

Zerocoins: 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?



Money

From Wikipedia, the free encyclopedia

For other uses, see [Money \(disambiguation\)](#).

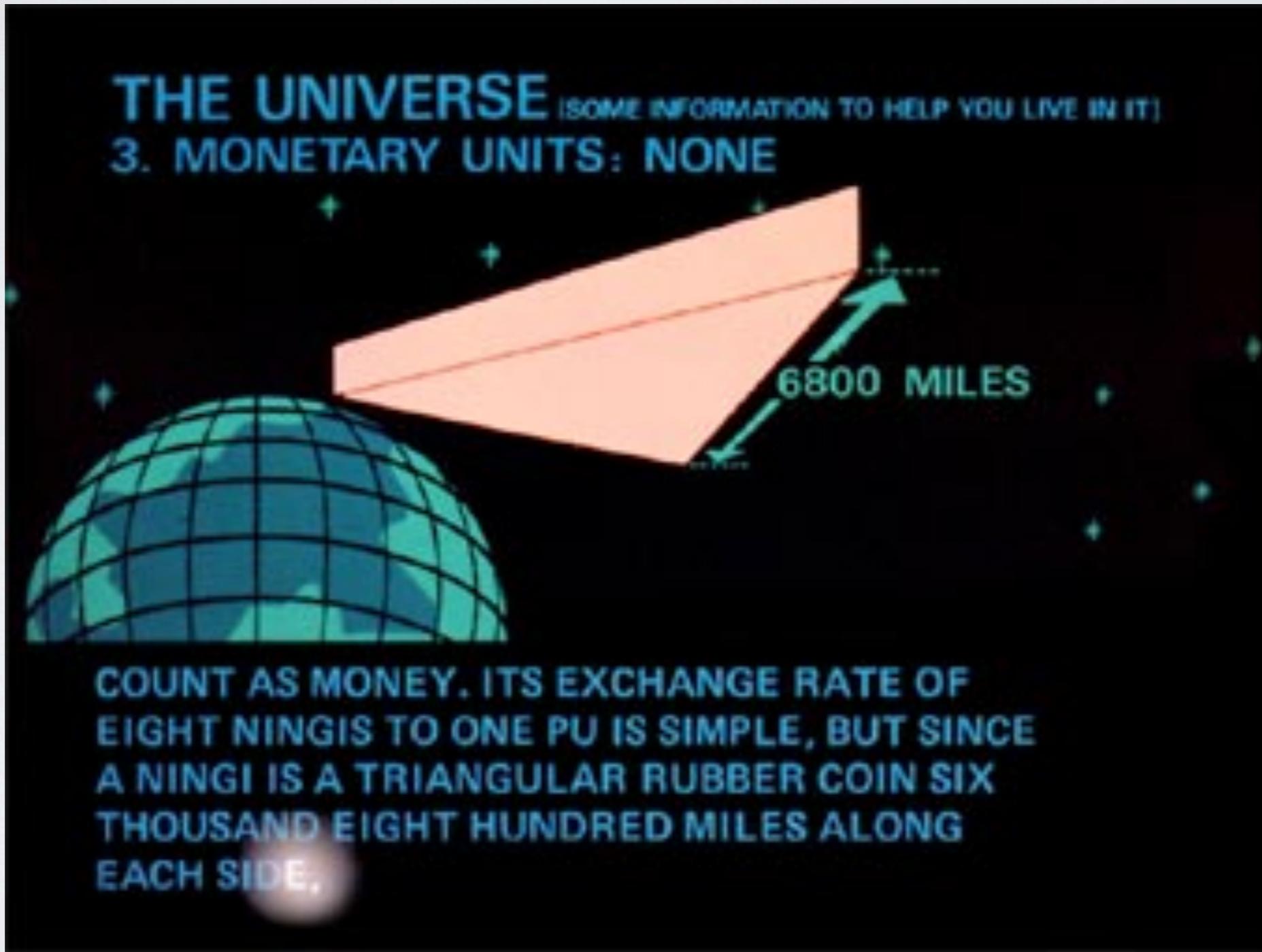
Money is any object or record that is generally accepted as [payment](#) for goods and [services](#) and repayment of [debts](#) in a given socio-economic context or [country](#).^{[1][2][3]} The main functions of money are distinguished as: a [medium of exchange](#), a [unit of account](#); a [store 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?

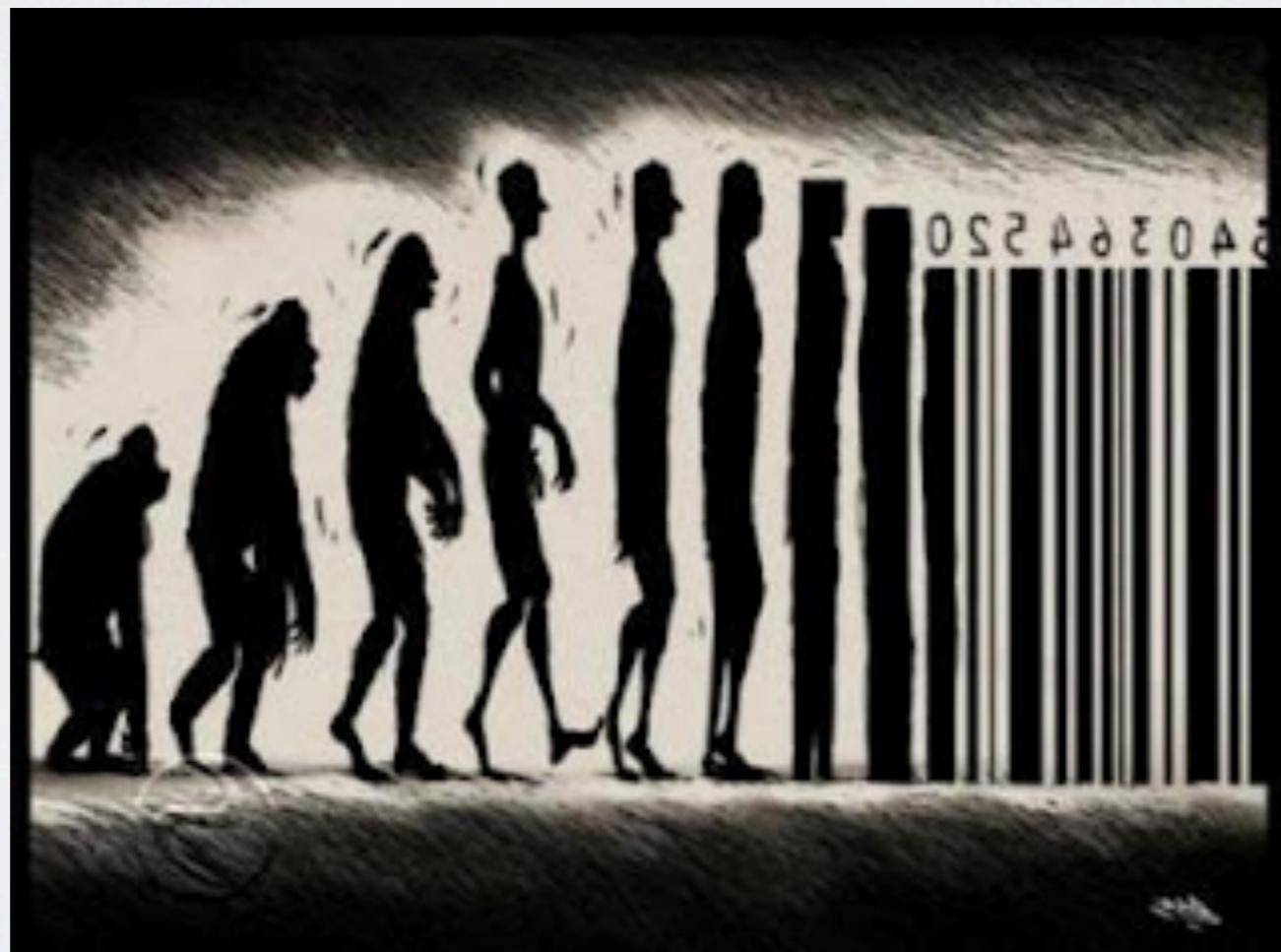


What is money?



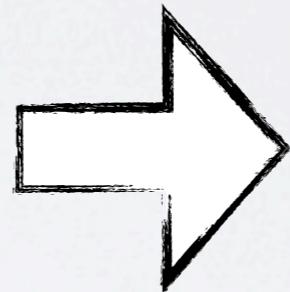
Problem: electronic money

- 1) Very difficult**
- 2) Very simple**



Naive approach

- 1) Very difficult
- 2) Very simple



Account-based approach

- 1) Very difficult
- 2) Very simple**


1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th	13th	14th	15th	16th	17th	18th	19th	20th	21st	22nd	23rd	24th	25th	26th	27th	28th	29th	30th	31st	32nd	33rd	34th	35th	36th	37th	38th	39th	40th	41st	42nd	43rd	44th	45th	46th	47th	48th	49th	50th	51st	52nd	53rd	54th	55th	56th	57th	58th	59th	60th	61st	62nd	63rd	64th	65th	66th	67th	68th	69th	70th	71st	72nd	73rd	74th	75th	76th	77th	78th	79th	80th	81st	82nd	83rd	84th	85th	86th	87th	88th	89th	90th	91st	92nd	93rd	94th	95th	96th	97th	98th	99th	100th	101st	102nd	103rd	104th	105th	106th	107th	108th	109th	110th	111th	112th	113th	114th	115th	116th	117th	118th	119th	120th	121st	122nd	123rd	124th	125th	126th	127th	128th	129th	130th	131st	132nd	133rd	134th	135th	136th	137th	138th	139th	140th	141st	142nd	143rd	144th	145th	146th	147th	148th	149th	150th	151st	152nd	153rd	154th	155th	156th	157th	158th	159th	160th	161st	162nd	163rd	164th	165th	166th	167th	168th	169th	170th	171st	172nd	173rd	174th	175th	176th	177th	178th	179th	180th	181st	182nd	183rd	184th	185th	186th	187th	188th	189th	190th	191st	192nd	193rd	194th	195th	196th	197th	198th	199th	200th	201st	202nd	203rd	204th	205th	206th	207th	208th	209th	210th	211st	212nd	213rd	214th	215th	216th	217th	218th	219th	220th	221st	222nd	223rd	224th	225th	226th	227th	228th	229th	230th	231st	232nd	233rd	234th	235th	236th	237th	238th	239th	240th	241st	242nd	243rd	244th	245th	246th	247th	248th	249th	250th	251st	252nd	253rd	254th	255th	256th	257th	258th	259th	260th	261st	262nd	263rd	264th	265th	266th	267th	268th	269th	270th	271st	272nd	273rd	274th	275th	276th	277th	278th	279th	280th	281st	282nd	283rd	284th	285th	286th	287th	288th	289th	290th	291st	292nd	293rd	294th	295th	296th	297th	298th	299th	300th	301st	302nd	303rd	304th	305th	306th	307th	308th	309th	310th	311st	312nd	313rd	314th	315th	316th	317th	318th	319th	320th	321st	322nd	323rd	324th	325th	326th	327th	328th	329th	330th	331st	332nd	333rd	334th	335th	336th	337th	338th	339th	340th	341st	342nd	343rd	344th	345th	346th	347th	348th	349th	350th	351st	352nd	353rd	354th	355th	356th	357th	358th	359th	360th	361st	362nd	363rd	364th	365th	366th	367th	368th	369th	370th	371st	372nd	373rd	374th	375th	376th	377th	378th	379th	380th	381st	382nd	383rd	384th	385th	386th	387th	388th	389th	390th	391st	392nd	393rd	394th	395th	396th	397th	398th	399th	400th	401st	402nd	403rd	404th	405th	406th	407th	408th	409th	410th	411st	412nd	413rd	414th	415th	416th	417th	418th	419th	420th	421st	422nd	423rd	424th	425th	426th	427th	428th	429th	430th	431st	432nd	433rd	434th	435th	436th	437th	438th	439th	440th	441st	442nd	443rd	444th	445th	446th	447th	448th	449th	450th	451st	452nd	453rd	454th	455th	456th	457th	458th	459th	460th	461st	462nd	463rd	464th	465th	466th	467th	468th	469th	470th	471st	472nd	473rd	474th	475th	476th	477th	478th	479th	480th	481st	482nd	483rd	484th	485th	486th	487th	488th	489th	490th	491st	492nd	493rd	494th	495th	496th	497th	498th	499th	500th	501st	502nd	503rd	504th	505th	506th	507th	508th	509th	510th	511st	512nd	513rd	514th	515th	516th	517th	518th	519th	520th	521st	522nd	523rd	524th	525th	526th	527th	528th	529th	530th	531st	532nd	533rd	534th	535th	536th	537th	538th	539th	540th	541st	542nd	543rd	544th	545th	546th	547th	548th	549th	550th	551st	552nd	553rd	554th	555th	556th	557th	558th	559th	560th	561st	562nd	563rd	564th	565th	566th	567th	568th	569th	570th	571st	572nd	573rd	574th	575th	576th	577th	578th	579th	580th	581st	582nd	583rd	584th	585th	586th	587th	588th	589th	590th	591st	592nd	593rd	594th	595th	596th	597th	598th	599th	600th	601st	602nd	603rd	604th	605th	606th	607th	608th	609th	610th	611st	612nd	613rd	614th	615th	616th	617th	618th	619th	620th	621st	622nd	623rd	624th	625th	626th	627th	628th	629th	630th	631st	632nd	633rd	634th	635th	636th	637th	638th	639th	640th	641st	642nd	643rd	644th	645th	646th	647th	648th	649th	650th	651st	652nd	653rd	654th	655th	656th	657th	658th	659th	660th	661st	662nd	663rd	664th	665th	666th	667th	668th	669th	670th	671st	672nd	673rd	674th	675th	676th	677th	678th	679th	680th	681st	682nd	683rd	684th	685th	686th	687th	688th	689th	690th	691st	692nd	693rd	694th	695th	696th	697th	698th	699th	700th	701st	702nd	703rd	704th	705th	706th	707th	708th	709th	710th	711st	712nd	713rd	714th	715th	716th	717th	718th	719th	720th	721st	722nd	723rd	724th	725th	726th	727th	728th	729th	730th	731st	732nd	733rd	734th	735th	736th	737th	738th	739th	740th	741st	742nd	743rd	744th	745th	746th	747th	748th	749th	750th	751st	752nd	753rd	754th	755th	756th	757th	758th	759th	760th	761st	762nd	763rd	764th	765th	766th	767th	768th	769th	770th	771st	772nd	773rd	774th	775th	776th	777th	778th	779th	780th	781st	782nd	783rd	784th	785th	786th	787th	788th	789th	790th	791st	792nd	793rd	794th	795th	796th	797th	798th	799th	800th	801st	802nd	803rd	804th	805th	806th	807th	808th	809th	810th	811st	812nd	813rd	814th	815th	816th	817th	818th	819th	820th	821st	822nd	823rd	824th	825th	826th	827th	828th	829th	830th	831st	832nd	833rd	834th	835th	836th	837th	838th	839th	840th	841st	842nd	843rd	844th	845th	846th	847th	848th	849th	850th	851st	852nd	853rd	854th	855th	856th	857th	858th	859th	860th	861st	862nd	863rd	864th	865th	866th	867th	868th	869th	870th	871st	872nd	873rd	874th	875th	876th	877th	878th	879th	880th	881st	882nd	883rd	884th	885th	886th	887th	888th	889th	890th	891st	892nd	893rd	894th	895th	896th	897th	898th	899th	900th	901st	902nd	903rd	904th	905th	906th	907th	908th	909th	910th	911st	912nd	913rd	914th	915th	916th	917th	918th</

