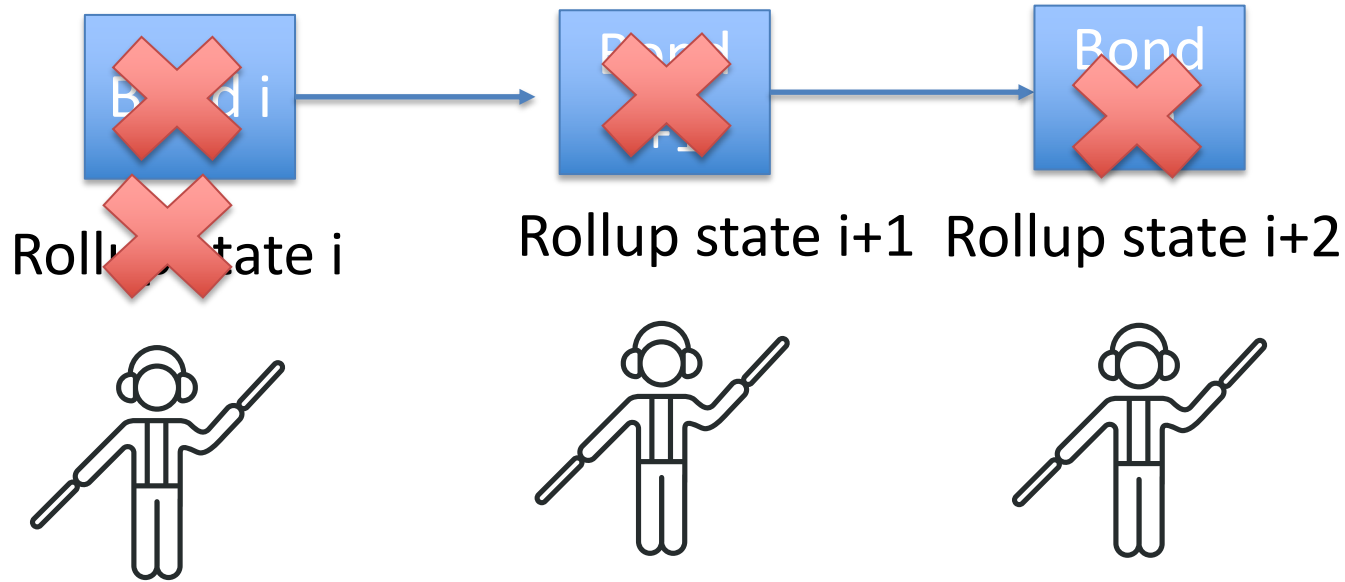
Coordinator and Validator run interactive binary search



Problem: Checks take a long time

- $\log_2(n)$ messages (1 hash per message)
- 1 Verification step on smart contract
- If either party timeouts declares winner
- Looser gets *slashed*, Winner rewarded
- Problem: $\log_2(n) * \text{timeout}$
- No incentive to cheat
- But: Long wait till finalization!

