

Lecture 23 – Cryptocurrency

Stephen Checkoway
University of Illinois at Chicago
CS 487– Fall 2017
Slides from Miller's ECE 422

The Times 03/Jan/2009 Chancellor on
brink of second bailout for banks.



Bitcoin: A Peer-to-Peer Electronic Cash System

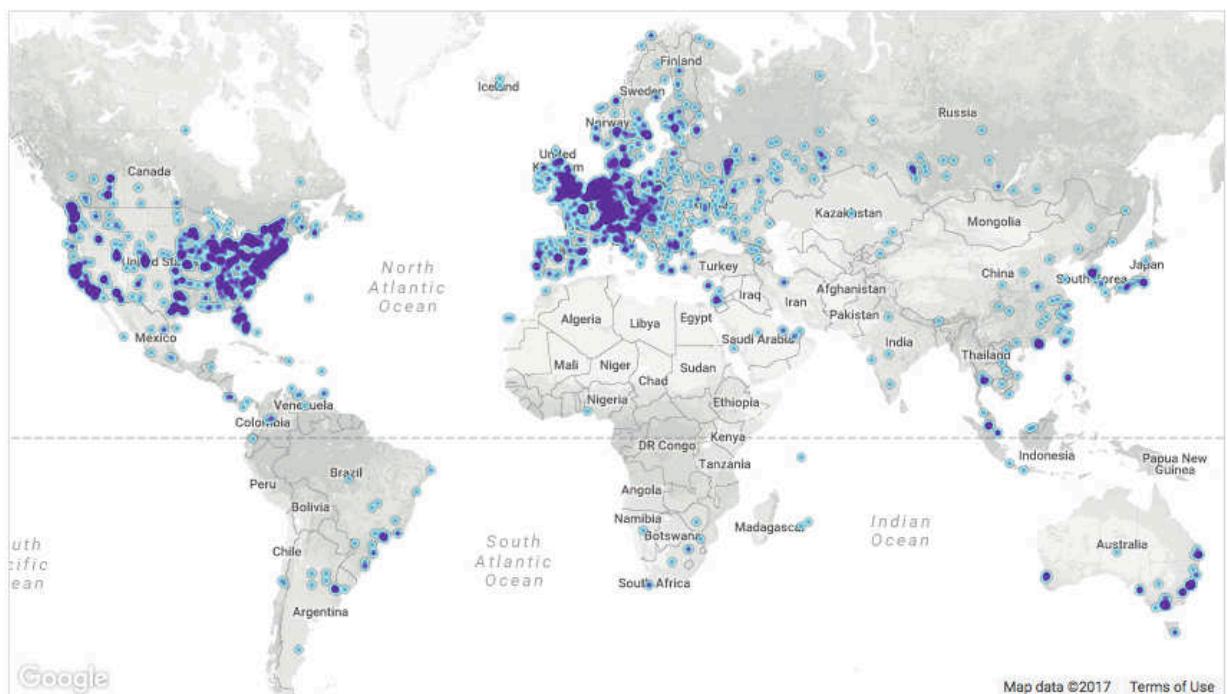
Satoshi Nakamoto
satoshi@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of

[bitcoin-0.1.0.rar](#)
[bitcoin-0.1.0.tgz](#)

≈11,000 reachable nodes (Nov, 2017)

RANK	COUNTRY	NODES
1	United States	3068 (27.83%)
2	Germany	1854 (16.82%)
3	France	767 (6.96%)
4	China	719 (6.52%)
5	Netherlands	531 (4.82%)
6	Canada	448 (4.06%)
7	United Kingdom	437 (3.96%)
8	n/a	378 (3.43%)
9	Russian Federation	354 (3.21%)
10	Singapore	220 (2.00%)



<https://bitnodes.earn.com/>

Market Capitalization

The total USD value of bitcoin supply in circulation, as calculated by the daily average market price across major exchanges.

