Zerocoin: Anonymous Distributed e-Cash from Bitcoin

or

'How will Satoshi Nakamoto spend his fortune?'

Matthew Green
Johns Hopkins University

(Joint work with Ian Miers, Christina Garman, Avi Rubin)

What is money?

Definition of **money** (n)

bing.com · Bing Dictionary

mon·ey [múnnee]

1. medium of exchange: a medium of exchange issued by a government or other public authority in the form of coins of gold, silver, or other metal, or paper bills, used as the measure of the value of goods and services
2. denomination: a form or denomination of coin or paper money
3. somebody's coins and bills: the amount of coins and bills in somebody's possession

Synonyms: cash, currency, ready money, ready cash, change, ready, coins, coinage, dosh, greenbacks, dough, bread, bucks

What is money?

WIKIPEDIA
The Free Encyclopedia

Money

From Wikipedia, the free encyclopedia

For other uses, see Money (disambiguation).

Money is any object or record that is generally accepted as payment for goods and services and repayment of debts in a given socio-economic context or country.[1][2][3] The main functions of money are distinguished as: a medium of exchange; a unit of account; a store of value; and, occasionally in the past, a standard of deferred payment.[4][5] Any kind of object or secure verifiable record that fulfills these functions can be considered money.

What is money?

WIKIPEDIA
The Free Encyclopedia

Money

From Wikipedia, the free encyclopedia

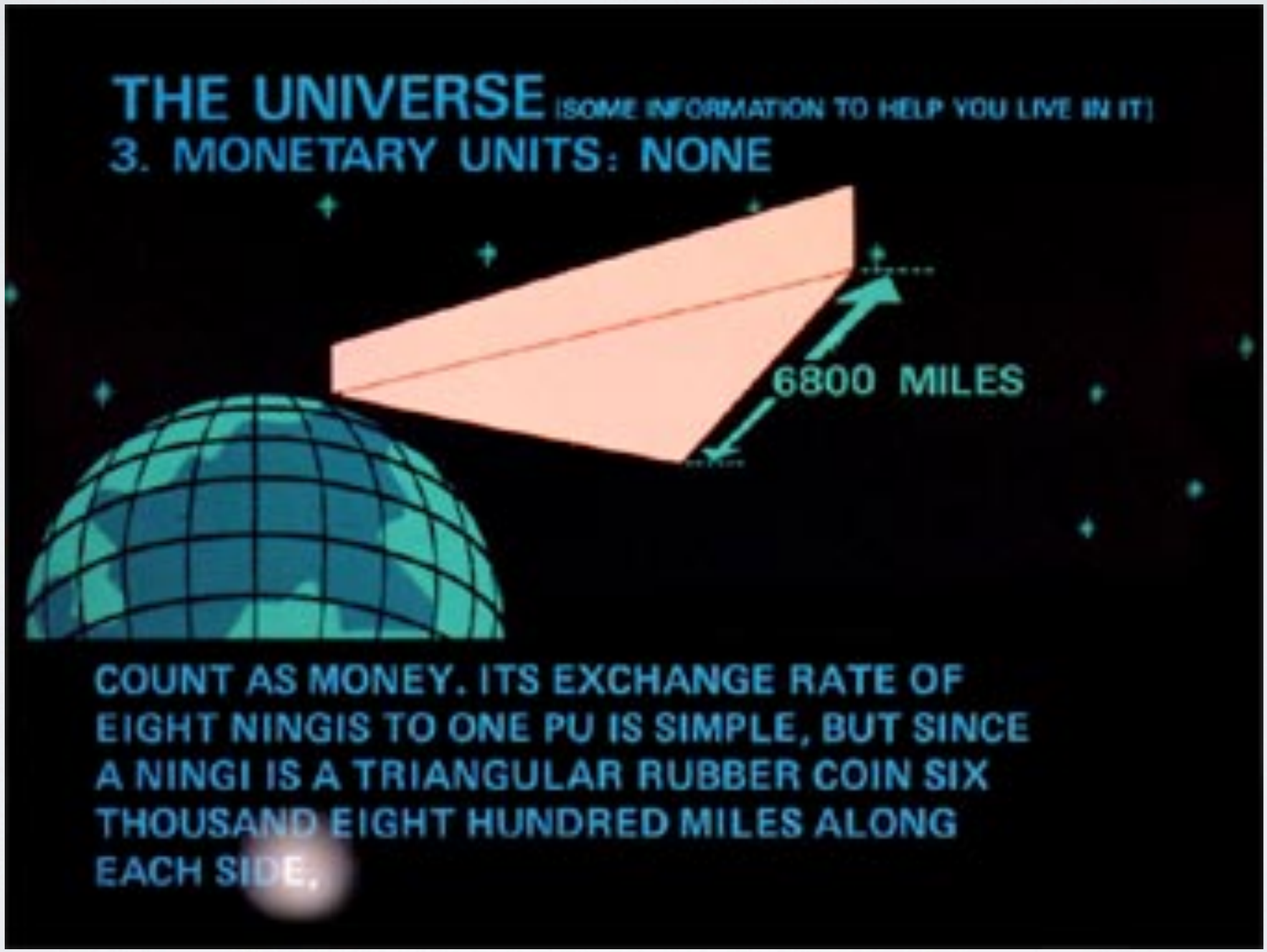
For other uses, see Money (disambiguation).

Money is any object or record that is generally accepted as payment for goods and services and repayment of debts in a given socio-economic context or country.[1][2][3] The main functions of money are distinguished as: a medium of exchange; a unit of account; a store of value; and, occasionally in the past, a standard of deferred payment.[4][5] Any kind of object or secure verifiable record that fulfills these functions can be considered money.

- **Limited quantity**
- **Widely accepted**
- **Easy to transfer**

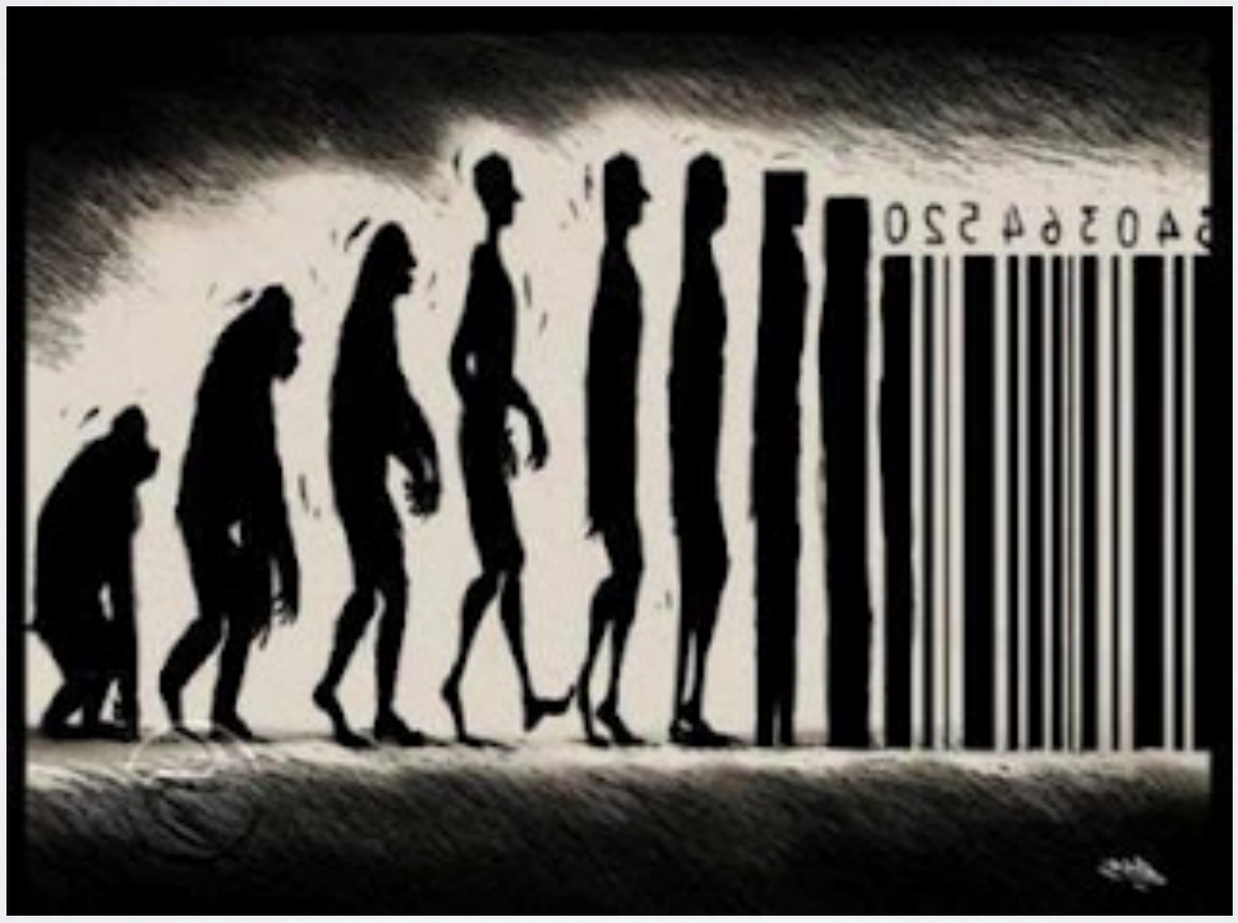
What is money?

What is money?



Problem: electronic money

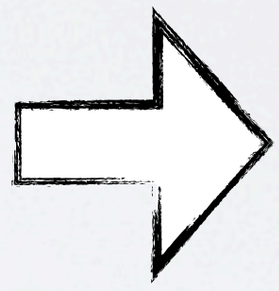
1) Very difficult
2) Very simple



Naive approach

1) Very difficult

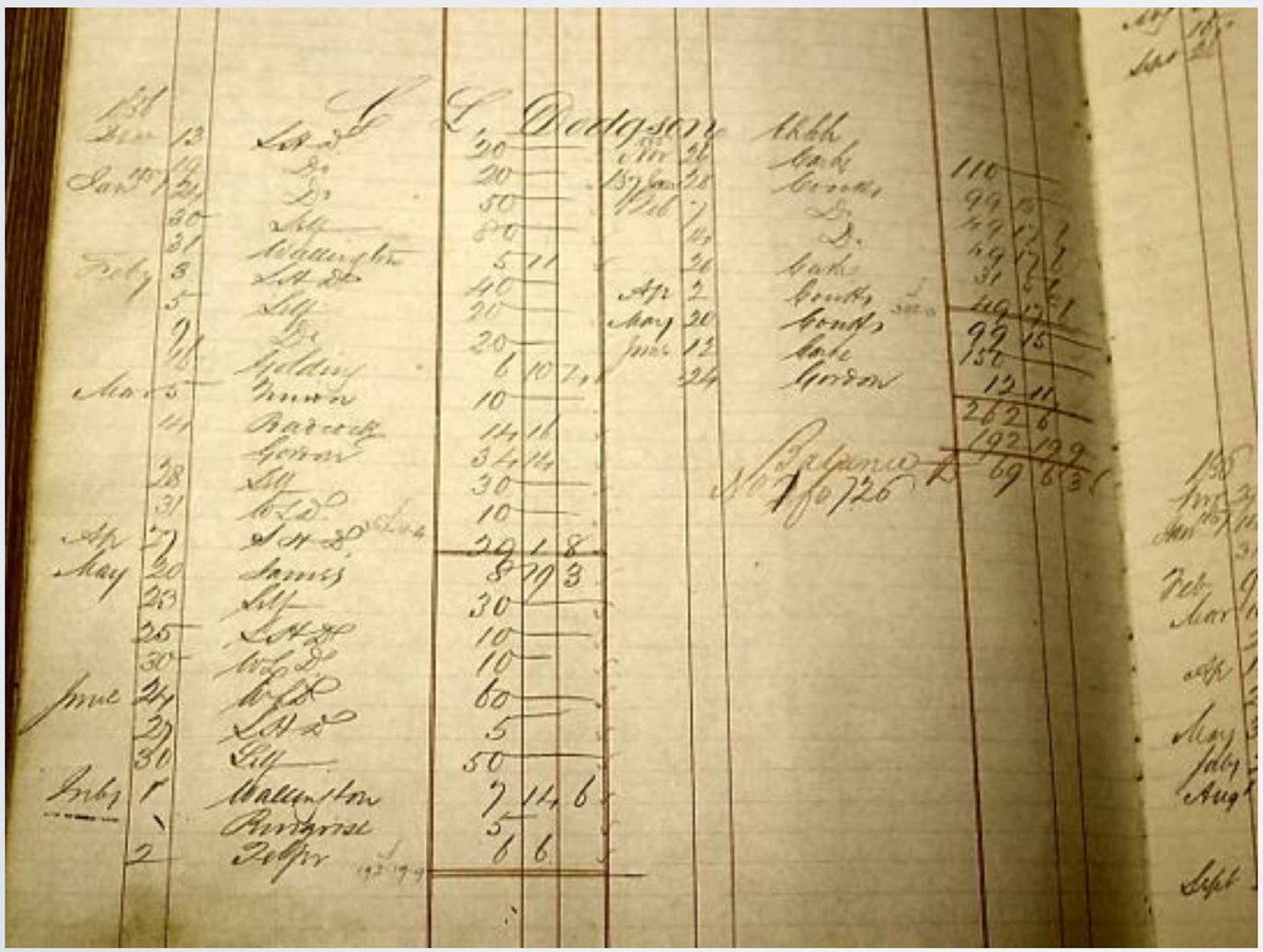
2) Very simple



Account-based approach

1) Very difficult

2) Very simple



Account-based approach

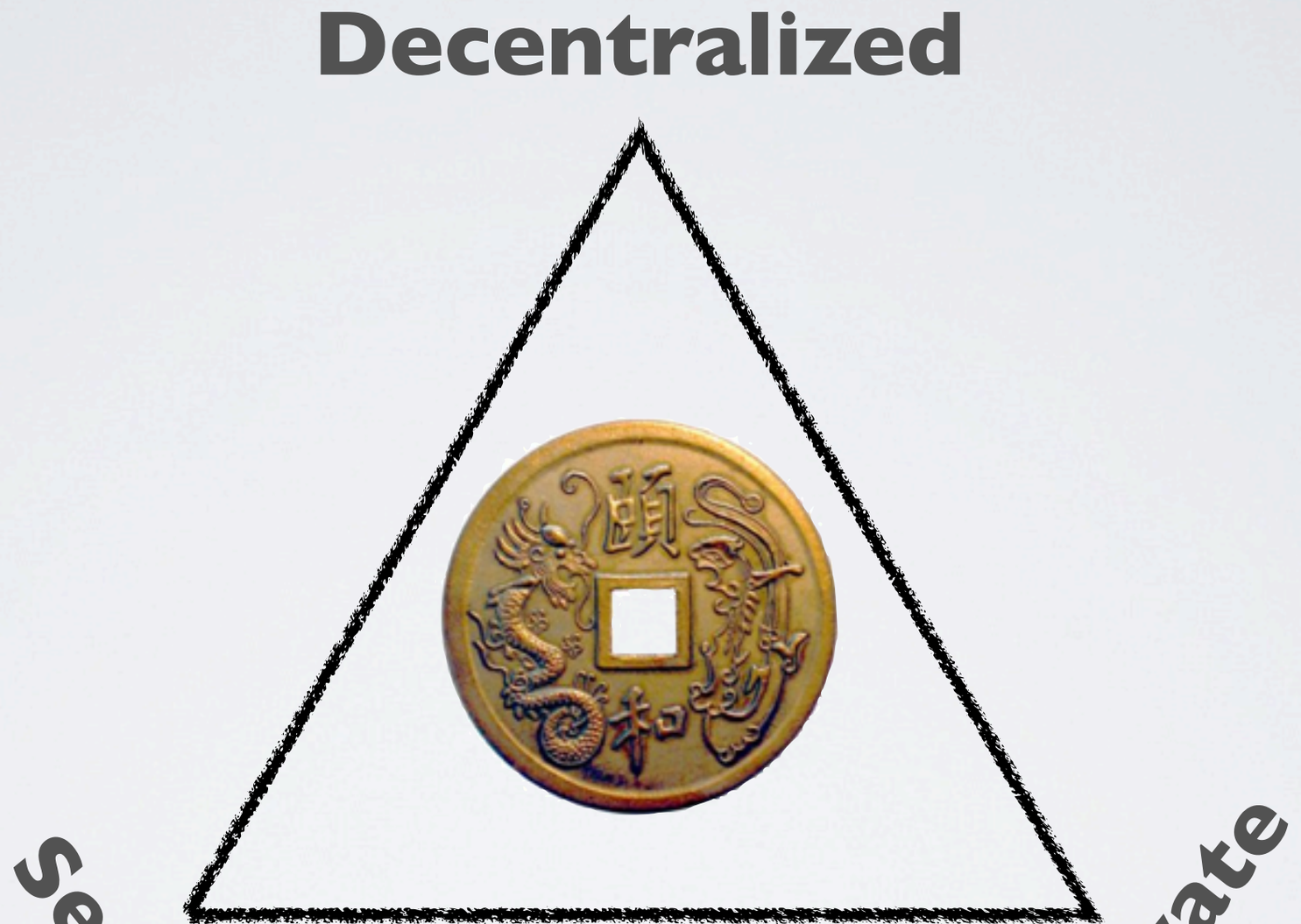
Problems

- **Centralization & Trust**
  - You need a trusted party to operate the bank
  - They can create currency, steal or simply fail

