THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Business Information Security

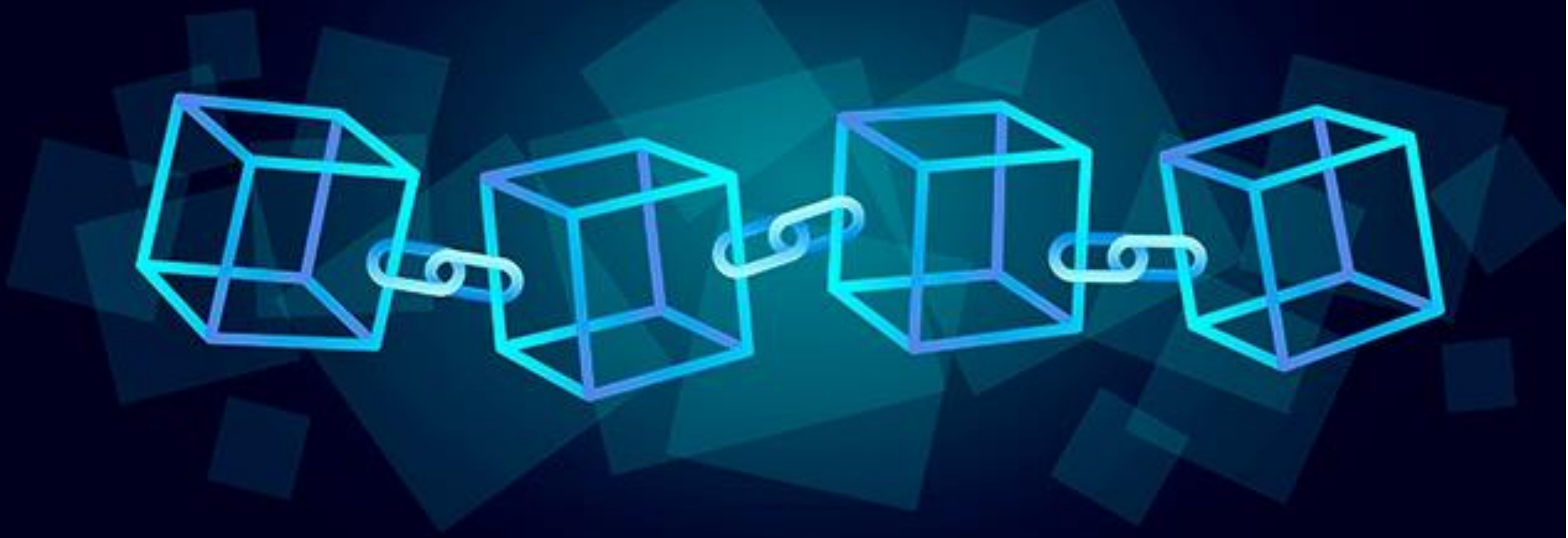
Week 11:

- Blockchain - Theory & Practice

Dr Alex Pudmenzky

Semester 2, 2024

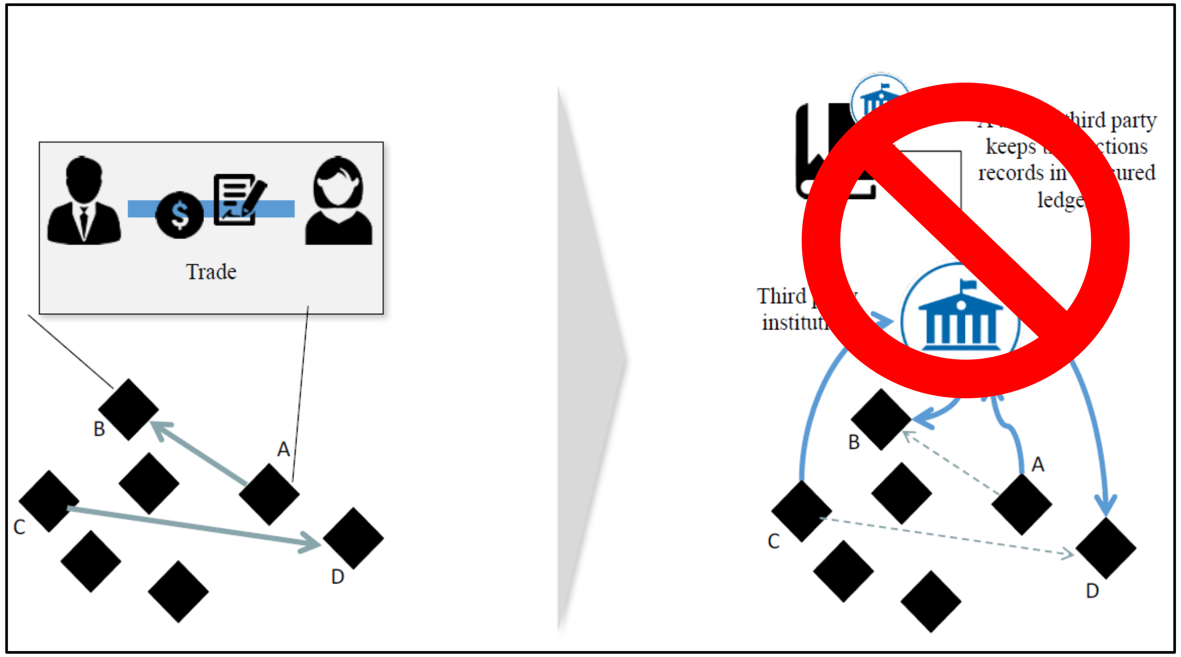
Blockchain & Cryptocurrencies



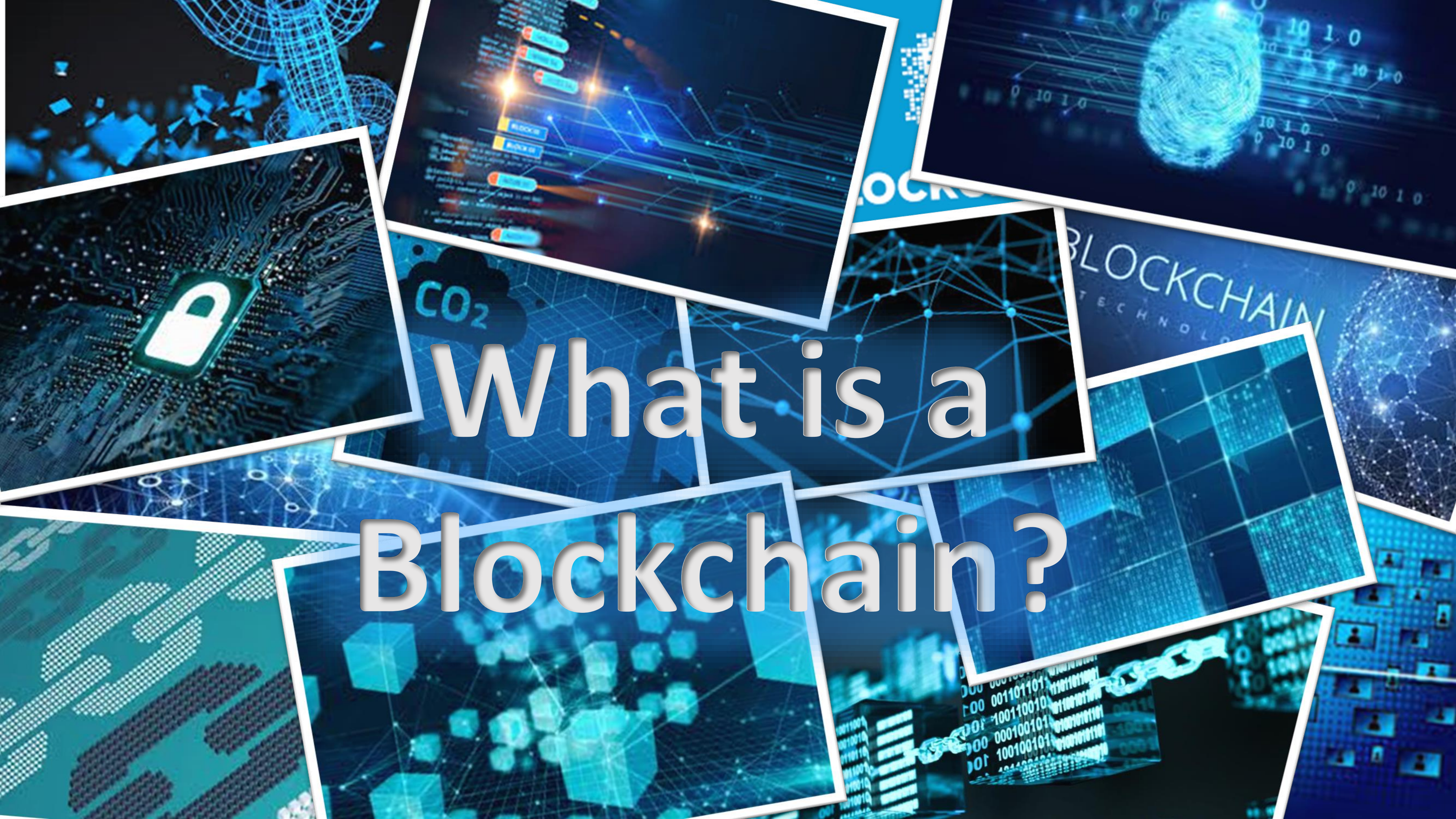
Dr Alex Pudmenzky

Overview

- Definition
- History
- Blockchain vs Database
- Key Features of Blockchain Technology
- Applications
- Double Spend Problem
- How to Trust the Data?
- What is a *hash*?
- What is a *nonce*?
- What is PoW?
- Putting it all together
- Summary



https://www.reply.com/solidsoft-reply/en/content/blockchain-an-overview



What is a Blockchain?

What is a Blockchain?

A digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network. *also :* the technology used to create such a database.

https://www.merriam-webster.com/dictionary/blockchain

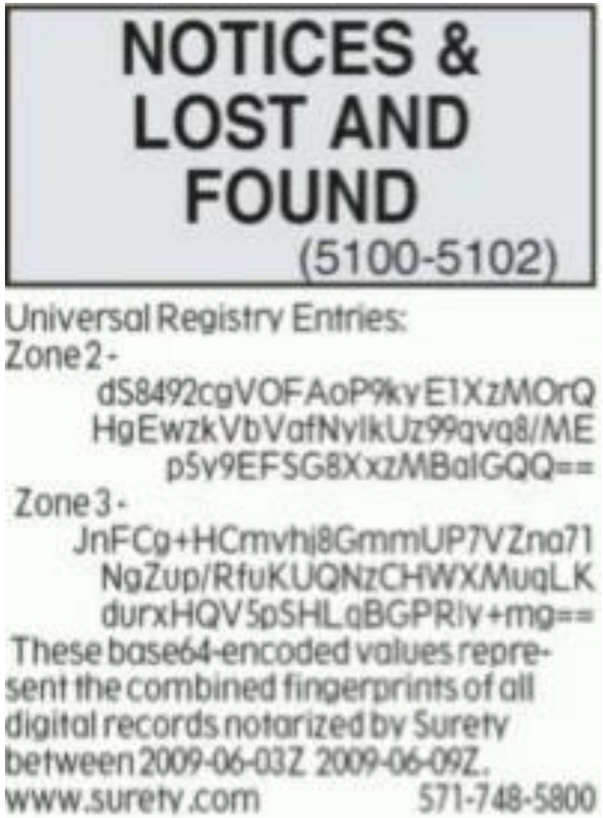
A blockchain is a digital record of transactions. The name comes from its structure, in which individual records, called blocks, are linked together in a single list, called a chain. Blockchains are used for recording transactions made with cryptocurrencies, such as Bitcoin, and have many other applications.

https://techterms.com/definition/blockchain

TEDx
Blockchain: Decentralization is Central | Stuart Haber | TEDxBeaconStreet

Watch this YouTube video now: https://youtu.be/AmQyJoTdnwo (12:27)

Stuart Haber Co-Inventor of Blockchain



NOTICES & LOST AND FOUND
(5100-5102)

Universal Registry Entries:
Zone 2 -
dS8492cgVOFAoP9kyE1XzMOrQ
HgEwzkVbVafNylkUz99qvq8/ME
p5y9EFSG8XxzMBalGQQ==
Zone 3 -
JnFCg+HCmvhj8GmmUP7VZna71
NgZup/RfuKUQNzCHWXMuqLK
durxHQV5pSHLqBGPRIy+mg==

