

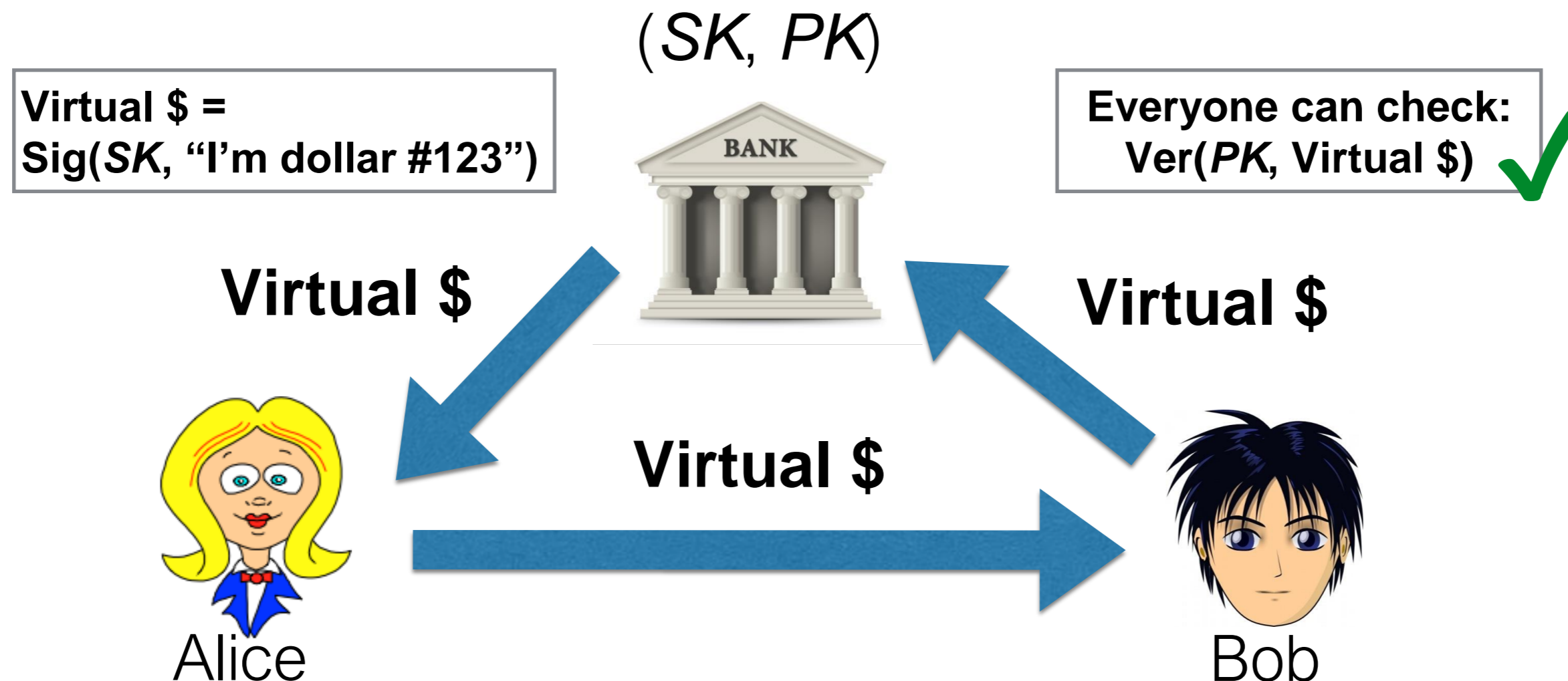
“Crypto” currencies

Thanks to [Ari Juels](#) for this deck!

The backdrop

One of the earliest proposed uses of digital signatures (RSA) was to create virtual currency (in Ireland)

- Idea: A bank creates coins consisting of digital signatures
- Simplified version...



The backdrop

- In 1982, “blind” digital signatures introduced by David Chaum
 - (Yes, the same Chaum who introduced Tor)
 - Allowed banks to sign *anonymous* virtual currency
 - Turned into Digital Cash
- Researchers proposed digital currency for decades after
 - Financial Cryptography
 - PayWord and MicroMint
 - MicroMint used *proof of work*
 - Turned into Peppercoin
 - 800+ citations
- But no one used virtual currency



Bitcoin

Bitcoin's face

- Created by “Satoshi Nakamoto”
 - Paper “Bitcoin: A peer-to-peer electronic cash system” [2008]
 - Source code [2009]
- As of today, \$320 billion market capitalization (143b ETH, 65b Tether)
- **But who is Nakamoto?**



Bitcoin

Another theory...

- Created in 2008 by “Satoshi Nakamoto”
 - Paper “Bitcoin: A peer-to-peer electronic cash system”
 - Source code
- As of today, \$1+ Trillion market capitalization
- **But who is Nakamoto?**



Bitcoin

And another...

- Created in 2008 by “Satoshi Nakamoto”
 - Paper “Bitcoin: A peer-to-peer electronic cash system”
 - Source code
- As of today, \$1+ Trillion market capitalization
- **But who is Nakamoto?**



How to Acquire and Spend Bitcoins

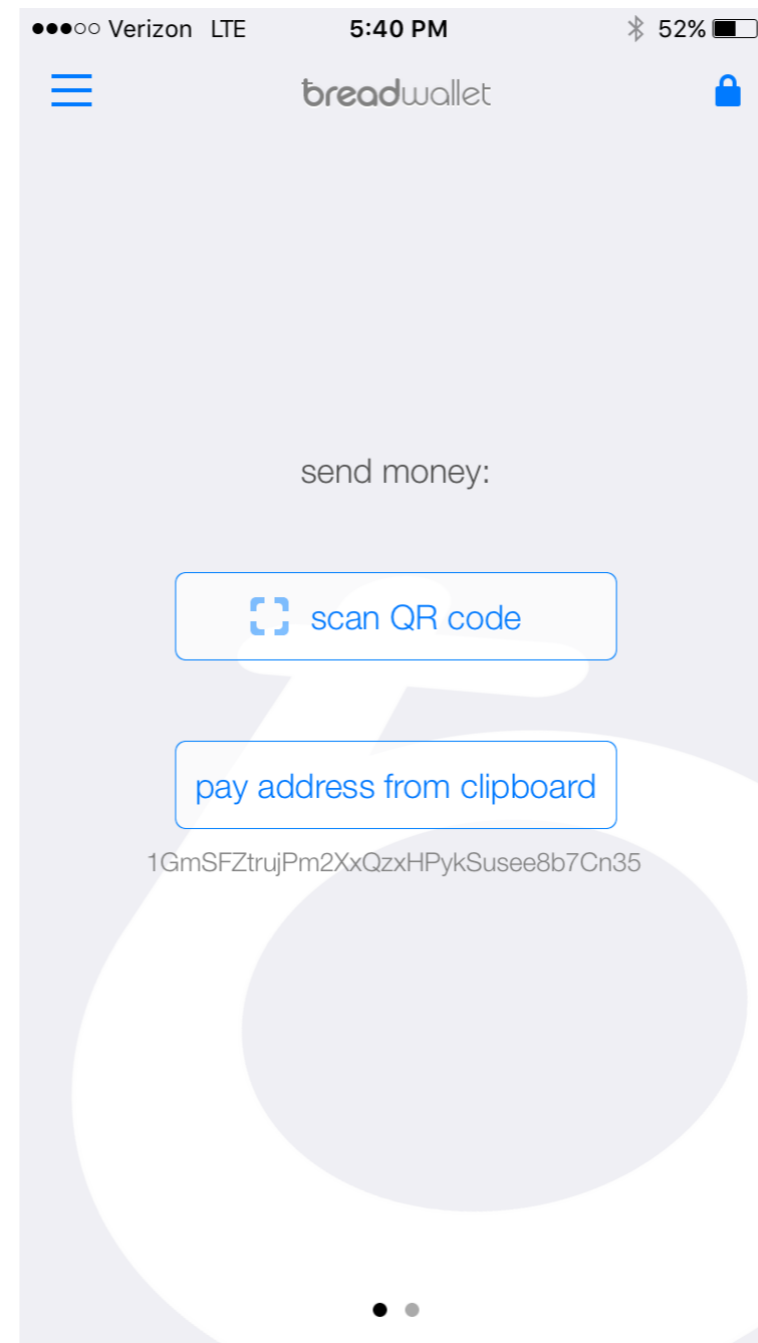
Getting started

- Let's understand how Bitcoin (BTC) is used
- To start, anyone can create her own Bitcoin "address" / account X
 - Digital wallet (app) can do this for you
 - Creates cryptographic "key pair" (SK_x , PK_x)
 - Secret key SK_x : to authorize use of your Bitcoin
 - Public key PK_x : public identifier and to validate transactions
 - **Address** comes from public key
 - We'll discuss details later...



Bitcoin wallet

- Also permits easy management of Bitcoins
- Sending and receiving...



Ways to score some BTC

- Buy through online exchange, e.g., Coinbase
 - Sent to wallet or “banked”
- "Mine" BTC
 - To be discussed...
- Have someone with BTC send some to your wallet
 - Buyer of some good you're selling, friend, etc.
 - Bitcoin ATM...
 - Exchange

Online sites

1.

Get Bitcoin

There are several ways to get Bitcoins, but the easiest is to exchange them for currency at your bank or a Bitcoin exchange. You can also buy Bitcoins from friends, accept them as payment for goods or services, or generate new Bitcoins through a process called "mining."

[Sign Up at Coinbase.com](https://www.coinbase.com)



2.

Shop Overstock.com

You can now pay for all your favorite products on Overstock.com using Bitcoins! As the first major retailer to accept Bitcoins, Overstock.com is expanding the possibilities of Bitcoin purchases by offering thousands of products to the Bitcoin community.



Bitcoin design—from basic principles

Key property #1:

Bitcoin is **pseudonymous**

- What does this mean?
- Each entity X has an (ECDSA) key pair (SK_X, PK_X)
- No association between X and real-world identity

Digital signatures are used in Bitcoin

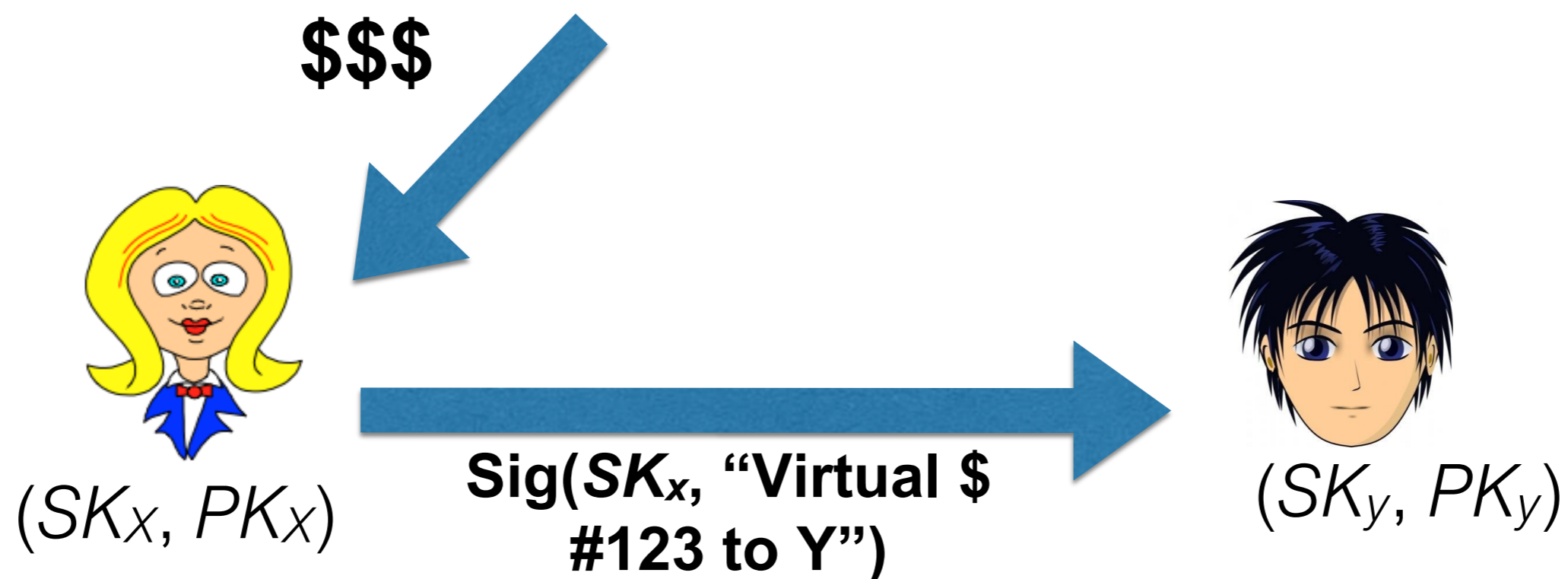
Bitcoin uses ECDSA

- “Elliptic-Curve Digital Signature Algorithm”
- Concretely, uses secp256k1 (slightly nonstandard) curve
 - Private key SK is 256 bits; (uncompressed) public key PK is 512 bits

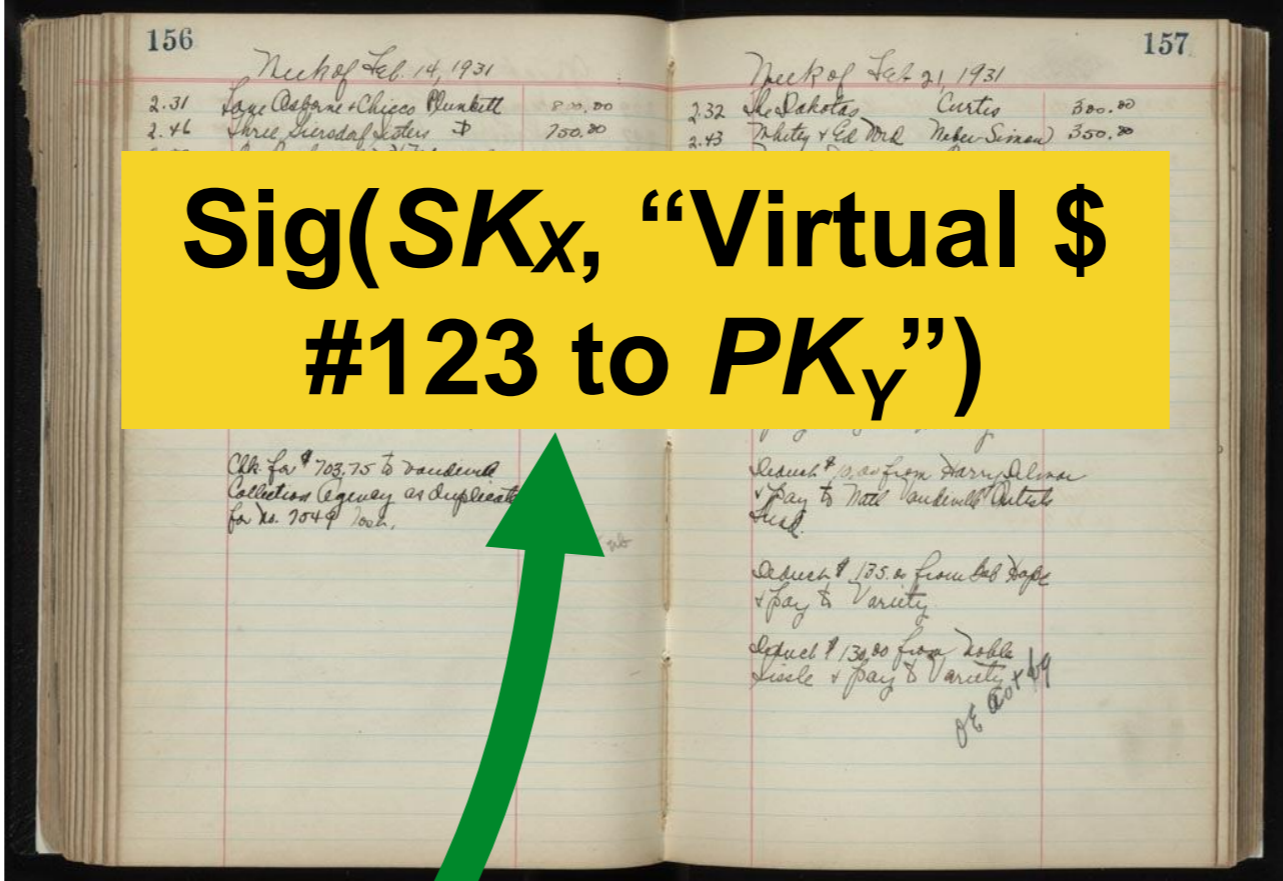


Could build naïve system...

- Idea: Coins *and* transactions, i.e., flow of money, can be authenticated—neither is forgeable
- Thanks to public-key crypto, everyone can verify all coins and transactions (if public keys are distributed throughout system)
- But we still have the double-spending problem...



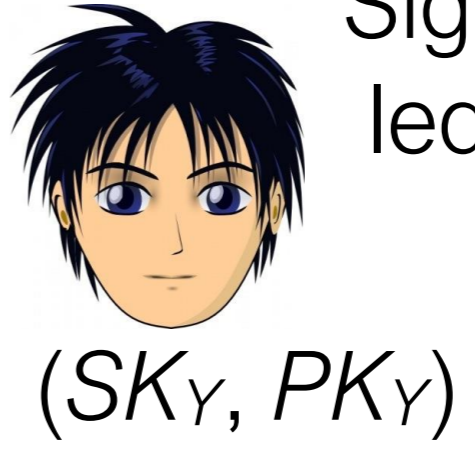
Idea: Bank maintains a *ledger*



Bob checks
Sig *and*
ledger ✓



Sig(SK_x , "Virtual \$ #123 to PK_y ")

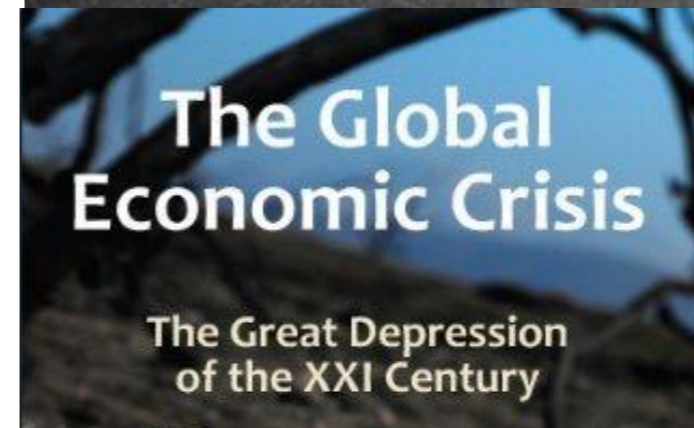


Ledger

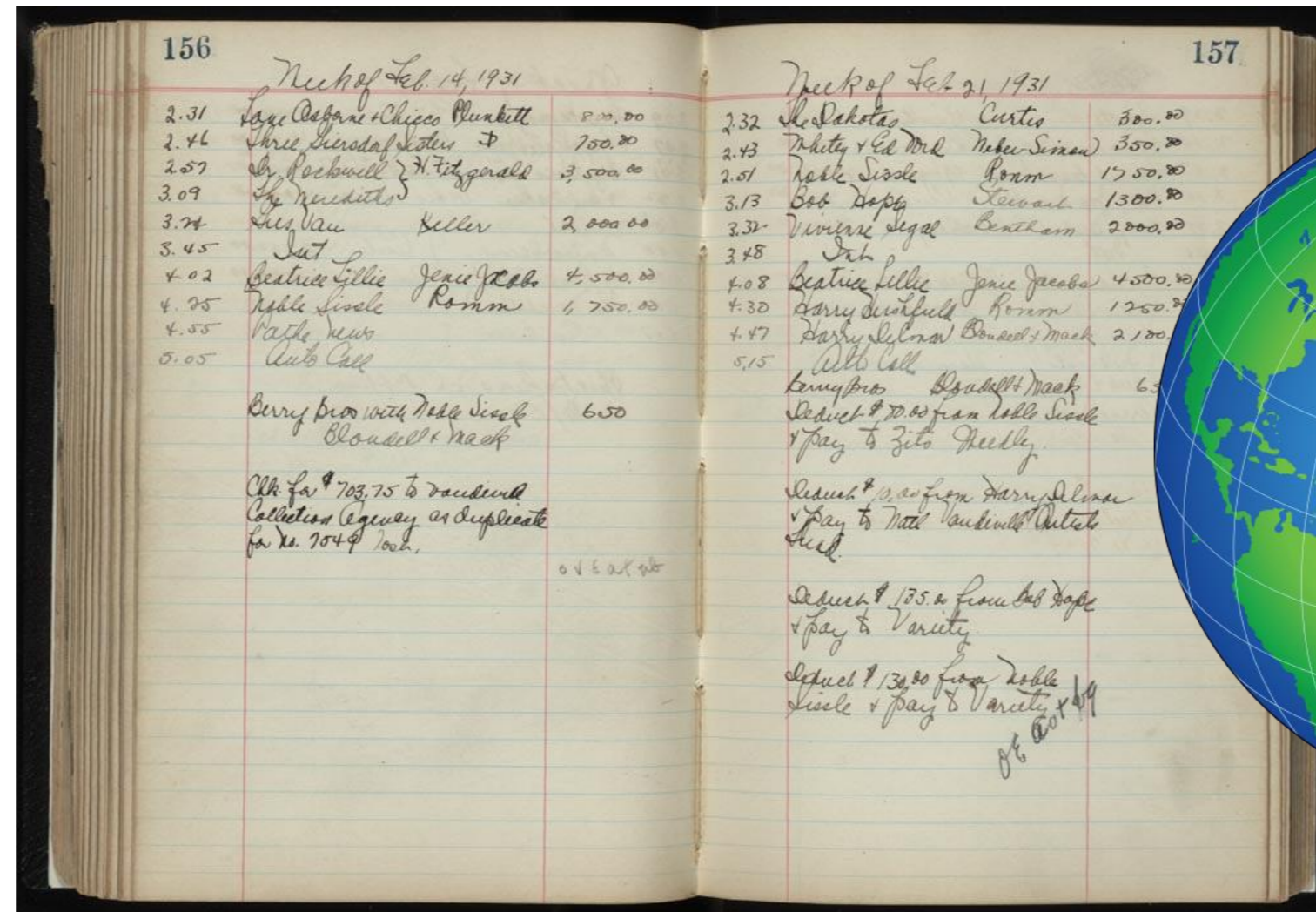
- Ledger is up-to-date record of all transactions.
- Bob now checks the ledger to be sure that Virtual \$ #123 hasn't been spent.
- Double-spending is now prevented!

But there's still a problem...

- You have to trust the Bank!
- Problems:
 - What if the Bank claims not to have received a transaction?
 - i.e., doesn't put it in ledger
 - What if the Bank confiscates money?
 - Who's going to create money? The Bank?
 - What if the Bank devalues money?



