CS251 Fall 2020

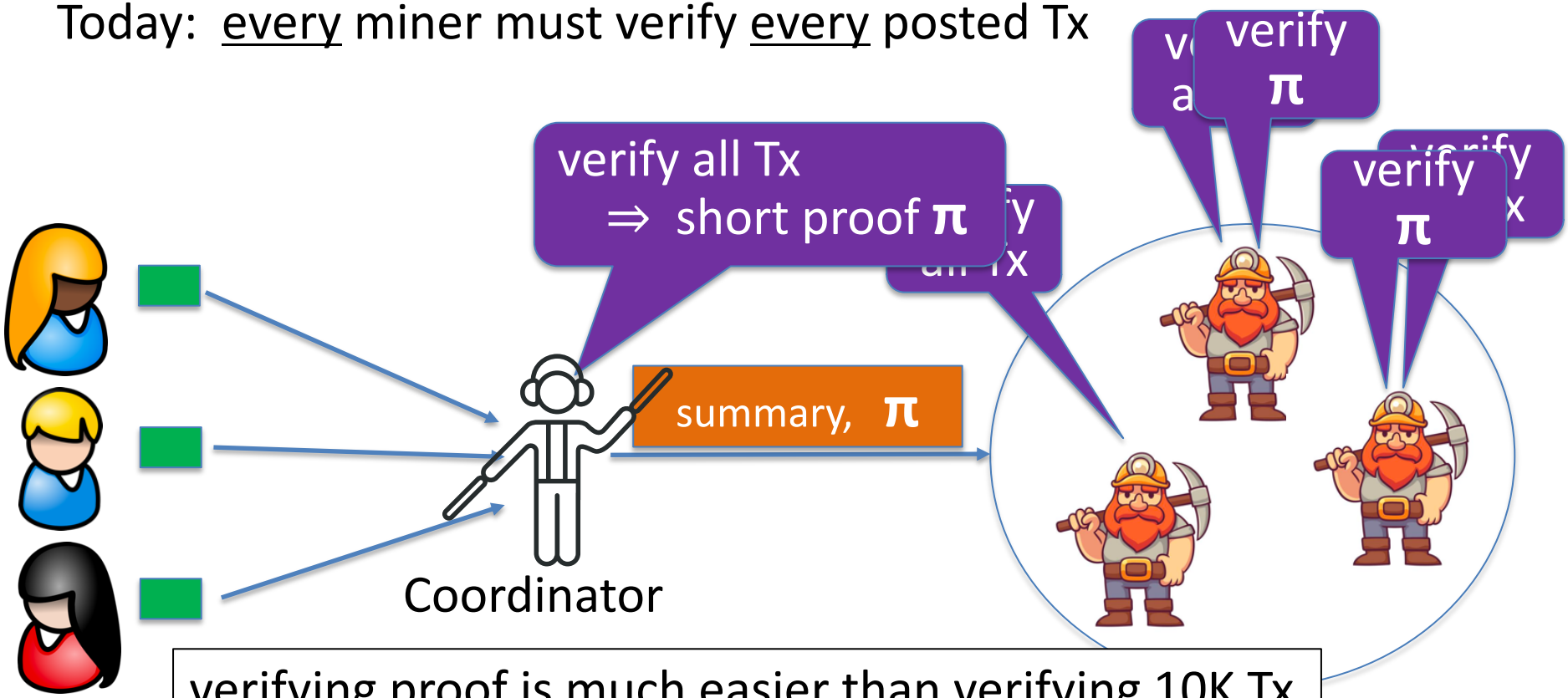
(cs251.stanford.edu)

Rollup, Privacy and Mixers

Benedikt Bünz

Recap: Rollup

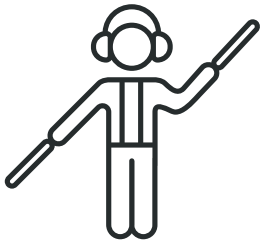
Today: <u>every</u> miner must verify <u>every</u> posted Tx



verifying proof is much easier than verifying 10K Tx

Referee Delegation

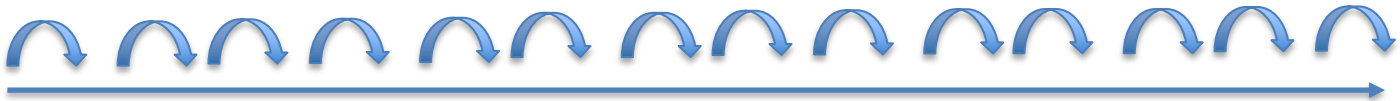
Coordinator and Validator run interactive binary search



