Zerocoin: Anonymous Distributed E-Cash from Bitcoin

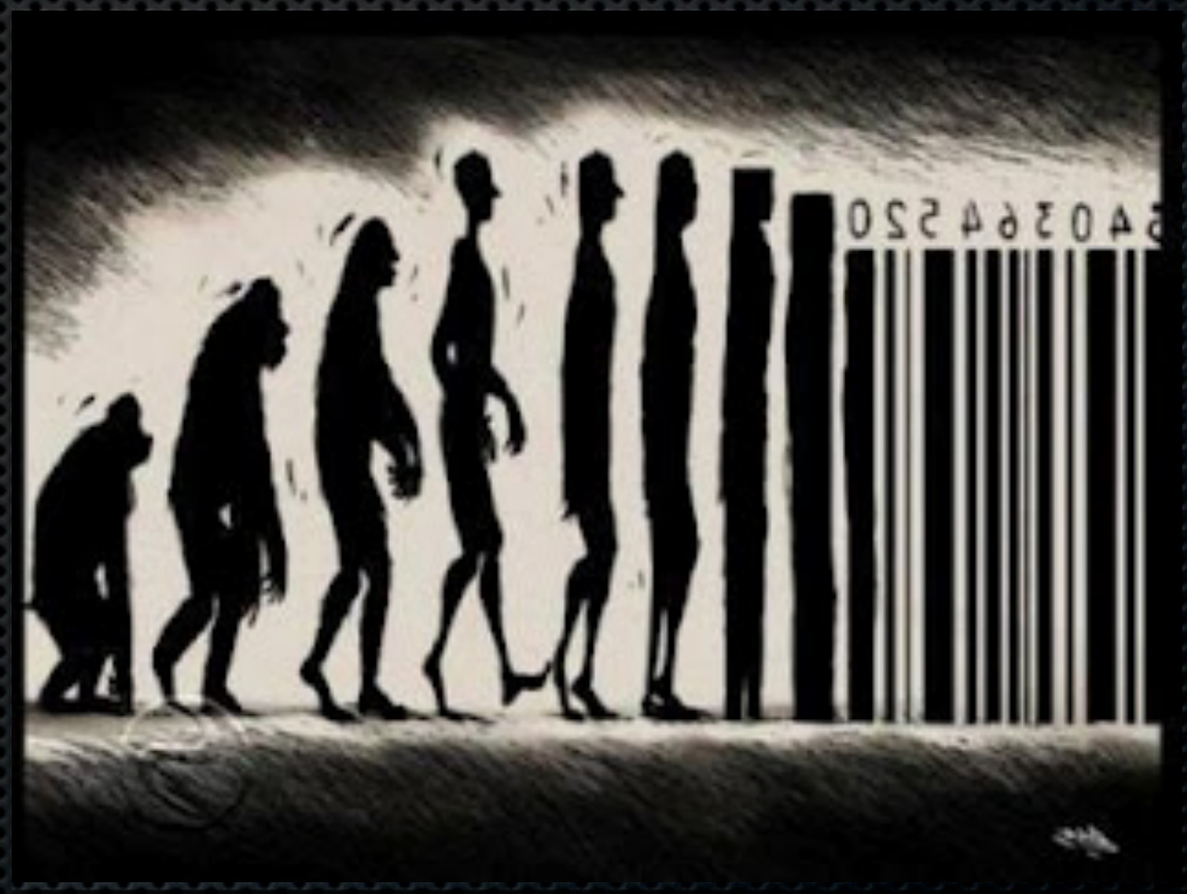
Ian Miers

Christina Garman | Matthew Green | Avi Rubin

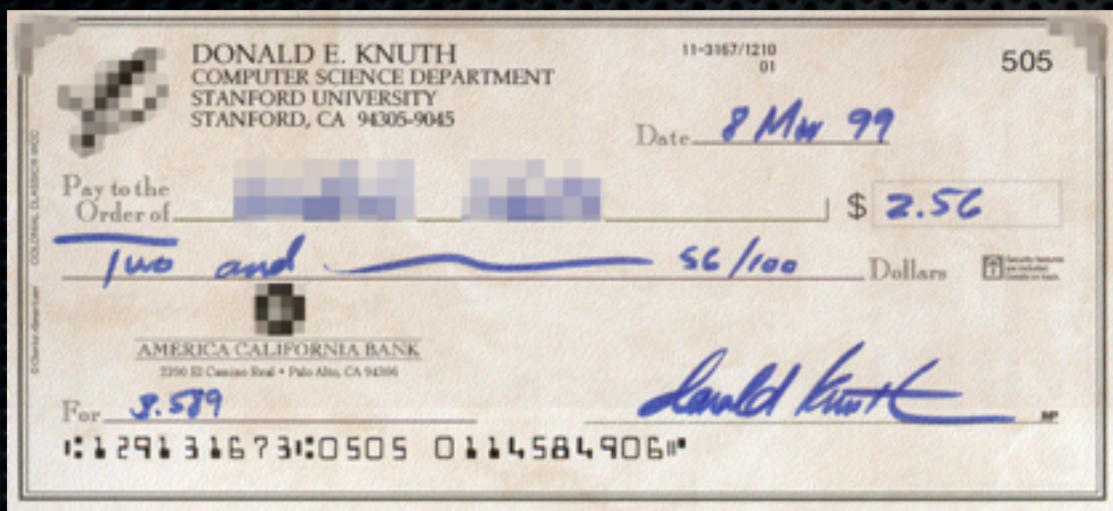
JOHNS HOPKINS UNIVERSITY

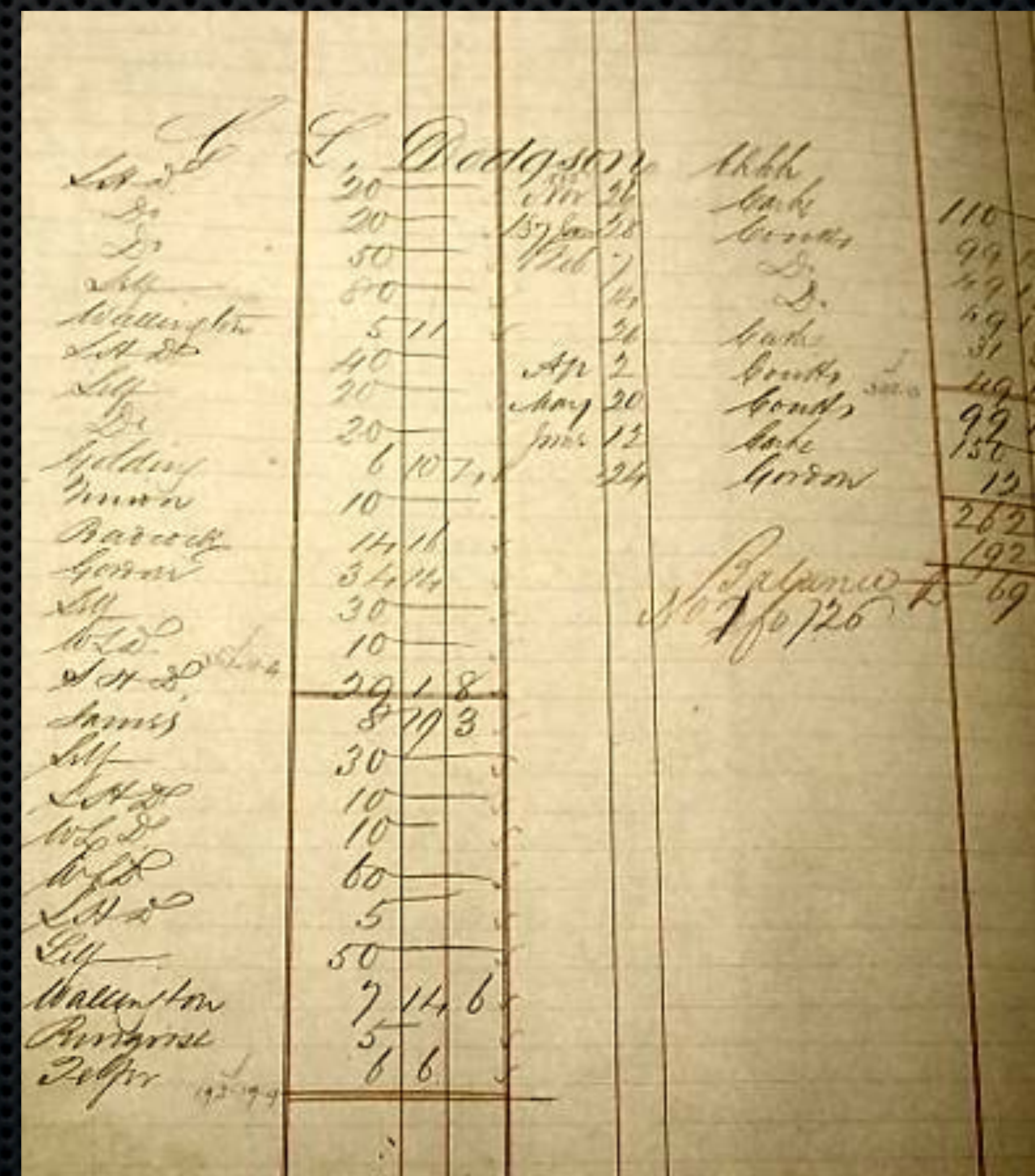
Digitizing money

- Two ways to do it
  - Create digital cash
  - Create digital checks



Bank accounts





Problem: privacy

- Bank sees every transaction
- Merchants can track customers across interactions

Digital cash

- Can’t make uncopyable digital currency
- Can make single use currency
  - Get a unique serial number when you withdraw money
  - Spend it by showing an unused serial number