Source: blockchain.info



source: blockchain.info

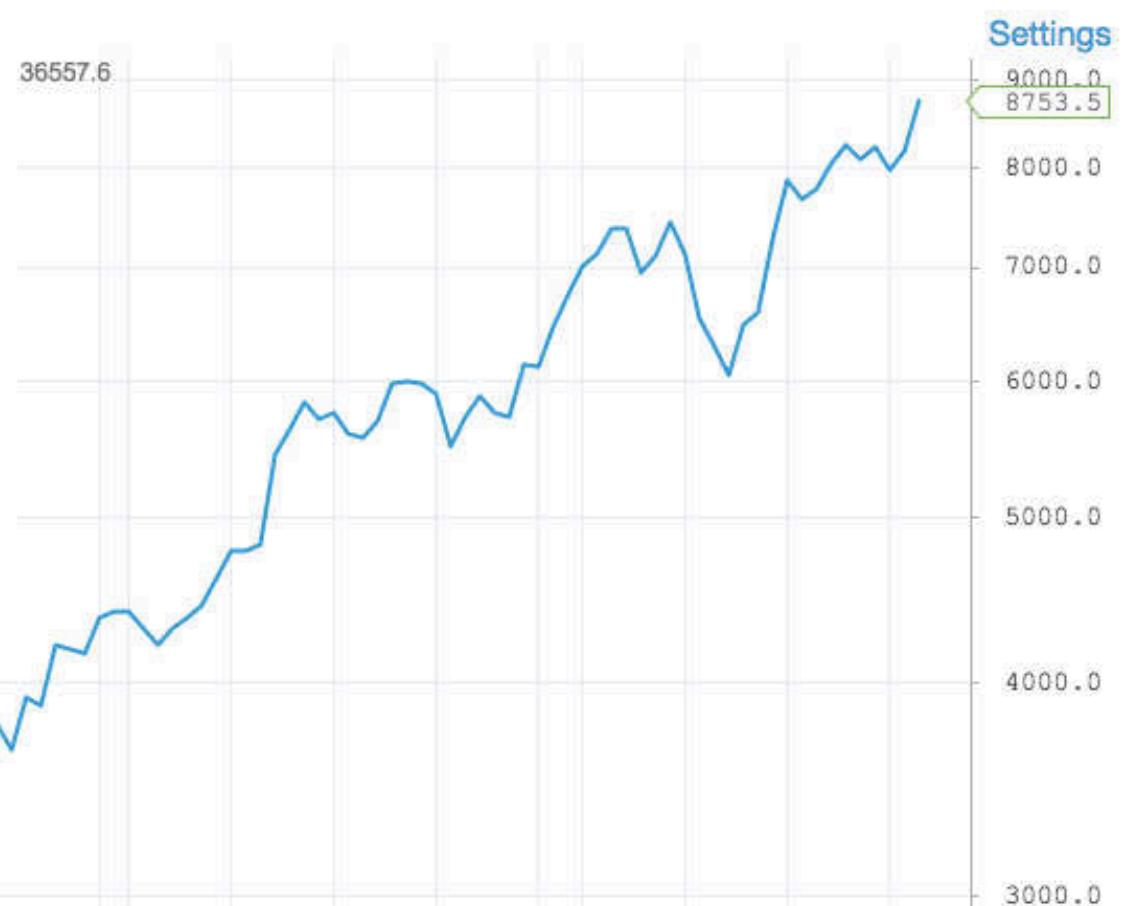
\$9,464.40

▲ 9.60%
Bitfinex

Currency USD—United States dollar

Bitfinex 9464.40 ▲ 9.60%

Bitstamp 9352.00 ▲ 8.64%



Bitcoin Market Cap

\$156.6B

24-hour Transaction Volume

\$2.1B

Bitcoin Money Supply

16.70M

7/22 Sep 9/8 9/15 9/22 Oct 10/8 10/15 10/22 Nov 11/8 11/15 11/22

Settings

9000.0

8753.5

8000.0

7000.0

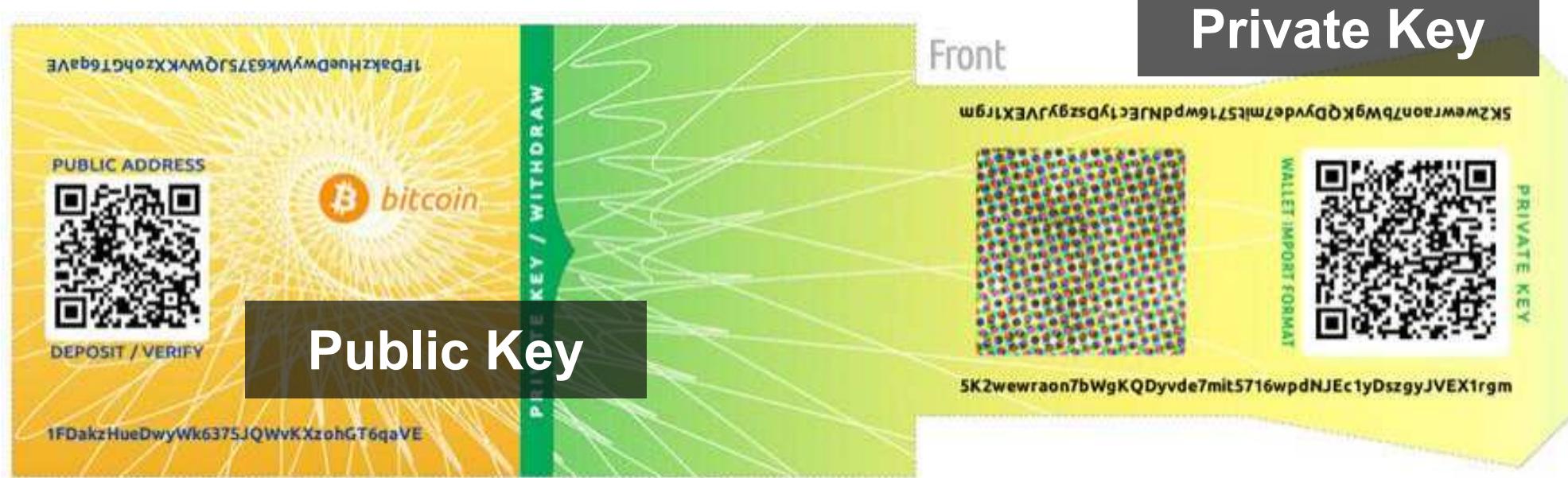
6000.0

5000.0

4000.0

3000.0

Bitcoin Paper Wallet



Front

Private Key

SK2weewraon7bWgKQDyvde7mit5716wpdNJEc1yDszyJVEX1rgm



WALLET IMPORT FORMAT



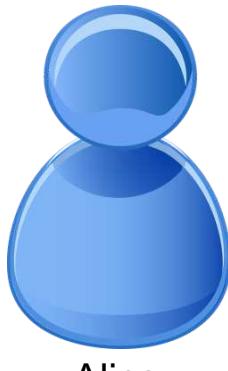
PRIVATE KEY

SK2weewraon7bWgKQDyvde7mit5716wpdNJEc1yDszyJVEX1rgm

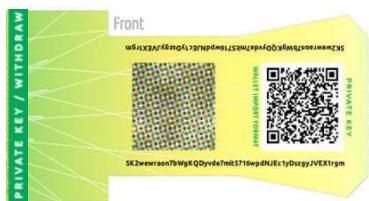


Public Key

Transfer 10 Bitcoins from me to Bob.

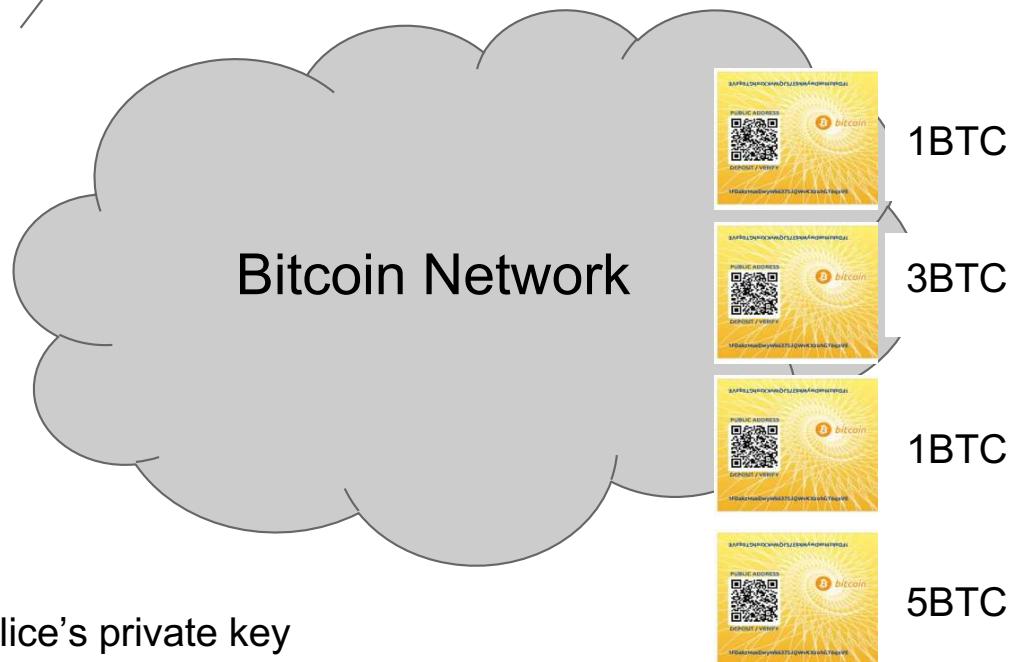


Alice



Signed with Alice's private key

Alice and Bob are only identified by public keys



LATEST BLOCKS

Height	Age	Transactions	Total Sent
496234	16 minutes	2356	5,709.20 BTC
496233	19 minutes	2750	6,188.44 BTC
496232	21 minutes	2119	4,374.67 BTC
496231	23 minutes	2532	6,900.23 BTC



HI MOM SEND



DAD
OK

MYC
GARDEN
IT





ATMs



Bitcoin is the first and largest of *hundreds* of cryptocurrencies

▲ #	Name	Market Cap	Price
1	฿ Bitcoin	\$158,904,206,299	\$9513.62
2	♦ Ethereum	\$43,854,960,273	\$456.96
3	฿ Bitcoin Cash	\$26,961,401,198	\$1602.60
4	Ripple	\$9,675,917,364	\$0.250523
5	฿ Bitcoin Gold	\$5,675,398,231	\$340.39
6	Dash	\$4,801,721,337	\$622.62
7	Litecoin	\$4,616,401,352	\$85.48
8	Monero	\$2,513,605,641	\$163.19
9	NEO	\$2,512,646,500	\$38.66
10	IOTA	\$2,222,893,210	\$0.799737
11	♦ Ethereum Classic	\$2,168,465,125	\$22.17
12	NEM	\$1,954,071,000	\$0.217119
13	EOS	\$1,310,607,703	\$2.62
14	Qtum	\$1,106,200,781	\$15.01
15	Cardano	\$1,027,194,237	\$0.039619
16	Zcash	\$921,864,283	\$340.71

Bitcoin exchanges

coinbase

- Dashboard
- Buy/Sell
- Send/Request
- Accounts
- Tools
- Settings

Price Charts

\$1,191.11
↑ \$220.38 (21.62%)

\$1,293



kraken

ETH: €1.81889 XBT: \$0.01365

ACCOUNT CHARTS HELP

LAST	HIGH	LOW	24 HOUR VOLU
\$0.015056	\$0.015600	\$0.014880	98,921.88

Trade Funding Security Settings History Get Verified MtGox Claim

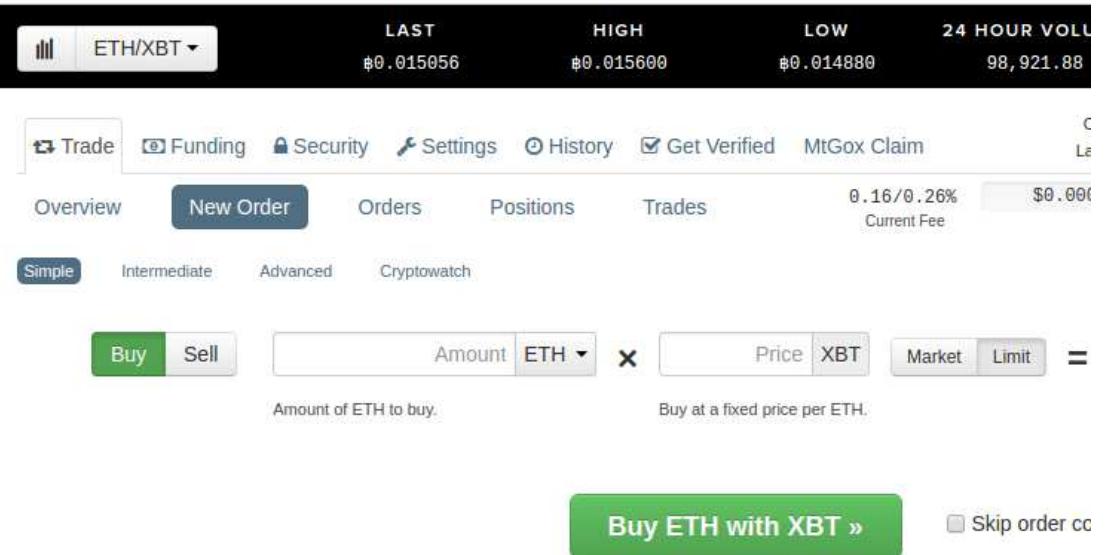
Overview New Order Orders Positions Trades 0.16/0.26% Current Fee \$0.00

Simple Intermediate Advanced Cryptowatch

Buy Sell Amount ETH ▾ Price XBT Market Limit

Amount of ETH to buy. Buy at a fixed price per ETH.