$S_{n/2}$

Checks whether
$S_{n/2}=S'_{n/2}$
If yes disagreement in fist half
Otherwise in second

root
txlist



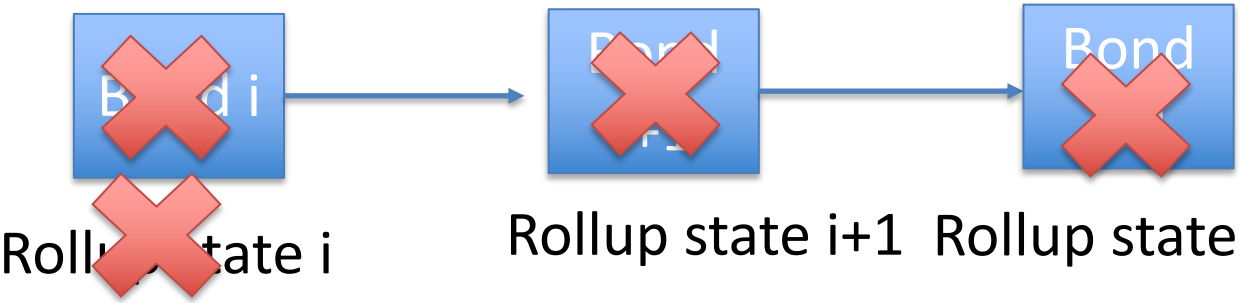
S_1 S_2 Computation S_{n-1} S_n

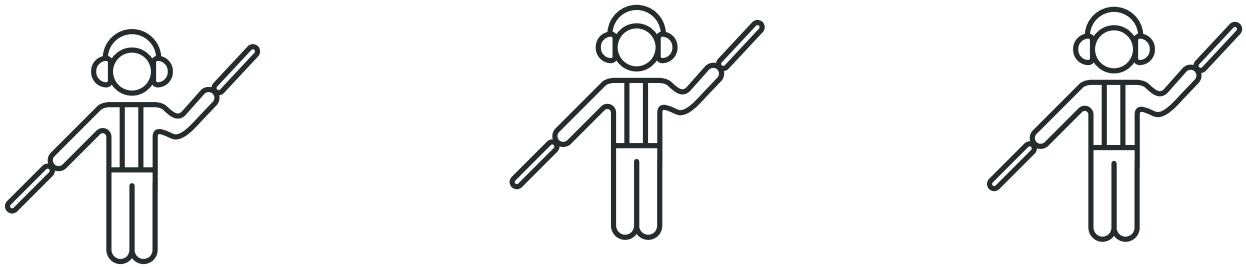
root'

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: $\log_2(n)$*timeout
- No incentive to cheat
- But: Long wait till finalization!