Problems

- **Centralization & Trust**
  - You need a trusted party to operate the bank
  - They can create currency, steal or simply fail
- **Privacy**
  - The bank sees every transaction you make!

“Ideal electronic currency”



Bitcoin


Bitcoin
Feared by corrupt politicians
and central bankers the
world over.
www.Bitcoin.org

Bitcoin

- Proposed in 2008 by "Nakamoto"
  - Extends and improves ideas of Dai (b-money), Szabo (bit gold)
  - Provides for effective, verifiable currency transfers & creation in a decentralized peer-to-peer setting
- A real system with a $1.38 billion 'market cap' (4/21/13)

This cashier's check is the equivalent of cash. In the event it is lost or stolen, it will not be replaced unless an indemnity bond is posted.

203064

Peoples Bank
OF NORTHERN KENTUCKY
CRESTVIEW HILLS, KENTUCKY

73-226/421

REMITTER JONATHAN BEN

DATE 5-20-04

PAY TO THE ORDER OF Alice

$ 9,500.00

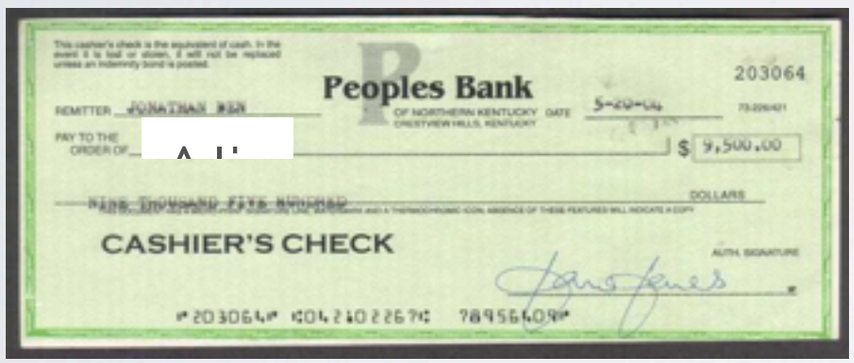
NINE THOUSAND FIVE HUNDRED DOLLARS

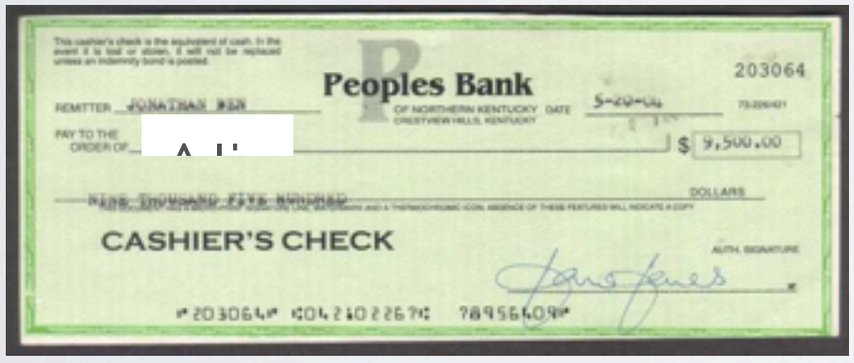
THIS DOCUMENT HAS A MICRO-PRINT SIGNATURE LINE, WATERMARK AND A THERMOCHROMIC ICON; ABSENCE OF THESE FEATURES WILL INDICATE A COPY

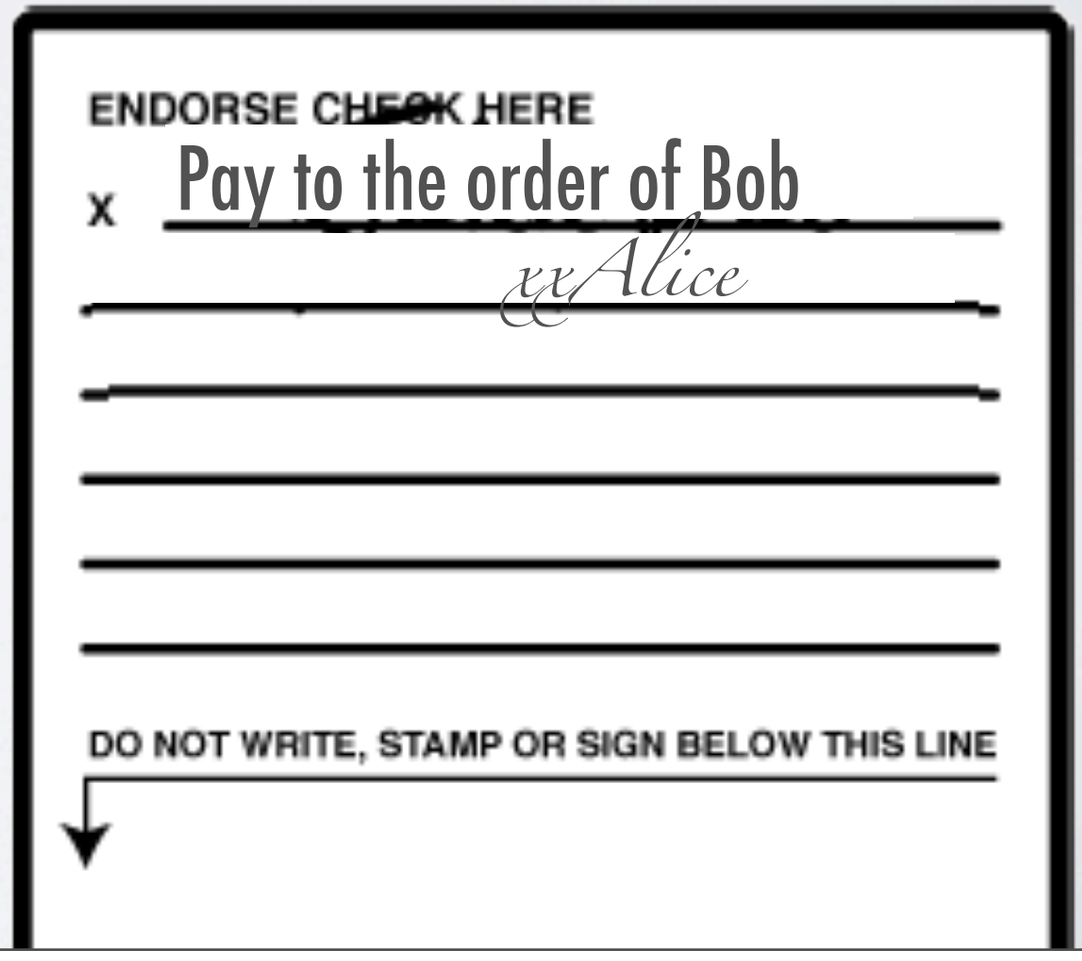
CASHIER'S CHECK

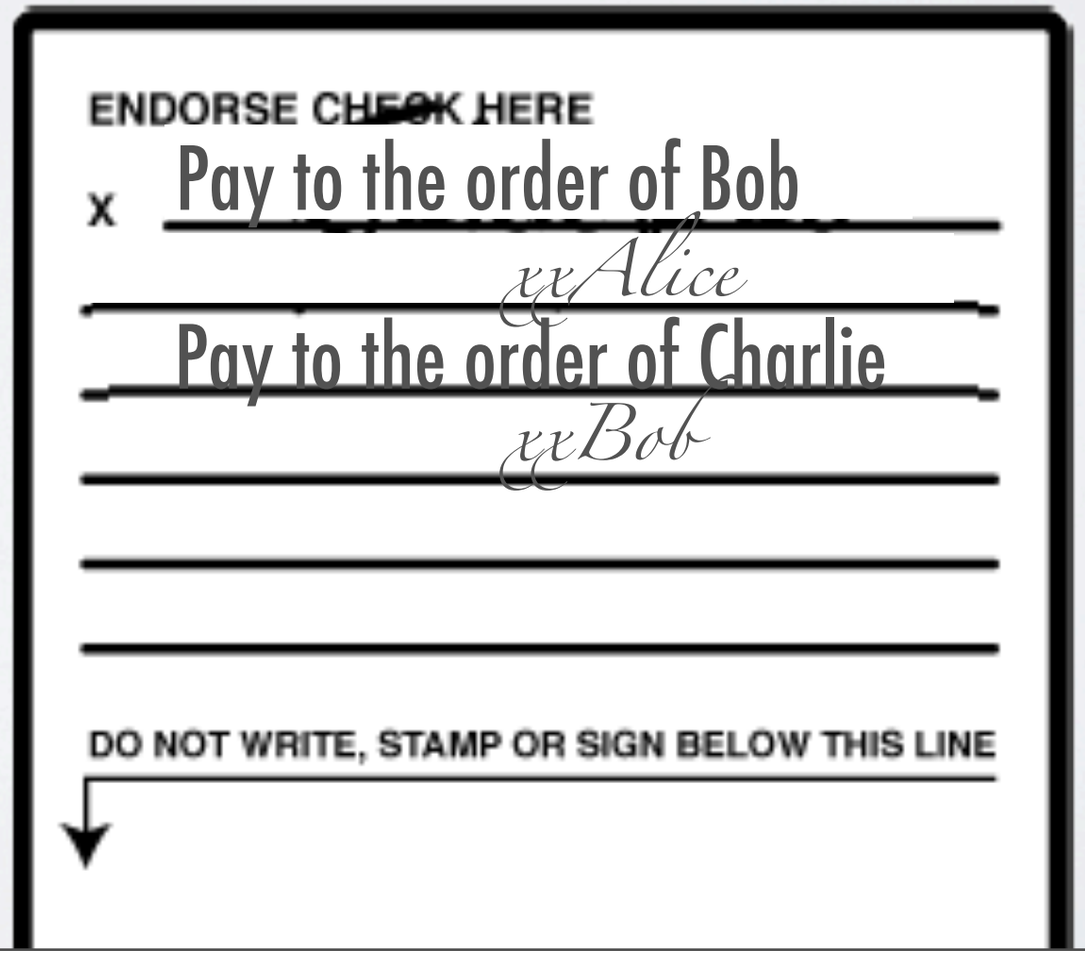
AUTH. SIGNATURE

⑈203064⑈ ⑆042102267⑆ 78956409⑈


Peoples Bank
OF NORTHERN KENTUCKY
CRESTVIEW HILLS, KENTUCKY
203064
CASHIER'S CHECK
$ 9,500.00

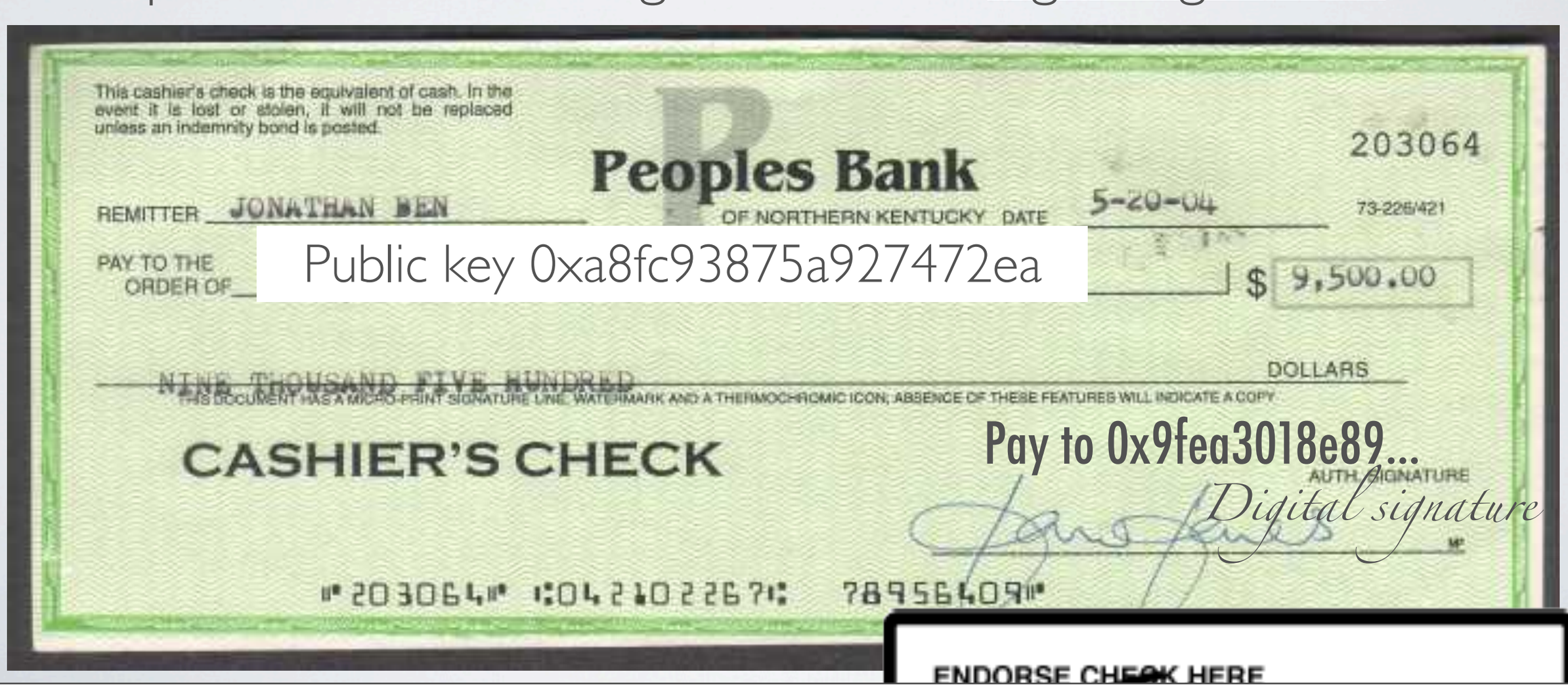

Peoples Bank
OF NORTHERN KENTUCKY
CRESTVIEW HILLS, KENTUCKY
203064
5-20-06
$ 9,500.00
CASHIER'S CHECK


ENDORSE CHECK HERE
X
Pay to the order of Bob
xxAlice
DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE


ENDORSE CHECK HERE
x
Pay to the order of Bob
xxAlice
&
Pay to the order of Charlie
xxBob
&
DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE

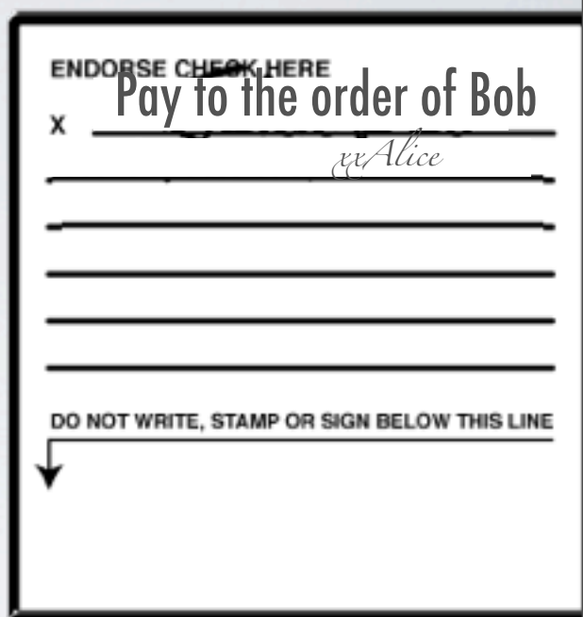
Can we make this electronic?