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

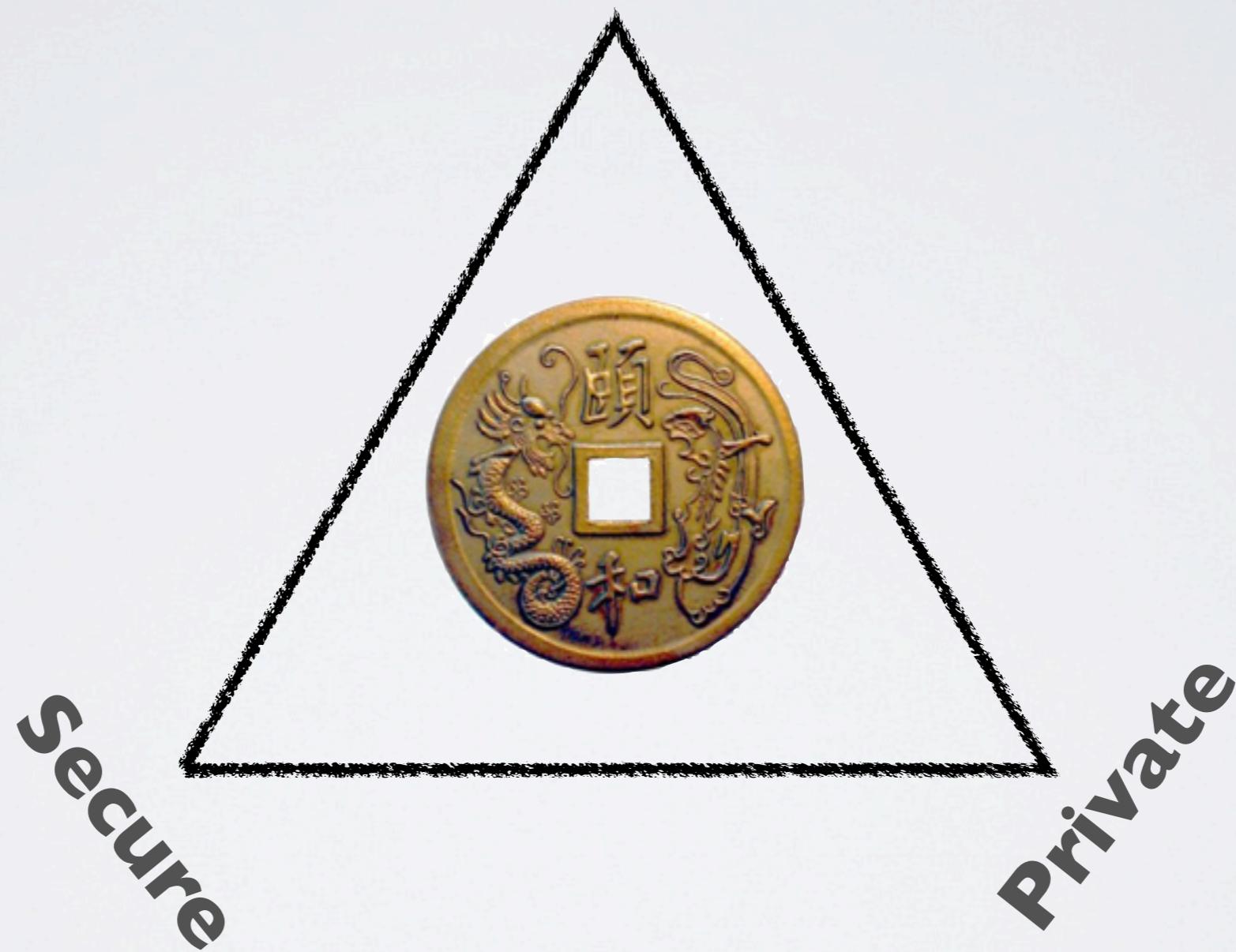
- **Privacy**

- The bank sees every transaction you make!



“Ideal electronic currency”

Decentralized



Bitcoin



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.

REMITTER JONATHAN BEN

PAY TO THE ORDER OF Alice

Peoples Bank
OF NORTHERN KENTUCKY
CRESTVIEW HILLS, KENTUCKY

203064 5-20-04 73-226421

\$ 9,500.00

NINE THOUSAND FIVE HUNDRED DOLLARS

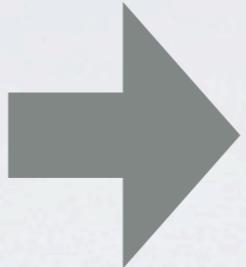
THIS DOCUMENT HAS A MICRO-PRINT SIGNATURE LINE, WATERMARK AND A THERMOCHROMIC ICON; ABSENCE OF THESE FEATURES WILL INDICATE A COPY.

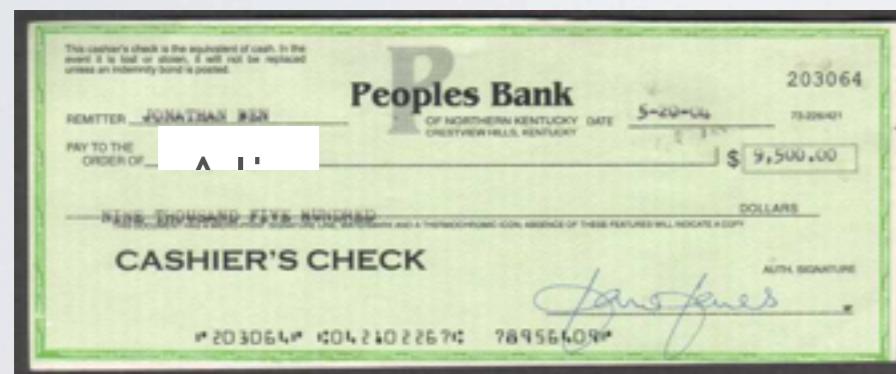
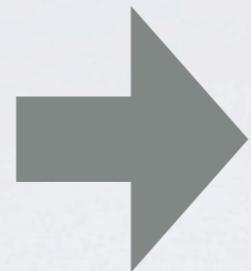
CASHIER'S CHECK

AUTH. SIGNATURE

[Handwritten signature of Jonathan Ben]

■ 203064 ■ 10421022671 ■ 78956409 ■





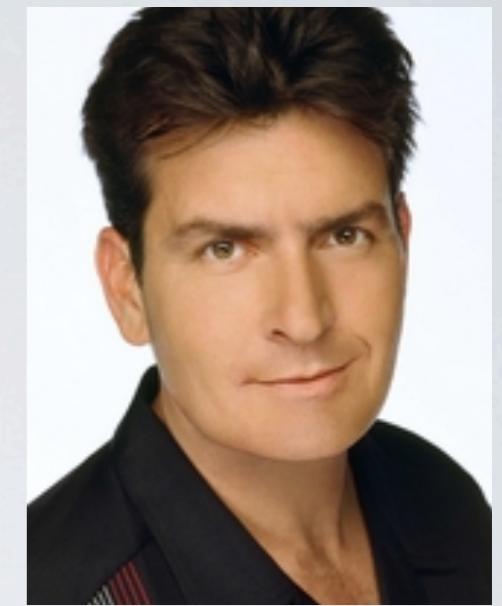
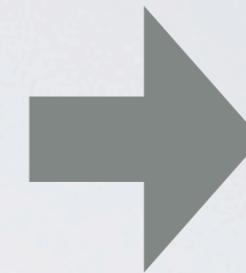
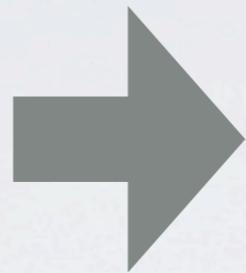
ENDORSE CHECK HERE