Pipelined Assertions

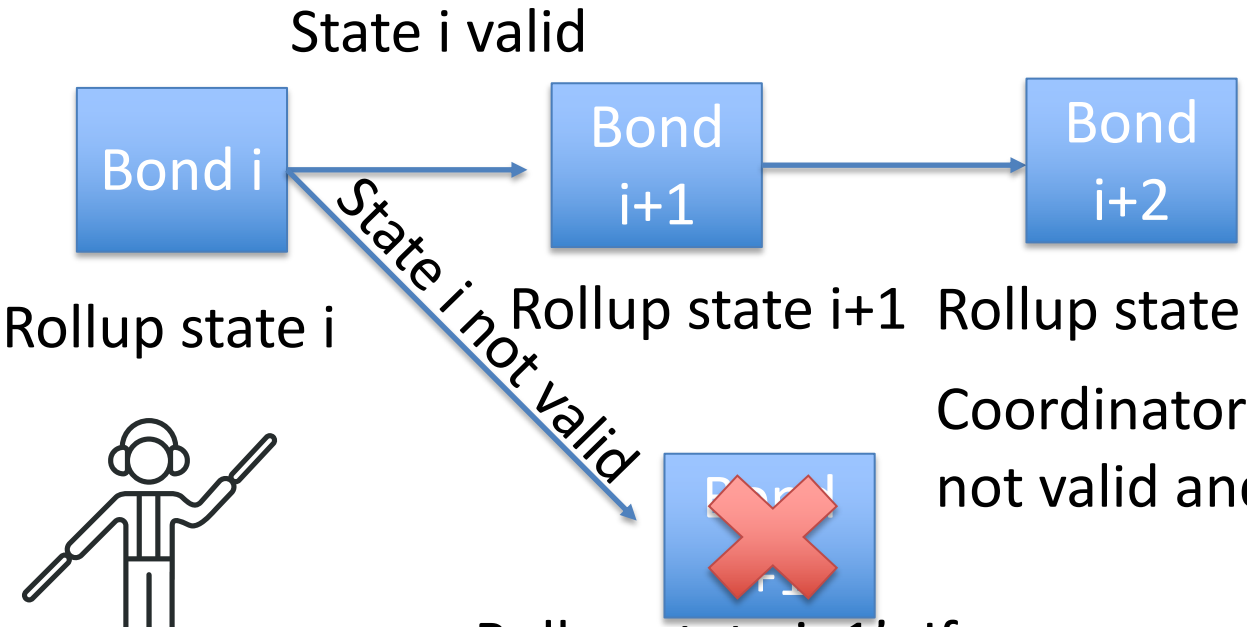




Coordinators can build on states before timeouts

If prior state invalid, all subsequent bonds are slashed

Pipelined Assertions



Coordinators can claim prior state not valid and continue given this.

If no successful fraud proof then reward gets slashed

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 2/3rd of coordinators sign roll up
  - If trusted instant finality

Multi Coordinator Insurance

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

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

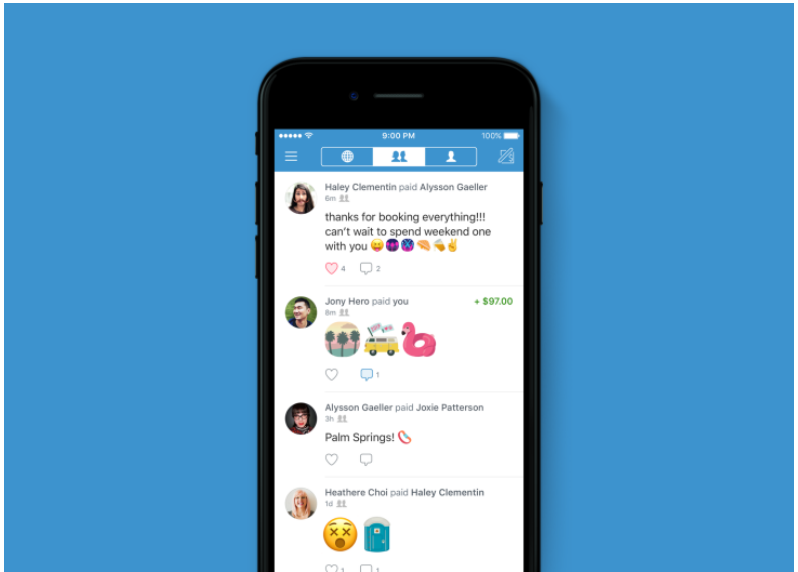
Hedge funds want to keep investments private