Buy ETH with XBT » Skip order confirmation



Beware the middleman: Empirical analysis of Bitcoin-exchange risk
Tyler Moore and Nicolas Christin, Financial Crypto 2013

Exchanges

Overview		Currencies		All Markets												
All	KRW	NMC	IDR	RON	ARS	AUD	BGN	BRL	BTC	CAD	CHF	CLP	CNY			
GBP	HKD	HUF	ILS	INR	JPY	LTC	MXN	NOK	NZD	PEN	PLN	RUB	SAR			
UAH	USD	XRP	ZAR													
				Symbol	Latest Price	30 days	Average		Volume	Low/Hight						
▼	coincheck			JPY	138498 just now		132166.30 6331.70 4.78%		383,317.61 50,561,671,049.88 JPY	98450 150300						
▼	OKCoin			CNY	7739.01 0 min ago		7402.24 336.77 4.55%		333,845.99 2,471,207,739.32 CNY	6300 8454.76						
▼	BTC China			CNY	7728.08 0 min ago		7361.13 366.95 4.99%		264,485.69 1,946,914,658.39 CNY	6434.9 8400.11						
▼	Kraken			EUR	1133.986 0 min ago		1054.65 79.34 7.52%		246,392.24 259,856,705.96 EUR	847.999 1225						
▼	BitStamp			USD	1200 0 min ago		1114.20 85.80 7.70%		223,675.31 249,218,776.14 USD	913.73 1298						
▼	btc-e			USD	1251 2 days, 6 hrs ago		1078.71 172.29 15.97%		165,215.69 178,219,756.55 USD	914 1269.999						
▼	itBit			USD	1192.72 1 min ago		1118.19 74.53 6.67%		95,202.12 106,453,658.42 USD	943.53 1293.55						
▼	Kraken			USD	1190 0 min ago		1117.04 72.96 6.53%		66,201.09 73,948,990.16 USD	940.006 1288						
▼	BitBay			PLN	5050 2 min ago		4537.18 512.82 11.38%		32,008.43 145,227,931.72 PLN	3849 5394.6						
▲	LocalBitcoins			USD	1632.65 3 min ago		1241.21 391.44 31.54%		27,629.53 34,293,925.71 USD	125.94 15625						
▼	bitcoin.co.id				16050700 1 min ago		14587600.26 14587600.26 0.00%		22,646.11 22,646.11 USD	12262200 12262200						

What are the security goals?

- Transactions are “valid”.

Alice can't spend more money than she has

- Transactions are “authorized”

Alice can't spend Bob's money

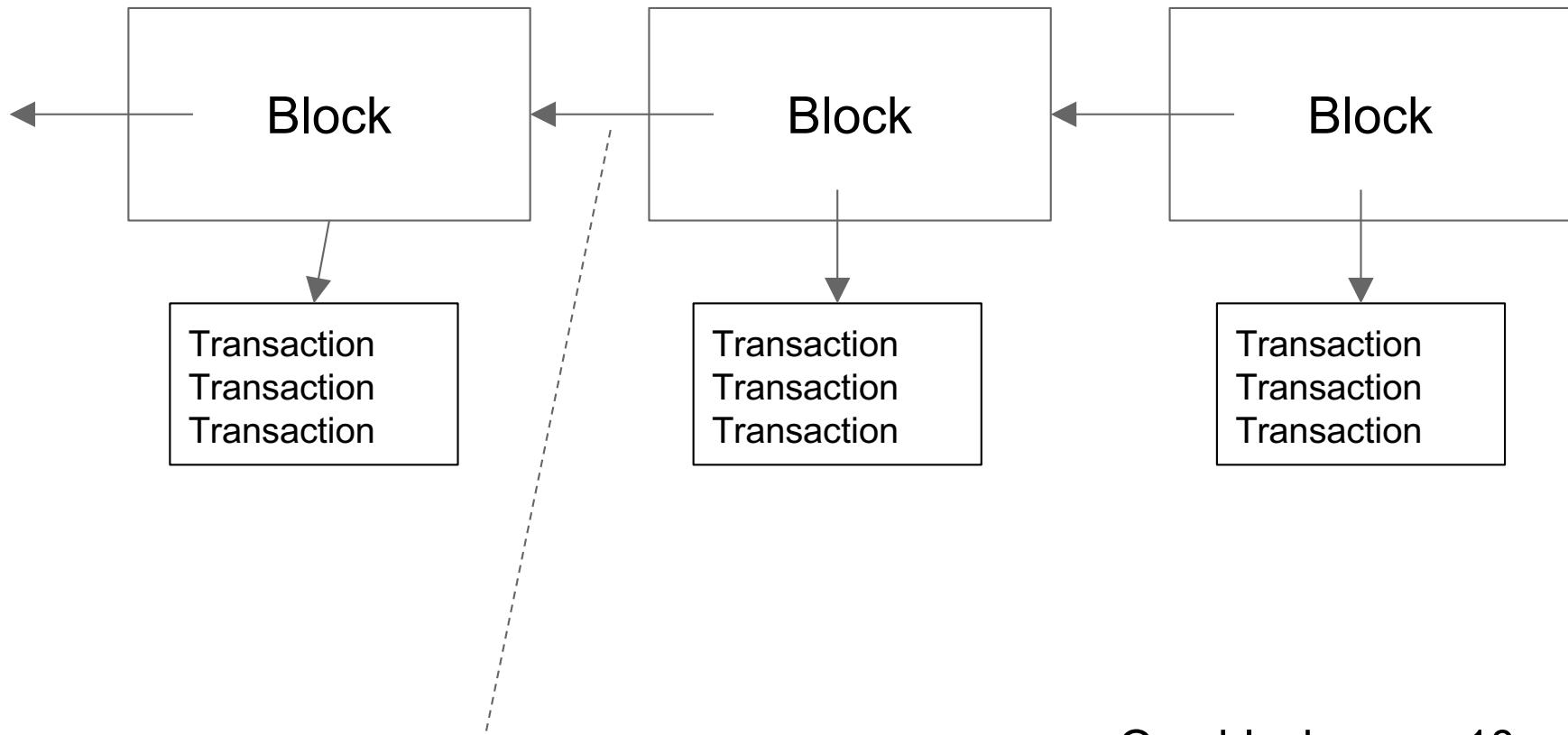
- The service is “available”

Alice can't prevent Bob from spending his own money

- Transactions are consistent, permanent

Alice can't send Bob money, and then take it back!

Blockchain Data Structure



Each “arrow” is actually a SHA2 *hash*

One block every 10 minutes

The hash of the most recent “block” is a hash of ALL of the transactions

An account-based ledger (*not* Bitcoin)