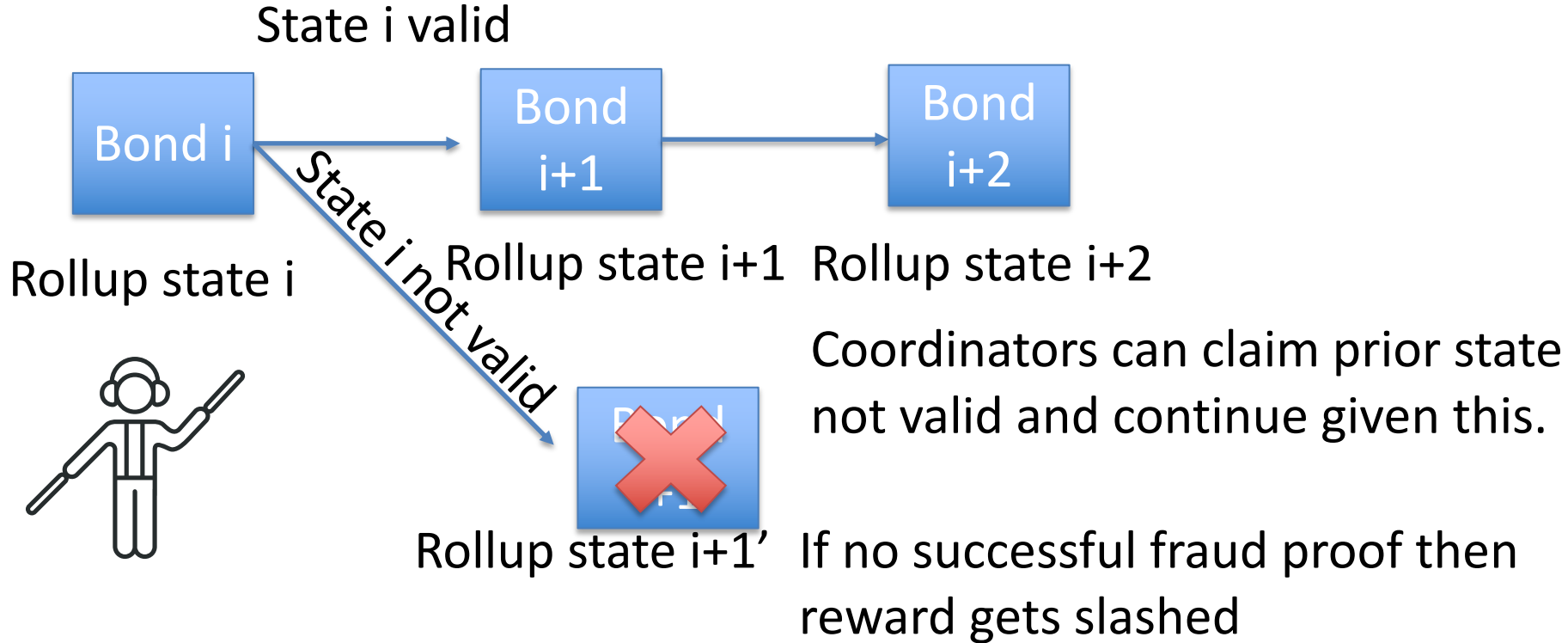
Pipelined Assertions



Coordinators can build on
states before timeouts

If prior state invalid, all
subsequent bonds are slashed

Pipelined Assertions



Multiple Rollup Coordinators

- Rollup coordinator (in either scheme) is not trusted for security
- It can reasonably be a single coordinator
- But it is trusted for liveness
 - Censorship resistance
 - Progress of rollup state
- Multiple Coordinators?

Multiple Rollup Coordinators

- Rotating coordinators
- Random coordinator (using Beacon)
- Race to submit new rollup state (usually same party wins)
- One solution is using classical consensus between fixed set of coordinators
 - At least $2/3^{\text{rd}}$ of coordinators sign roll up
 - If trusted instant finality

Multi Coordinator Insurance

- Get insurance signature from $2/3^{\text{rd}}$ of coordinators
- If next block does not include transaction post signature
- Slash reward from intersection of insurer and rollup block signers
 - At least $1/3^{\text{rd}}$ of the coordinators

Comparison SNARK vs Optimistic Rollup

Optimistic Rollup

- Higher TPS
- Arbitrary Smart complex
- Slow finality (hours/days)
- Instant finality with insurance
- Trust that someone verifies

zkRollup

- Lower TPS
- Only simple transfers
- Faster Finality (minutes)
- Instant finality with insurance
- No trust required

Privacy

Privacy for Cryptocurrencies

What information might a user want to hide?

Identity (anonymity):

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

Metadata:

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

Amounts:

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

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

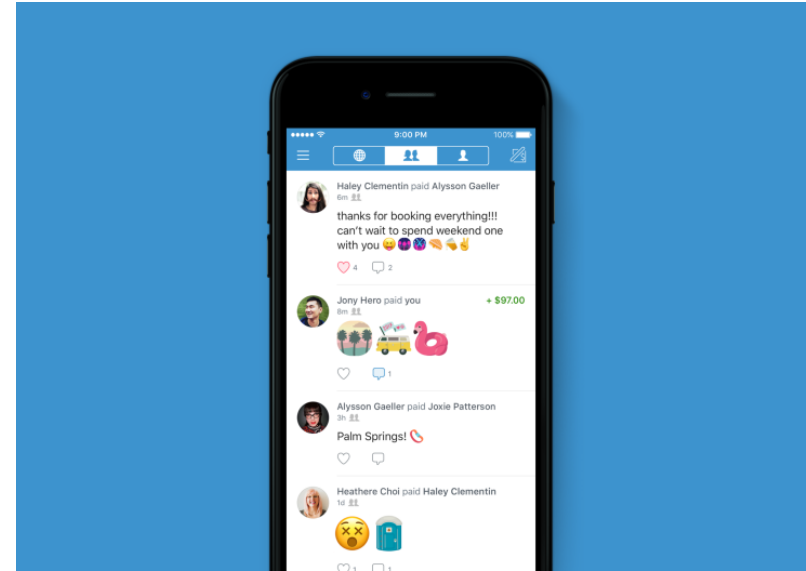
Hedge funds want to keep investments private