Who needs privacy for payments

Consumers

Salary, Rent, Purchasing things online, Donations

Planned Parenthood®



Who needs privacy for payments

- Criminals

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

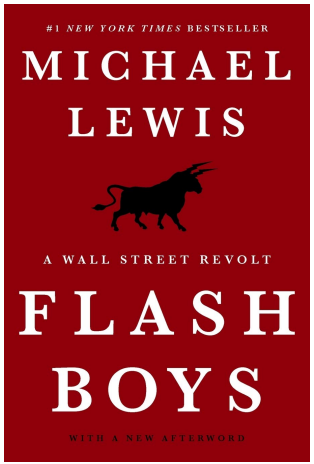
Who needs privacy for payments

- 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

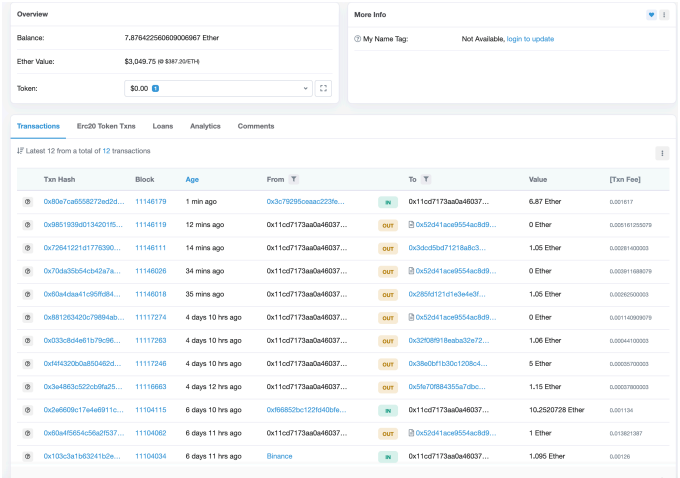
More private

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 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	000000000000000001f0115cca585646832b337404032c88539ce2995e799e5c

Details

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

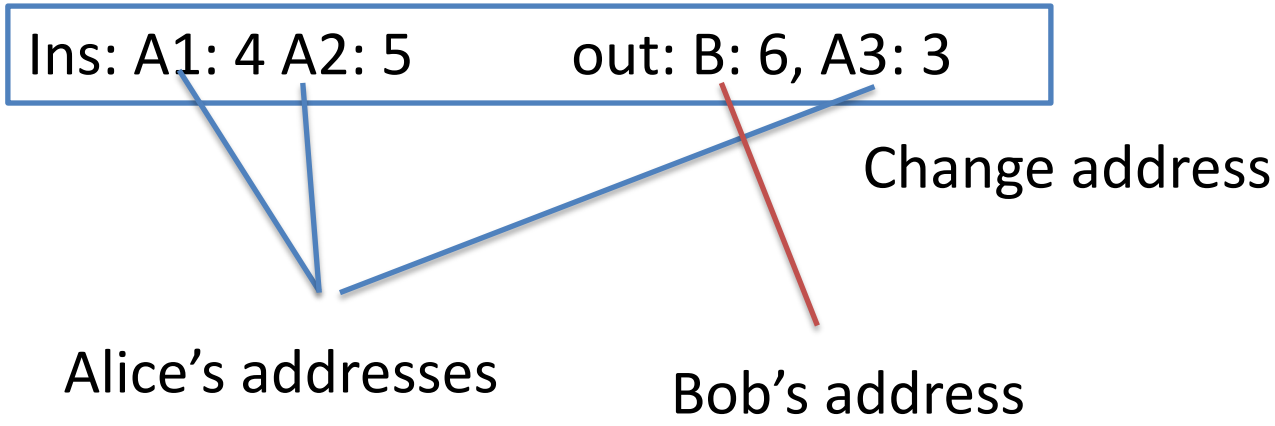
16k4365RzdeCPKGwJDNNBEkXj696MbChwx	0.53333328 BTC	1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA	0.01031593 BTC (U)
1Bsh4KD9ZJT4dJcoo7S5uS1jvtmtVmREb7	1.47877788 BTC	1AFLhD4EtG2uZmFxmfdXCyGUNqCqD5887u	2 BTC (S)

FEE: 0.00179523 BTC

1 CONFIRMATIONS 2.01031593 BTC

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

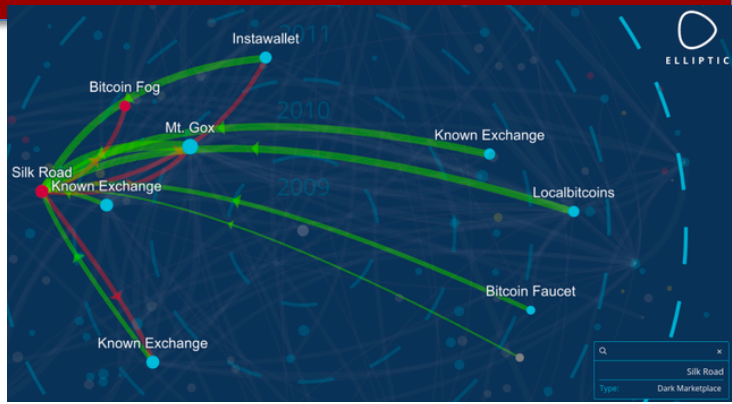
- Buying book from merchant
  - Alice learns one of merchant's addresses (B)
  - Merchant learns three of Alice's addresses
- Alice uses an exchange BTC ←→ $
  - KYC (Know your customer)
  - Money serving business collect and verify IDs
  - Exchange learns real ID

Donating to Wikileaks

Wikileaks had one address -> Easy to see who donates

Is Bitcoin Anonymous?