time

Create 25 coins and credit to Alice_{ASSERTED BY MINERS}

Transfer 17 coins from Alice to Bob_{SIGNED(Alice)}

Transfer 8 coins from Bob to Carol_{SIGNED(Bob)}

Transfer 5 coins from Carol to Alice_{SIGNED(Carol)}

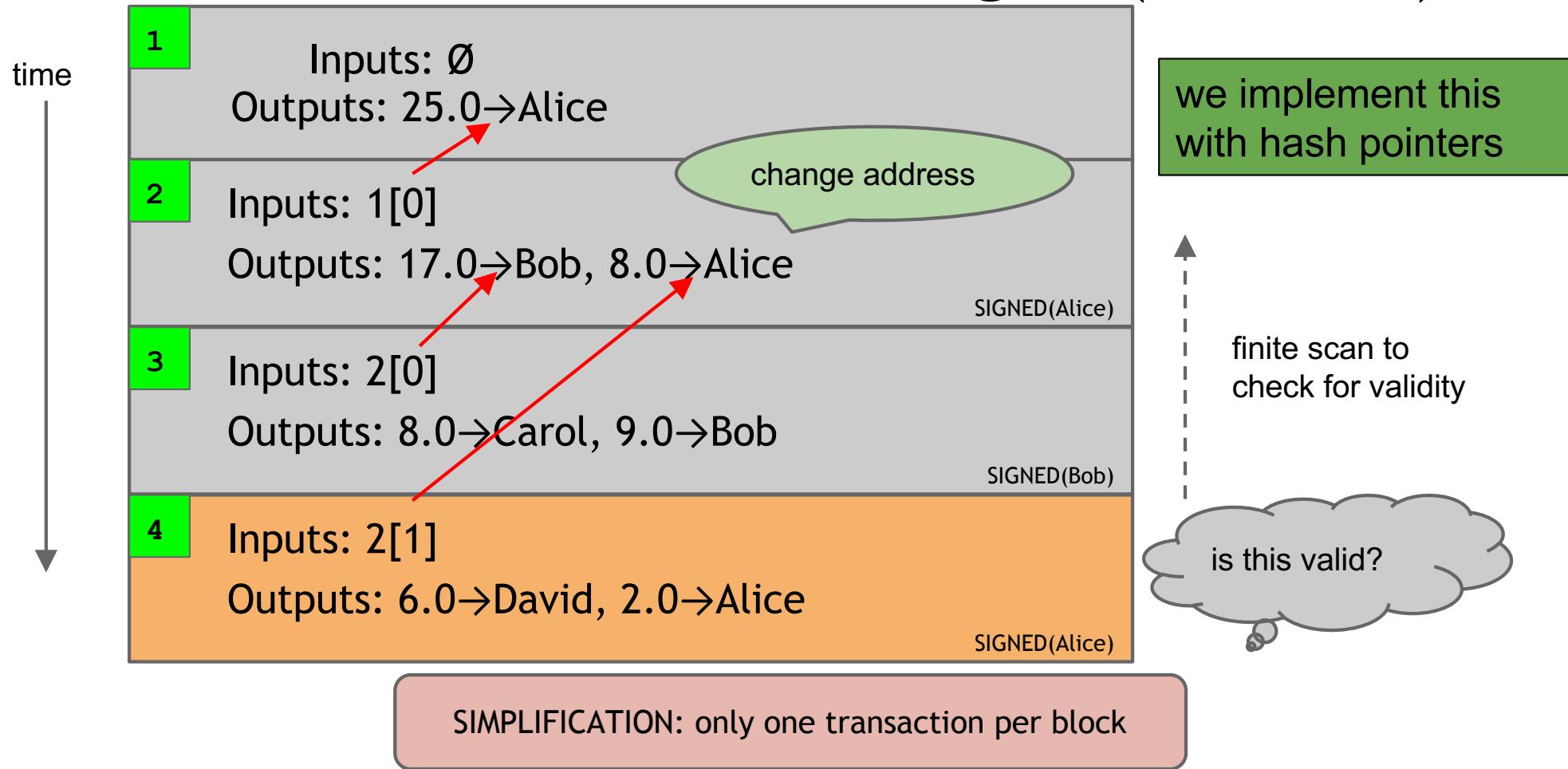
Transfer 15 coins from Alice to David_{SIGNED(Alice)} .. .

might need to
scan backwards
until genesis!

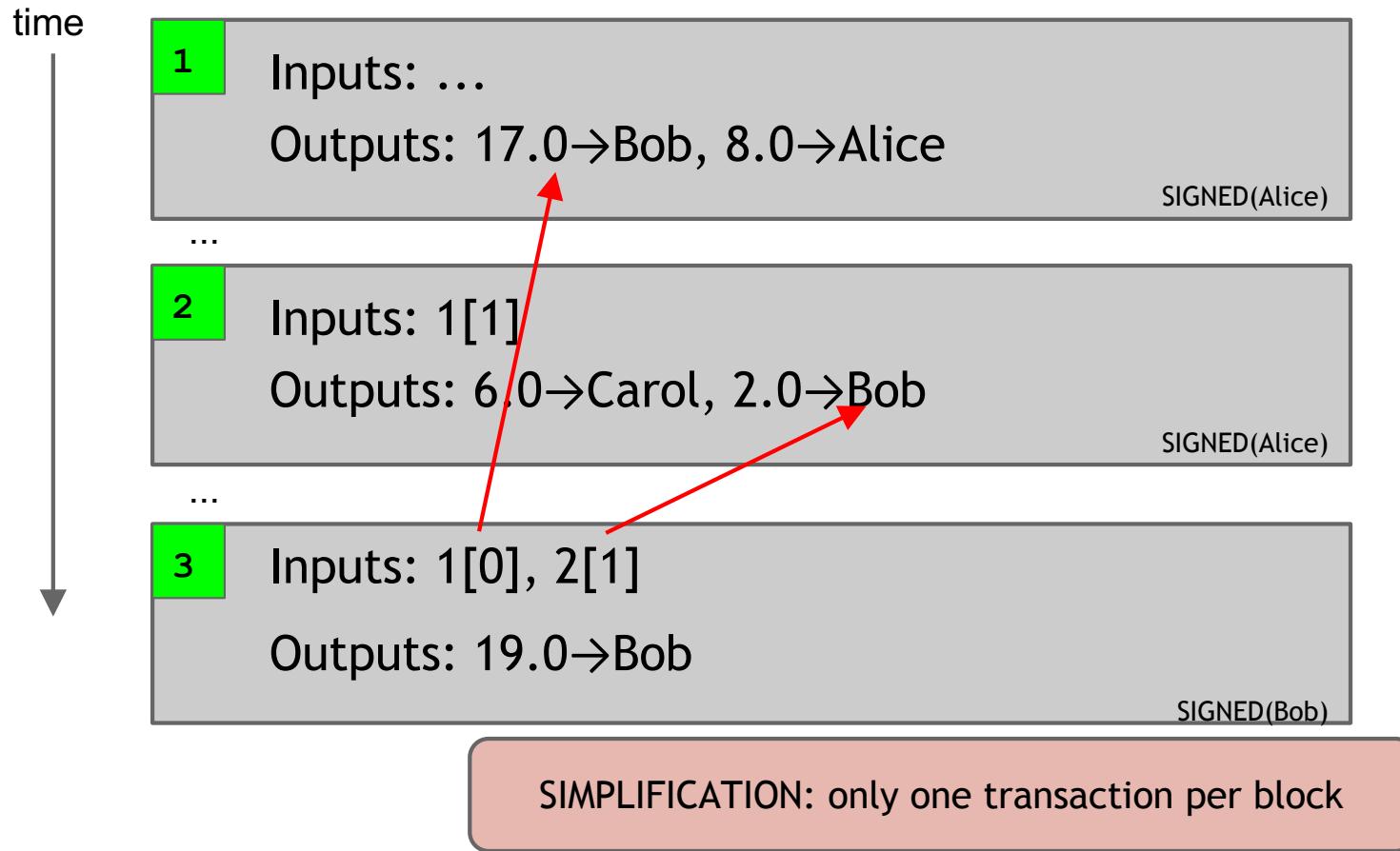
is this valid?

SIMPLIFICATION: only one transaction per block

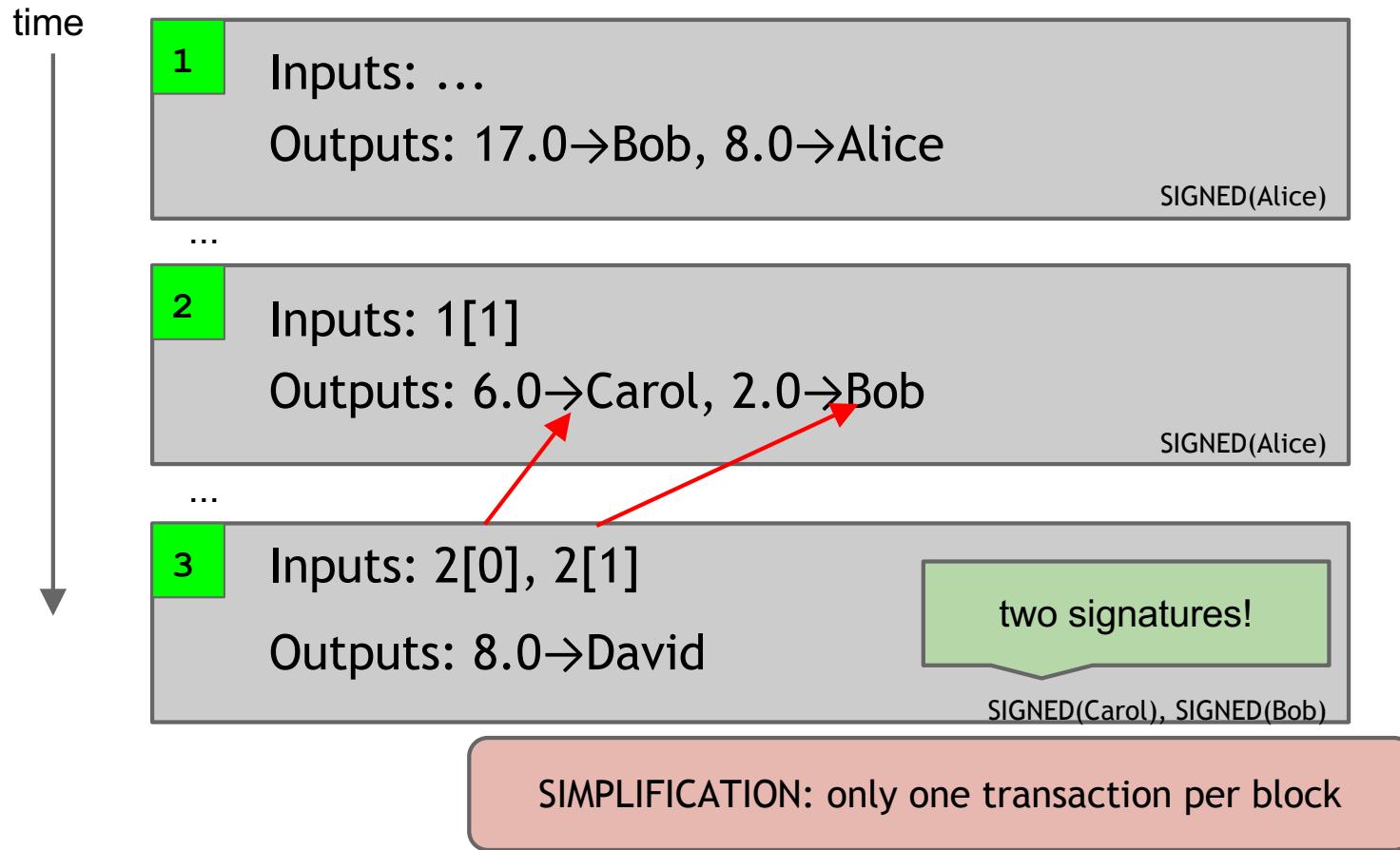
A transaction-based ledger (Bitcoin)