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



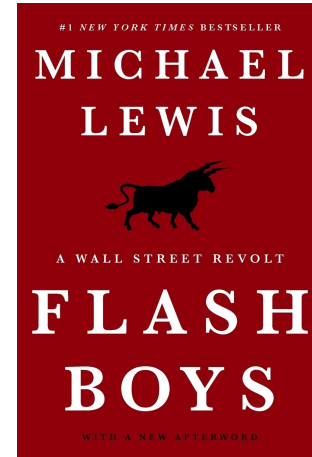
Who needs privacy for payments

- Applications

Privacy can prevent frontrunning

Exchanges may want to keep orderbook private

Sealed bid auction



Privacy of Digital Payments

Payments publicly
visible/linkable

libra



ethereum



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



Unlinkable private payments



Zcash



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	0.004326148 Eth	▼ 6.871617
	Nonce: 20	Nonce: 21	

Overview

Balance:

7.876422560609006967 Ether

Ether Value:

\$3,049.75 @ 3947.14ETH

Token:

More Info

My Name Tag:

Not Available, [login to update](#)

Transactions

Erc20 Token Trans

Loans

Analytics

Comments

12 Latest 12 from a total of 12 transactions

Txn Hash	Block	Age	From	To	Value	[Txn Fee]
0x8be7ca958872ed2d...	11146179	1 min ago	0x3c79295ceaac223fe...	0x11cd7173aa0a46037...	6.87 Ether	0.001917
0x9851938d01342015...	11146119	12 mins ago	0x11cd7173aa0a46037...	0x52d41ace9554ac8b...	0 Ether	0.000191250079
0x7264112d1d1776390...	11146111	14 mins ago	0x11cd7173aa0a46037...	0x3d0d90d71218a6c3...	1.05 Ether	0.00091493003
0x73ad35d4cd42a7a...	11146026	34 mins ago	0x11cd7173aa0a46037...	0x52d41ace9554ac8b...	0 Ether	0.000911980079
0x0a4d4a41d59f84...	11146018	35 mins ago	0x11cd7173aa0a46037...	0x285d121d1e3e4e3f...	1.05 Ether	0.00090200003
0x81263420c7984ab...	11117274	4 days 10 hrs ago	0x11cd7173aa0a46037...	0x52d41ace9554ac8b...	0 Ether	0.00114300079
0x033c8d4d1b79c96...	11117263	4 days 10 hrs ago	0x11cd7173aa0a46037...	0x3f099f18eab32e72...	1.05 Ether	0.00044100003
0x443328c0a850462d...	11117246	4 days 10 hrs ago	0x11cd7173aa0a46037...	0x3e6b7b30c120b4...	5 Ether	0.00090700003
0x3e4863c22c2d962...	11116663	4 days 12 hrs ago	0x11cd7173aa0a46037...	0x5b70984355a70bc...	1.15 Ether	0.00037000003
0x0a6060e17e4d891c...	11104115	6 days 10 hrs ago	0x686832bc122940b6...	0x11cd7173aa0a46037...	10.2520728 Ether	0.001134
0x0a4f664c56d7837...	11104062	6 days 11 hrs ago	0x11cd7173aa0a46037...	0x52d41ace9554ac8b...	1 Ether	0.013871387
0x103c3a1b432415b2...	11104034	6 days 11 hrs ago	Binance	0x11cd7173aa0a46037...	1.095 Ether	0.00126

Weak Pseudonymity

Account public

Values public

Mostly one account per user

Some accounts known (Binance)

Summary

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)

