ECE 422
Bitcoin and cryptocurrency

April 11, 2018

Prof. Andrew Miller (ECE)

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

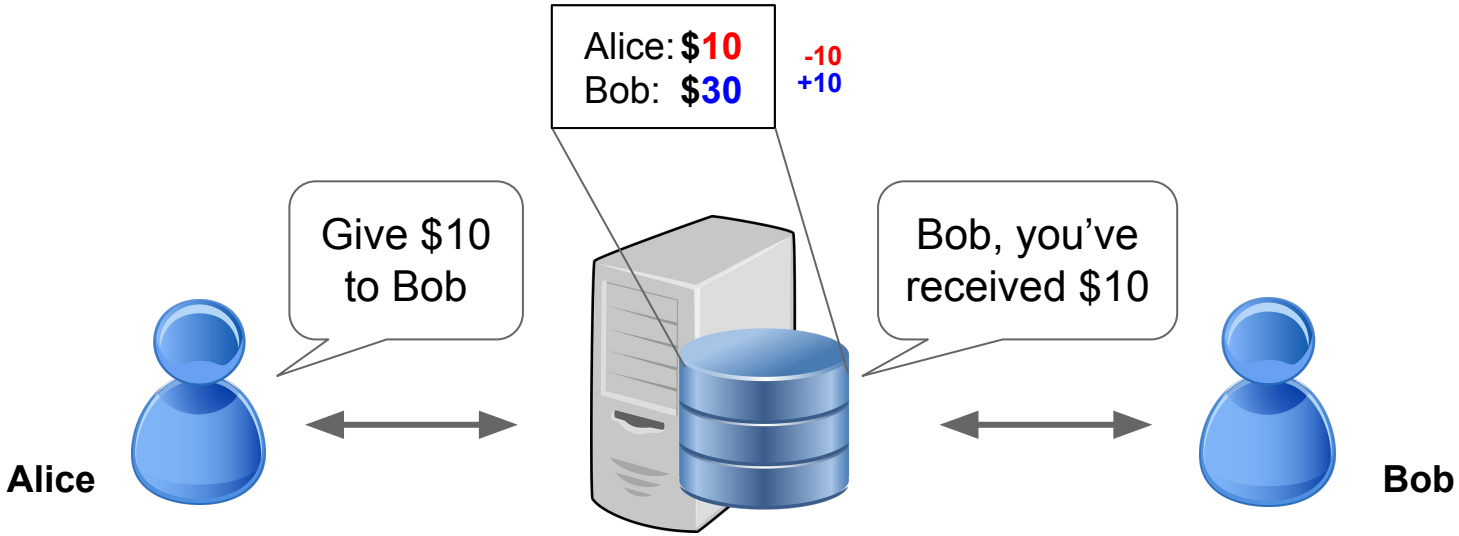
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@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
```

Virtual currencies are implemented on top of a ***shared database***



Desired security properties:

- Consistency
- Availability
- Application-defined access controls (for writes/updates)
- Privacy

~10,000 reachable nodes

http://bitnodes.earn.com/

GLOBAL BITCOIN NODES DISTRIBUTION

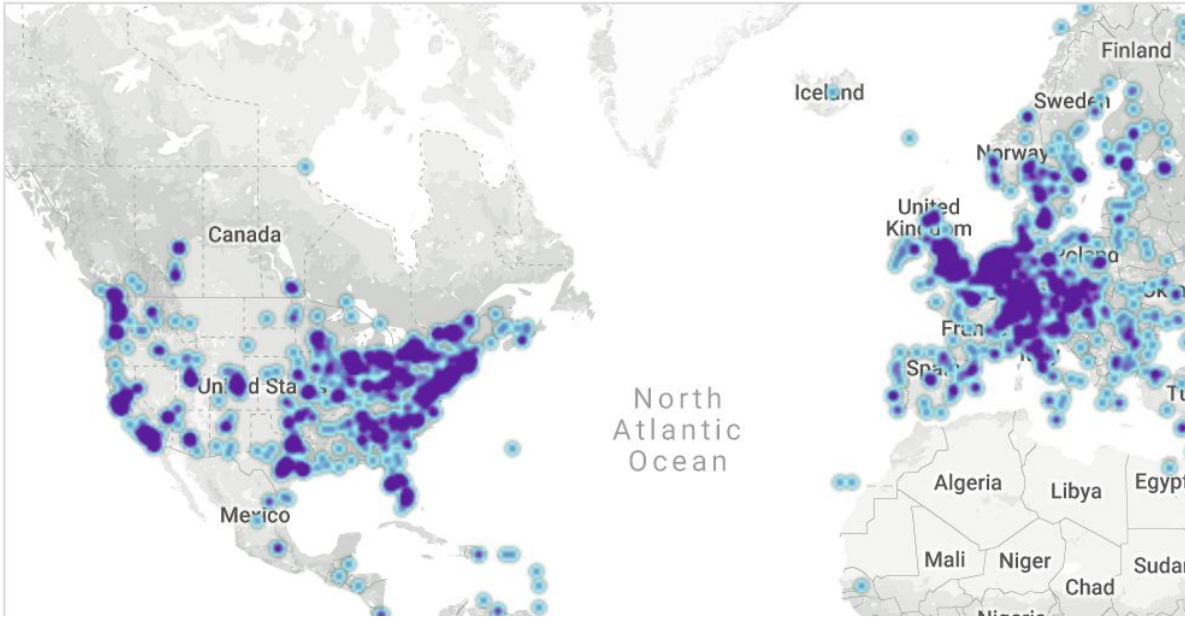
Reachable nodes as of Mon Mar 12 2018 22:56:53 GMT-0500 (Central Daylight Time).