Now commercialized:



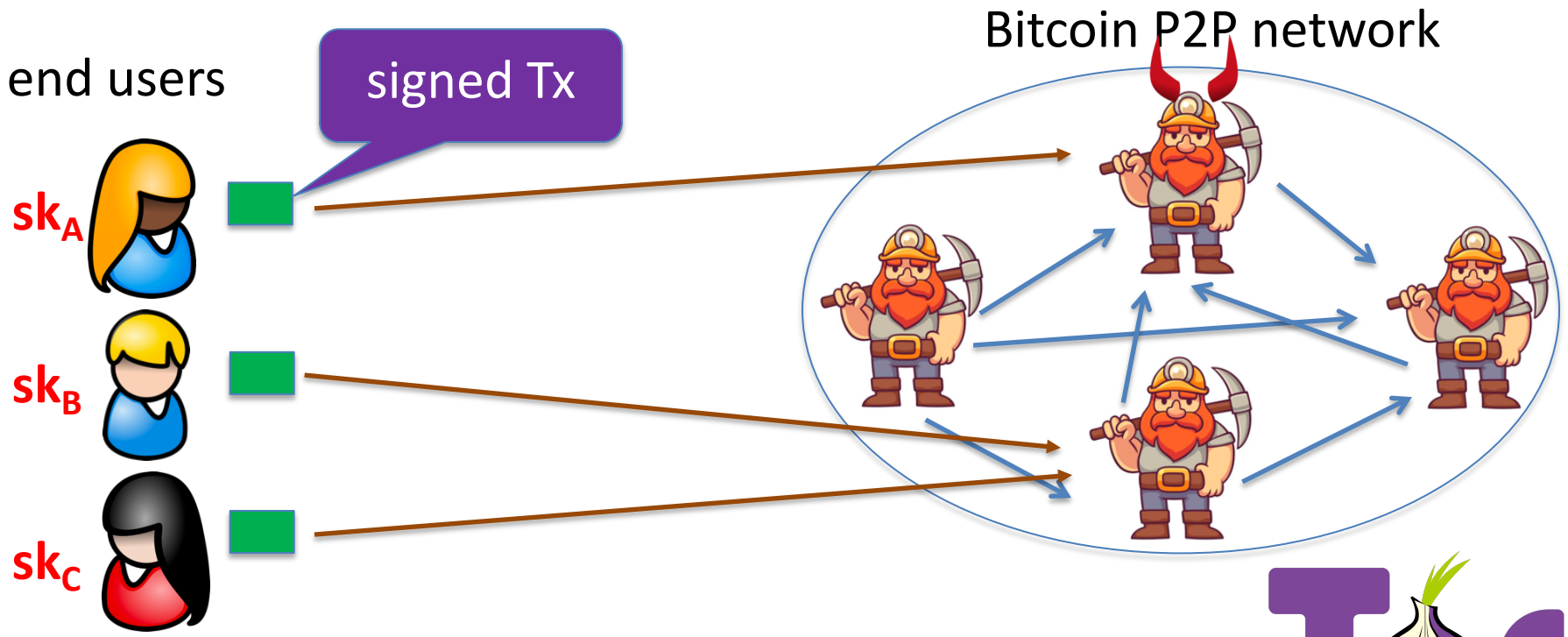
No!