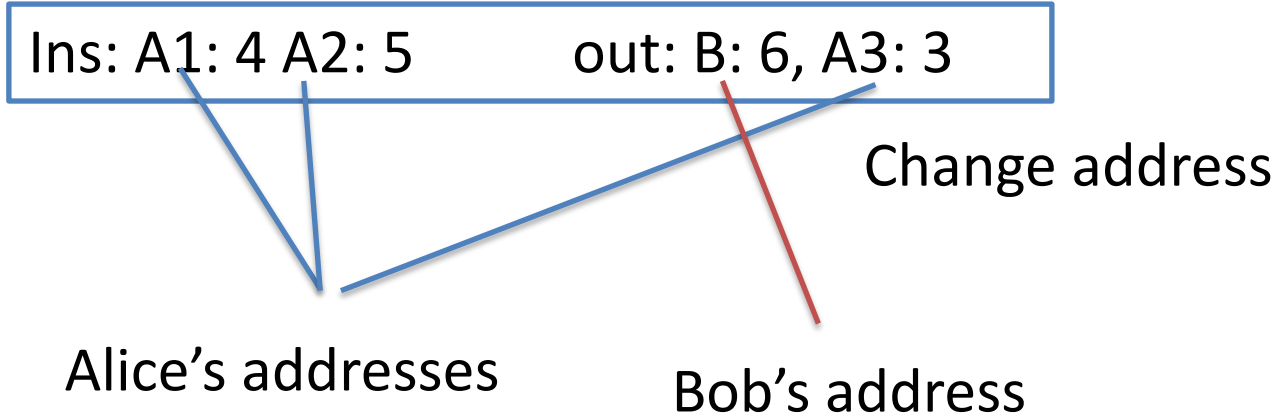
Ins: A1: 4 A2: 5

out: B: 6, A3: 3

Change address

Alice's addresses

Bob's address



Linking Addresses to Identities

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

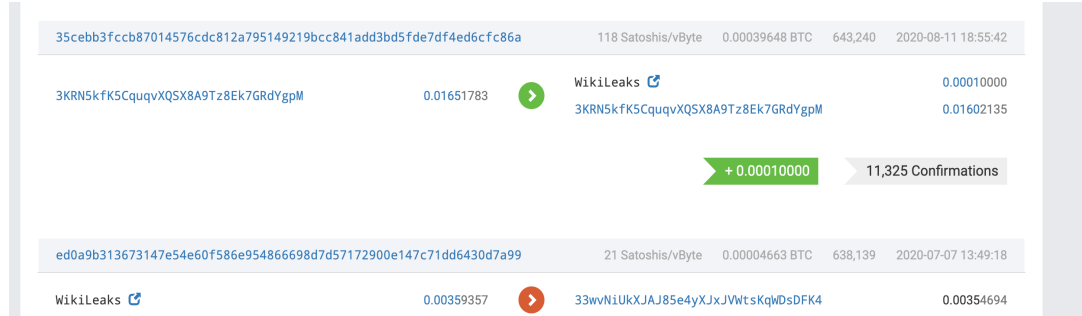
- Buying book from merchant
 - Alice learns one of merchant's addresses (B)
 - Merchant learns three of Alice's addresses
- Alice uses an exchange BTC $\leftrightarrow$ \$
 - KYC (Know your customer)
 - Money serving business collect and verify IDs

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 $\leftrightarrow$ \$
 - KYC (Know your customer)
 - Money serving business collect and verify IDs
 - Exchange learns real ID

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 had one address -> Easy to see who donates

Is Bitcoin Anonymous?

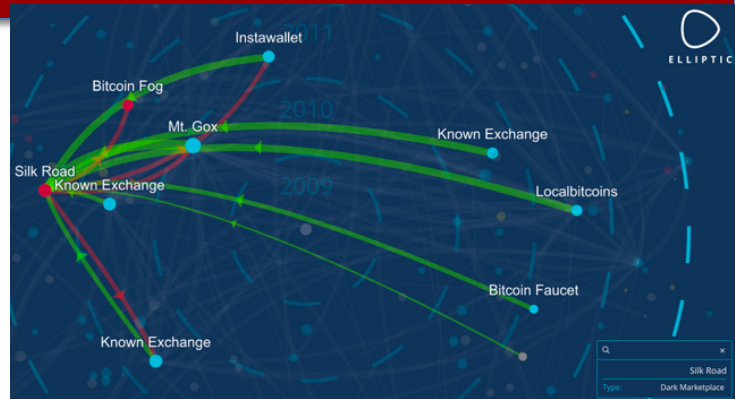
No!