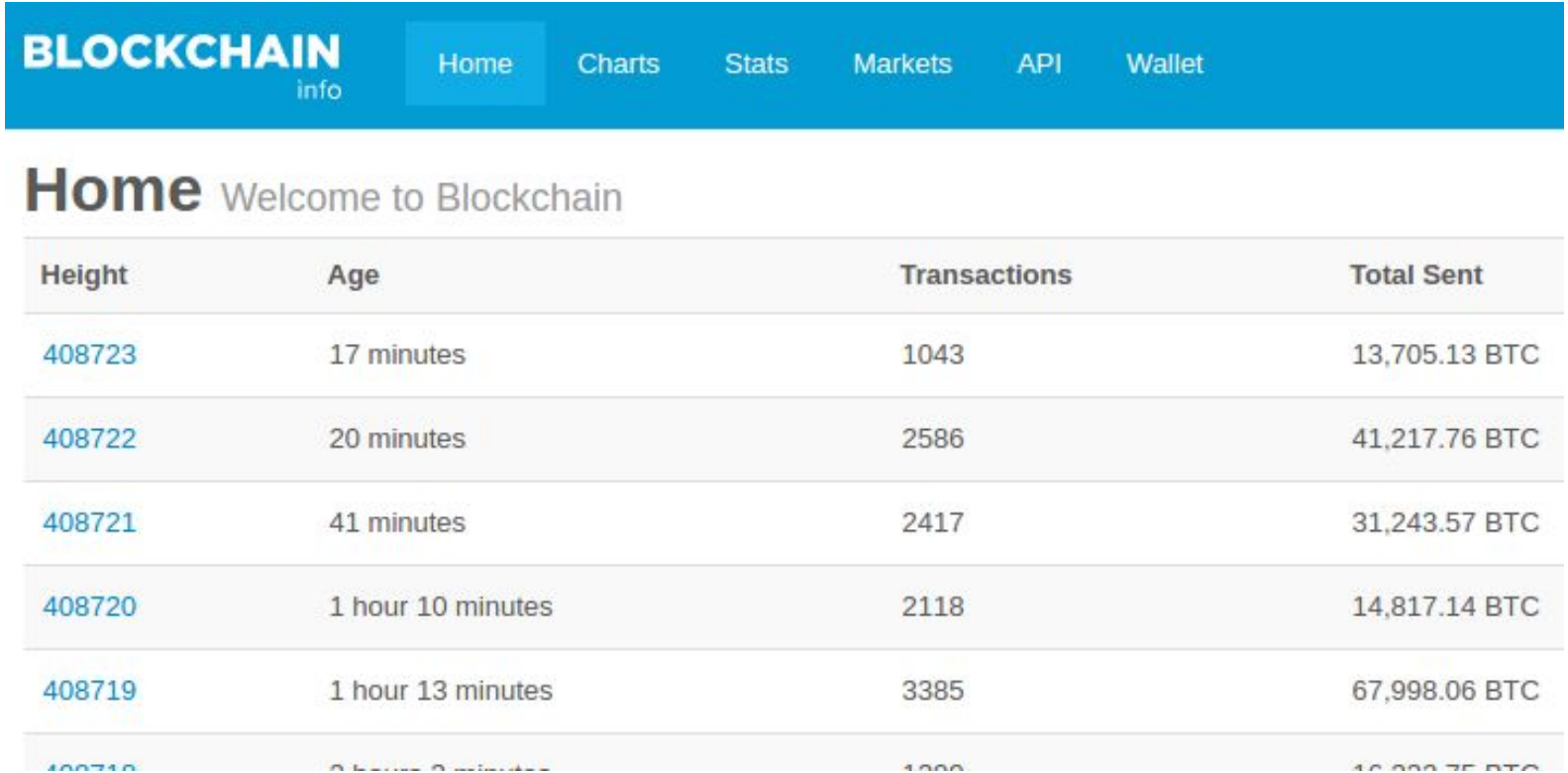
12207 NODES

24-hour charts »

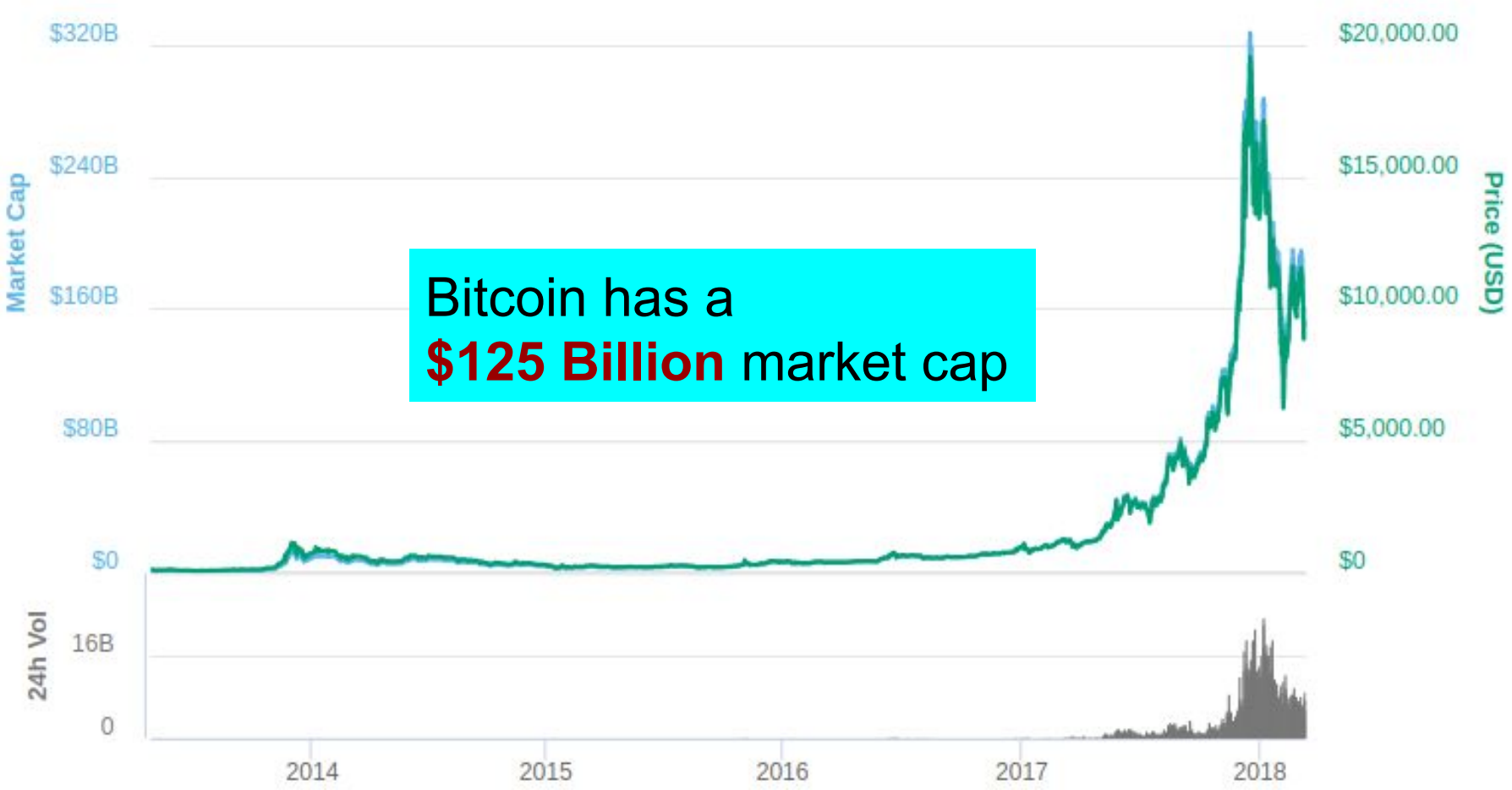
Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2786 (22.82%)
2	China	2245 (18.39%)
3	Germany	1962 (16.07%)





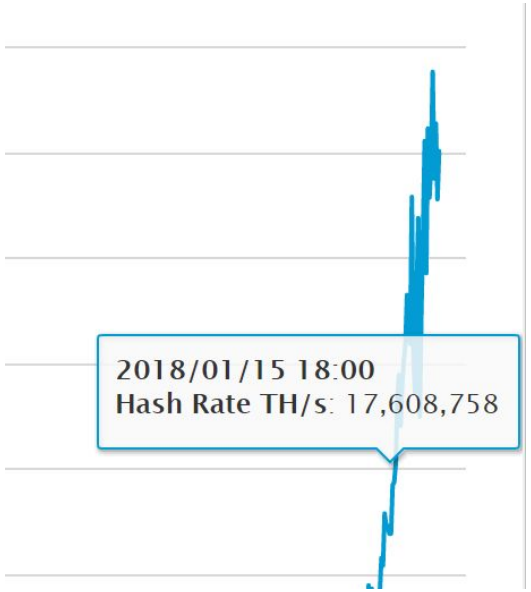
https://etherscan.io/ https://blockchain.info/



Source: coinmarketcap

Bitcoin Mining

~$10M per day of newly minted bitcoins awarded to miners
What do they spend it on?



Why study blockchains and computer security?

Optimistic: a chance to build security into new platforms from the start

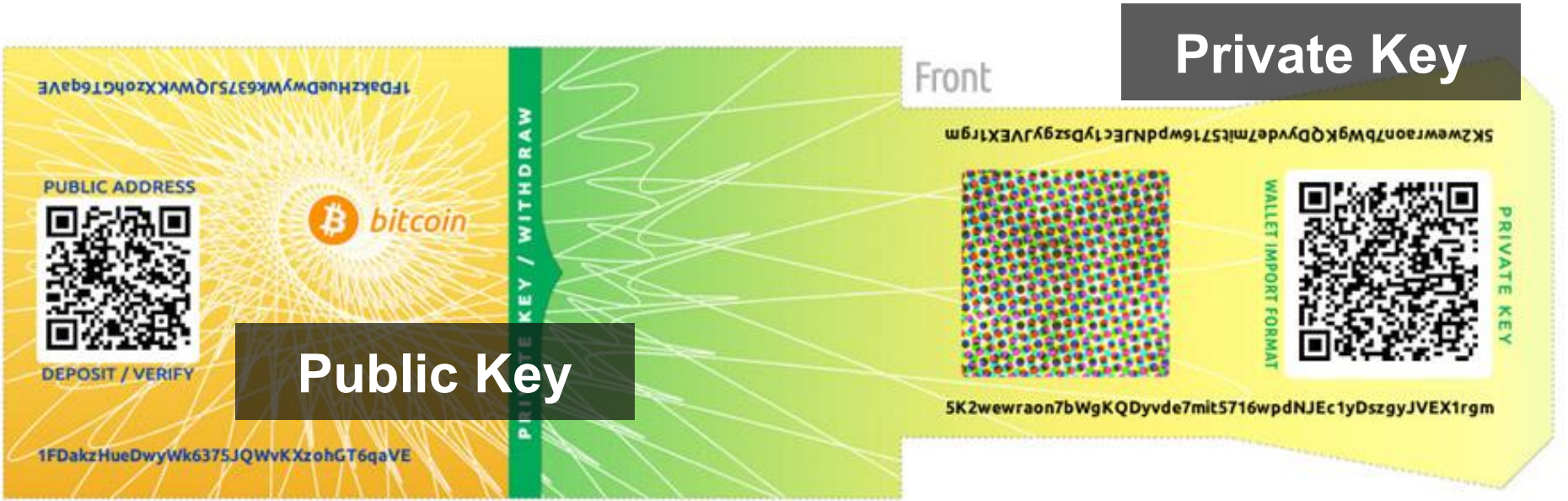
Realistic: security hazards in blockchains are so blatant and visible on the surface, they make for good learning examples!

Realistic: attract criminals, sometimes an important component of crimes

Cryptocurrencies encourage DIY security, “be your own bank”

Cryptocurrencies are open systems, easy to experiment with

Bitcoin Paper Wallet



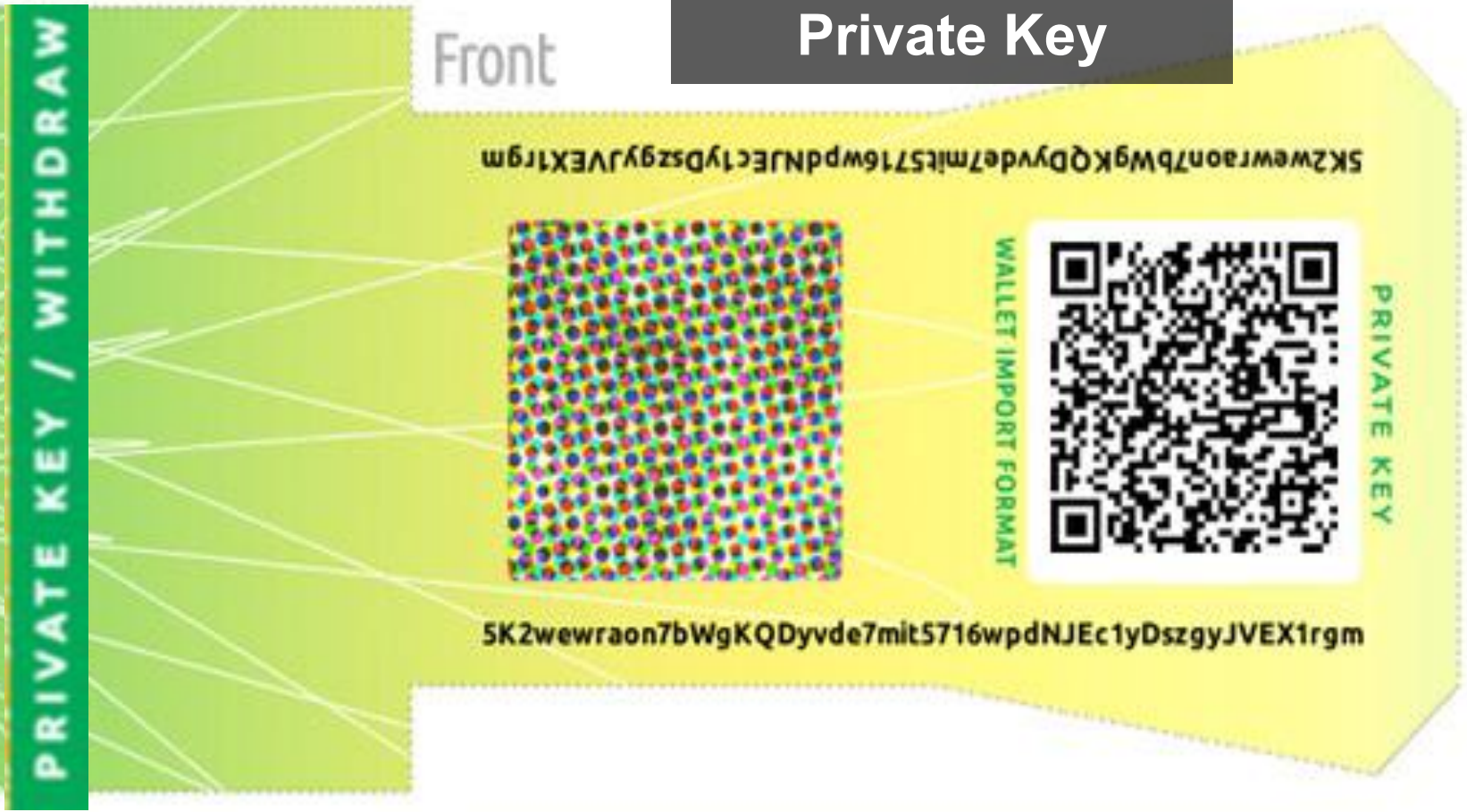
Public key / private key in bitcoin

- If someone has your public key (i.e. “address”, they can send you money.

- If you lose your private key (i.e., “wallet”), you can’t spend your money.

- If a thief gets your private key, they can steal your money.

Private Key


PRIVATE KEY / WITHDRAW
Front
5K2wewraon7bWgKQDyvde7mit5716wpdNJEc1yDszgyJVEX1rgm
WALLET IMPORT FORMAT
PRIVATE KEY
5K2wewraon7bWgKQDyvde7mit5716wpdNJEc1yDszgyJVEX1rgm


1FDakzHueDwyWk6375JQWvKXzohGT6qaVE
PUBLIC ADDRESS
bitcoin
DEPOSIT / VERIFY
1FDakzHueDwyWk6375JQWvKXzohGT6qaVE

Public Key

Alice and Bob are only identified by public keys

Transfer 10 Bitcoins from me to Bob.

Bitcoin Network

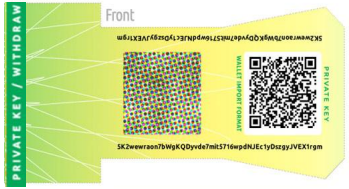
1BTC

3BTC

1BTC

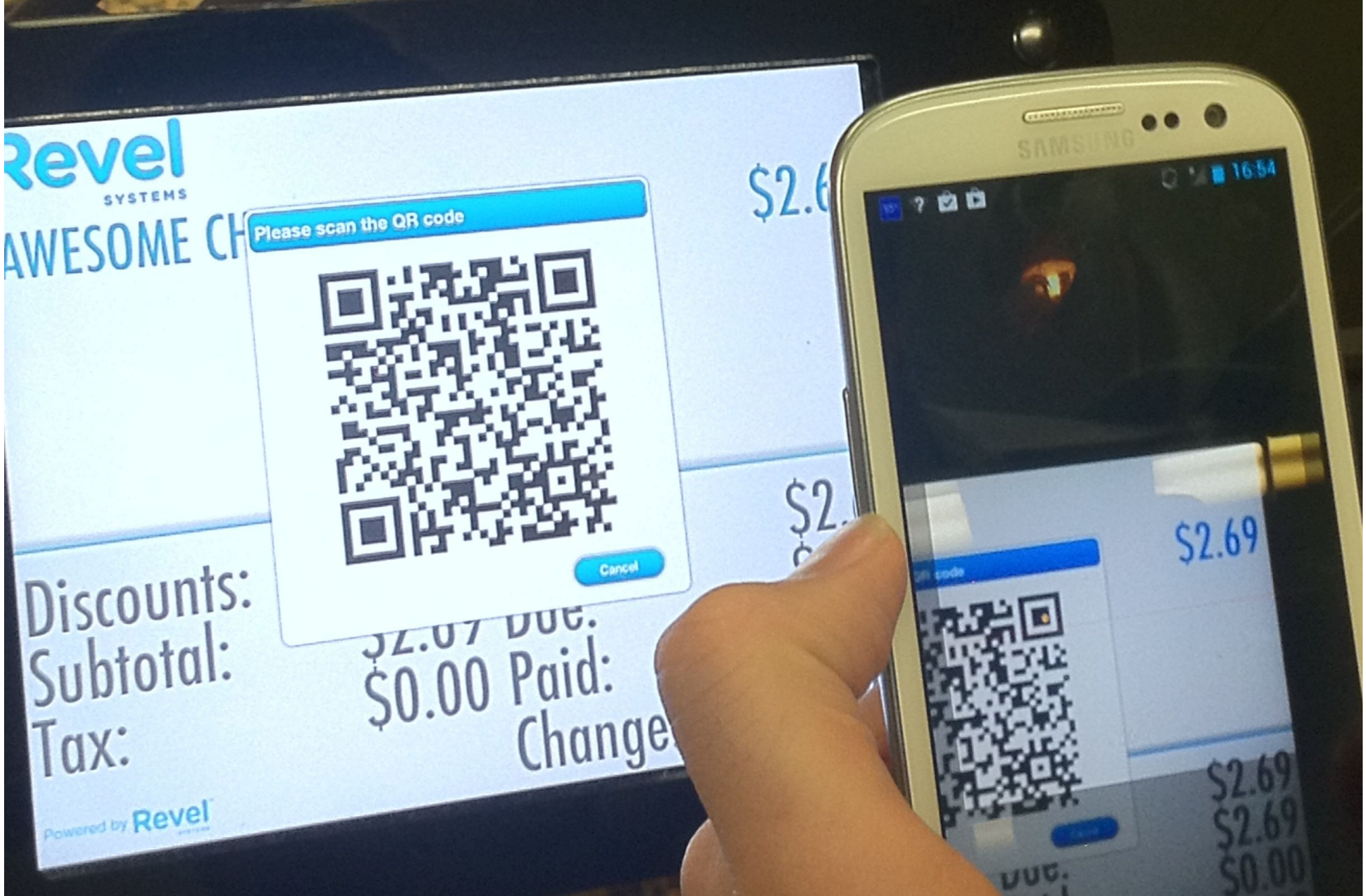
5BTC

Alice



Signed with Alice's private key

(Public Key Digital Signature)


Revel
SYSTEMS
AWESOME CH
$2.6
Please scan the QR code
Cancel
Discounts:
Subtotal:
Tax:
$0.00 Paid:
Change
Powered by Revel
SAMSUNG
16:54
$2.69
$2.69
$2.69
$0.00

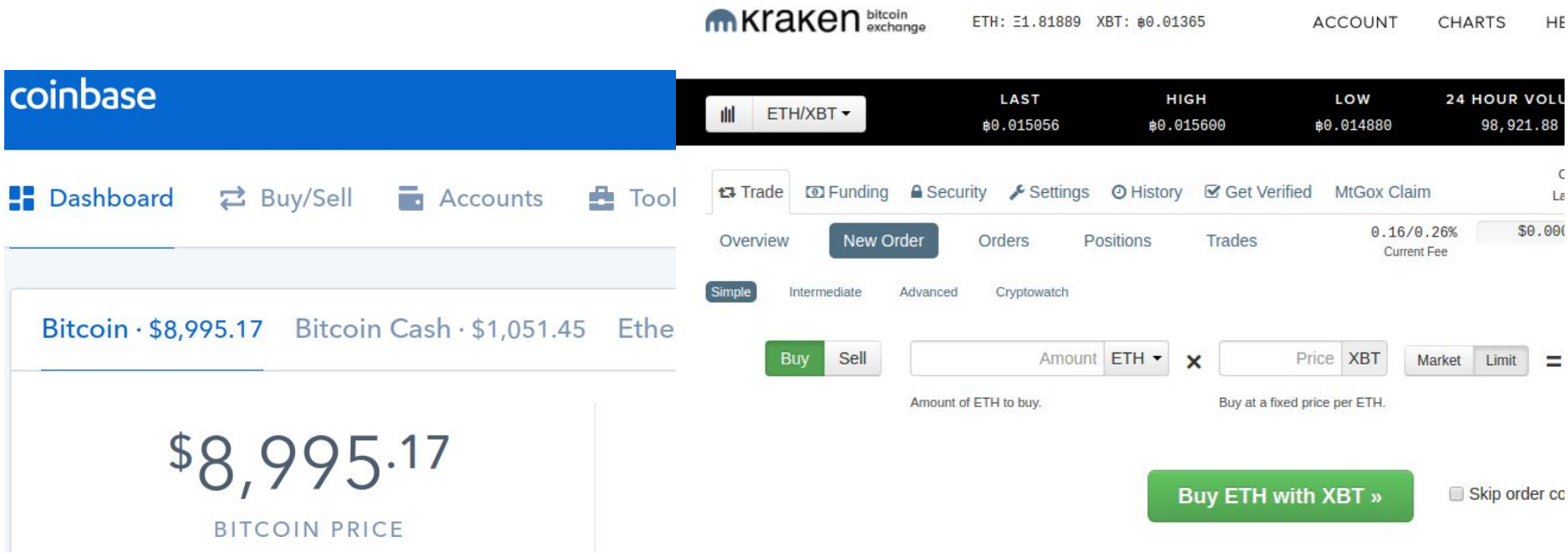
Bitcoin is the first and largest of ***hundreds*** of cryptocurrencies

All ▾ Coins ▾ Tokens ▾

#	Name	Market Cap	Price
1	Bitcoin	$158,487,664,907	$9,369.05
2	Ethereum	$69,592,728,347	$709.01
3	Ripple	$31,329,975,058	$0.801443
4	Bitcoin Cash	$18,383,130,216	$1,080.42
5	Litecoin	$10,000,508,493	$179.85
6	Cardano	$5,858,040,099	$0.225943
7	NEO	$5,738,850,000	$88.29

https://coinmarketcap.com

Cryptocurrency exchange markets



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


HI MOM SEND

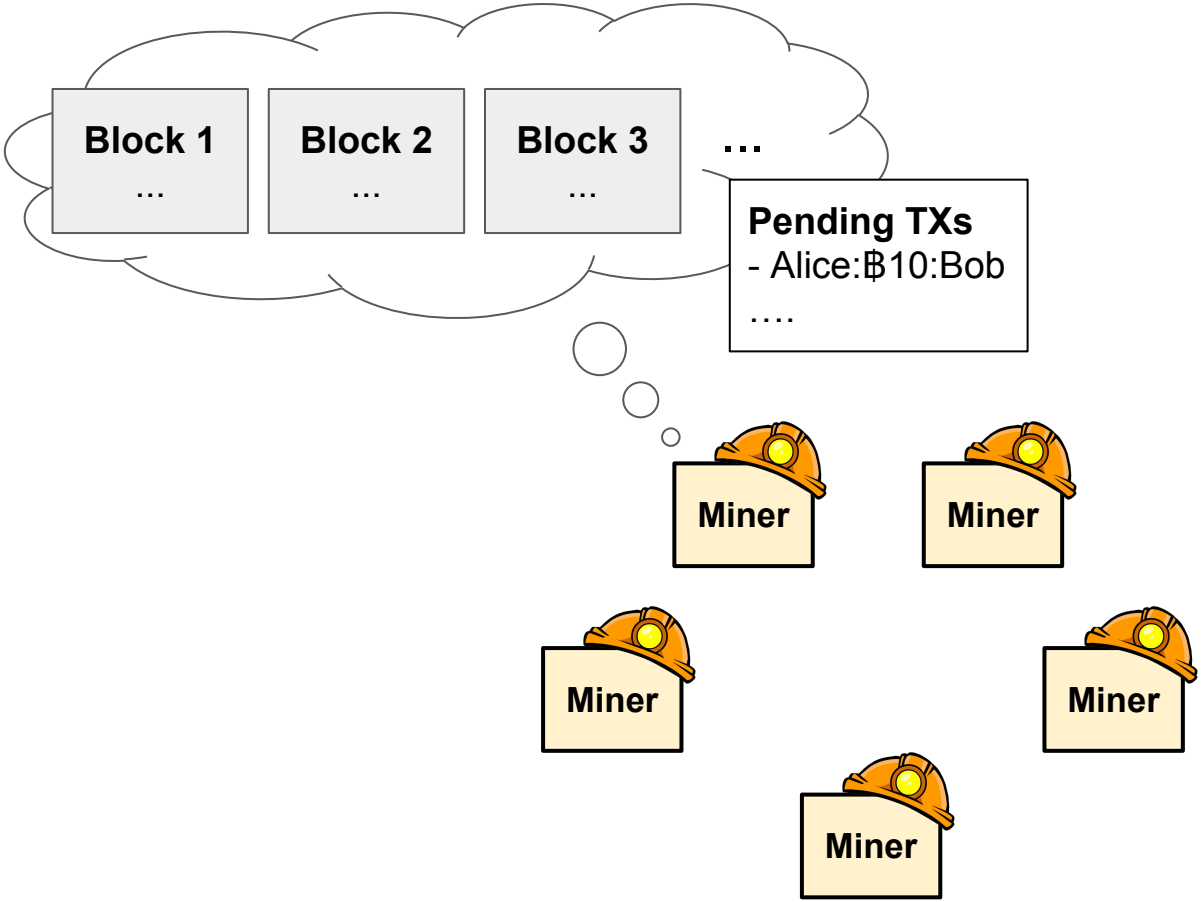

TREZOR
Confirm sending
0.0469 BTC
to
1NuuZ7S3n7h3ZnCQJ
CT2HVKTFfQjhpXhcw
Cancel
Confirm

ATMs

There's a Bitcoin ATM in Champaign!
https://imgur.com/a/DRhWL

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!


Block 1
…
Block 2
…
Block 3
…
…
Pending TXs
- Alice:฿10:Bob
….
Miner
Miner
Miner
Miner
Miner

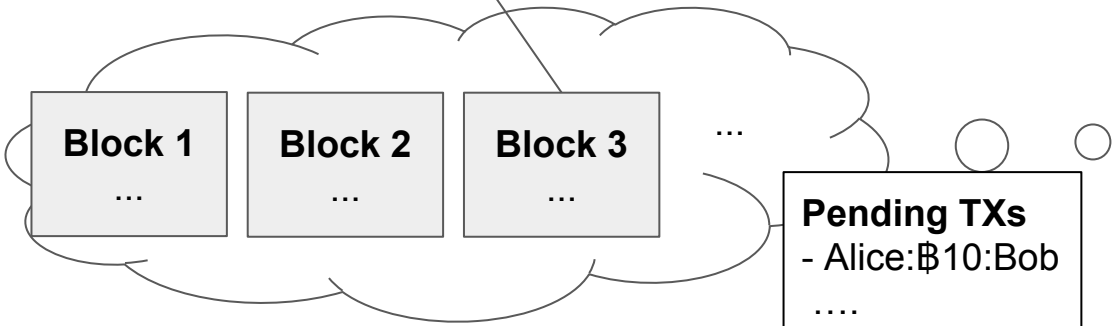
Miners commit new transactions by solving puzzles

= 0x000***...

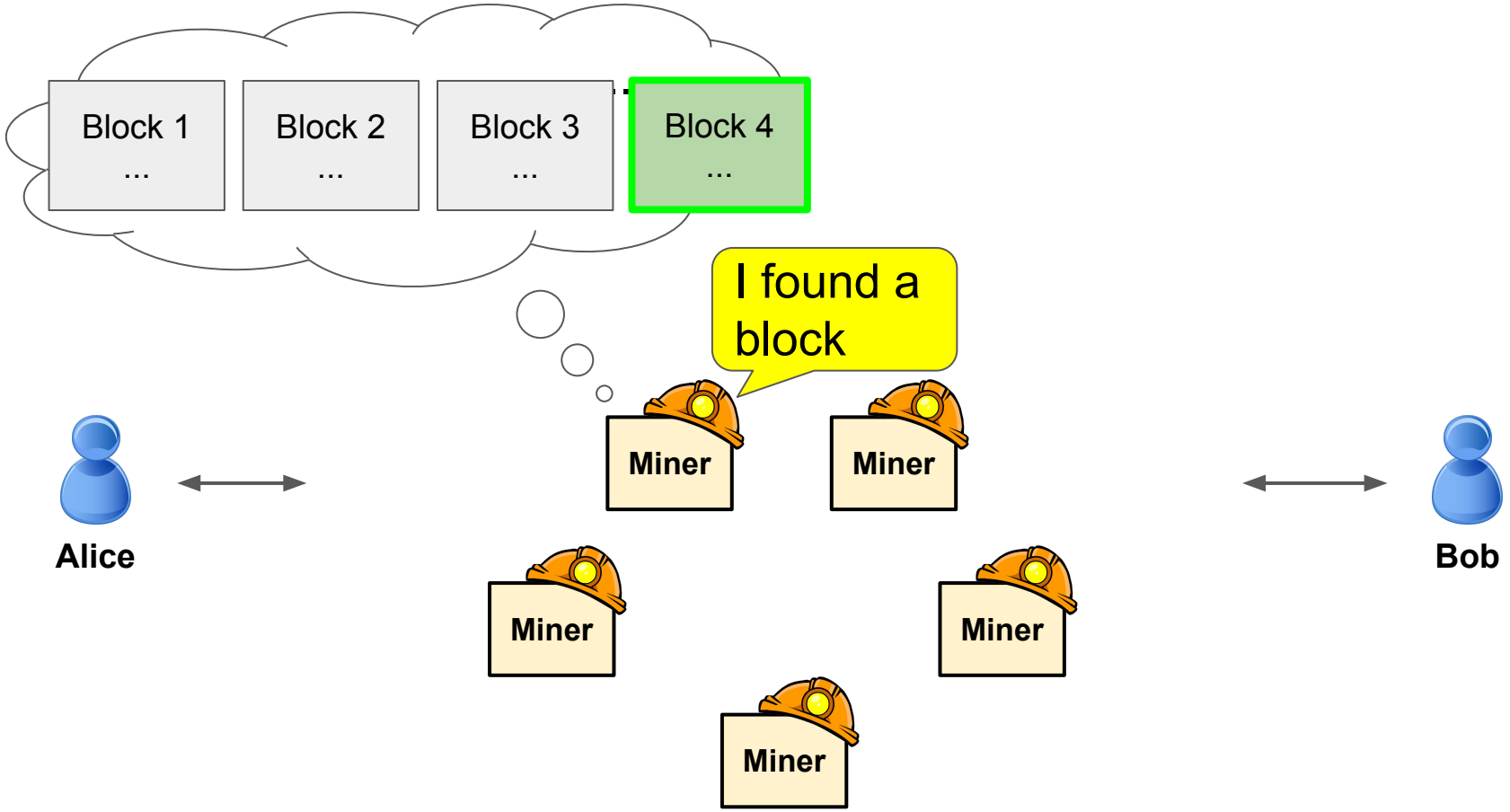
Hash(Block 3 | newTXs | 0xb9824) = 0x000c3f...

- ฿25 bonus for Miner
- Alice:฿10:Bob
...

Each attempt has 16^{-3} chance of success



Pending TXs
- Alice:฿10:Bob
....


Block 1
...
Block 2
...
Block 3
...
Block 4
...
I found a block
Miner
Miner
Miner
Miner
Miner
Alice
Bob

Evolution of mining

CPU

GPU

FPGA

ASIC

gold pan

sluice box

placer mining

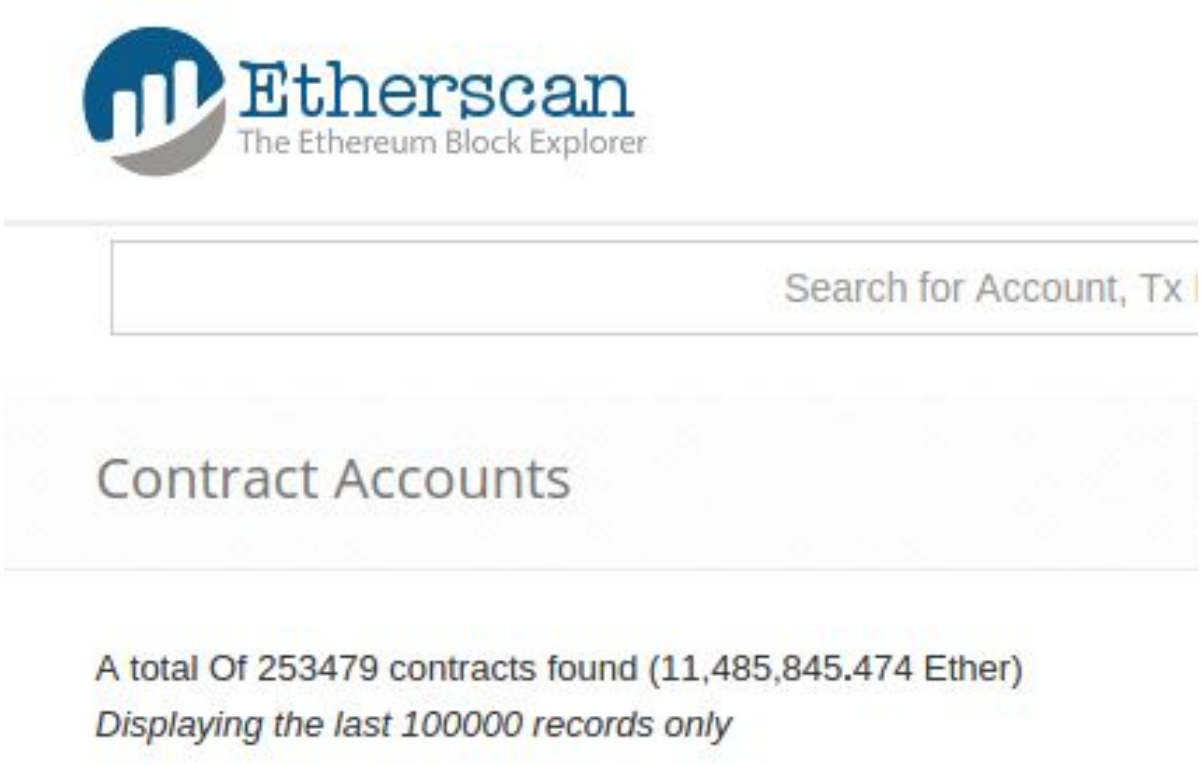
pit mining


Google
($10million per day) / (12 cents per kilowatt-hour) to megawatts
All
News
Shopping
Images
Videos
More
Settings
Tools
About 62,800 results (1.22 seconds)
($10 million per day) / (12 (U.S. cents per kilowatt hour)) =
3 472.22222 megawatts
Disclaimer - More info

Top 20 largest power producing facilities [edit]

Rank	Station	Country	Location	Capacity (MW)
1.	Three Gorges Dam	China	30°49′15″N 111°00′08″E	22,500
2.	Itaipu Dam	Brazil Paraguay	25°24′31″S 54°35′21″W	14,000
3.	Xiluodu	China	28°15′52″N 103°38′47″E	13,860
4.	Guri	Venezuela	07°45′59″N 62°59′57″W	10,235
5.	Tucuruí	Brazil	03°49′53″S 49°38′36″W	8,370
6.	Kashiwazaki-Kariwa	Japan	37°25′45″N 138°35′43″E	7,965
7.	Robert-Bourassa	Canada	53°47′43″N 77°26′26″W	7,722
8.	Grand Coulee	United States	47°57′23″N 118°58′56″W	6,809
9.	Xiangjiaba	China	28°38′57″N 104°22′14″E	6,448

More generally: “programmable money”



Ethereum Tokens Market Capitalization

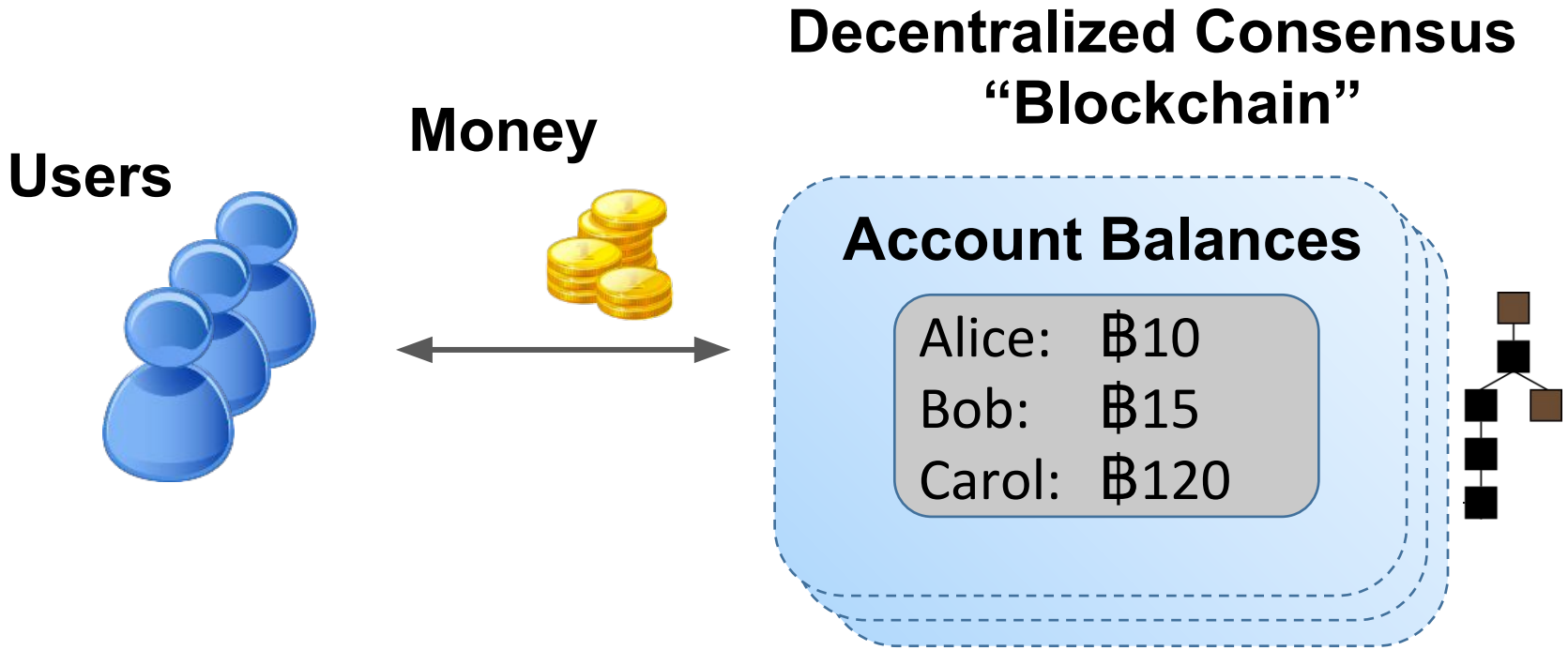
A total of 67681 ERC20 Token Contracts found

Search for any ERC20 Token Name/Address

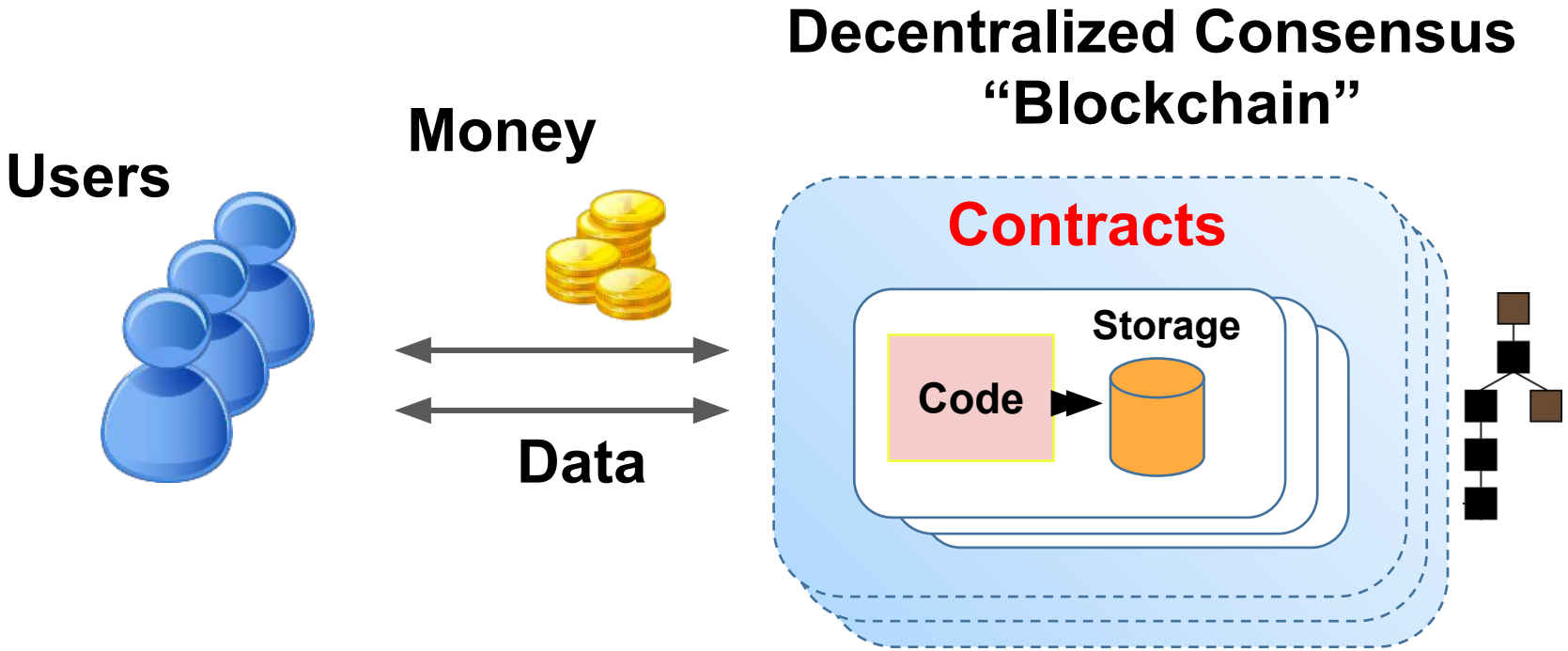
First Prev Page **1** of **9** Next Last

	Token	Price	%Change	Volume (24h)	MarketCap
1	EOS (EOS)	$6.0412 0.00088582 Btc 0.014598 Eth	▲ 3.37%	$228,197,000	$4,740,560,222
2	Tronix (TRX)	$0.0369 0.00000542 Btc 0.000089 Eth	▲ 3.75%	$304,975,000	$2,428,636,622
3	VeChain (VEN)	$2.7610	▲ 6.41%	$72,408,500	$1,448,865,120

Digital currency is just one application on top of a blockchain



Smart Contracts: user-defined programs running on top of a blockchain



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

Other examples abound:

Auctions, elections, lotteries, escrow, ...

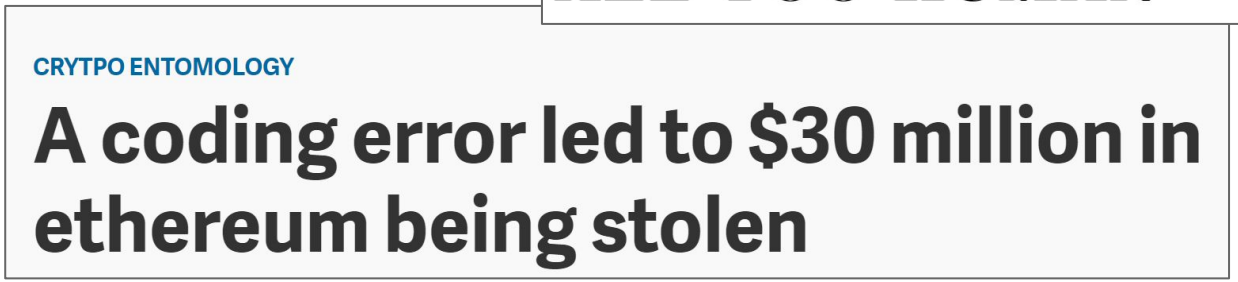
Ethereum's timeline has been pocked by failures caused by buggy and insecure smart contracts


'$300m in cryptocurrency' accidentally lost forever due to bug

User mistakenly takes control of hundreds of wallets containing cryptocurrency Ether, destroying them in a panic while trying to give them back


KLINT FINLEY BUSINESS 06.18.16 04:30 AM

A $50 MILLION HACK JUST SHOWED THAT THE DAO WAS ALL TOO HUMAN


CRYTPO ENTOMOLOGY

A coding error led to $30 million in ethereum being stolen

Cause of the Parity Wallet Disaster

* Toy version of code

Wallet contracts (one for each user):

```
contract Wallet {
   address _walletLibrary;
   address owner;

   function Wallet(address _owner) {
delegate[_walletLibrary].initWallet(_owner);
   }

   function withdraw(uint amount) {
     return
_delegate[_walletLibrary].withdraw(amount);
   }
   ...
 }
```

Wallet Library contract (shared by all users):

```
contract WalletLibrary {
     address owner;
     // called by constructor
     function initWallet(address _owner) {
         owner = _owner;
         // ... more setup ...
     }

     function withdraw(uint amount);
     function changeOwner(address _new_owner)
     function () payable {
         // ... receive money, log events, ...
     }
     ...
}
```

0xa657491c1e7f16adb39b9b60e87bbb8d93988bc3

Multiple Wallet contracts, all refer to Wallet Library
Why? Reduces fees from duplicate data!

anyone can kill your contract #6995

Open **devops199** opened this issue 22 hours ago · 12 comments

The WalletLibrary contract

devops199 commented 22 hours ago • edited

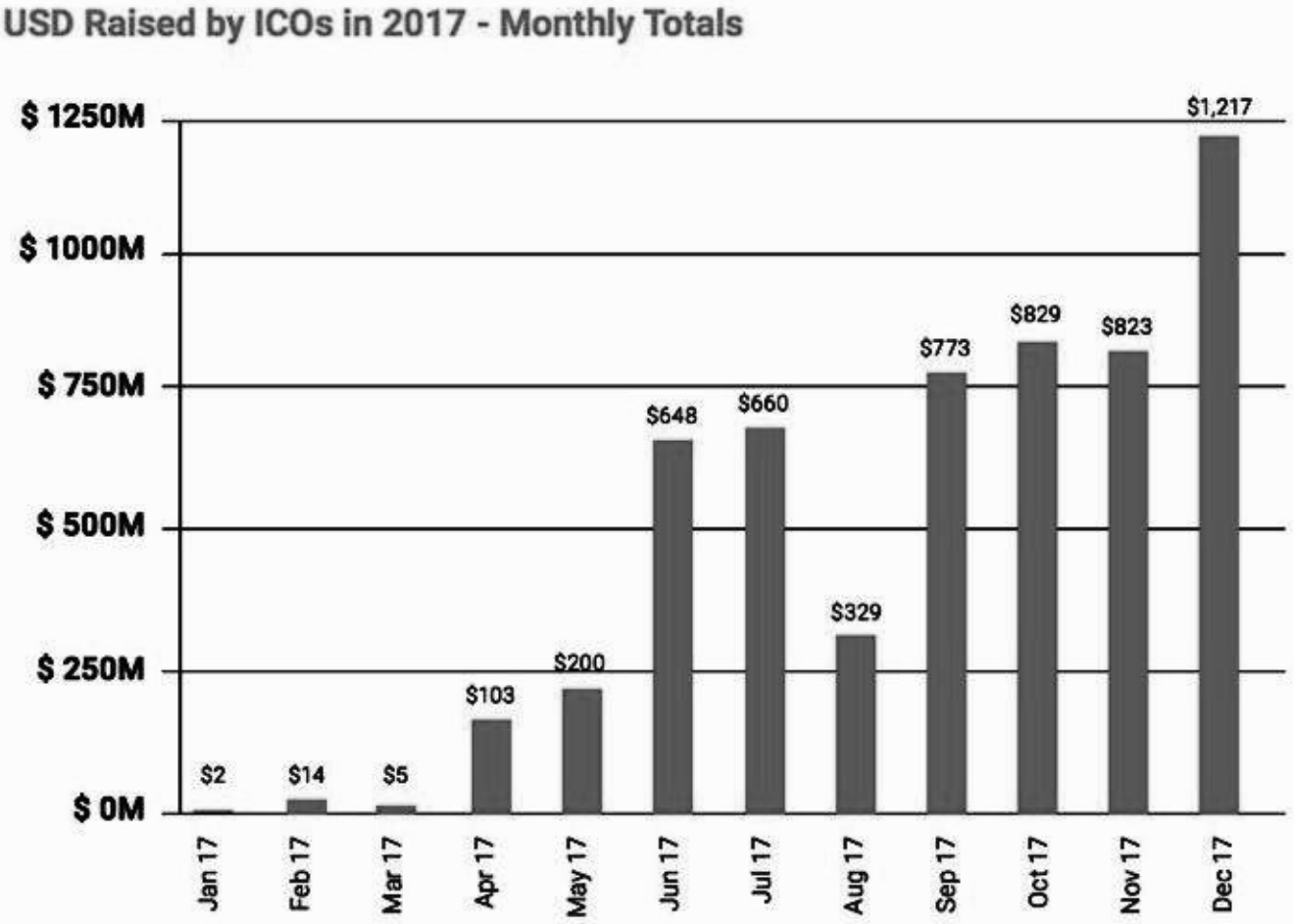
I accidentally killed it.

https://etherscan.io/address/0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4

Hello, first of all i'm not the owner of that contract. I was able to make myself the owner of that contract because its uninitialized.

These (https://pastebin.com/ejakDR1f) multi_sig wallets deployed using Parity were using the library located at "0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4" address. I made myself the owner of "0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4" contract and killed it and now when i query the dependent contracts "isowner(<any_addr>)" they all return TRUE because the delegate call made to a died contract.

I believe some one might exploit.