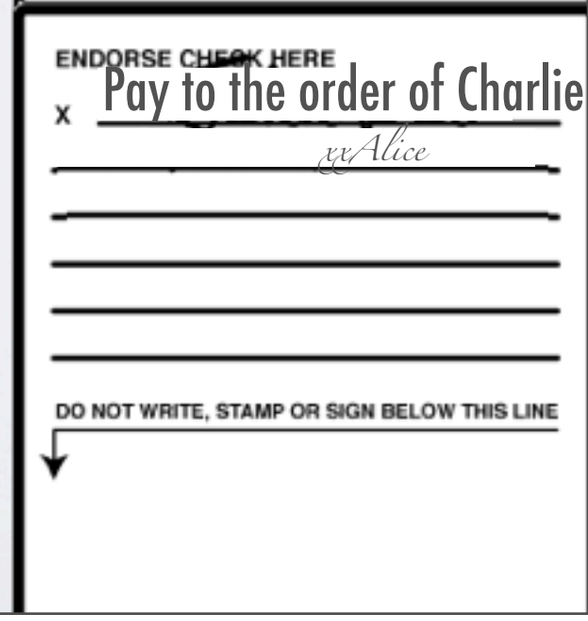
- Idea:
  - Replace names with public keys
  - Replace handwritten signatures with digital signatures



Can we make this electronic?

- **Problem: Alice can still double spend!**
  - Alice "gives" the same check to Bob and Charlie



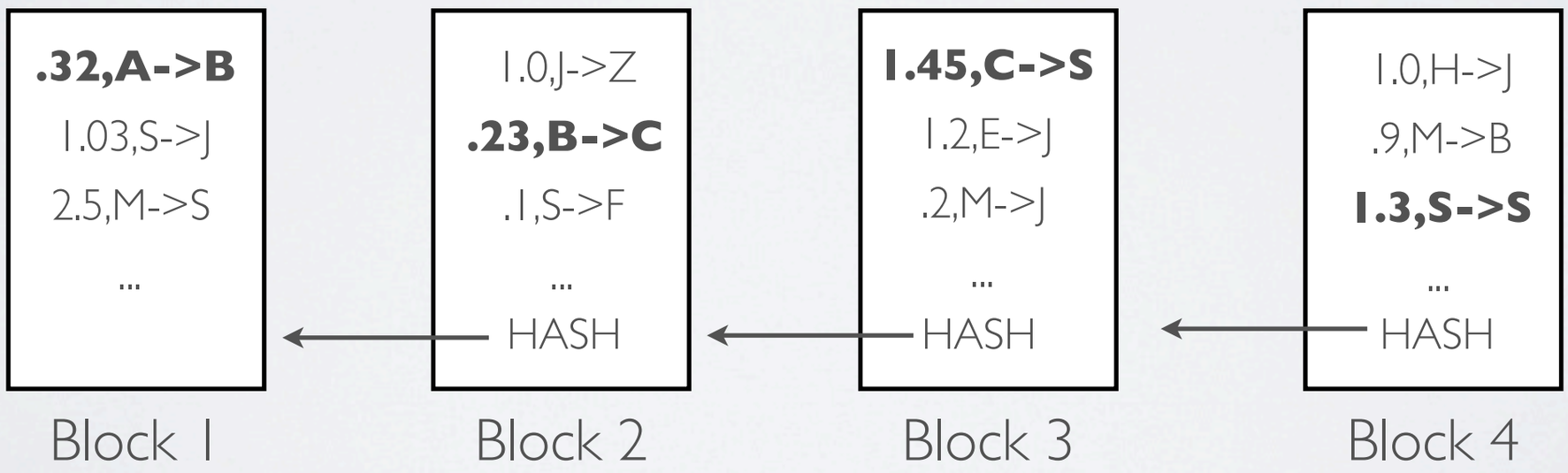


Double-spending

- Keep a central 'ledger' of all transfers
  - Register all transfers on the ledger
  - Recipients can check if money has already been 'spent'
- How to do this in a decentralized fashion??

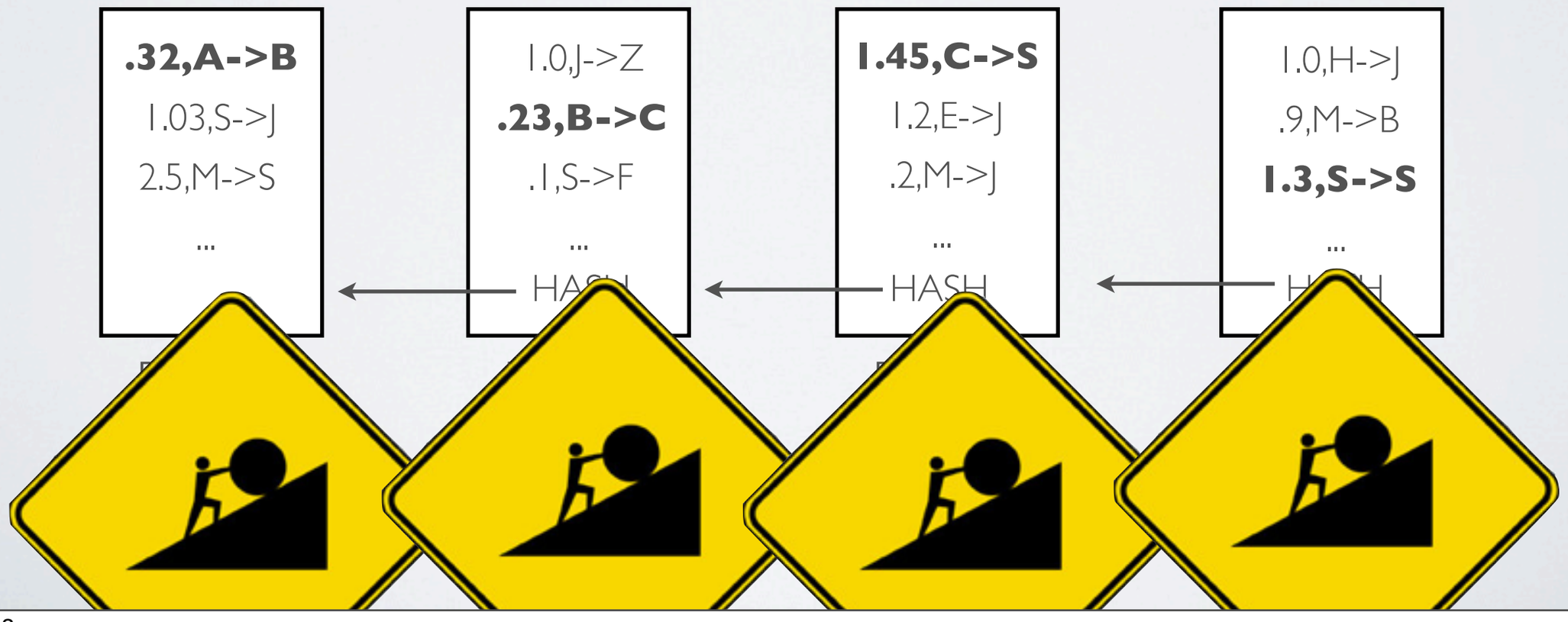
The block chain

- Bitcoin solves this through **consensus**
  - All participants keep a copy of the ledger (divided into 'blocks' of many transactions)
  - The blocks are connected through hash chaining



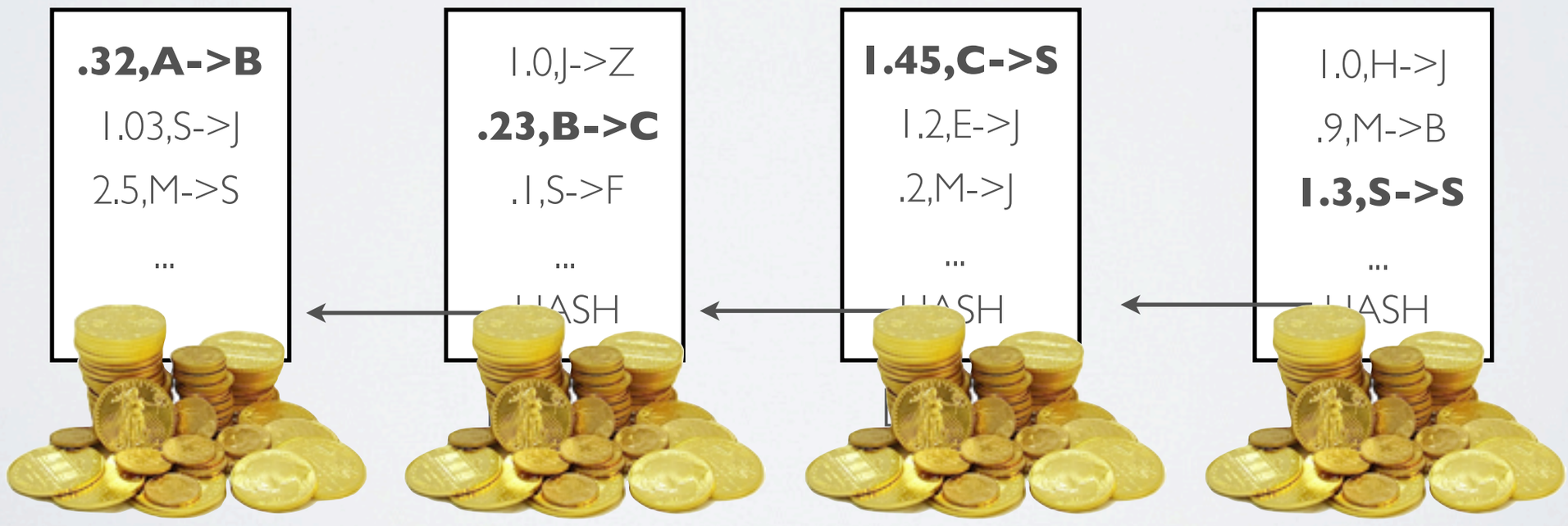
The block chain

- Nodes compete to add new blocks to the chain
  - This is done by making nodes solve a simple "proof of work"
  - This prevents a single node from controlling the chain

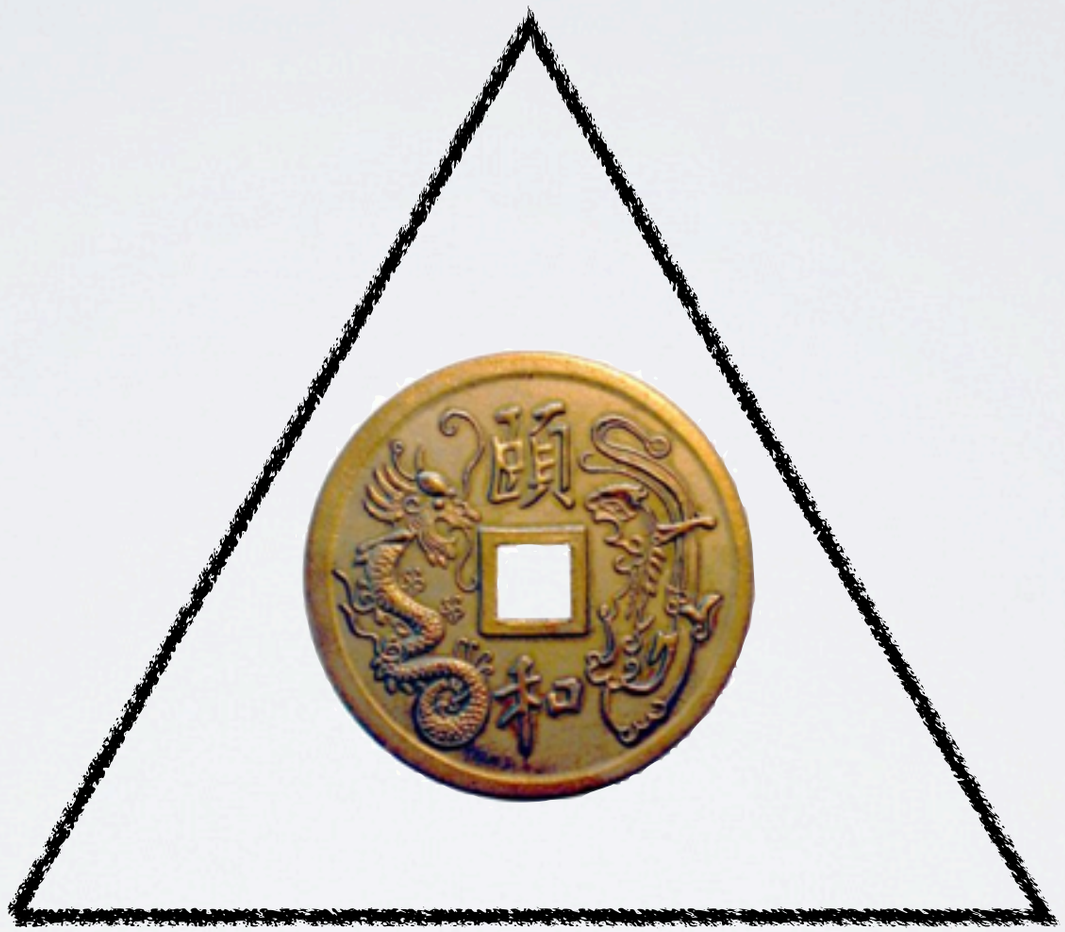


The block chain

- Nodes get a reward for 'winning' the PoW on a given block
  - They're allowed to 'mint' 25 new Bitcoin out of thin air
  - (They can also receive transaction fees)