Now commercialized:

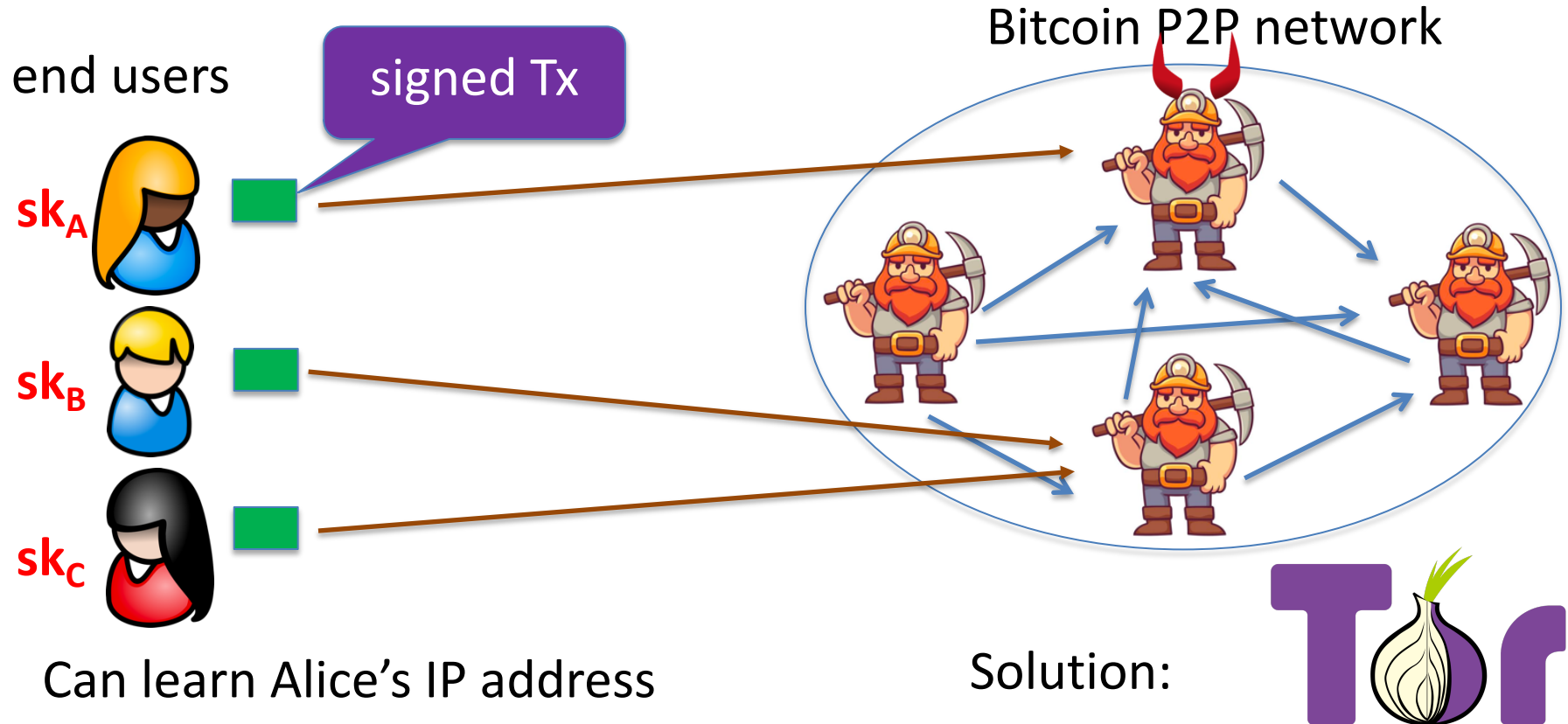
It is possible to:

- Link all addresses of a single entity:
 - Determine total assets
- Given two TX $A \rightarrow B$, $C \rightarrow D$, 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