Merging value



Joint payments



The real deal: a Bitcoin transaction

```
{  
  "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",  
  "ver":1,  
  "vin_sz":2,  
  "vout_sz":1,  
  "lock_time":0,  
  "size":404,  
  "in": [  
    {  
      "prev_out": {  
        "hash": "3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",  
        "n": 0  
      },  
      "scriptSig": "30440..."  
    },  
    {  
      "prev_out": {  
        "hash": "7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",  
        "n": 0  
      },  
      "scriptSig": "3f3a4ce81...."  
    }  
  ],  
  "out": [  
    {  
      "value": "10.12287097",  
      "scriptPubKey": "OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"  
    }  
  ]  
}
```

1. metadata

2. input(s)

3. output(s)

The real deal: 1. transaction metadata

```
{  
  transaction hash   { "hash": "5a42590...b8b6b",  
                      "ver": 1,  
  housekeeping       { "vin_sz": 2,  
                      "vout_sz": 1,  
  "not valid before" { "lock_time": 0,  
                      "size": 404,  
  housekeeping       { ...  
                        }  
  }
```

The real deal: 2. transaction inputs

```
"in": [  
  {  
    "prev_out": {  
      "hash": "3be4...80260",  
      "n": 0  
    },  
    "scriptSig": "30440....3f3a4ce81"  
  },  
  ...  
]
```

previous transaction {

signature {

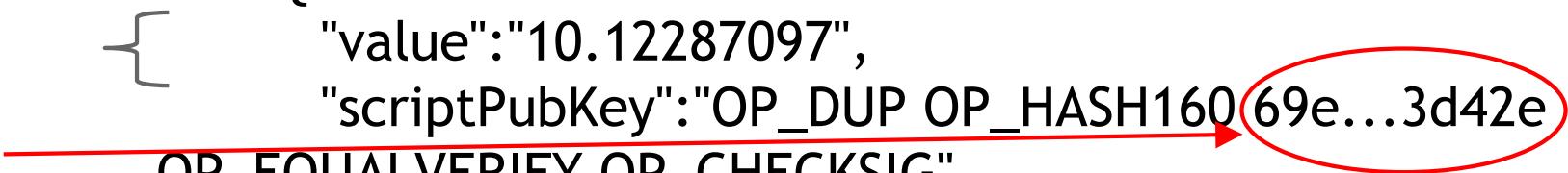
(more inputs) {

The real deal: 3. transaction outputs

```
"out": [  
    {  
        "value": "10.12287097",  
        "scriptPubKey": "OP_DUP OP_HASH160 69e...3d42e  
        OP_EQUALVERIFY OP_CHECKSIG"  
    },  
    ...  
]
```

output value
recipient address??
(more outputs)

“Addresses” are actually programs



Bitcoin Mining

How do we commit new transactions?

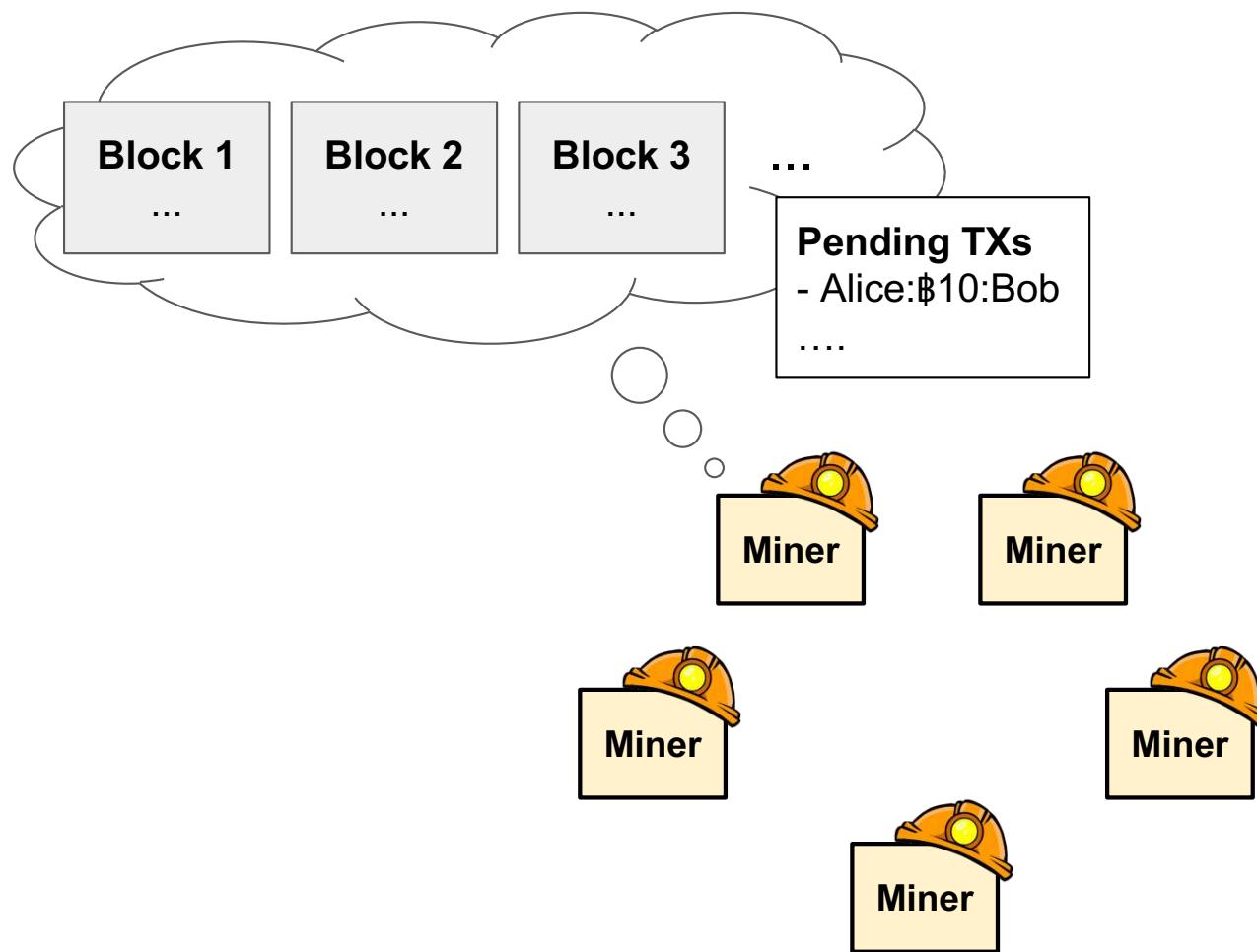
Why not have 1 trusted “transaction authority”?

What happens if it’s compromised?

Why not sample/count based on IP addresses?