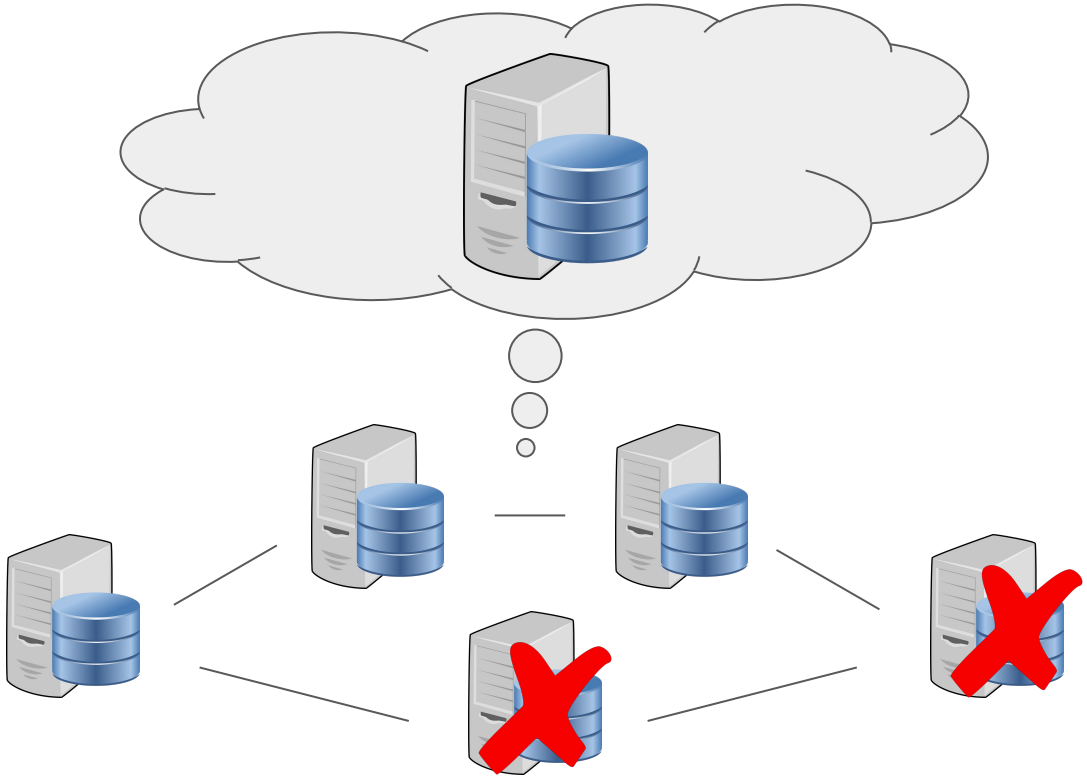


Source: Business insider

U.S. SECURITIES AND EXCHANGE COMMISSION

https://www.sec.gov/ICO

A blockchain is a *Distributed Trusted Computer*



Ordinary databases:

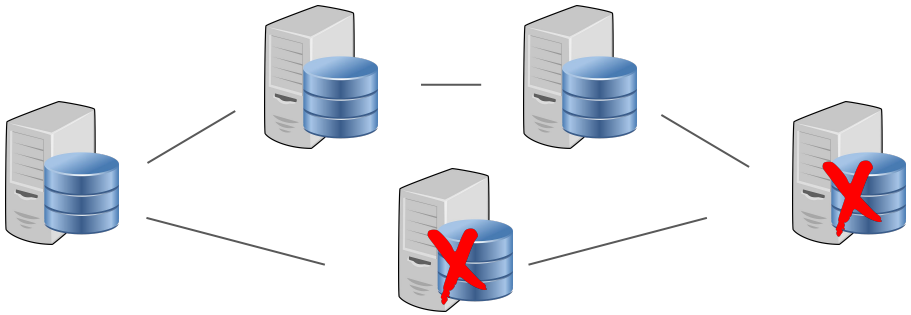
- distributed within one company
- distributed for performance and availability

Blockchain databases:

- distributed across multiple entities
- distributed for privacy and security against attacks

Permissioned Blockchains

AKA “Consortium blockchain”
Nodes are run by well-known, mostly trusted entities



Public Blockchains

Open for participation by anyone

Bitcoin is used for Crime

Ransomware

Brain Wallets

- Derive a private key from a password

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

- 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”

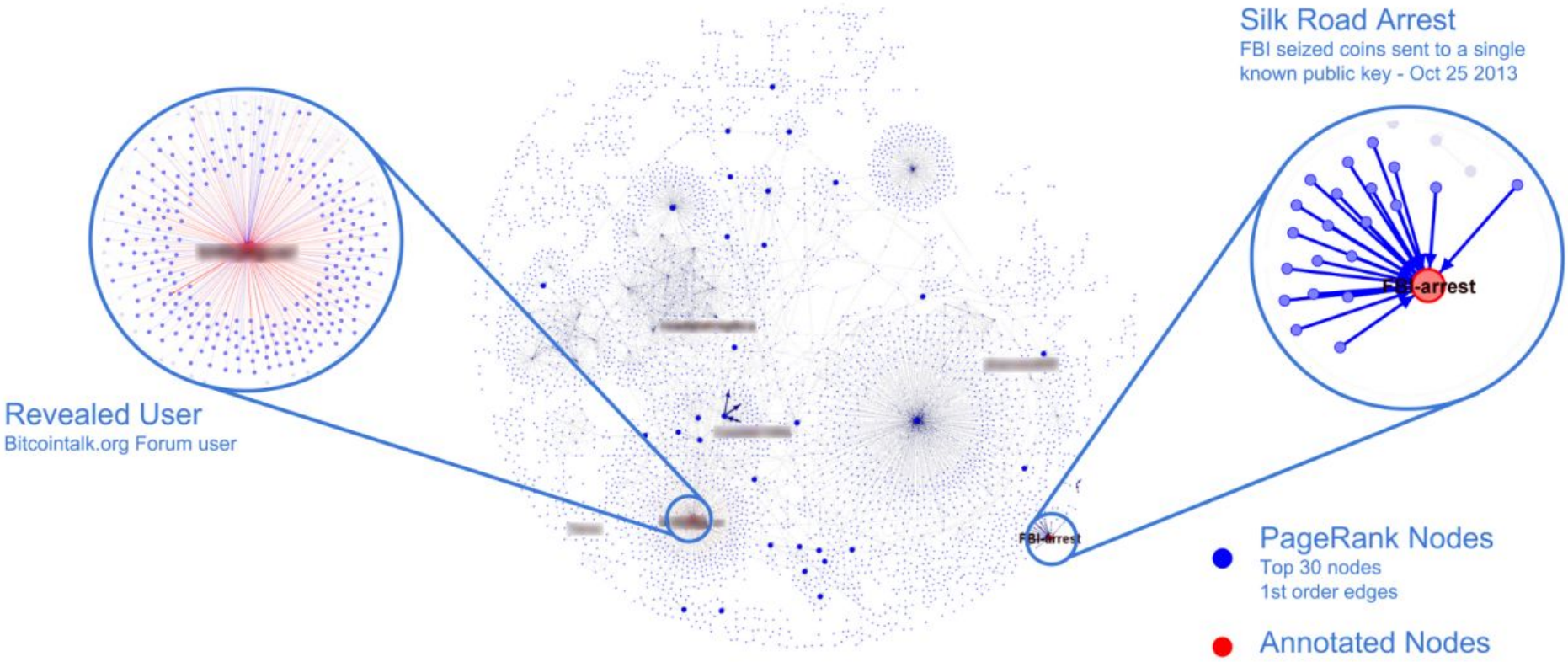
- Transaction graph analysis, clustering

    Can be traced to exchanges

- Mixers….. they mix your coins, but might take them.

- Cryptography can avoid this

    Coinshuffle, Tumblebit, Monero, Zcash, and more…



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

Discussion Questions

- Are we getting “decentralization” worth what we pay?

- Who are Bitcoin’s stakeholders? De-facto administrators?

- Those nodes in the P2P network, are they secure?

- In what ways could Bitcoin fail?

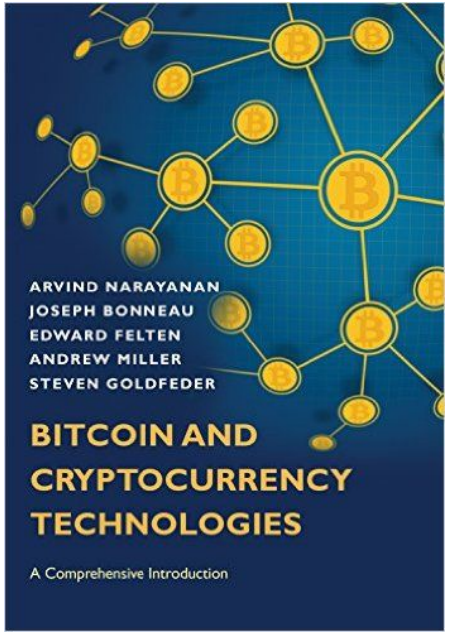
- What else can we do with Bitcoin/blockchain technology?

More Resources

PRINCETON UNIVERSITY

Bitcoin and Cryptocurrency Technologies

https://www.coursera.org/course/bitcointech



ECE 398 SC: Smart Contracts and Blockchain Security

http://soc1024.ece.illinois.edu/teaching/ece398sc/spring2018/