Light client network anonymity

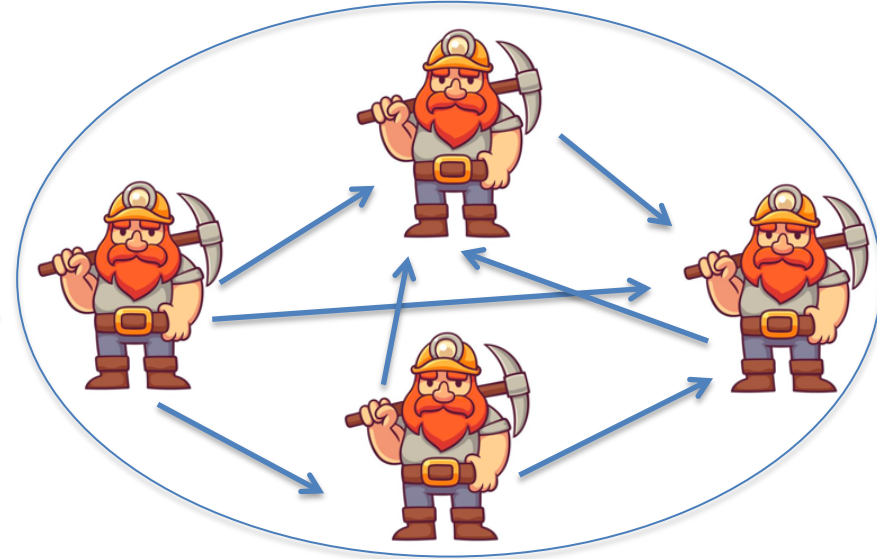
SPV client



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

Transaction ID: [c2561b292ed4878bb28478a8cafd1f99a01faeb9c5a906715fa595cac0e8d1d8](#) mined Apr 10, 2017 12:38:00 AM

Address	Amount (BTC)
16k4365RzdeCPKGwJDNNBEkXj696MbChwx	0.53333328 BTC
1Bsh4KD9ZJT4dJcoo7S5uS1jvtmtVmREb7	1.47877788 BTC
1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA	0.01031593 BTC (U)
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