E-cash

- Chaum82: blind signatures for e-cash
- Chaum88: retroactive double spender identification
- Brandis95: restricted blind signatures
- Camenisch05: compact offline e-cash

An ideal digital currency

Bitcoin

- A distributed digital currency system
- Released by Satoshi Nakamoto 2008
- Market cap of 1.2 Billion USD (as of early May 2013)
- Effectively a bank run by an ad hoc network
  - Digital checks
  - A distributed transaction log

Bitcoin: digital checks

Bitcoin: transaction log

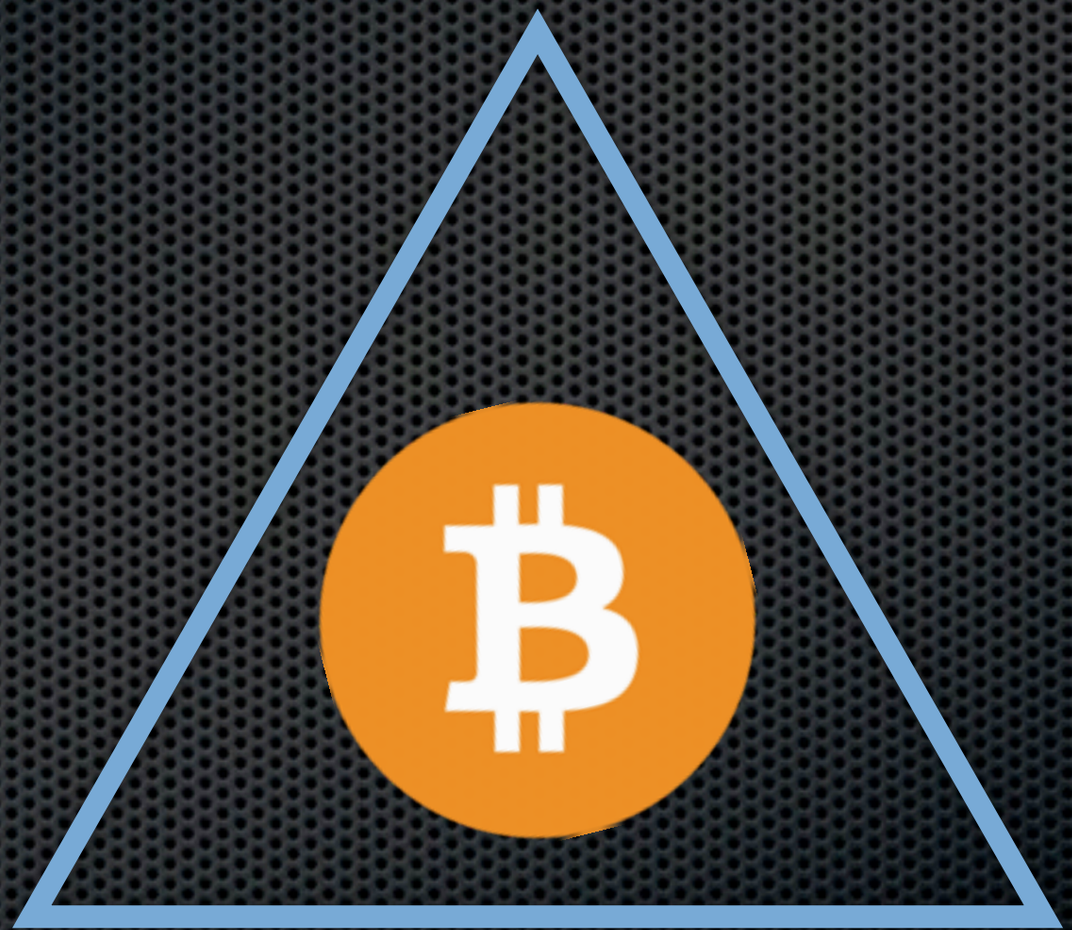
- How do you maintain a transaction log?
  - Pick a trusted party
  - Vote

