

# 블록체인 #5

서울대학교 산업공학과 장우진

01

02

03

04

05

06

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

The address that received the very first Bitcoin block reward in the genesis block, base58 encoded.



Figure 4.1: a QR code representing an actual Bitcoin address.

- 비트코인을 사용하기 위해선 Public 블록체인의 정보들과 비트코인 소유자의 Secret signing key가 필요하다.
- 비트코인을 저장하고 사용하는 것은 실제론 비트코인의 Secret Keys를 저장하고 관리하는 것.
- 세 가지 Goal
  - 1) availability
  - 2) security
  - 3) convenience
- Local device, Wallet software, Encoding addresses

01

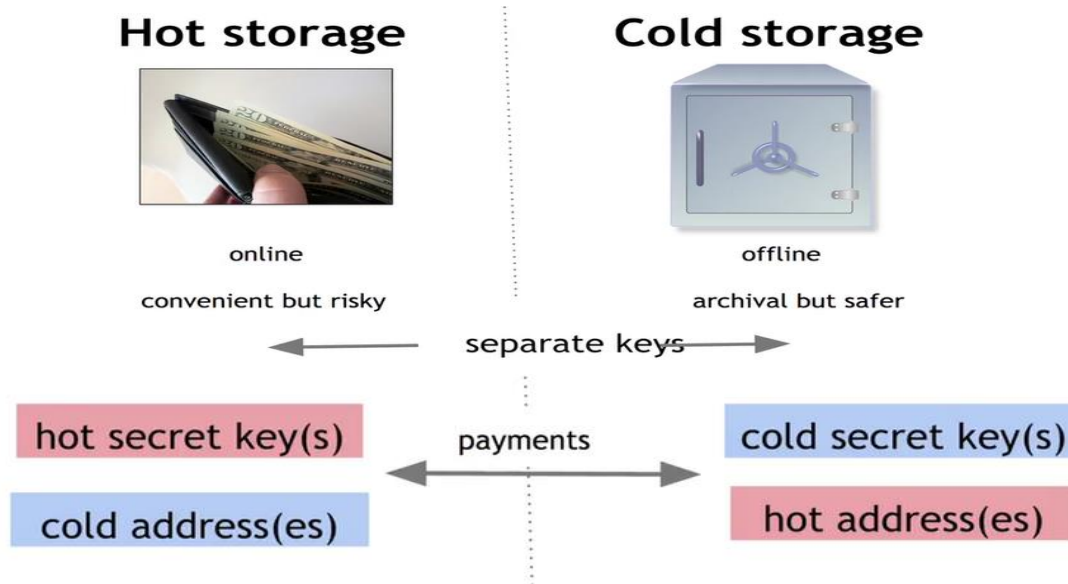
02

03

04

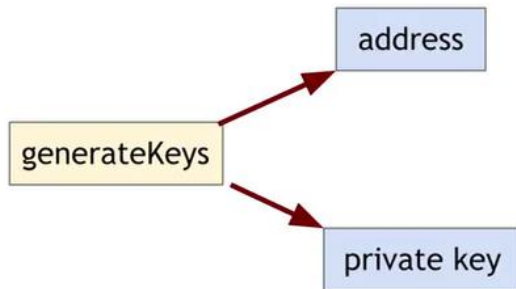
05

06

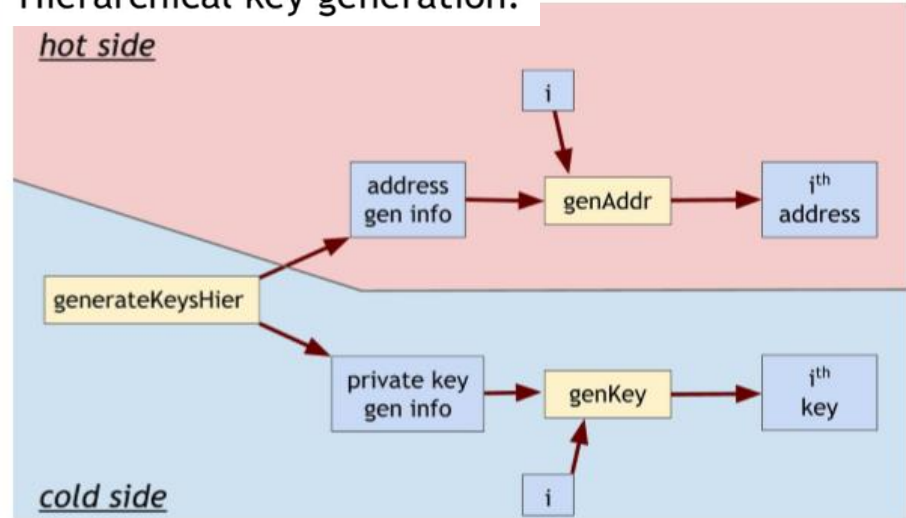


- 편리하지만 다소 위험이 존재하는 “Hot Storage” 와 Offline 으로 유지되어 안전하지만 편리하지 않은 “Cold Storage”를 분리하여 사용하는 것은 약간의 돈만 지갑에 넣고 나머지는 통장에 보관하는 것과 같다.
- 두 Storage가 동시에 취약해지는 것을 방지하기 위해 따로 분리된 Secret Key를 사용해야 하며 코인을 서로 주고 받기 위해 public Key를 서로 공유해야 한다. (Offline 상태에서도 가능)
- 하지만 코인에 따라 새롭게 Cold Storage의 address를 생성하여 사용하고 싶을 때 Cold Storage의 Offline 특성이 문제가 된다.
- 대량의 addresses/keys 묶음을 미리 생성해놓는 해결책도 있지만 근본적인 해결책은 아님

## Regular key generation:



## Hierarchical key generation:



- Hierarchical key generation을 이용하여 Cold storage의 address 생성 문제를 해결
- 일반적인 key generation 과정은 왼쪽 그림과 같이 address와 private key를 생성하는 반면 Hierarchical key generation은 address gen info. 와 private key get info.를 생성함
- Cryptographic 을 이용하여 any integer 'i' 에 대한 address/key 쌍을 생성 가능 . Address 생성 및 송금은 Cold side가 Offline시에도 가능하며, 이후 Cold side가 네트워크에 연결되면 생성된 address 들을 체크한다.
- 또한 보안적으로도 hot side에는 key에 관한 어느 정보도 담겨 있지 않기 때문에 정보가 누설될 일이 없다.

# Splitting and Sharing Keys

Idea: split secret into  $N$  pieces, such that  
 given any  $K$  pieces, can reconstruct the secret  
 given fewer than  $K$  pieces, don't learn anything

Example:  $N=2$ ,  $K=2$

$P$  = a large prime

$S$  = secret in  $[0, P)$

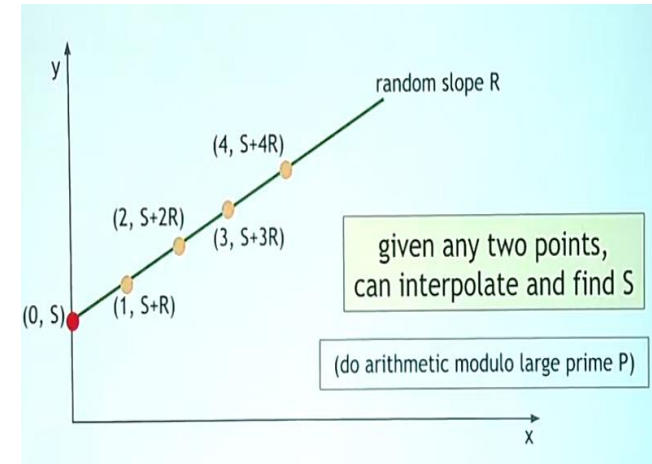
$R$  = random in  $[0, P)$

split:

$$X_1 = (S+R) \bmod P \quad X_2 = (S+2R) \bmod P$$

reconstruct:

$$(2X_1 - X_2) \bmod P = S$$

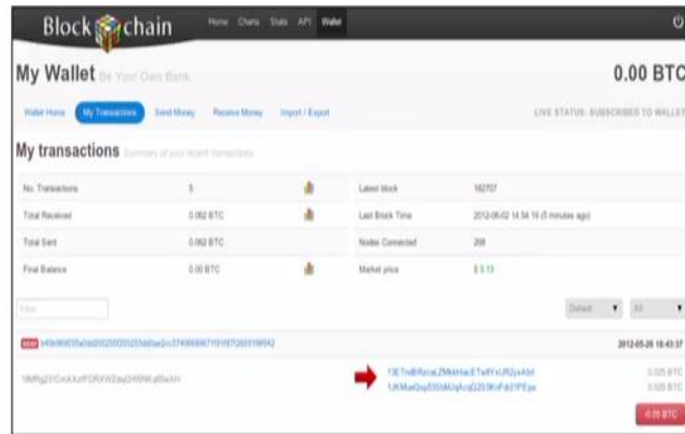


Equation	Random parameters	Points needed to recover $S$
$(S + RX) \bmod P$	$R$	2
$(S + R_1X + R_2X^2) \bmod P$	$R_1, R_2$	3
$(S + R_1X + R_2X^2 + R_3X^3) \bmod P$	$R_1, R_2, R_3$	4

- 장점 : Key를 나눠서 보관할 수 있으며, 이를 악용하기 위해선  $K$ 개 이상의 조각을 모아야 함
- 단점 : sign 시 share 들을 모아서 Key를 reconstruct 해야 하는 번거로움이 존재하며, share들이 모였을 때 공격으로부터 조심해야 함
- 이와 유사한 방법으론 Multi sig.가 있다

# Online Wallets and Exchanges

## Online Wallet



- Online wallet은 우리가 들고 다니는 지갑과 같은 개념이지만 모든 정보는 Cloud에 저장되어 있고 Web interface, app을 통해 사용 가능하다.
- Web interface의 경우 설치할 필요가 없고, 여러 장치를 통해 사용 가능한 장점이 있지만 site(Cloud)가 정보를 악용하거나 해킹 당할 경우 모든 것을 잃을 수 있다.

## Exchanges



- Bitcoins 및 달러, 유로와 같은 통화를 예치 시킬 수 있는 은행과 같은 역할
- Make and receive Bitcoin payments, buy/sell Bitcoins

## What happens when you buy BTC

suppose my account at Exchange holds \$5000 + 3 BTC  
I use Exchange to buy 2 BTC for \$580 each

result: my account holds \$3840 + 5 BTC

note: no BTC transaction appears on the blockchain  
only effect: Exchange is making a different promise now

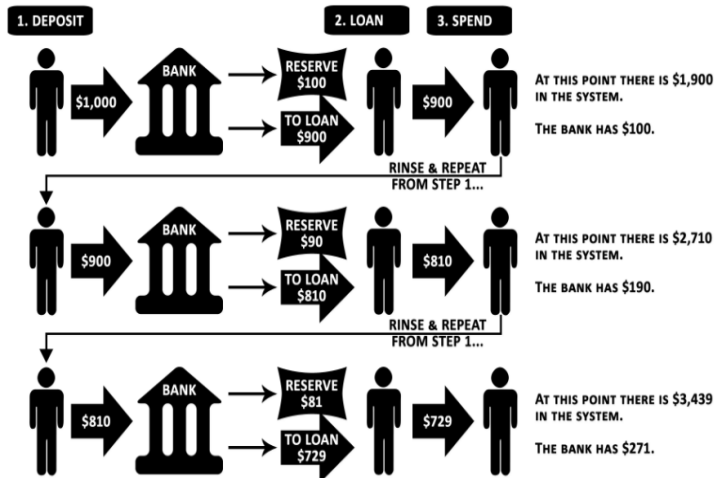
## Exchanges: Pros and Cons



- 장 점 : Connects BTC economy to fiat currency economy
- 단점 : Some kinds of risks as banks
  - 1) Bank run
  - 2) Ponzi scheme
  - 3) Hack

## Bank regulation

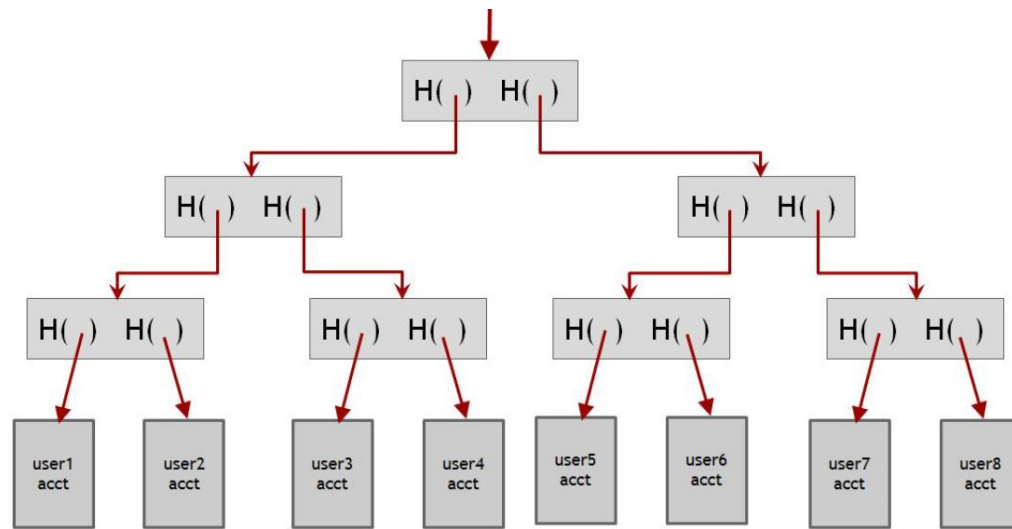
### THE BASIC FRACTIONAL RESERVE BANKING CYCLE



- Bitcoins 및 달러, 유로와 같은 통화를 예치 시킬 수 있는 은행과 같은 역할
- Make and receive Bitcoin payments, buy/sell Bitcoins for fiat currency, match up BTC buyer with seller
- 전통적인 은행은 minimum reserve system을 통해 규제를 받지만 Bitcoin exchange는 그렇지 않다. 그렇다면 Bitcoin exchange or Bitcoin business 는 어떻게 규제를 해야할까 (Chapter 7)
- Exchange는 Proof of reserve / Proof of liabilities를 통해 고객들에게 reserve 상황을 증명한다.



## Proof of reserve / Proof of liabilities



**Figure 4.5: Proof of liabilities.** The exchange publishes the root of a Merkle tree that contains all users at the leaves, including deposit amounts. Any user can request a proof of inclusion in the tree, and verify that the deposit sums are propagated correctly to the root of the tree.

- Proof of reserve : Publish valid payment-to-self of that amount. if they claim to have 100,000 bitcoins, they create a transaction in which they pay 100,00 bitcoins to themselves and show that that transaction is valid
- Proof of liabilities : Prove how many demand deposit exchange holds. Chapter1에서 설명한 Merkle tree를 이용.





Choose A Way To Accept Bitcoin [or see examples](#) of each payment method.


Type ☒ Button ☐ Hosted Page ☐ iFrame ☐ Email invoice

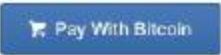
Payment ☒ Buy now ☐ Donation ☐ Subscription

Button Style

☒ 

☐ 

☐ 

☐ 

Item Name  Amount

Item Description

Send Funds To

[Show Advanced Options](#)

[Generate Button Code](#)

**Figure 4.7: Example payment service interface for generating a pay-with-Bitcoin button.** A merchant can use this interface to generate a HTML snippet to embed on their website.

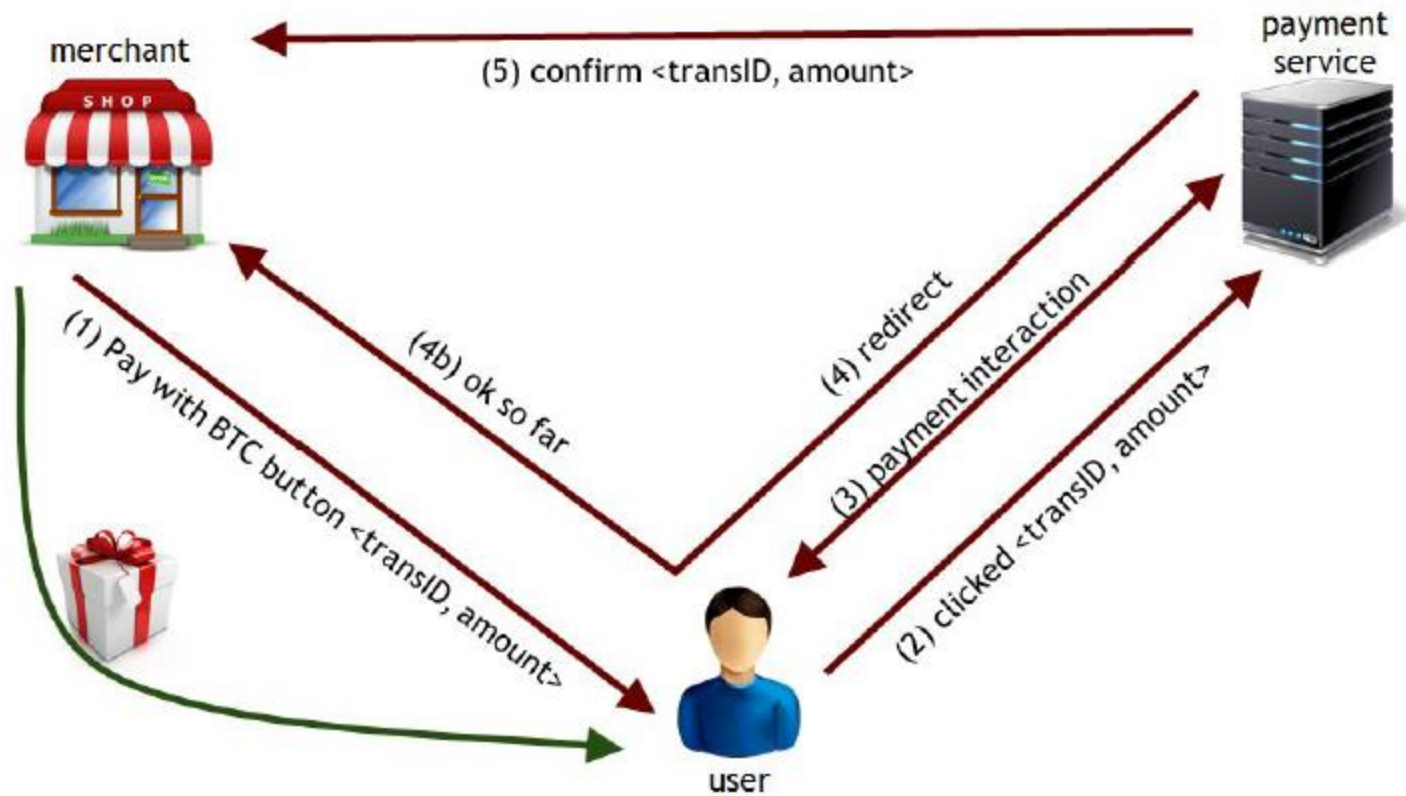


Figure 4.8: Payment process involving a user, merchant, and payment service.



출처 <http://bitcoinfees.com>

Current consensus fees:

No fee if

tx less than 1000 bytes in size,  
all outputs are 0.01 BTC or larger, and  
priority is large enough

Priority = (sum of inputAge\*inputValue) / (trans size)

Otherwise fee is 0.0001 BTC per 1000 bytes

Approx transaction size:  $148 N_{\text{inputs}} + 34 N_{\text{ouputs}} + 10$

- Transaction fee : Input – Output
- Transaction이 Bitcoin block chain에 포함되는 과정에서 Transaction fee가 발생한다.
- Transaction의 크기에 따라 Block의 사이즈가 달라지는데 사이즈가 클 경우 network에 Block을 전파하는데 시간이 더 걸리게 되고 이 경우 해당 블록이 도태 될 확률이 높아진다.
- 따라서 이러한 비용에 대한 보상으로 Transaction fee가 존재한다.

01

## Supply of Bitcoins

02

supply = coins in circulation (+ demand deposits?)

03

coins in circulation: fixed number, currently ~13.1 million

04

When to include demand deposits?

When they can actually be sold in the market.

05

06

## Demand for Bitcoins

BTC demanded to mediate fiat-currency transactions

Alice buys BTC for \$

Alice sends BTC to Bob

Bob sells BTC for \$

} BTC "out of circulation" during this time

BTC demanded as an investment

if the market thinks demand will go up in future



## Simple model of transaction-demand

T = total transaction value mediated via BTC (\$ / sec)

D = duration that BTC is needed by a transaction (sec)

S = supply of BTC (not including BTC held as long-term investments)

$\frac{S}{D}$  Bitcoins become available per second

$\frac{T}{P}$  Bitcoins needed per second

Equilibrium:

$$P = \frac{TD}{S}$$

# 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

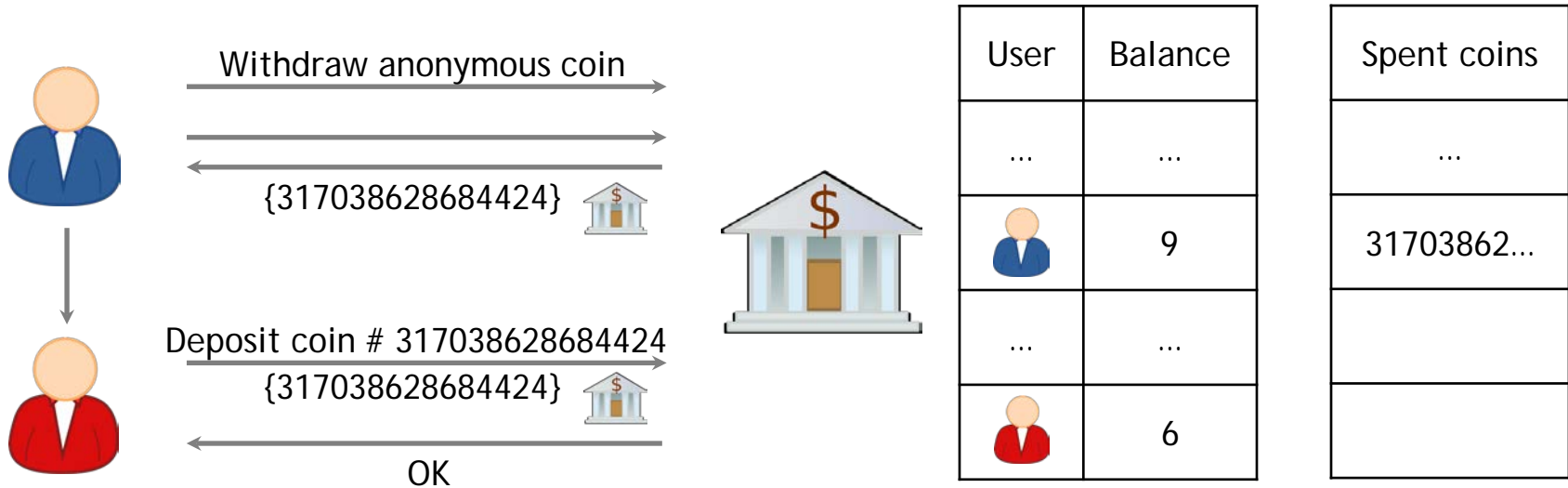
# Why anonymous cryptocurrencies?

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

Without anonymity, privacy is much worse than traditional banking!



# Anonymous e-cash via blind signatures




Bank cannot link the two users

# Anonymity & decentralization: in conflict

- Interactive protocols with bank are hard to decentralize
- Decentralization often achieved via public traceability to enforce security

# Bitcoin

**Bitcoin** is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

13DFamCvSxG8EG16VyXzdpfqxyooifswYx 


Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (<http://bitcoin.org>) or read more on [Wikipedia](#).

To generate a new, private address for your donation, click the refresh button above.



# Bitcoin

**Bitcoin** is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

16nLrMAQma6GJ4AavfxXLaZoeCHBBqqzX3 

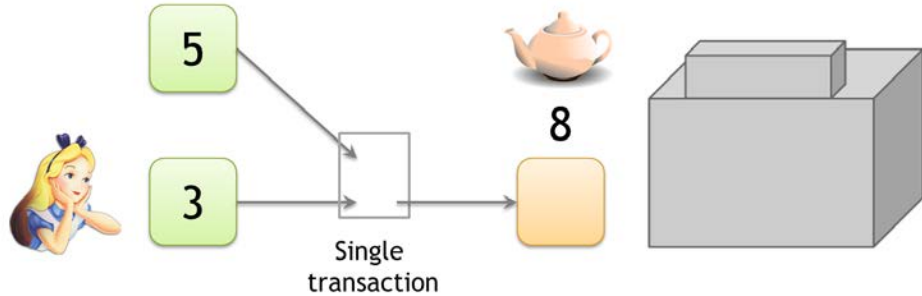
Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (<http://bitcoin.org>) or read more on [Wikipedia](#).

To generate a new, private address for your donation, click the refresh button above.



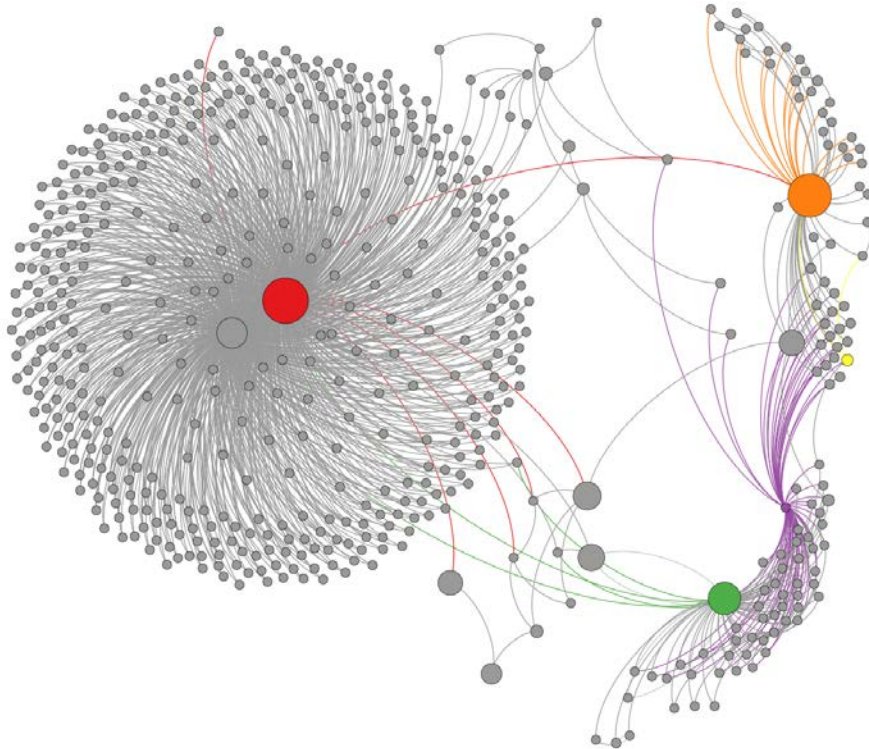
# Linking addresses

Shared spending is evidence of joint control



Addresses can be linked transitively

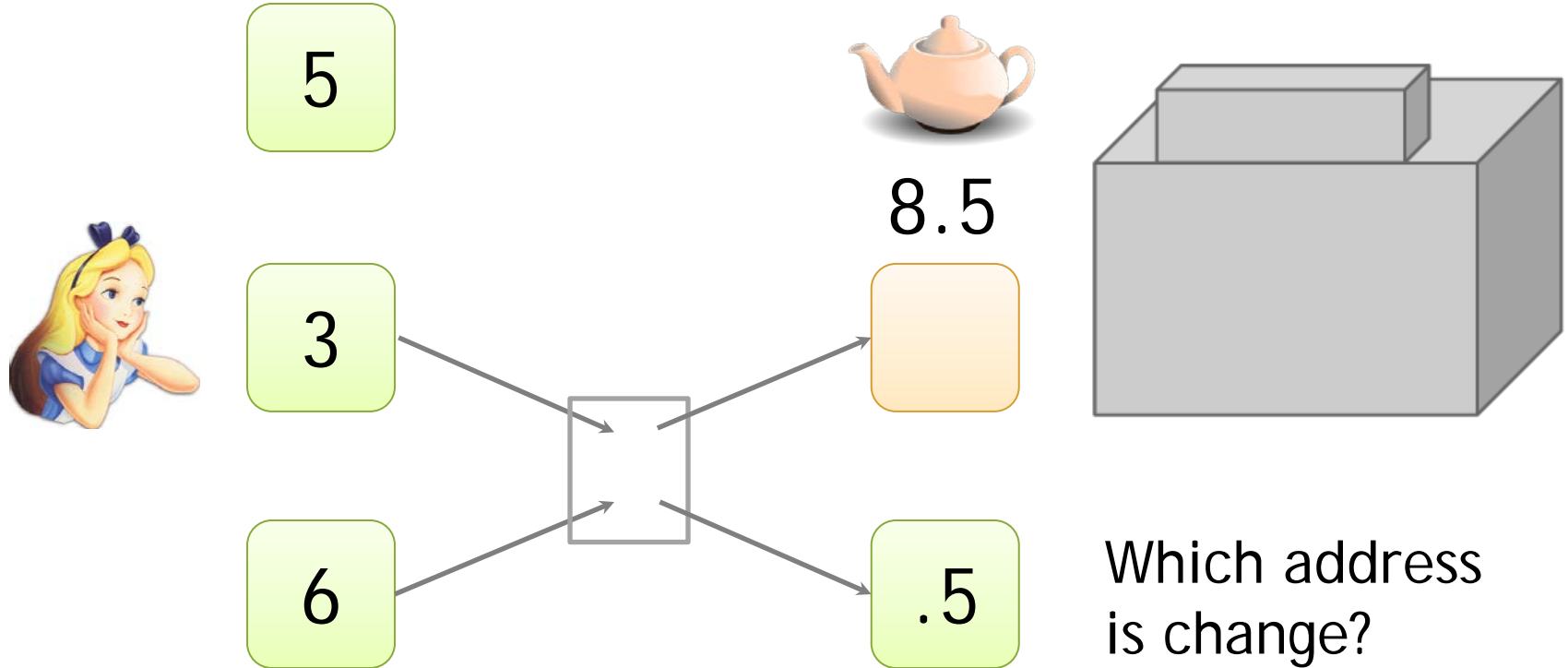
# Clustering of addresses



*An Analysis of Anonymity  
in the Bitcoin System*

F. Reid and M. Harrigan  
PASSAT 2011

# Change addresses

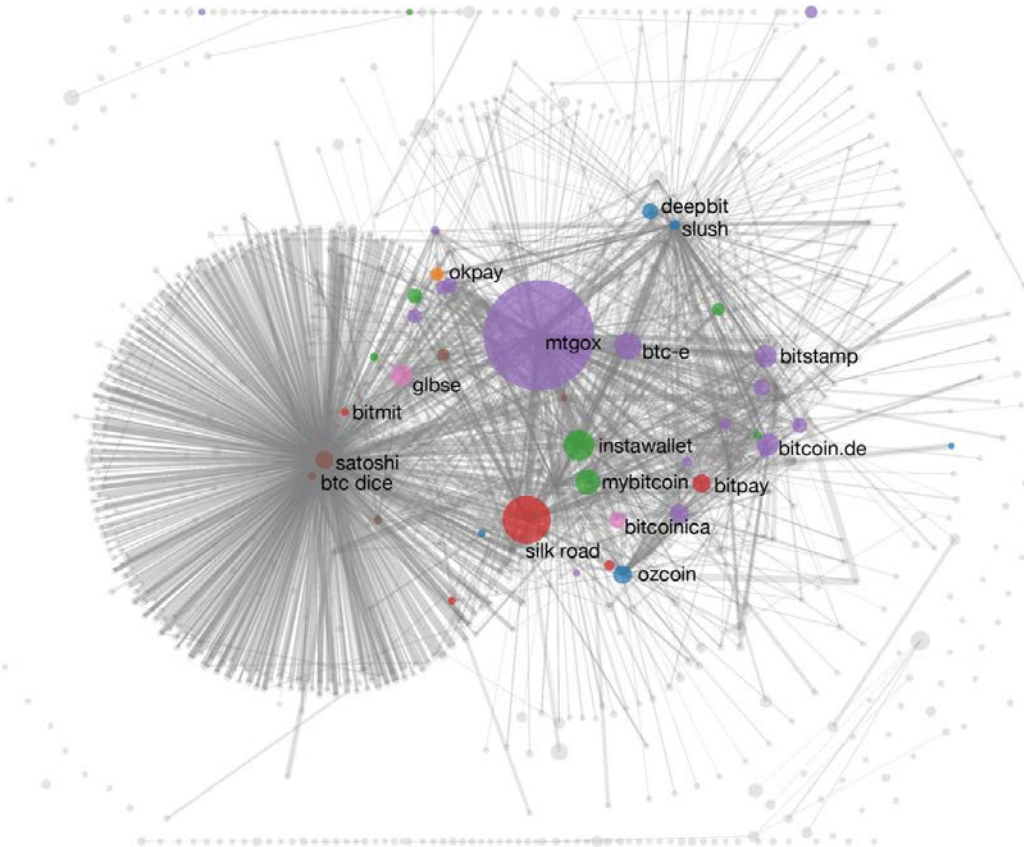




# Shared spending + idioms of use

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

S. Meiklejohn et al.



# To tag service providers: transact!



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

S. Meiklejohn et al.

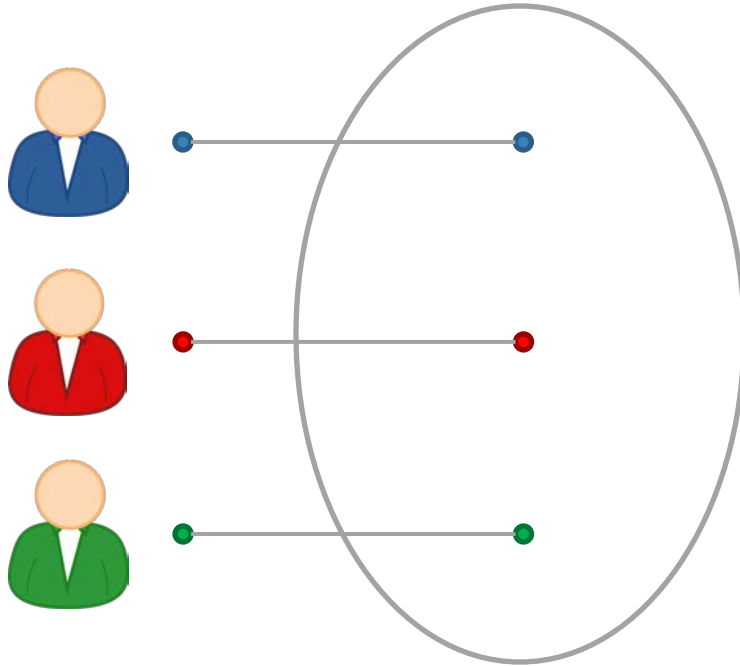
344 transactions

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

# Dedicated mixing services

- Promise not to keep records
- Don't ask for your identity

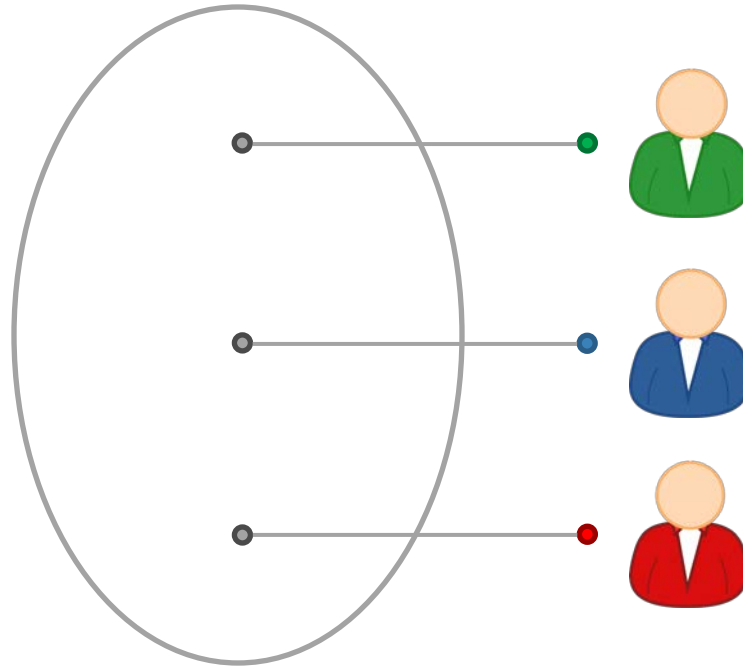
# To protect anonymity, use an intermediary



# To protect anonymity, use an intermediary

Online wallets  
do this

Do they provide  
anonymity?!



# Online wallets

Reputable, often regulated, businesses

- Typically require identity, keep records →  
no anonymity w.r.t. wallet service
- Users trust them with their bitcoins →  
keep them for longer →  
bigger anonymity set w.r.t. everyone else

# Principles for mixing services

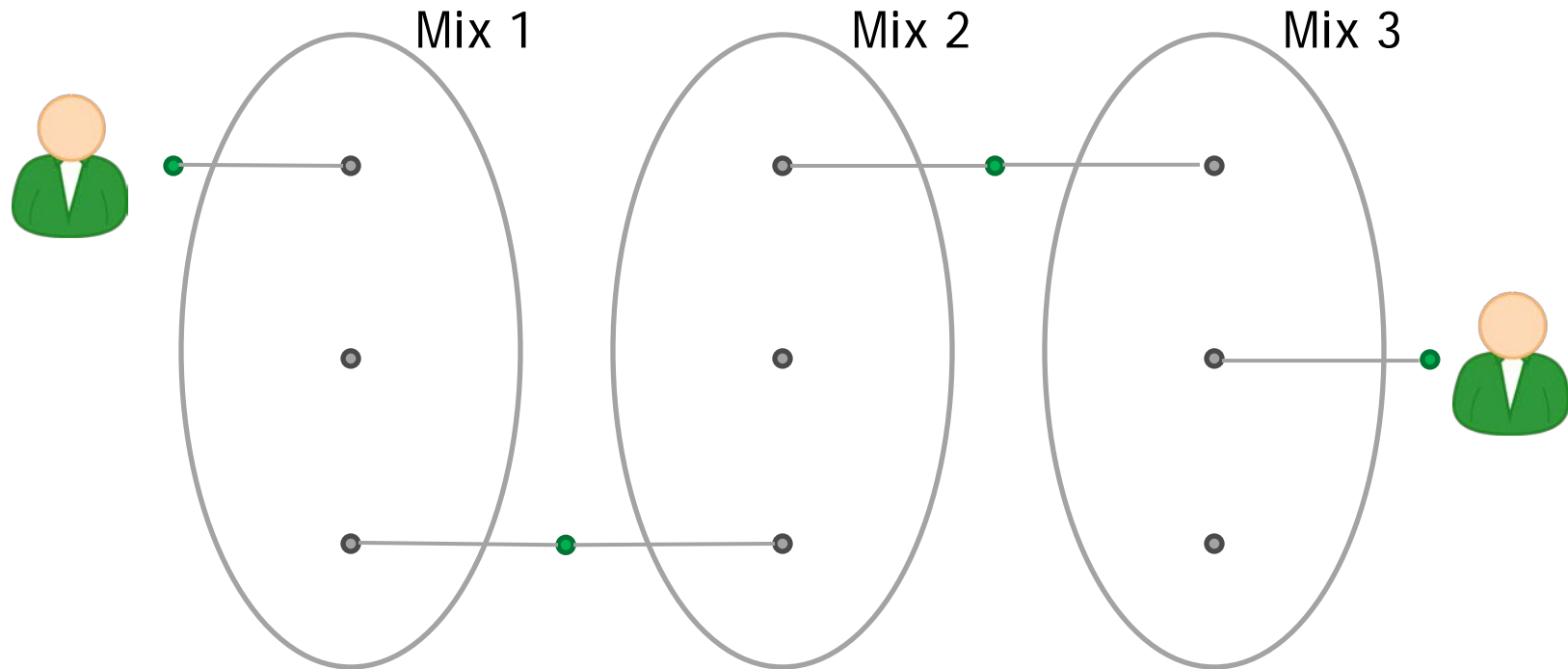
1. Use a series of mixes  
Mixes should implement a standard API to make this easy
2. Uniform transactions  
In particular: all mix transactions must have the same value!
3. Client side must be automated  
Desktop wallet software
4. Fees must be all-or-nothing

Current mixes follow none of these principles





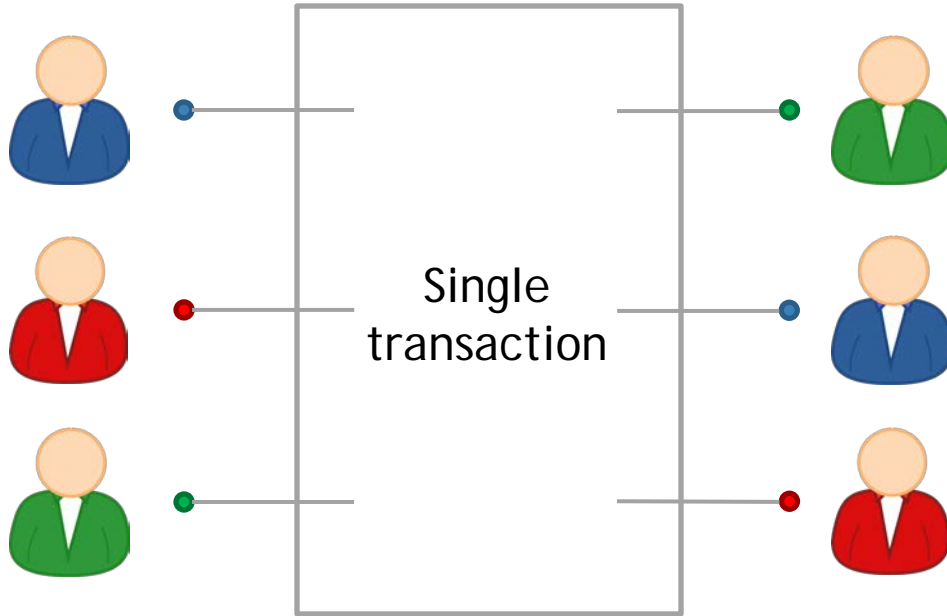
# Series of mixes



# Why decentralized mixing?

- No bootstrapping problem
- Theft impossible
- Possibly better anonymity
- More philosophically aligned with Bitcoin

# Coinjoin



Each signature is entirely separate

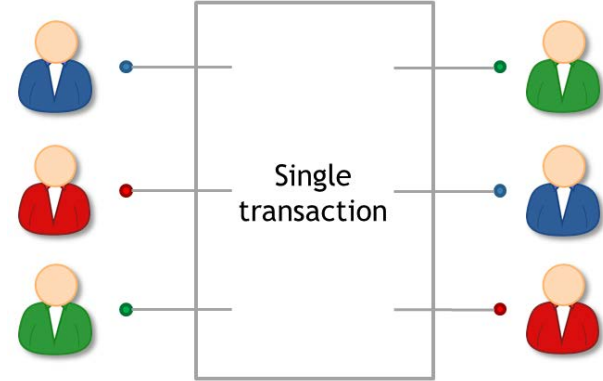
This is 1 mixing round

Mixing principles from before apply on top of basic protocol

Proposed by Greg Maxwell, Bitcoin core developer

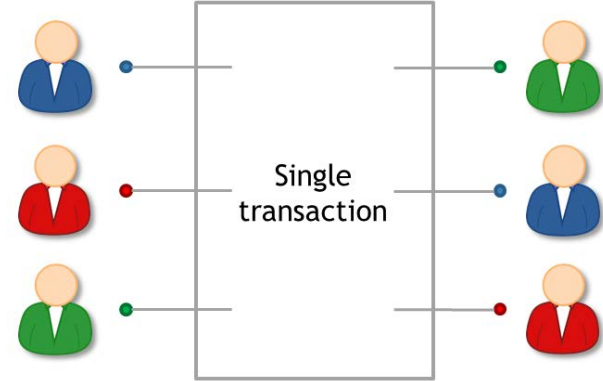
# Coinjoin algorithm

1. Find peers who want to mix
2. Exchange input/output addresses
3. Construct transaction
4. Send it around, collect signatures  
(Before signing, each peer checks if her output is present)
5. Broadcast the transaction



# Coinjoin: remaining problems

- How to find peers
- Peers know your input-output mapping  
(This is a worse problem than for centralized mixes)
- Denial of service



# Denial of service

Proposed solutions:

- Proof of work
- Proof of burn
- Server kicks out malicious participant
- Cryptographic “blame” protocol

*(CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin T. Ruffing et al., PETS 2014)*

# Zerocoin: protocol-level mixing

Mixing capability baked into protocol

Advantage: cryptographic guarantee of mixing

Disadvantage: not currently compatible with Bitcoin



# Basecoin and Zerocoin

Basecoin: Bitcoin-like Altcoin

Zerocoin: Extension of Basecoin

Basecoins can be converted into zerocoins  
and back

Breaks link between original and new basecoin

# Zerocoins

A Zerocoin is a cryptographic proof that you owned a Basecoin and made it unspendable

Miners can verify these proofs

Gives you the right to redeem a new Basecoin  
(Somewhat like poker chips)

# Two challenges

How to construct these proofs?

How to make sure each proof can only be “spent” once?

# Zero-knowledge proofs

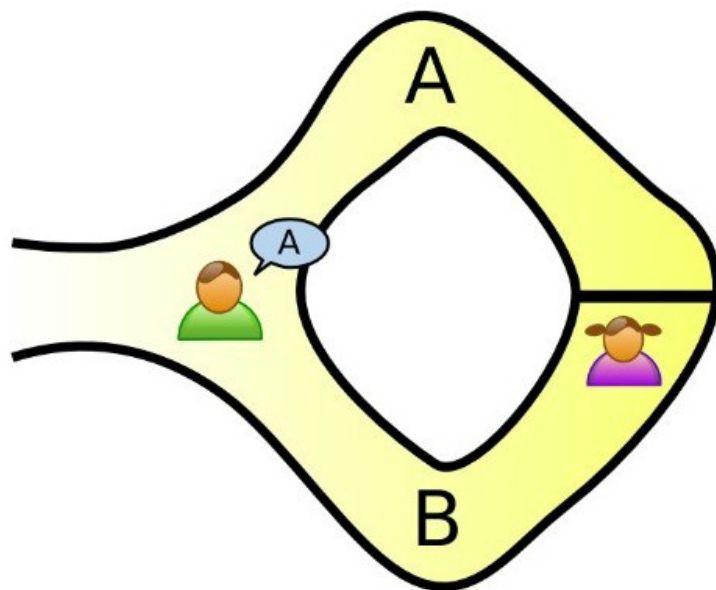
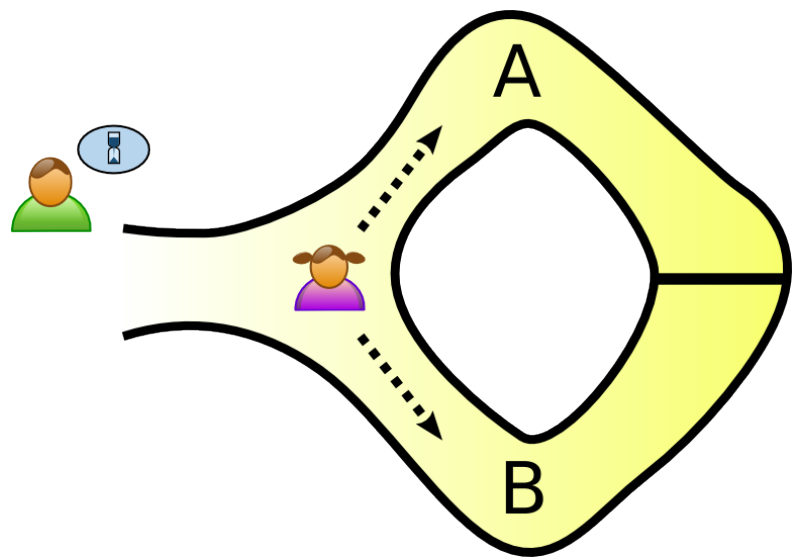
A way to prove a statement without revealing any other information



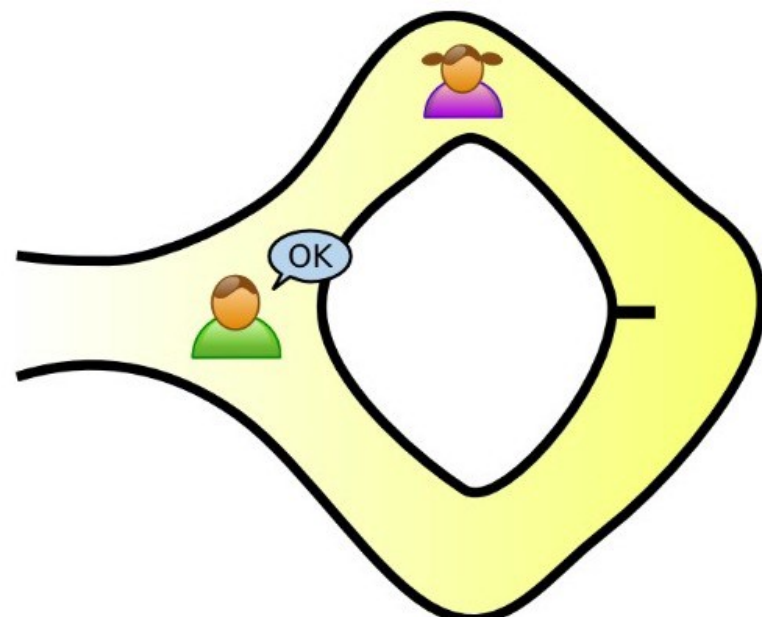
Crypto  
magic

Example:

- “I know an input that hashes to **da39a3ee5e**”
- “I know an input that hashes to some hash in the following set: ... ”



(i)

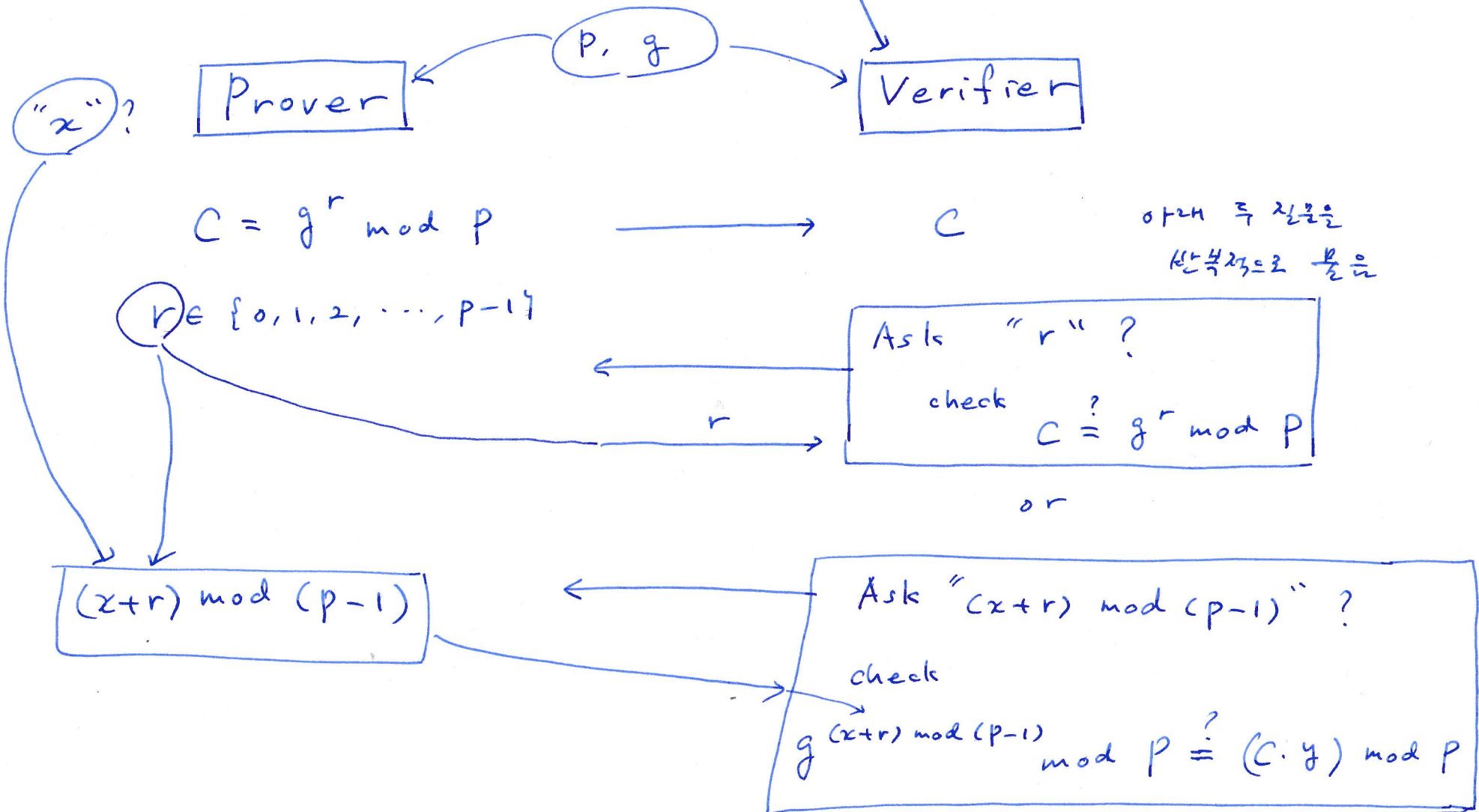


(ii)

# < Discrete log of a given value >

Given prime number  $p$  and generator  $g$

secret value (key)  $x \rightarrow y = g^x \bmod p$



# Minting zerocoins

Zerocoins come in standard denominations  
(Let's assume 1 basecoin)

Anyone can make one!

They have value once put on the block chain  
That costs 1 basecoin

# Minting a zerocoin: “commitment”

Generate serial number  $S$   
(eventually made public)

and random secret  $r$   
(never public, ensures  
unlinkability)

Compute  $H(S, r)$

Simplification

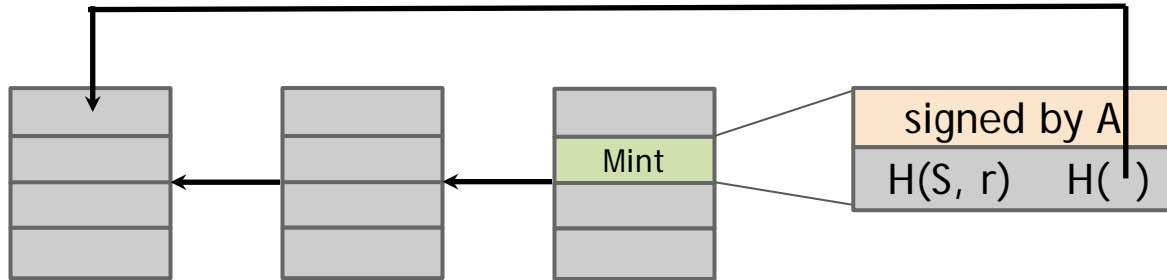




# Minting a zerocoin

To put  $H(S, r)$  on block chain

Create Mint Tx with 1 basecoin as input



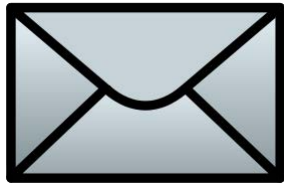
# To spend a zerocoin $S$ :

- Reveal  $S$   
(miners will verify  $S$  hasn't been spent before)
- Create zero-knowledge proof that:  
"I know a number  $r$  such that  $H(S, r)$  is one of the zerocoins in the block chain"
- Pick arbitrary zerocoin in block chain & use as input to your new transaction

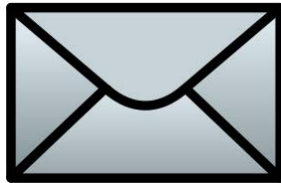
# Zerocoin is anonymous

Since  $r$  is secret, no one can figure out *which* zerocoin corresponds to serial number  $S$

$H(S, r)$

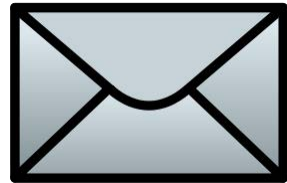


$h_1$



$h_2$

...



$h_N$

# Zerocoin is “efficient”

The proof is a giant  
disjunction over all  
zerocoins

Yet the proof is  
relatively small!

*I know  $r$  such that*

$$H(S, r) = h_1$$

*OR*

$$H(S, r) = h_2$$

*OR*

*...*

*OR*

$$H(S, r) = h_N$$



# Zerocash: Zerocoin without Basecoin

Two differences

- Different crypto for proofs (More efficient)
- Proposal to run system without Basecoin

*Zerocash: Decentralized Anonymous Payments from Bitcoin* E. Ben-Sasson et al. Usenix Security 2014



# Zerocash: untraceable e-cash

All transactions are zerocoins

Splitting and merging supported

Put transaction value inside the envelope

Ledger merely records existence of transactions



# Zerocash: the catch

Random, secret inputs are required to generate public parameters

These secret inputs must then be securely destroyed

No one can know them (anyone who does can break the system)

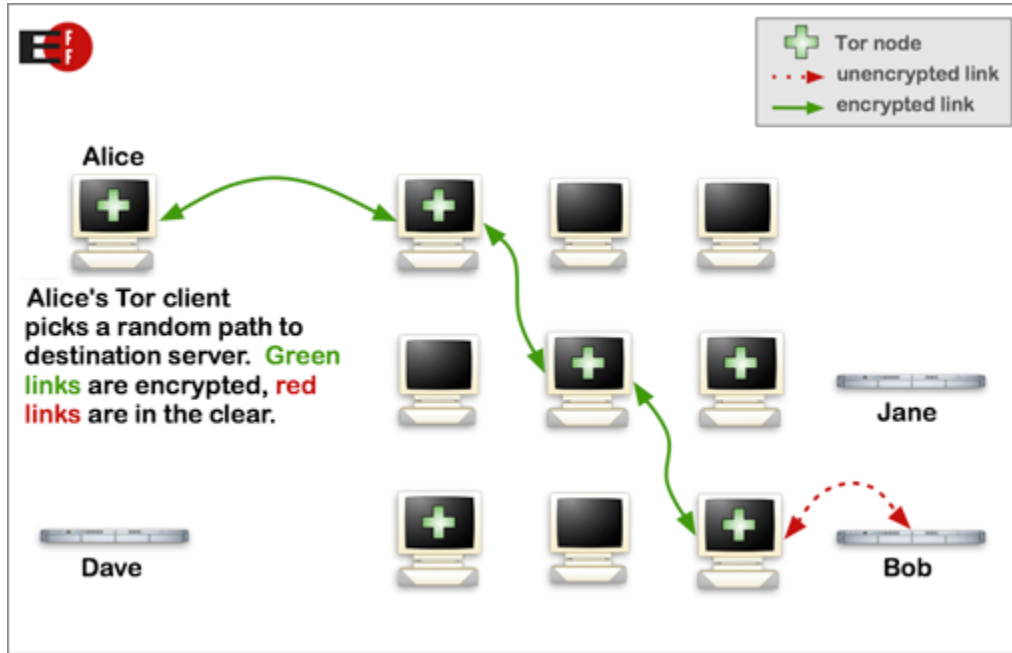


# 5 levels of anonymity

System	Type	Anonymity attacks	Deployability
Bitcoin	Pseudonymous	Tx graph analysis	Default
Single mix	Mix	Tx graph analysis, bad mix	Usable today
Mix chain	Mix	Side channels, bad mixes/peers	Bitcoin-compatible
Zerocoin	Cryptographic mix	Side channels (possibly)	Altcoin
Zerocash	Untraceable	None	Altcoin, tricky setup



# How Tor works



Safe(ish) if at least one router honest

Key challenge: hiding routing information

# Hidden services

What if the server wants to hide its address?

Simplified:

1. Connect to “rendezvous point” through Tor
2. Publish name → rendezvous point mapping
3. Client connects to rendezvous point

Onion address looks like

**`http://3g2up14pq6kufc4m.onion/`**

# Silk Road

- Communication: Tor hidden service
- Payment: Bitcoin
- Security?
- Anonymous shipping?



# Silk Road

anonymous marketplace

Welcome [redacted]  
 messages(0) | orders(0) | account(\$0.00) | settings | log out

|

## Shop by category:

Drugs(1249)  
 Cannabis(410)  
 Ecstasy(86)  
 Dissociatives(47)  
 Psychedelics(142)  
 Opioids(92)  
 Stimulants(107)  
 Other(150)  
 Benzos(96)  
 Lab Supplies(23)  
 Digital goods(93)  
 Services(107)  
 Money(71)  
 Weaponry(9)  
 Home & Garden(4)  
 Food(1)  
 Electronics(11)  
 Books(76)  
 Drug paraphernalia(46)  
 XXX(48)  
 Medical(3)  
 Computer equipment(19)  
 Art(1)  
 Apparel(8)  
 Sporting goods(3)  
 Tickets(1)  
 Forgeries(13)  
 Fireworks(2)



1g Tangerine Kush  
Bubble Hash

**\$60.96**



-NN- DMT YELLOW  
CLASSIC (500mg)

**\$19.39**



Barcode Manipulation  
scam keeping...

**\$2.31**



3.5g OG Kush

**\$22.17**



MDMA and MDEA mixture  
1 gram

**\$23.44**



Guerrilla Warfare Book's

**\$0.46**



co-codamol 30mg  
codeine / 500mg...

**\$4.59**



CASH BLOWOUT!!  
Vendors, SYG is...

**\$0.01**



\*Super BOMB\* Jolly  
Rancher 1/8...

**\$24.20**

## News:

- Site **glitches**
- Missing **deposits**
- Site **restored**
- Forum bugs **addressed**
- Pricing and hedging **improvements**
- Escrow hedging **update**
- New feature to help protect **sellers**
- Seller ranking and feedback **overhaul**

## Silk Road

- largest online market for illegal drugs
- ran as a Tor hidden service
- payment in Bitcoins
- site held BTC in escrow while goods shipped
- eBay-like reputation system
- run by "Dread Pirate Roberts"

operated February 2011 to October 2013



Ross Ulbricht (1984, Mar. 27)  
alleged operator of Silk Road

arrested October 2013  
Serving a life sentence without the possibility  
of parole

government says he tried to cover his tracks,  
but they connected the dots

government seized 174,000 BTC  
auctioned them to the public

consensus about rules

Agree on:

- what makes a transaction valid
- what makes a block valid
- how P2P nodes should behave
- protocols and formats

consensus that coins  
are valuable

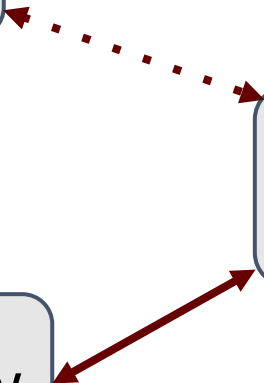
General agreement that coins have value  
Any currency needs this “Tinkerbell effect”

consensus about history

Agree on contents of the blockchain

therefore: which transactions have occurred

therefore: which coins exist and who owns them



Bitcoin Core software

open source (MIT license)

the most widely used Bitcoin software

those who don't use it follow its lead on rules

Bitcoin Core is the de facto rule book of Bitcoin



# Core developers:



Wladimir van der Laan



Gavin Andresen



Jeff Garzik



Gregory Maxwell



Satoshi Nakamoto



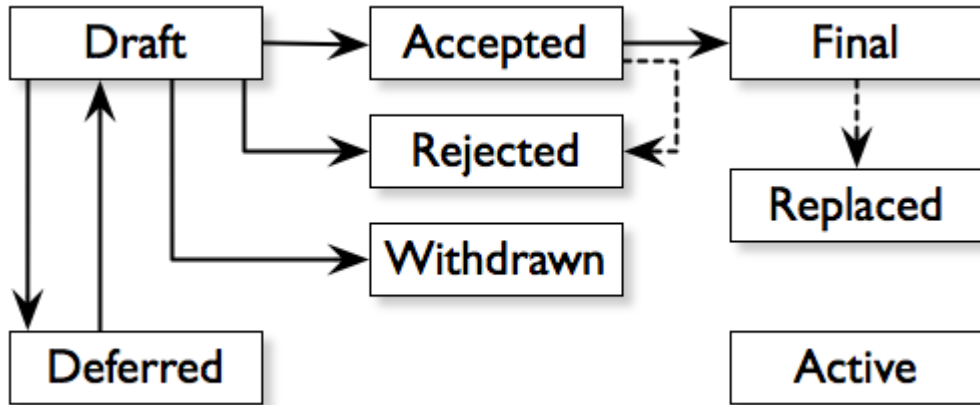
Pieter Wuille

## Bitcoin Improvement Proposals (BIPs)

“formal” proposal for changes to Bitcoin includes technical spec and rationale published in a numbered series

each BIP has a champion to evangelize / coordinate

also: informational BIPs, process-oriented BIPs



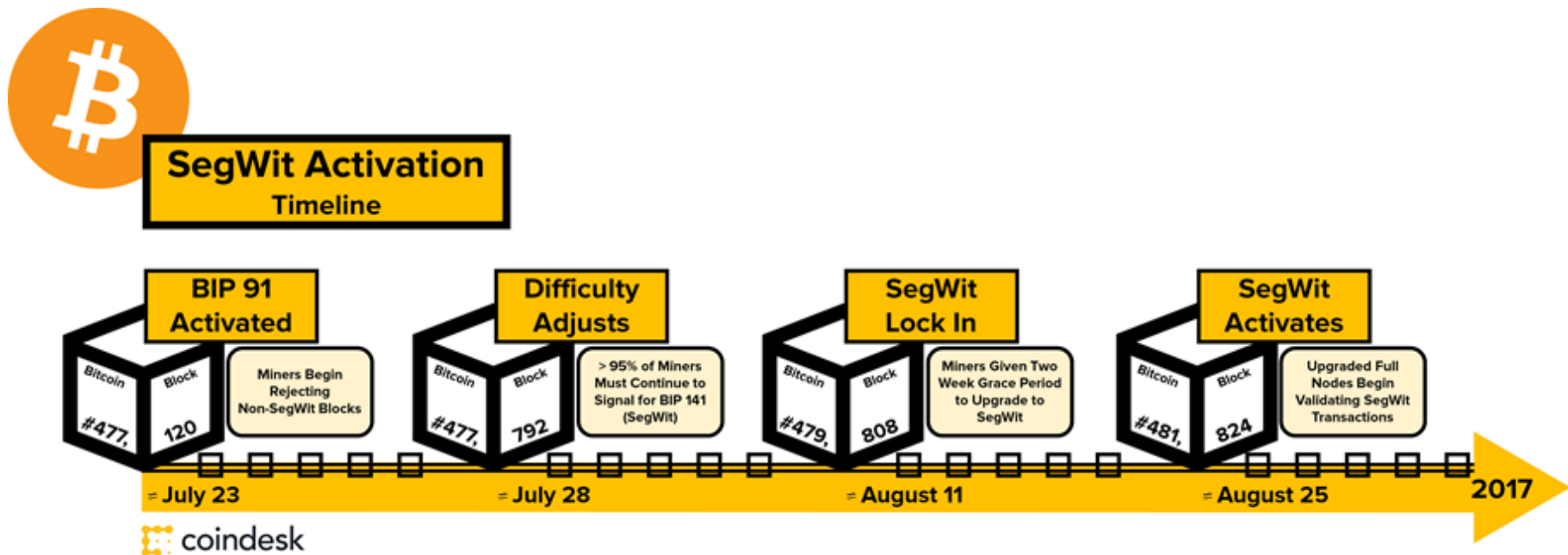


# Bitcoin 의 문제점과 해결 방안

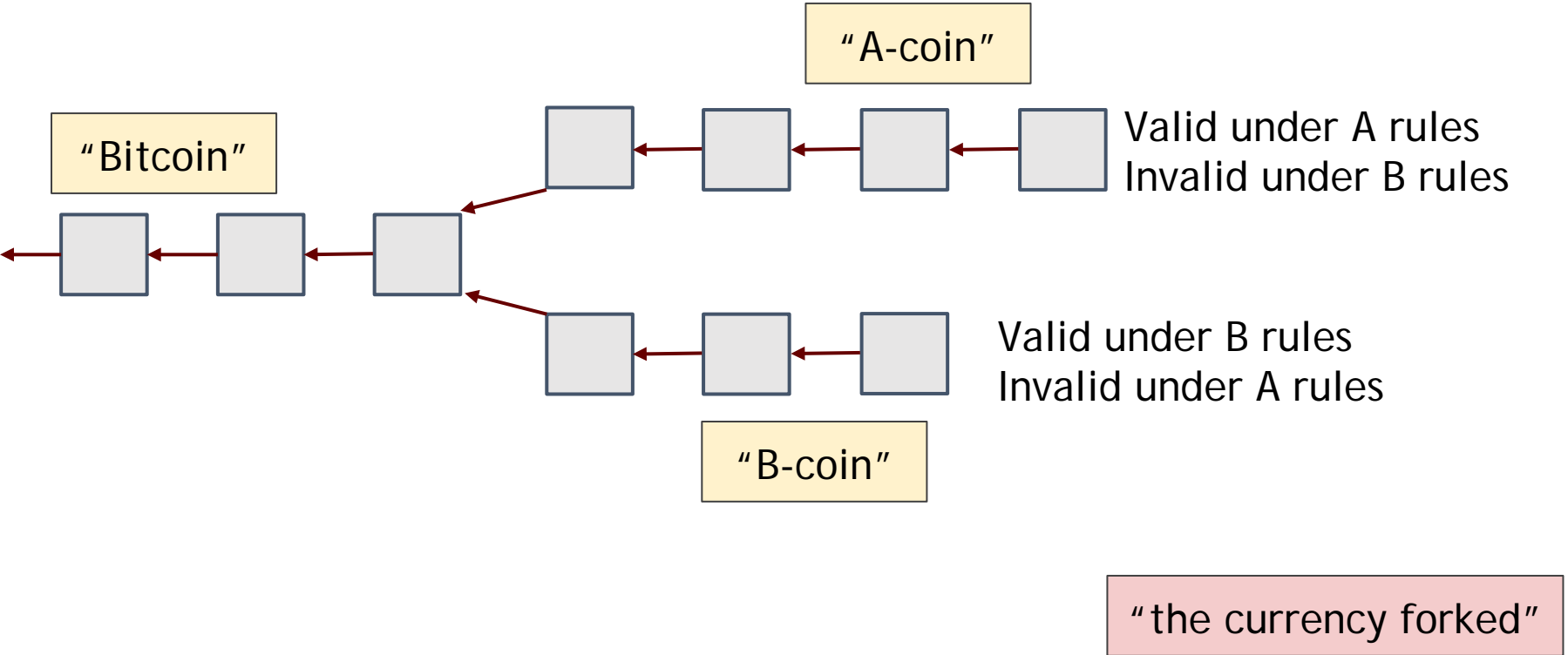
- Block size limit 로 인한 처리 속도 저하
  - 비트코인이 최대 처리할 수 있는 거래량 초당 7건
  - bitcoin scalability problem
- Bitcoin core (개발자)는 Softfork를 통한 SegWit 활성화
- SegWit 2X (SegWit2Mb) by Digital Currency Group (채굴자)
- Bitcoin Cash (BCH), Hardfork took effect on August 1, 2017
- Bitcoin Cash proposed by Chinese mining pool ViaBTC
- 'Lightning Network' by SegWit as a solution

## Segregated Witness (BIP141, activated on August 24, 2017)

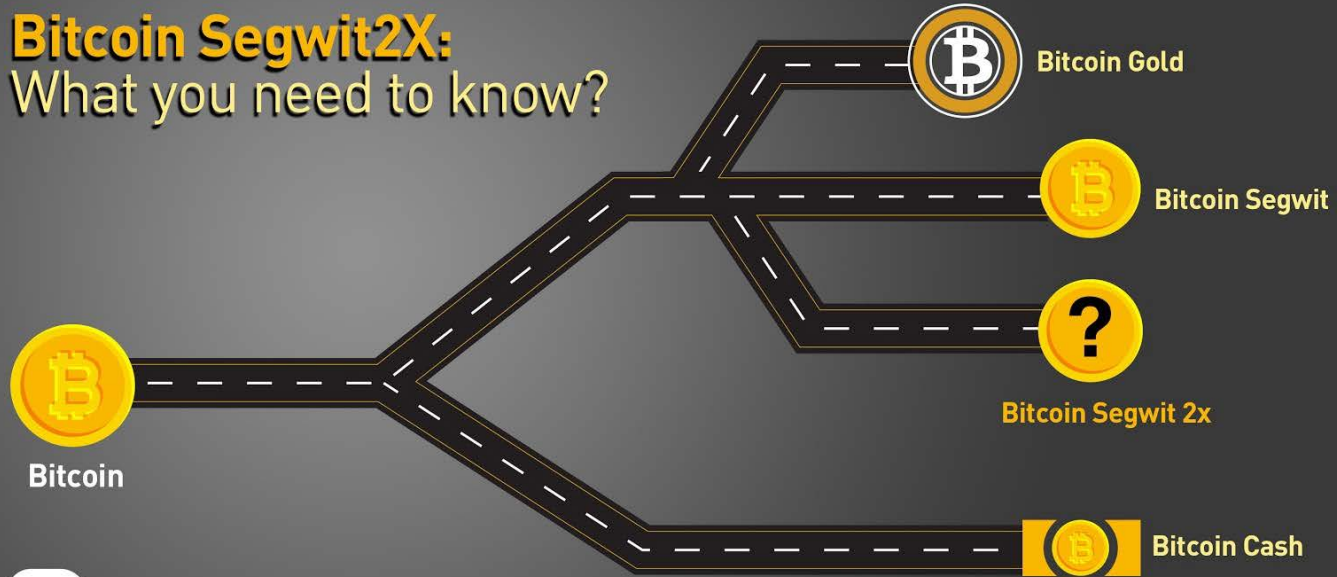
1MB 사이즈의 블록에서 서명 (witness signature) 을 Merkle tree 와 분리하여 1.8 MB 블록사이즈 효과를 내는 SoftFork



If there's a (hard) fork in the rules:



## Bitcoin Segwit2X: What you need to know?





## ***Bitcoin Cash***

- 2017년 8월 1일에 일어난 Bitcoin의 hard fork
- SegWit 방식에 대항하기 위해, 마이닝풀 연합 앤트풀을 이끄는 우지한 비트에인 대표 주도
- 블록체인 용량을 늘리는 방법을 두고 개발자와 채굴자의 대립



- 2017년 10월 24일에 일어난 Bitcoin의 hard fork
- 홍콩의 비트코인 채굴업체 라이트닝ASIC이 주도
- 수천 달러에 이르는 specialized ASICs 을 이용하지 않는, GPU minin을 지향 (Make Bitcoin Decentralized Again)

After a hard fork:

- If fork reflected a fight over future of Bitcoin:

  - branches fight for market share

  - branches fight to be seen as “the real Bitcoin”

  - probably one branch wins, one melts away

Who has the power in the Bitcoin ecosystem?

Suppose there is a negotiation about rule-setting.

Who controls the outcome?

Depends who would win the fight if they fail to agree



*Claim: Bitcoin Core developers have the power.*

They write the rulebook.

Almost everybody uses their code, follows their rules.

*Claim: Miners have the power.*

Miners write the history.

History will be consistent with miners' consensus rules.

*Claim: Investors have the power.*

Investors determine whether Bitcoin has any value.

In case of hard-fork, investors decide which branch wins.

*Claim: Merchants and their customers have the power.*

They generate the primary demand for Bitcoins.

They drive the long-term price of Bitcoin.

Investors are just guessing where merchants and customers will go.

*Claim: Payment services have the power.*

They are the ones that really handle transactions.

So they drive primary demand.

Merchants, customers, and investors will follow them.

## Know Your Customer (KYC):

- (1) identify and authenticate clients,
- (2) evaluate risk of client,
- (3) watch for anomalous behavior.

Note well: government takes this very seriously!  
Bitcoin businesses have been shut down.  
Businesspeople have been arrested

# Regulation

Argument against regulation is common, well understood.

Argument for regulation not as well understood.

*When markets fail and produce bad outcomes, regulation can address the failure.*

NEW YORK STATE  
DEPARTMENT OF FINANCIAL SERVICES  
PROPOSED  
NEW YORK CODES, RULES AND REGULATIONS  
  
TITLE 23. DEPARTMENT OF FINANCIAL SERVICES  
CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES  
PART 200. VIRTUAL CURRENCIES

New York “BitLicense” proposal  
July 2014

<http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf>

- 2015년 8월 8일 실시, “Great Bitcoin Exodus”
- 2015년 9월 보스톤 소재 Circle, BitLicense 획득
- 2016년 7월 샌프란시스코 소재 Ripple, BitLicense 획득
- 2017년 1월 샌프란시스코 소재 Coinbase, BitLicense 획득

- Puzzles are the core of Bitcoin
- Incentive system steers participants
- Basic features of Bitcoin's puzzle (recap)
- The puzzle is difficult to solve, so attacks are costly ... but not too hard, so honest miners are compensated
- What other features could a puzzle have?

- Alternative puzzle designs  
Used in practice, and speculative
- Variety of possible goals
- ASIC resistance, pool resistance, intrinsic benefits...
- Essential security requirements

# Puzzle requirements

- Cheap to Verify
- Adjustable difficulty
- Chance of winning is proportional to hashpower
  - Large players get only proportional advantage
  - Even small players get proportional compensation
- CPU-bound function (e.g. SHA-256 in Bitcoin)
- Memory-bound function (e.g. CryptoNote in Monero)





# Bad puzzle: a sequential puzzle

Problem: fastest miner **always** wins the race!



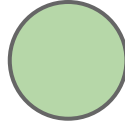
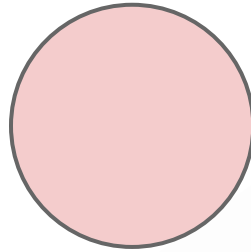
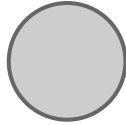
ASIC



Solution Found!



# Good puzzle $\rightarrow$ Weighted sample



This property is sometimes called “progress-free”

# ASIC resistance - Why? (1 of 2)

Goal: Ordinary people with idle laptops, PCs, or even mobile phones can mine!

Lower barrier to entry

Suitable for both CPU and GPU mining

Approach: reduce the gap between custom hardware and general purpose equipment



# ASIC resistance - Why? (2 of 2)

Goal: Prevent large manufacturers from dominating the game

“Burn-in” advantage

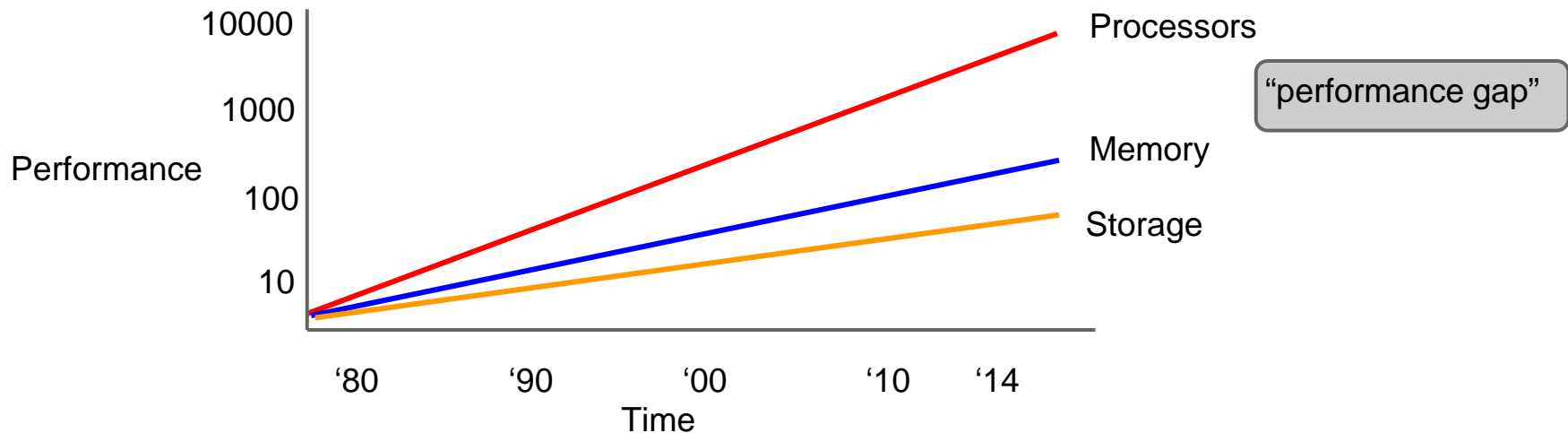
In-house designs



Approach: reduce the “gap” between future hardware and the custom ASICs we already have

# Memory hard puzzles

Premise: the cost and performance of memory is more stable than for processors





# scrypt

Colin Percival, 2009

- Memory hard hash function

***Constant time/memory tradeoff***

- Most widely used alternative Bitcoin puzzle
  - Also used elsewhere in security (PW-hashing)
1. Fill memory with random values
  2. Read from the memory in random order

# script - step 1 of 2 (write)

Input:  $\mathbf{x}$

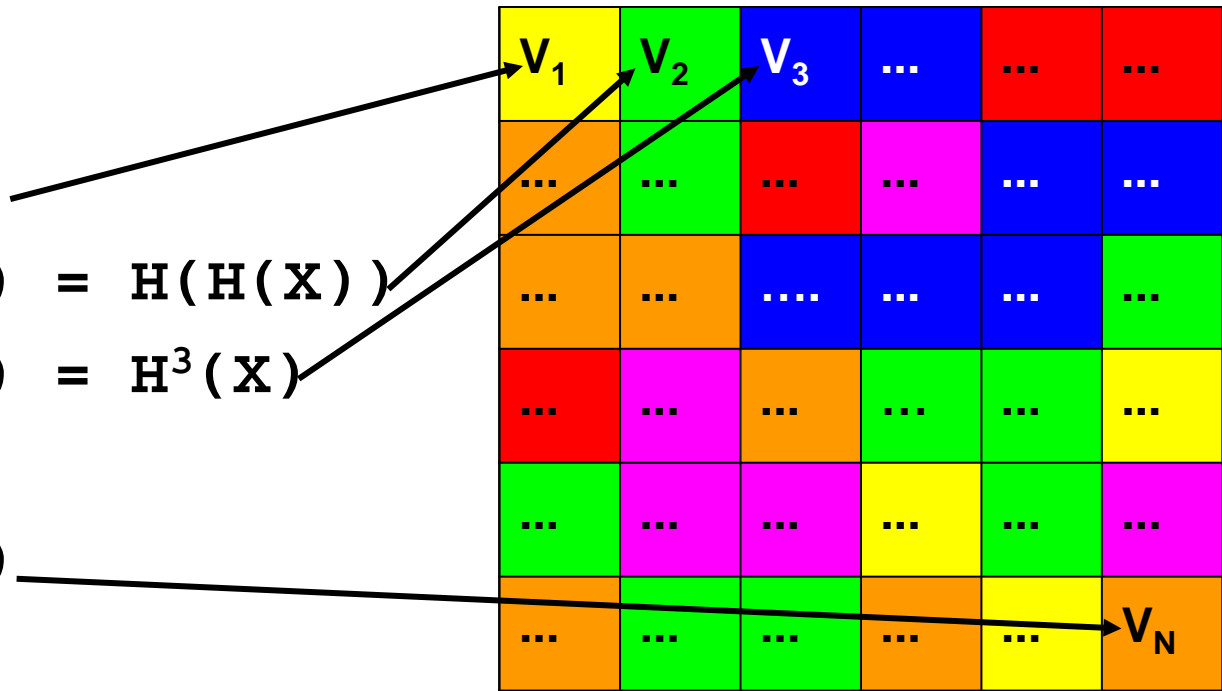
$$\mathbf{V}_1 = \mathbf{H}(\mathbf{X})$$

$$\mathbf{V}_2 = \mathbf{H}(\mathbf{V}_1) = \mathbf{H}(\mathbf{H}(\mathbf{x}))$$

$$V_3 = H(V_2) = H^3(X).$$

...

$$\mathbf{V}_N = \mathbf{H}^N(\mathbf{x})$$



## script - step 2 of 2 (read)

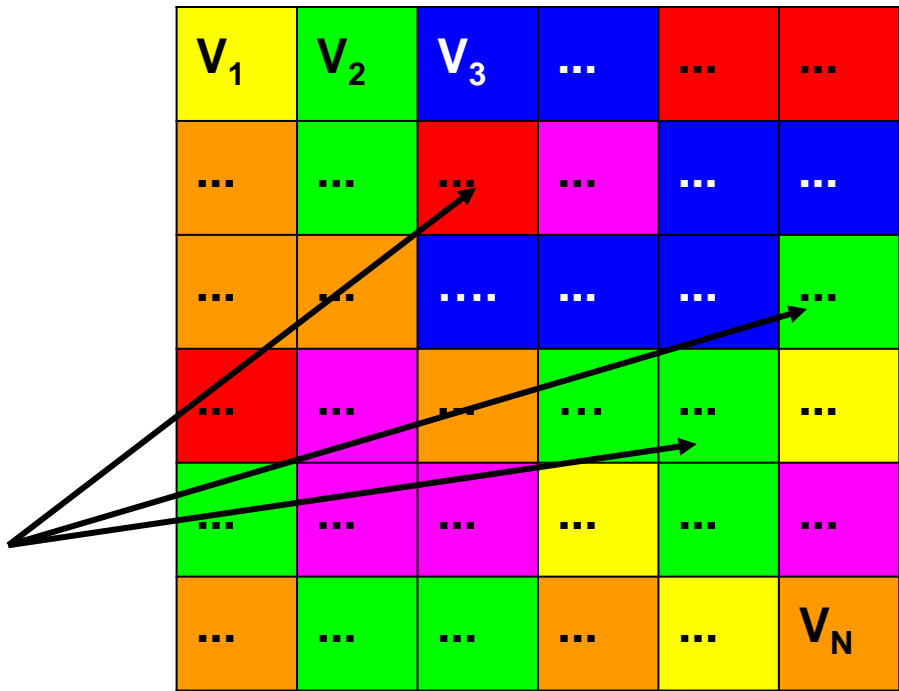
Input:  $X$

$$\mathbf{A} \quad := \quad \mathbf{H}^{N+1}(\mathbf{X})$$

For N iterations:

$$i := A \bmod N$$
$$\mathbf{A} := \mathbf{H}(\mathbf{A} \text{ xor } \mathbf{V}_i)$$

Output: A







# script

Disadvantages:

Also requires  $N$  steps,  $N$  memory to check

Is it actually ASIC resistant?

script ASICs *are* already available

Future: PW-hashing research



<http://zeusminer.com/>

# X11: 11 different hash functions combined

More complicated hash functions  
DASH is no more ASIC resistant



**D3 Antminer** ASIC

Price

**1,599 USD**

Payback period

**176 days**



**Buy now**



Power	Power cost per day	Return Per Week	Cost per GH/s
1200	\$ 3.46	\$ 63.24	\$ 106.60
Hash Rate	Return Per Day	Return Per Month	Payback period
<b>15.0 GH/s</b>	\$ 9.03	\$ 271.02	176 days
Mines	Profit Ratio	Return Per Year	Annual Return Percentage
 DigitalCash	261%	\$ 3,297.40	206%

# Recovering wasted work

Recall:

(as of mid-2014)

between 150 MW - 900 MW power consumed

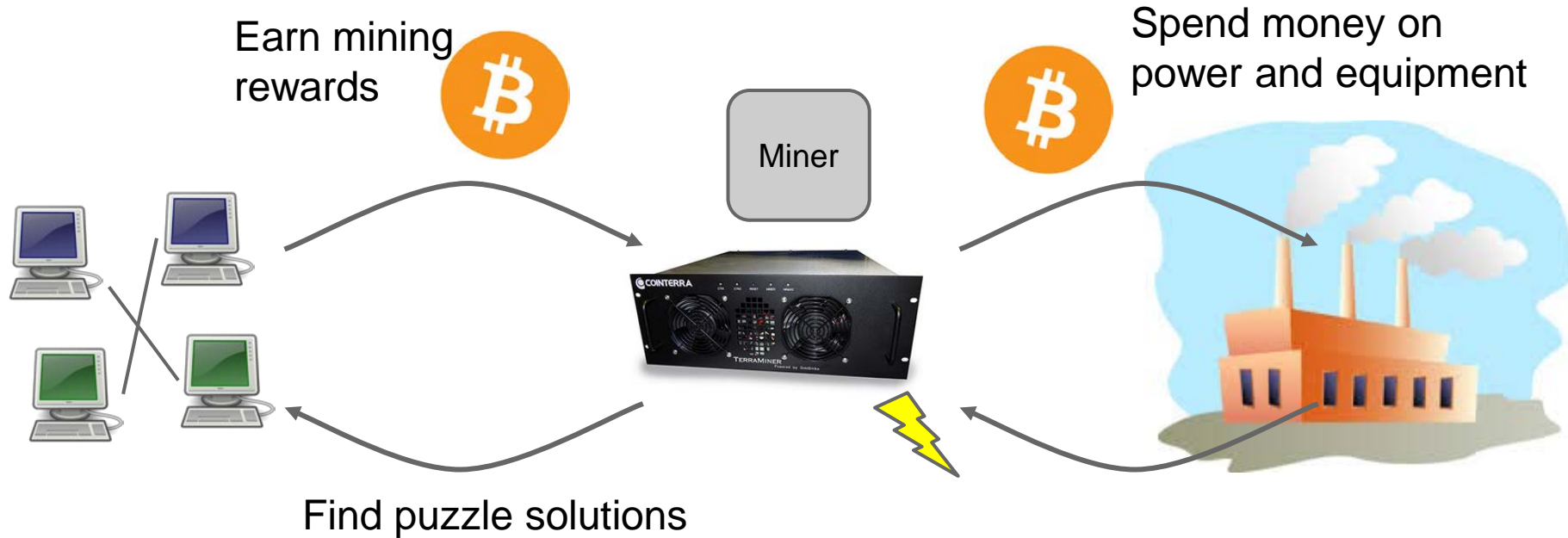
Natural question:

Can we recycle this and do something useful?



# Mining has an unnecessary step

## Proof-of-Work Mining:



# 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

# Proof of Stake

The creator of the next block is chosen via various combination of random selection and wealth or age (the stake).

- Randomized block selection: practically random manner with greater amounts of stake increasing the likelihood of adding a block to the chain (e.g. Nxt)
- Coin age-based selection: No. of coins  $\times$  No. of unspent days (at least 30 days, at most 90 days), minting vs. mining (e.g. Peercoin)

But, there is little cost to working on several chains