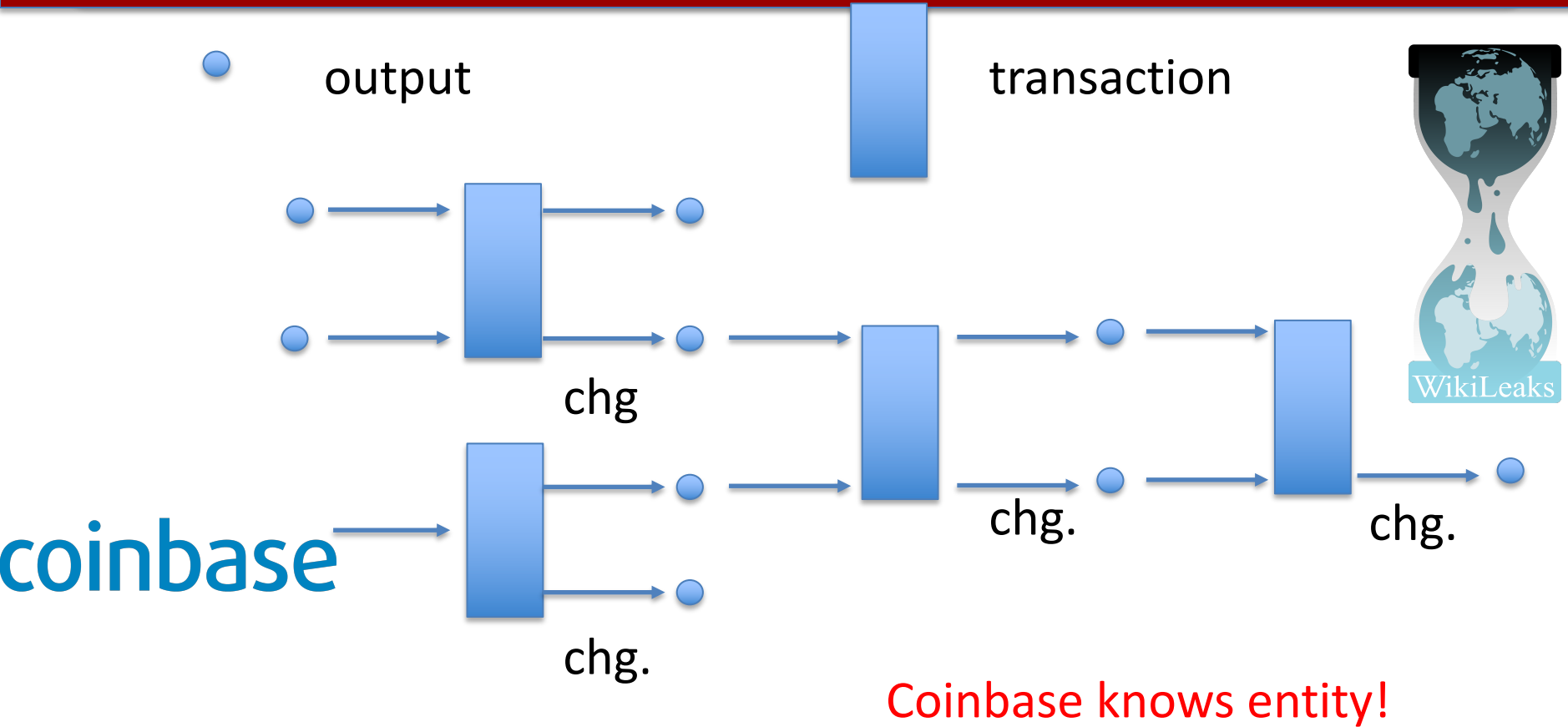
The screenshot displays a Bitcoin transaction interface. At the top, a transaction ID is shown: `c2561b292ed4878bb28478a8cafd1f99a01faeb9c5a906715fa595cac0e8d1d8`, with a timestamp "mined Apr 10, 2017 12:38:00 AM". Below this, the transaction details are organized into two columns separated by a right-pointing arrow. The left column lists two input addresses: `16k4365RzdeCPKGwJDNNBEkXj696MbChwx` (0.53333328 BTC) and `1Bsh4KD9ZJT4dJcoo7S5SuS1jvtmtVmREb7` (1.47877788 BTC). The right column lists two output addresses: `1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA` (0.01031593 BTC (U)) and `1AFLhD4EtG2uZmFxmfdXCyGUNqCqD5887u` (2 BTC (S)). At the bottom left, the fee is shown as "FEE: 0.00179523 BTC". At the bottom right, there are two buttons: "1 CONFIRMATIONS" in blue and "2.01031593 BTC" in green.

Address	Amount (BTC)
<code>16k4365RzdeCPKGwJDNNBEkXj696MbChwx</code>	0.53333328
<code>1Bsh4KD9ZJT4dJcoo7S5SuS1jvtmtVmREb7</code>	1.47877788
<code>1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA</code>	0.01031593 (U)
<code>1AFLhD4EtG2uZmFxmfdXCyGUNqCqD5887u</code>	2 (S)

FEE: 0.00179523 BTC

1 CONFIRMATIONS 2.01031593 BTC

Example tracing



Experiment (2013)

- Use Heuristic 1 and 2 -> 3.3M clusters
- ID 1070 addresses 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

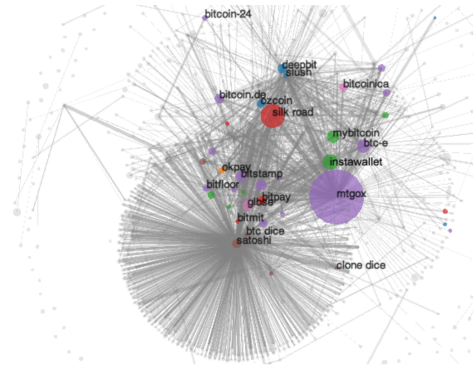
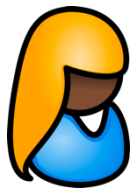


Figure 6: A visualization of the user network. The area of the cluster represents the external income value: i.e., the bitcoins received from