Avoiding the clone wars

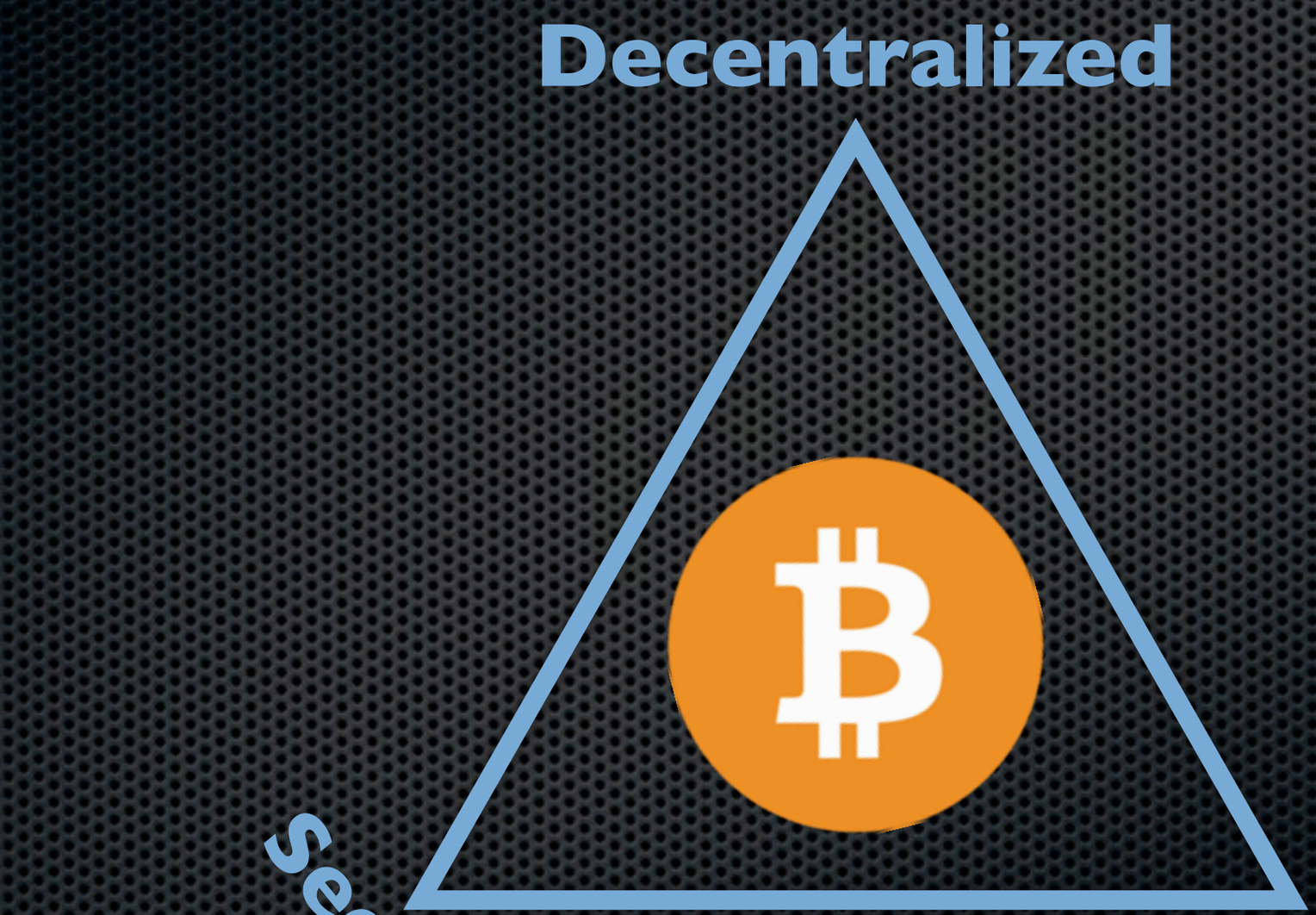
- Select a node at random proportional to its computational power to update the log
- Nodes race to compute a partial hash collision:
  hash(data || nonce) < x
- Pick the longest chain
- Bitcoin calls this ledger the block chain