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



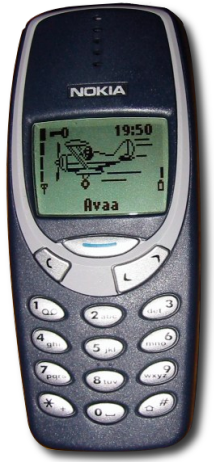
Can learn Alice's IP address

Solution:

Tor

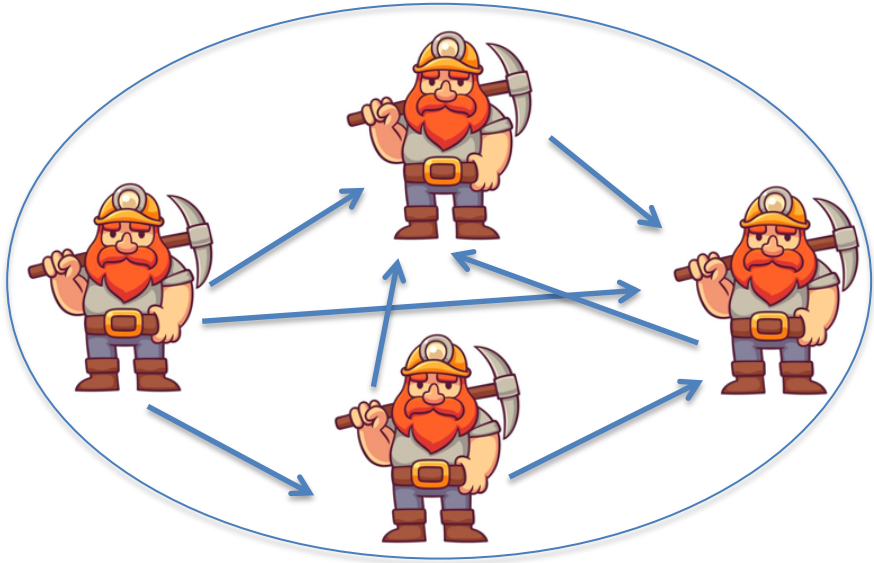
Light client network anonymity

SPV client



All addresses and transactions

Full node



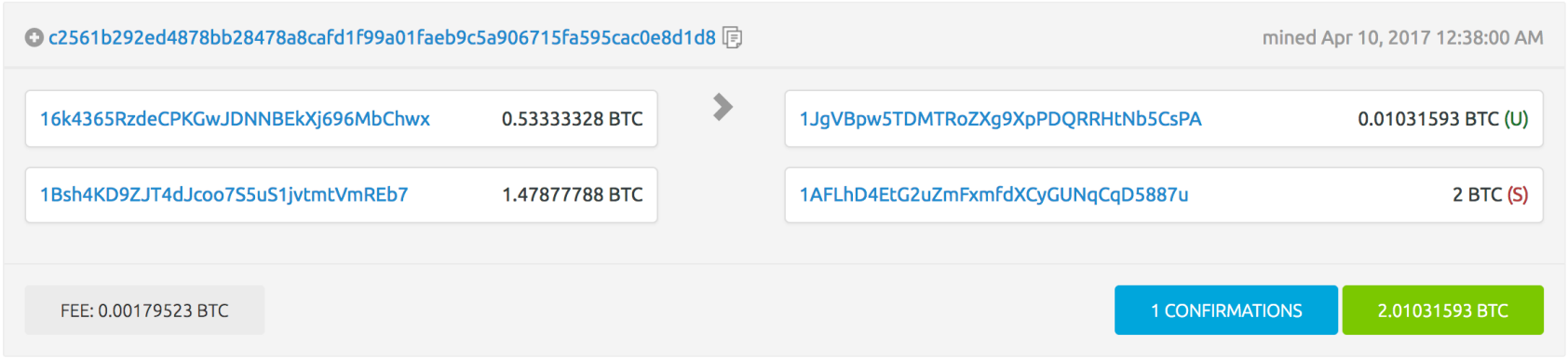
Fully linkable!

Idioms of use

Heuristic 1:

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

-> both addresses are controlled by same entity



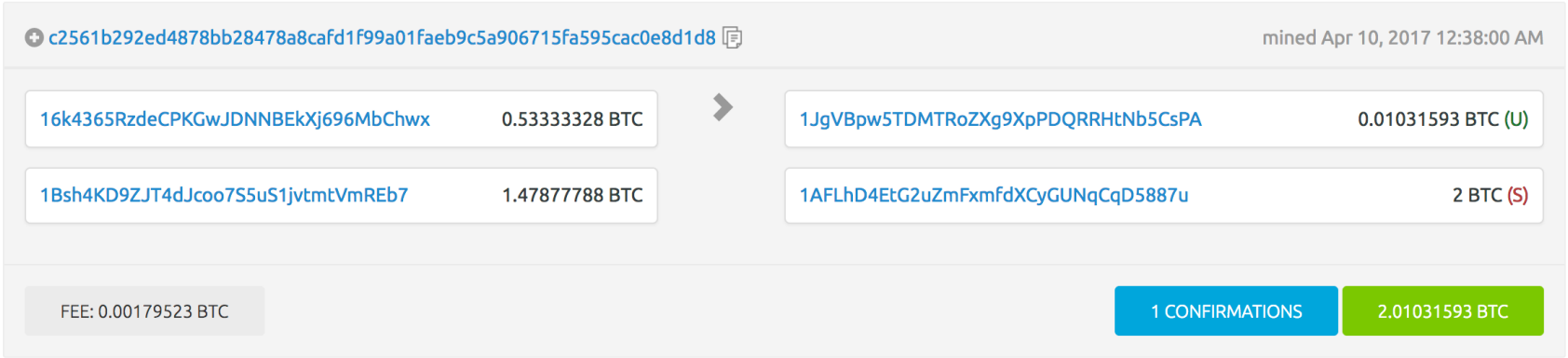
Idioms of use

Heuristic 2:

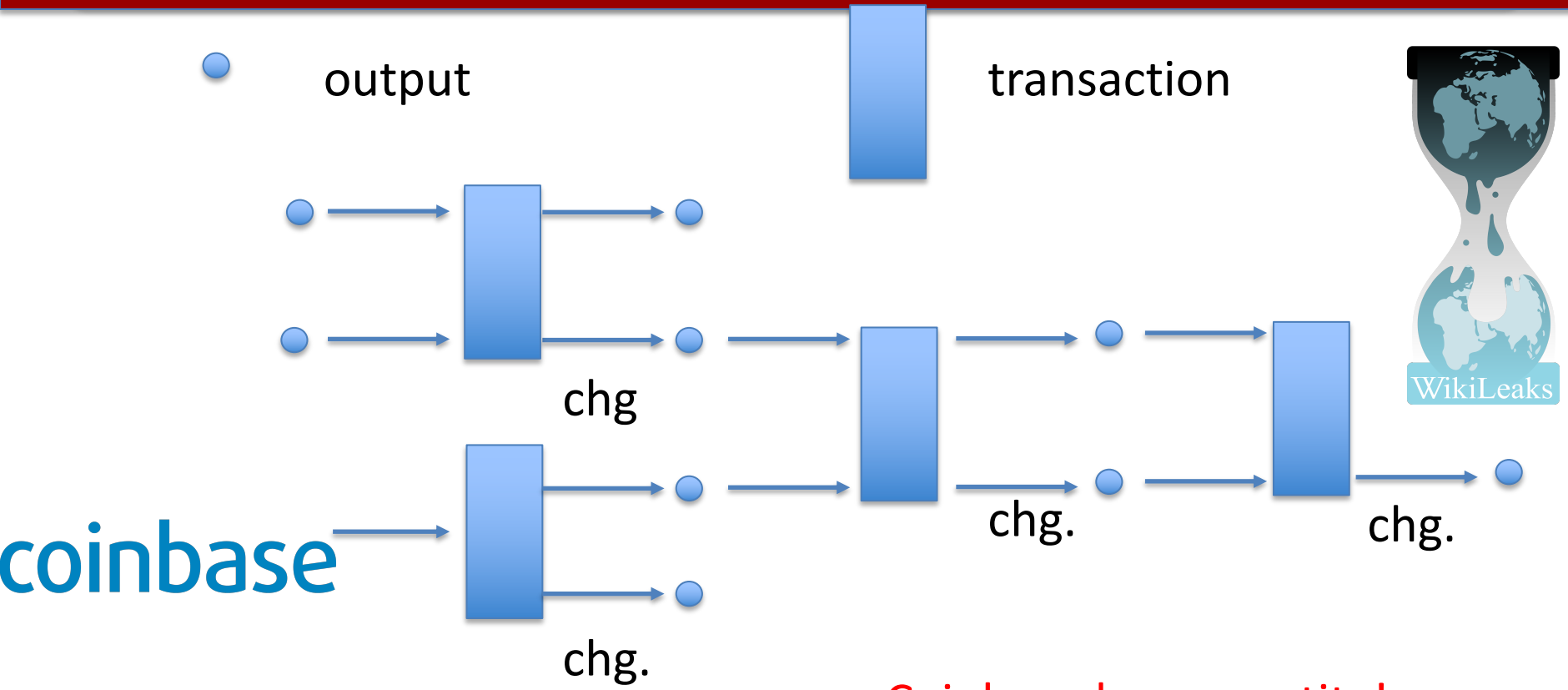
Change address is controlled by same user as input address