Pay to the order of Bob

& Alice

DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE

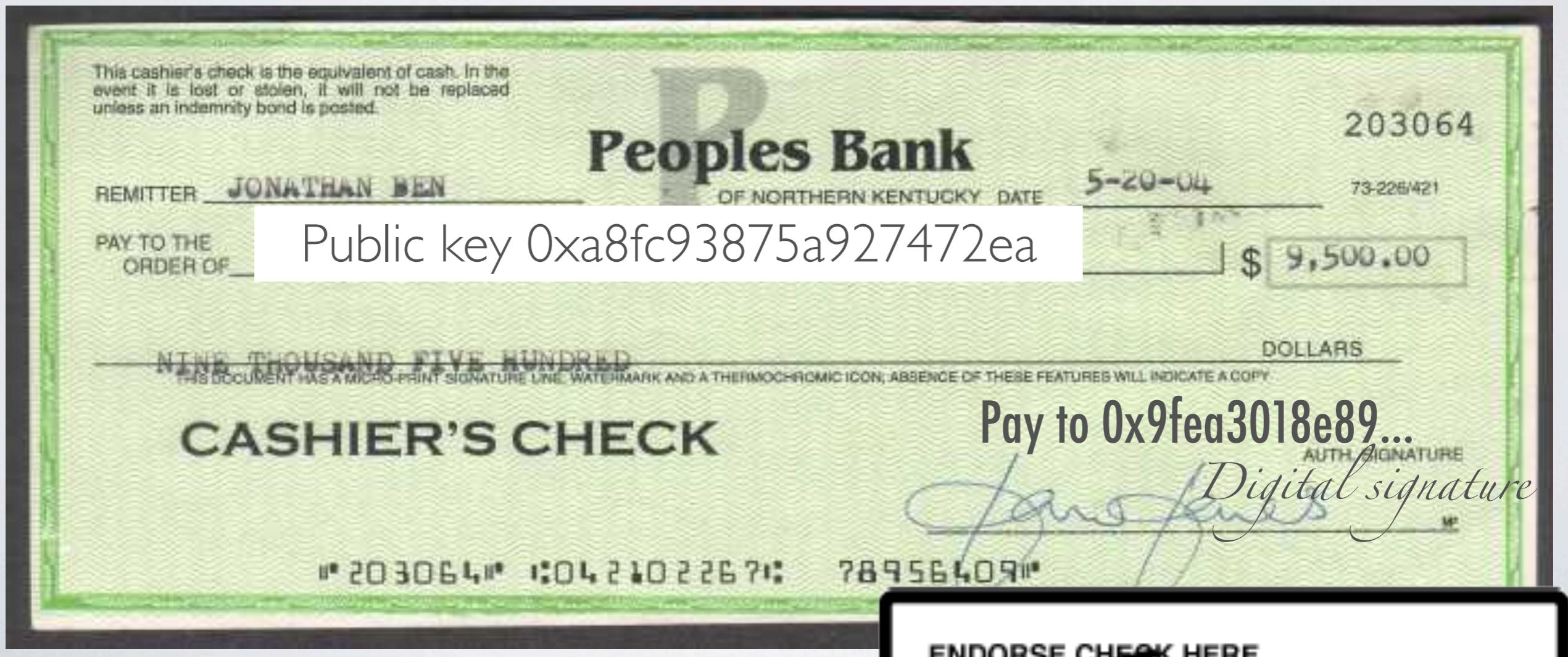
↓



ENDORSE CHECK HERE	
<input checked="" type="checkbox"/>	<u>Pay to the order of Bob</u> <i>Alice</i>
<input type="checkbox"/>	<u>Pay to the order of Charlie</u> <i>Bob</i>
<hr/> <hr/>	
DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE	
↓	

Can we make this electronic?

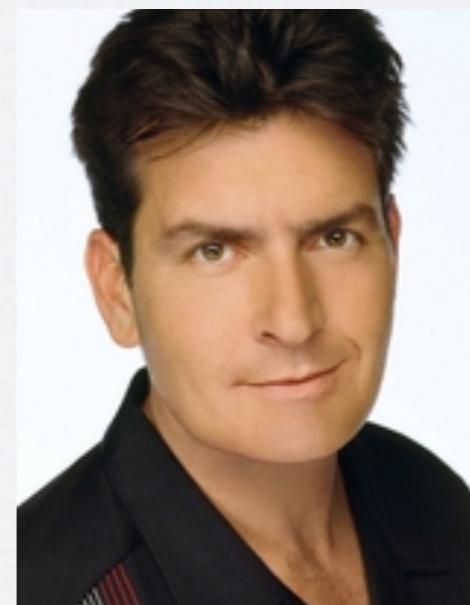
- Idea:
 - Replace names with public keys
 - Replace handwritten signatures with digital signatures



Can we make this electronic?

- **Problem: Alice can still double spend!**

- Alice “gives” the same check to Bob and Charlie



<small>ENDORSE CHECK HERE</small>	<input checked="" type="checkbox"/> Pay to the order of Bob
<i>Alice</i>	
DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE	
↓	
<small>ENDORSE CHECK HERE</small>	<input checked="" type="checkbox"/> Pay to the order of Charlie
<i>Alice</i>	
DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE	
↓	

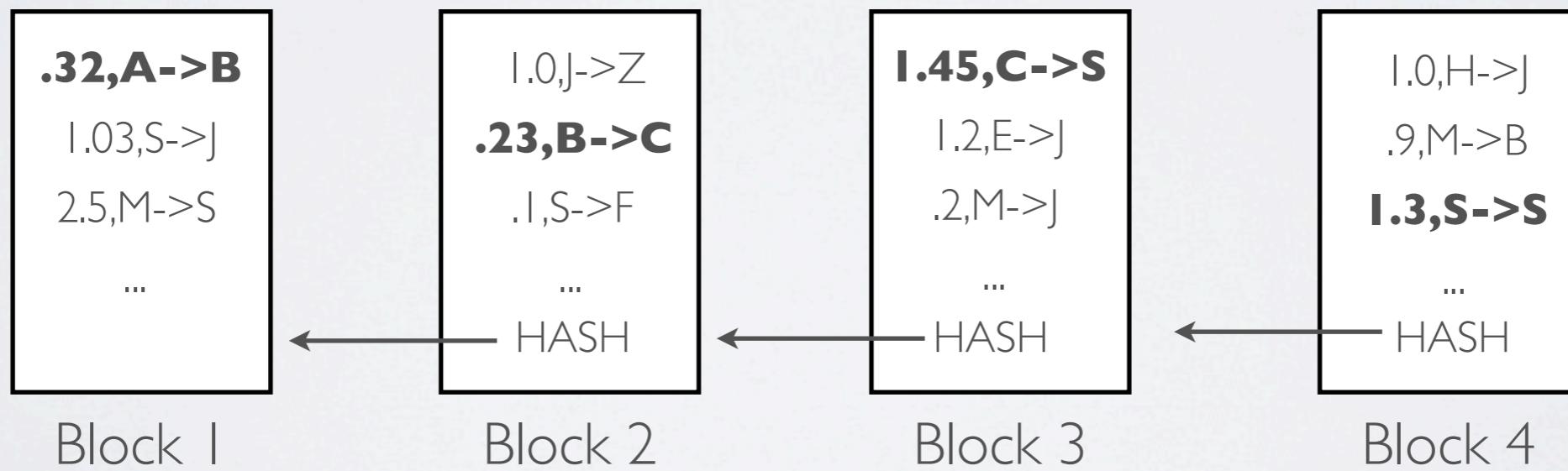
Double-spending

- 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??