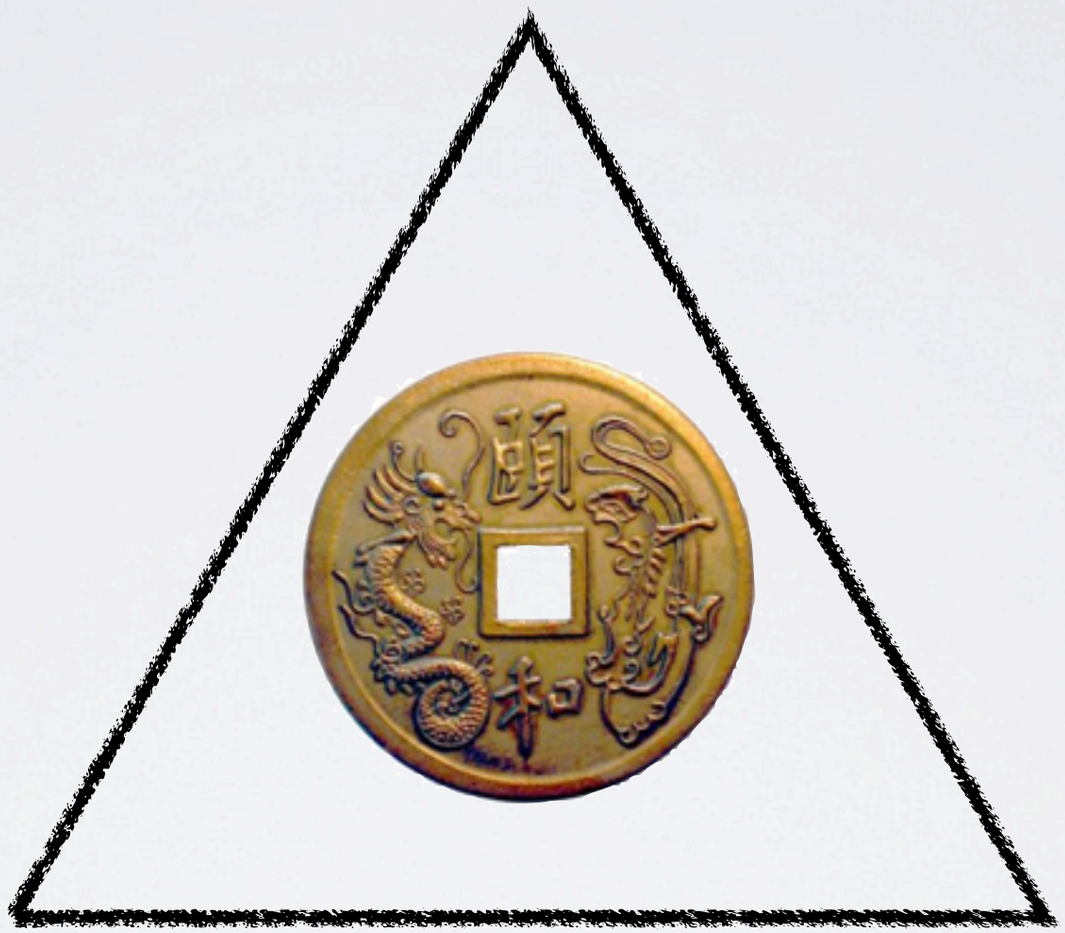


Bitcoin triangle



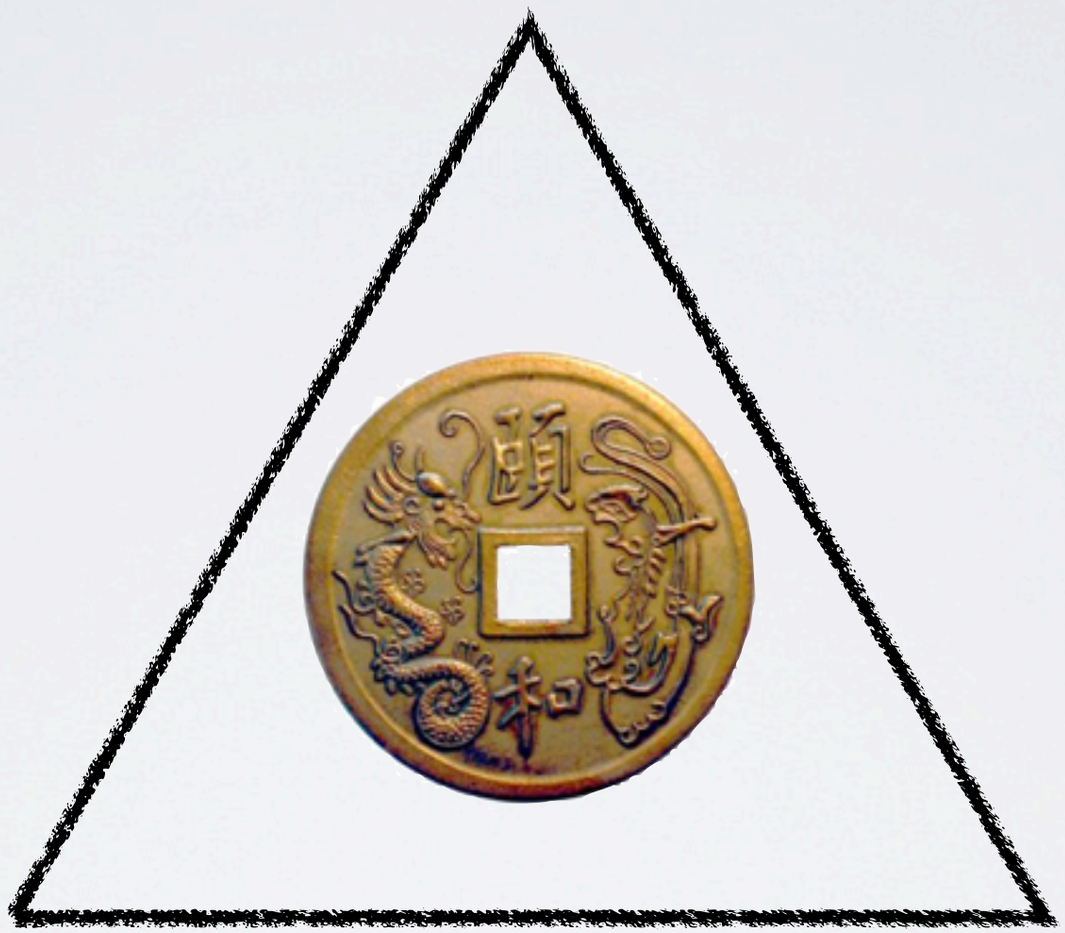
Bitcoin triangle

Decentralized



Bitcoin triangle

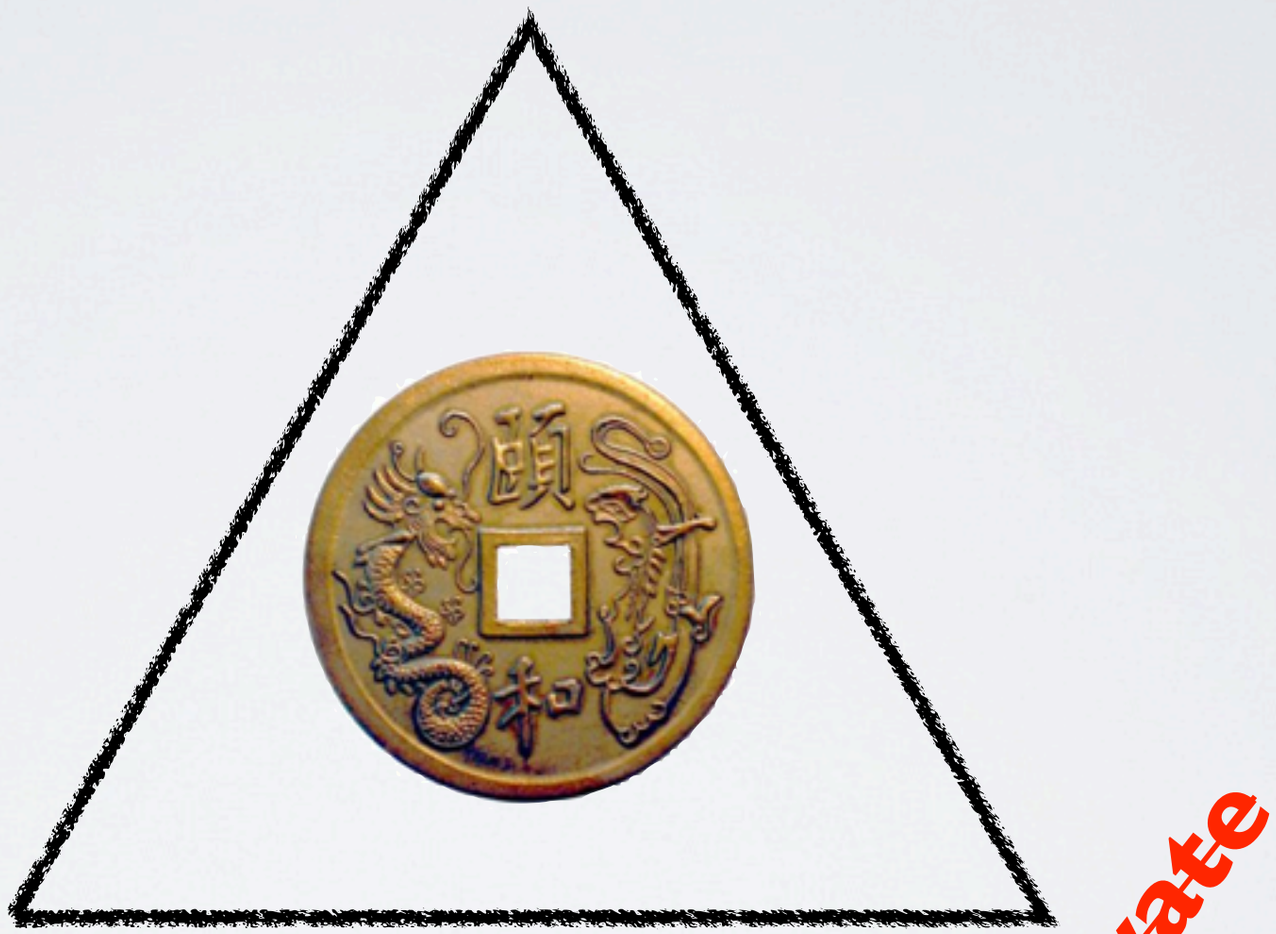
Decentralized



Secure

Bitcoin triangle

Decentralized

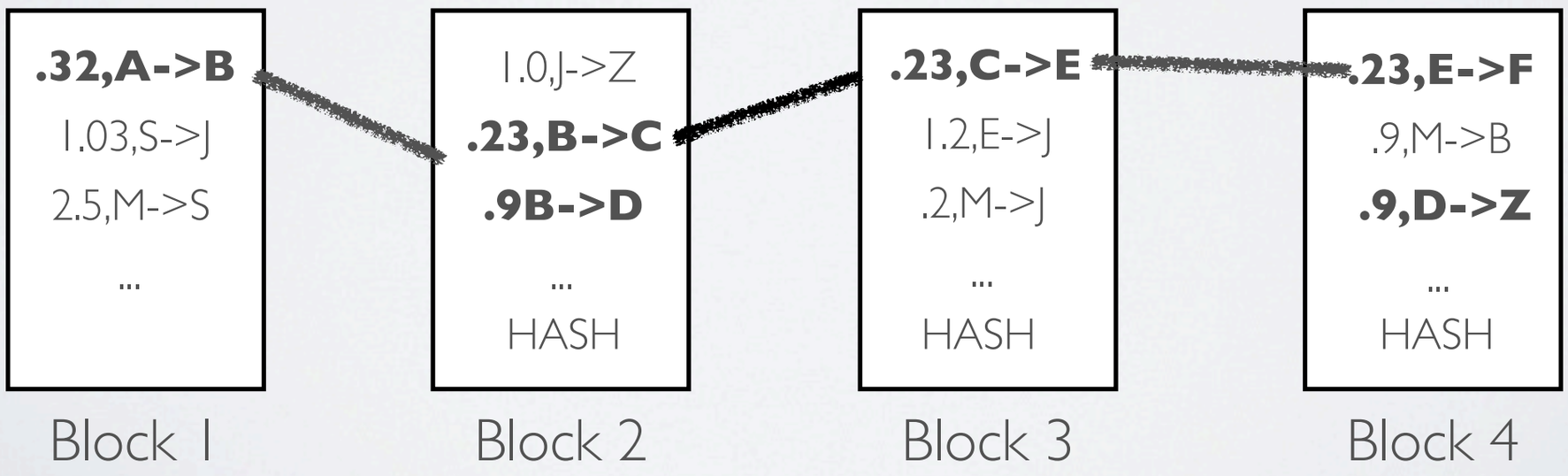


Secure

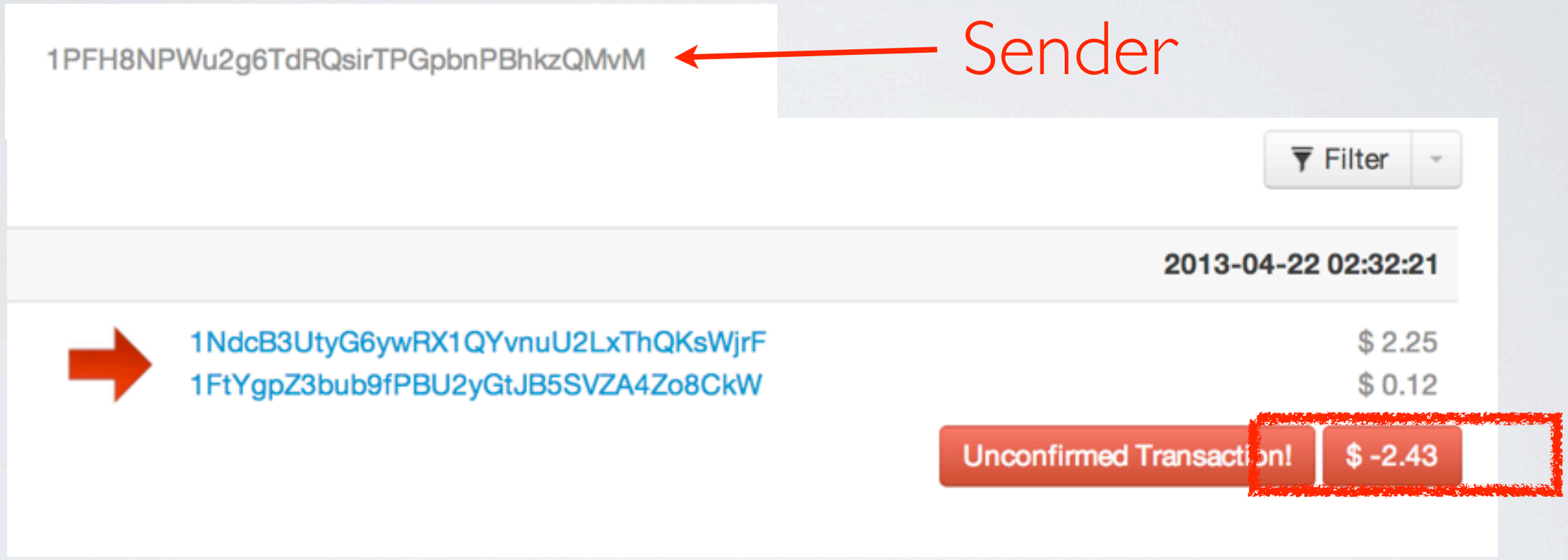
Private

Bitcoin privacy

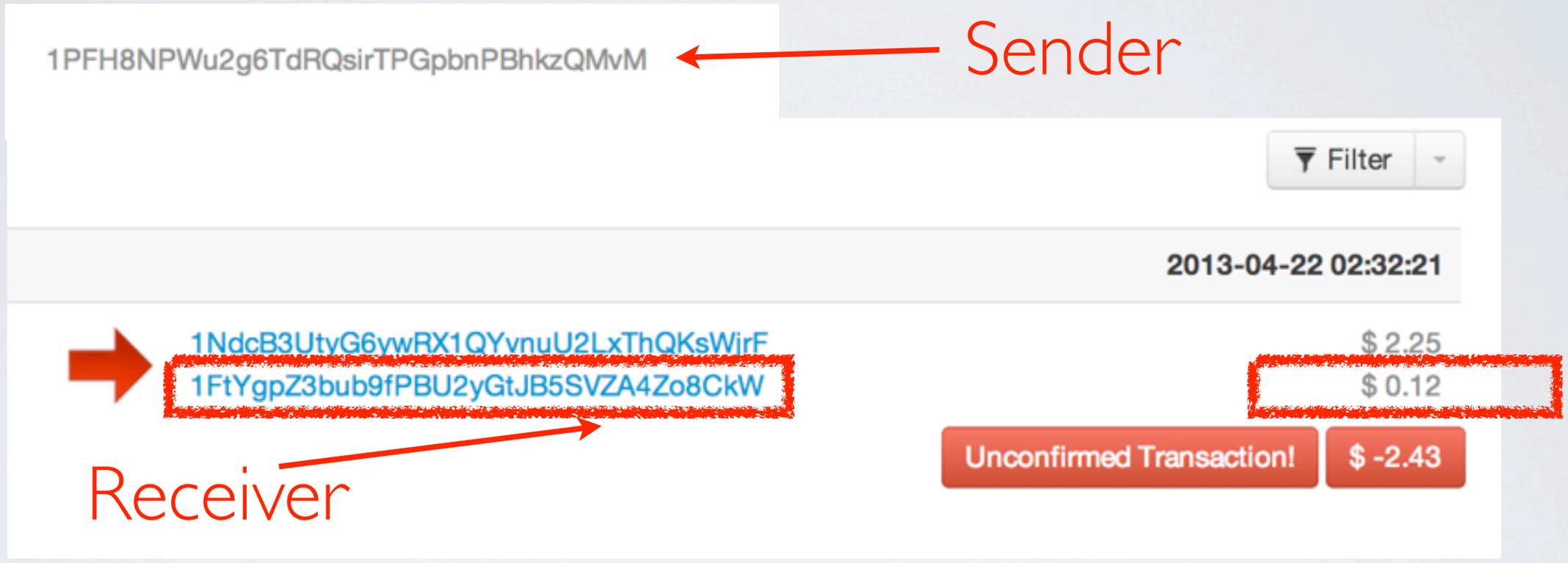
- The block chain is a history of every Bitcoin transaction ever!
  - Identifiers are public keys not names ("pseudonyms")
  - You can make as many public keys as you want
- But these still leak information!



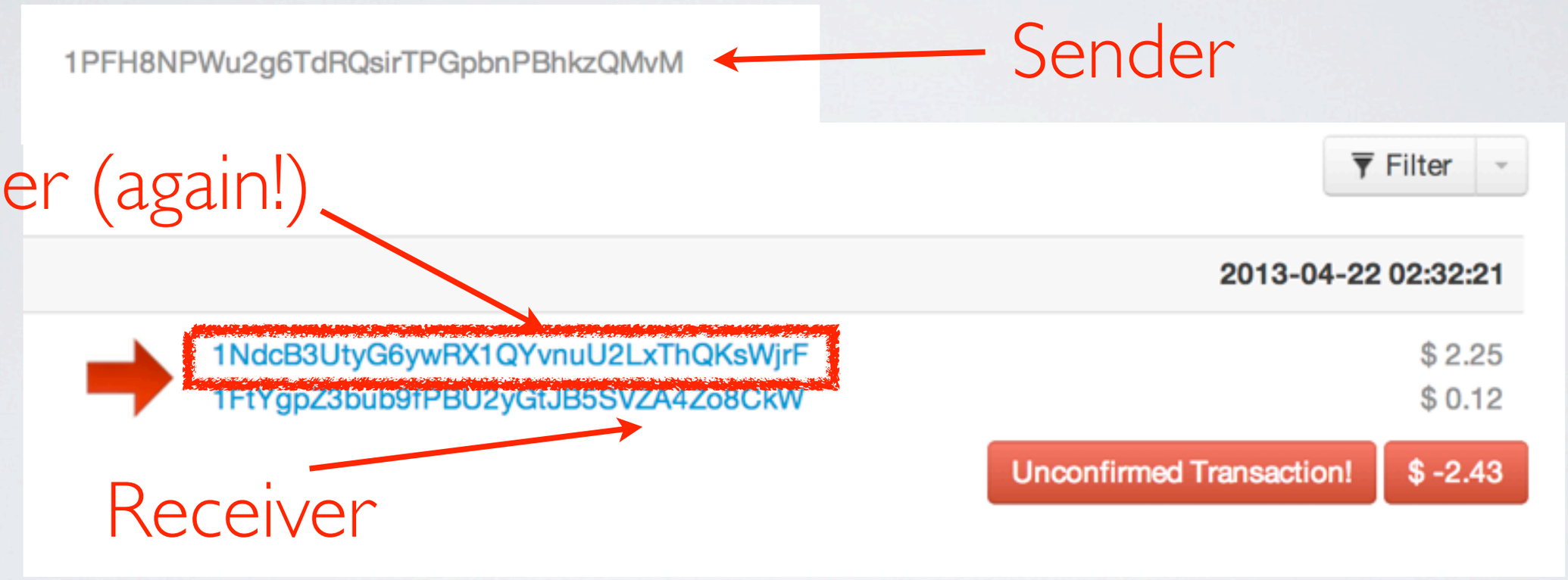
Bitcoin privacy



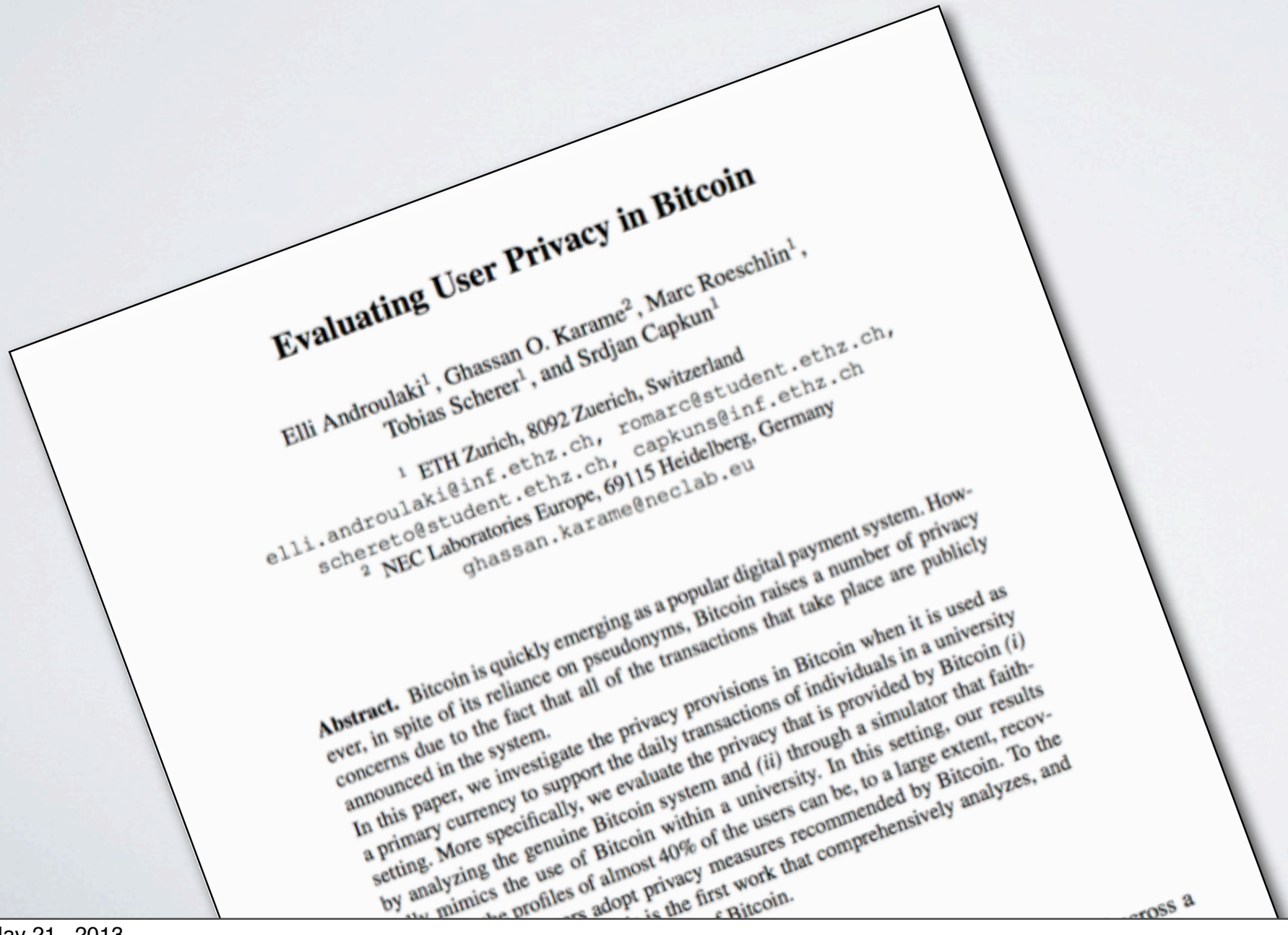
