Zerocoin: Anonymous Distributed E-Cash from Bitcoin

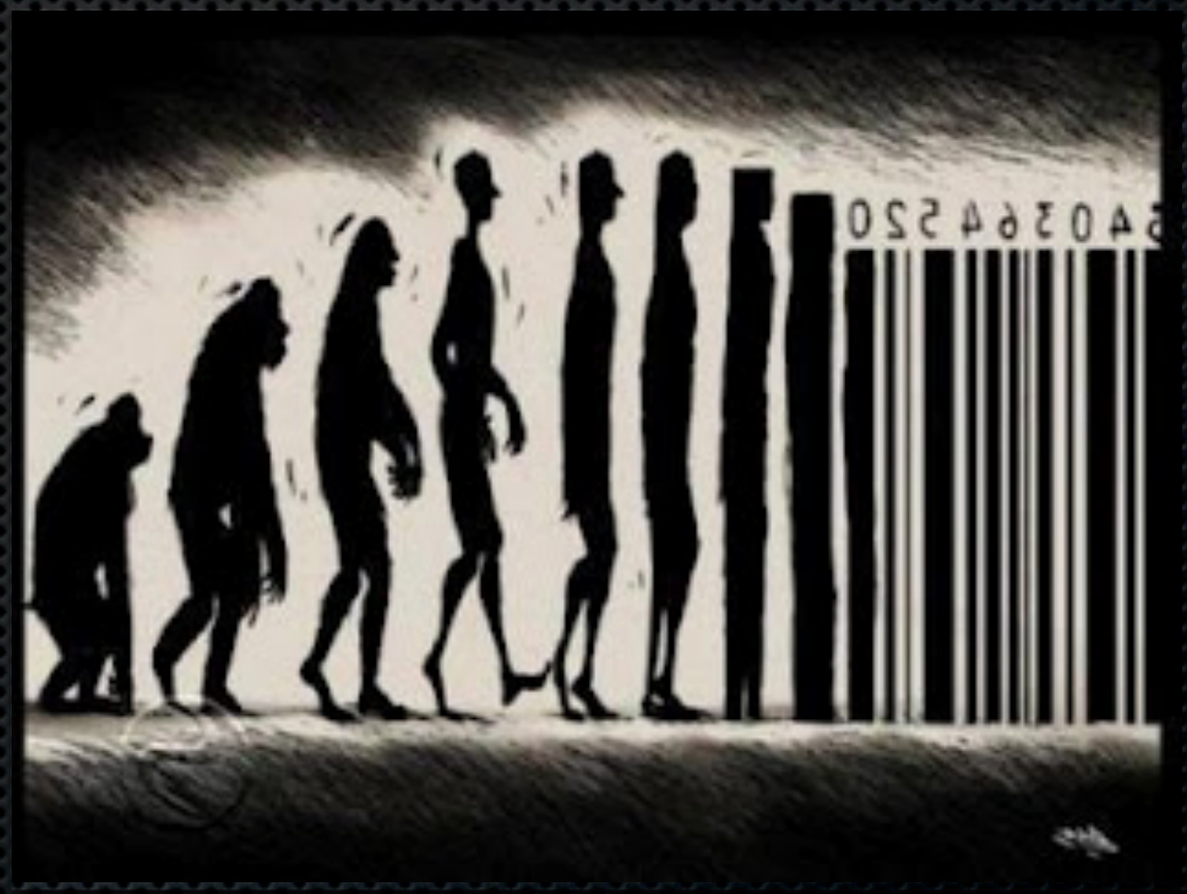
Ian Miers, Christina Garman,
Matthew Green, Avi Rubin

JOHNS HOPKINS
UNIVERSITY

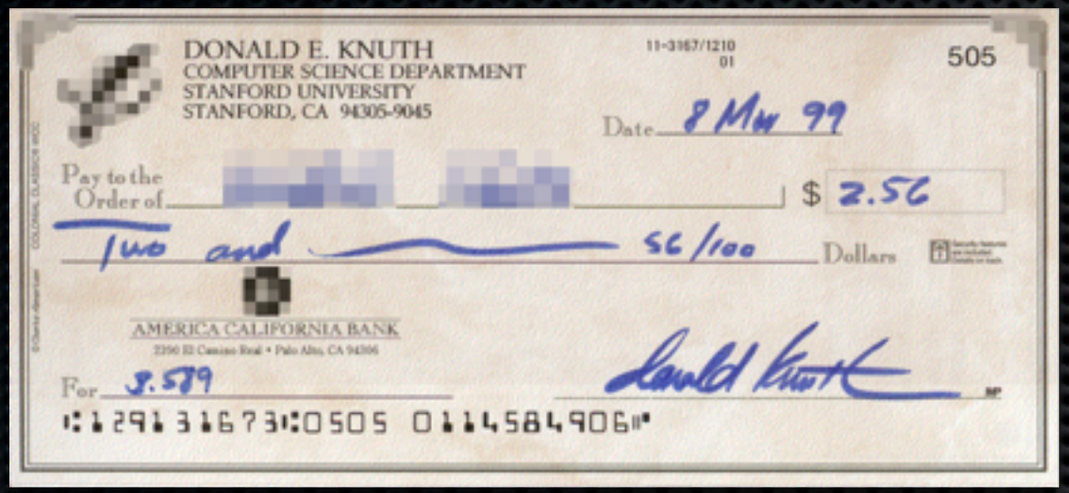
What is money?

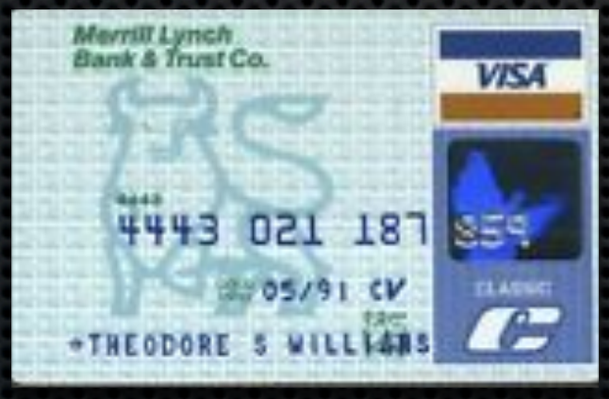
Digitizing money

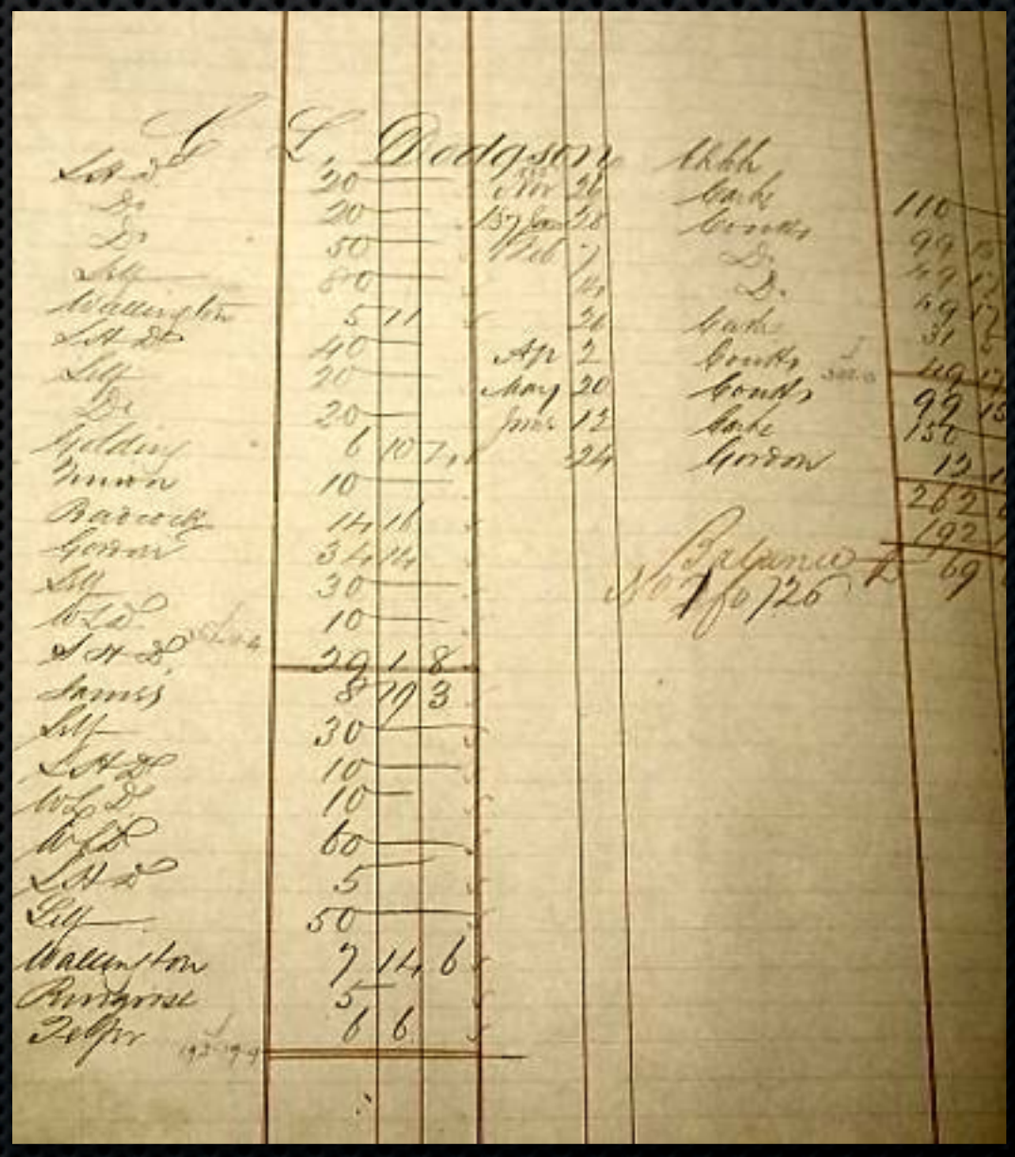
- Two ways to do it
  - Create digital cash
  - Create digital checks



Bank accounts







Problem: privacy

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

Digital cash

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

E-cash schemes

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

An ideal digital currency

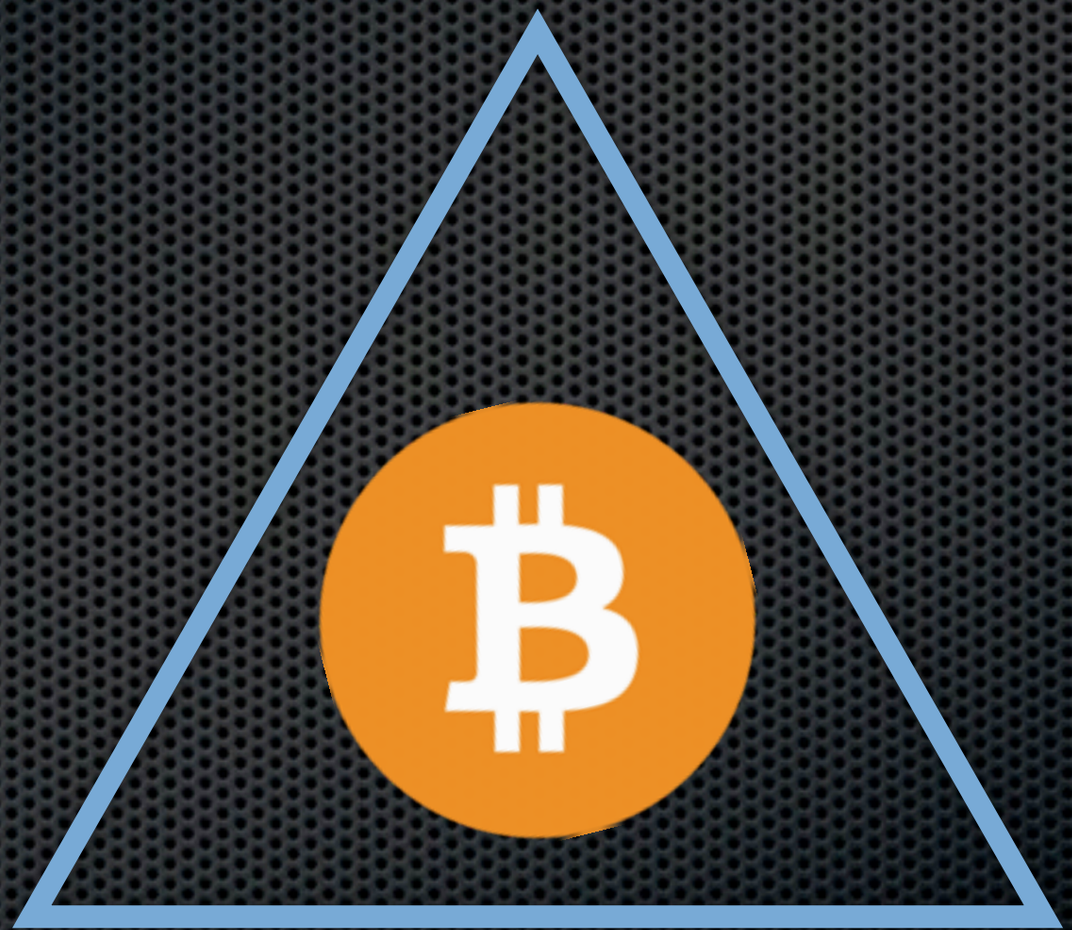
Bitcoin

- A distributed digital currency system
- Released by Satoshi Nakamoto 2008
- Market cap of 1.2 Billion USD (as of early May 2013)

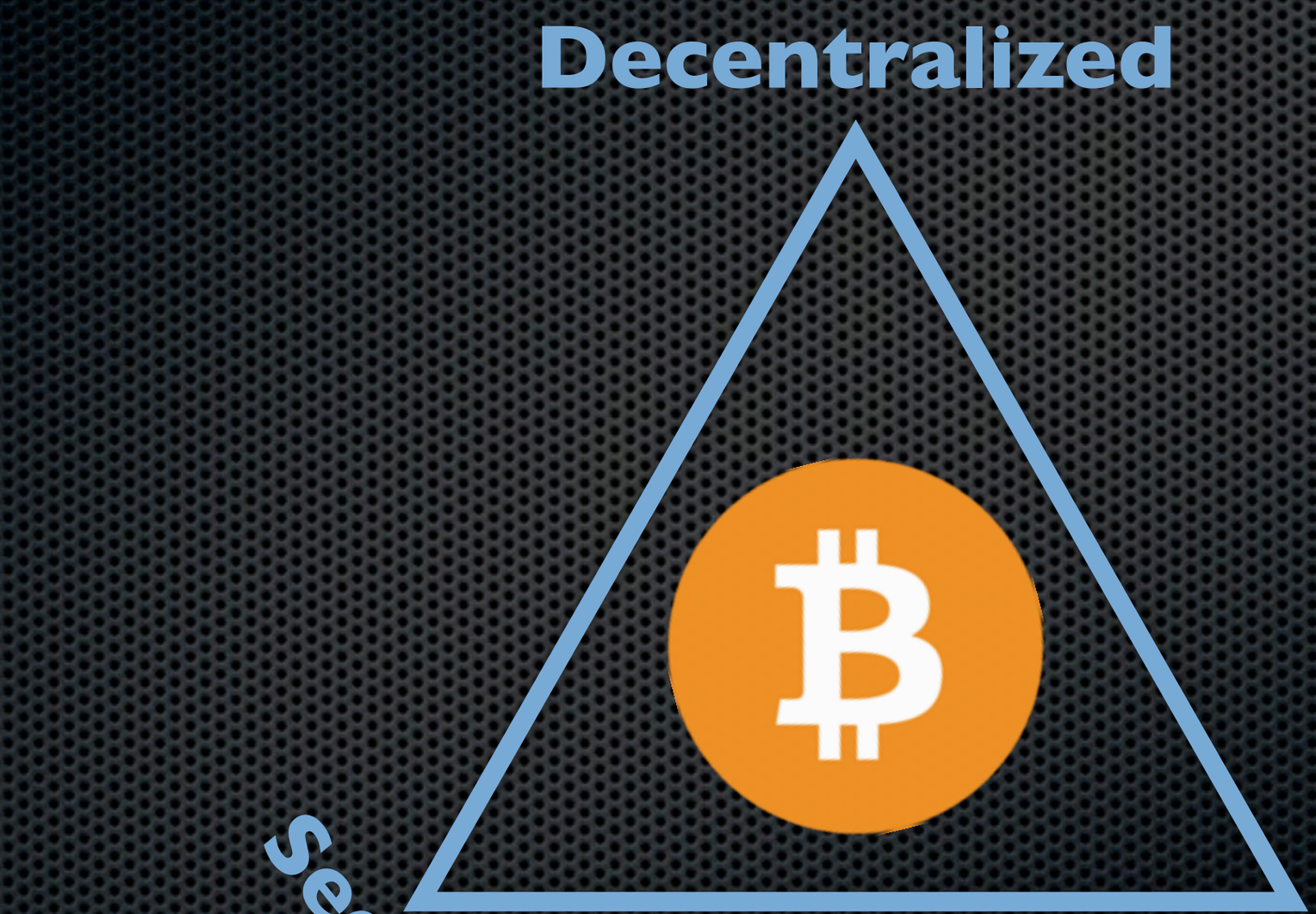
- Effectively a bank run by an ad hoc network
  - Digital checks
  - A distributed transaction log

Bitcoin

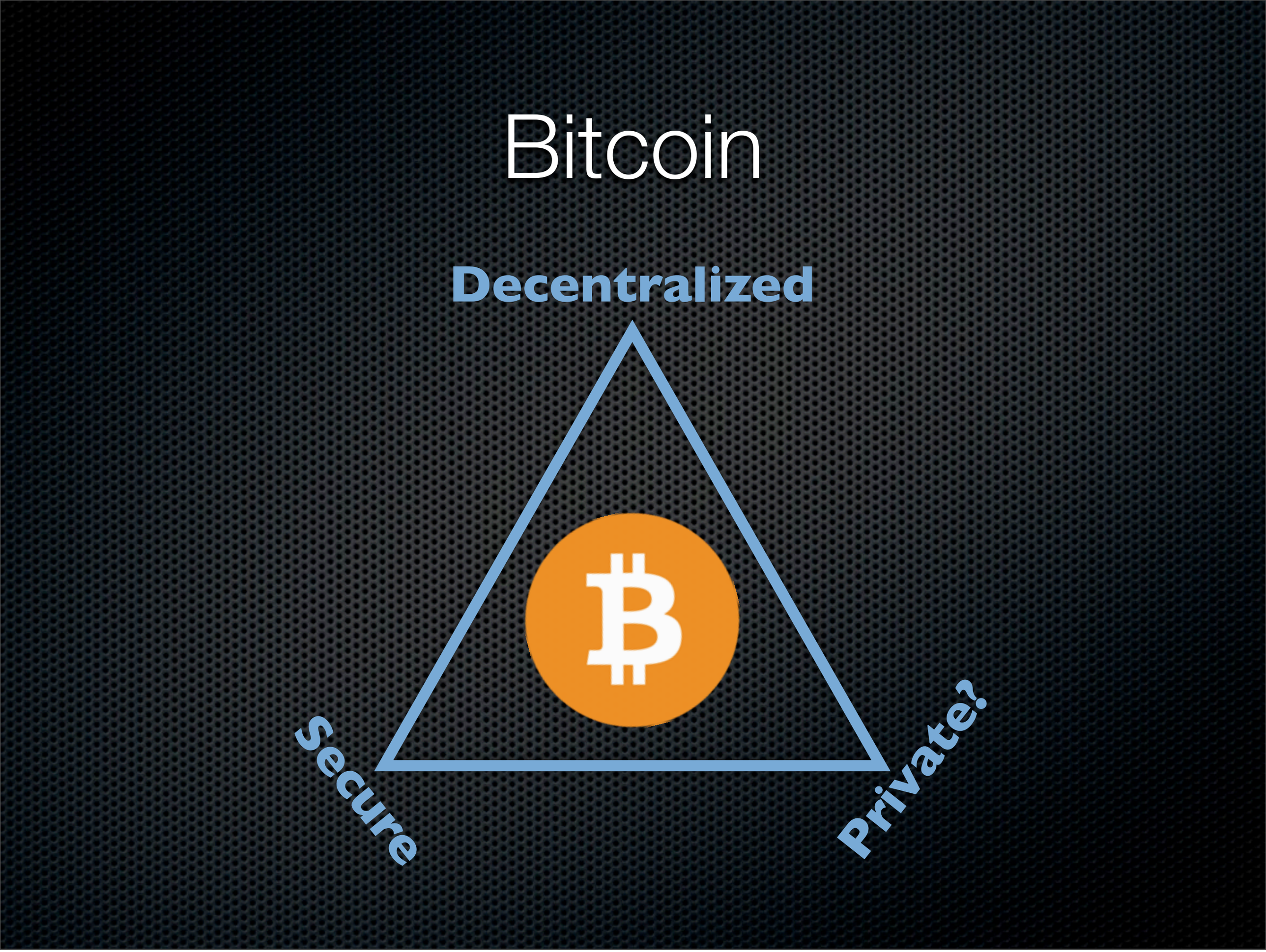
Decentralized



Bitcoin

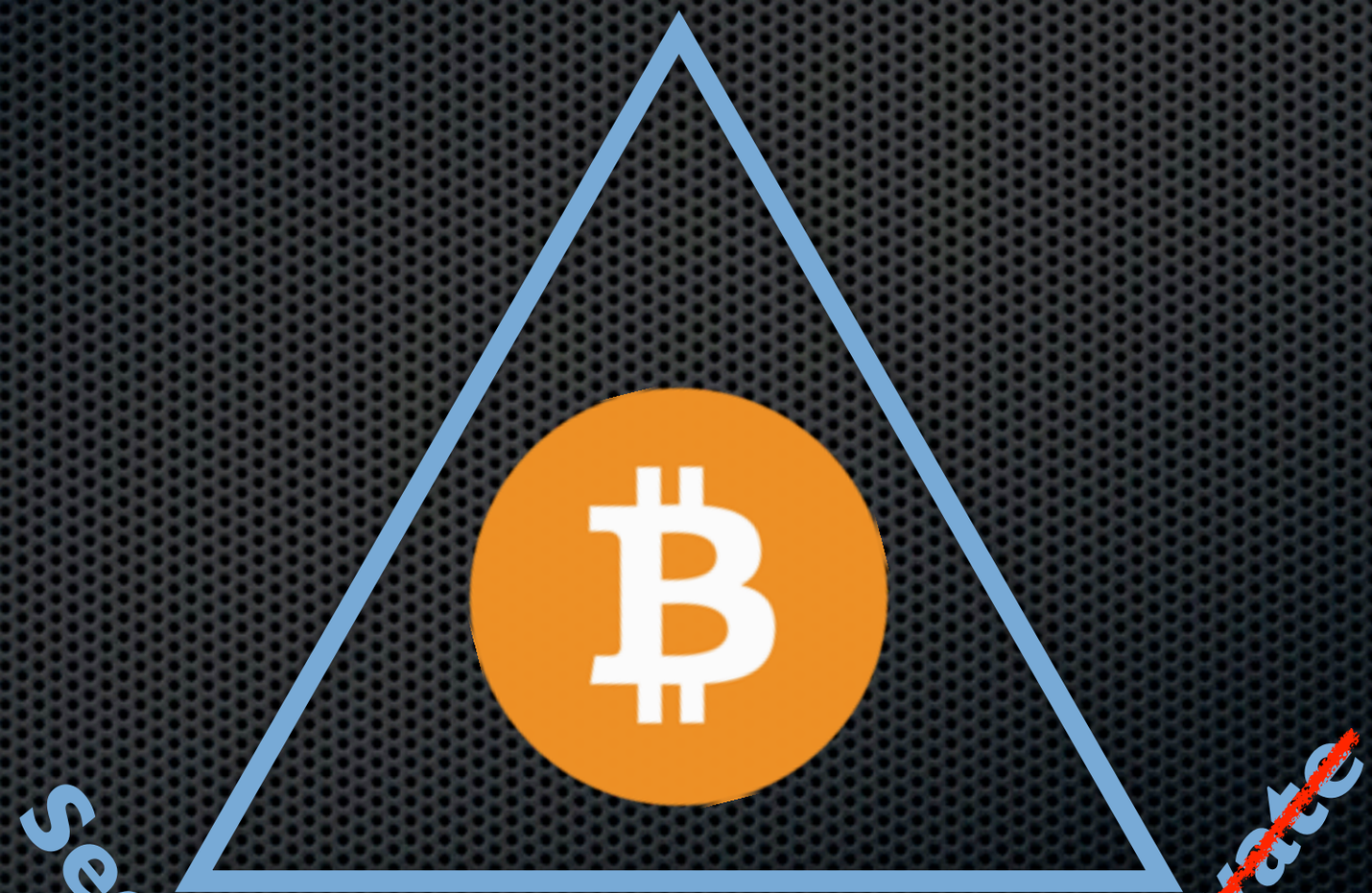


Bitcoin



Bitcoin

Decentralized



Secure

~~Private~~

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 that the profiles of almost 40% of the users can be, to a large extent, recovered if users adopt privacy measures recommended by Bitcoin. To the best of our knowledge, this is the first work that comprehensively analyzes, and

of Bitcoin.

gross 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

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

Data mining and privacy

- Target used data mining on customer purchases to identify pregnant women and target ads at them (NYT 2012)
  - Ended up informing a woman's father that his teenage daughter was pregnant
- Imagine what credit card companies could do with the data

Chaum's e-cash + Bitcoin

~~Decentralized~~

Secure

Private

Bitcoin laundries

~~Decentralized~~

Secure

~~Private~~

Zerocoin

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

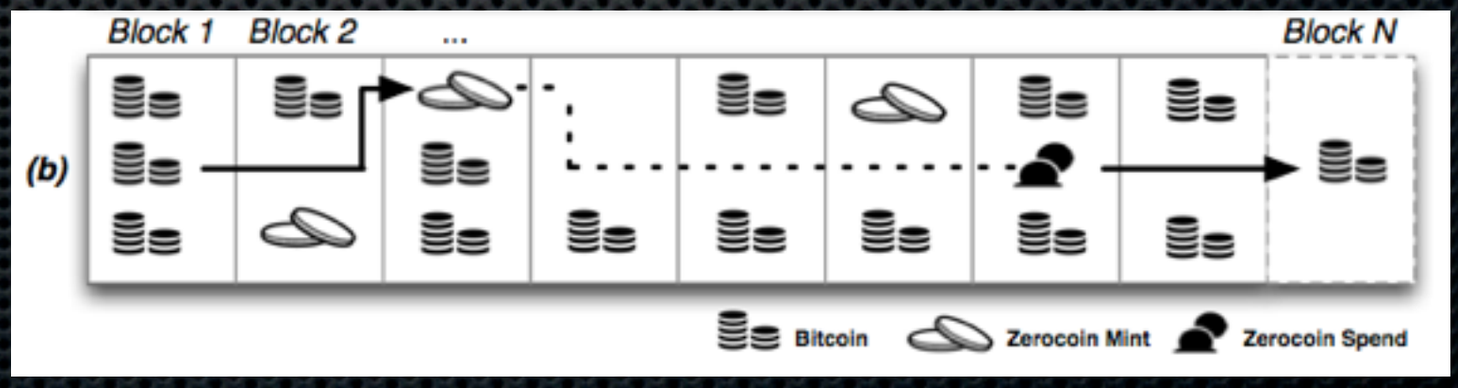
What is a zerocoin?

- 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

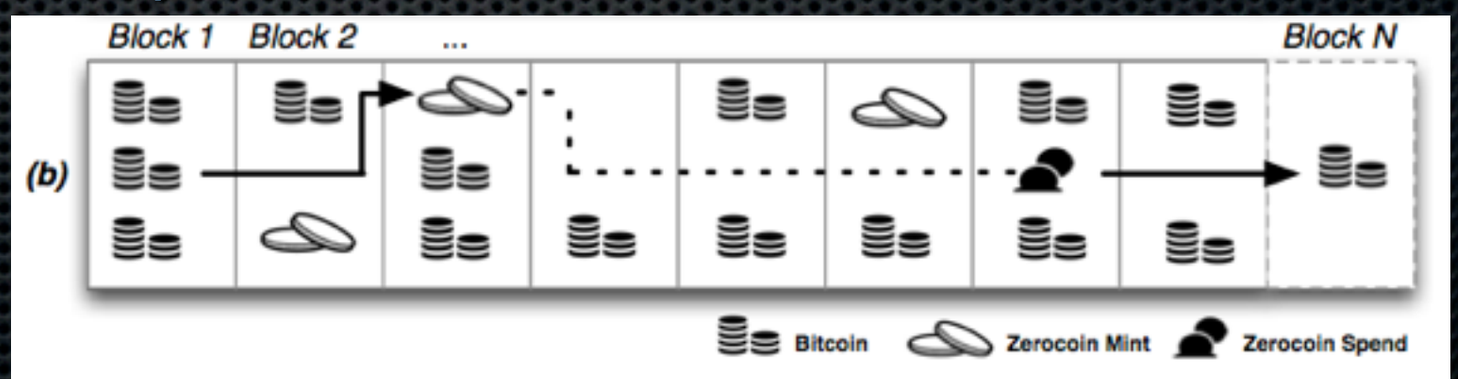
Zerocoins: where do they come from?

- Anyone can make one
- Create an envelope containing a random serial number
- Mint a zerocoin by putting a mint transaction in the block chain which “spends” a bitcoin
- Spending a zerocoin gets you back a bitcoin



Zerocoins: ...and where do they go?

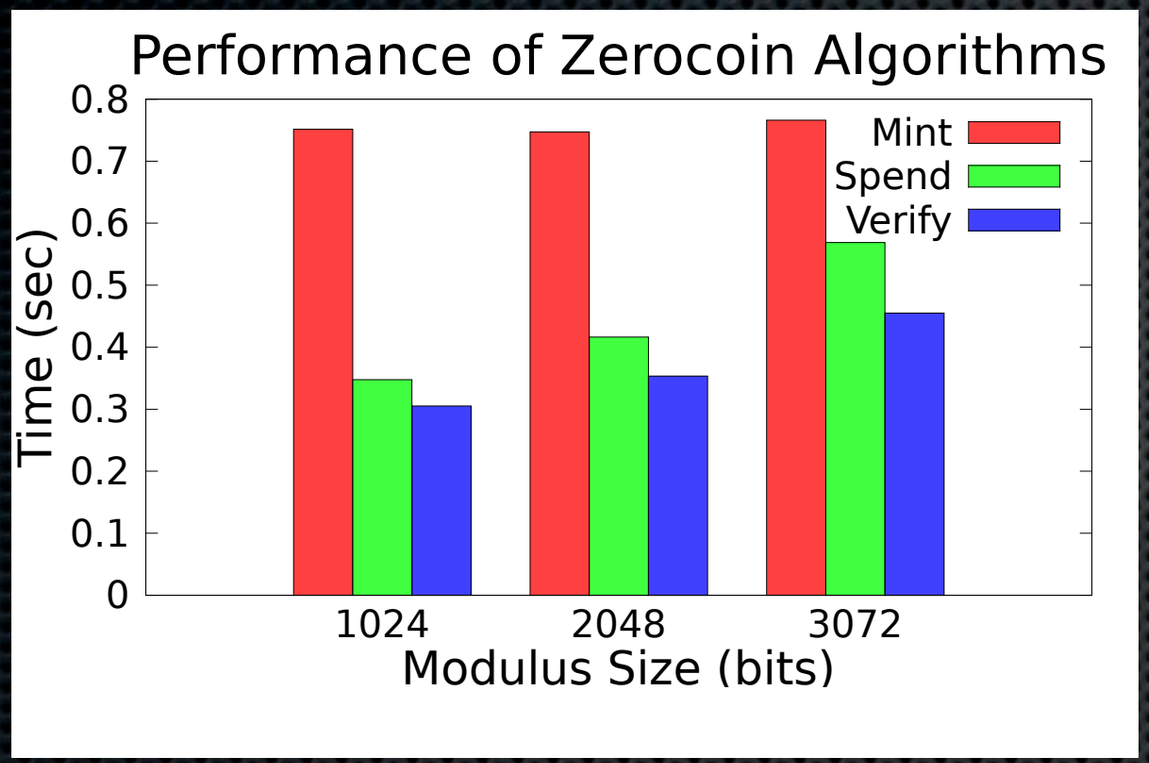
- The “spent” bitcoins end up escrowed
- To spend a zerocoin, you reveal the serial number and prove it is from some zerocoin in the block chain
- The serial number is marked as spent in the block chain
- The recipient gets back a random bitcoin from the escrow pool

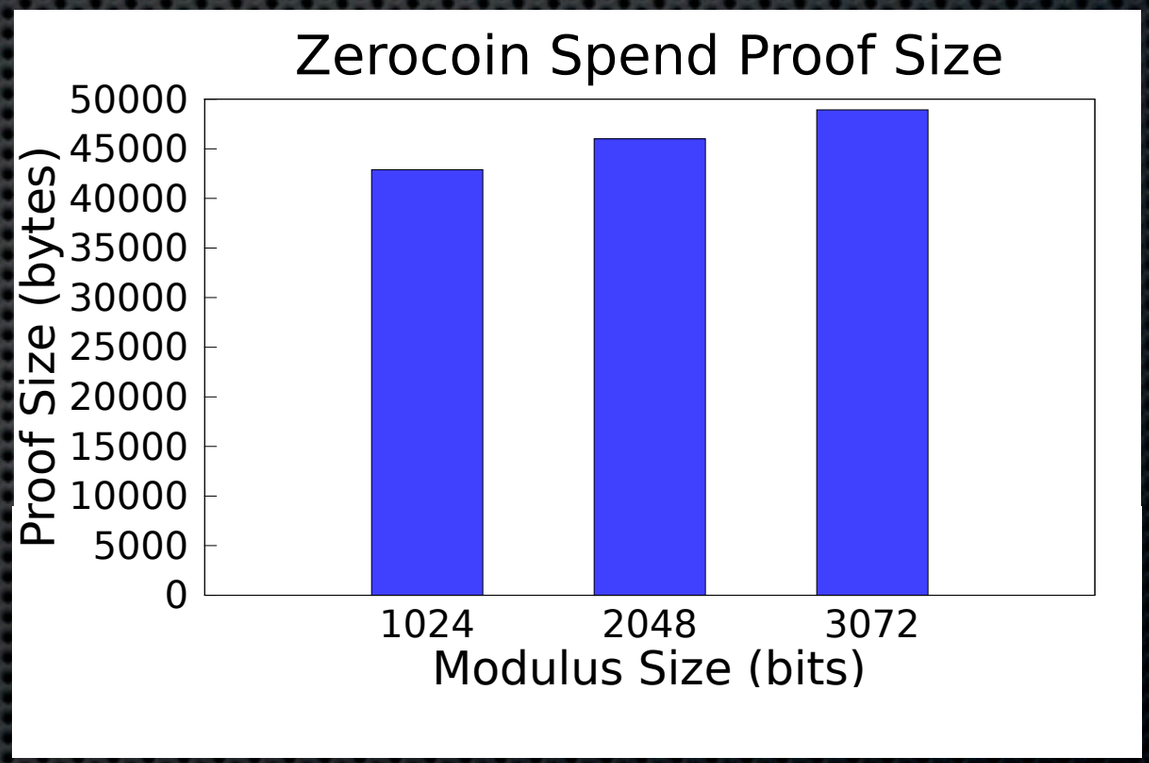


Zero-knowledge proofs

- 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

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

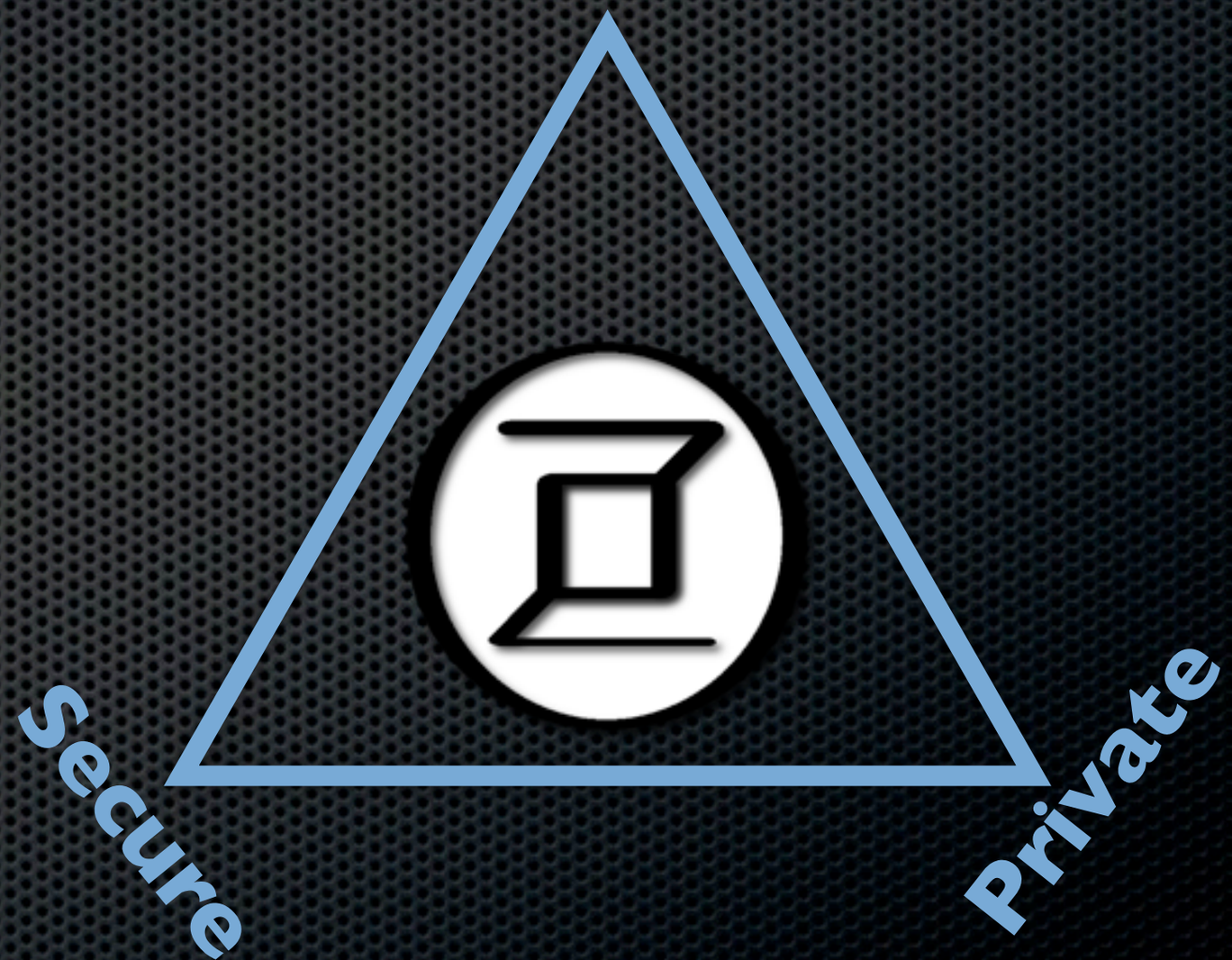
- Scale to larger networks
- Reduce proof size (duh)
- Make divisible coins (we have a construction)
- Get people to believe this works

How does this get adopted?

- How does this get adopted?
  - As part of Bitcoin?
  - As part of an alternative currency?
- Where do we store the proofs?
  - Do people care if they go away?
  - Can you meaningfully verify anonymous transactions?
- How to explain Zerocoin to people?

Zerocoin

zerocoin.org



Follow @zerocoinproject

Ian Miers|Christina Garman|Matthew Green|Avi Rubin

http://zerocoin.org/