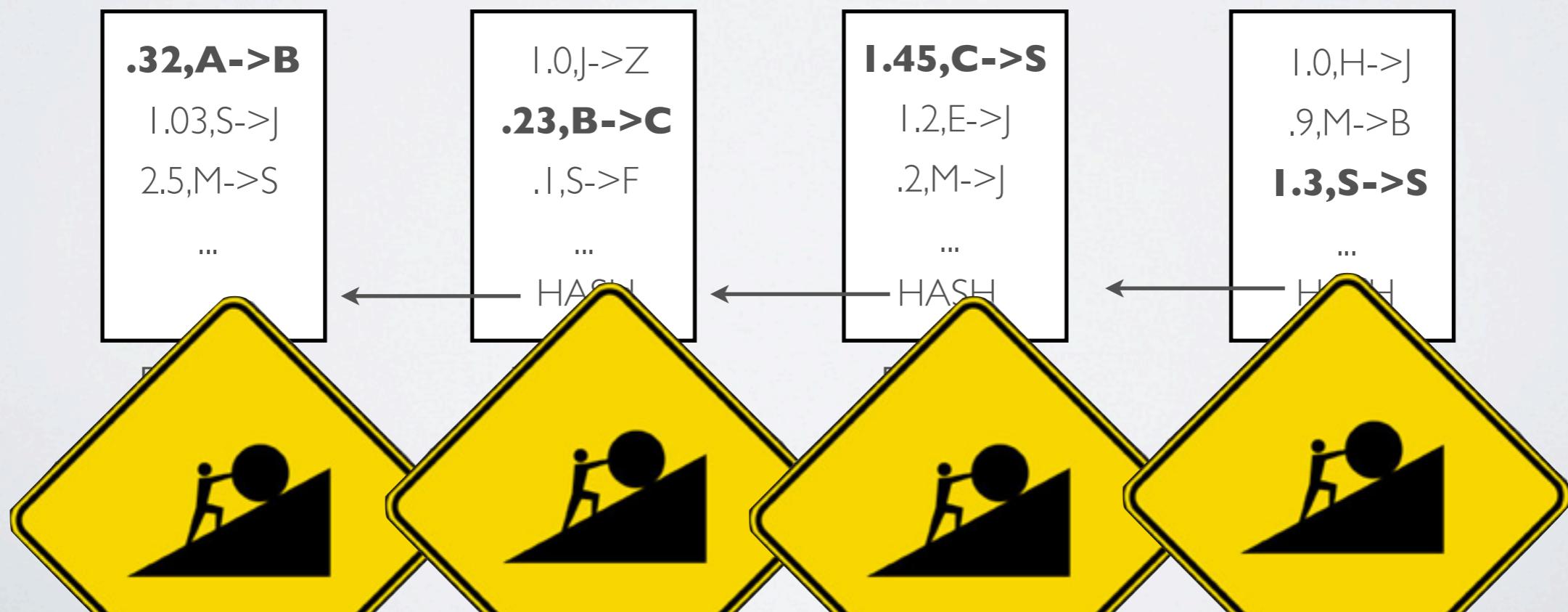
The block chain

- 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



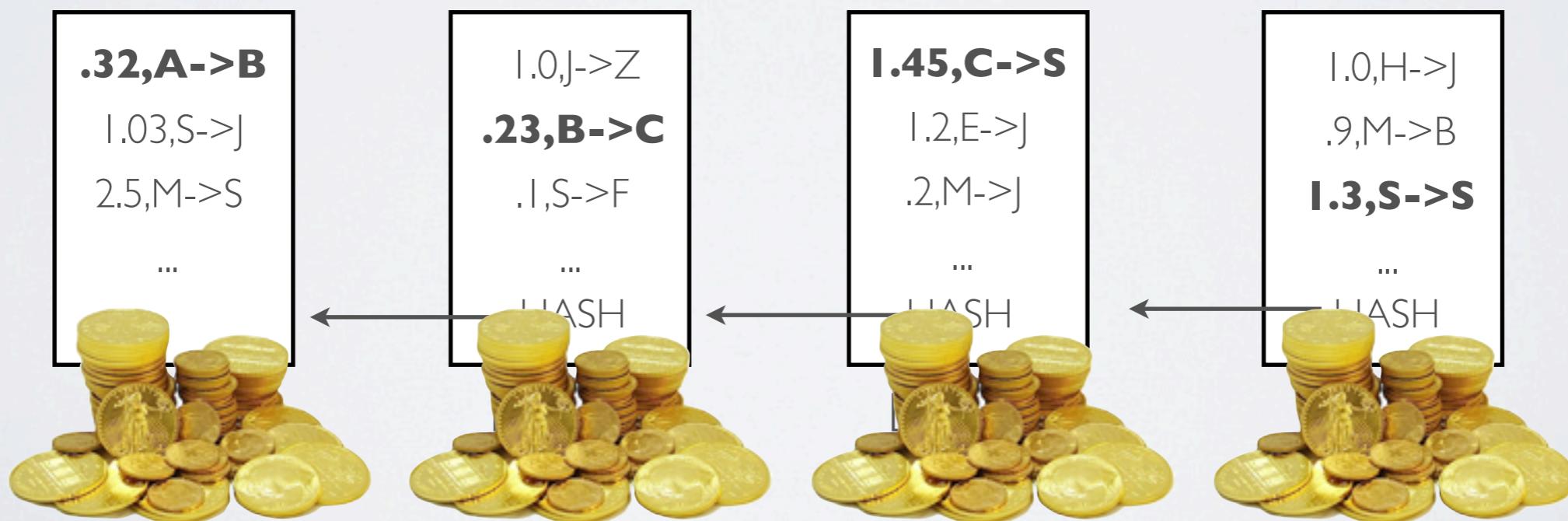
The block chain

- 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

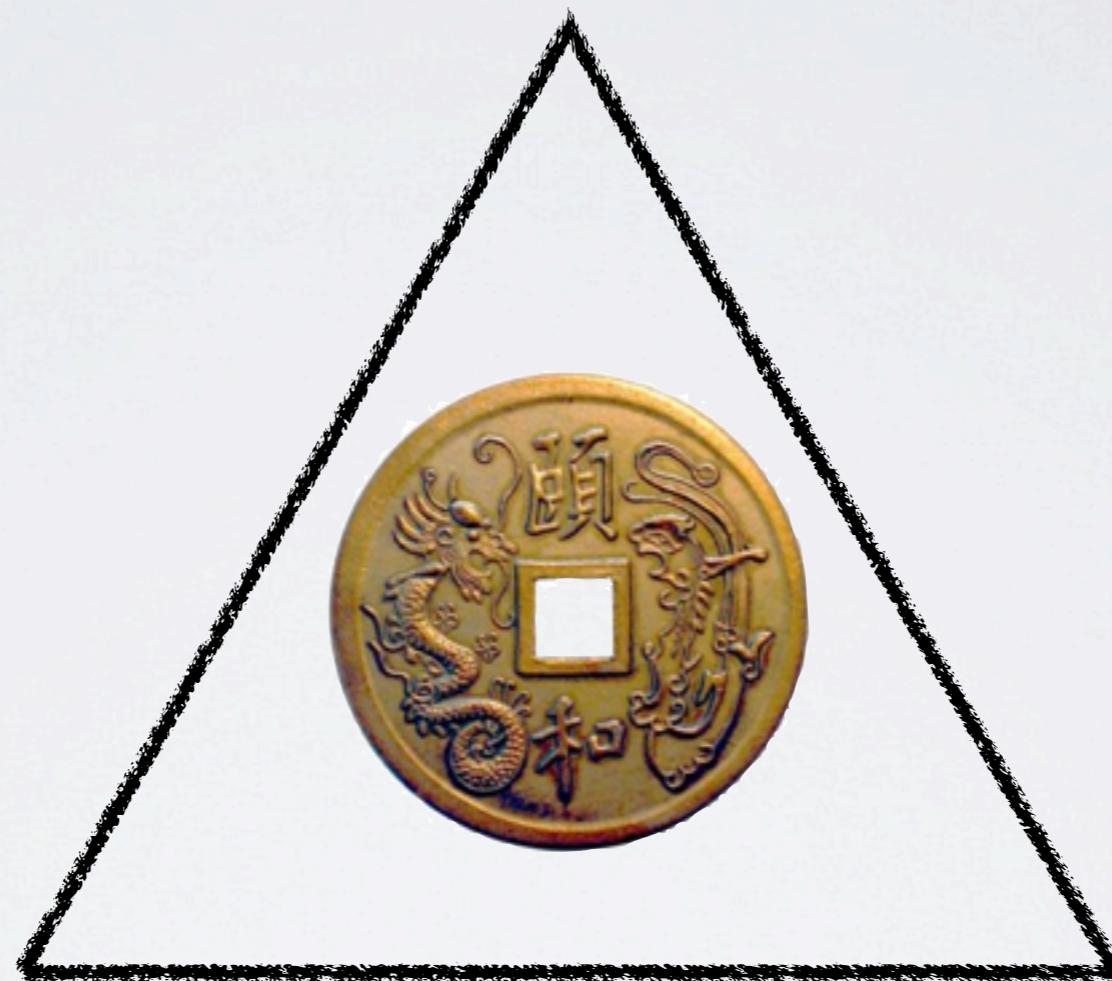


The block chain

- 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)