Which is change address: Used to be first address

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



Example tracing



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

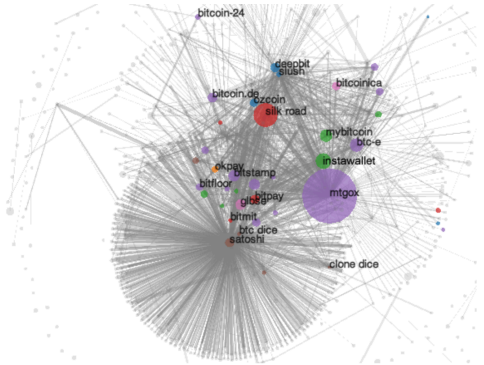
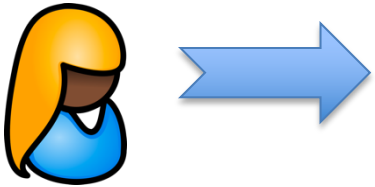


Figure 6: A visualization of the user network. The area of the cluster represents the external incoming value; i.e., the bitcoins received from

Another example



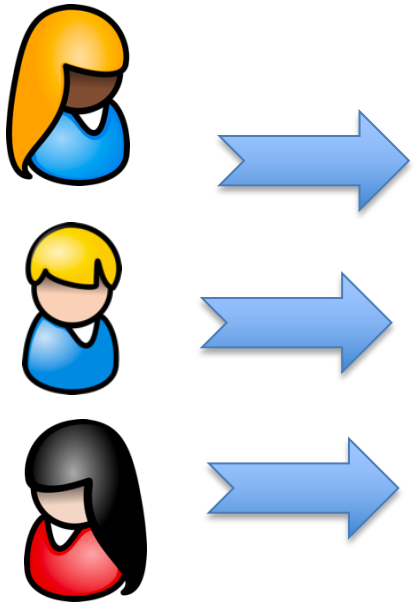
Ins: A1: 1. out: EC1 1

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

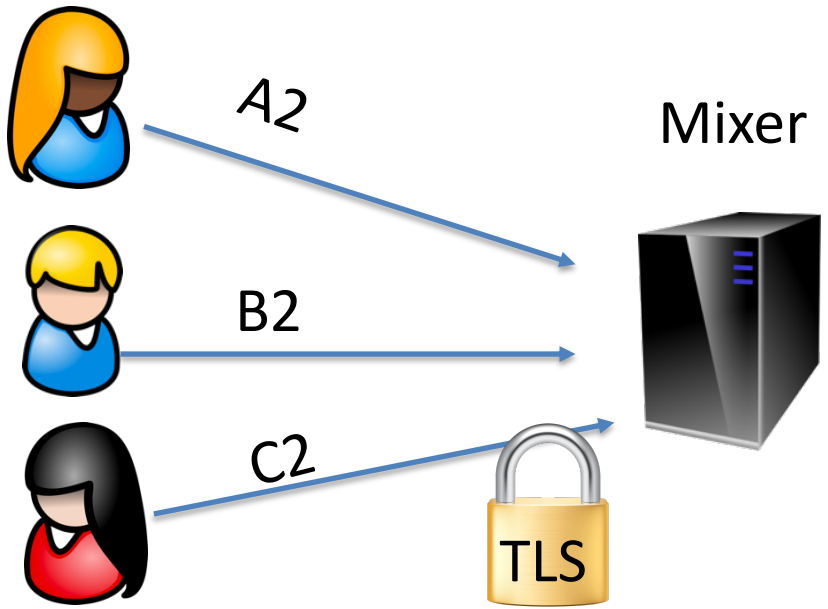
Anonymous cryptocurrencies

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 ∈ $\{Alice, Bob, Carol\}$
- For Bob
  - A2 ∈ $\{Alice, \cancel{Bob}, Carol\}$
- 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)

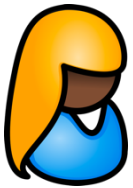
CoinJoin TX

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