Mining Bitcoins in 6 easy steps

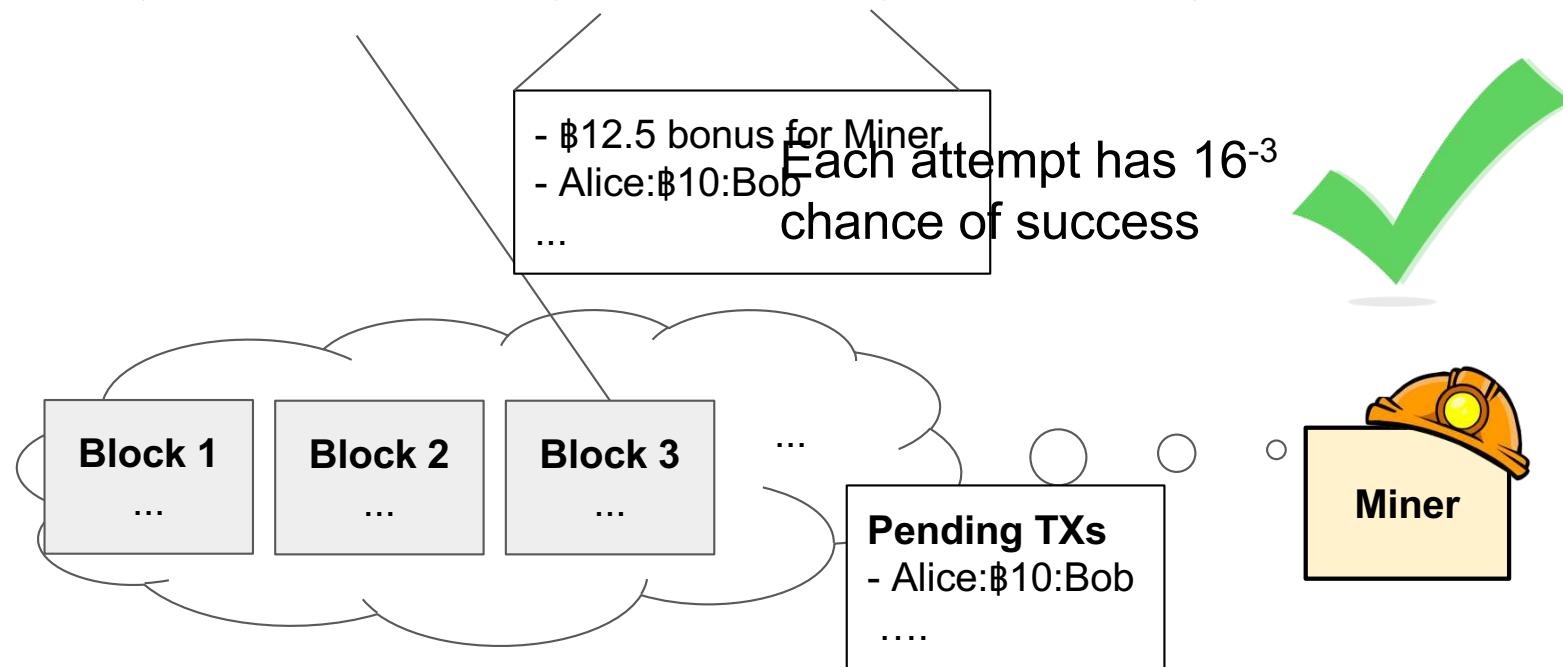
1. Join the network, listen for transactions
 - a. Validate all proposed transactions
2. Listen for new blocks, maintain block chain
 - a. When a new block is proposed, validate it
3. Assemble a new valid block
4. Find the nonce to make your block valid
5. Hope everybody accepts your new block
6. Profit!

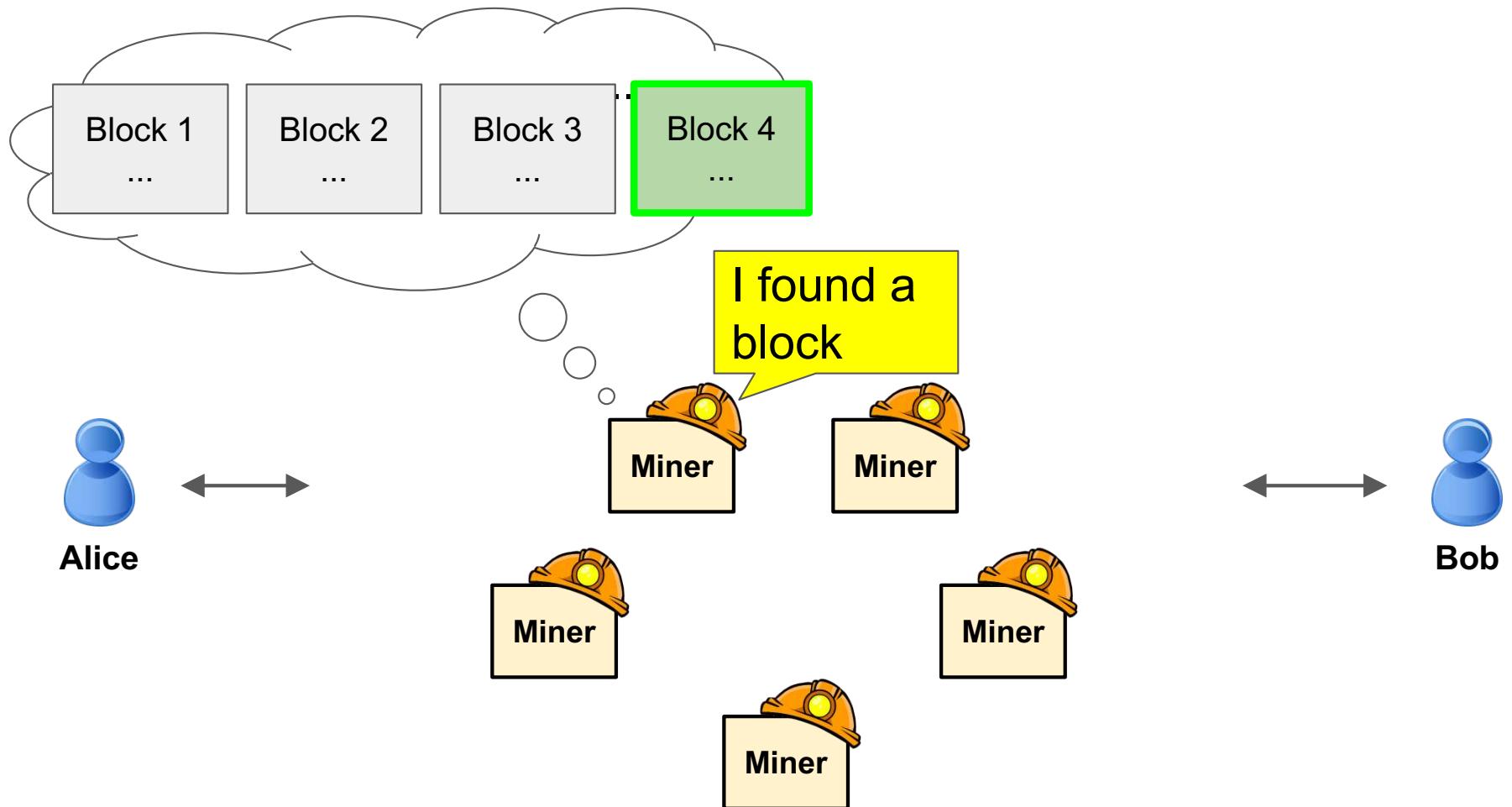


Miners commit new transactions
by solving puzzles

= 0x000***...

Hash(Block 3 | newTXs | 0xb9824) = 0x000c3f...