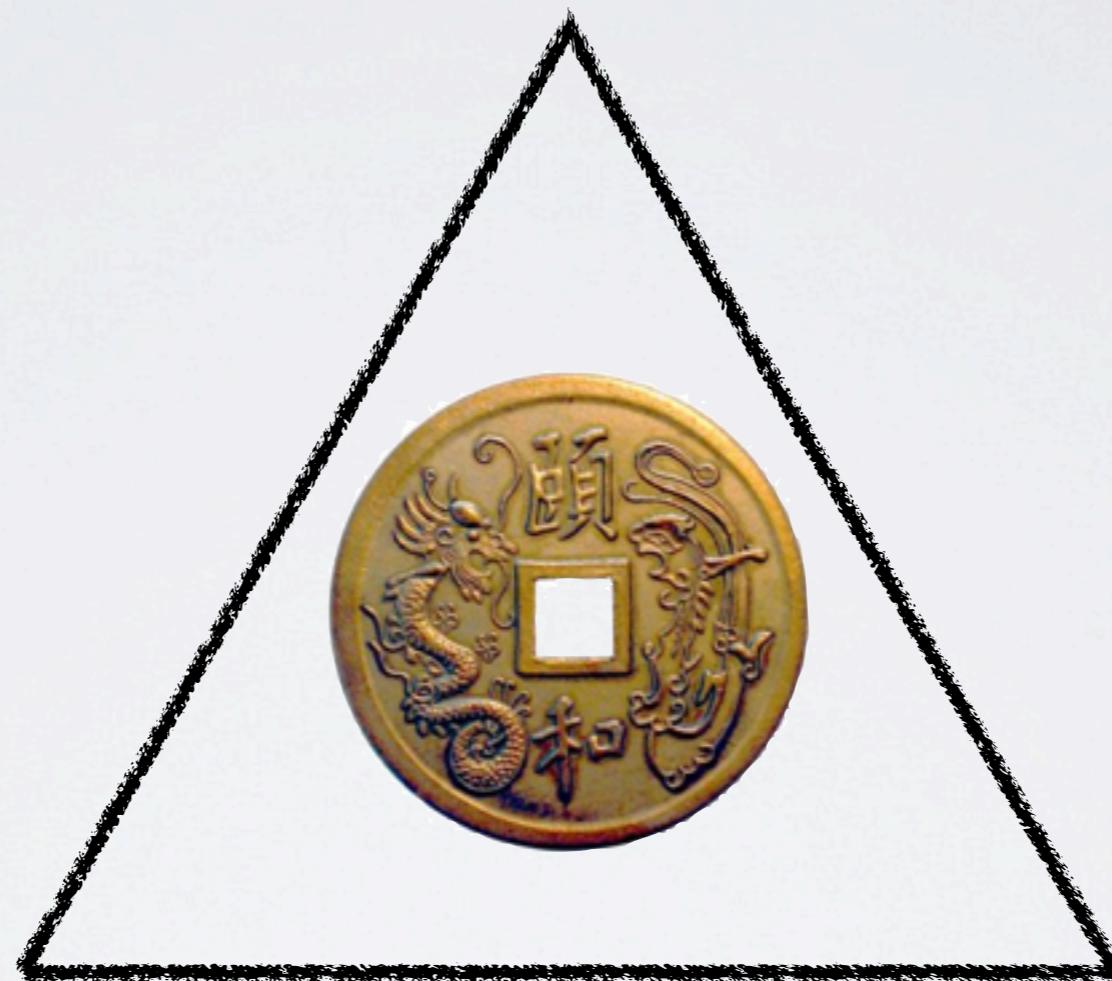


Bitcoin triangle



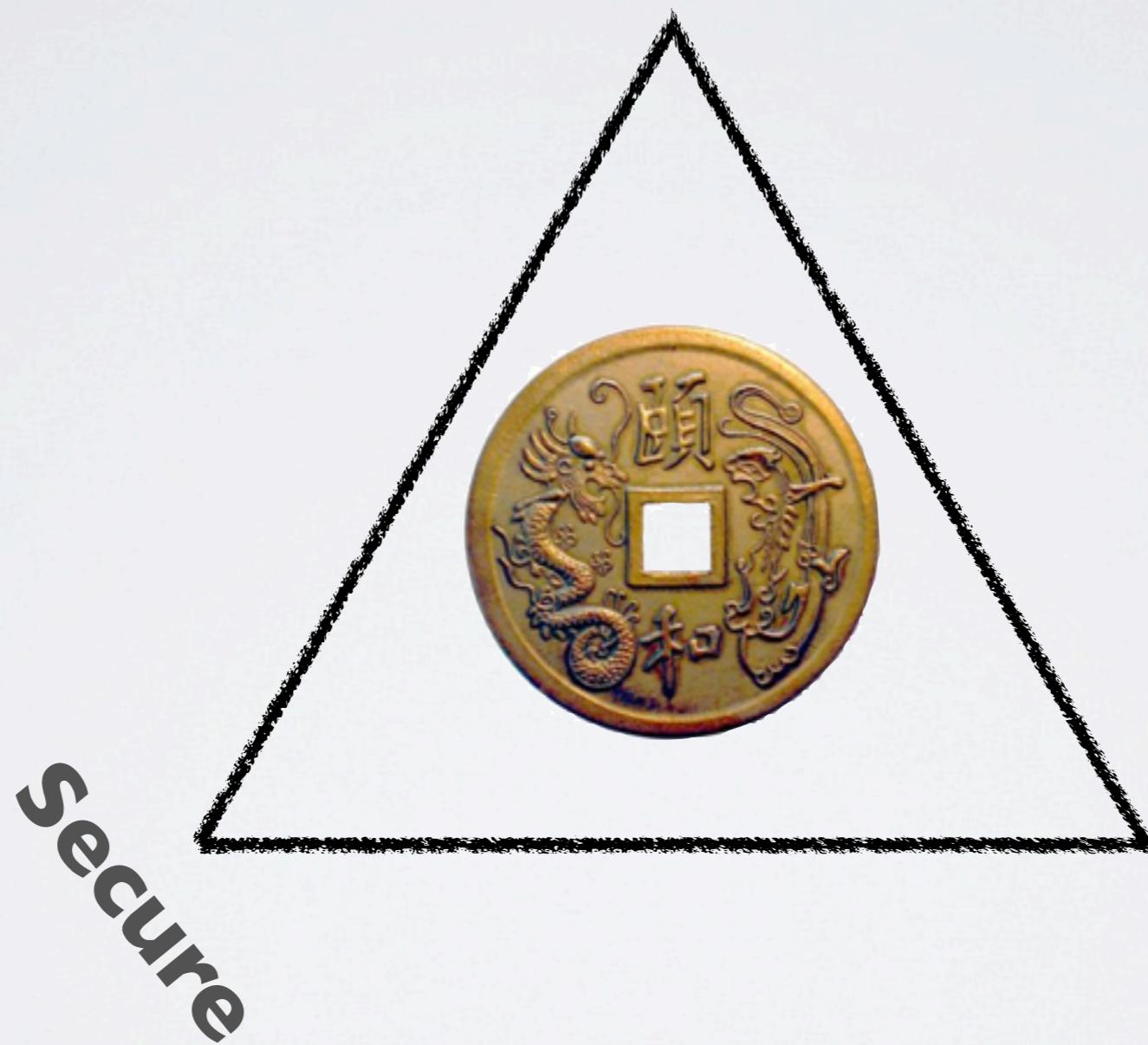
Bitcoin triangle

Decentralized



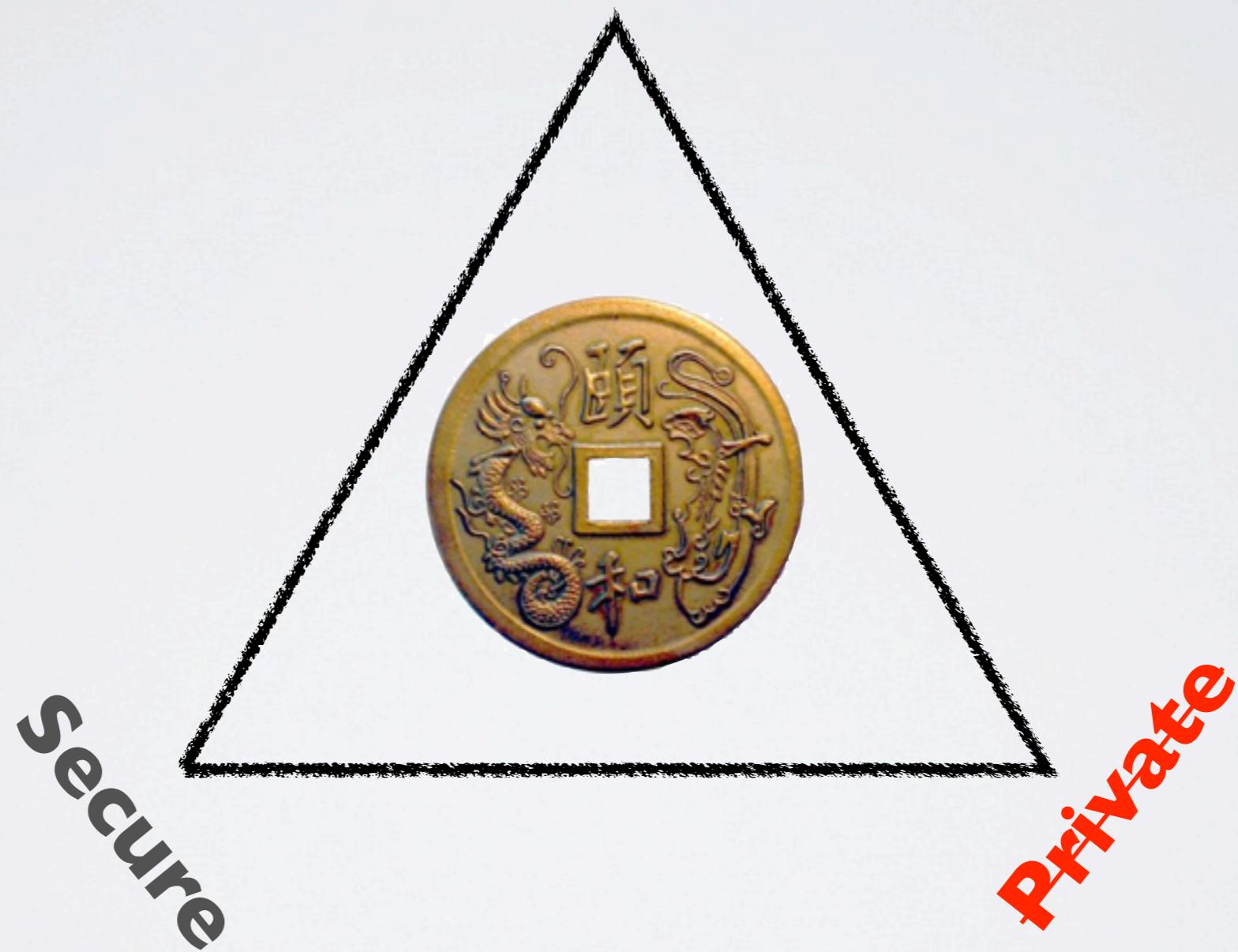
Bitcoin triangle

Decentralized



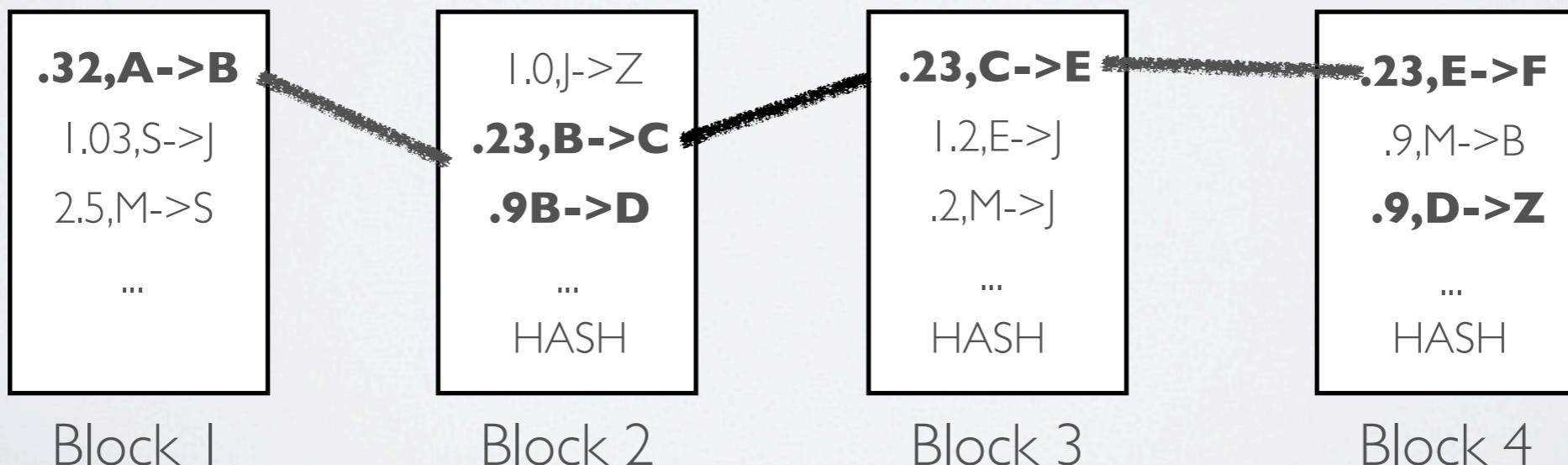
Bitcoin triangle

Decentralized



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!

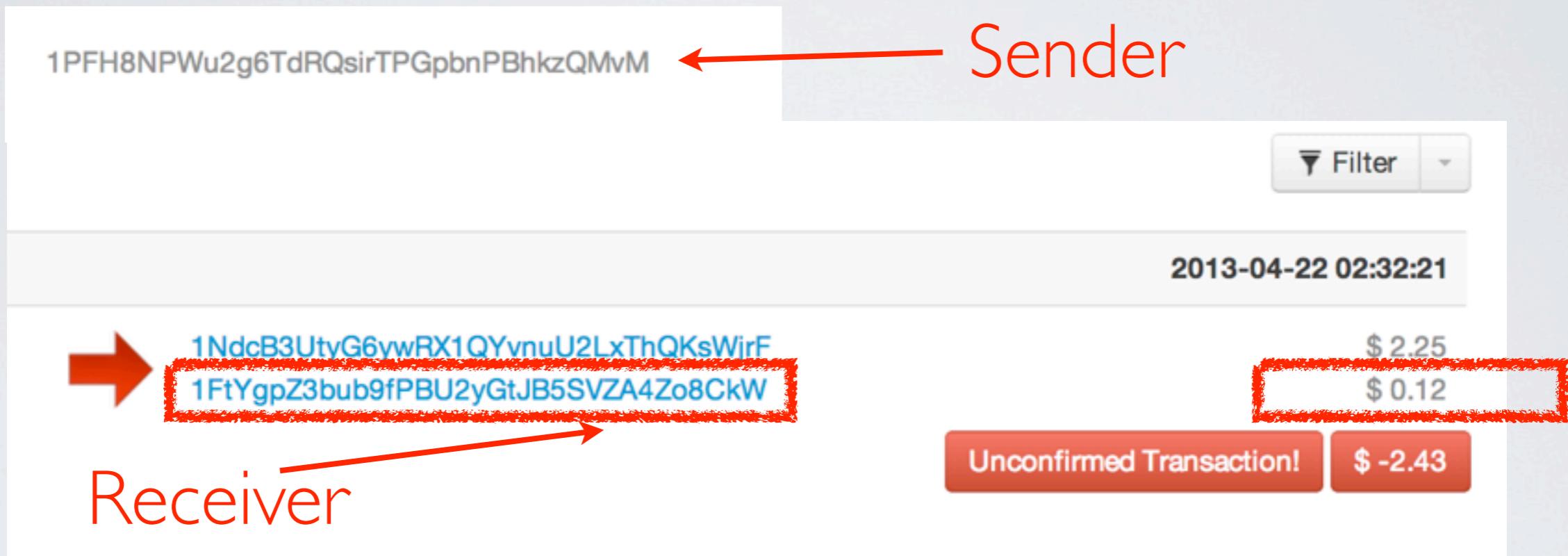


Bitcoin privacy

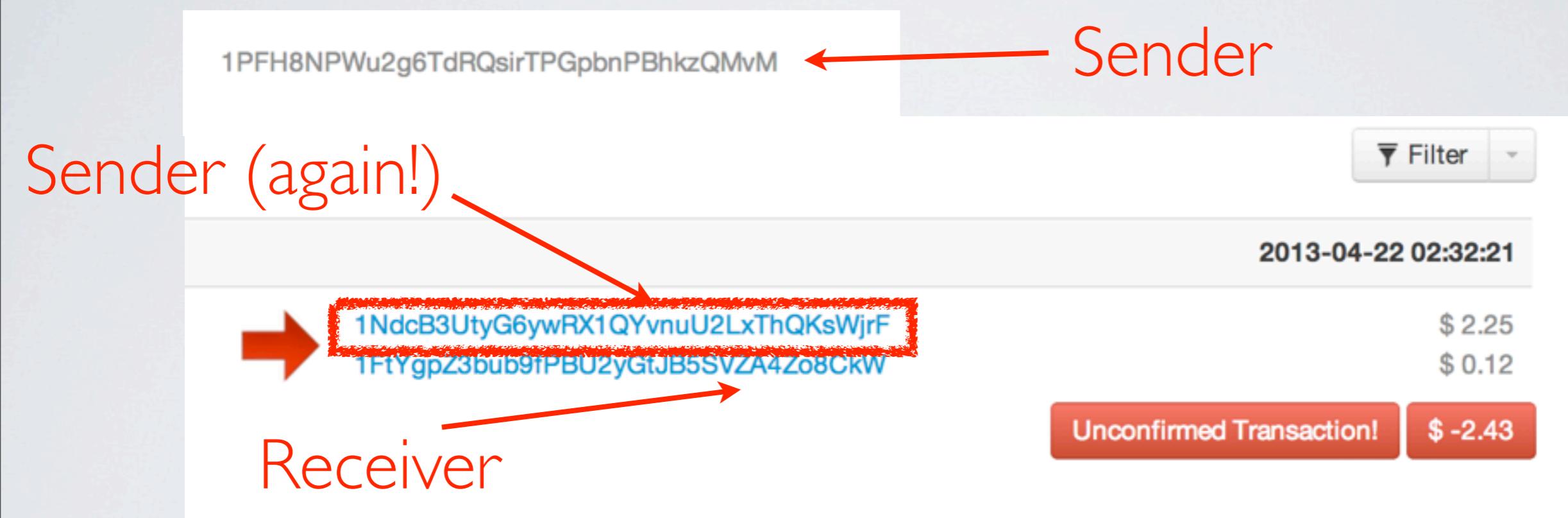
A screenshot of a Bitcoin transaction history interface. At the top left, a Bitcoin address is shown: 1PFH8NPWu2g6TdRQsirTPGpbnPBhkzQMvM. A red arrow points from the word "Sender" to this address. At the top right, there is a "Filter" button. Below the addresses, the timestamp 2013-04-22 02:32:21 is displayed. The main transaction list shows two entries: one recipient receiving \$2.25 and another receiving \$0.12. A red arrow points from the word "Receiver" to the recipient addresses. At the bottom right, a red box highlights the status "Unconfirmed Transaction!" and the amount "\$ -2.43".

Recipient	Amount
1NdcB3UtyG6ywRX1QYvnuU2LxThQKsWjrF	\$ 2.25
1FtYgpZ3bub9fPBU2yGtJB5SVZA4Zo8CkW	\$ 0.12
Unconfirmed Transaction! \$ -2.43	

Bitcoin privacy



Bitcoin privacy



Bitcoin privacy

Evaluating User Privacy in Bitcoin

Elli Androulaki¹, Ghassan O. Karame², Marc Roeschlin¹,
Tobias Scherer¹, and Srdjan Capkun¹

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

cross 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 transaction graph.

...nic cash, payment systems, trans-

Bitcoin privacy

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](#).