Key property #2: Bitcoin is decentralized



- No Bank!
- Ledger is *agreed upon* and *distributed* among many entities
- Called the **blockchain** in Bitcoin
- The key innovation in Bitcoin over older virtual currencies

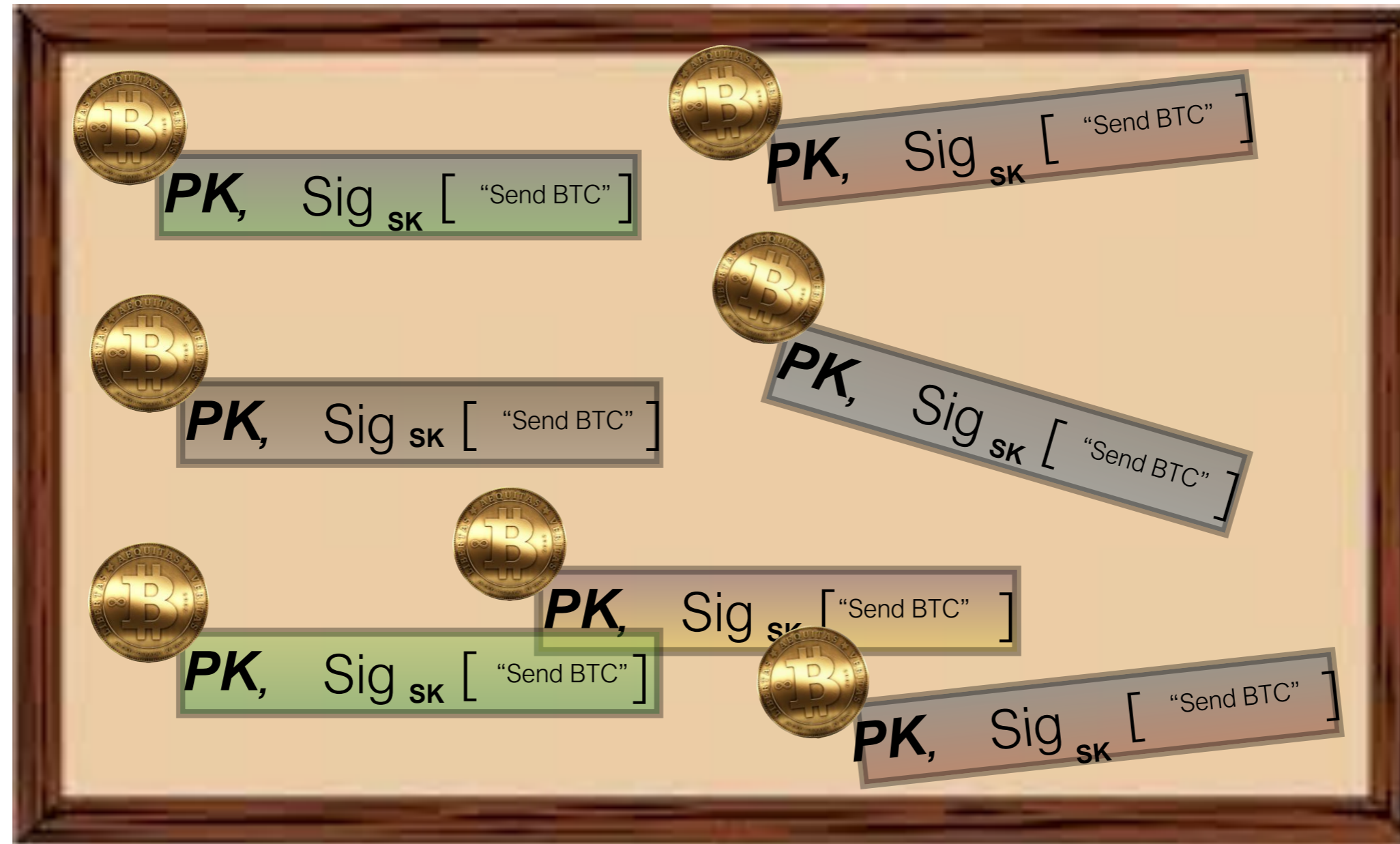
How does Bitcoin work?

- Every "account" holder has an (ECDSA) private / public digital signature key pair (***SK***, ***PK***)
- (Account *address* is $Addr = H(\mathbf{PK})$)
- Private keys sign (authorize) movement of money
- *Simplified* transaction...
 - ("Pay to PubKey Hash (P2PKH)")



PK_A, Sig_{***SK_A***} ["Send 1 BTC to ***PK_B***"]

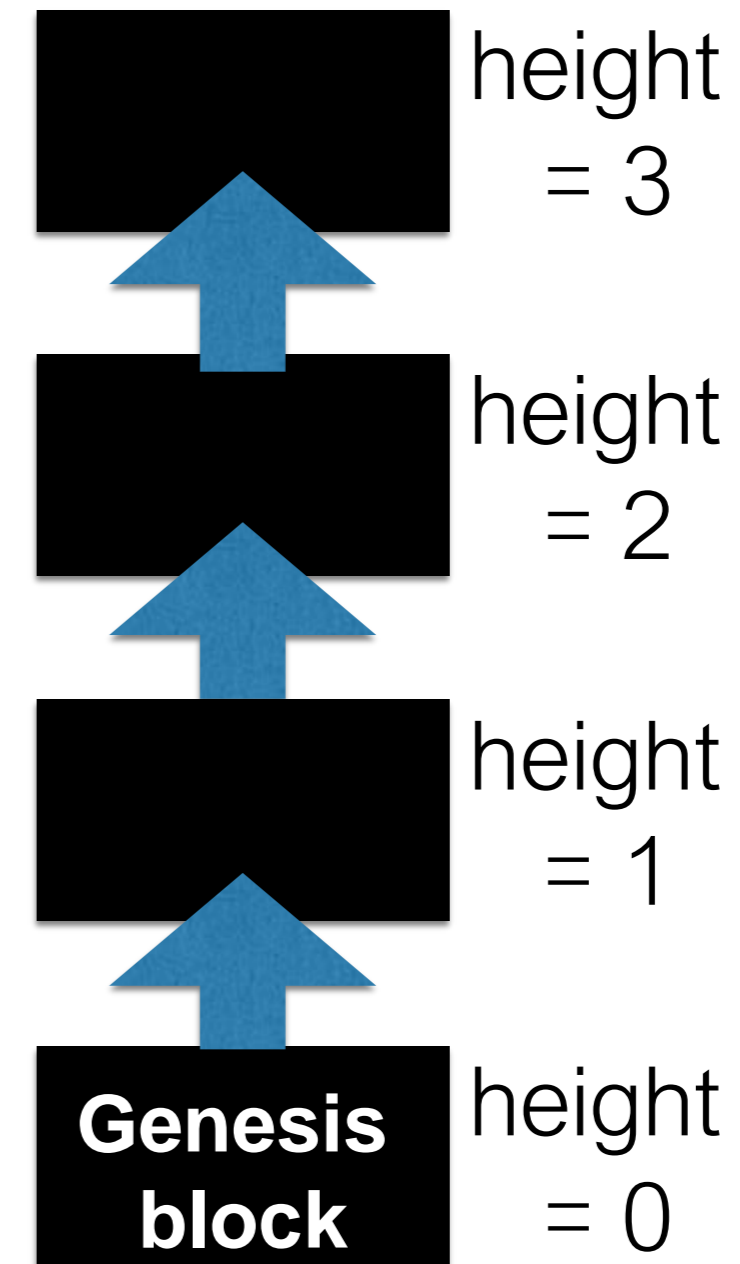
Global ledger (“*blockchain*”)



- Publicly records all Bitcoin transactions worldwide over time

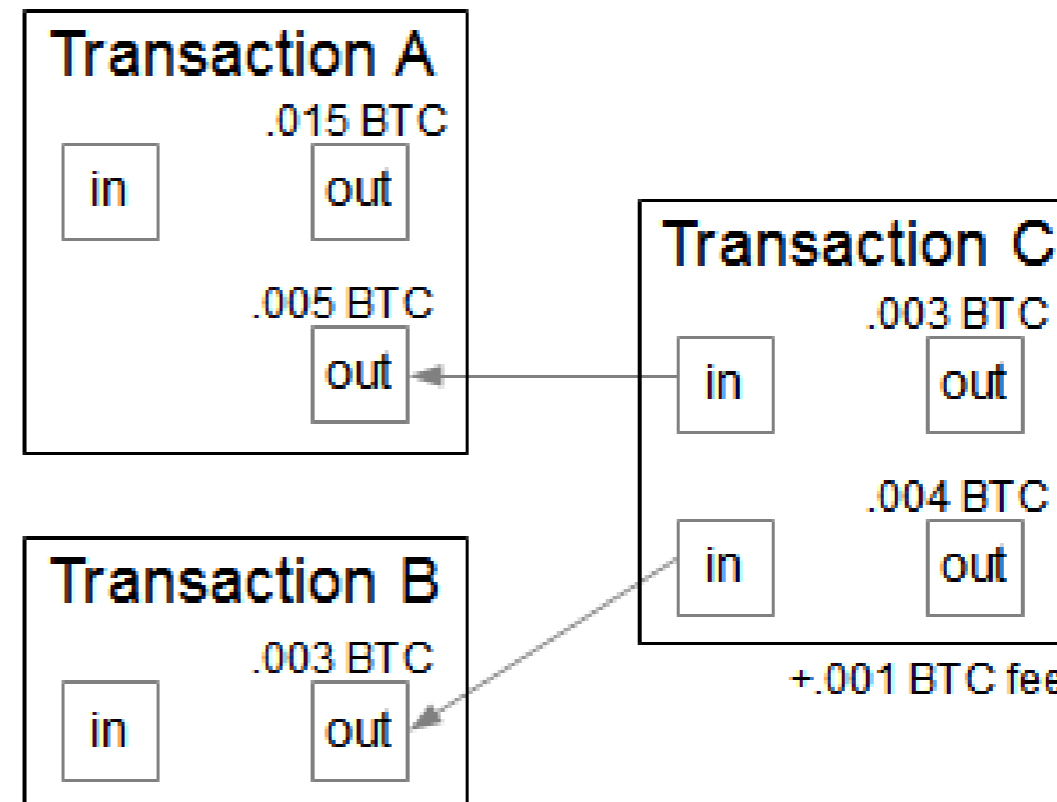
Blockchain

- Record of *every* transaction in Bitcoin system
- Maintained as append-only data structure
- New block added every 10 minutes (on average)
- Each block contains a bundle of latest transactions.
 - E.g., $\text{SIG}_{\text{PKA}}[\text{"Alice sends 0.4 BTC to Bob"}]$
 - (Actually, there's a scripting language, but we'll gloss over it...)



Blockchain

- Because full chain is a complete ledger / history of *all* transactions...
- Computing over the full block chain reveals the state / ownership of all BTC
- No explicit “account balances”
- Structured in terms of transactions



[Figure source: <http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html>;

Hi, Ken!]

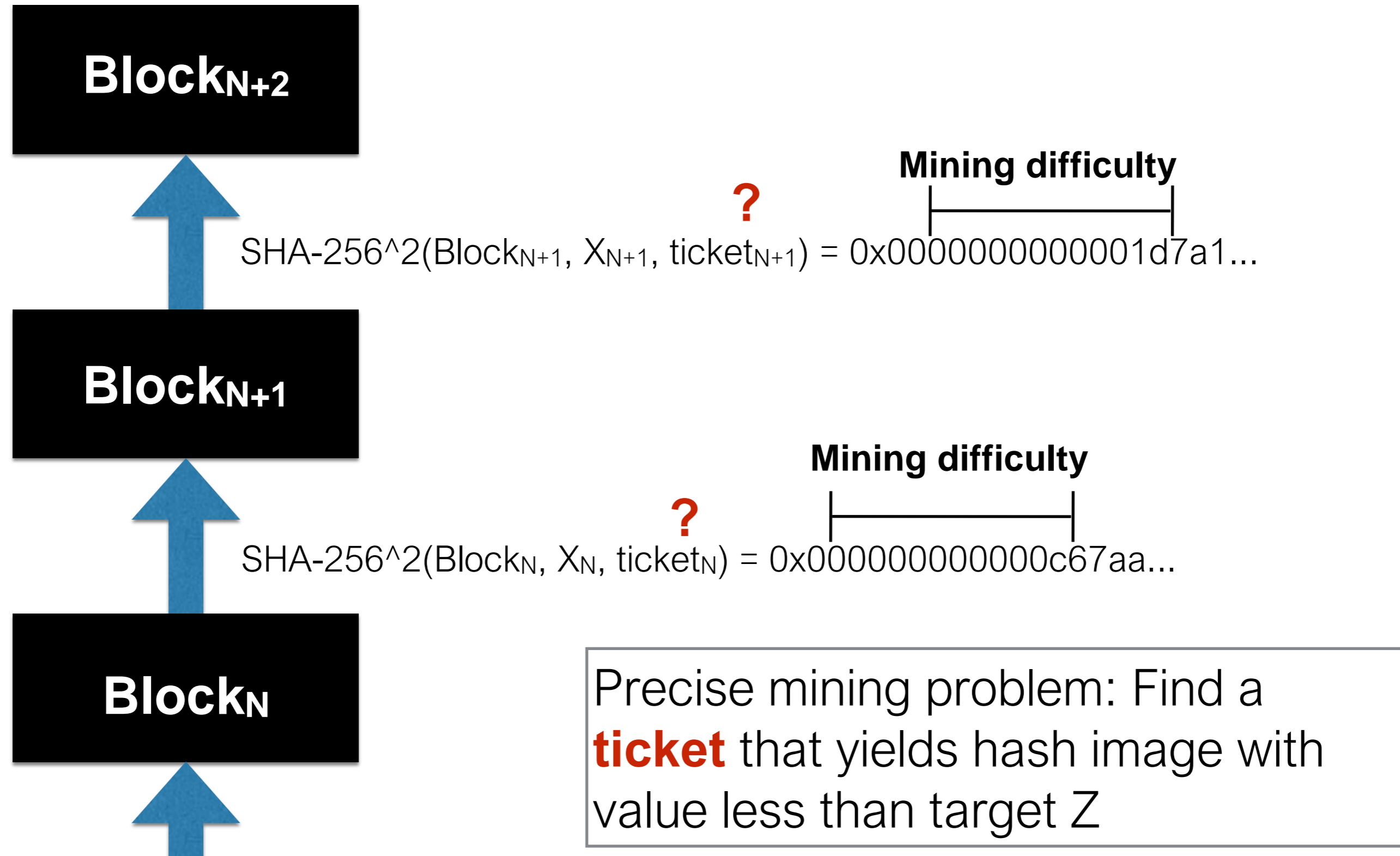
But how is a block validated?

- I.e., how does system decide what transactions go into next block?
- Ideal for P2P system: All clients in the world *vote* on the correct block chain.
- But it's hard to ensure one vote per machine.
 - E.g., there's the problem of "Sybil" attacks: How to prevent one user from creating multiple identities?
- So "voting" (cleverly) in Bitcoin takes the form of hash power.
 - I.e., one vote per CPU (roughly speaking)

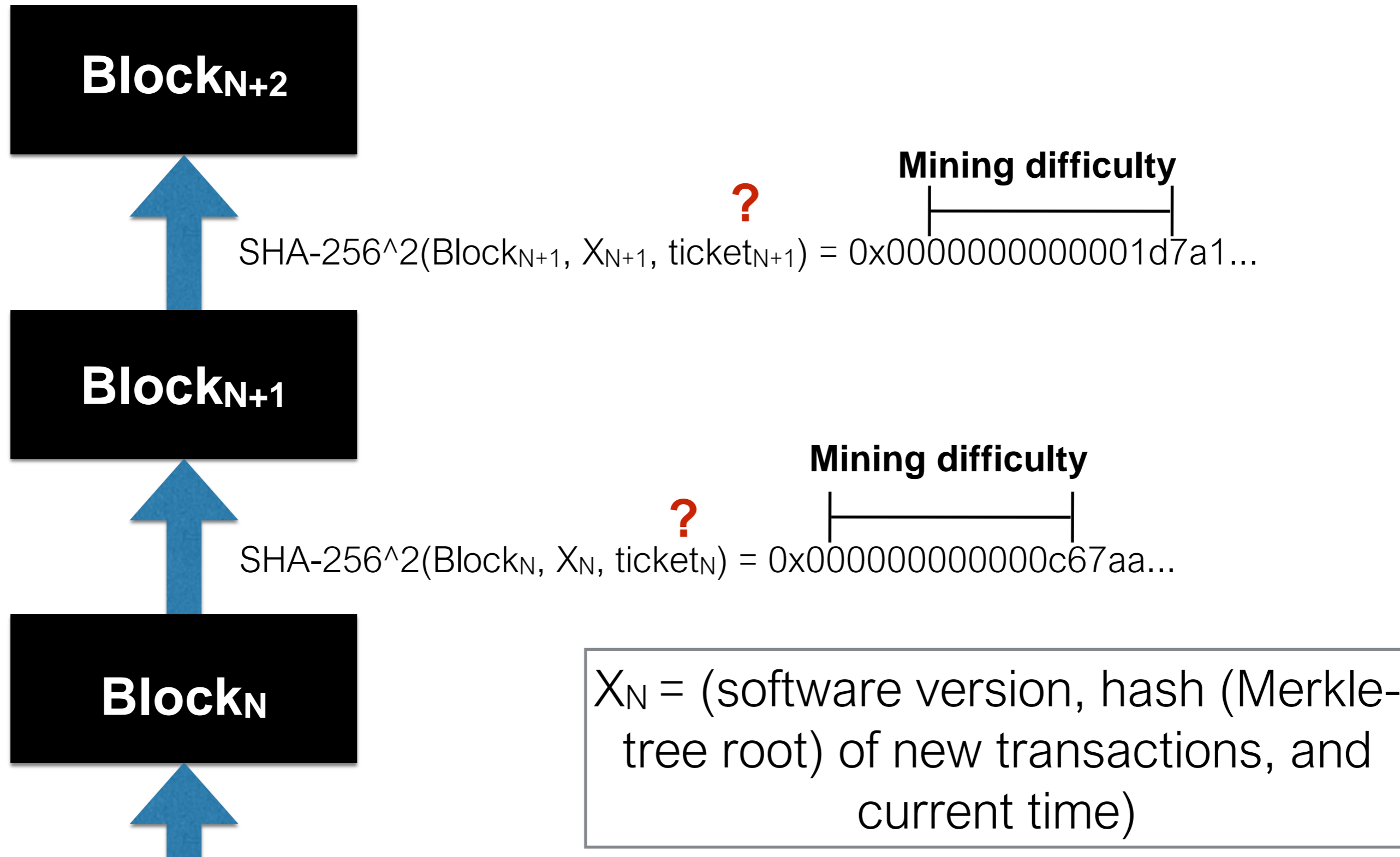
But how is a block validated?

- Communal, computationally-intensive process called *mining*.
 - Together, mining community defines blockchain
- Intuition:
 - All miners collectively search for hard-to-compute “signature” on new block
 - Solution proves w.h.p. that result is communal effort
 - Attacker with little computing power unlikely to mine block

Block mining



Block mining



This problem requires a massive amount of hash power

- The mining puzzle is called a *Proof of Work* (PoW)
- In Random Oracle Model for SHA-256, expected (double) hashes to mine a block is...
 - $2^{256} / Z$
 - = (Bitcoin “Difficulty” factor) $\times 2^{32}$
- Difficulty adjusted every 2016 blocks to achieve 10-minute block mining epoch

$$\text{SHA-256}^2(\text{Block}_{N+1}, X_{N+1}, \text{ticket}_{N+1}) \stackrel{?}{\leq} Z$$

This problem requires a massive amount of hash power

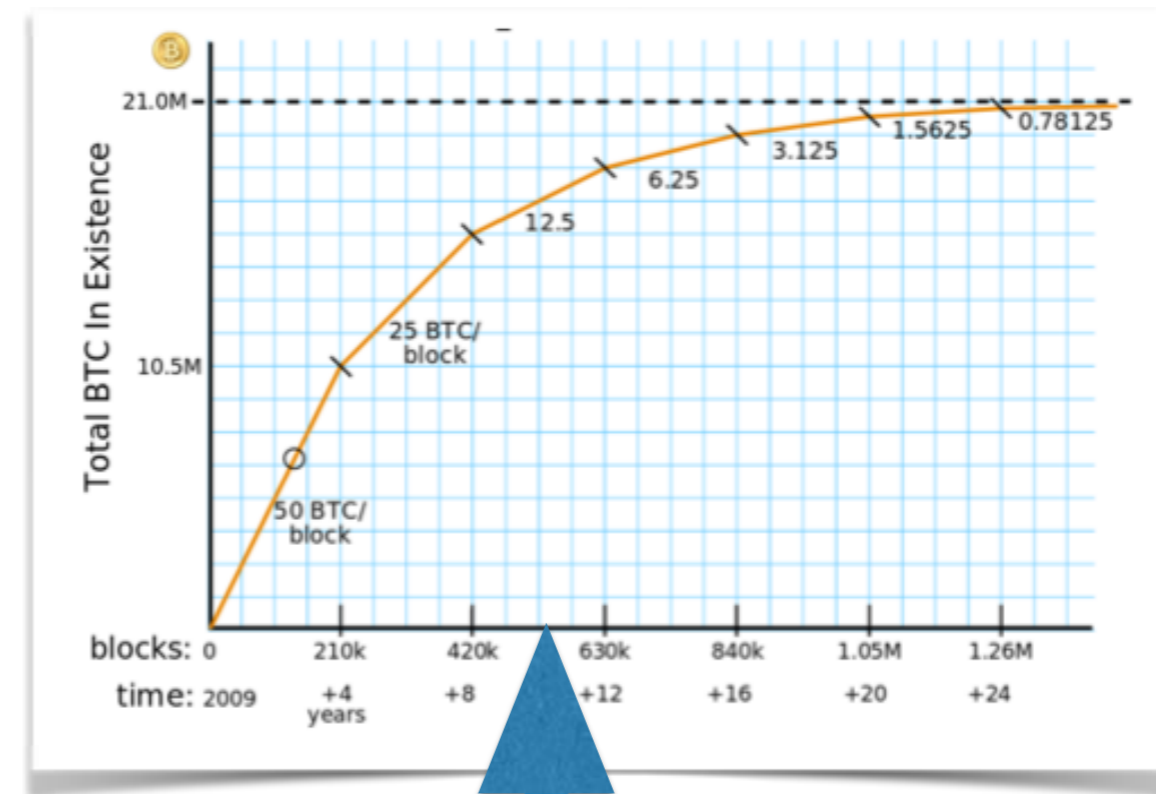
- In Nov. 2017, expected number of (double) hashes to mine a block was roughly 10^{22} .
- In Nov. 2021, Whole Bitcoin network is running at about 180,000,000,TH/s!
- Not easily duplicated, so hard for attacker to seize control of network

$$\text{SHA-256}^2(\text{Block}_{N+1}, X_{N+1}, \text{ticket}_{N+1}) \stackrel{?}{\leq} Z$$

What's the incentive for miners to mine?



- Key idea: Bitcoin is a lottery.
- Every miner tries tickets until a “winning” one is found.
- The prize for the winner: Bitcoins!
 - Special transaction in block assigns BTC to winner
 - Originally, 50 BTC; today (nov 2021), 6.25 BTC (\$351,000+ on 23 Nov 2021.)
 - Winner also gets transaction fees
- 21 million BTC will be produced over the lifetime of the system.



Nov. 2017
height ≈
493k

Courtesy:
Brian Warner

$$\text{SHA-256}^2(\text{Block}_{N+1}, X_{N+1}, \text{ticket}_{N+1}) \stackrel{?}{\leq} Z$$

What's the incentive for miners?



- In principle, Bitcoin is democratic
- *Anyone* can mine.
- Reward is proportional to computational investment.
- But...

How do miners mine?

- In the early days, people just used their PCs.
- ASIC (Application-Specific Integrated Circuit) hardware is much more cost-effective.
- Professionals buy and replace ASICs frequently.

Major Update (September 10, 2014): Speed increase; 6TH/s Yukon is now \$3,920.00 !! (Best on the Market for now)

The SP31 Yukon Power Miner

The introduction of the SP31 Yukon powerful miner is good news to the bitcoin markets. The essential 5.5 **TH/s** mining machine focuses on the affairs of traders, it has an amazing hash power and consumes relatively very low power. It has been understood that the hashing power of SP31 has four times the power of SP10 and relatively twice the hash to power ratio.



Start Mining Bitcoin

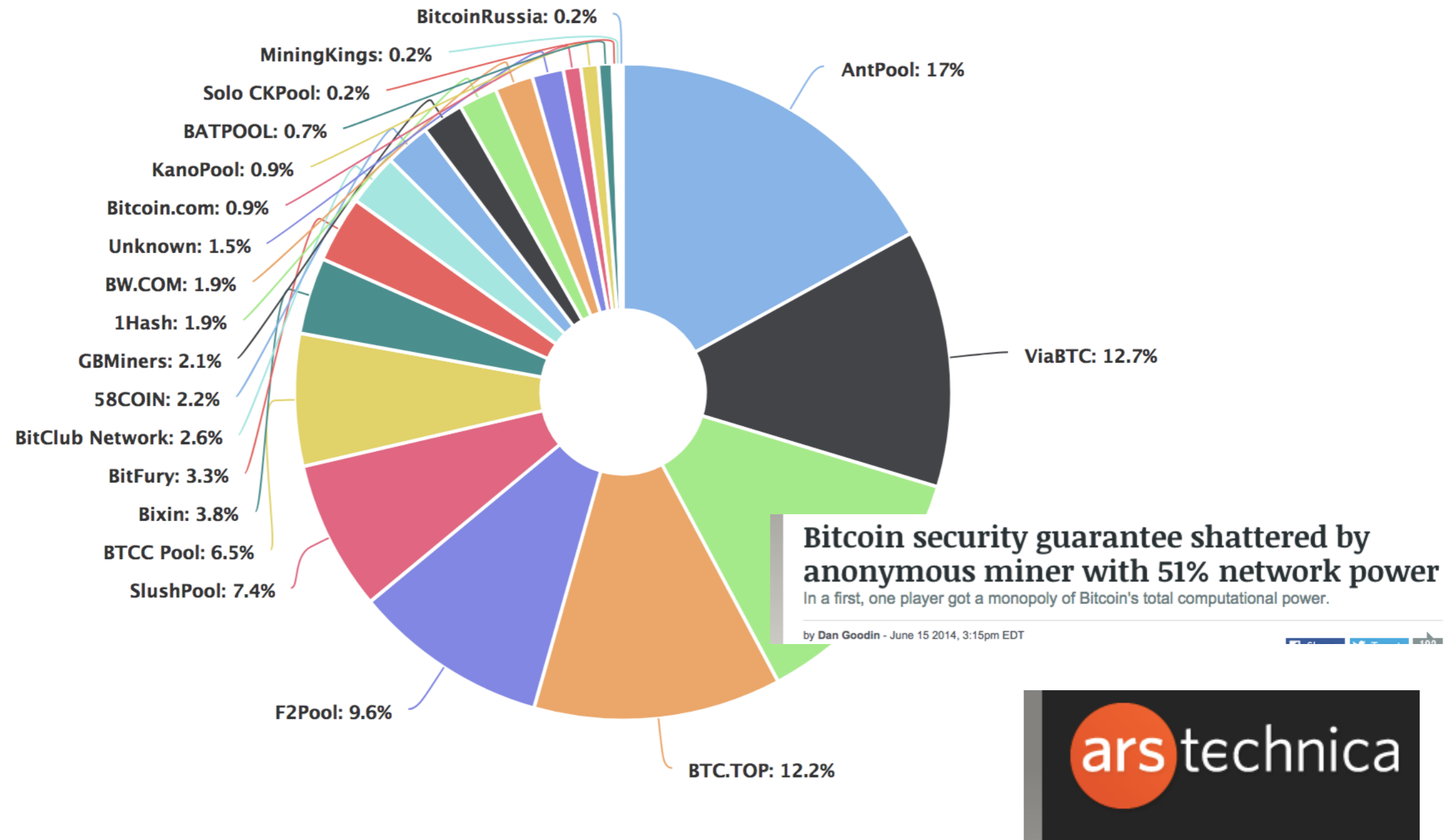
Get started now for only \$24.99




GAWMiners

[Learn More >>](#)

Mining pools



Researchers from Cornell University say that on multiple occasions, a single mining pool repeatedly contributed more than 51 percent of Bitcoin's total cryptographic hashing output for spans as long as 12 hours. The contributor was **GHash**, which bills itself as the "#1 Crypto & Bitcoin Mining Pool." During

How Bitcoin Is Like North Korea



JOE WEISENTHAL

JAN. 12, 2014, 11:04 AM

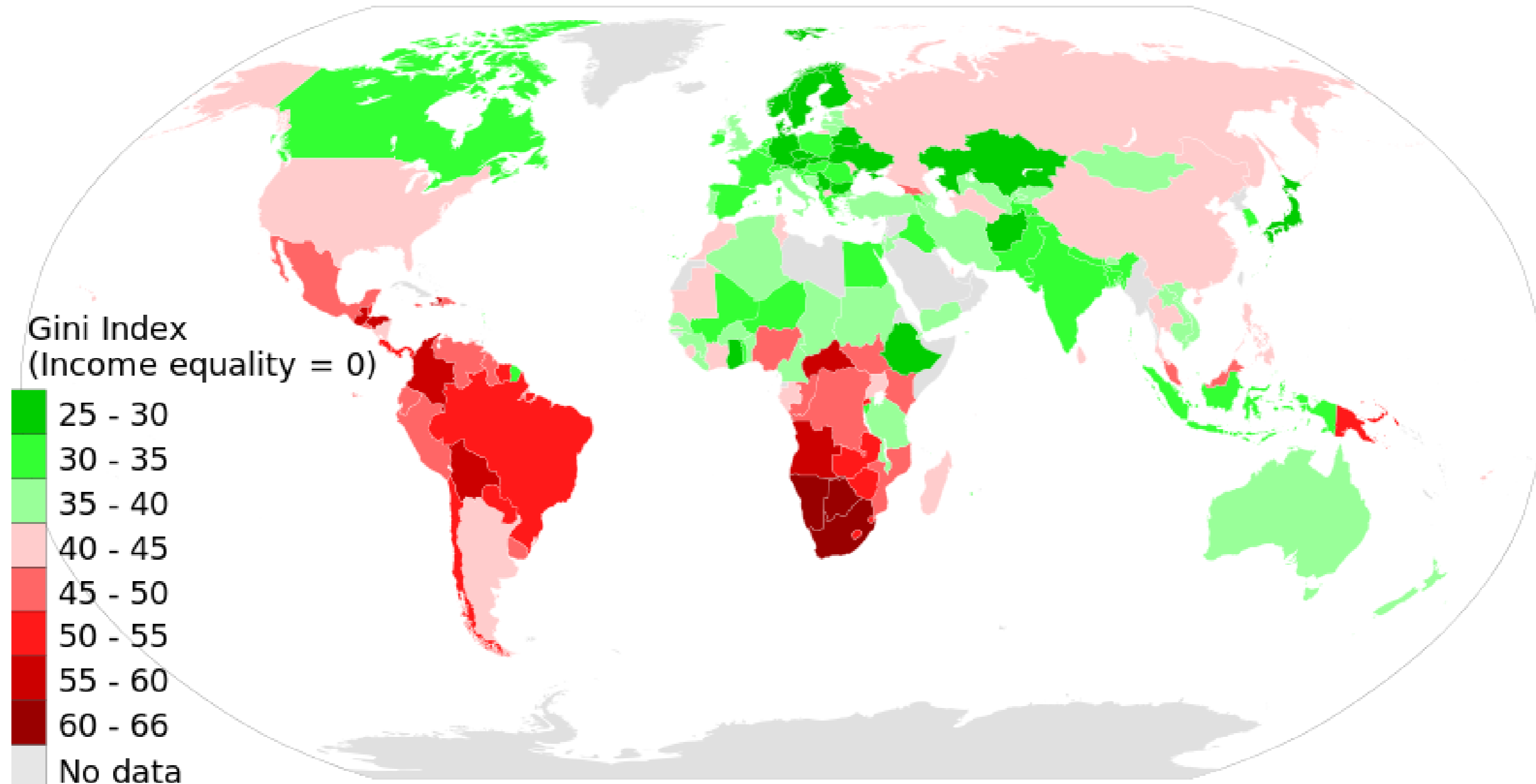


11,529

BUSINESS
INSIDER

Estimate for Bitcoin: 88

GINI Index (Inequality Index)

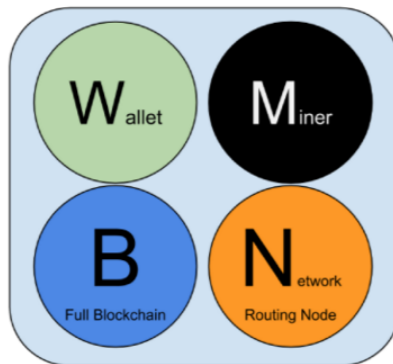


Other parts of Bitcoin

Mining blocks isn't enough

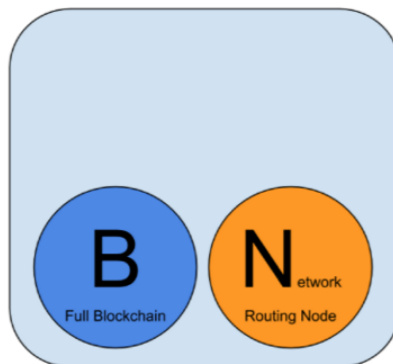
- What else is needed to make a working monetary system?
 - Broadcasting transactions and blocks
 - Storing ledger / blockchain
 - Enabling users to spend and receive money

Some node types in Bitcoin network



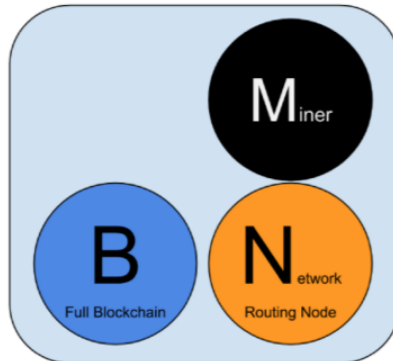
Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



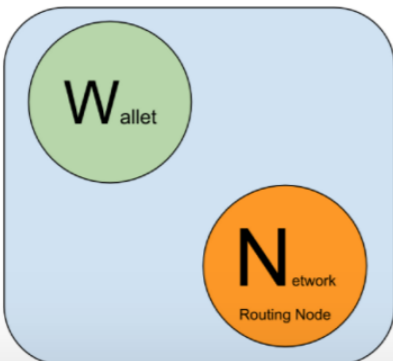
Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.



Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

+Super Node

- **Publicly accessible**

+Pool Miner

- **Lacks full blockchain**

Routing functionality

- Transactions and blocks are broadcast to *entire network of full nodes*
- Rebroadcast protocol
 - Each node transmits to 8 other (randomly selected) nodes
 - TCP on port 8333

Full nodes

- Store entire blockchain
- Enforce consensus rules, ensuring blocks in blockchain adhere to
 - 12.5 BTC reward
 - Correct signatures on transactions
 - BTC not double-spent
 - Etc., etc.

Full node distribution

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Tue Nov 21 2017
09:10:20 GMT-0500 (EST).

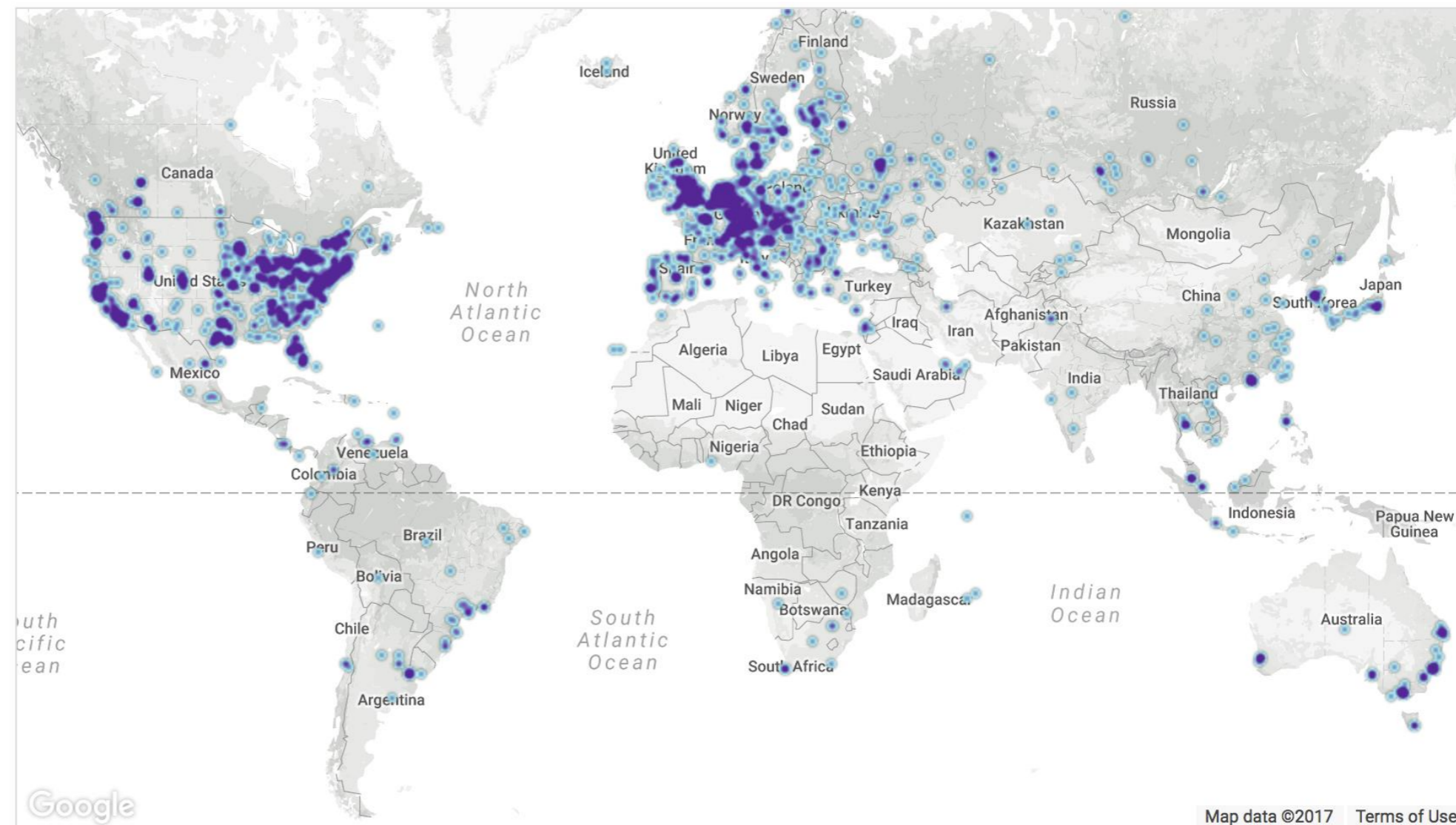
10975 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	3090 (28.15%)
2	Germany	1849 (16.85%)
3	France	748 (6.82%)
4	China	662 (6.03%)
5	Netherlands	529 (4.82%)
6	Canada	450 (4.10%)
7	United Kingdom	439 (4.00%)
8	n/a	370 (3.37%)
9	Russian Federation	350 (3.19%)
10	Singapore	236 (2.15%)

[More \(99\) »](#)

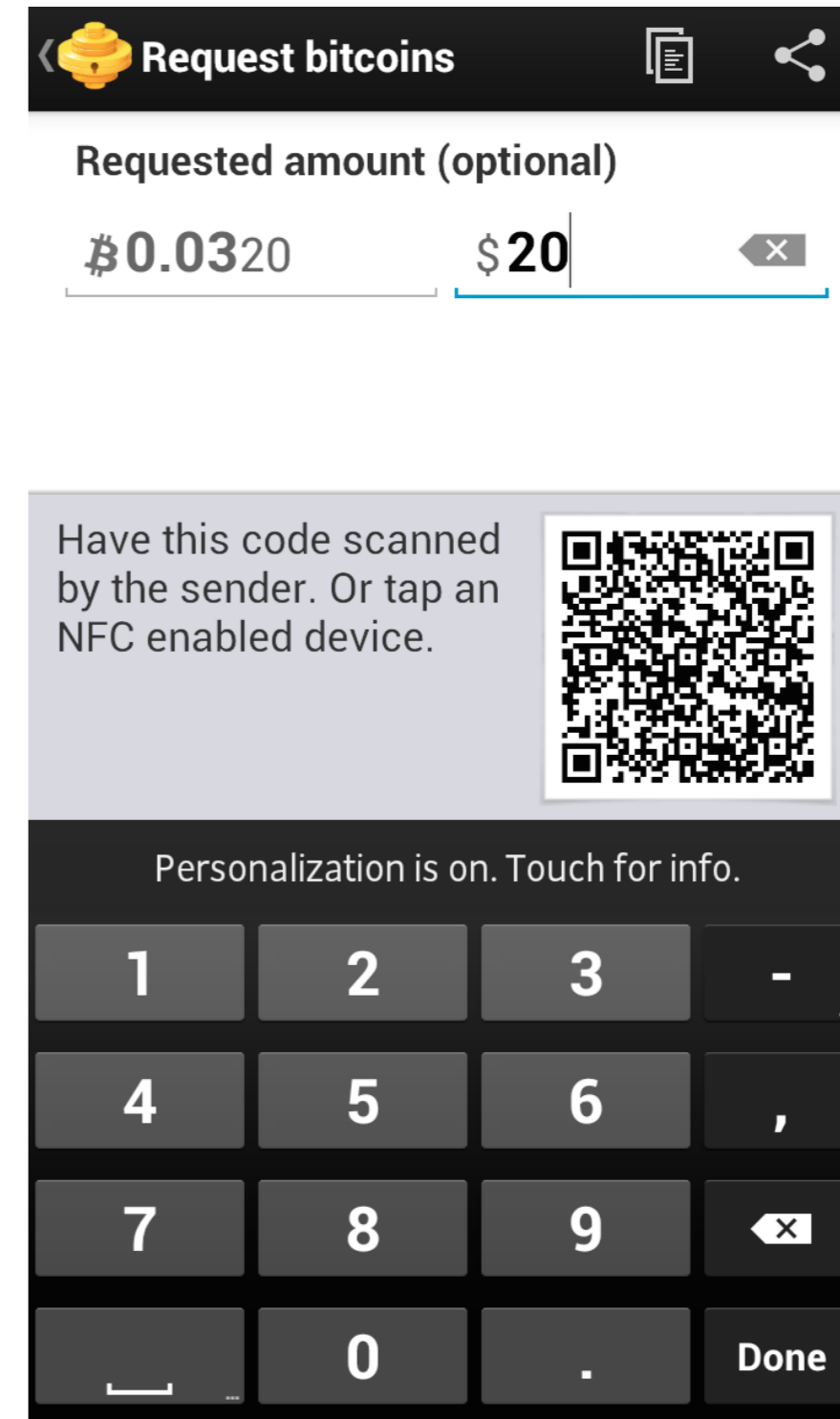


Map shows concentration of reachable Bitcoin nodes found in countries around the world.

[LIVE MAP](#)

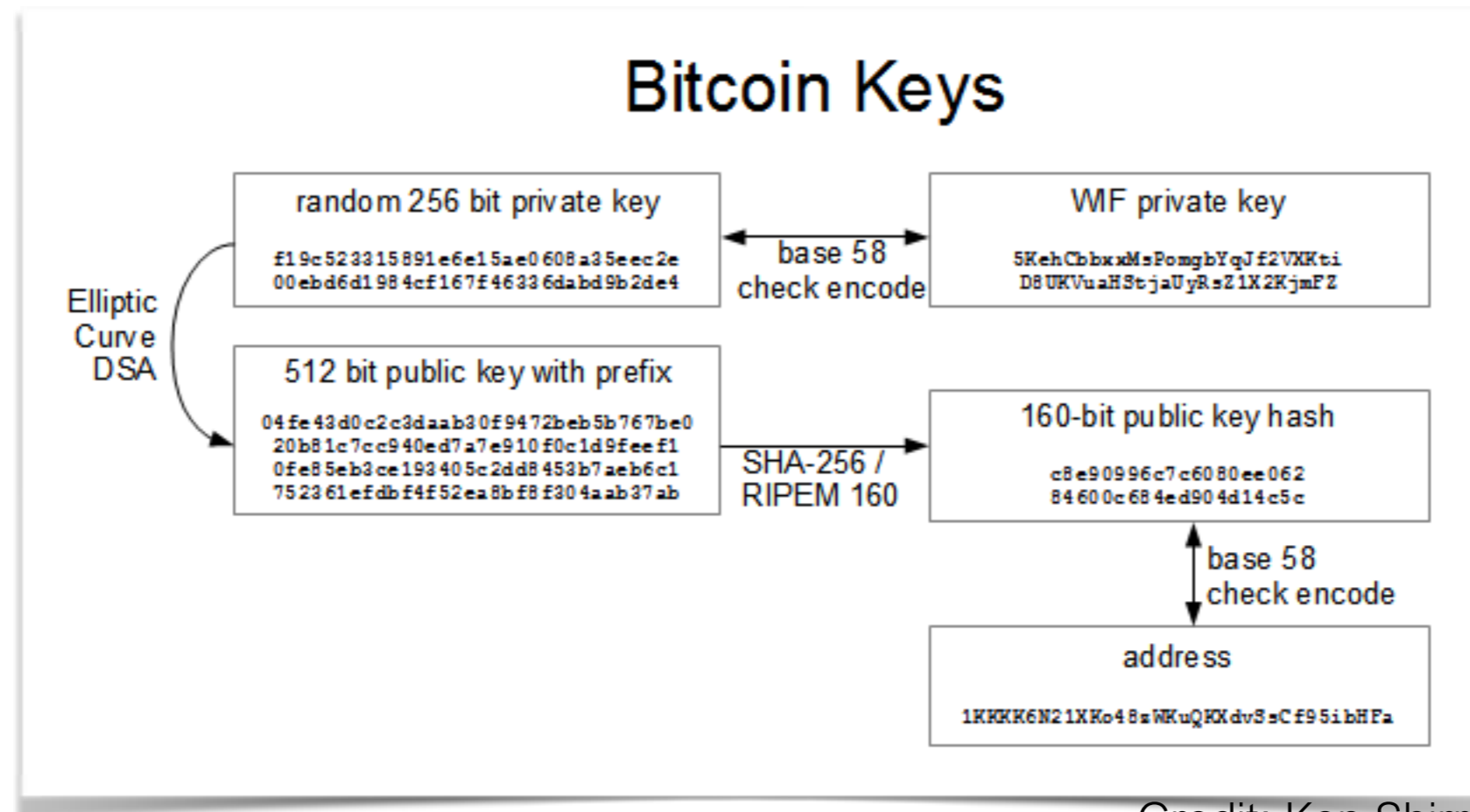
Bitcoin wallets

- You don't need to mine or run full node to use Bitcoin
- Wallet are applications that permit easy management of a Bitcoins.
- What's going on under the hood?



Bitcoin wallets: Under the hood

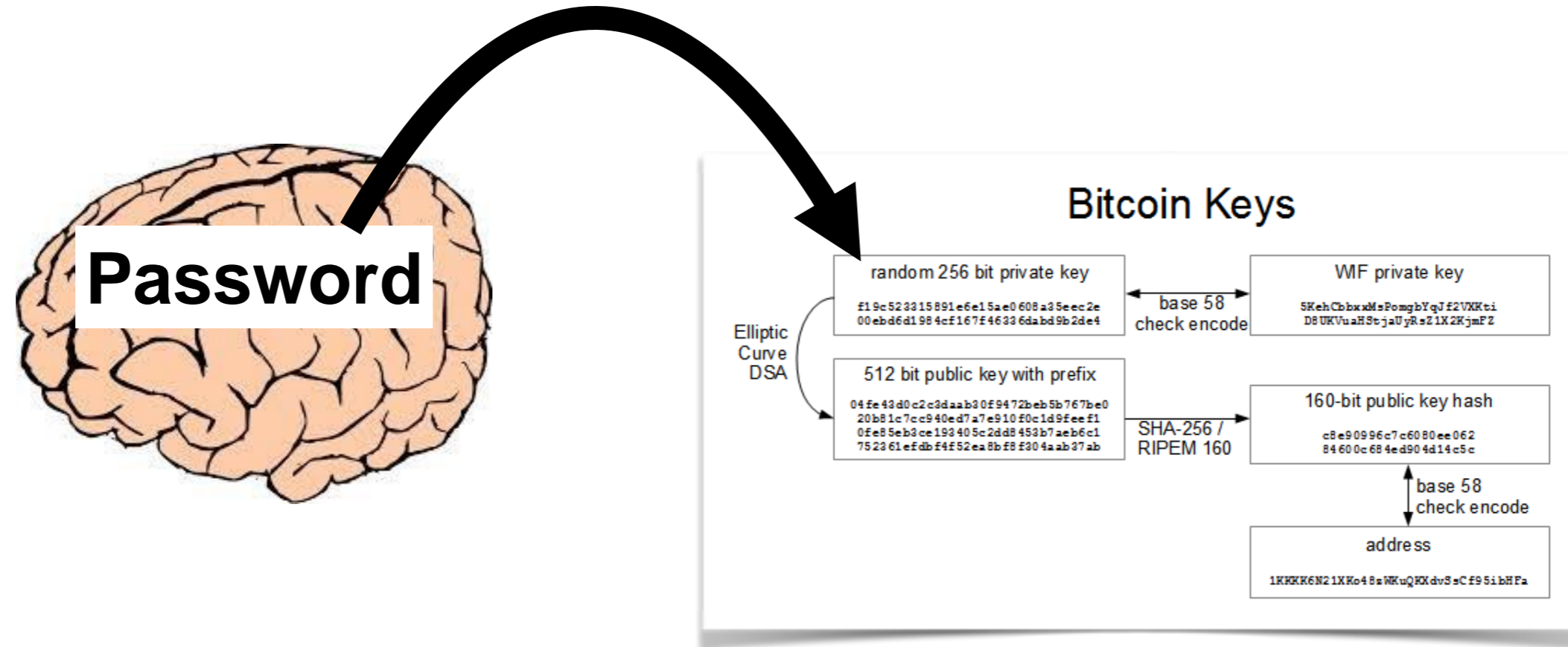
- Remember: identity associated with ECDSA digital signature key pair
 - *SK* used to sign / authorize transactions.
 - *PK* used to identify users and verify transactions.
- Bitcoin wallet stores, protects, and allows use of *SK* to make transactions.



Credit: Ken Shirriff

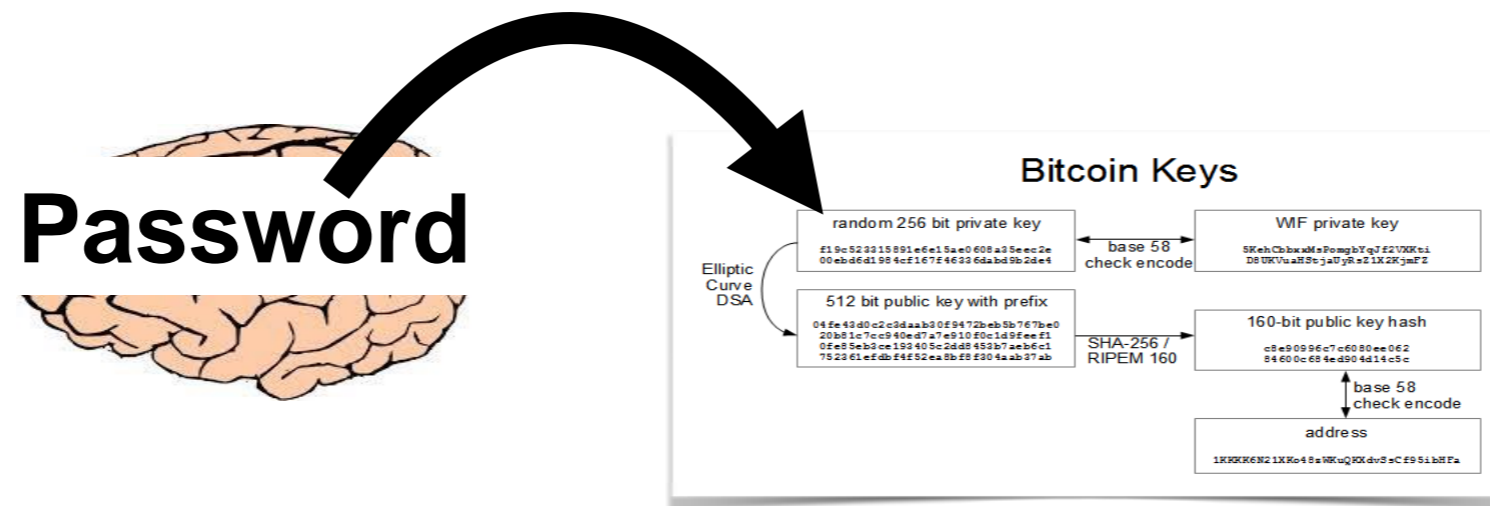
Brain wallets

- You can generate *SK* from a password



- Your Bitcoin are then completely portable.

Brain wallets



- Unfortunately, human brains are poor password stores...
- Cracking brainwallets at one point rumored more profitable than mining...



Finders keepers? I found an address with 50 BTC via brain wallet!

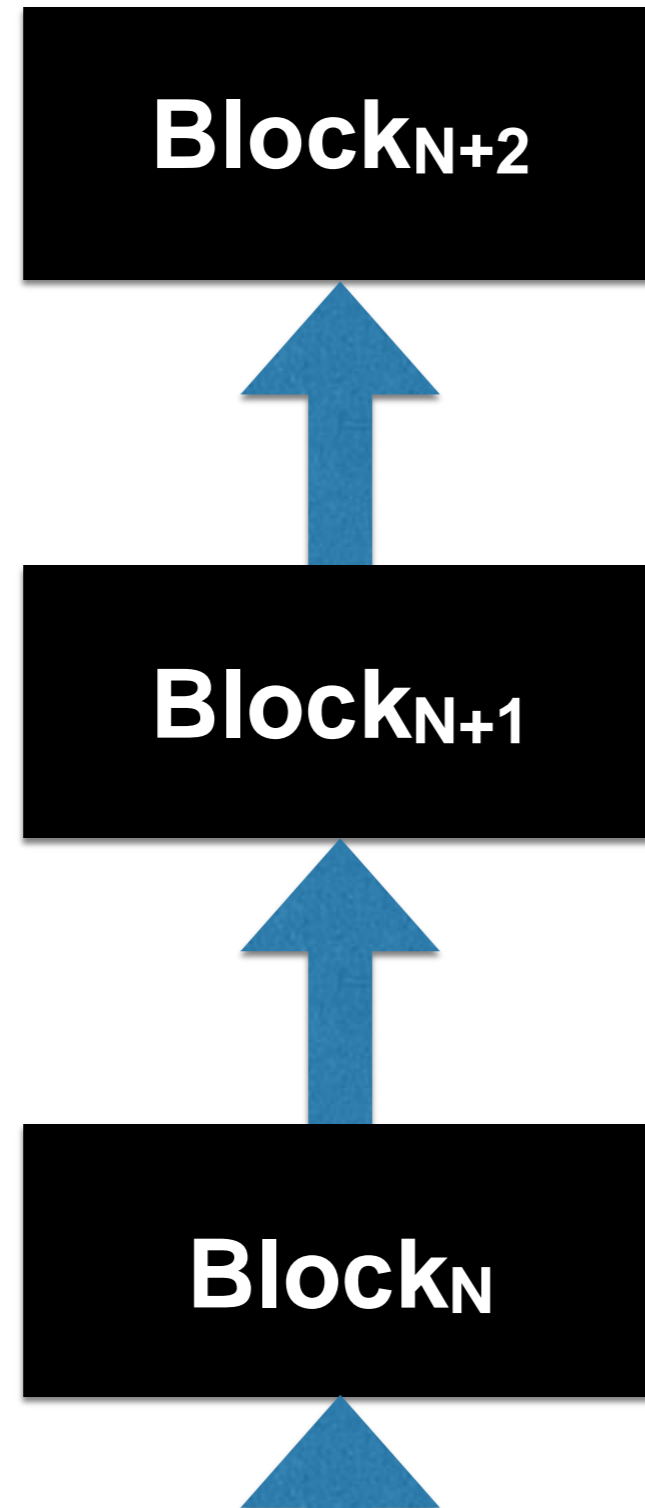
January 18, 2014, 04:58:04 PM

#1

I was playing around with the brain wallet and checking the addresses with blockchain. I found a wallet with a balance of 50 BTC! The coins were put in the wallet in 2011 and there hasn't been any activity since. I don't want to steal someones coins but if they are "lost" I don't want to have them just sitting there. It's a lot of money! I was thinking of sending a small amount into the wallet with a message letting the person know the situation. If nothing happens after a while I guess it's "Finders Keepers, Losers Weepers." What's the right thing to do in this situation?

Bitcoin's good features

The **blockchain** means much more than Bitcoin



- Nebulous term...
- Generally refers to *ledger*
- Distributed, robust, publicly visible piece of memory
- Good for things other than money!
 - Timestamping documents
 - Audit
 - Etc., etc.

Bitcoin's nice properties

- Low transaction fees + no middleman
 - 👉 Low-fee payments
- Decentralized
 - 👉 Cross-border remittances

But Bitcoin basically only good for moving currency around...

Bitcoin problems

Ponzi Scheme with Huge Marketing Push

Laura Sagers releases world's first Bitcoin love song



bitcoin pet tag
\$21.95

Including your dog...

Huge environmental impact

Major Update (September 10, 2014): Speed increase; 6TH/s Yukon is now \$3,920.00 !! (Best on the Market for now)

The SP31 Yukon Power Miner

The introduction of the SP31 Yukon powerful miner is good news to the bitcoin markets. The essential 5.5 TH/s mining machine focuses on the affairs of traders, it has an amazing hash power and consumes relatively very low power. It has been understood that the hashing power of SP31 has four times the power of SP10 and relatively twice the hash to power ratio.




Mining Software	cgminer with custom plugin
Form Factor	2 U rack mountable (mounting ears provided)
Network	Single 10/100 Ethernet port
Fans	4 X 80 mm
Power Supply	2 x 1200 W - Drawing 1500 W "at the wall" manufacturer)
Input Rating	90 - 264 VAC
Nominal Power Consumption	3000 W

Exclusive 1st Review: Bitmain Antminer S7, 4.8+ th/s Using Only 1250 Watts

By Bitcoinist.net | Sep 13, 2015 8:17 AM EST



IMPACT OF ZEROACCESS BOTNET



One of the largest P2P botnets ever known

X 1.9 million

ZeroAccess carries out two revenue generation activities

?

?


*Botnet generates...

1.9M x

Earns US\$ 2,165/day


488 TB network traffic/day

Per annum earnings: Tens of millions US\$!!!



3,458 MWh/day

=




Power for > 111,000 homes/day

Cost of electricity > US\$ 560,887/day

Sources: <http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3>, http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_6_a, <http://www.symantec.com/connect/symantec-blogs/sr>

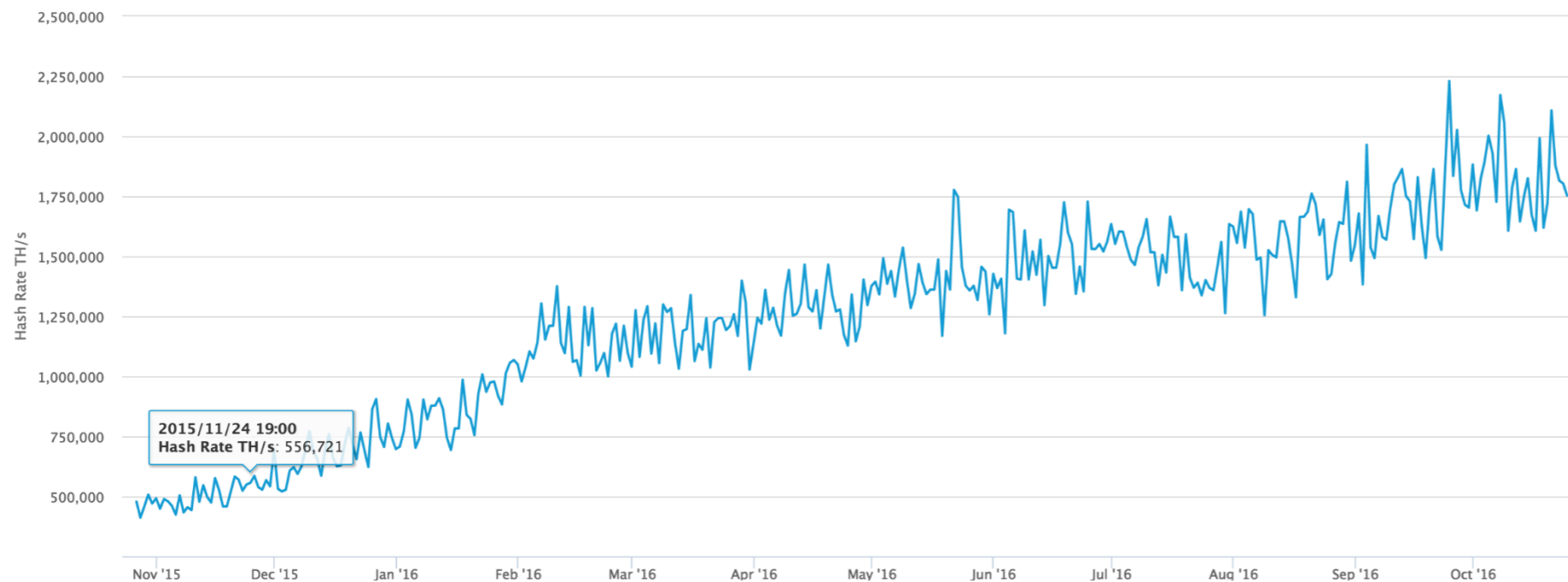
*Based on a test PC with Pentium D 945 3.4 GHz CPU running 24 hours a day. Unit price of electricity of \$0.1622 KWh. Annual US average home electricity usage of 11,280 KWh.


@threatintel | www.symantec.com

Huge Environmental Impact

- 2017: \$1+ billion in computing hardware invested in Bitcoin ecosystem
- 2800+ MW
(<http://realtimebitcoin.info/>)

and growing...



Power station	# Units	Net Capacity (MWe)	Country	Location	Refs
Brokdorf	1	1,410	Germany	53°51'03"N 09°20'41"E	
Callaway Plant	1	1,190	United States	38°45'42"N 91°46'48"W	
Clinton Nuclear Generating Station	1	1,043	United States	40°10'20"N 88°50'06"W	
Cofrentes Nuclear Power Plant	1	1,064	Spain	39°13'00"N 01°03'00"W	
Columbia Generating Station	1	1,131	United States	46°28'16"N 119°20'02"W	
Enrico Fermi Nuclear Generating Station	1	1,122 ^[note 7]	United States	41°57'46"N 83°15'27"W	
Emsland Nuclear Power Plant	1	1,329	Germany	52°28'27"N 07°19'04"E	
Fangchenggang Nuclear Power Plant	1	1,000 ^[note 8]	China	21°40'36"N 108°33'38"E	
Grand Gulf Nuclear Generating Station	1	1,266	United States	32°0'24"N 91°2'54"W	
Grohnde Nuclear Power Plant	1	1,360	Germany	52°02'07"N 09°24'48"E	
Higashidōri Nuclear Power Plant	1	1,067	Japan	41°11'17"N 141°23'25"E	[5]
Hope Creek Nuclear Generating Station	1	1,191	United States	39°28'04"N 75°32'17"W	
Leibstadt Nuclear Power Plant	1	1,190	Switzerland	47°36'11"N 08°11'05"E	
Perry Nuclear Generating Station	1	1,240	United States	41°48'03"N 81°08'36"W	
Seabrook Station Nuclear Power Plant	1	1,247	United States	42°53'56"N 70°51'03"W	
	1	1,188	United Kingdom	52°12'48"N 01°37'07"E	
	1	1,060 ^[note 32]	Japan	36°27'59"N 140°36'24"E	[5]
	1	1,003	Spain	40°42'04"N 02°37'19"W	
	1	1,108 ^[note 33]	Japan	35°40'22"N 136°04'38"E	[5]
	1	1,045 ^[note 34]	Spain	40°57'05"N 00°52'00"E	
	1	1,168	United States	29°59'43"N 90°28'16"W	
	1	1,123 ^[note 36]	United States	35°36'10"N 84°47'22"W	
	1	1,160	United States	38°14'00"N 05°41'00"W	

Huge destabilizing effect

The image displays two screenshots of online marketplaces. The top screenshot is from Silk Road, an anonymous market, featuring a navigation menu with categories like Drugs (2,399 items), Apparel (114 items), and Art (7 items). The main content area shows a grid of drug listings with images and prices. The bottom screenshot is from an 'anonymous marketplace' and shows a detailed listing for 'Meth (1g) High-grade Crystal Meth' by the seller 'vortexmilkman(99)'. The listing includes a price of \$155.36, shipping information, and a description: 'As of NOV 14...got the crystal situation better than ever...got a guaranteed & consistent flow of the highest quality crystal available.' A photograph of the white crystal methamphetamine is also visible.

Silk Road anonymous market
messages 1 | orders 0 | account \$0.00

Shop by Category

- Drugs 2,399
 - Cannabis 341
 - Dissociatives 65
 - Ecstasy 209
 - Opioids 156
 - Other 144
 - Precursors 12
 - Prescription 526
 - Psychedelics 427
 - Stimulants 273
- Apparel 114
- Art 7
- Books 743
- Collectibles 12
- Computer equipment 19
- Custom Orders 26
- Digital goods 310
- Drug paraphernalia 89
- Electronics 20
- Erotica 319
- Fireworks 2
- Food 3
- Forgeries 58
- Hardware 2
- Home & Garden 7
- Jewelry 48
- Lab Supplies 5
- Lotteries & games 29
- Medical 5

5x - 10mg Dexedrine (Pure Dextroamphetamine) \$4.94

2 x 0,25 mg Xanax (Alprazolam) \$1.50

Malana charas hand rubbed Indian hash 100g \$75.83

1 Gram OG NUSH OIL 81% THC 90% TOTAL \$4.13

14 grams (1/2 Ounce) of Nebula JWH-122 \$2.63

3.5g Crystal Meth Ice Shards \$31.92

20 x 25mg C \$2.57

100 x Orange Star Very High MDMA content 180mg

100x 200mg White XTC 'Speakers'

3g Methylon Lab Grade

anonymous marketplace

Meth (1g) High-grade Crystal Meth

Seller: vortexmilkman(99)

Price: \$155.36

Ships from: United States of America
Ships to: Worldwide

Description:
-----Δ•This listing is for 1g of Crystal•Δ-----

As of NOV 14...got the crystal situation better than ever...got a guaranteed & consistent flow of the highest quality crystal available.

Why bother with newcomers to the SR Crystal scene with high prices and international customs hoopla.... Best price on SR, and operates with your safety in mind.

-----Δ•This listing is for 1g of Crystal•Δ-----

Tor + Bitcoin = End-to-end anonymity for commercial transactions

Ransomware

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: ~~XXXXXXXXXX~~

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC Cyborg CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-41 Panama 7, Panama.

Press ENTER to continue

1989 PC Cyborg

Your personal files are encrypted



Your files will be lost
without payment on:

11/24/2013 3:16:34 PM

See files

Info

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

<< Back

Proceed to payment >>

Not truly anonymous

- Recall Bitcoin is *pseudonymous*, i.e., traceable on per-identity basis
- E.g., suppose you're Satoshi Nakamoto and you want to spend your 1,624,500 BTC (\$1 billion) anonymously...
- Thus NSA conspiracy theory...

Table 2. The distribution of the accumulated incoming BTC's per owner

Larger or equal to	Smaller than	Number of owners
0	1	893,763
1	10	389,302
10	100	881,273
100	1,000	255,826
1,000	10,000	36,713
10,000	50,000	3,593
50,000	100,000	181
100,000	200,000	55
200,000	400,000	30
400,000	800,000	76
800,000		4

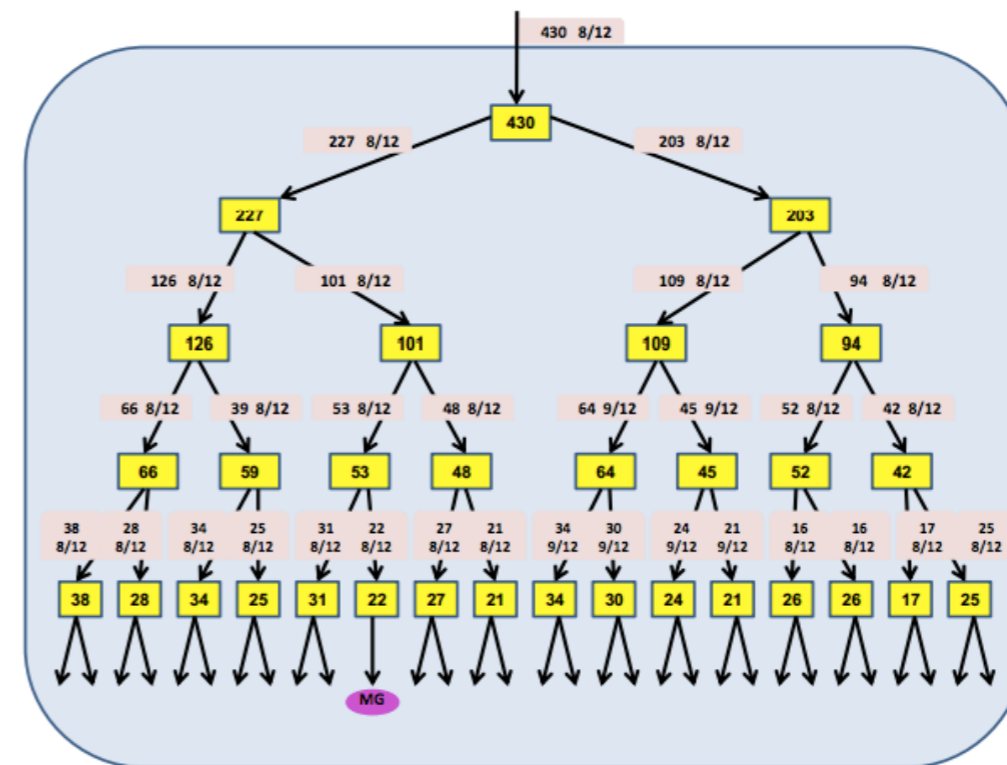


Fig. 10. A Sub graph of Fig. 1: The largest amount of transferred BTC's is finally distributed among many addresses via a binary tree-like structure.

But...

Greetings! New to Zcash?

The Zcash network is young, but evolving quickly! Sign up and we'll be in touch with more information about how you can get started with Zcash!

[Subscribe](#)



[ABOUT](#)

[TECH](#)

[BLOG](#)

[BUZZ](#)

[SUPPORT](#)

[FAQ](#)

[LANGUAGE](#)

Internet money

Bitcoin and most cryptocurrencies expose your entire payment history to the public. Zcash is the first open, permissionless cryptocurrency that can fully protect the privacy of transactions using zero-knowledge cryptography.

[GET STARTED](#)

[LEARN MORE](#)

New York one of the first states to regulate Bitcoin

DealB%k WITH FOUNDER ANDREW ROSS SORKIN

MERGERS & ACQUISITIONS | INVESTMENT BANKING | PRIVATE EQUITY | HEDGE FUNDS | I.P.O./OF

New York Proposes First State Regulations for Bitcoin

By SYDNEY EMBER JULY 17, 2014 3:01 PM 6 Comments



Bitcoin Regulation in New York

bitcoi
ACCEPTED HERE

CNBC EXCLUSIVE

REGULATING BITCOIN IN NEW YORK

WTI CRUDE(Aug)
+0.95 +0.94%
102.15

00:00 02:47

CNBC

Know-your-customer (KYC) at odds with pseudonymity / anonymity!

Long-term problems

- Scaling!
- Blocks are at most around 1MB in size
 - Transaction about 500B on average
 - Typically around 2000-2500 transactions per block
 - About 4 transactions / sec. throughput
- Should we:
 - Increase the block size or
 - Increase the mining rate or
 - Do something else?
- Big controversy!
- Solutions:
 - Segwit (partially) deployed in Bitcoin
 - Bitcoin Cash has 8MB blocks

Proof of stake



The probability of validating a new block is determined by how large of a stake a person hold.



The validators do not receive a block reward, instead they collect network fees as their reward.



Proof of stake systems can be much more cost and energy efficient than proof of work, but are less proven.

Proof of Work

vs

Proof of Stake



The first miner who solves the asymmetric puzzle is selected. Competition between miners to solve the puzzle.



Using deterministic selection process. Competition between miners to be selected.



Specialized equipment to optimize processing power.



Standard server grade unit is usually (more than) enough.



Initial investment to buy the hardware.



Initial investment to buy the stake and build the reputation.



High energy consumption



Standard energy consumption

Proof-of-Work (PoW)
“one-CPU-one-vote”



Proof-of-Stake (PoS)
“one-coin-one-vote”



Proof-of-Capacity (PoC)
“one-disk-one-vote”