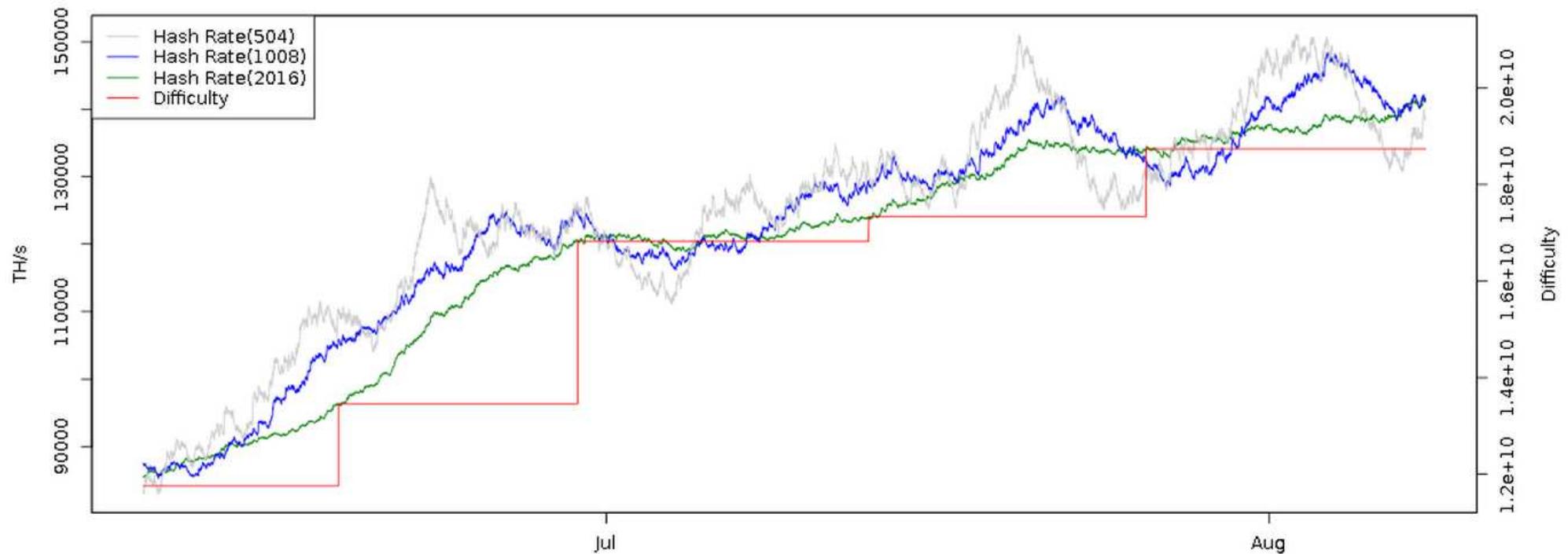




Mining difficulty adjusts over time

One block
every 10 min

Bitcoin Hash Rate vs Difficulty (2 Months)



Evolution of mining



CPU



GPU



FPGA



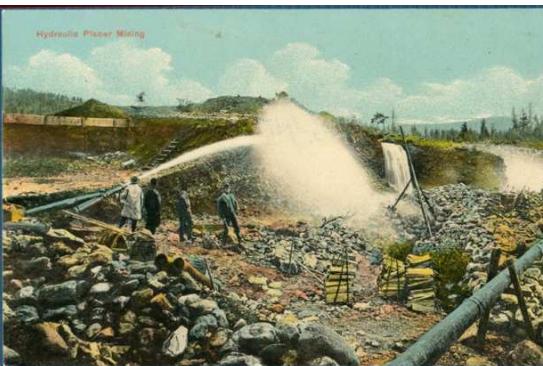
ASIC



gold pan



sluice box

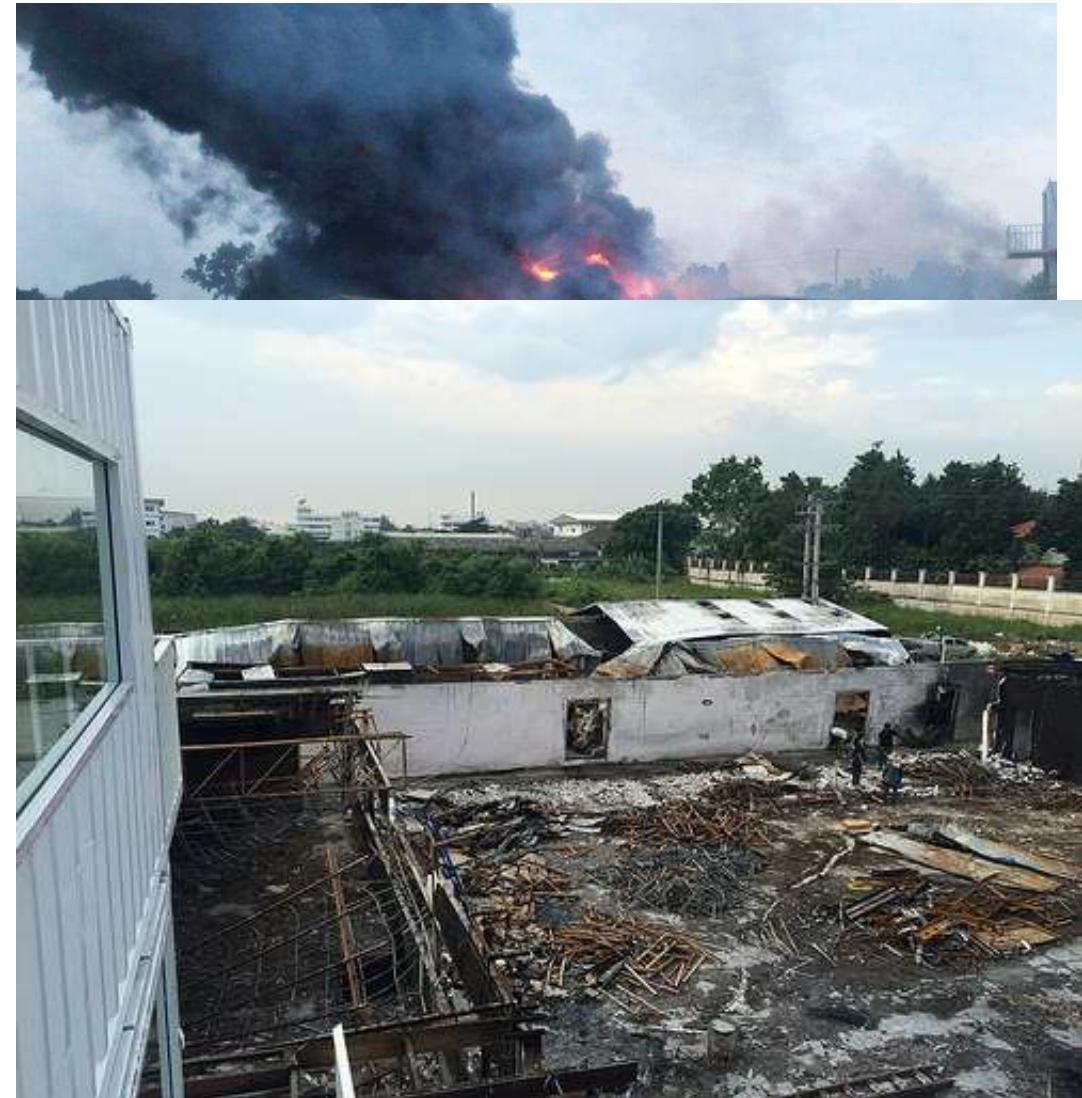


placer mining



pit mining





Mining difficulty “target” (2016-04-24)

256 bit hash output

64+ leading zeroes required

Current difficulty = 2^{68}

What happens if 2 blocks found at the same time?

Miners use longest chain

Two valid blocks produced

495171

Timestamp	2017-11-20 03:21:15	Timestamp	2017-11-20 03:21:35
Number Of Transactions	2281	Number Of Transactions	2228
Relayed By	BTC.com	Relayed By	BTC.TOP

Orphan block

Block on the chain

495170

Timestamp	2017-11-20 03:08:10
Number Of Transactions	2294
Relayed By	ViaBTC

More generally: “programmable money”

The screenshot shows the Etherscan interface. At the top, there is a navigation bar with links for HOME, BLOCKCHAIN, ACCOUNT (which is underlined), and TOOLS. There are also LOGIN and SEARCH buttons. The main content area is titled "Contract Accounts". A message indicates that over 999,999 contracts were found, with approximately 12,658,485.768 Ether in total. It notes that only the last 10,000 records are being displayed. Below this, a table lists the top four Ethereum addresses by balance:

Rank	Address	Balance
1	0xab7c74abc0c4d48d1bdad5dc...83e	1,500,000.00134197094280789 Ether
2	0xde0b295669a9fd93d5f28d9ec85e40f4cb697bae (EthDev)	737,021.593340895468356351 Ether
3	0x61edcdf5bb737adffe5043706e7c5bb1f1a56eea	580,000 Ether
4	0xf1ce0a98efbfa3f8ebec2399847b7d88294a634e	550,000.02 Ether

Smart Contract Example (very high level)

If GOOG rises to \$1,000 by
30 June 2015, assign 10
shares from Alice to Bob and
pay Alice \$10,000

Smart contracts

- Smart contracts run in a virtual machine (EVM)
- Turing-complete programming language
- Each operation is executed by every node
- Operations
 - Read or write data
 - Cryptographic primitives
 - Send messages to other contracts
- Each operation costs “gas”

Smart contract problems

- Smart contracts often have exploitable vulnerabilities too
- The DAO (decentralized autonomous organization) was a type of venture capital fund run as a smart contract
- A bug was exploited leading to theft of ~\$60M
 - Clawed back by a “hard fork” that cancelled the transaction

Hard fork

- Cryptocurrency splits into two different chains
- Longest chain is supposed to be authoritative but now there are two
- After DAO attack, Ethereum split into Ethereum (ETH) and Ethereum Classic (ETC)
- What are the consequences of splitting the blockchain?