Bitcoin privacy



Bitcoin privacy



Bitcoin privacy



Evaluating User Privacy in Bitcoin

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

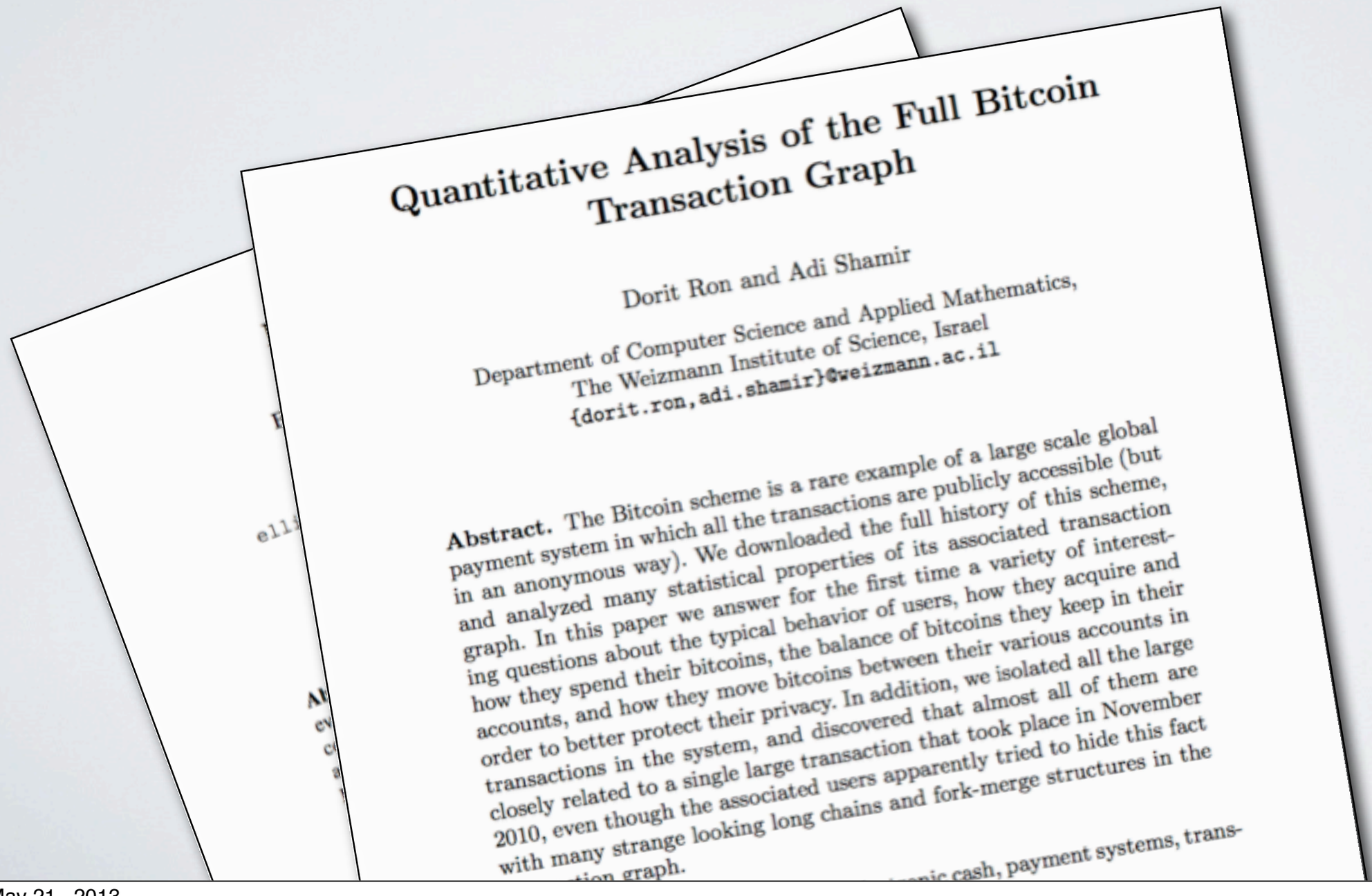
[1] ETH Zurich, 8092 Zuerich, Switzerland
elli.androulaki@inf.ethz.ch, romarc@student.ethz.ch,
schereto@student.ethz.ch, capkuns@inf.ethz.ch
[2] NEC Laboratories Europe, 69115 Heidelberg, Germany
ghassan.karame@neclab.eu

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 [illegible] the profiles of almost 40% of the users can be, to a large extent, recovers adopt privacy measures recommended by Bitcoin. To the [illegible] is the first work that comprehensively analyzes, and [illegible] of Bitcoin.

[illegible] across a

Bitcoin privacy



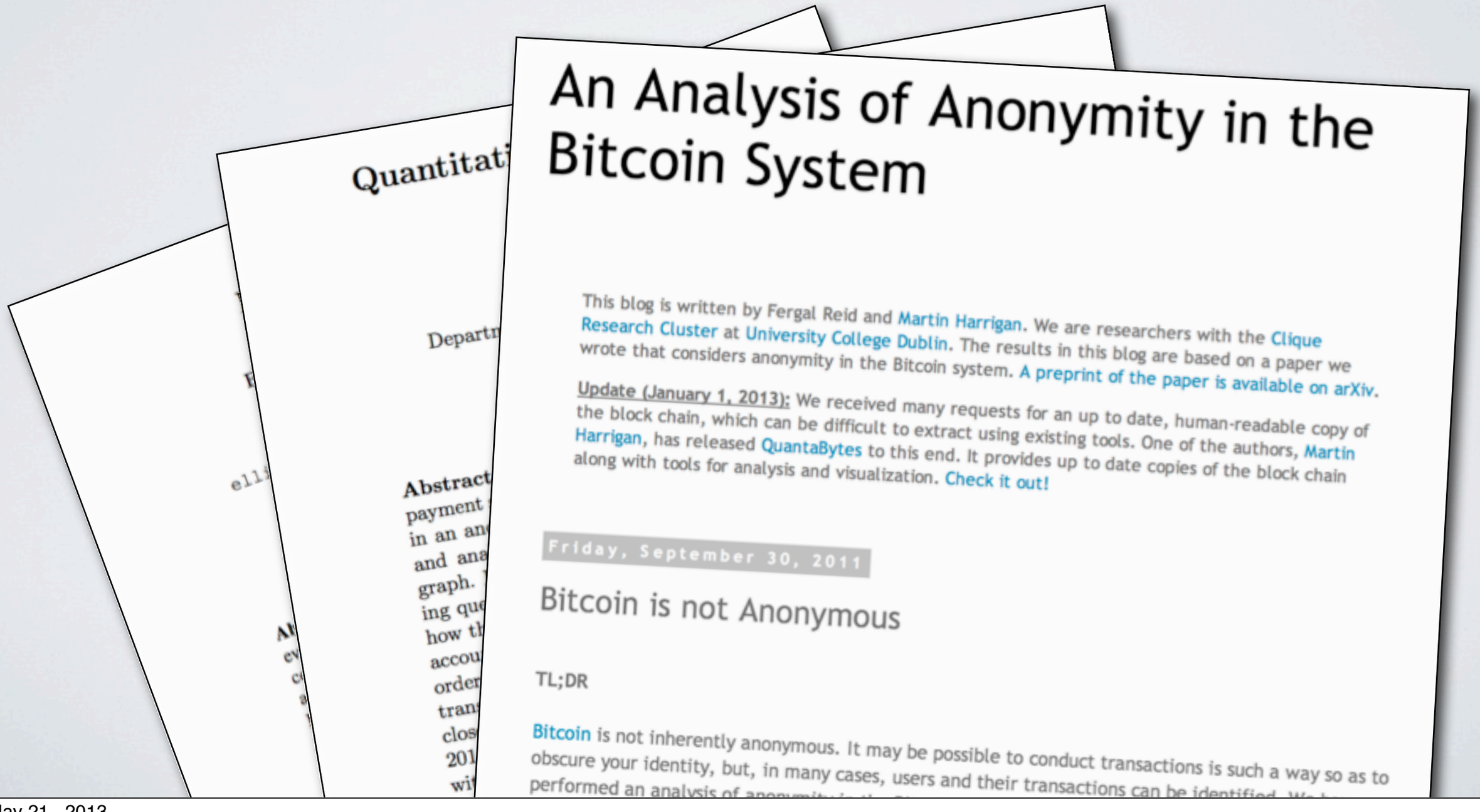
Quantitative Analysis of the Full Bitcoin Transaction Graph

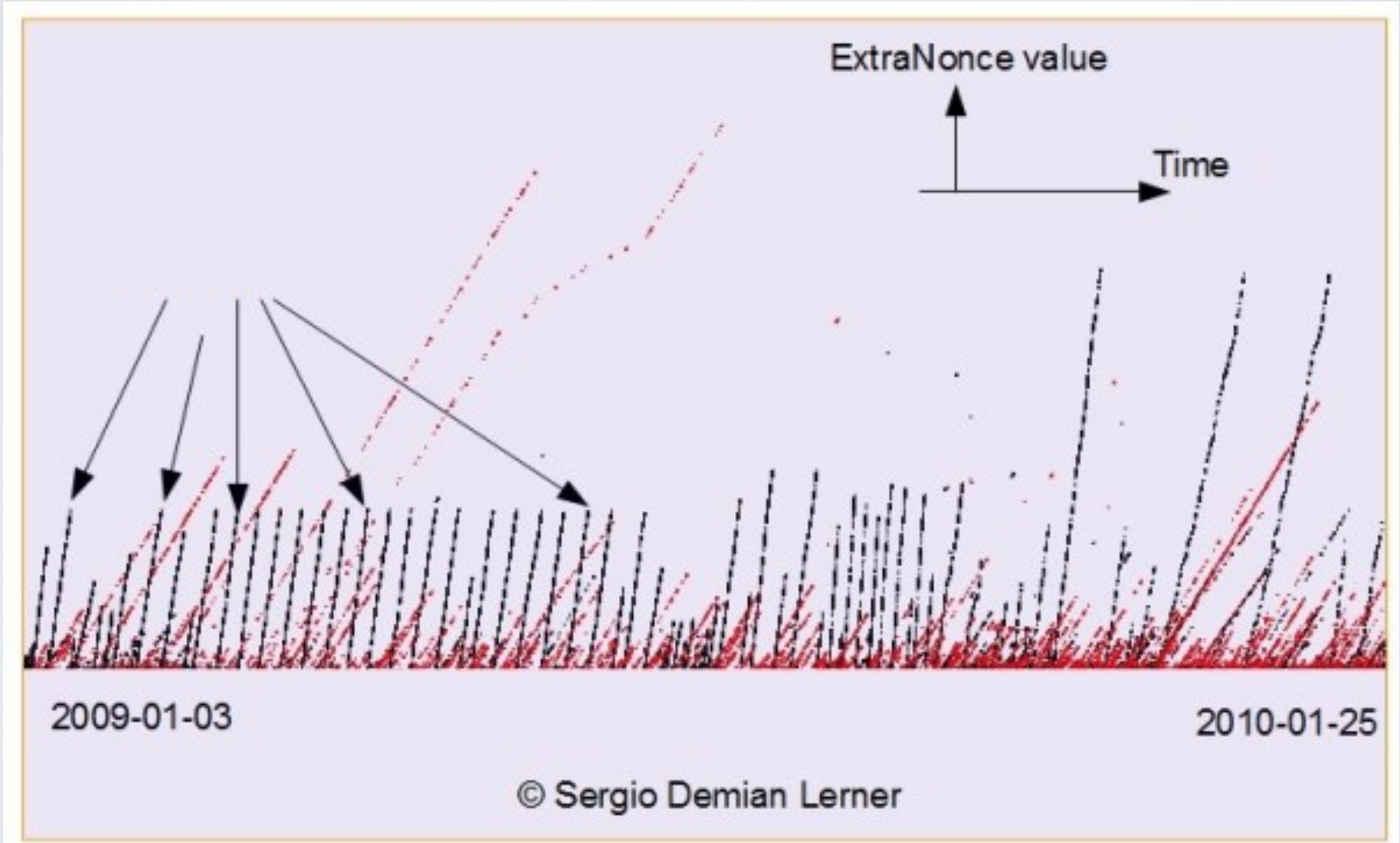
Dorit Ron and Adi Shamir

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

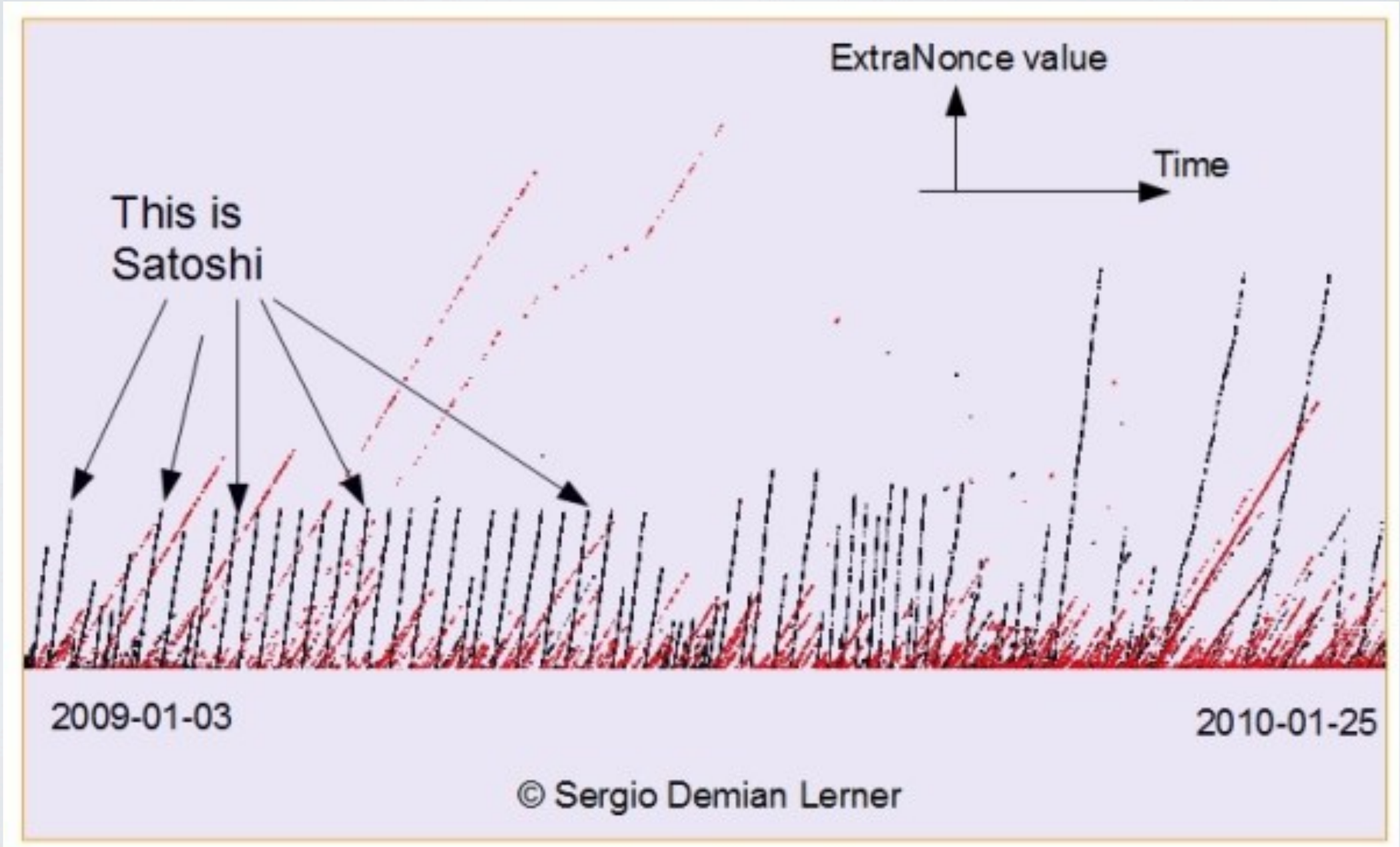
Bitcoin privacy





http://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/

The Nakamoto Treasure



http://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/

Privacy solutions

- "Be careful"
- Use 'laundry' services
  - Mix many users' coins together
  - You must really trust the laundry

Chaumian e-Cash

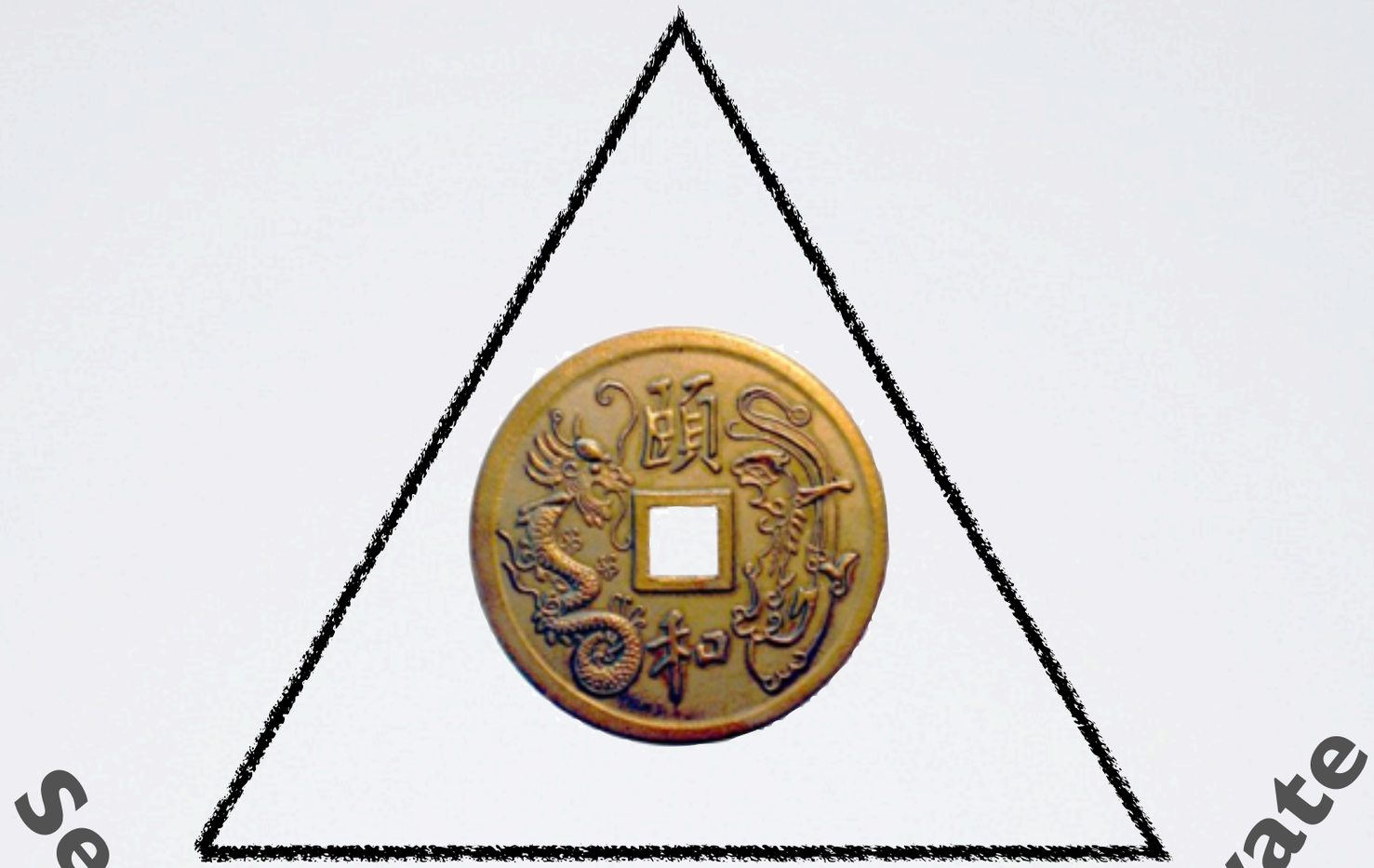
- Dates to Chaum [82] (many subsequent works)
  - Completely untraceable electronic cash
  - Withdraw 'coins' from a **central bank** (using blind signatures)
  - Even the bank can't track the coins

Blind sign "s"

signature(s)

Laundries & Chaum

~~**Decentralized**~~



Secure

Private

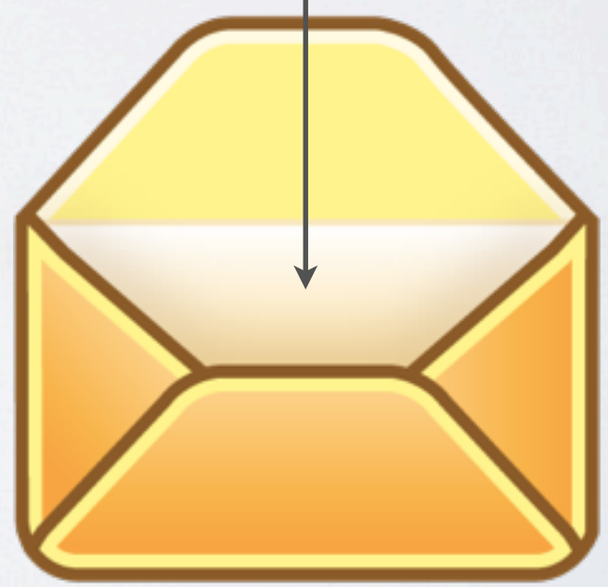
Zerocoin

- New approach to creating electronic coins
  - Based on a technique due to Sander and Ta-shma
  - Extends Bitcoin by adding a ‘decentralized laundry’
- Requires only a trusted, append-only bulletin board
  - Bitcoin block chain gives us this ‘for free’!