Another example

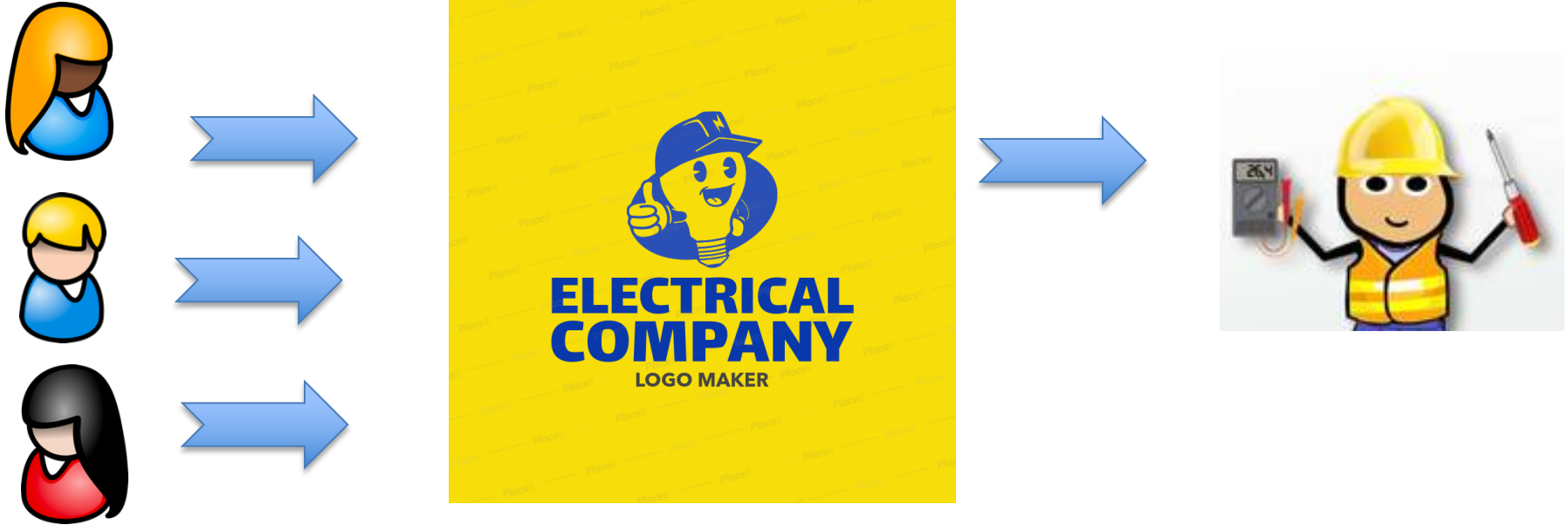


Ins: A1: 1. out: EC1 1

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

Making Cryptocurrencies anonymous



Mixing



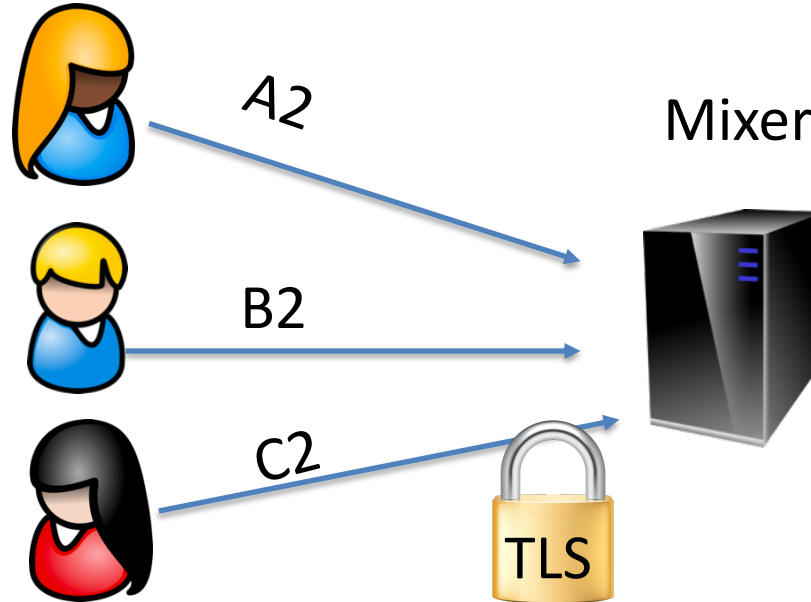
Anonymous cryptocurrencies

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)



Same



Add Signatures



Online Forum



A1: 5, A3

B1: 3, B3

C1: 2, C3

B2, A2, C2

Publish Transaction

What if A1 is spent?

END OF LECTURE

Next lecture:

Zero-knowledge SNARKs