Bitcoin is used for Crime



Ransomware

Bitcoin may be an important tool for freedom/privacy

- A global currency that is not easily bound by borders
- Resilient architecture, seems difficult to shut down
- A competitive force leading banks to “blockchain” movement
- Disintermediation - removing “middlemen”

Global energy usage of Bitcoin mining alone

Average yearly energy consumption of Bitcoin in 2017: 29 TWh

That's 0.13% of total, global energy consumption

For comparison, Ireland consumes 25 TWh

Morocco consumes 29 TWh

<https://powercompare.co.uk/bitcoin/>





Global energy usage of Bitcoin mining alone

Average yearly energy consumption of Bitcoin in 2017: 29 TWh

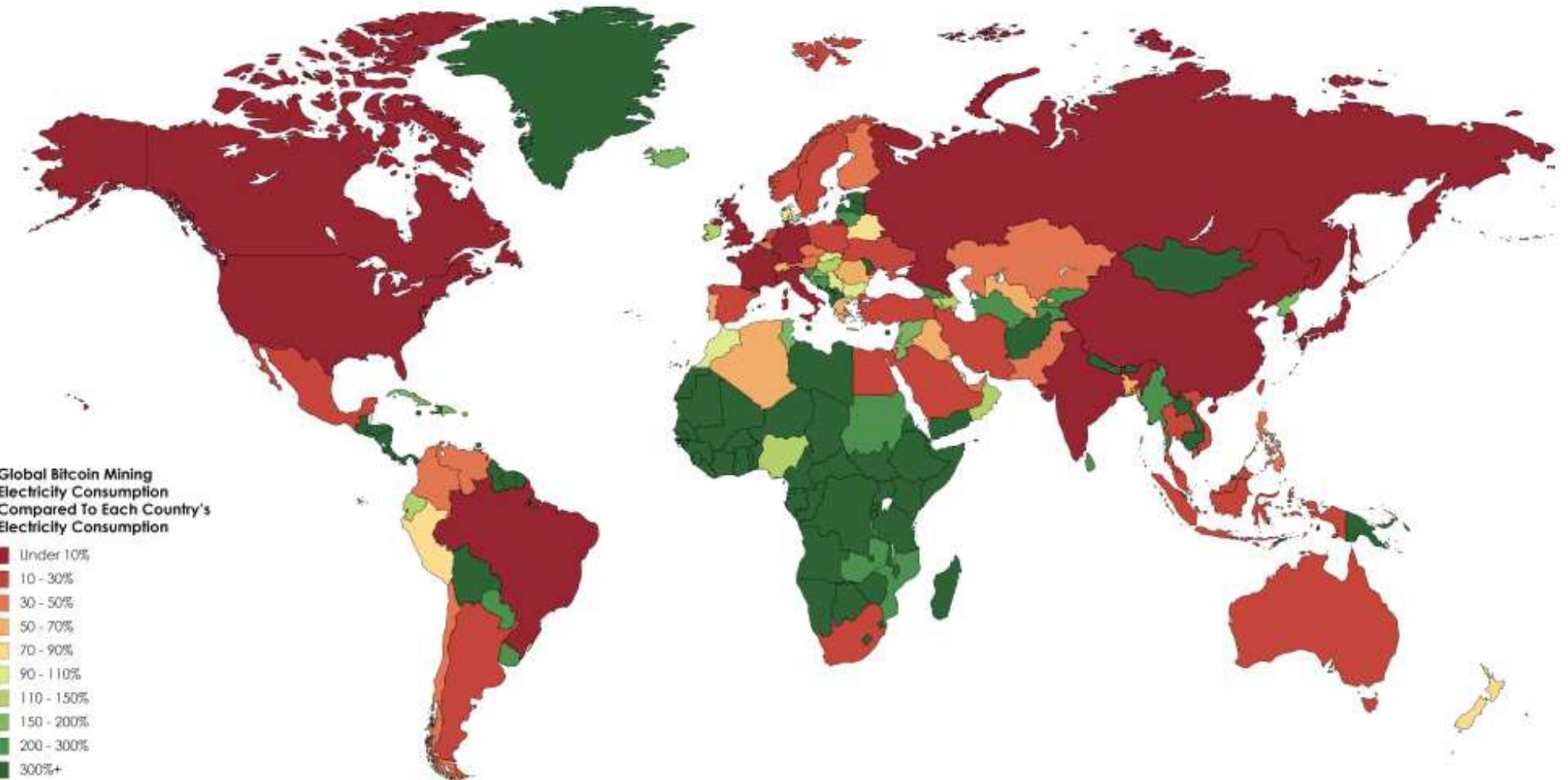
That's 0.13% of total, global energy consumption

For comparison, Ireland consumes 25 TWh, Morocco consumes 29 TWh

159 countries consume less energy than Bitcoin mining

Other cryptocurrencies consume less energy, globally, but still a significant amount

<https://powercompare.co.uk/bitcoin/>



Source: <https://powercompare.co.uk/bitcoin>

Brain Wallets

- Derive a private key from a password

$$\text{secretkey} = \mathbf{hash}(\text{salt}, \text{password})$$

- Hash function should be:
 - “Random Oracle” (PRF does not apply, collision resistance not enough)
 - Slow-ish to compute (require space not just *cpu*, no amortization)
- Also used for encrypting files on a hard drive
- If you send a bitcoin transaction to a “low entropy” brain wallet address it will be taken within seconds

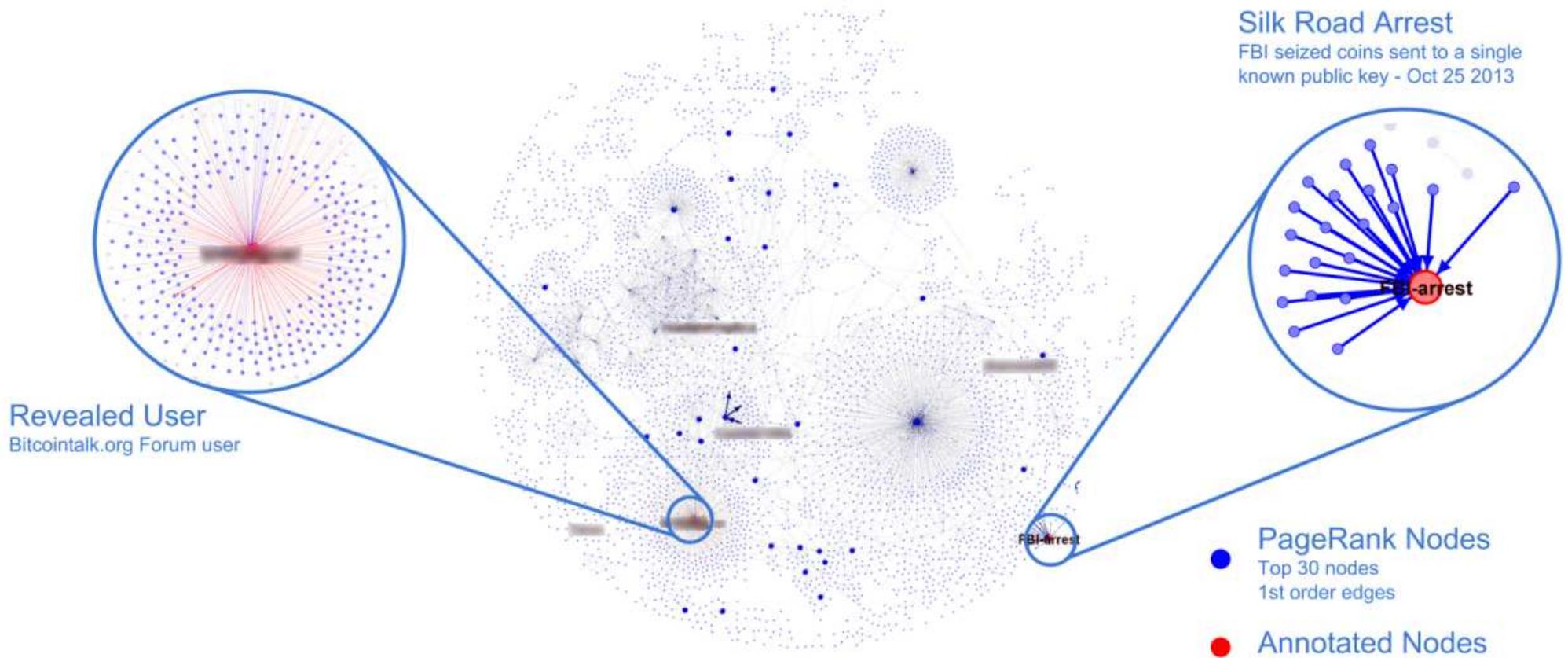
Bitcoin is not completely private

- Pseudonymous, not “anonymous”
- Transaction graph analysis, clustering

Can be traced to exchanges

- Mixers..... they mix your coins, but might take them.
- Cryptography can avoid this!

Coinshuffle, Tumblebit, Zcash, and more...



<https://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf>