Alternative mining puzzles (concluded)
Anonymity

Instructor: Matthew Green
Fall 2020

Some slides adapted from NBFMG

Housekeeping

- Midterm out 10/27, due approx 1 day later

News?

News?

COMPANY NEWS OCTOBER 21, 2020 / 7:30 AM / UPDATED 4 HOURS AGO

PayPal to allow cryptocurrency buying, selling and shopping on its network

By Anna Irrera

3 MIN READ

LONDON, Oct 21 (Reuters) - PayPal Holdings Inc joined the cryptocurrency market on Wednesday, allowing customers to buy, sell and hold bitcoin and other virtual coins using the U.S. digital payments company's online wallets.

Today

- Finishing talk about useful work PoW puzzles
- Then anonymity

Proof-of-useful-work

Recovering wasted work

Recall: power consumed by Bitcoin network in 2019 ~ power consumed by Switzerland :(

Natural question:

Can we recycle this and do something useful?

Candidates - needle in a haystack

- Natural choices:
  - Protein folding (find a low energy configuration)
  - Search for aliens (find an anomalous region of a signal)
- Challenges:
  - Randomly chosen instances must be hard

    Who chooses the problem?
  - Verification must also be efficient

Primecoin

Sunny King, 2013

Puzzle based on finding large prime numbers

Cunningham chain:

$p_1, p_2, \ldots p_n$ where $p_i = 2^i a + 1$

Each p_i is a large (probable) prime

`origin` is divisible by

`H(prev || mrkl_root || nonce)`

Primecoin

- Many of the largest known Cunningham chains have come from Primecoin miners
- Hard problem? Studied by others (e.g., PrimeGrid)
- Usefulness? Some applications to crypto (e.g., Young-Yung'98)

Recovering wasted hardware

Estimate: more than $100M spent on customized Bitcoin mining hardware

This hardware investment is otherwise useless

Idea: a puzzle where hardware investment is useful, even if the work is wasted?

Short Paper: The Proof is in the Pudding

Proofs of Work for Solving Discrete Logarithms

Marcella Hastings[1], Nadia Heninger[2], and Eric Wustrow[3]

[1] University of Pennsylvania
[2] University of California, San Diego
[3] University of Colorado Boulder

Abstract. We propose a proof of work protocol that computes the discrete logarithm of an element in a cyclic group. Individual provers generating proofs of work perform a distributed version of the Pollard rho algorithm. Such a protocol could capture the computational power expended to construct proof-of-work-based blockchains for a more useful purpose, as well as incentivize advances in hardware, software, or algorithms for an important cryptographic problem. We describe our proposed construction and elaborate on challenges and potential trade-offs that arise in designing a practical proof of work.

Keywords: Proofs of work, discrete log, Pollard rho

Permacoin - Mining with storage

Miller et al., 2014

Bitcoin

Permacoin

Side effect:

Massively distributed, replicated storage system

Permacoin

Assume we have a large file **F** to store

For simplicity: **F** is chosen globally, at the beginning, by a trusted dealer

Each user stores a random subset of the file

Storage-based puzzle

1. Build a Merkle tree, where each leaf is a segment of the file

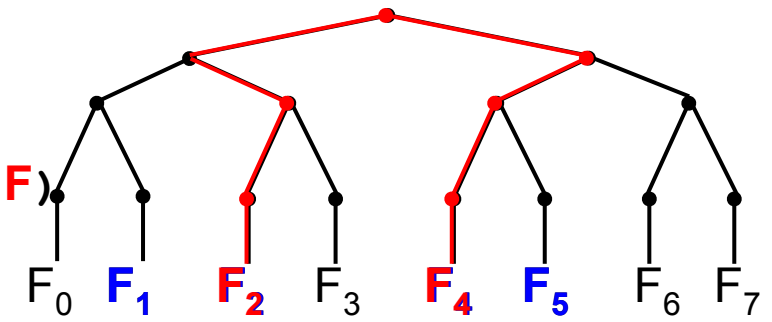
2. Generate a public signing key pk, which determines a random subset of file segments

F_1 F_2 F_4 F_5

3. Each mining attempt:

F_2 F_4

a) Select a random nonce
b) h1 := H(prev || mrkl_root || PK || nonce)
c) h1 selects *k* segments from subset
d) h2 := H(prev || mrkl_root || PK || nonce || F)
e) Winner if h2 < TARGET



Proofs of Space

- Require non-trivial storage (as opposed to computational power) to solve a puzzle
  [Dziembowski et al. CRYPTO'15, Ateniese et al. SCN'14]

- More environmental-friendly
- Used in FileCoin
  - Combination of Proof of Space & Proof of Storage

Summary

- Useful proof-of-work is a natural goal

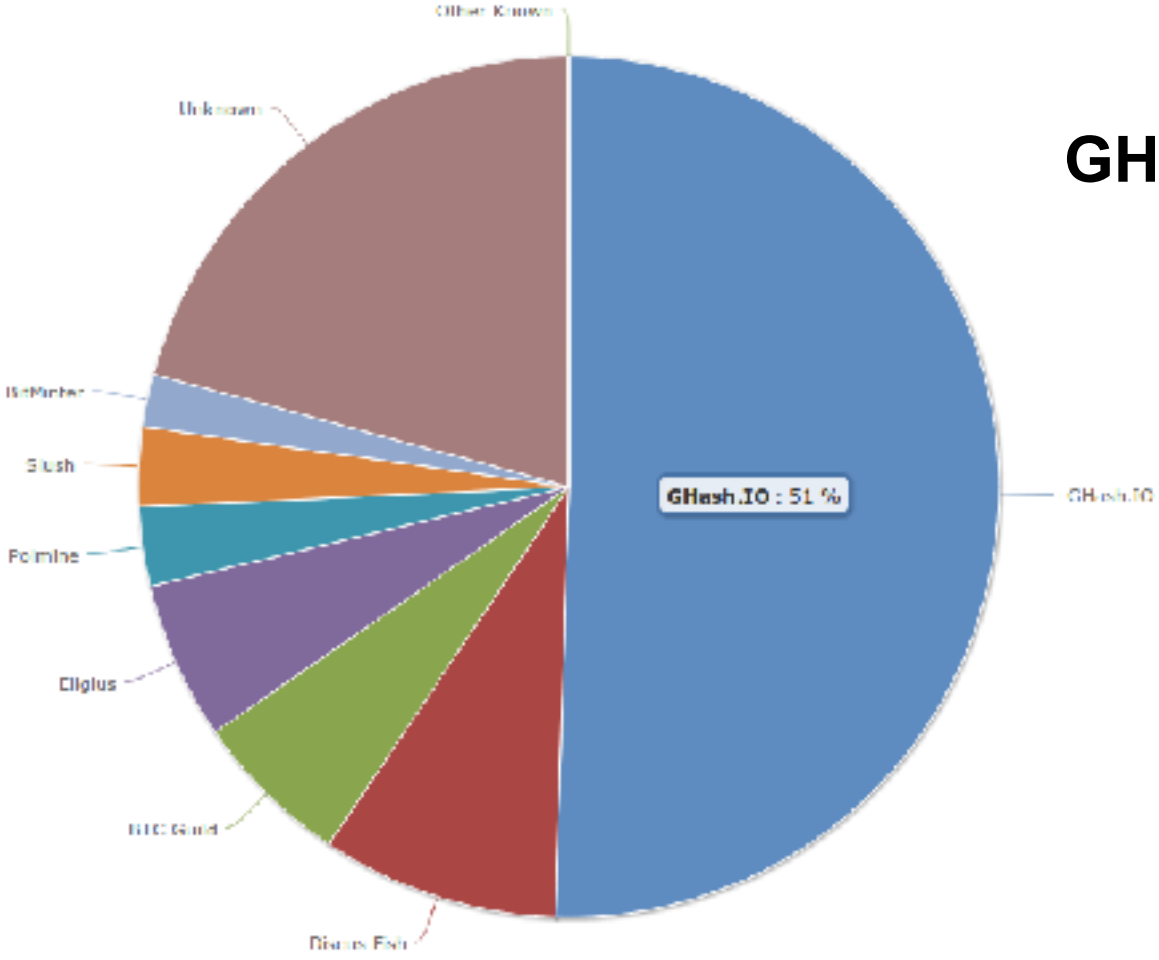
  (while maintaining security requirements)
- The benefit must be a pure public good
- Viable approaches include storage, prime-finding, others may be possible
- Realized benefit so far has been limited

Nonoutsourceable Puzzles

Large mining pools are a threat

- Bitcoin’s core value is decentralization
- If power is consolidated in a few large pools, the operators are targets for coercion/hacking
- Position: large pools should be discouraged!

  Analogy to voting: It’s illegal (in US) to sell your vote



June 12, 2014

GHash.IO large mining pool crisis

Hacking, Distributed

It's Time For a Hard Bitcoin Fork

Ittay Eyal, and Emin Gün Sirer — Friday June 13, 2014 at 02:05 PM

A Bitcoin mining pool, called GHash and operated by an anonymous entity called CEX.io, just reached 51% of total network mining power today. Bitcoin is no longer decentralized. GHash can control Bitcoin transactions.

Is This Really Armageddon?

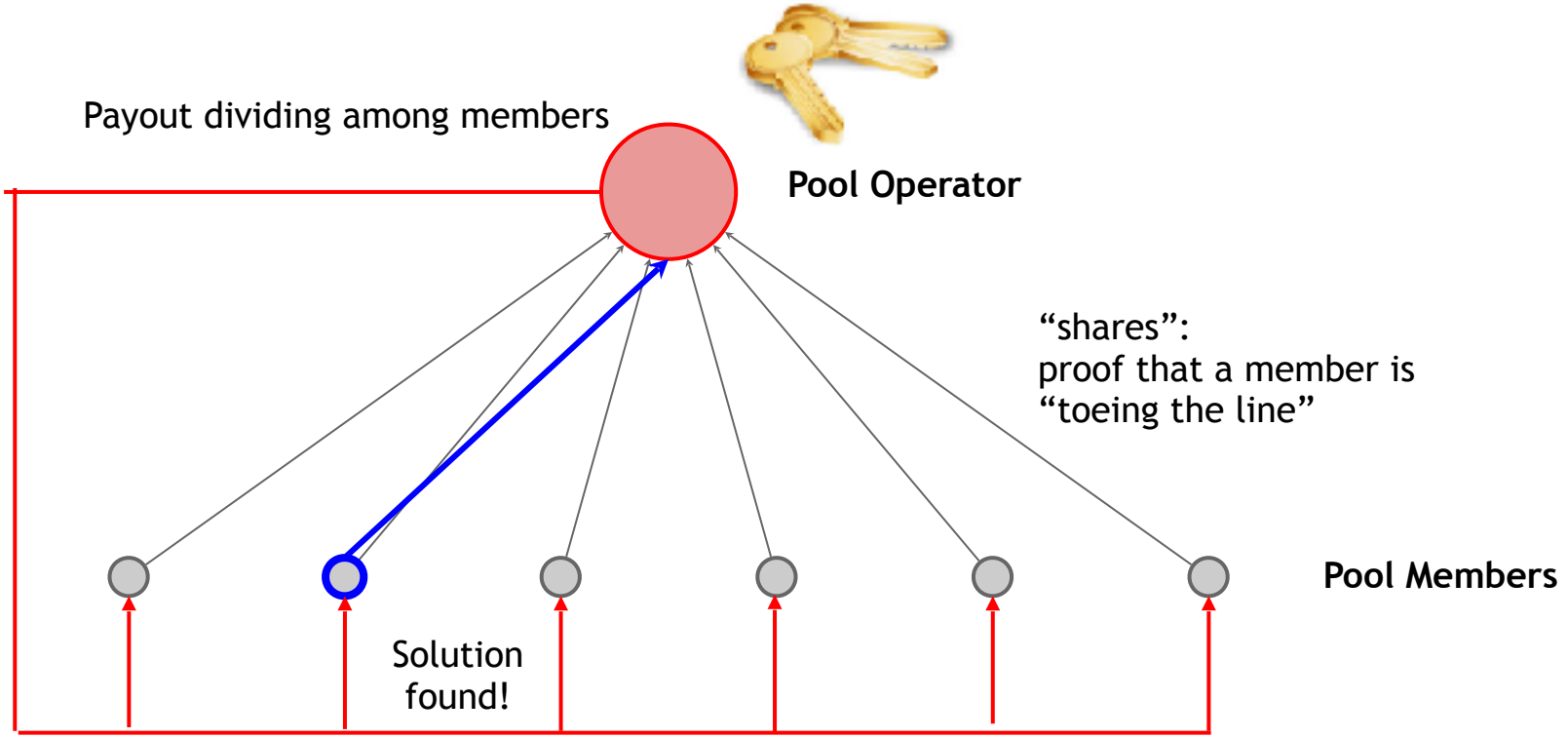
Yes, it is. GHash is in a position to exercise complete control over which

Observation:

Pool participants don’t trust each other

Pools only work because the “shares” protocol lets members ***prove*** cooperation

Standard Bitcoin mining pool



The Vigilante Attack

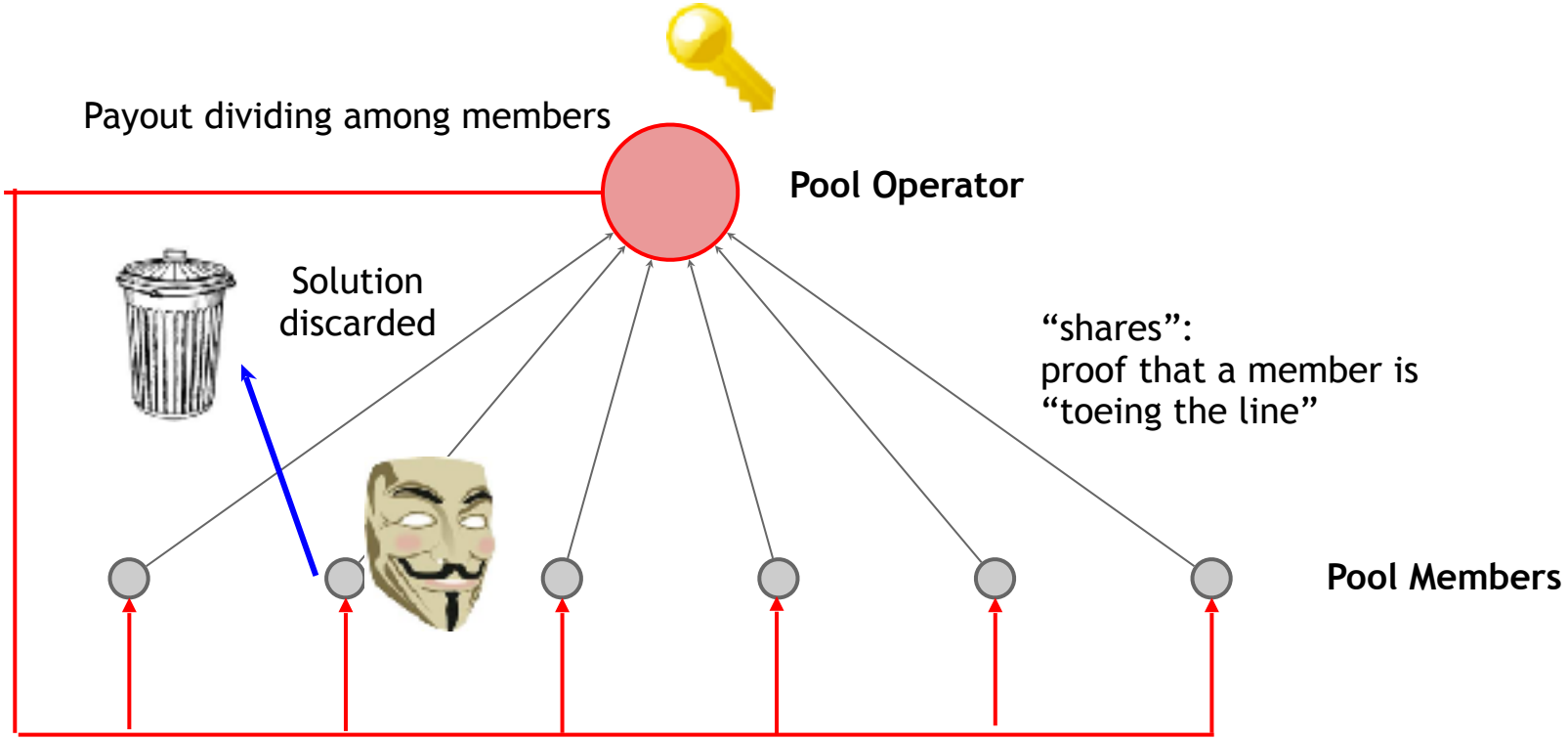
Suppose a Vigilante is angry with a large pool

He submits “shares” like normal….

… but if he finds a real solution, discards it

Pool output is reduced, Vigilante loses a little

The Vigilante Attack



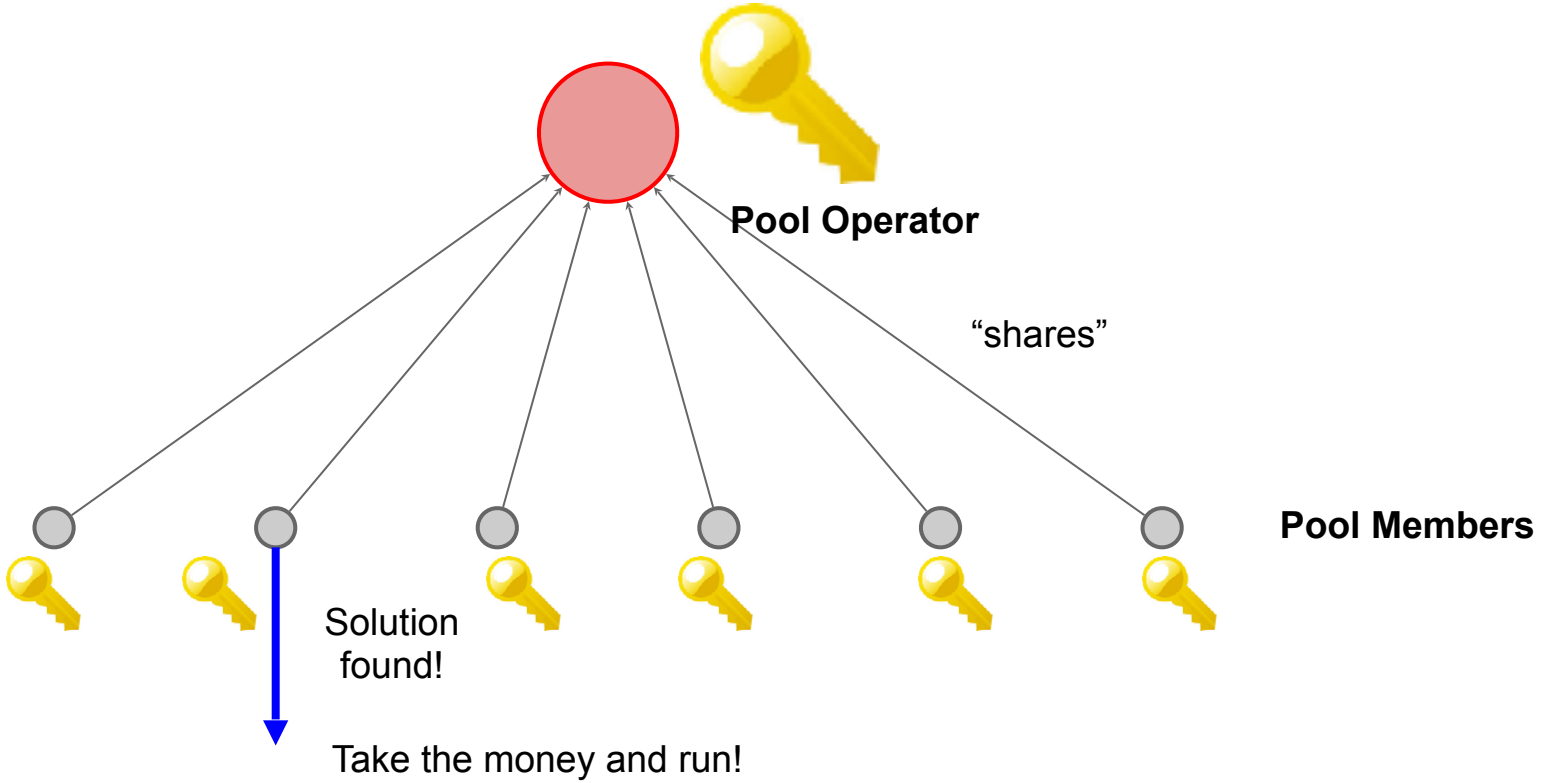
Encouraging the Vigilante

Whoever ***FINDS*** a solution spends the reward

Approach:

- searching for a solution requires ***SIGNING***, not just hashing. (Knowledge of a private key)
- Private key can be used to spend the reward

Encouraging the Vigilante



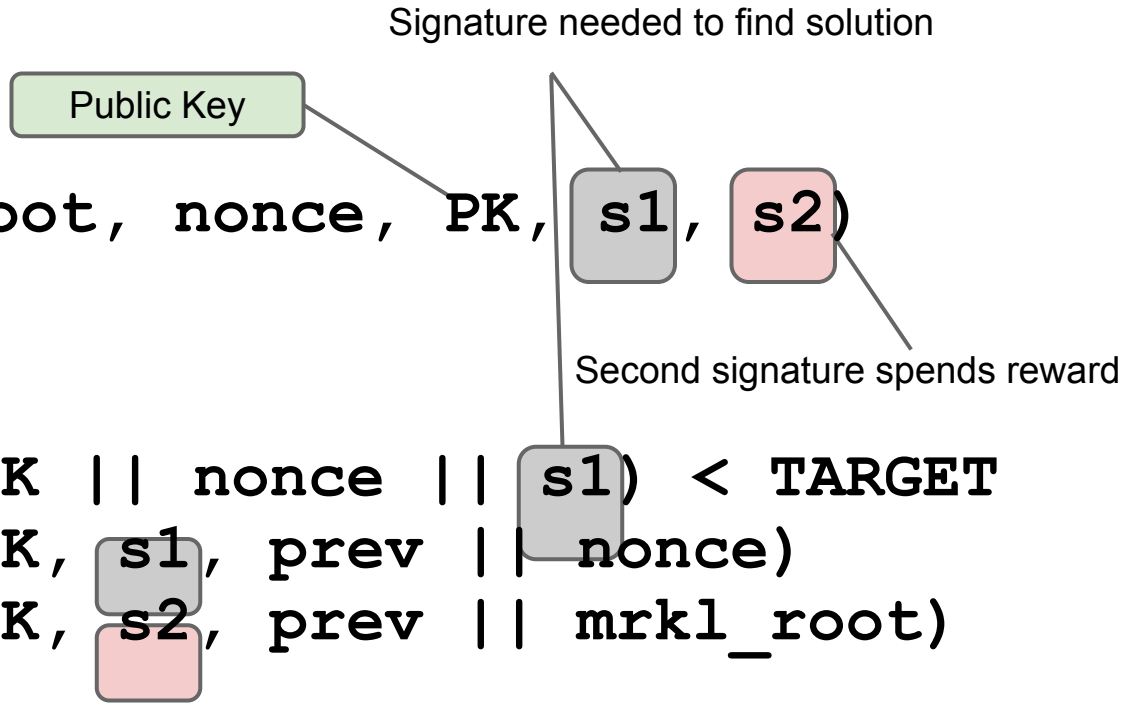
Nonoutsourceable puzzle

Solution:

```
(prev, mrkl_root, nonce, PK, s1, s2)
```

such that:

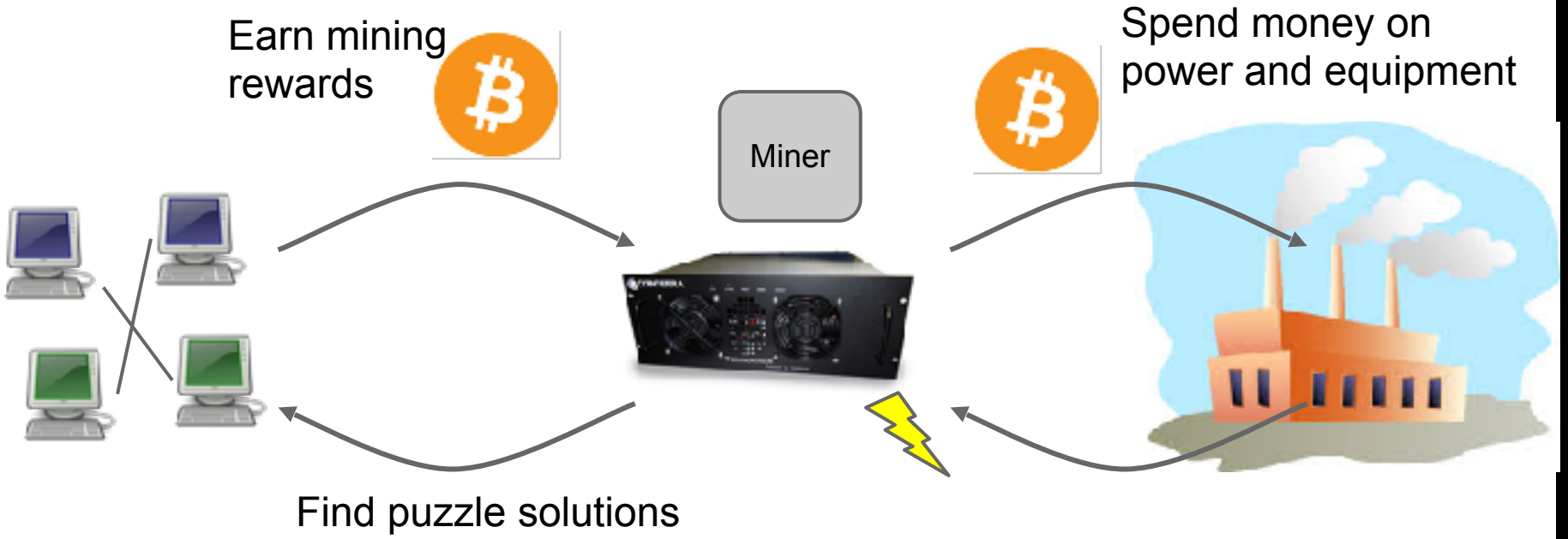
```
H(prev || PK || nonce || s1) < TARGET
VerifySig(PK, s1, prev || nonce)
VerifySig(PK, s2, prev || mrkl_root)
```



Proof-of-Stake
“Virtual Mining”

Bitcoin Mining has an unnecessary step

Proof-of-Work Mining:



Bitcoin Mining has an unnecessary step

Proof of Stake:

- Creator of next block chosen at random based on current stake in the system

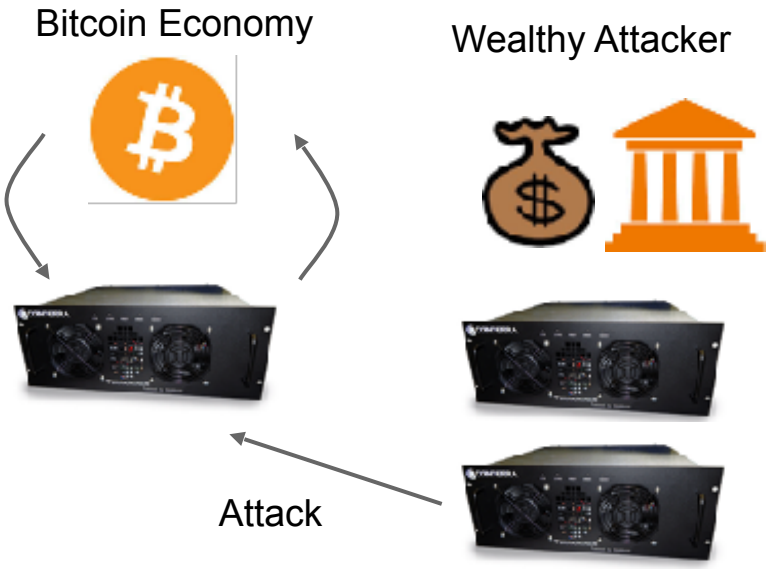
Potential benefits

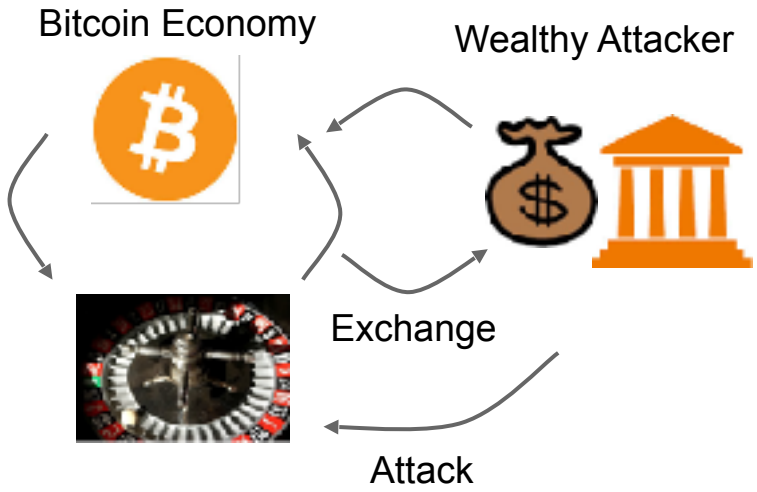
- Lower overall costs
  - No harm to the environment
  - Savings distributed to all coin holders
- Stakeholder incentives - good stewards?
- No ASIC advantage
- 51% attack is even harder

51% attack prevention argument

The Bitcoin economy is smaller than the world

Wealth *outside* Bitcoin has to move *inside*





Variations of Virtual Mining

- Proof-of-Stake: “Stake” of a coin grows over time as long as the coin is unused (but potentially some upper limit)
- Proof-of-Burn: mining with a coin destroys it
- Proof-of-Deposit: can reclaim a coin after some time
- Proof-of-Activity: any coin might be win (if online)

Questions with Virtual Mining

Is there any security that can only be gained by consuming “real” resources?

- If so, then “waste” is the cost of security
- If not, then PoW mining may go extinct

Examples of PoS based Cryptocurrencies

- Cardano
- Algorand
- Ethereum 2 (one hopes!)

Examples of secure PoS systems

- Algorand [Full version: Chen-Micali'17]
- Ourboros [Kiayias-Russel-David-Oliynykov'17]
- Snow white [Daian-Pass-Shi'17]

Conclusion

- Many possible design goals
  - Prevent ASIC miners from dominating
  - Prevent large pools from dominating
  - Intrinsic usefulness
  - Eliminate the need for mining hardware at all
- Further research required to understand the best tradeoffs
- Many competing systems already co-exist

Some say Bitcoin provides anonymity

“ Bitcoin is a secure and anonymous digital currency ”

— WikiLeaks donations page

Others say it doesn’t

“ Bitcoin won't hide you from the NSA's prying eyes”

— Wired UK

What do we mean by anonymity?

Literally: anonymous = without a name

Bitcoin addresses are public key hashes rather than real identities

Computer scientists call this pseudonymity

Anonymity in computer science

Anonymity = pseudonymity + unlinkability

Different interactions of the same user with the system should not be linkable to each other

Pseudonymity vs anonymity in forums

Reddit: pick a long-term pseudonym

vs.

4Chan: make posts with no attribution at all

Why is unlinkability needed?

1. Many Bitcoin services require real identity

1. Linked profiles can be deanonymized by a variety of side channels

Defining unlinkability in Bitcoin

- Hard to link different addresses of the same user
- Hard to link different transactions of the same user
- Hard to link sender of a “payment” to its recipient

Quantifying anonymity

Anonymity set: Anonymity set of a transaction T is the set of transactions which an adversary cannot distinguish from T.

To calculate anonymity set:

- define adversary model
- reason carefully about: what the adversary knows, does not know, and cannot know

Why anonymous cryptocurrencies?

Block chain based currencies are totally, publicly, and permanently traceable

Without anonymity, privacy is much worse than traditional banking!

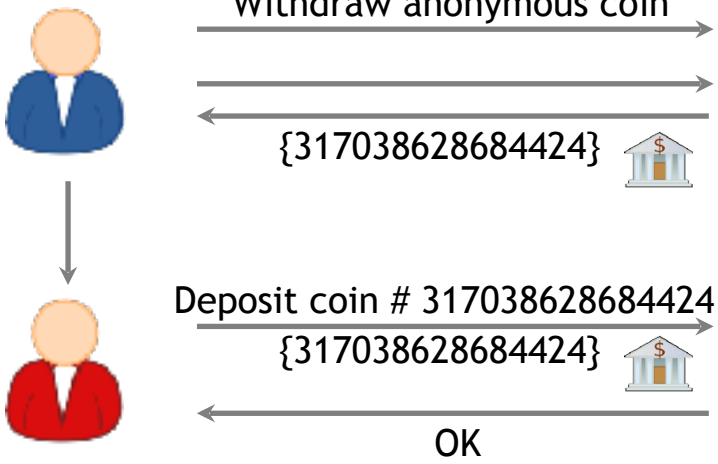
Anonymous e-cash: history

Introduced by David Chaum, 1982

Blind signature: a two-party protocol to create digital signature without signer learning which message is being signed

- An example of secure two-party computation

Anonymous e-cash via blind signatures



User	Balance
…	…
	9
…	…
	6

Spent coins
…
31703862…

Bank cannot link the two users

Anonymity & decentralization: in conflict

- Interactive cryptographic protocols with bank are hard to decentralize
  - Later: Zerocoin and Zerocash overcome this challenge by using non-interactive cryptographic techniques
- Decentralization often achieved via public traceability to enforce security

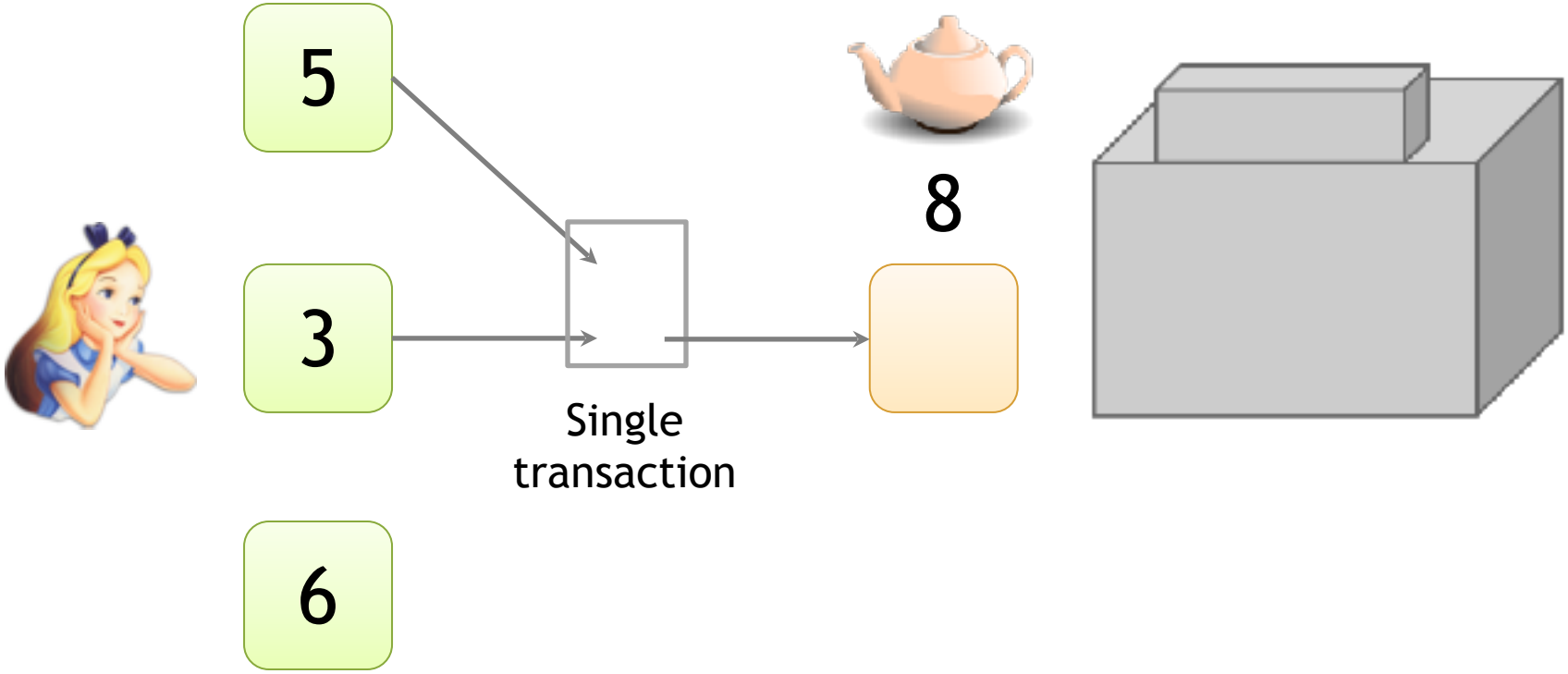
How to de-anonymize Bitcoin

Trivial to create new addresses in Bitcoin

Best practice: always receive at fresh address

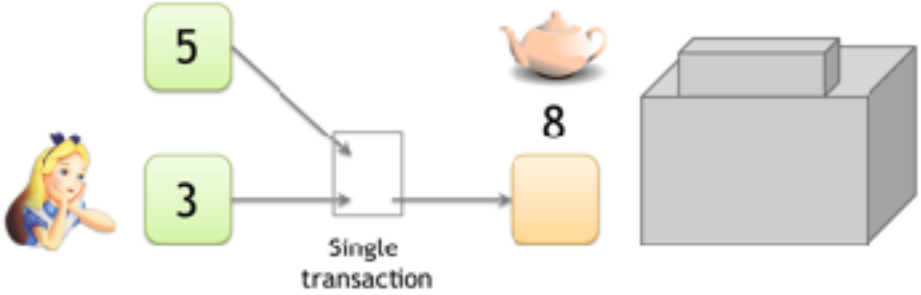
So, unlinkable?