Bitcoin

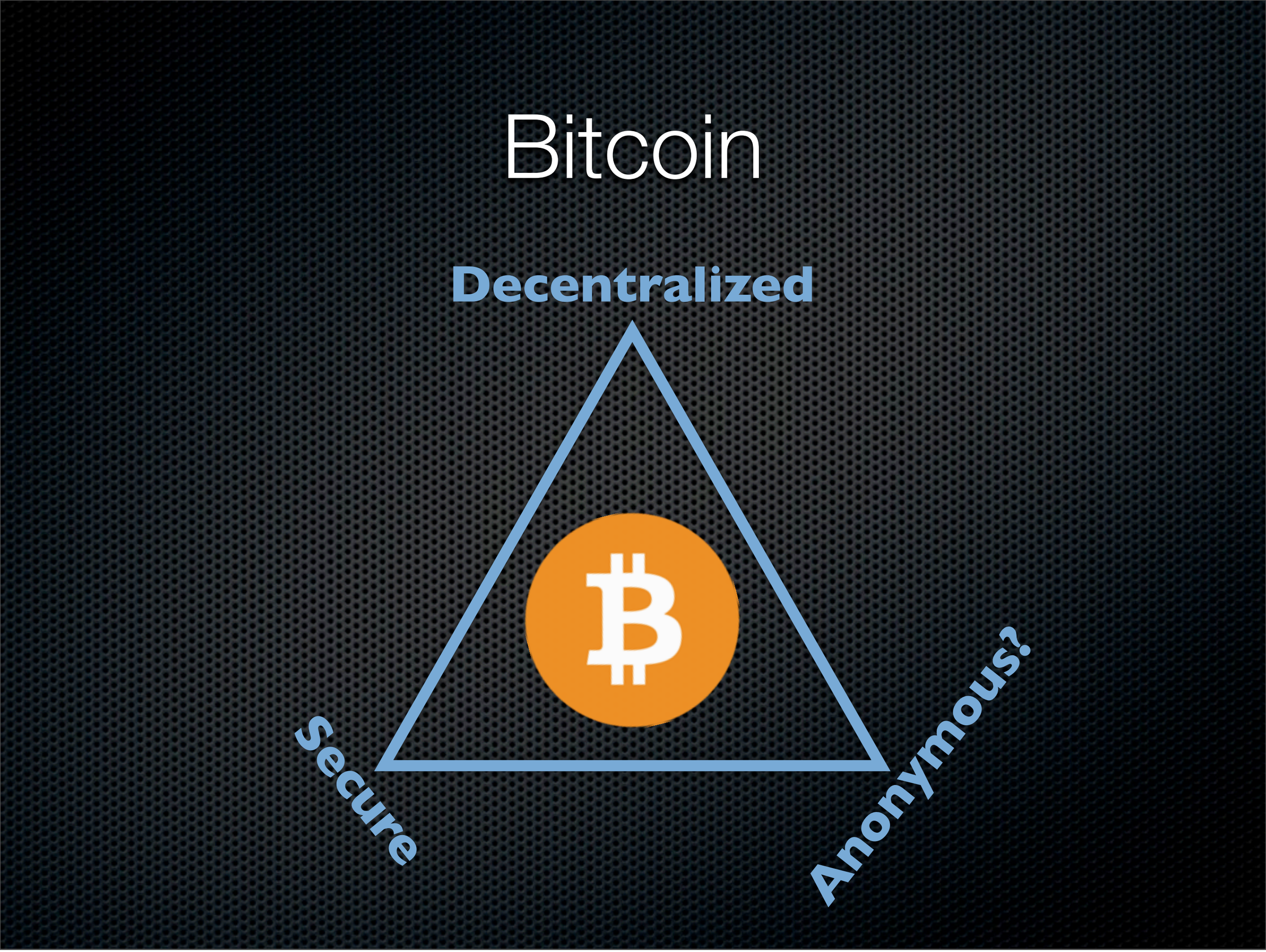
Decentralized



Bitcoin



Bitcoin



Evaluating User Privacy in Bitcoin

Elli Androulaki[1], Ghassan O. Karame[2], Marc Roeschlin[1],
Tobias Scherer[1], and Srdjan Capkun[1]

[1] ETH Zurich, 8092 Zuerich, Switzerland
elli.androulaki@inf.ethz.ch, romarc@student.ethz.ch,
schereto@student.ethz.ch, capkuns@inf.ethz.ch
[2] NEC Laboratories Europe, 69115 Heidelberg, Germany
ghassan.karame@neclab.eu

Abstract. Bitcoin is quickly emerging as a popular digital payment system. However, in spite of its reliance on pseudonyms, Bitcoin raises a number of privacy concerns due to the fact that all of the transactions that take place are publicly announced in the system.
In this paper, we investigate the privacy provisions in Bitcoin when it is used as a primary currency to support the daily transactions of individuals in a university setting. More specifically, we evaluate the privacy that is provided by Bitcoin *(i)* by analyzing the genuine Bitcoin system and *(ii)* through a simulator that faithfully mimics the use of Bitcoin within a university. In this setting, our results show the profiles of almost 40% of the users can be, to a large extent, recovered. Users adopt privacy measures recommended by Bitcoin. To the best of our knowledge, this is the first work that comprehensively analyzes, and
of Bitcoin.
across a

Quantitative Analysis of the Full Bitcoin Transaction Graph

Dorit Ron and Adi Shamir

Department of Computer Science and Applied Mathematics,
The Weizmann Institute of Science, Israel
{dorit.ron,adi.shamir}@weizmann.ac.il

Abstract. The Bitcoin scheme is a rare example of a large scale global payment system in which all the transactions are publicly accessible (but in an anonymous way). We downloaded the full history of this scheme, and analyzed many statistical properties of its associated transaction graph. In this paper we answer for the first time a variety of interesting questions about the typical behavior of users, how they acquire and how they spend their bitcoins, the balance of bitcoins they keep in their accounts, and how they move bitcoins between their various accounts in order to better protect their privacy. In addition, we isolated all the large transactions in the system, and discovered that almost all of them are closely related to a single large transaction that took place in November 2010, even though the associated users apparently tried to hide this fact with many strange looking long chains and fork-merge structures in the

ic cash, payment systems, trans-

Quantitati

Departm

elli

Abstract

payment
in an an
and ana
graph.
ing que
how th
accou
order
trans
clos
201
wi

An Analysis of Anonymity in the Bitcoin System

This blog is written by Fergal Reid and Martin Harrigan. We are researchers with the Clique Research Cluster at University College Dublin. The results in this blog are based on a paper we wrote that considers anonymity in the Bitcoin system. A preprint of the paper is available on arXiv.

Update (January 1, 2013): We received many requests for an up to date, human-readable copy of the block chain, which can be difficult to extract using existing tools. One of the authors, Martin Harrigan, has released QuantaBytes to this end. It provides up to date copies of the block chain along with tools for analysis and visualization. Check it out!

Friday, September 30, 2011

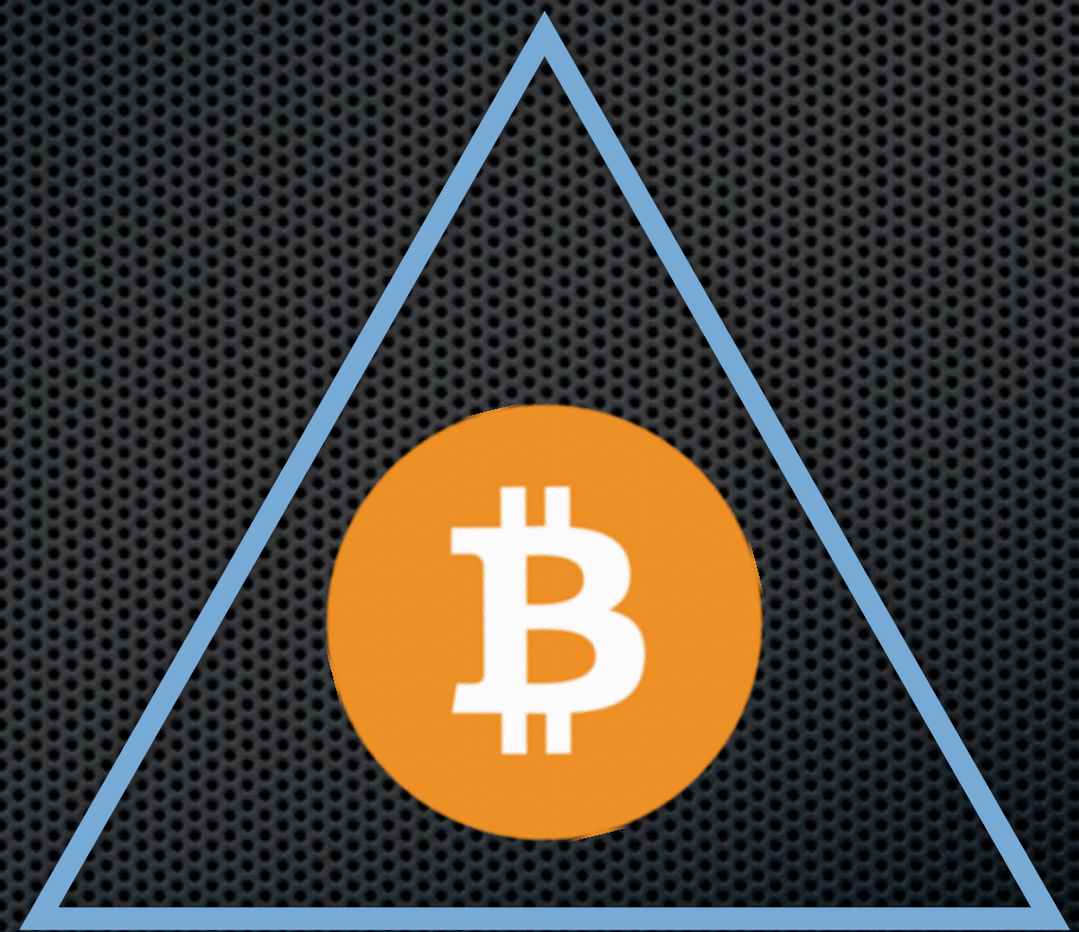
Bitcoin is not Anonymous

TL;DR

Bitcoin is not inherently anonymous. It may be possible to conduct transactions is such a way so as to obscure your identity, but, in many cases, users and their transactions can be identified. We

Bitcoin

Decentralized



Secure

~~Anonymous~~

Bitcoin: all of your information is **known to** ~~the bank~~ the merchants **EVERYONE**

Chaum's e-cash + Bitcoin

~~Decentralized~~

Secure

Anonymous

Bitcoin laundries & mixes

~~Decentralized~~

Secure

~~Anonymous~~

Zerocoin

- A distributed approach to private electronic cash
- Extends Bitcoin by adding an anonymous currency on top of it
- Zerocoins are exchangeable for bitcoins
- Similar to techniques by Sander and Ta-shma

What is a zerocoin?

- A zerocoin is:
  - Economically: a promissory note redeemable for a bitcoin
  - Cryptographically: an opaque envelope containing a serial number used to prevent double spending

8238482734710

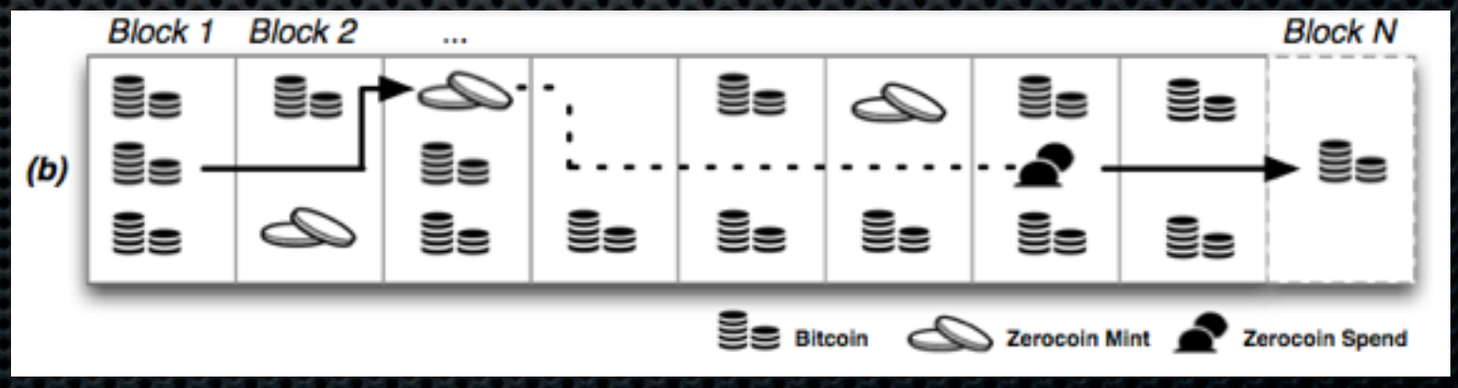
Commitments

- Allow you to commit to and later reveal a value
- Binding: value cannot be tampered with
- Blinding: value cannot be read until revealed
- We use Pedersen commitments

$$C = g^x h^r \bmod q$$

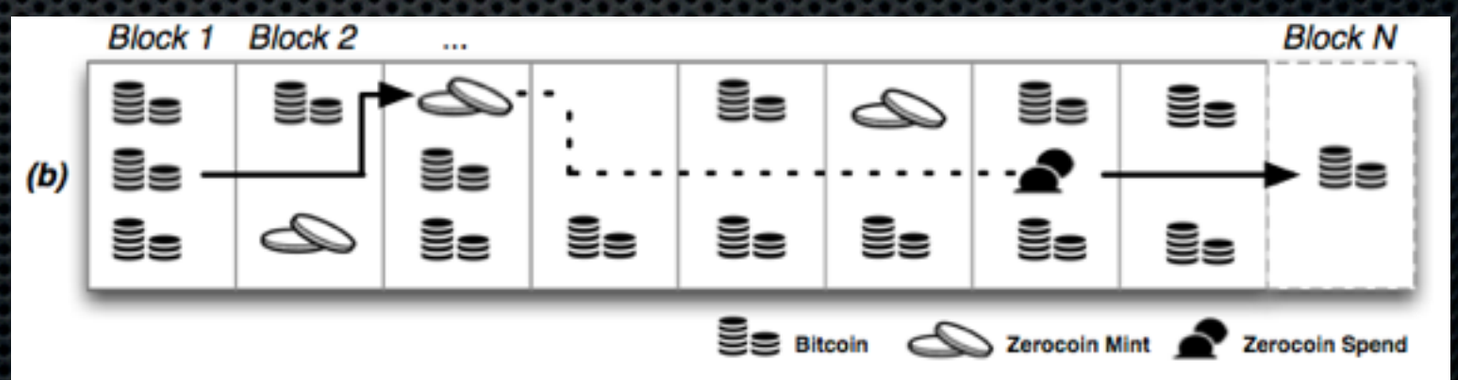
Zerocoins: where do they come from?

- Anyone can make one
- Choose a random serial number and commit to it
- Mint a zerocoin by putting a mint transaction in the block chain which “spends” a bitcoin and includes the commitment
- Spending a zerocoin gives the recipient a bitcoin



Zerocoins: ...and where do they go?

- The “spent” bitcoins end up escrowed
- To spend a zerocoin
  - You reveal the serial number
  - Prove it is from some zerocoin in the block chain
  - Put the spent serial number in the block chain



Zero-knowledge proofs

- Zero-knowledge [Goldwasser, Micali 1980s, and beyond]
- Prove knowledge of a witness satisfying a statement
- Specific variant: non-interactive proof of knowledge
- Here we prove we know:
  1. The serial number of a zerocoin
  2. That the coin is in the block chain

An inefficient approach

- Inefficient proof
  - Identify all valid zerocoins in the block chain (call them $C_1 \ldots C_N$)
  - Prove that S is the serial number of a coin C and $C = C_1 \vee C = C_2 \vee \ldots C_N$
  - This “OR” proof is O(N)

Cryptographic accumulators

- Allow constant size set membership proofs
- Strong RSA accumulator originally due to Benaloh and de Mare
- Efficient proof for accumulation of primes proposed by Camenisch and Lysyanskaya ‘01

$$N = p \cdot q, u \in QR_N \, (u \neq 1)$$

$$A = u^{c_1 \cdot c_2 \cdot \ldots c_n} \bmod N$$

$$w_i = u^{c_1 \cdot c_2 \cdot c_{i-1} \cdot c_{1+1} \cdot \ldots \ldots c_n} \bmod N$$

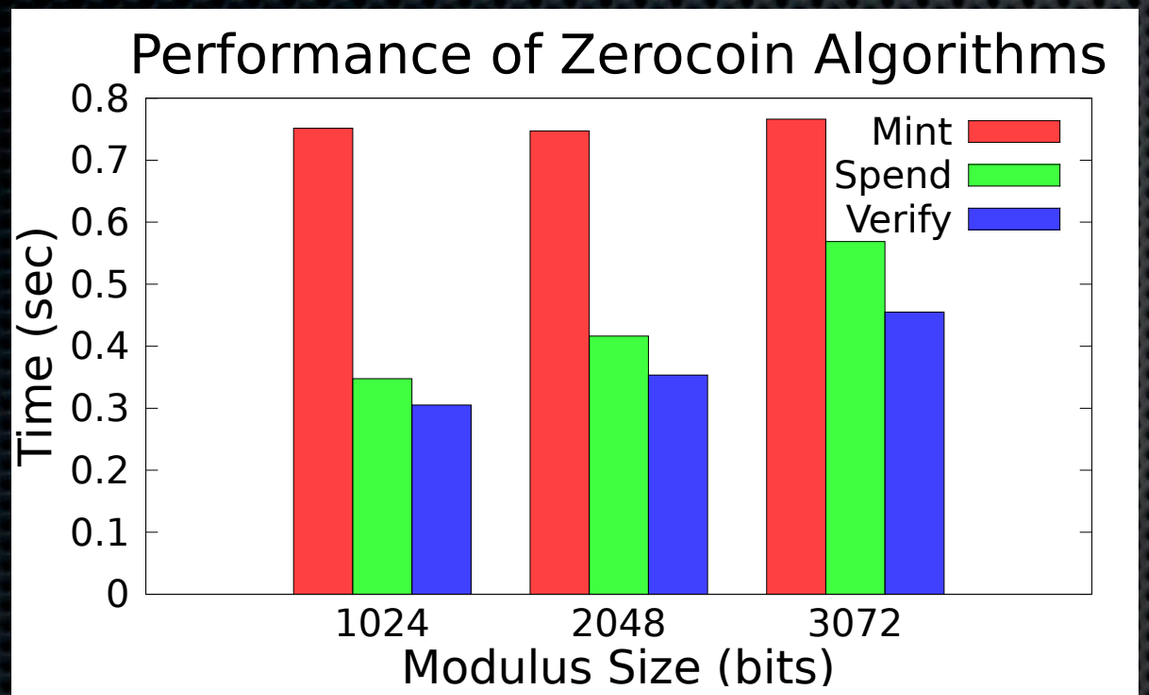
Zerocoin protocol

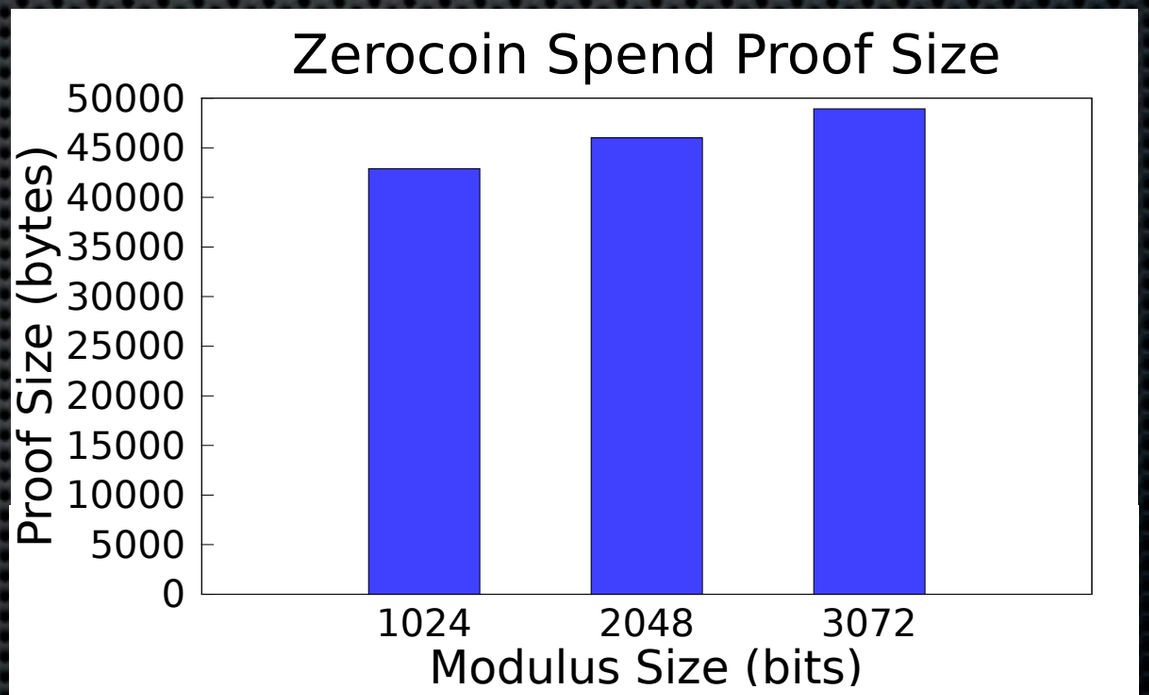
- Generate a commitment to a random serial number S:

$$\text{C} = g^s h^r \bmod q \quad \text{where C is prime}$$

- (Store serial number S and randomness r)
- Accumulate all valid coins, compute witness w_i
- Reveal S and prove knowledge of witness to commitment accumulation and its randomness r

Performance





Modified **BITCOIND** client on 3.5GZ Intel Xeon E3-1270V2

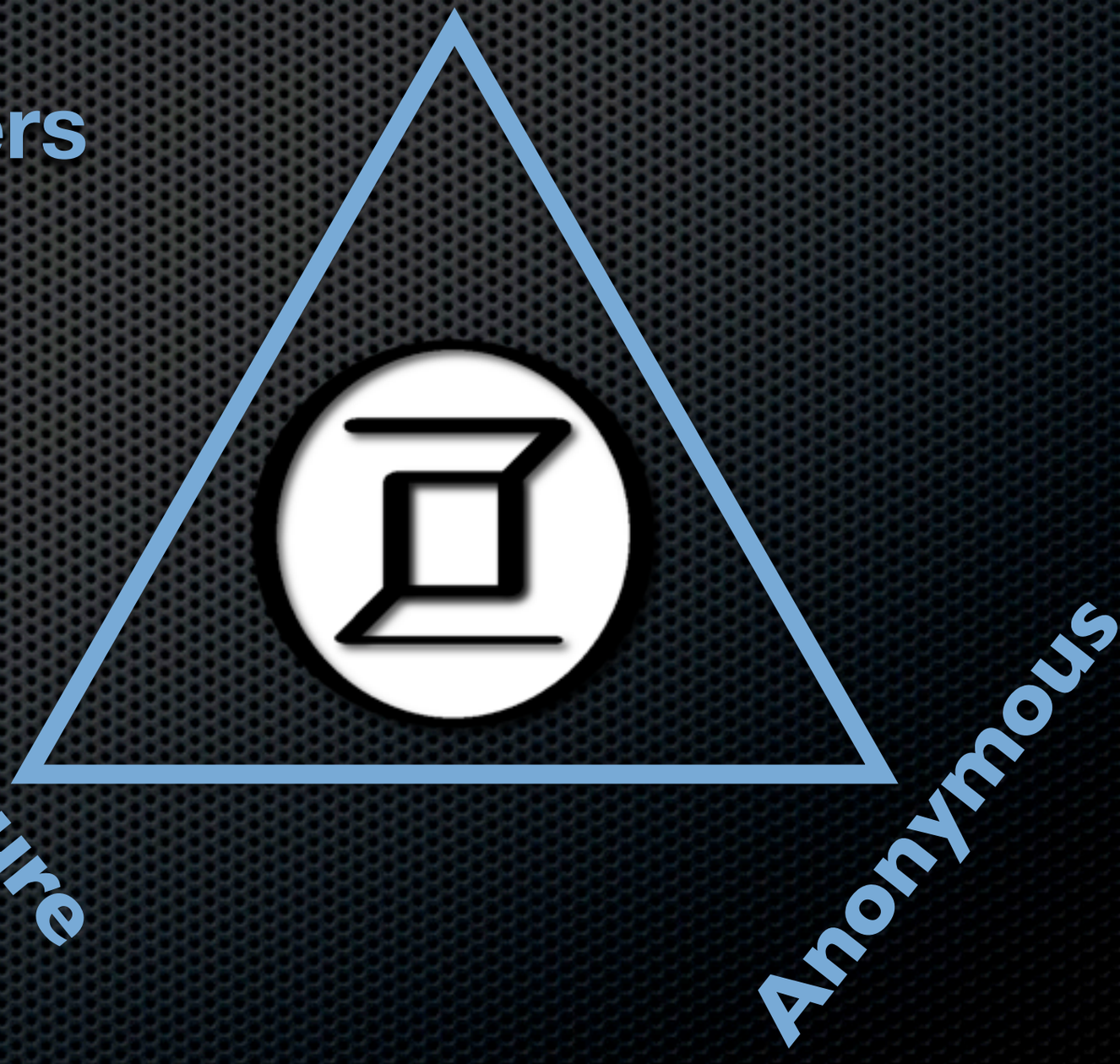
- 1024 bit commitments
- 1024, 2048, and 3072 bit RSA moduli

Obstacles and future work

- Scale to larger networks
- Reduce proof size (duh)
- Make divisible coins (we have a construction)
- Get people to believe this works

Zerocoin.org

Ian Miers @imichaelmiers
Christina Garman
Matthew Green
Avi Rubin



Divisible coins (Not in paper)

- Encode both a serial number and a denomination in the coin commitment as the low and high order bits
- To divide a coin C with balance b and serial number S
  - Mint two new coins c',c" with balances b' and b"
  - Prove in zero knowledge that b = b' + b" and those are the high order bits
  - Reveal S to prevent reuse

Prime commitments

Perfectly Blinding

$$\forall s \, \exists r \text{ s.t. } p = g^s h^r \bmod q$$

Binding under discrete log

$$C = g^{x_1} h^{r_1} \wedge C = g^{x_2} h^{r_2}$$

$$g^{x_1} h^{r_1} = g^{x_2} h^{r_2}$$

$$h = g^{\epsilon}$$

$$g^{x_1} g^{\epsilon r_1} = g^{x_2} g^{\epsilon r_2}$$

$$x_1 + r_1 \epsilon = x_2 + r_2 \epsilon$$

$$\log_g(h) = \epsilon = \frac{x_1 - x_2}{r_2 - r_1}$$

How much anonymity

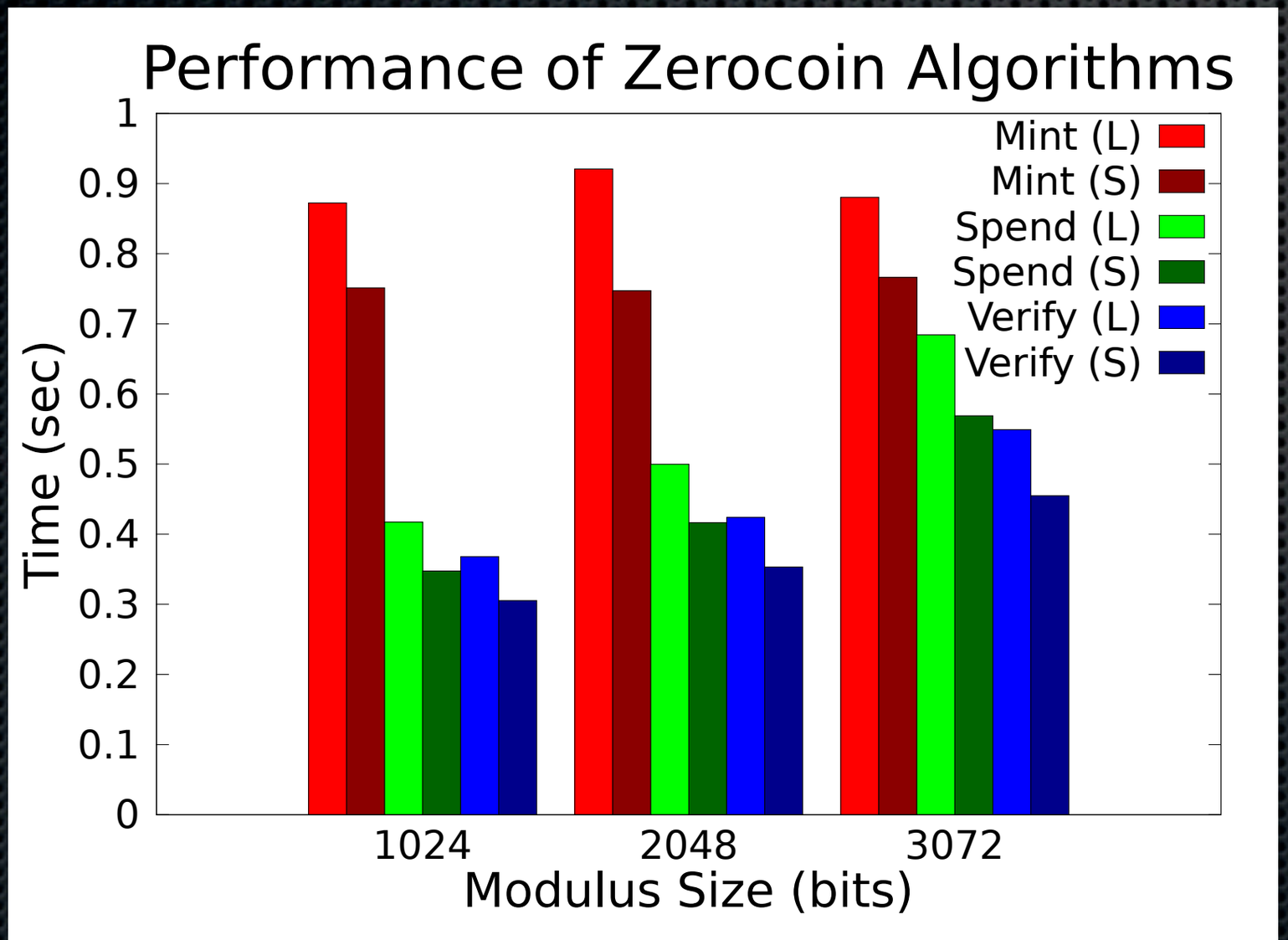
- Consider a universe where 10 coins exist and one more coin is minted and then spent
  - If all 10 original coins are already spent before minting, k =1
    - If only 9 of them are spent, k = 11
- Lower bound: All unspent coins controlled by honest parties
- Upper bound: All the coins

Why so large?

$$SoK[Recipient]\{(coin, w, r) : A = w^{coin} \bmod N \wedge coin = \hat{g}^S \hat{h}^r\}$$

$$SoK[Recipient]\{(w, r) : A = w^{\hat{g}^S \hat{h}^r} \bmod N\}$$

Laptop performance



- Not much slower (our code is single threaded)

In UFOs we trust

- RSA moduli of **U**nknown **F**act**O**rization (Sander99)
- N is an RSA-UFO if it has at least two large prime factors P and Q and no one can find N_1,N_2 such that Q divides N_1 and P divides N_2
- Get an assumption analogous to the Strong RSA assumption

UFOs: Impractically Large

Problem: for the security of a 1024 bit RSA modulus, we need a 40k bit UFO