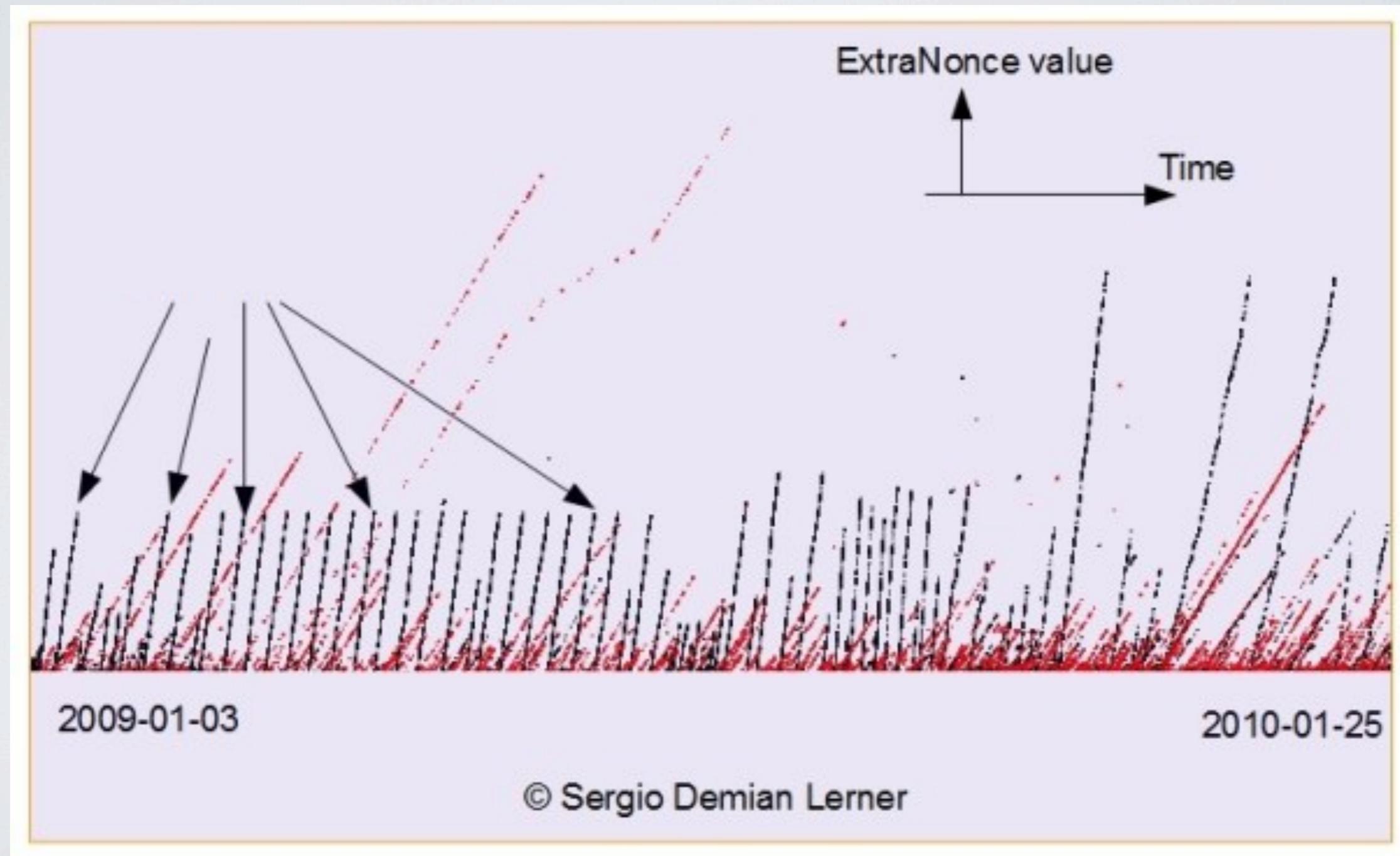
Update (January 1, 2013): We received many requests for an up to date, human-readable copy of the block chain, which can be difficult to extract using existing tools. One of the authors, [Martin Harrigan](#), has released [QuantaBytes](#) to this end. It provides up to date copies of the block chain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

Friday, September 30, 2011

Bitcoin is not Anonymous

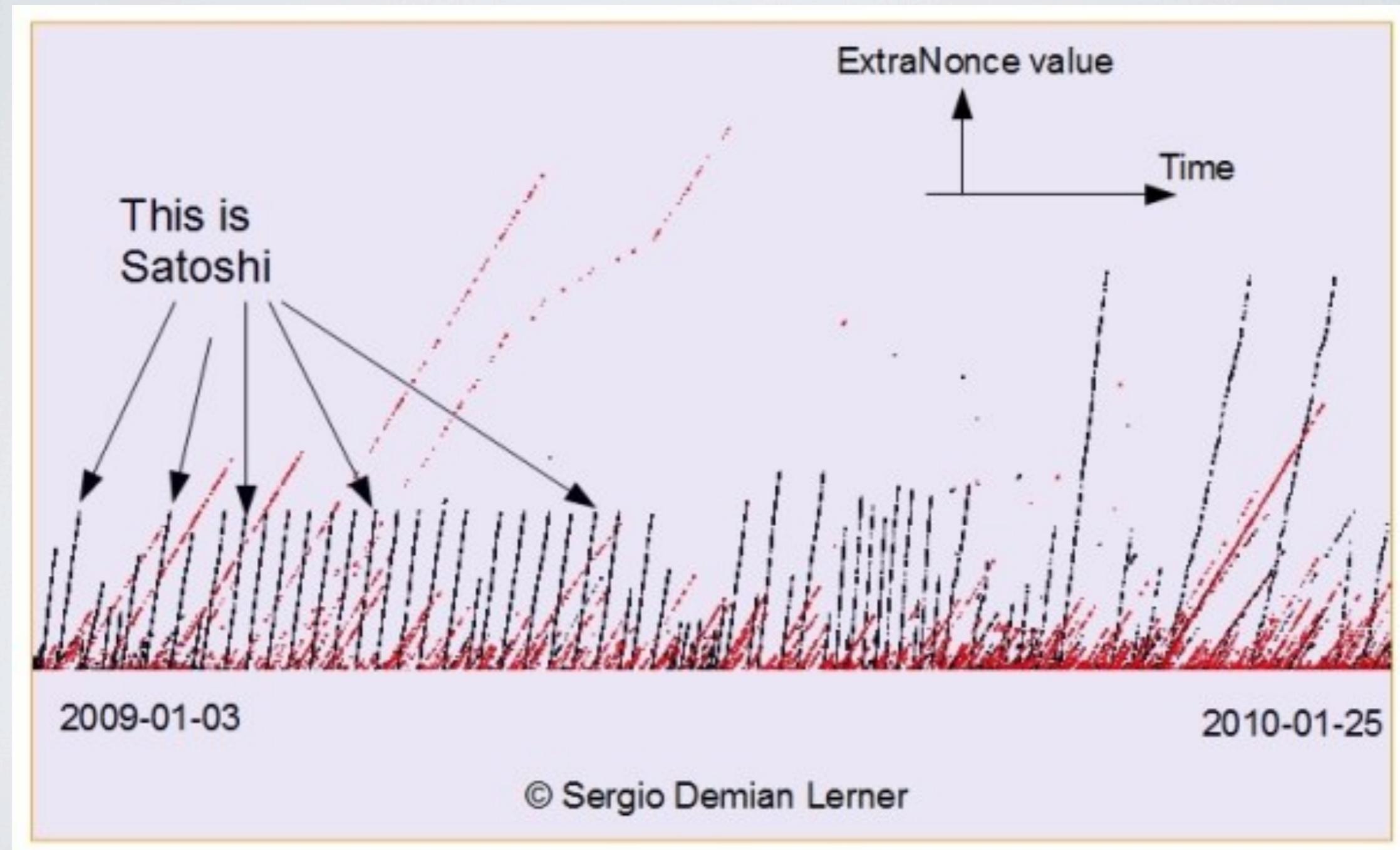
TL;DR

[Bitcoin](#) is not inherently anonymous. It may be possible to conduct transactions in such a way so as to obscure your identity, but, in many cases, users and their transactions can be identified. We have performed an analysis of anonymity in the Bitcoin system.



<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



LAUNDER
BITCOINS

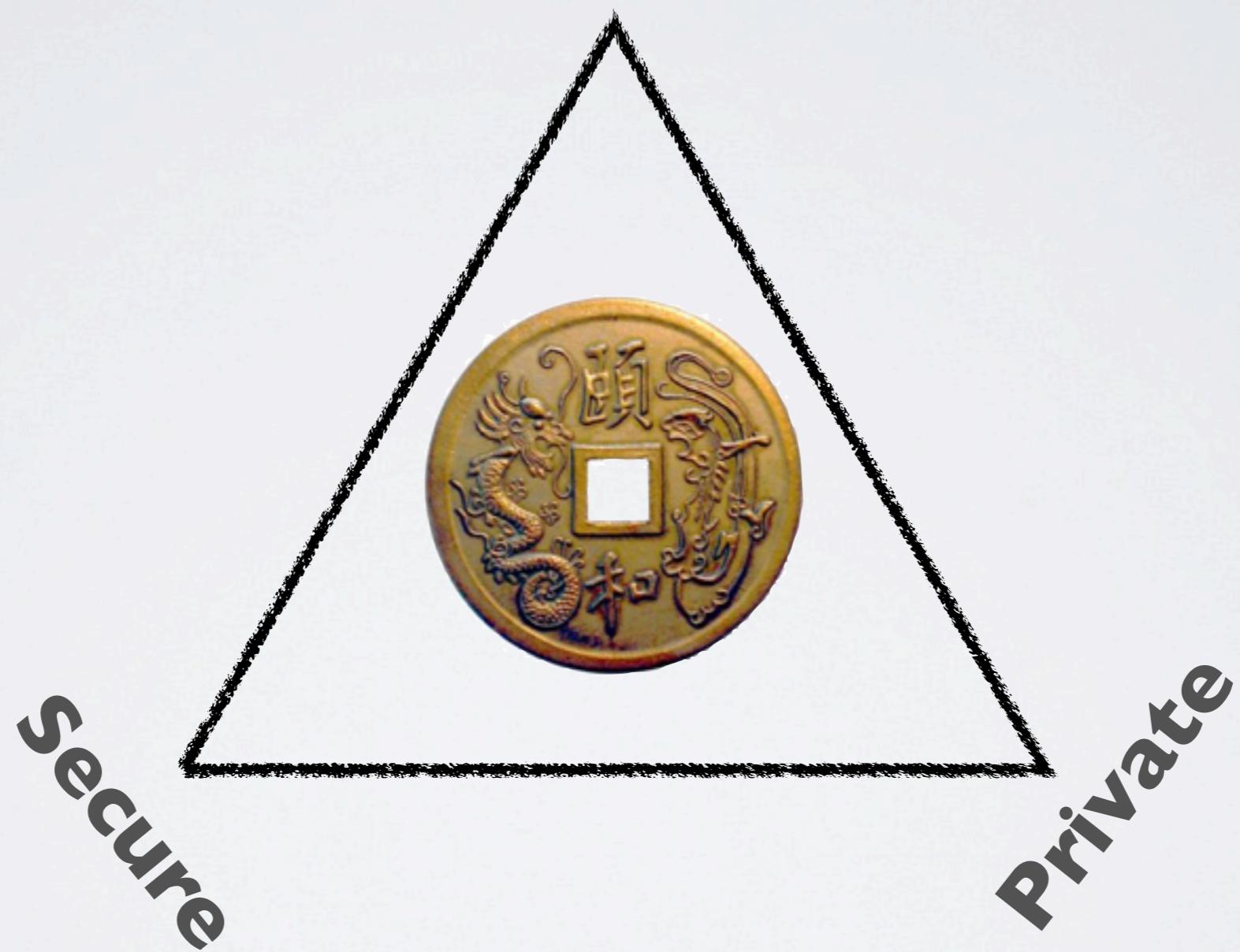
Chaumian e-Cash

- 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



Laundries & Chaum

Decentralized



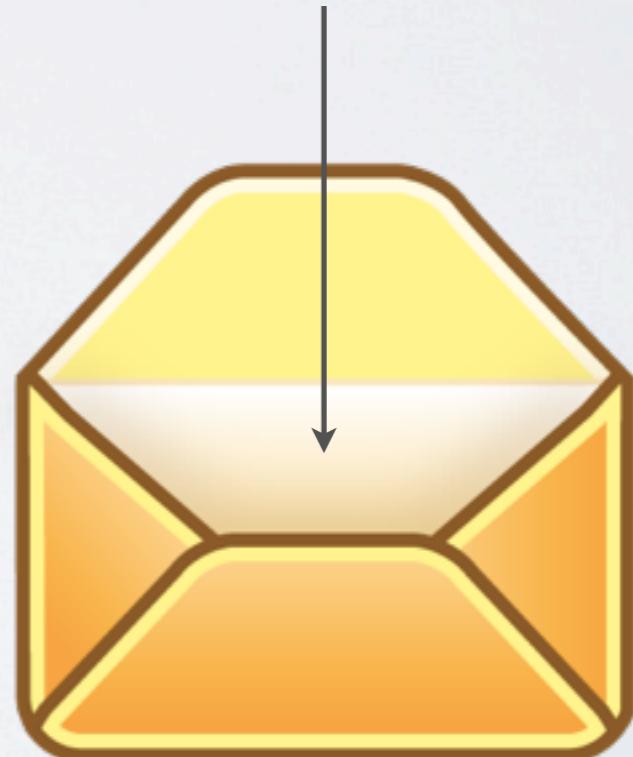
Zerocoins

- 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 Zerocoins

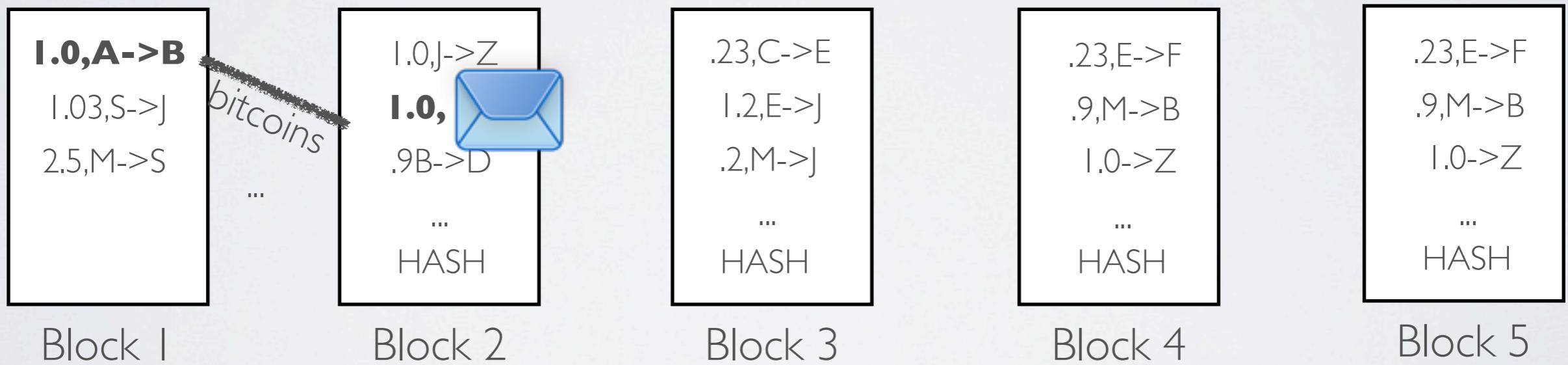
- Zerocoins are just numbers
 - Each is a digital commitment to a random serial number
 - Anyone can make one!

823848273471012983

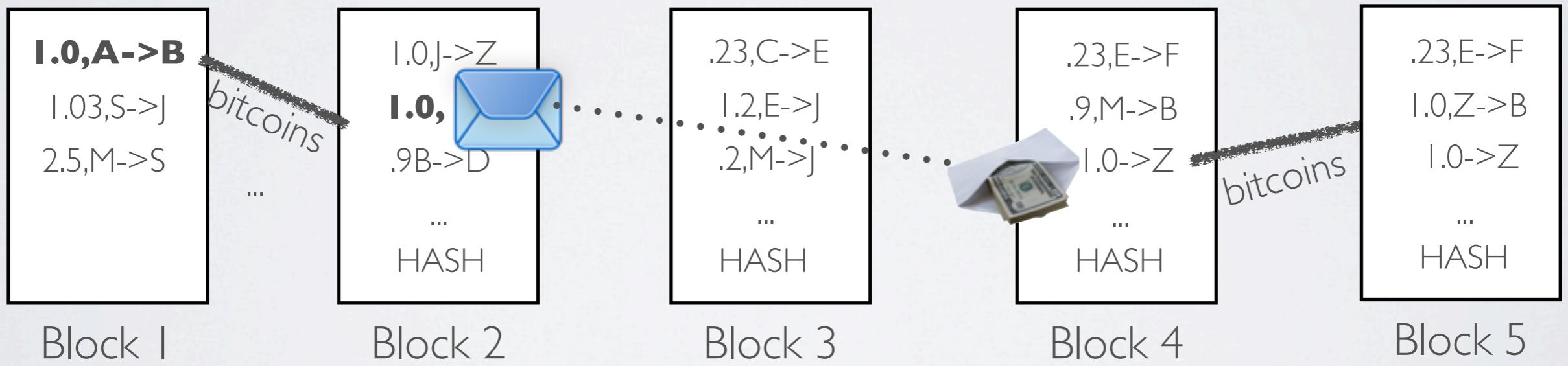


Making Zerocoins

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

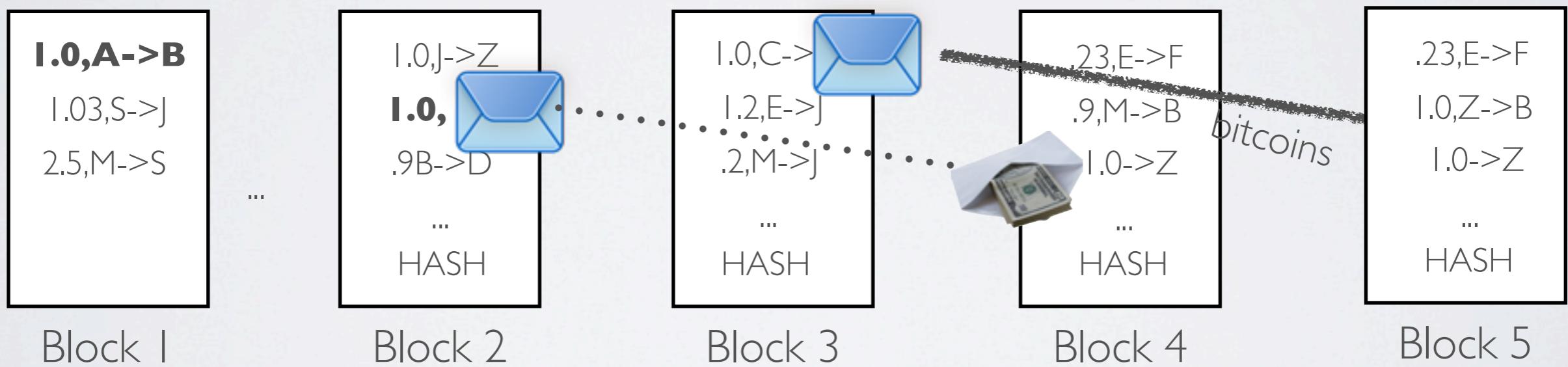


Spending Zerocoins



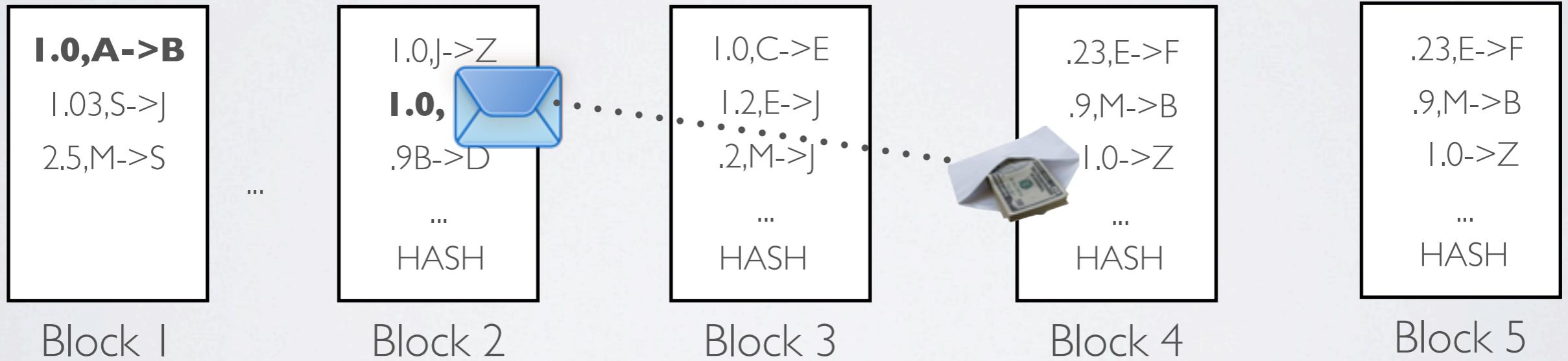
Spending Zerocoins

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



Spending Zerocoins

- Why is this anonymous?
 - It's all in the way we 'prove' we have a Zerocoins
 - 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 Zerocoins

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

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

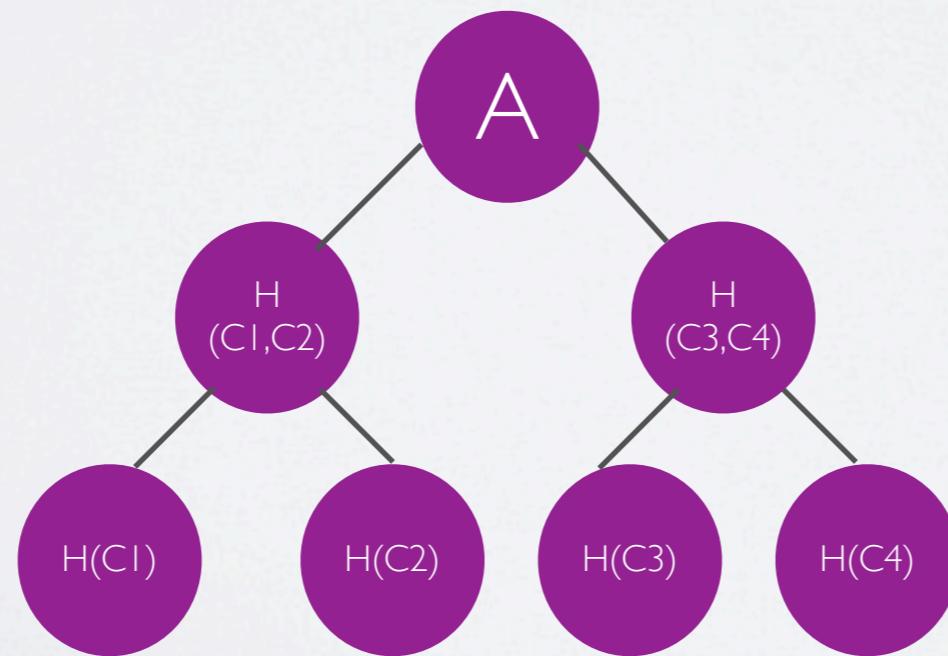
These ‘or’ proofs have cost $O(N)$

Spending Zerocoin

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

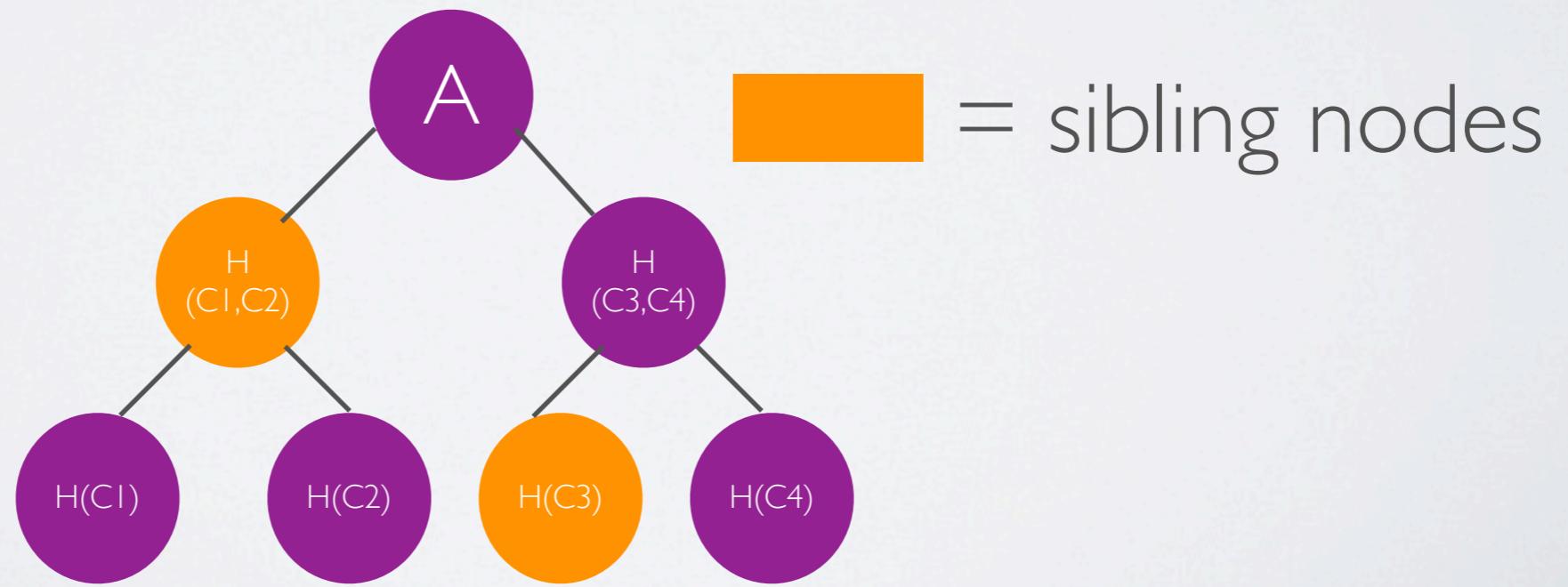
Spending Zerocoins

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



Spending Zerocoins

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



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, \dots, C_N compute:

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

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

An efficient ZKPoK proposed by
Camenisch/Lysyanskaya '01!

The protocol overview

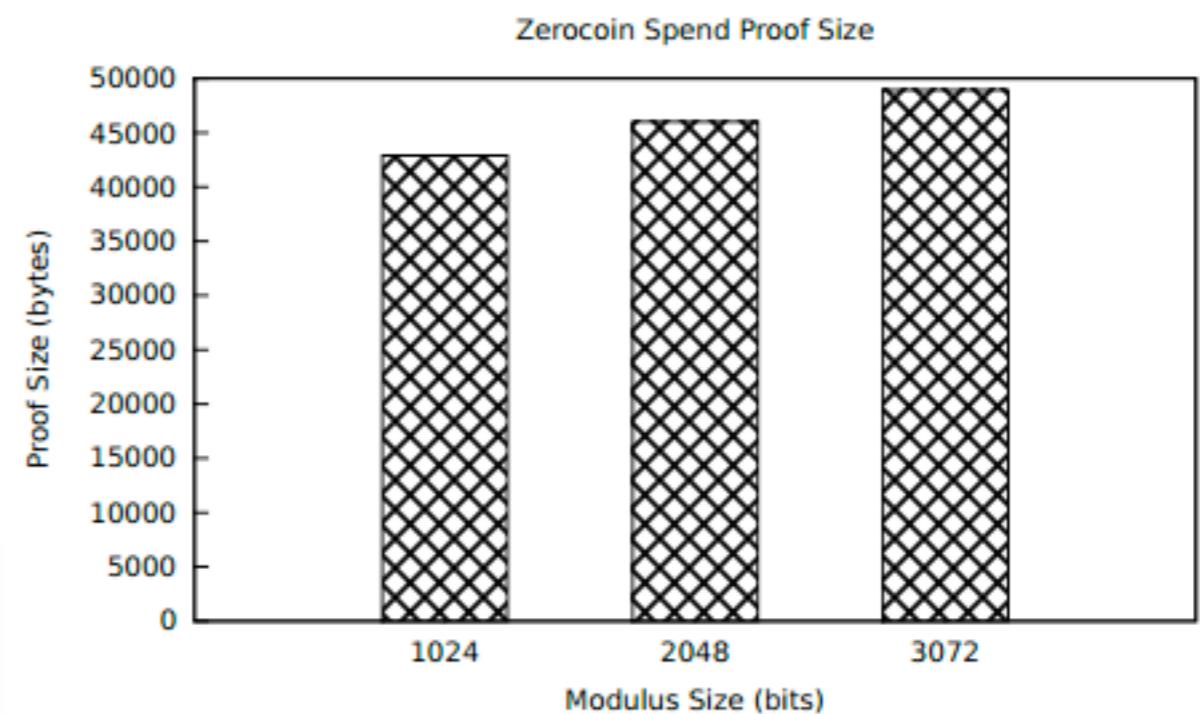
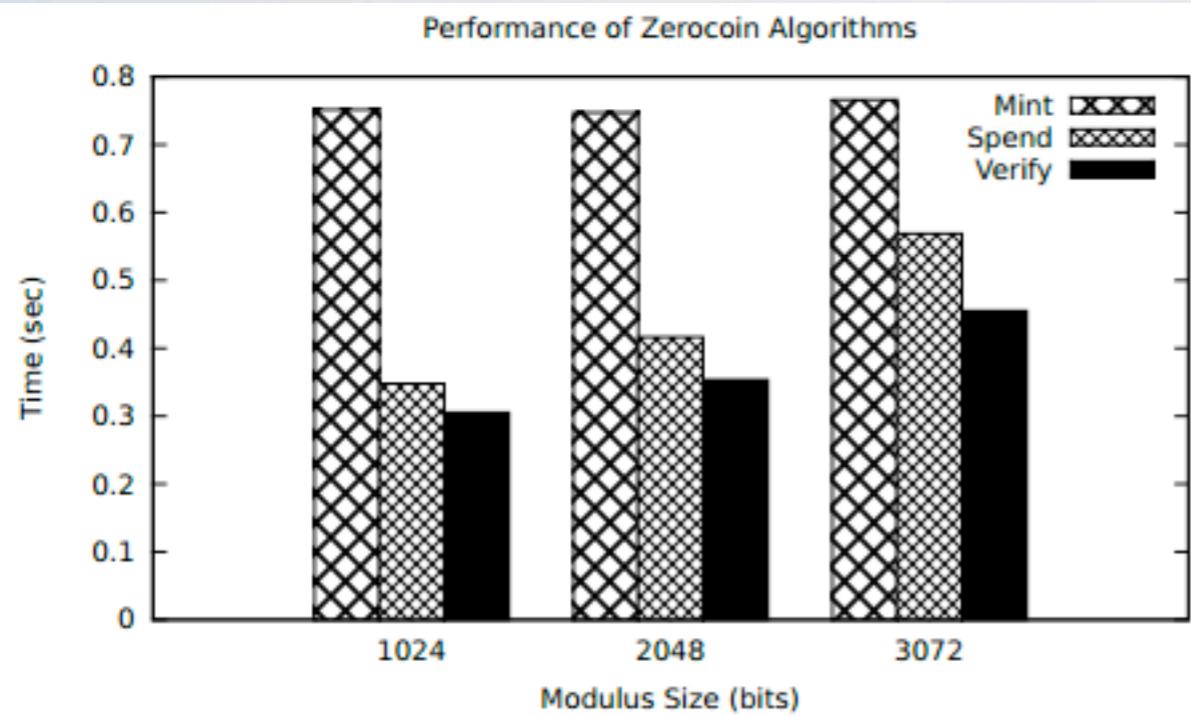
- The protocol:
 - Generate random serial number S . Compute:
 $C = g^S h^r$ s.t. C is prime, $\$r$
 - (Retain S , commitment randomness r)
 - Accumulate all valid coins, compute witness w_i
 - Reveal S , prove knowledge of accumulator witness w_i and commitment randomness r

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



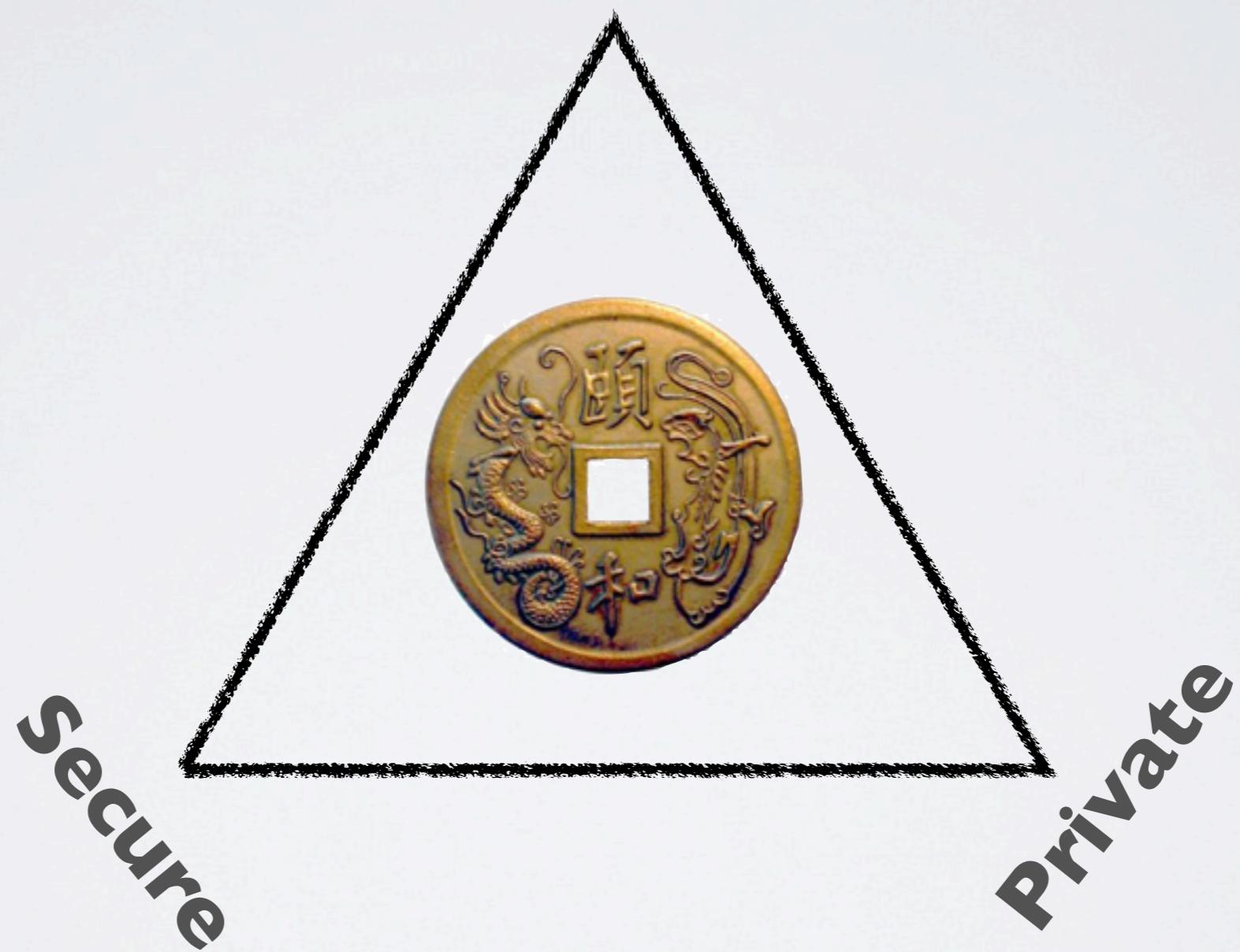
The upshot

- 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!



Zerocoins

Decentralized



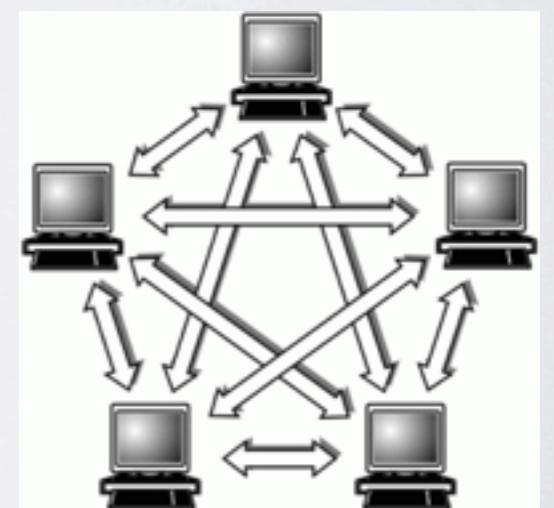
Divisible Zerocoins!

- Make coins divisible!
 - Include coin values in the commitment C
 - Users can insert ‘divide’ instructions that convert a single Zerocoins 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