Alice buys a teapot at Big box store



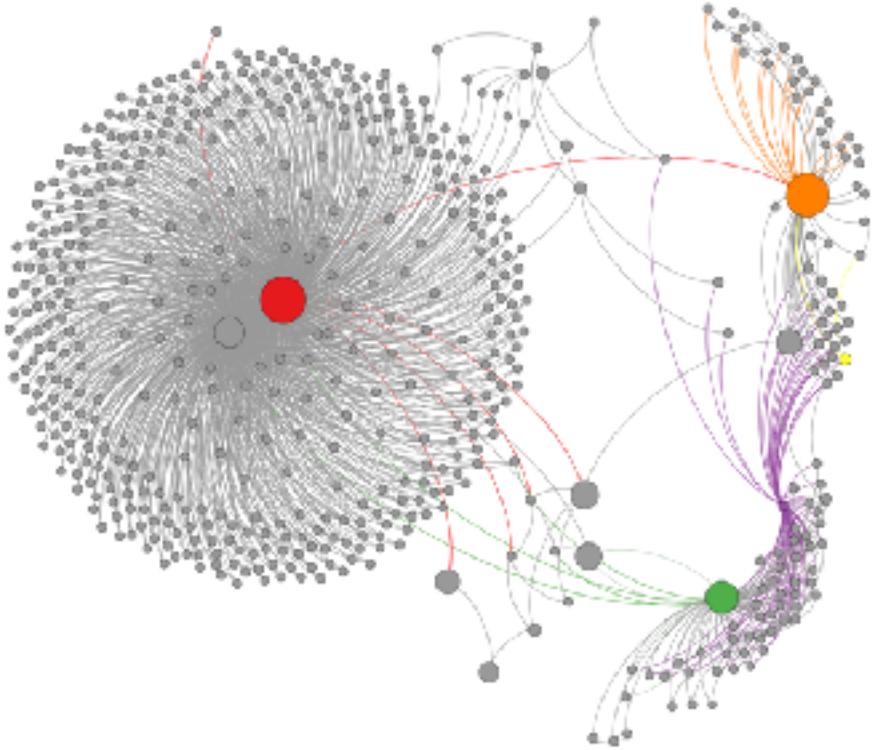
Linking addresses

Shared spending is evidence of joint control



Addresses can be linked transitively

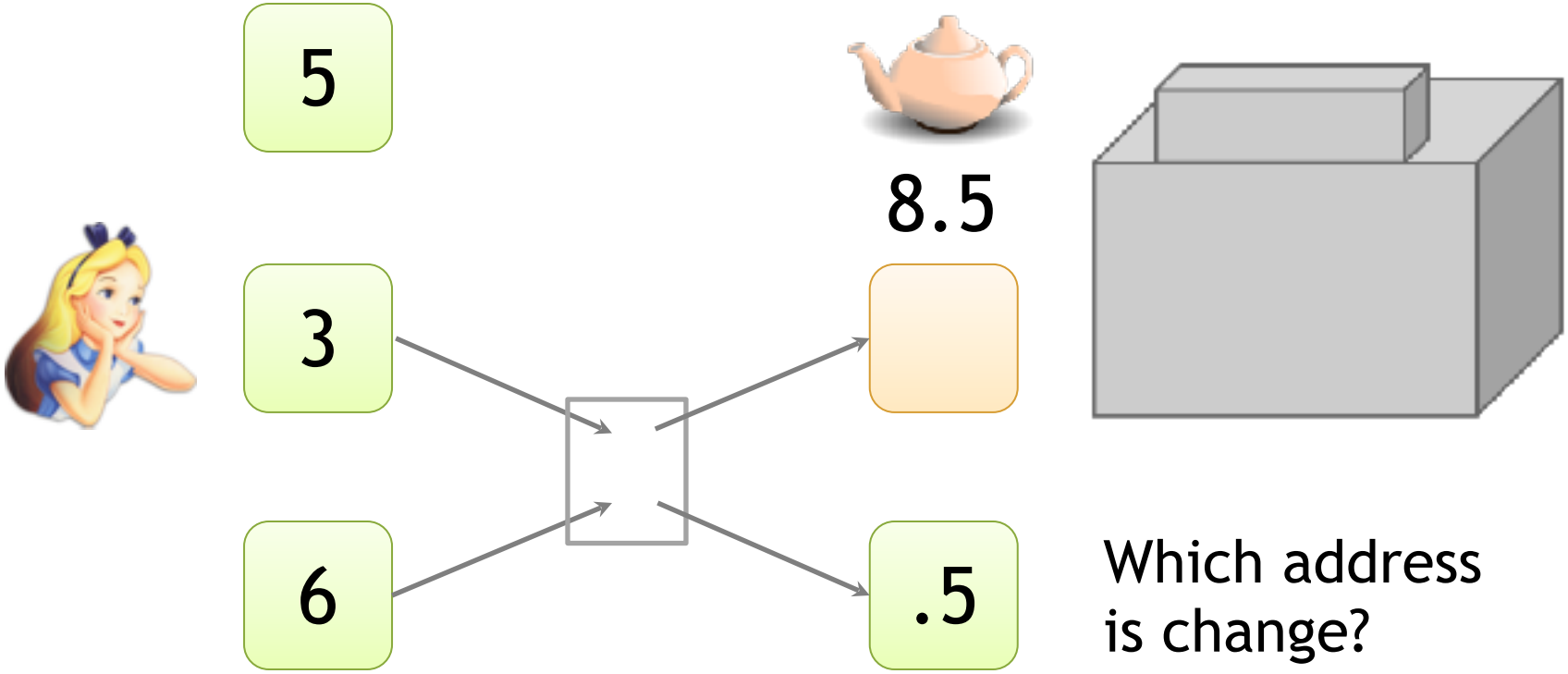
Clustering of addresses



An Analysis of Anonymity in the Bitcoin System

F. Reid and M. Harrigan
PASSAT 2011

Change addresses



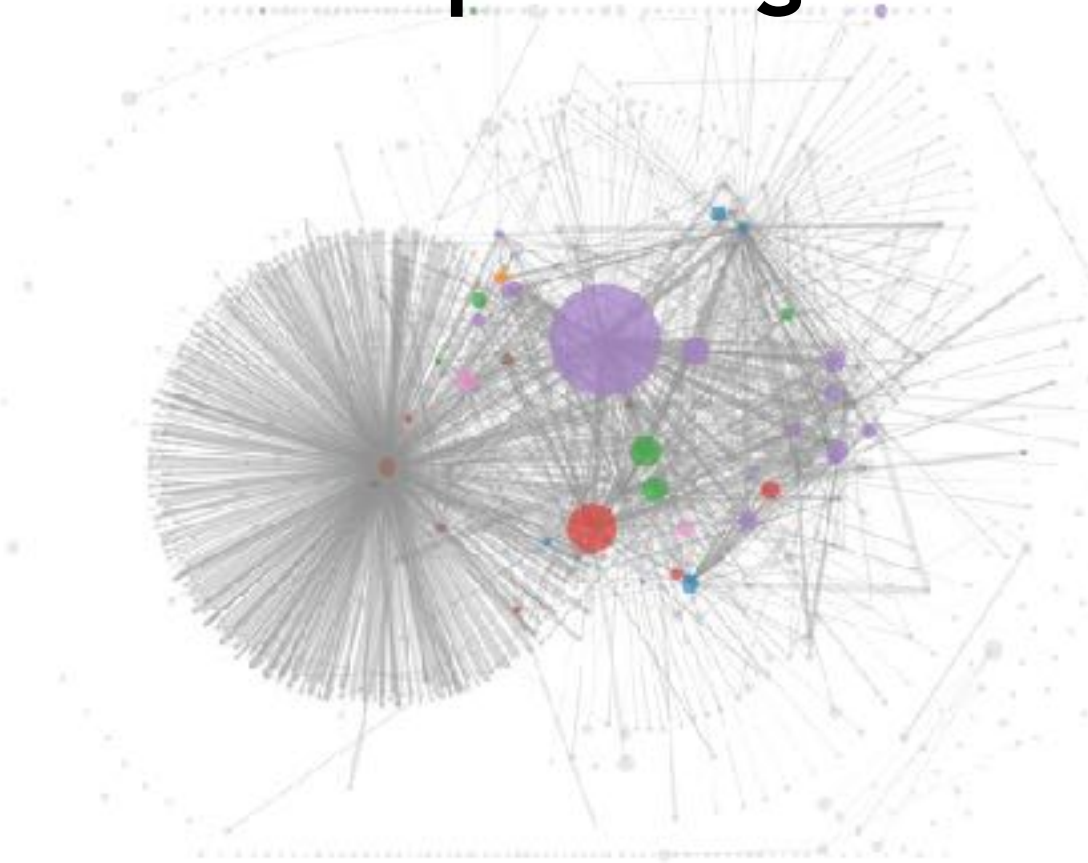
Which address is change?

“Idioms of use”

Idiosyncratic features of wallet software

e.g., each address used only once as change

Shared spending + idioms of use



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

S. Meiklejohn et al.
IMC 2013

To tag service providers: transact!

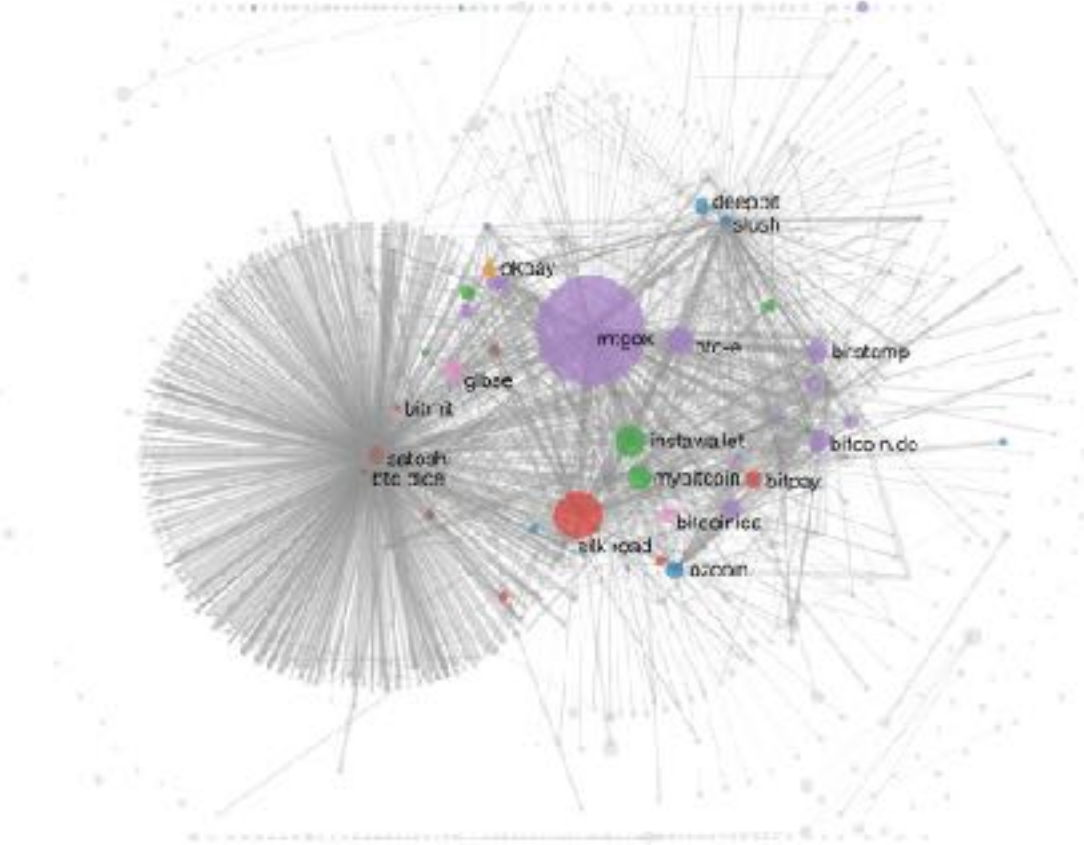
A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

S. Meiklejohn et al.

344 transactions

- Mining pools
- Wallet services
- Exchanges
- Vendors
- Gambling sites

Shared spending + idioms of use



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

S. Meiklejohn et al.
IMC 2013

From services to users

1. High centralization in service providers

   Most flows pass through one of these — in a traceable way

2. Address — identity links in forums

Achieving Anonymity

Approaches

- **Mixing**: Pool in multiple transactions (ideally same value), and then create new transactions
  - Centralized: E.g., online wallets
  - Decentralized: E.g., CoinJoin
  - Untrusted intermediary using crypto: Tumblebit
- **New cryptocurrencies:**
  - Using Zero-knowledge proofs: Zerocoin and Zerocash
  - Using Ring signatures: Monero

Approaches

- **Mixing**: Pool in multiple transactions (ideally same value), and then create new transactions
  - Centralized: E.g., online wallets
  - Decentralized: E.g., CoinJoin (e.g., implementation: Dash)
  - Untrusted intermediary using crypto: Tumblebit
- **New cryptocurrencies:**
  - Using Zero-knowledge proofs: Zerocoin and Zerocash
  - Using Ring signatures: Cryptonote (e.g., implementation: Monero)