Busting the Blockchain Myths

SECURE SUMMITS / DC

Debra Baker, CISSP CCSP

Cygnacom Solutions

Secure Summits DC

#ISC2Summits

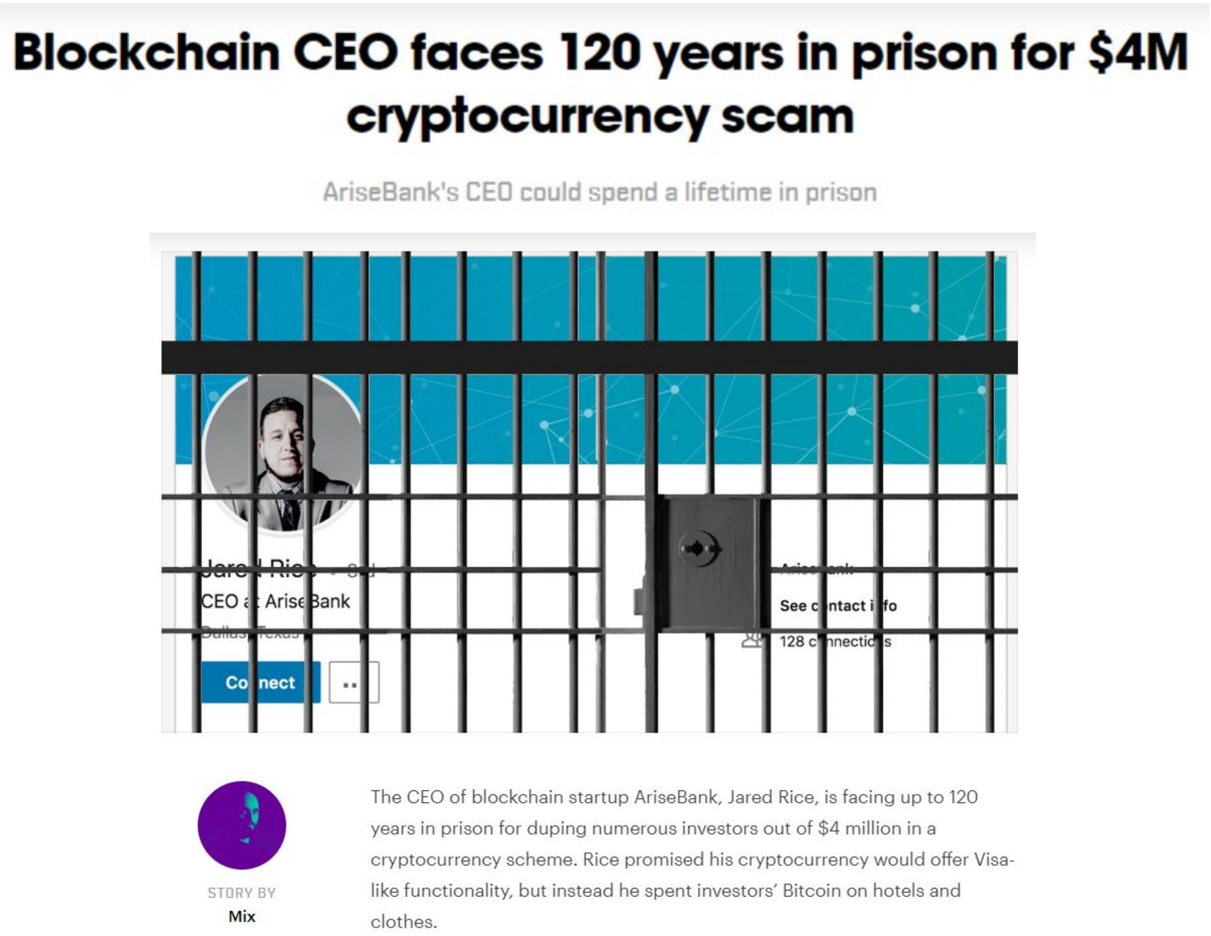
>whoami

Cygnacom Solutions

- Debra Baker, CISSP CCSP
- 20 years of practical experience in security starting in USAF – IBM

  - Entrust – Cisco – Cygnacom (Entrust Datacard)
- Founder of JHU Cryptographic Knowledge Base

  https://CryptoDoneRight.org
- Distinguished SME in Information Security (ISC2)
- Twitter: @deb_infosec

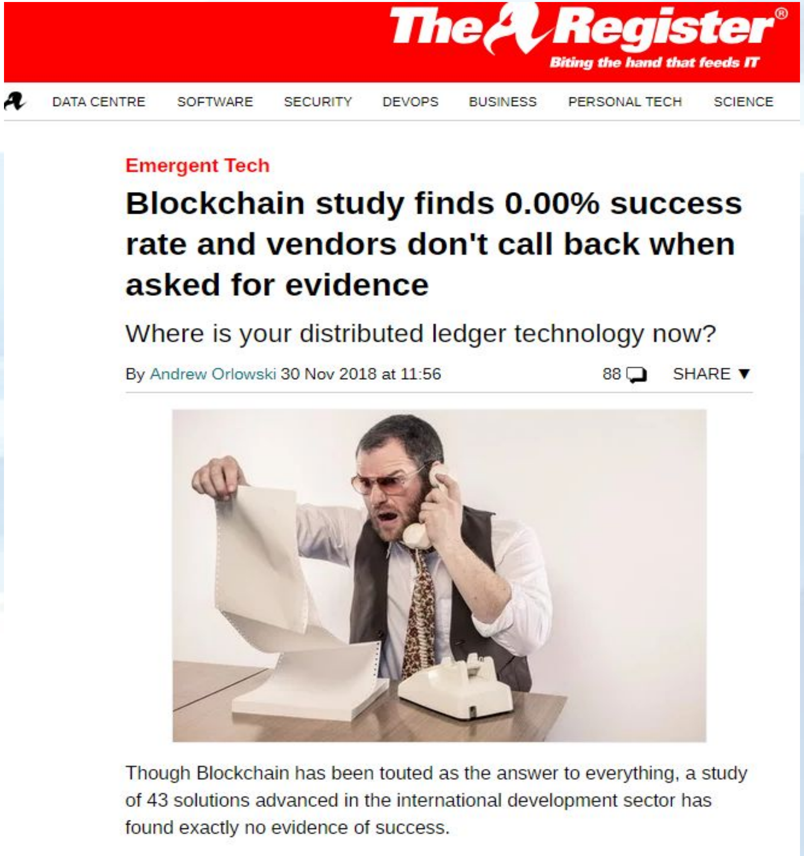


Blockchain CEO faces 120 years in prison for $4M cryptocurrency scam

AriseBank's CEO could spend a lifetime in prison

STORY BY
Mix

The CEO of blockchain startup AriseBank, Jared Rice, is facing up to 120 years in prison for duping numerous investors out of $4 million in a cryptocurrency scheme. Rice promised his cryptocurrency would offer Visa-like functionality, but instead he spent investors’ Bitcoin on hotels and clothes.



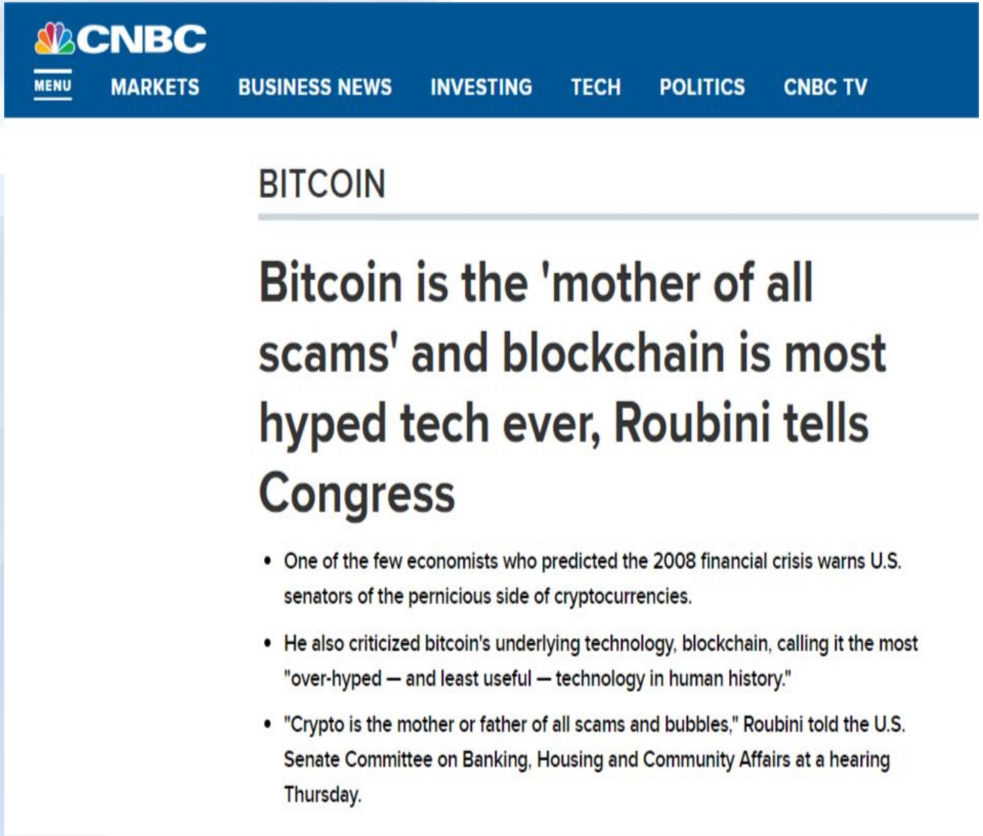
Emergent Tech

Blockchain study finds 0.00% success rate and vendors don't call back when asked for evidence

Where is your distributed ledger technology now?

By Andrew Orlowski 30 Nov 2018 at 11:56

Though Blockchain has been touted as the answer to everything, a study of 43 solutions advanced in the international development sector has found exactly no evidence of success.



BITCOIN

Bitcoin is the 'mother of all scams' and blockchain is most hyped tech ever, Roubini tells Congress

- One of the few economists who predicted the 2008 financial crisis warns U.S. senators of the pernicious side of cryptocurrencies.
- He also criticized bitcoin's underlying technology, blockchain, calling it the most "over-hyped — and least useful — technology in human history."
- "Crypto is the mother or father of all scams and bubbles," Roubini told the U.S. Senate Committee on Banking, Housing and Community Affairs at a hearing Thursday.

Common Myths

BUSTED!

Cygnacom Solutions

- Blockchain is as secure as TLS channel
- Blockchain is Immutable
- Blockchain will replace Databases
- Blockchain will replace PKI
- Blockchain has built in Disaster Recovery
- Blockchain is DDOS proof

JP Morgan CIO: Blockchain Will Replace Existing Technology

In a few years blockchain will replace the existing technology, today it only coexists with the current one," - Lori Beer

Courtesy of Coin Telegraph

What is JP Morgan Doing?

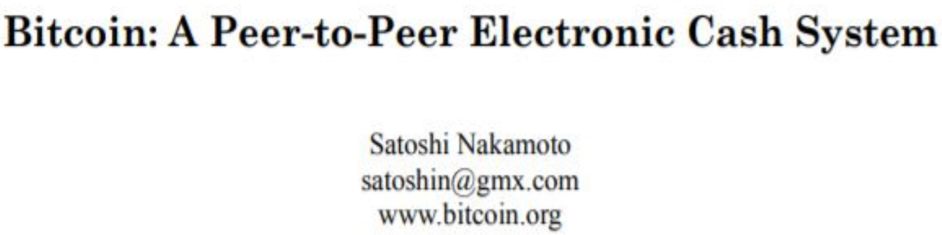
- JP Morgan filed a patent for a blockchain using Ethereum
- Used to settle inter and intra-bank transactions
- Using the blockchain as a “distributed ledger to process payments in real-time, without having to rely on a trusted third party to hold the true "golden copy” of the audit trail.”

How is Blockchain being used?

- Bitcoin, Alt Currencies (Ethereum and dApps)
- Distributed Ledger (IBM Diamond Industry and Food Safety)
- Smart Contracts (electronic P2P transactions or Conditions for a transaction to occur)
- IOT Blockchain (IOTA and Tangle)

History of Blockchain

- Bitcoin was invented by **Satoshi Nakamoto** in 2008

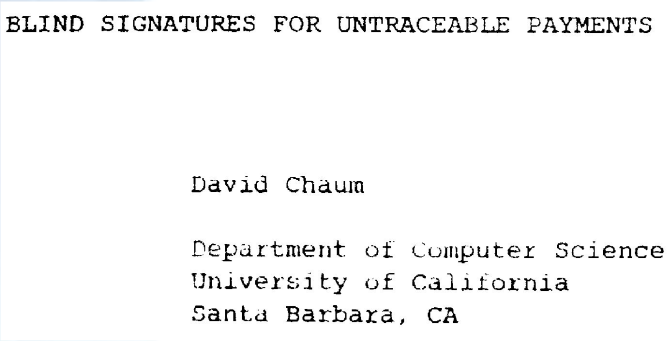


Bitcoin: A Peer-to-Peer Electronic Cash System

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

History

- 1982 - David Chaum “e-cash”
- 1997 - Adam Back “hashcash”
- 1999 – Sandeer and TaShama e-cash with Merkle trees
- 2008 - Bitcoin



BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

Department of Computer Science
University of California
Santa Barbara, CA

Hash Function

- Digital Fingerprint of data (document, image, etc) – provides integrity
- One way hash is generated always same size, SHA-256 is 256 bits

.docx

ABC Defg

.docx

ABC Defg

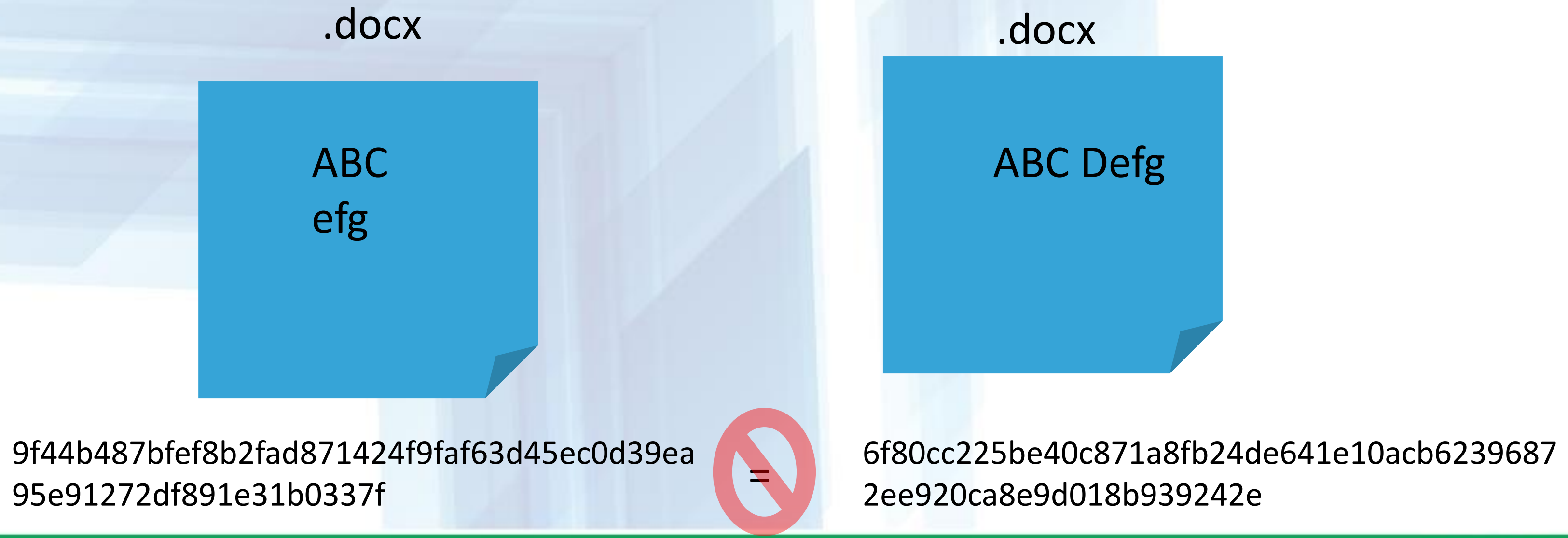
6f80cc225be40c871a8fb24de641e10acb623968
72ee920ca8e9d018b939242e

=

6f80cc225be40c871a8fb24de641e10acb6239687
2ee920ca8e9d018b939242e

Hash Function

- Digital Fingerprint of data (document, image, etc) – provides integrity
- One way hash is generated always same size, SHA-256 is 256 bits



.docx

ABC
efg

.docx

ABC Defg

9f44b487bfef8b2fad871424f9faf63d45ec0d39ea
95e91272df891e31b0337f

=

6f80cc225be40c871a8fb24de641e10acb6239687
2ee920ca8e9d018b939242e

What is Blockchain?

“Blockchain at its core is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.”

-Mastering Blockchain, Imran Bashir

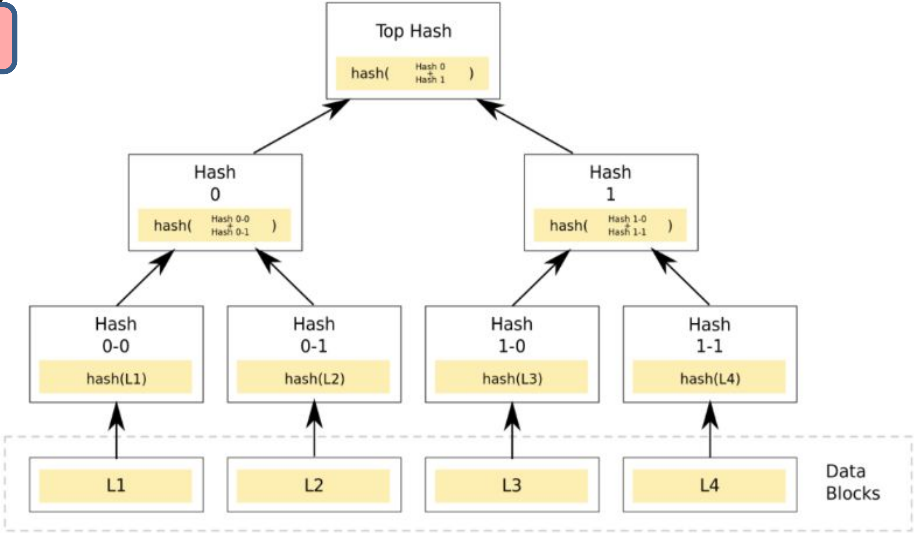


Diagram courtesy of Medium.com

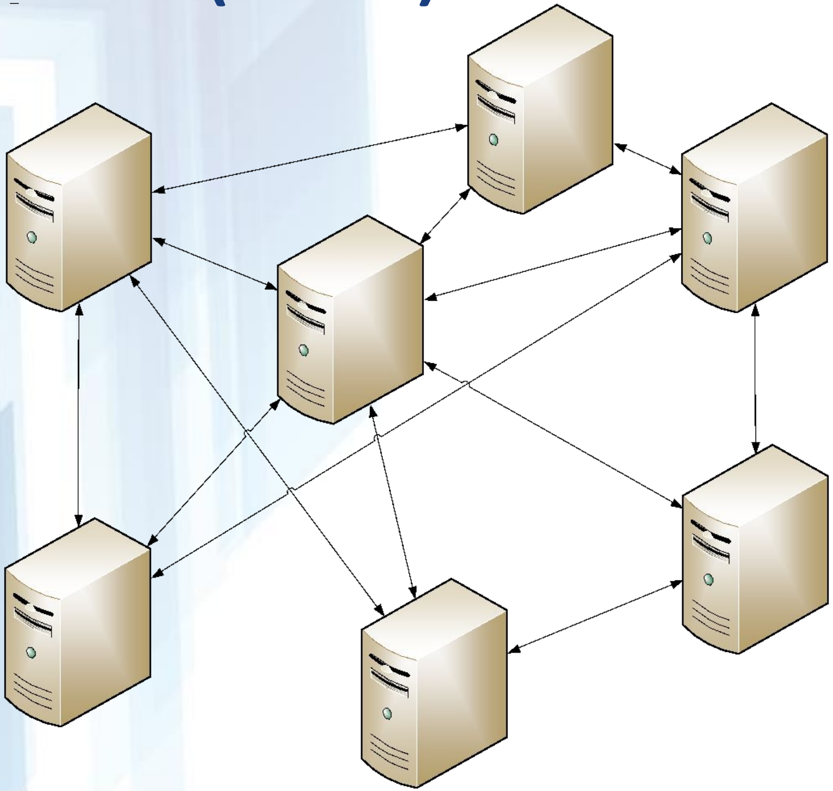
Blockchain is Immutable

BUSTED!

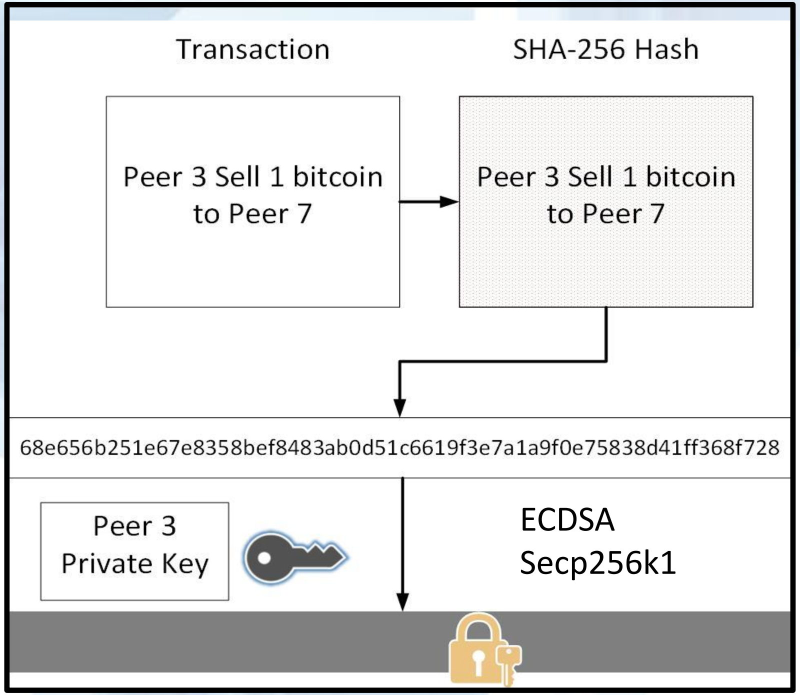
- Immutable means unchangeable, but in blockchain the longest chain wins > Proof of Work (POW).
- In 2016, someone figured out how to mine Ethereum faster than anyone else which lead to them creating the longest chain and taking over the blockchain > stealing $50 million
- To fix it a hard fork of Ethereum, led to $50 million in Ethereum being stolen
- This created a new Ethereum and the old blockchain was named Ethereum classic.

Peer to Peer Network (P2P)

- Based on client installed
  - Client Node
  - Miner Node
  - Full Node
- Client Discovery
  - Client finds node’s external IP
  - Resolves known BTC miners via DNS seed file
  - Client remembers previous connected nodes



Digital Signatures



Transaction

SHA-256 Hash

Peer 3 Sell 1 bitcoin to Peer 7

Peer 3 Sell 1 bitcoin to Peer 7

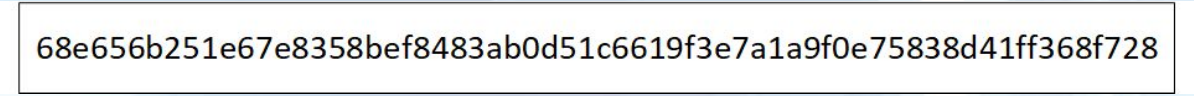
68e656b251e67e8358bef8483ab0d51c6619f3e7a1a9f0e75838d41ff368f728

Peer 3 Private Key

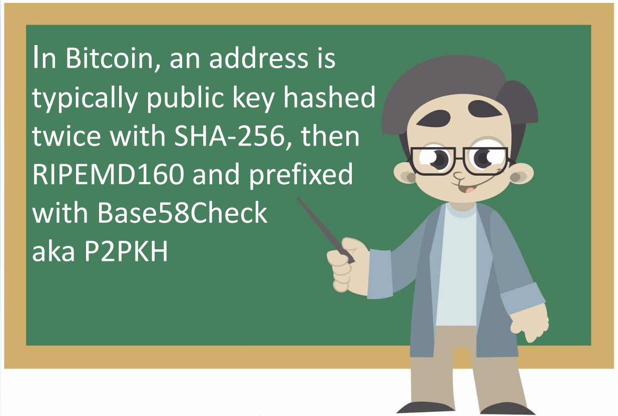
ECDSA
Secp256k1

What are we encrypting?

- The hash value



68e656b251e67e8358bef8483ab0d51c6619f3e7a1a9f0e75838d41ff368f728



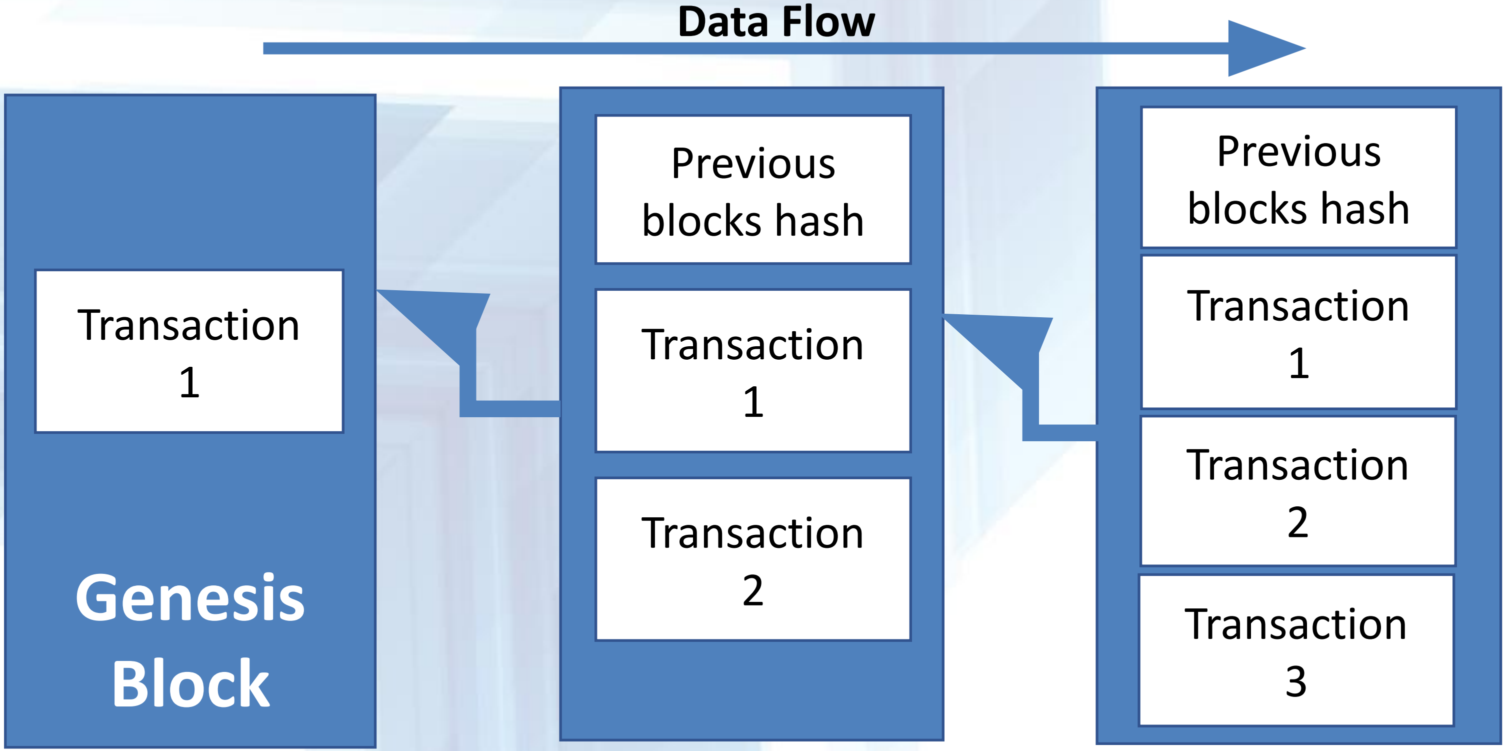
In Bitcoin, an address is typically public key hashed twice with SHA-256, then RIPEMD160 and prefixed with Base58Check aka P2PKH

- The data within the blockchain is not encrypted
- It does provide integrity
- Even though considered ‘Anonymous’ still not private and law enforcement can locate person

Blockchain as secure as TLS Channel

BUSTED!

Block Chain – Miner and Full Node



Data Flow

Transaction 1

Genesis Block

Previous blocks hash

Transaction 1

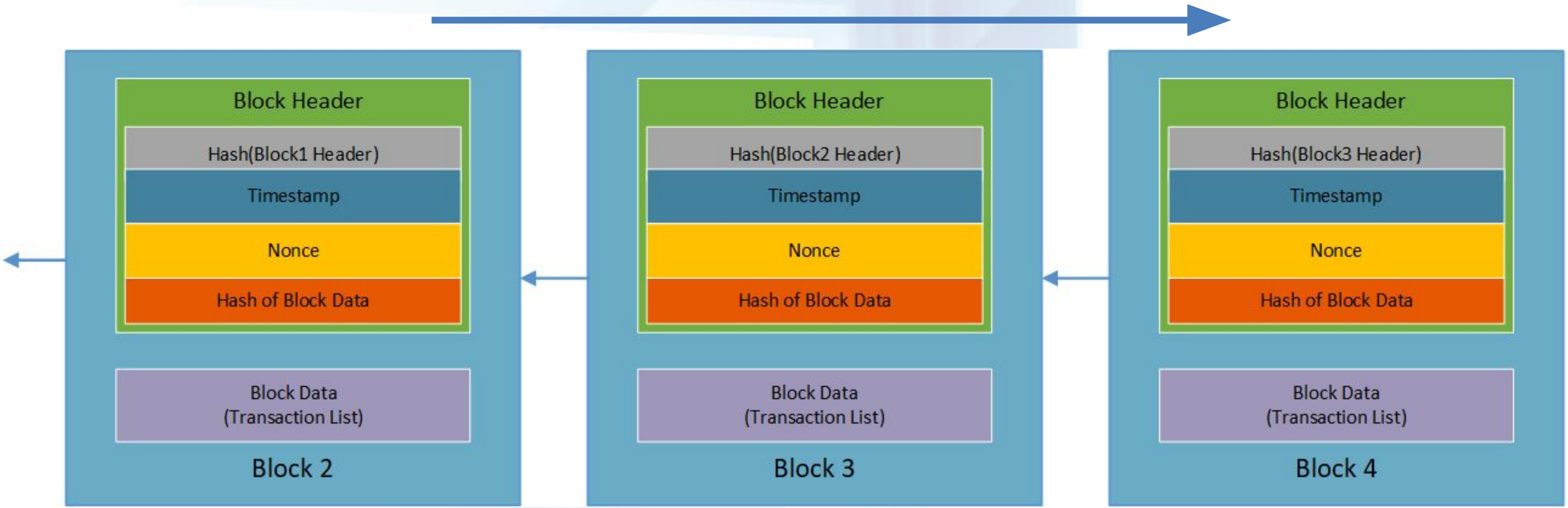
Transaction 2

Previous blocks hash

Transaction 1

Transaction 2

Transaction 3


Data Flow
Block Header
Hash(Block1 Header)
Timestamp
Nonce
Hash of Block Data
Block Data
(Transaction List)
Block 2
Block Header
Hash(Block2 Header)
Timestamp
Nonce
Hash of Block Data
Block Data
(Transaction List)
Block 3
Block Header
Hash(Block3 Header)
Timestamp
Nonce
Hash of Block Data
Block Data
(Transaction List)
Block 4

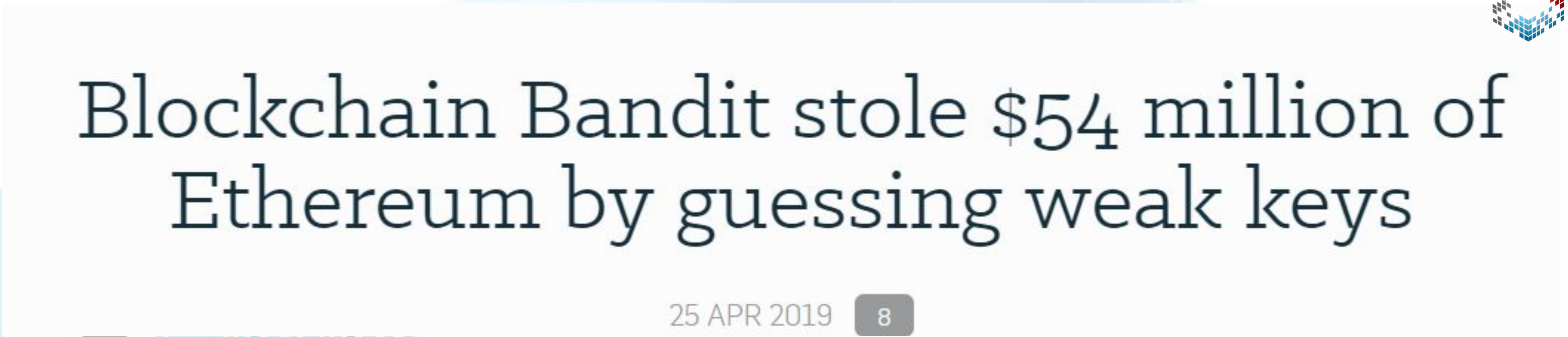
Merkle Tree or “Block Tree”

- Transactions are paired ar hashed forming merkle root
- Uses Hash pointers
  - Pointer to data
    - ○ Address (hashed public key) ie. PTPKH
  - Hash Value of Data

Where are the keys generated?

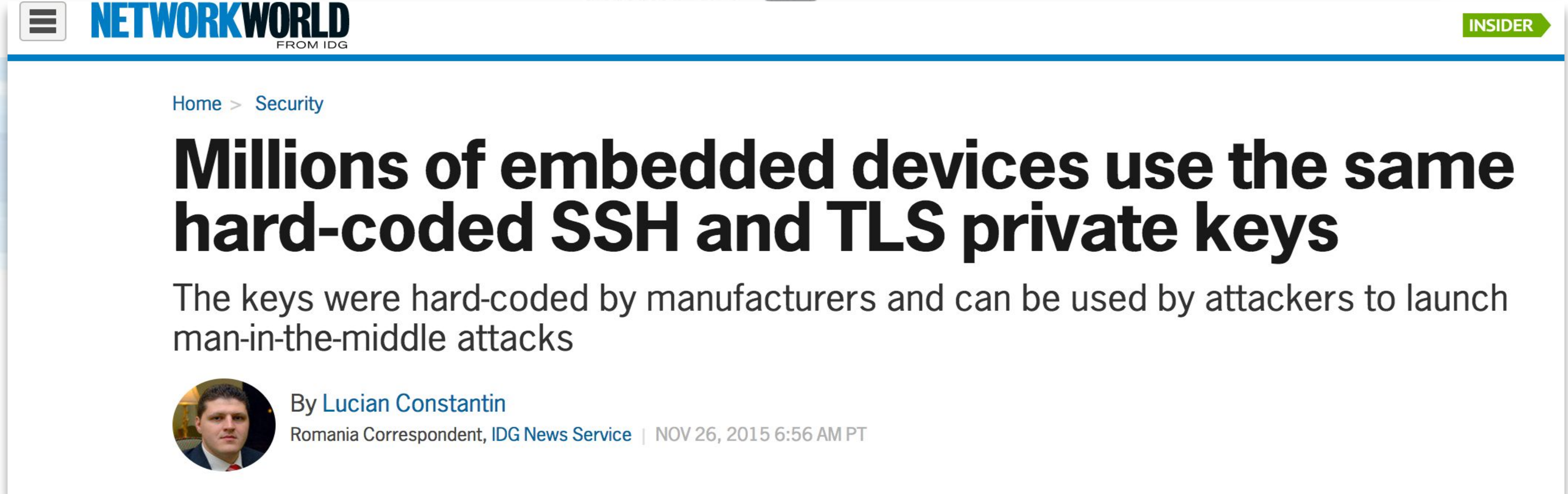
- On the **client machine!**
- Must have good entropy ‘randomness’ to generate strong crypto keys
- True for ANY crypto key, but if randomness is poor when using ECDSA, then probably will leak your private key in generating a key pair or even signing!!!

oh no!!! I can leak my private key when signing!!!



Blockchain Bandit stole $54 million of Ethereum by guessing weak keys

25 APR 2019 8



Home > Security

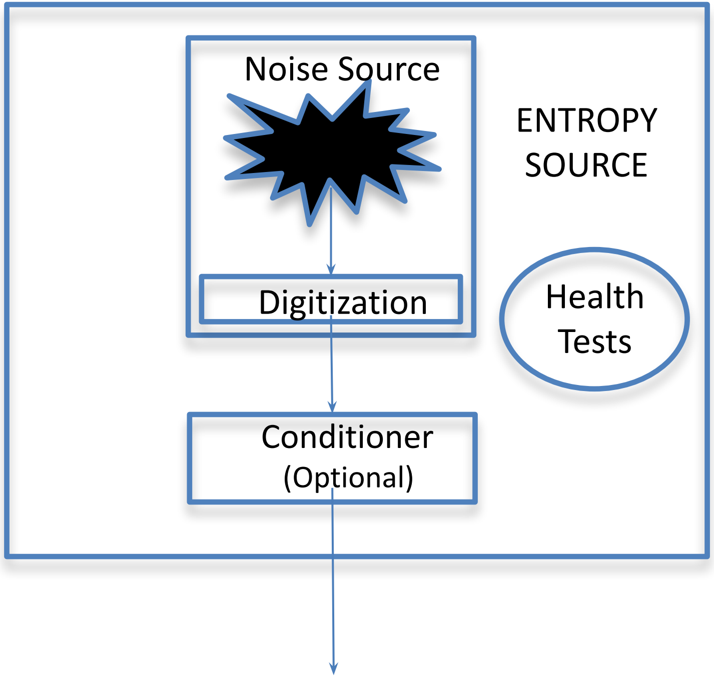
Millions of embedded devices use the same hard-coded SSH and TLS private keys

The keys were hard-coded by manufacturers and can be used by attackers to launch man-in-the-middle attacks

By Lucian Constantin

Romania Correspondent, IDG News Service | NOV 26, 2015 6:56 AM PT

Entropy Overview



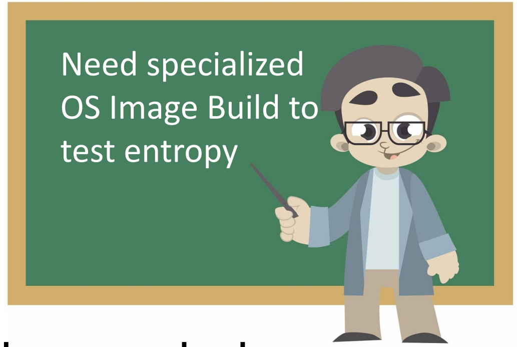
Entropy output to Deterministic Random Bit Generator (DRBG)

How to get Good Entropy?

- Use Servers - with hardware entropy processor (Act2Lite, Cavium, Intel chip with on board entropy these meet NIST800-90B)

  -OR-

- QNX 7.x (random.c) using Fortuna
- FreeBSD 11.1 or above - using Fortuna
- Truerand.c
- Make sure your entropy pool is seeded on boot and reseeded properly
- Test the PRNG using NIST SP800-90B assessment tools

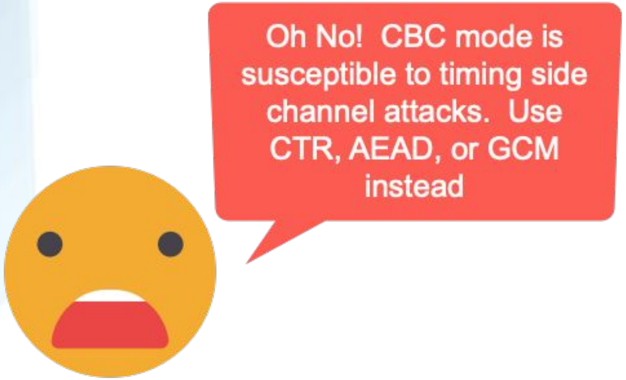


Need specialized OS Image Build to test entropy

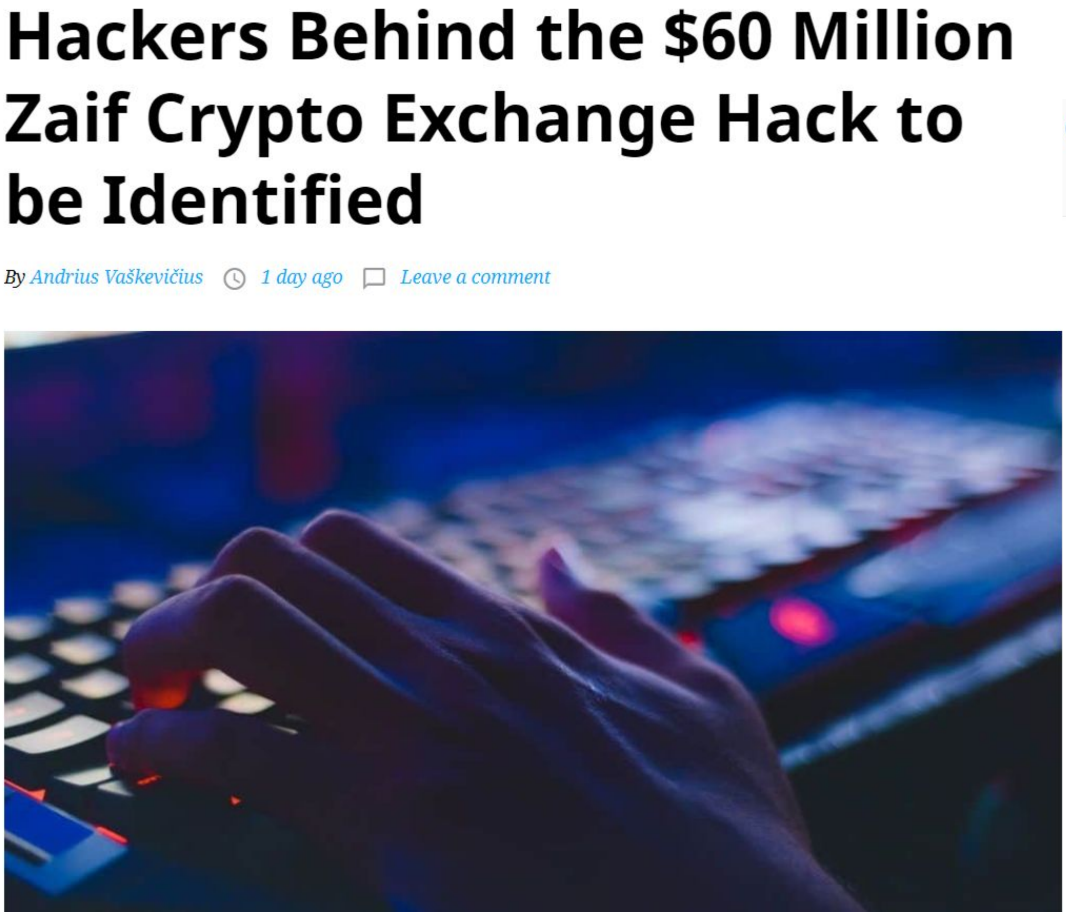
Securing your Wallet

- **If you lose access to your wallet, then you lose all of your bitcoin**
  - Strong Password
  - 2FA
  - Offline storage
- Wallet is encrypted using **AES-CBC** mode
- The private key is stored in the wallet as the Berkely DB file:

```
:~/.bitcoin$ file wallet.dat
```

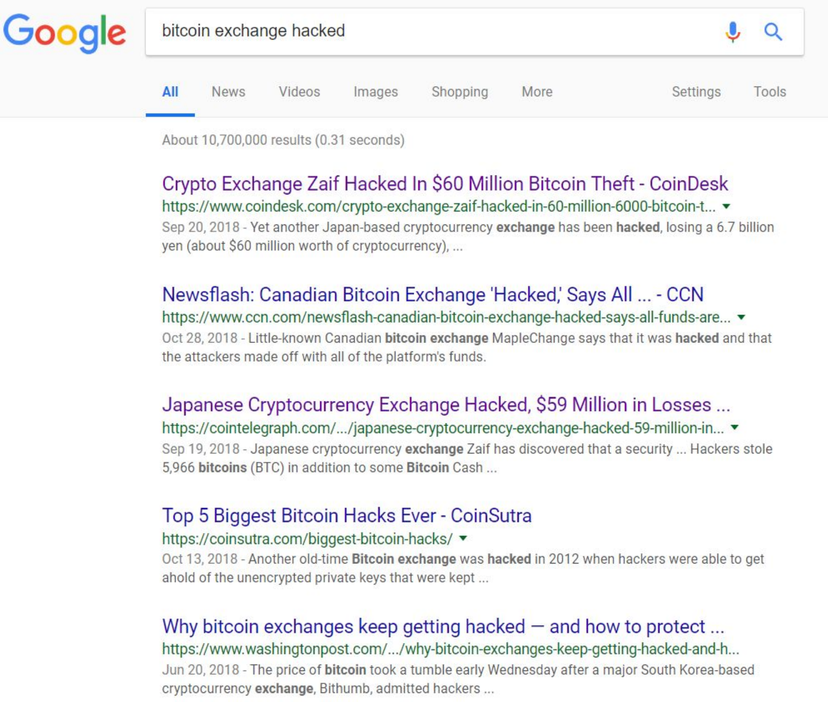


Oh No! CBC mode is susceptible to timing side channel attacks. Use CTR, AEAD, or GCM instead



Hackers Behind the $60 Million Zaif Crypto Exchange Hack to be Identified

By Andrius Vaškevičius *1 day ago* *Leave a comment*



bitcoin exchange hacked

About 10,700,000 results (0.31 seconds)

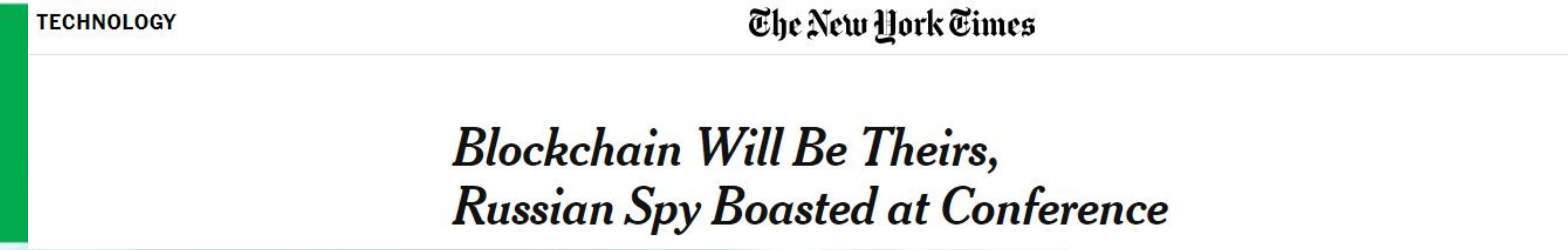
Crypto Exchange Zaif Hacked In $60 Million Bitcoin Theft - CoinDesk
https://www.coindesk.com/crypto-exchange-zaif-hacked-in-60-million-6000-bitcoin-t... ▾
Sep 20, 2018 - Yet another Japan-based cryptocurrency **exchange** has been **hacked**, losing a 6.7 billion yen (about $60 million worth of cryptocurrency), ...

Newsflash: Canadian Bitcoin Exchange 'Hacked,' Says All ... - CCN
https://www.ccn.com/newsflash-canadian-bitcoin-exchange-hacked-says-all-funds-are... ▾
Oct 28, 2018 - Little-known Canadian **bitcoin exchange** MapleChange says that it was **hacked** and that the attackers made off with all of the platform's funds.

Japanese Cryptocurrency Exchange Hacked, $59 Million in Losses ...
https://cointelegraph.com/.../japanese-cryptocurrency-exchange-hacked-59-million-in... ▾
Sep 19, 2018 - Japanese cryptocurrency **exchange** Zaif has discovered that a security ... Hackers stole 5,966 **bitcoins** (BTC) in addition to some **Bitcoin** Cash ...

Top 5 Biggest Bitcoin Hacks Ever - CoinSutra
https://coinsutra.com/biggest-bitcoin-hacks/ ▾
Oct 13, 2018 - Another old-time **Bitcoin exchange** was **hacked** in 2012 when hackers were able to get ahold of the unencrypted private keys that were kept ...

Why bitcoin exchanges keep getting hacked — and how to protect ...
https://www.washingtonpost.com/.../why-bitcoin-exchanges-keep-getting-hacked-and-h...
Jun 20, 2018 - The price of **bitcoin** took a tumble early Wednesday after a major South Korea-based cryptocurrency **exchange**, Bithumb, admitted hackers ...



TECHNOLOGY

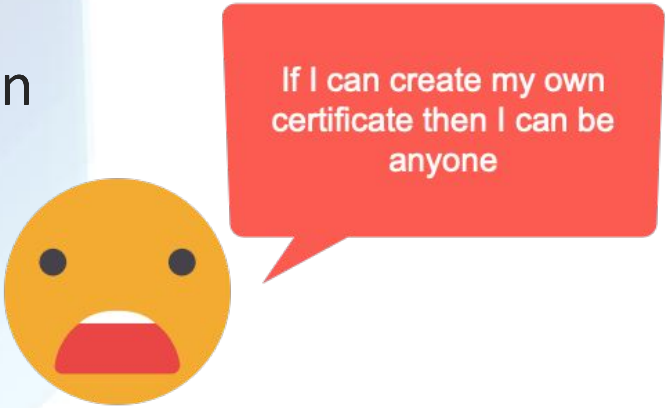
The New York Times

Blockchain Will Be Theirs, Russian Spy Boasted at Conference

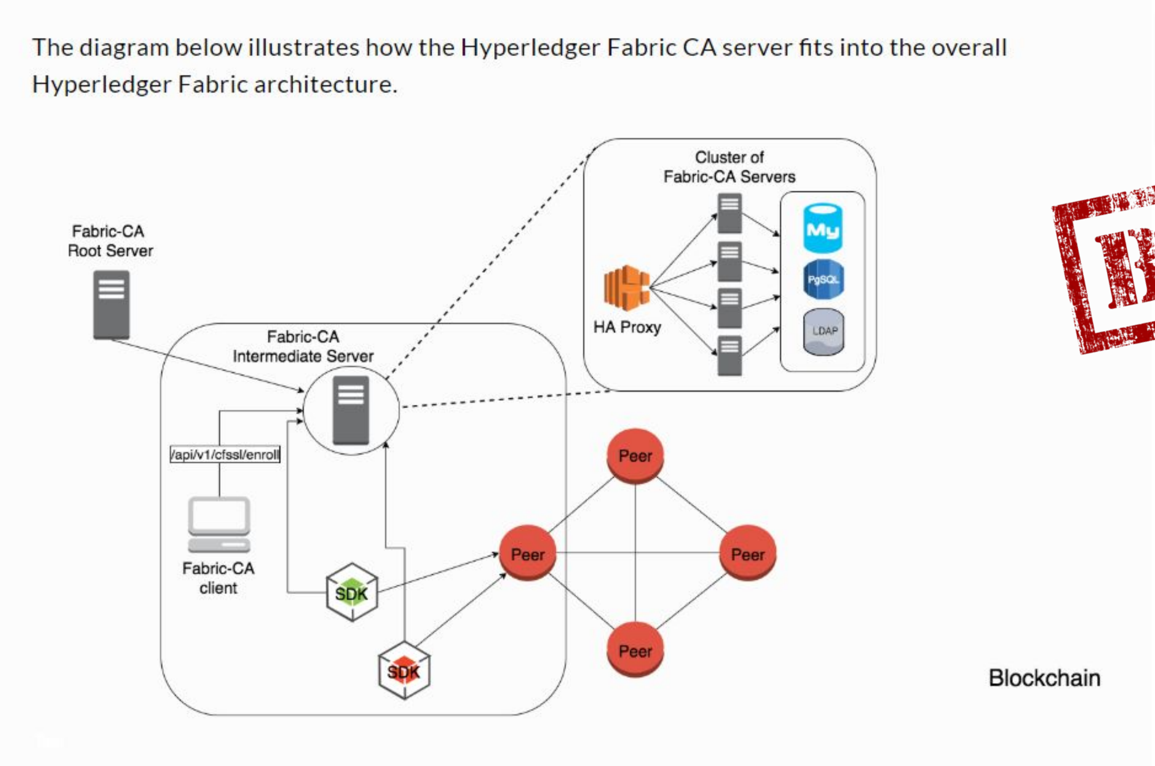
“Some of the technologists at the meeting of the International Standards Organization were surprised when they learned that the head of the Russian delegation, Grigory Marshalko, worked for the F.S.B., the intelligence agency that is the successor to the K.G.B.” – NY Times

What about X.509 certificates?

- You can use certificates in the blockchain
- You create your own!
- Therefore there is no trust in the certificates



Hyperledger Fabric CA

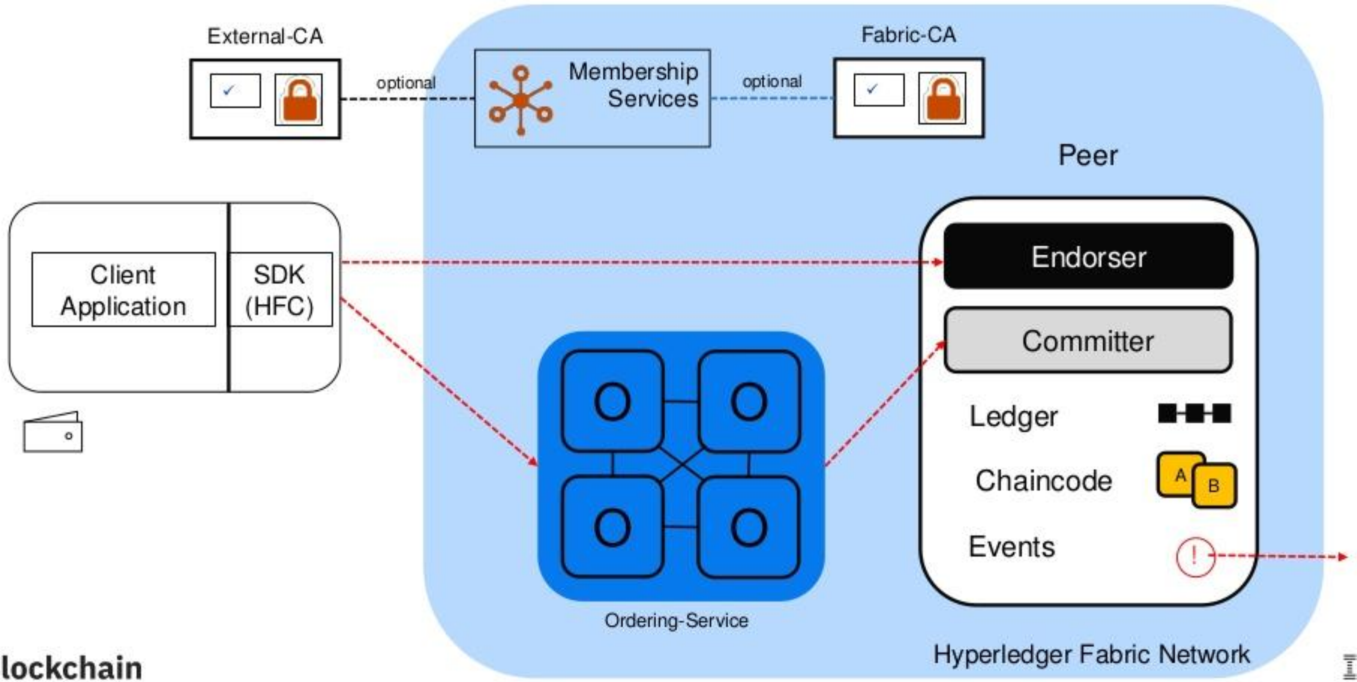


The diagram below illustrates how the Hyperledger Fabric CA server fits into the overall Hyperledger Fabric architecture.

Blockchain will replace PKI

BUSTED!

Hyperledger Fabric V1 Architecture



IBM **Blockchain**

Public Blockchains (Permissionless)

- Anyone can join blockchain
- Anyone can add data such as pictures or illegal content to the blockchain, and this will be on the miner and full node computers.
    - Links to Child Porn – problem is every mining device on the blockchain has a copy of the entire blockchain
    - For example law enforcement could say you have child porn when all you are doing is mining some bitcoin
- Not GDPR compliant – when info is leaked on a public blockchain there is no way to delete it

Private Blockchains (Permissioned)

Blockchain will replace DBs

BUSTED!

Cygnacom Solutions

- Publishing blocks must be authorized by some authority
- Companies are using Permissioned Blockchain in a Consortium
- Using with Backend databases to tie to the distributed ledger
- Certificates signed by trusted Certification Authority tied to blockchain user or to individual transaction
- IBM and AWS is using Linux Foundation Hyperledger

Use Permissioned for Business

Blockchain for Business

Cygnacom Solutions

- Permissioned
- IAM
- X.509 certificates using trusted CA hierarchy
- DDOS – Less likely to take down whole blockchain since it's distributed
- Availability built into the blockchain > data is stored on full nodes
- Unauthorized change to code all nodes will be alerted via hash failures
- All nodes ensure good entropy > use servers and stored in secured location

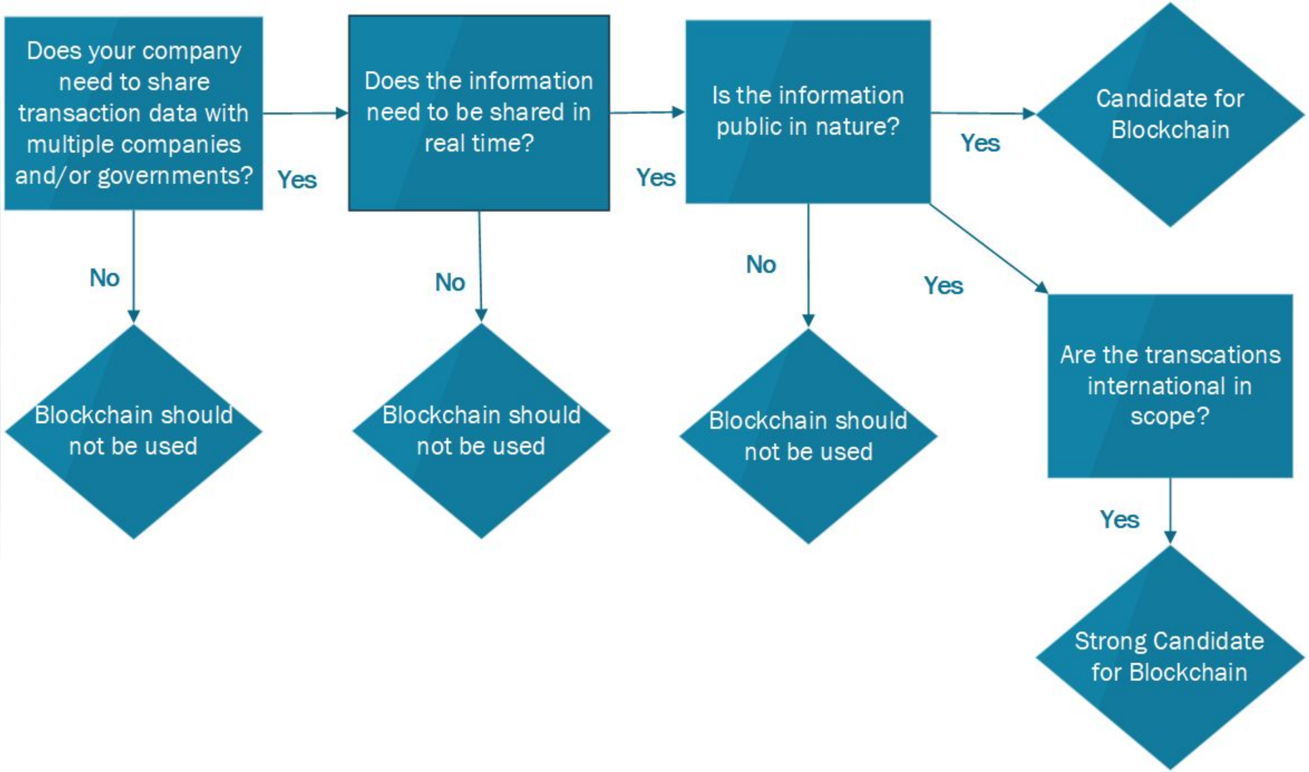
Blockchain is DDOS proof

BUSTED!

How is blockchain going to impact my business?

- May be asked to participate in a consortium where permissioned blockchain will be used
  - Ex. JP Morgan’s intra and inter bank transactions blockchain
- May want to accept payment or pay in bitcoin or another alternate currency

Should I use Blockchain?



Does your company need to share transaction data with multiple companies and/or governments?

Yes

No

Blockchain should not be used

Does the information need to be shared in real time?

Yes

No

Blockchain should not be used

Is the information public in nature?

Yes

Candidate for Blockchain

No

Blockchain should not be used

Yes

Are the transcations international in scope?

Yes

Strong Candidate for Blockchain

Questions???

References

- www.bitcoin.org
- Mastering Blockchain by Imran Bashir
- Coursera - Princeton’s blockchain course “Bitcoin and Cryptocurrency Technologies” >> Best Resource
- Yaga, Dylan, et al. “Blockchain Technology Overview.” *NISTIR 8202, Blockchain Technology Overview* , NIST, 3 Oct. 2018, csrc.nist.gov/publications/detail/nistir/8202/final.
- https://CryptoDoneRight.org
- Blockchain for Dummies 2nd Limited Edition by Manav Gupta
- https://www.theregister.co.uk/2018/11/30/blockchain_study_finds_0_per_cent_success_rate/
- https://thenextweb.com/hardfork/2018/11/29/blockchain-cryptocurrency-arisebank-prison/

Cygnacom Solutions

Is Blockchain Quantum safe?

- Hashing SHA-256 and Symmetric Encryption (AES) are Quantum Resistant.
- The weakness is in the Asymmetric Encryption ECDSA.
- The private key could be discovered via the public key