Making Zerocoin

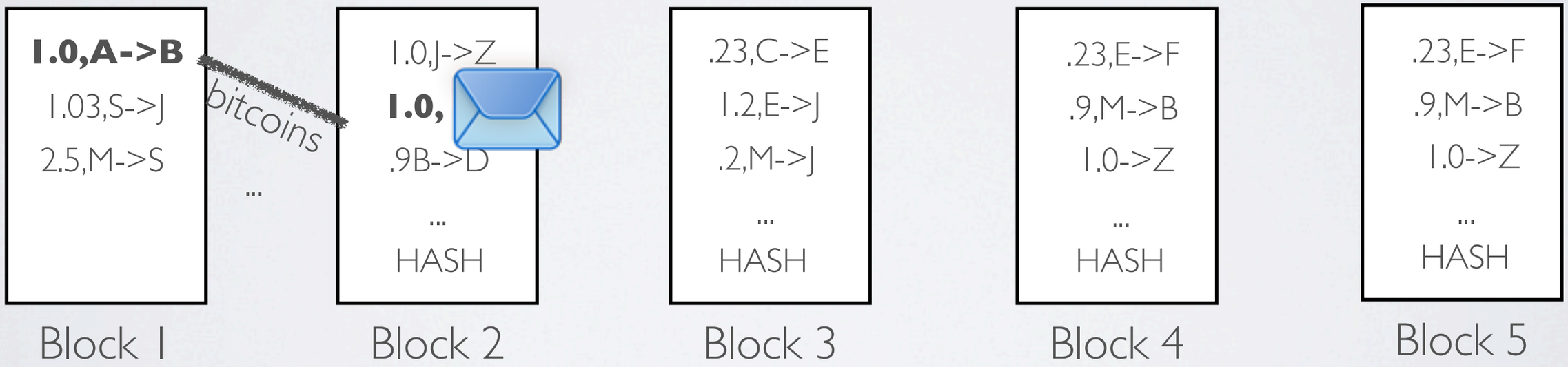
- Zerocoins are just numbers
  - Each is a digital commitment to a random serial number
  - Anyone can make one!

8238482734710l2983

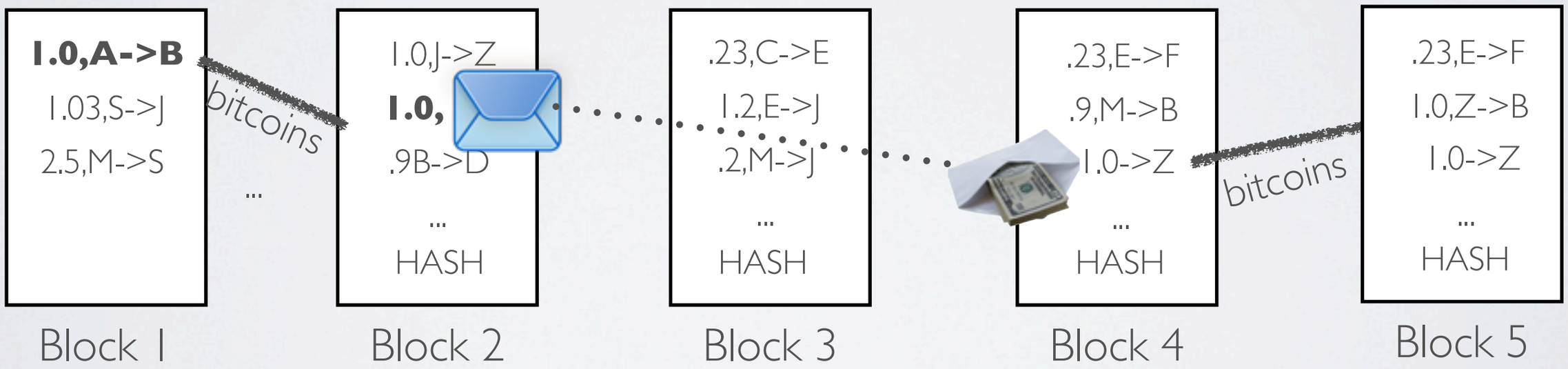


Making Zerocoin

- Zerocoins are just numbers
  - They have value once you put them on the block chain
  - This costs e.g., 1 bitcoin

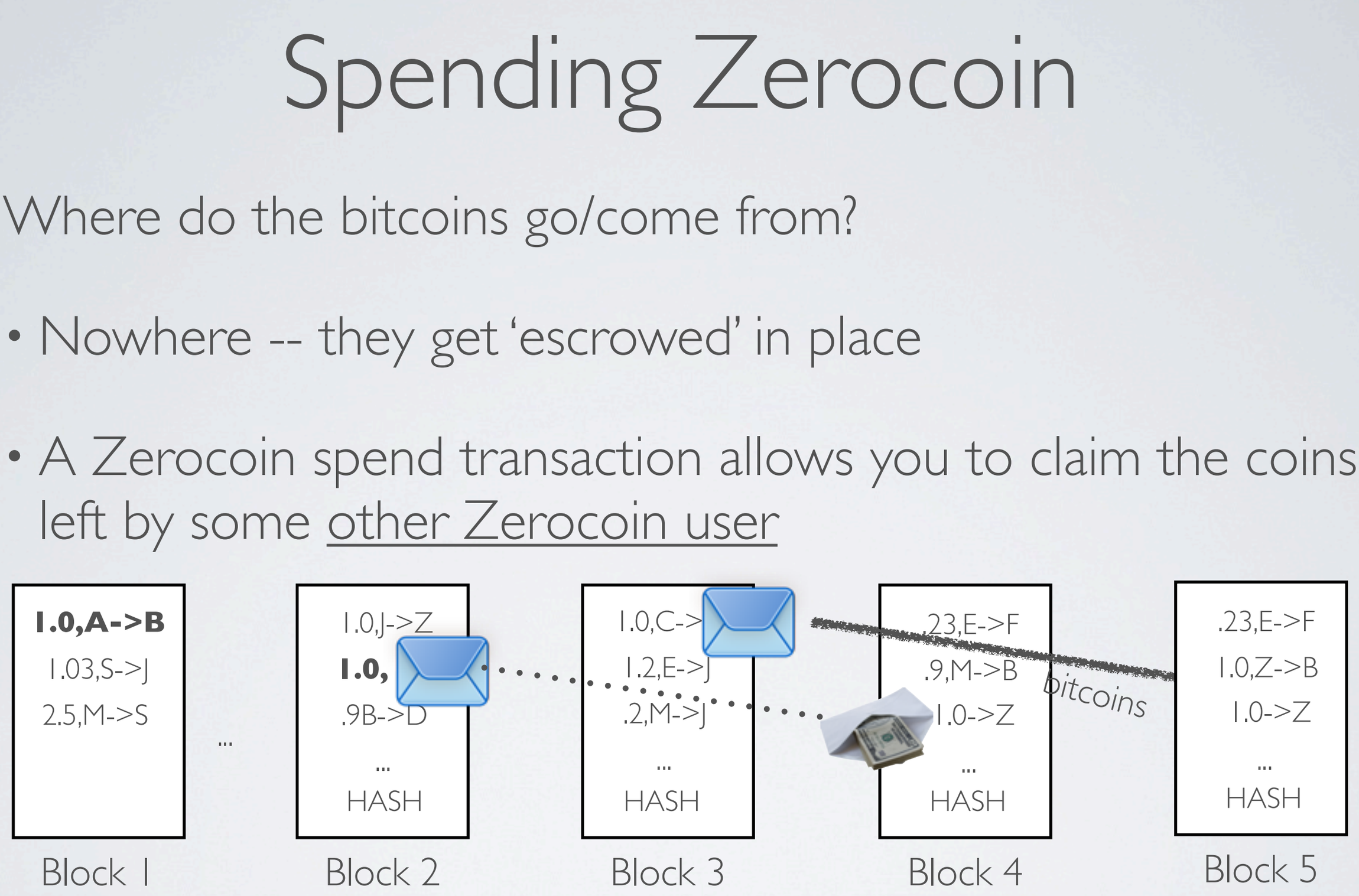


Spending Zerocoin



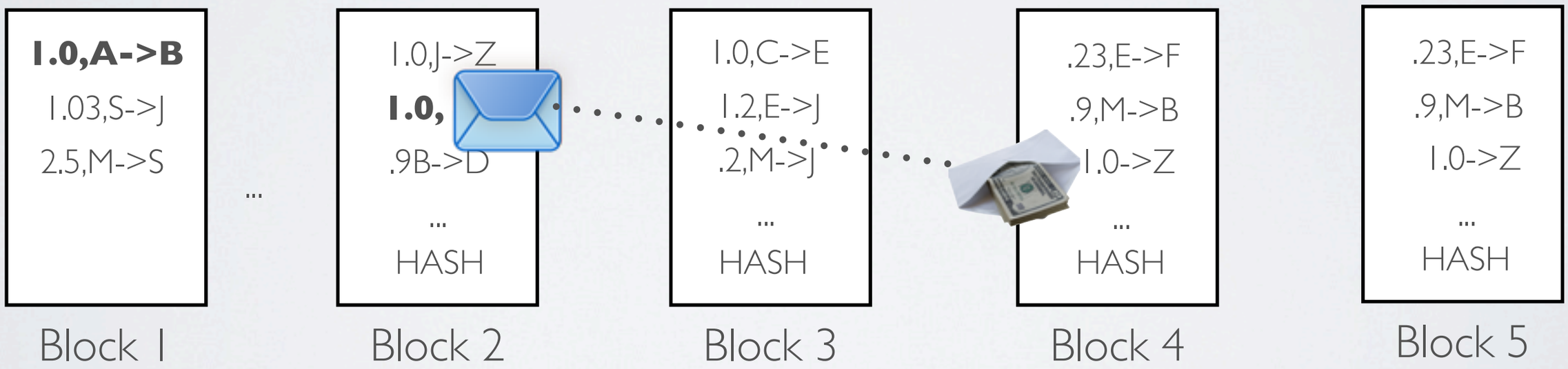
Spending Zerocoin

- Where do the bitcoins go/come from?
  - Nowhere -- they get 'escrowed' in place
  - A Zerocoin spend transaction allows you to claim the coins left by some other Zerocoin user



Spending Zerocoin

- Why is this anonymous?
  - It's all in the way we 'prove' we have a Zerocoin
  - This is done using a zero knowledge proof



Spending Zerocoin

- Zero knowledge [Goldwasser, Micali 1980s, and beyond]
  - Prove a statement without revealing any other knowledge
  - Specific variant: proof of knowledge

- Here we prove knowledge of:
  (a) a Zerocoin in the block chain
  (b) we just revealed the actual serial number inside of it

- The trick is doing this efficiently!

Spending Zerocoin

- Inefficient proof
  - Identify all valid Zerocoins in the blockchain (call them $C_1, C_2, \ldots, C_N$)
  - Prove knowledge of C such that:

$$(C = C_1) \vee (C = C_2) \vee \cdots \vee (C = C_N)$$

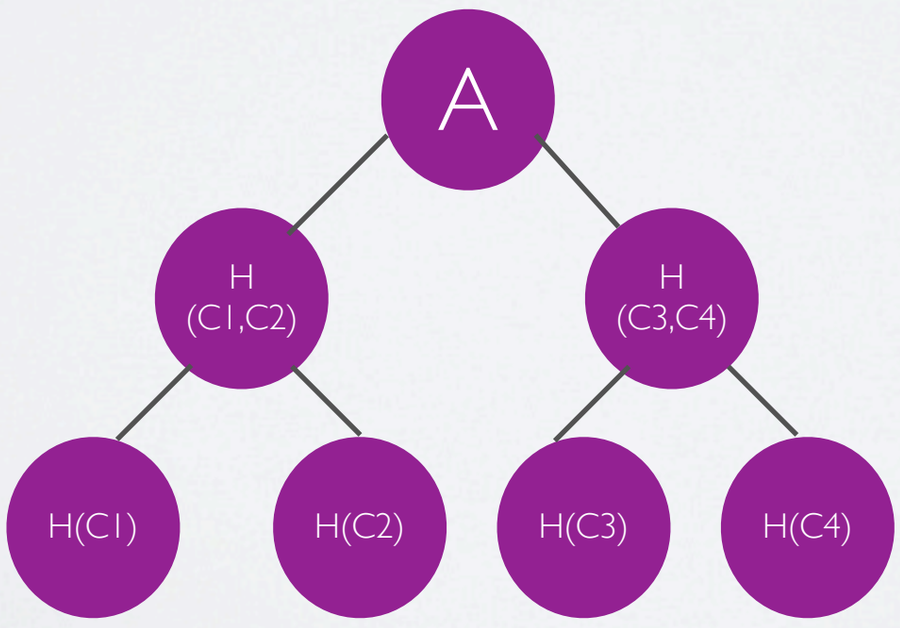
These ‘or’ proofs have cost O(N)

Spending Zerocoin

- Better approach
  - Use an efficient one-way accumulator
  - Accumulate $C_1, C_2, \ldots, C_N$ to produce accumulator A
  - Then prove knowledge of a witness s.t. $C \in inputs(A)$

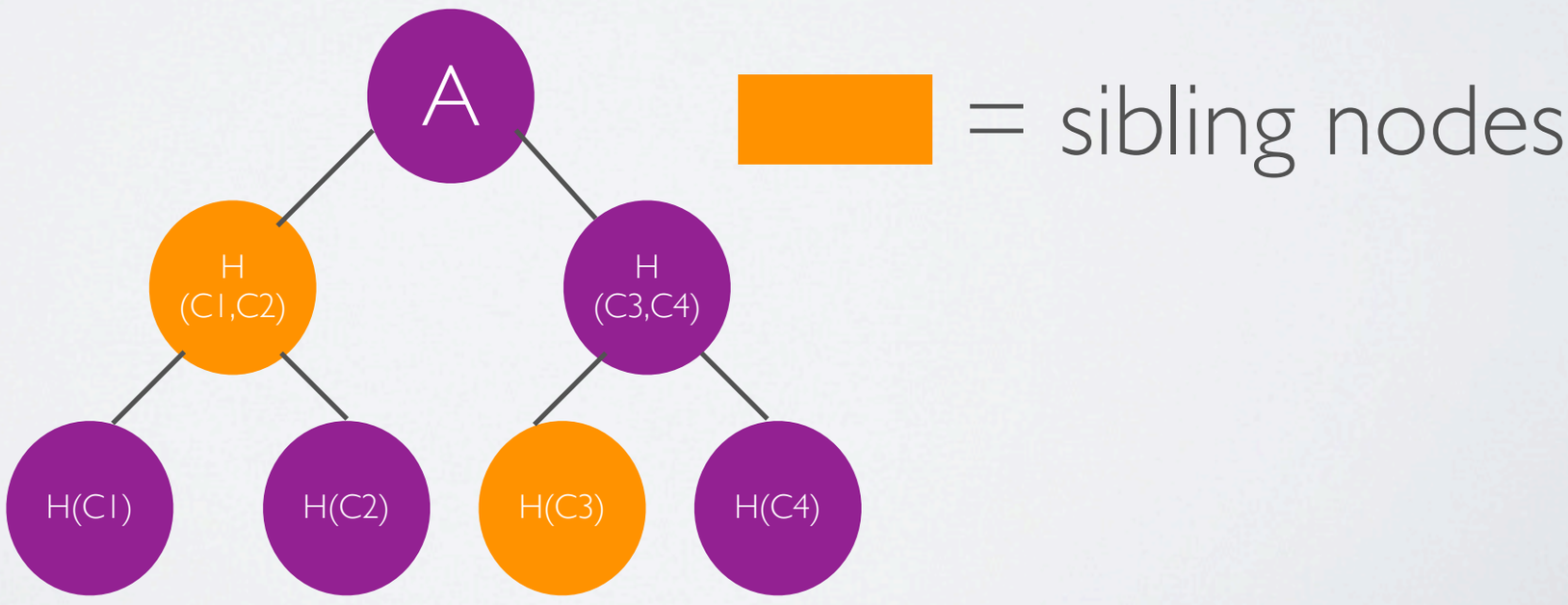
Spending Zerocoin

- Better approach
  - Use an efficient one-way accumulator
  - Accumulate $C_1, C_2, \ldots, C_N$ to produce accumulator A
  - Then prove knowledge of a witness s.t. $C \in inputs(A)$



Spending Zerocoin

- Better approach
  - Use an efficient one-way accumulator
  - Accumulate $C_1, C_2, \ldots, C_N$ to produce accumulator A
  - Then prove knowledge of a witness s.t. $C \in inputs(A)$



Spending Zerocoin

- Problem:
  - There are relatively few accumulators that meet our criteria

1. Computing the accumulator should not require any secrets (i.e., it's publicly computable/verifiable)
2. There must be an efficient ZK proof of knowledge of a witness.

Merkle trees don't (seem) to possess one

Strong RSA Accumulator

(Benaloh & de Mare)

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

To accumulate *primes* $C_1, C_2, \ldots, C_N$ compute:

$$A = u^{C_1 \cdot C_2 \cdot \cdots \cdot C_N}$$

$$w_i = u^{C_1 \cdot C_2 \cdot C_{i-1} \ldots C_{i+1} \cdot \cdots \cdot C_N}$$

An efficient ZKPoK proposed by Camenisch/Lysyanskaya '01!

The protocol overview

- The protocol:
  - Generate random serial number *S*. Compute:

$C = g^S h^r$ s.t. *C* is prime, $\$r$

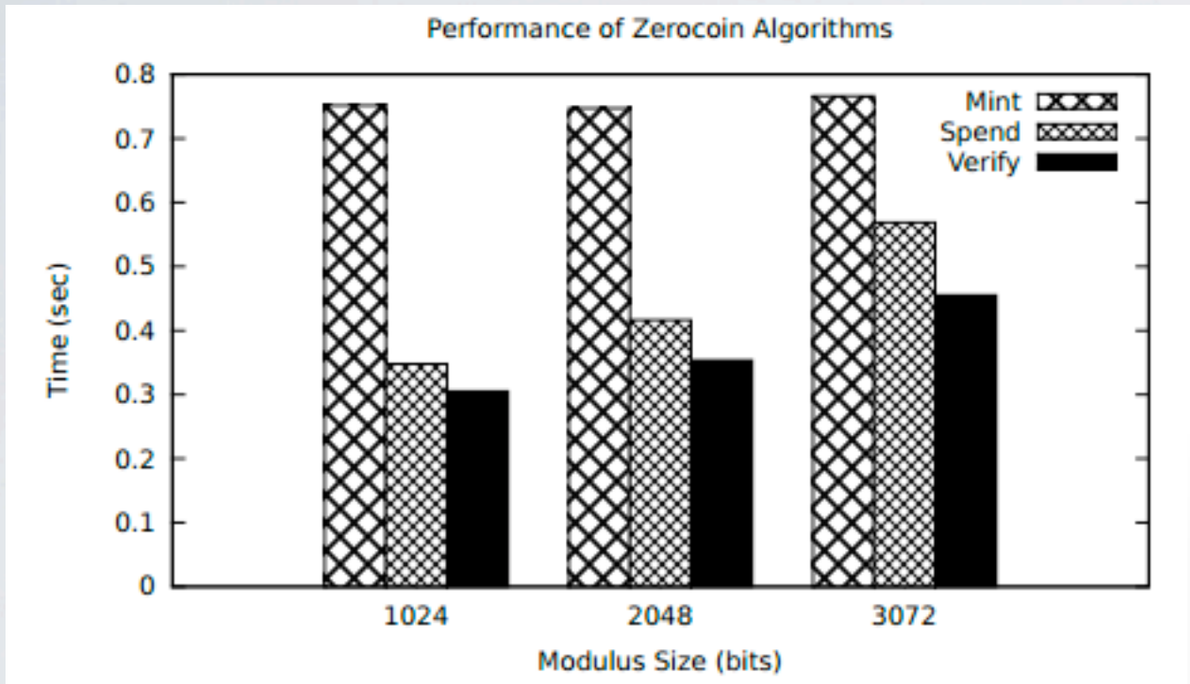
    - (Retain *S*, commitment randomness r)
  - Accumulate all valid coins, compute witness w_i
  - Reveal *S*, prove knowledge of accumulator witness w_i and commitment randomness r

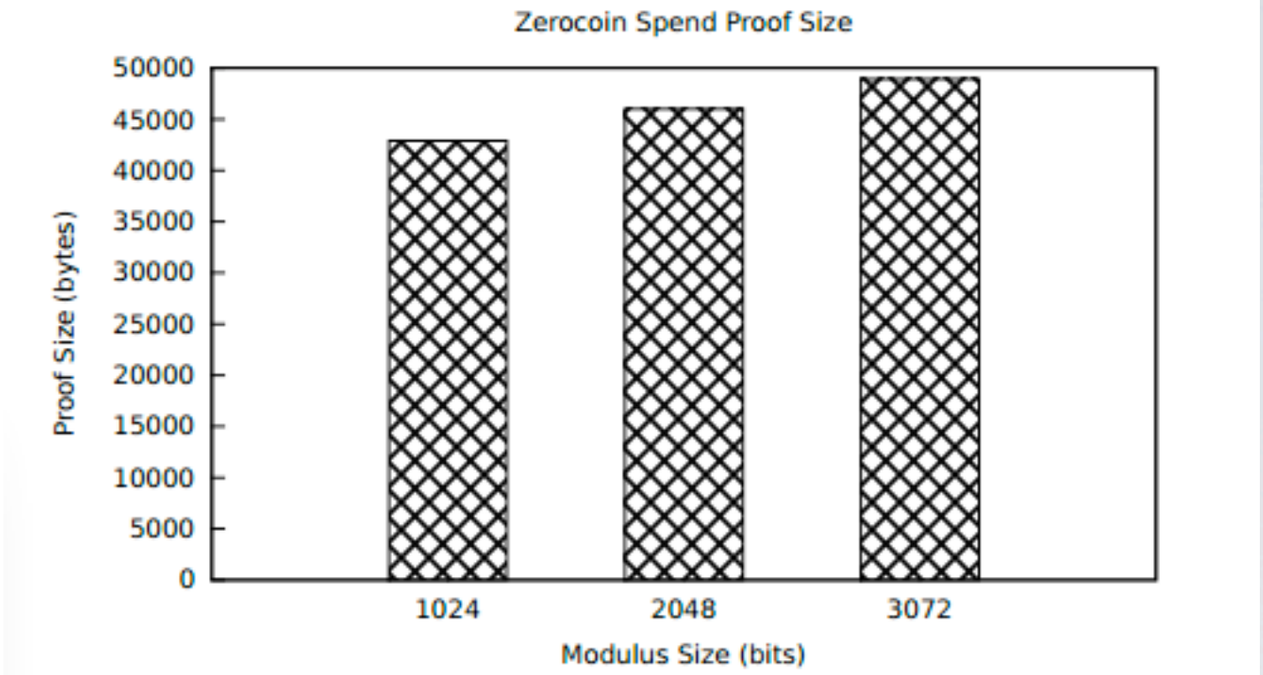
Requires a DDL proof (~40kb)

Optimizations

- Accumulator can be incrementally computed
  - Don't make Prover do it: have the miners compute an accumulator 'checkpoint' each block
  - This minimizes accumulator computation time
- Probabilistic verification
  - The proof doesn't need to be fully verified
  - Verify random portions (reduces certainty)

Performance



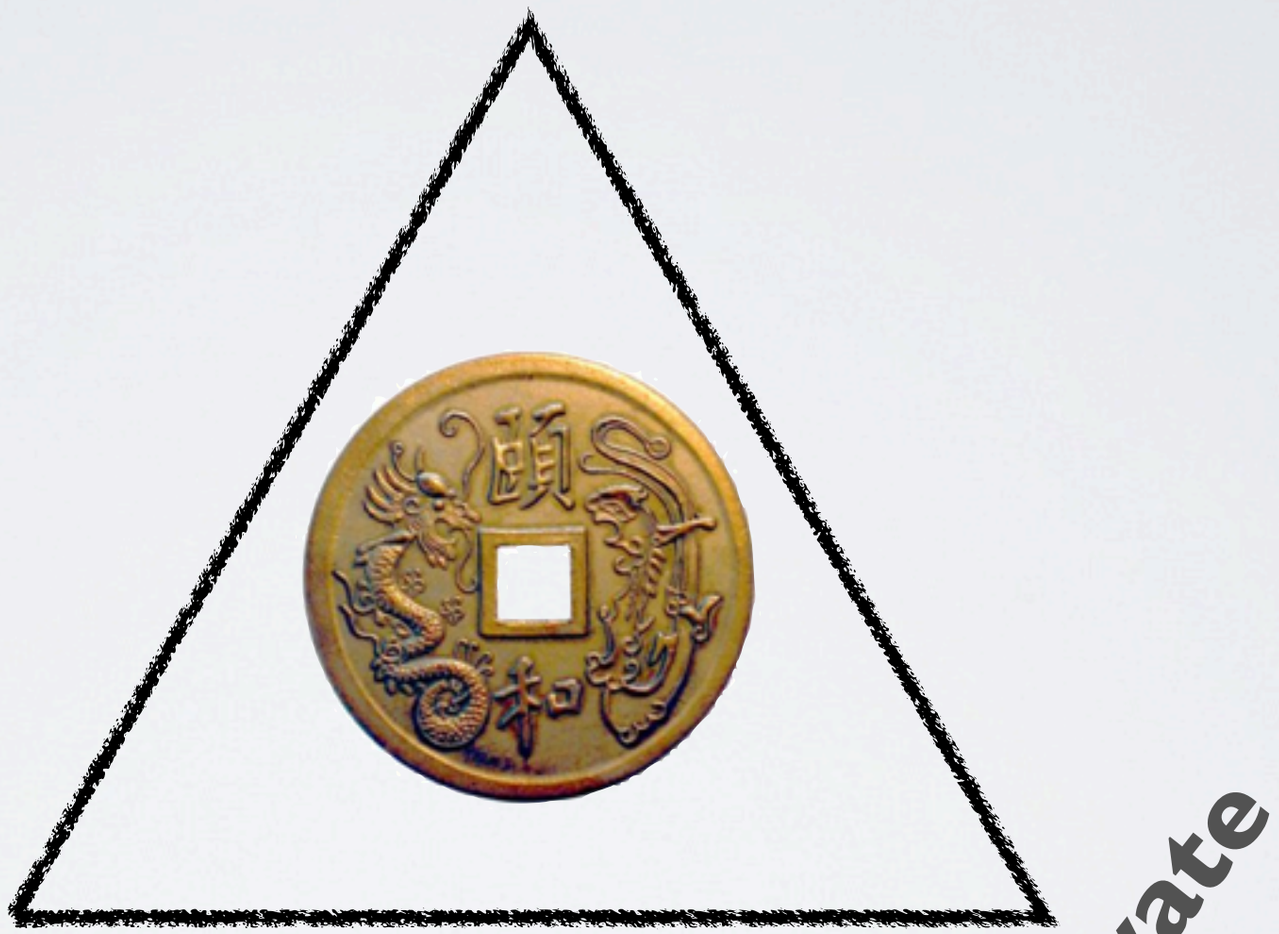


The upshot

- I can take Bitcoin from my wallet
  - Turn them into Zerocoins
  - Where they get ‘mixed up’ with many other users’ coins
  - I can redeem them to a new fresh Wallet
  - Nobody will be able to link the new ones to the old!

Zerocoin

Decentralized



Secure

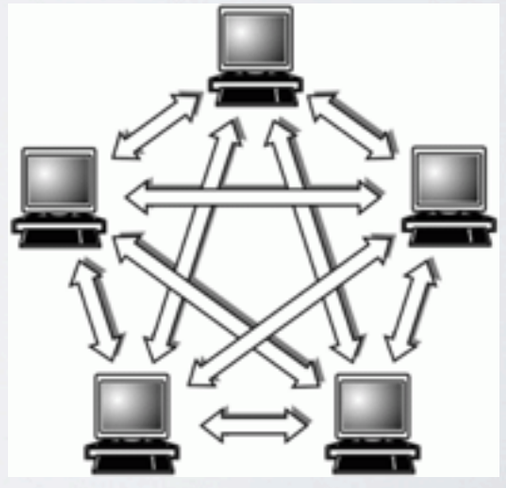
Private

Divisible Zerocoin!

- Make coins divisible!
  - Include coin values in the commitment C
  - Users can insert 'divide' instructions that convert a single Zerocoin into two separate coins that sum to the original value
    - Note: doesn't even require ZK proofs!

Anonymous Credentials!

- Wait a second: e-Cash is just a form of anonymous credential
  - New systems like Namecoin allow us to establish identities (with attributes, e.g., time identity established)
  - By adding similar commitments to the identities/attributes we can prove statements about our identity
  - No trusted credential issuer
  - Can use this to implement decentralized anonymous reputation systems & 'subscription' services to manage resources in ad-hoc networks!



Can we build this today?

- Short answer: yes and no
  - We have code that does all of it (update to the **bitcoind** client)
  - But to make this work we need to get the new transactions built into Bitcoin
  - The algorithms add cost to the Bitcoin network and many will be unwilling to do this

The future

- There's much more to talk about
  - Can something like this be deployed?
  - What are the ethics of doing it?
  - What's the future of Bitcoin as a technology? As a currency?
  - What about identity management?

The paper:

spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

Code & website (coming soon):

zerocoin.org

blog.cryptographyengineering.com