These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 2009-06-03Z 2009-06-09Z.

www.surety.com 571-748-5800

Haber, S., Stornetta, W.S. How to time-stamp a digital document. *J. Cryptology* **3,** 99–111 (1991). https://doi.org/10.1007/BF00196791

Satoshi Nakamoto

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 hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

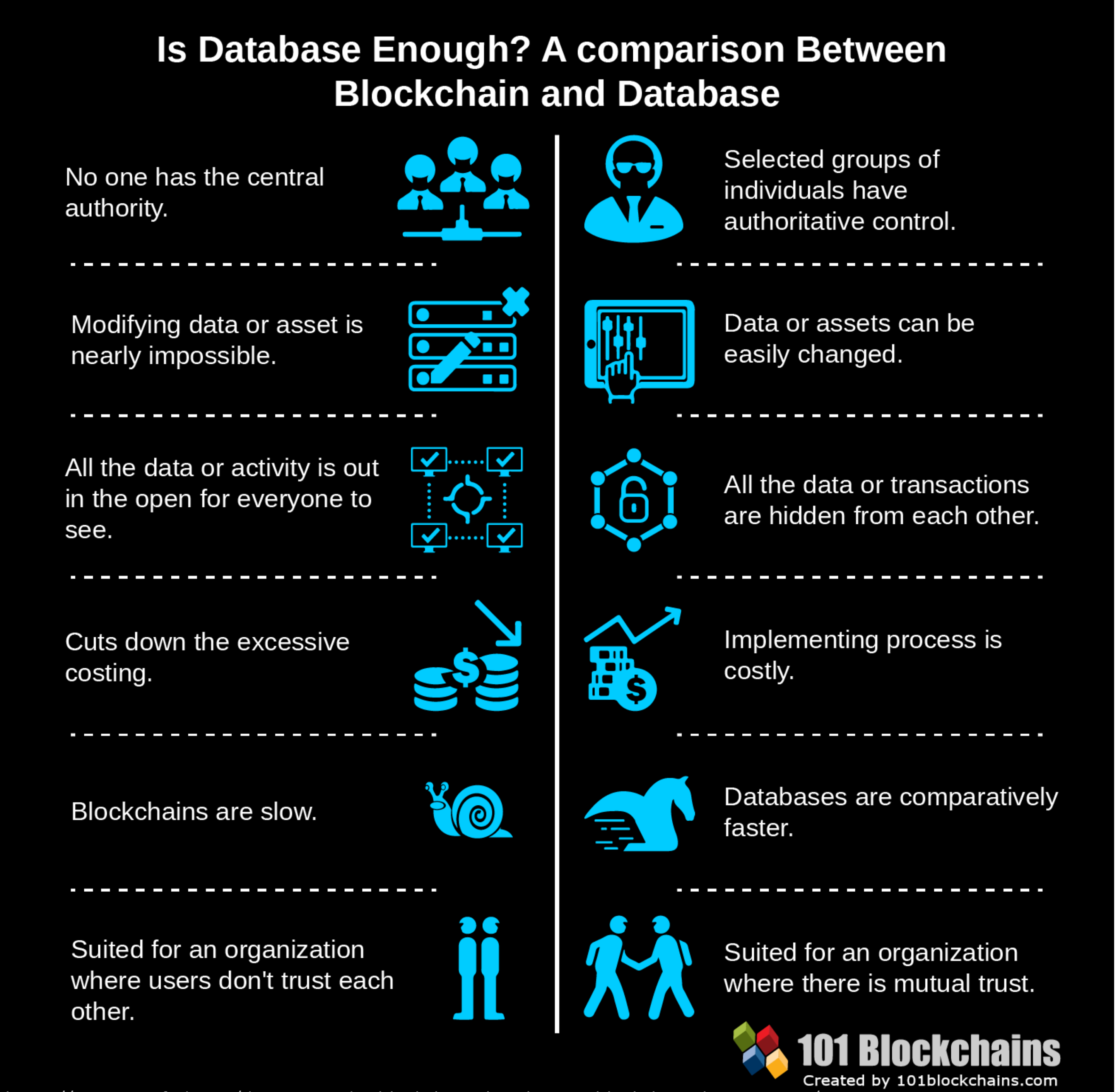
Oct. 31, 2008

https://bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

https://www.huffpost.com/entry/the-mysterious-disappeara_2_b_7217206

?



Is Database Enough? A comparison Between Blockchain and Database

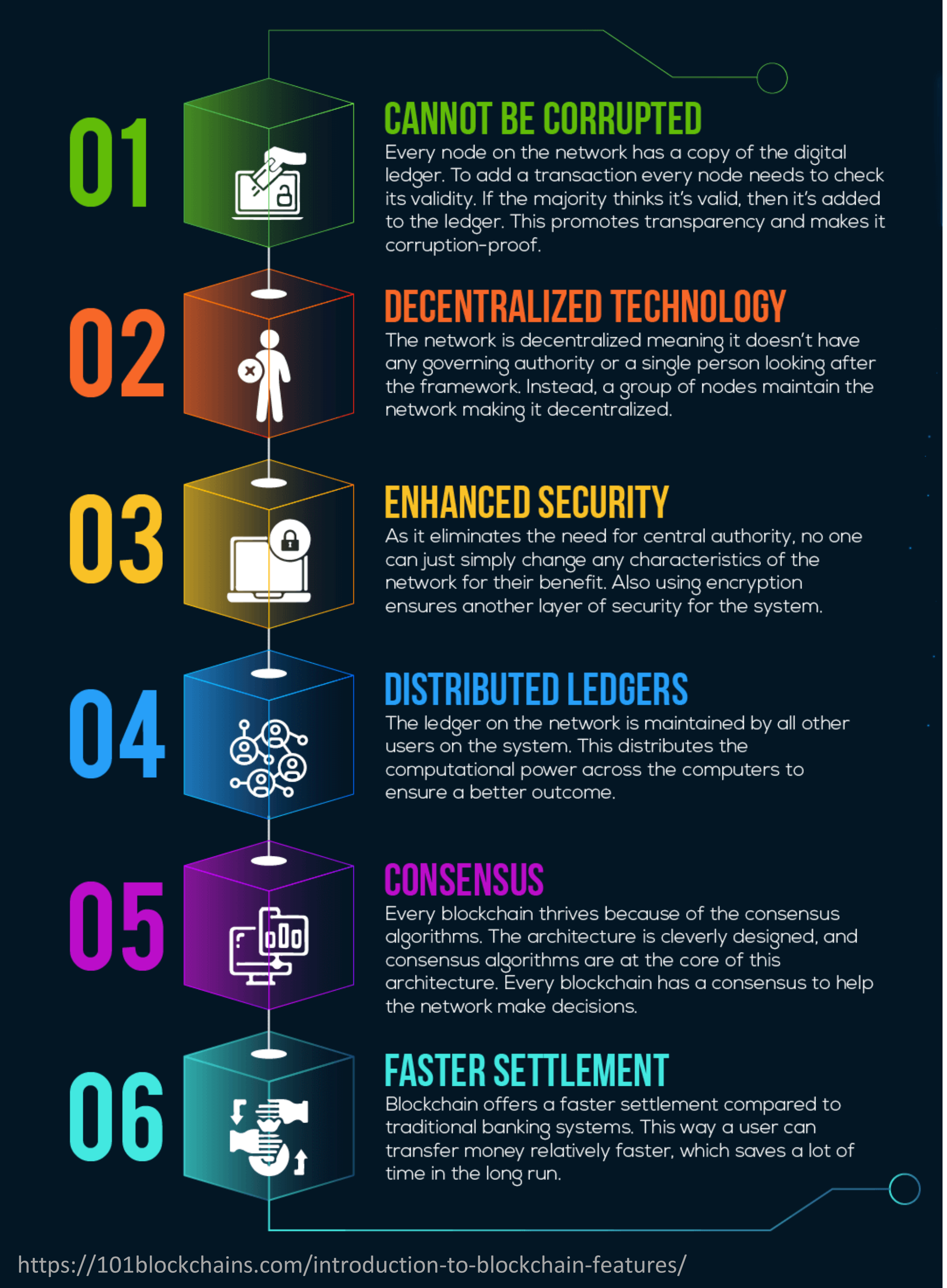
No one has the central authority.	Selected groups of individuals have authoritative control.
Modifying data or asset is nearly impossible.	Data or assets can be easily changed.
All the data or activity is out in the open for everyone to see.	All the data or transactions are hidden from each other.
Cuts down the excessive costing.	Implementing process is costly.
Blockchains are slow.	Databases are comparatively faster.
Suited for an organization where users don't trust each other.	Suited for an organization where there is mutual trust.

101 Blockchains
Created by 101blockchains.com

https://www.rmafed.com/do-you-need-a-blockchain-the-ultimate-blockchain-decision-tree/

Blockchain vs Database

Key Features of Blockchain Technology



01 **CANNOT BE CORRUPTED**

Every node on the network has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof.

02 **DECENTRALIZED TECHNOLOGY**

The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework. Instead, a group of nodes maintain the network making it decentralized.

03 **ENHANCED SECURITY**

As it eliminates the need for central authority, no one can just simply change any characteristics of the network for their benefit. Also using encryption ensures another layer of security for the system.

04 **DISTRIBUTED LEDGERS**

The ledger on the network is maintained by all other users on the system. This distributes the computational power across the computers to ensure a better outcome.

05 **CONSENSUS**

Every blockchain thrives because of the consensus algorithms. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.

06 **FASTER SETTLEMENT**

Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster, which saves a lot of time in the long run.

https://101blockchains.com/introduction-to-blockchain-features/

Applications

Blockchain is starting to disrupt many industries in the next 5 to 10 years

Banking and payments
- Bitcoin - https://bitcoin.org/
- Abra - https://www.goabra.com/

Cyber Security

Supply Chain Management
- Provenance - https://www.provenance.org/
- Fluent (Rebranded to Hijro) - https://hijro.com/
- SKUChain - https://skuchain.com/
- Blockverify - http://www.blockverify.io/

Forecasting
- Augur - https://augur.net/

Networking and IoT
- Adept - http://www.coindesk.com/ibm-reveals-p...

Insurance
- Aeternity - https://www.aeternity.com/

Private Tansport and Ride Sharing
- Arcade City - https://arcade.city/
- La'Zooz - http://www.shareable.net/blog/lazooz-...
- Innogy - https://bitcoinmagazine.com/articles/...
- UBS - https://www.ubs.com/microsites/blockc...
- ZF - http://www.econotimes.com/UBS-bank-in...

Cloud Storage
- Online Data Storage Storj - https://storj.io/
- IPFS - https://ipfs.io/

Charity
- BitGive Foundation - https://bitgivefoundation.org/

Voting
- Democracy Earth - http://democracy.earth/
- Follow My Vote - https://followmyvote.com/

Government
- Dubai Blockchain Strategy - http://www.smartdubai.ae/dubai_blockc...

Public Benefits
- GovCoin - http://www.businesswire.com/news/home...
- Circles - aboutcircles.com

Healthcare
- Gem - https://gem.co/
- Tierion - https://tierion.com/

Energy Management
- TransactiveGrid - http://transactivegrid.net/

Online Music
- Mycelia - http://myceliaformusic.org/
- Ujo Music - https://ujomusic.com/

Retail
- OpenBazaar - https://www.openbazaar.org/
- OB1 - https://ob1.io/

Real Estate
- Ubitquity - https://www.ubitquity.io/

General
- Consensys - https://consensys.net/about/
- Ethereum - https://www.ethereum.org/

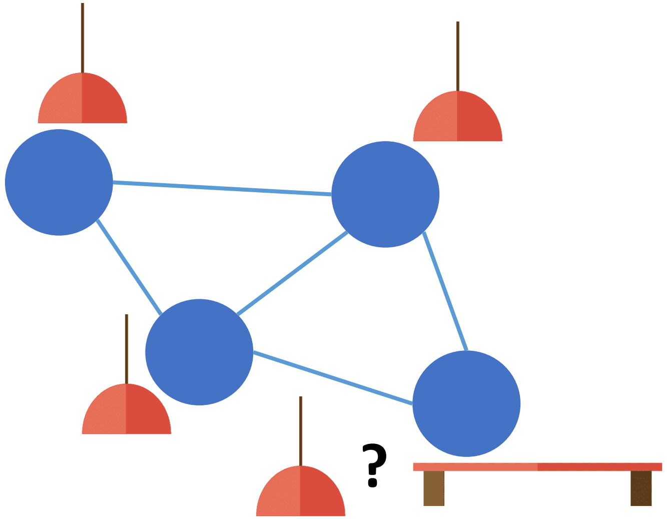
https://www.youtube.com/watch?v=G3psxs3gyf8

Double Spend Problem in a Distributed Ledger

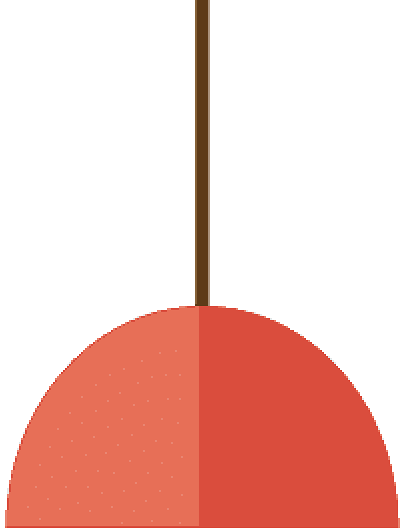
Ann has $100 and she wants to buy a lamp and a table.
They each cost $100, so she should only be able to buy one item.

No problem in day-to-day transaction since goods and money are exchanged together.

In case of distributed systems Alice broadcasts the transaction on the network so that every node on the network is made aware that “Alice has used up $100 to buy a lamp”.



This is the double spend problem

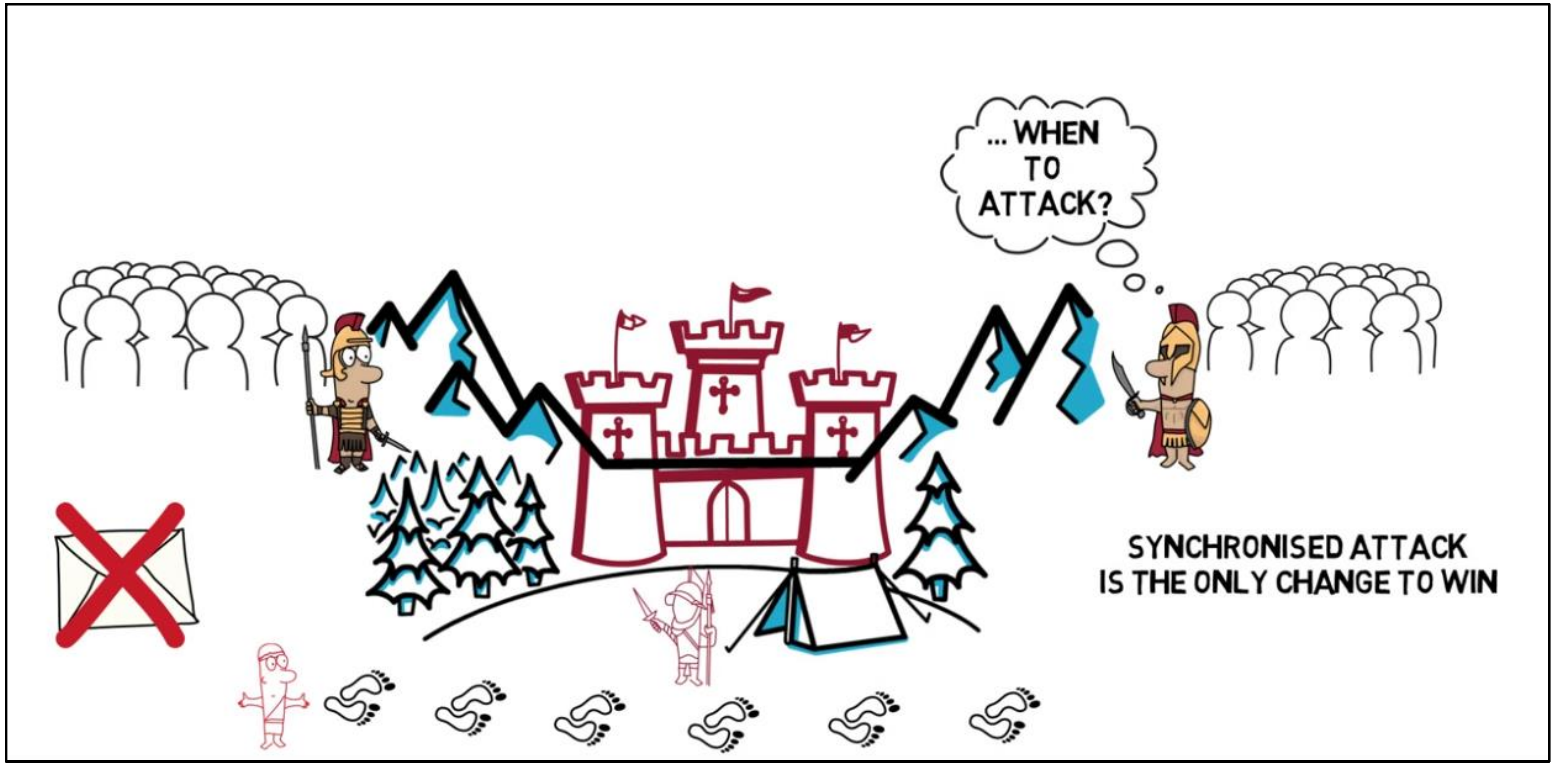


How to
Trust the Data?

"The truth isn't a thing of fact or reason. It is simply what everyone agrees on."
Gregory Maguire, *Wicked: The Life and Times of the Wicked Witch of the West*

Two General's Problem (1975)

Watch this YouTube video now:
https://www.youtube.com/watch?v=s8Wbt0b8



The Two Generals' Problem and its impossibility proof was first published by E. A. Akkoyunlu, K. Ekanadham, and R. V. Huber in 1975 in "Some Constraints and Trade-offs in the Design of Network Communications", p. 67 in the context of communication between two groups of gangsters.

Byzantine Generals Problem (1982)

Generalisation of the Two Generals' Problem
https://www.youtube.com/watch?v=dfsRQyYXOsQ

Byzantine Faults are the most severe and difficult to deal with. Byzantine Fault Tolerance has been needed in airplane engine systems, nuclear power plants and pretty much any system whose actions depend on the results of a large amount of sensors. Even SpaceX was considering it as a potential requirement for their systems.

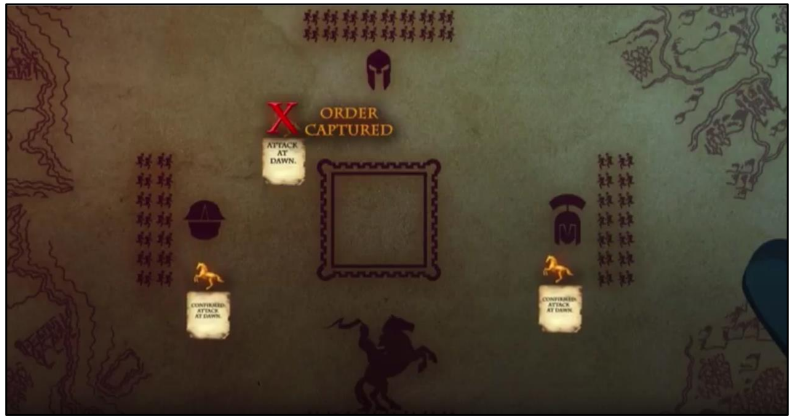
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.126.9525&rep=rep1&type=pdf

Proof of Work (PoW)

Cryptography Mailing List

Bitcoin P2P e-cash paper
2008-11-13 22:56:55 UTC
James A. Donald wrote:
> It is not sufficient that everyone knows X. We also
> need everyone to know that everyone knows X, and that
> everyone knows that everyone knows that everyone knows X
> - which, as in the Byzantine Generals problem, is the
> classic hard problem of distributed data processing.

https://satoshi.nakamotoinstitute.org/emails/cryptography/11/

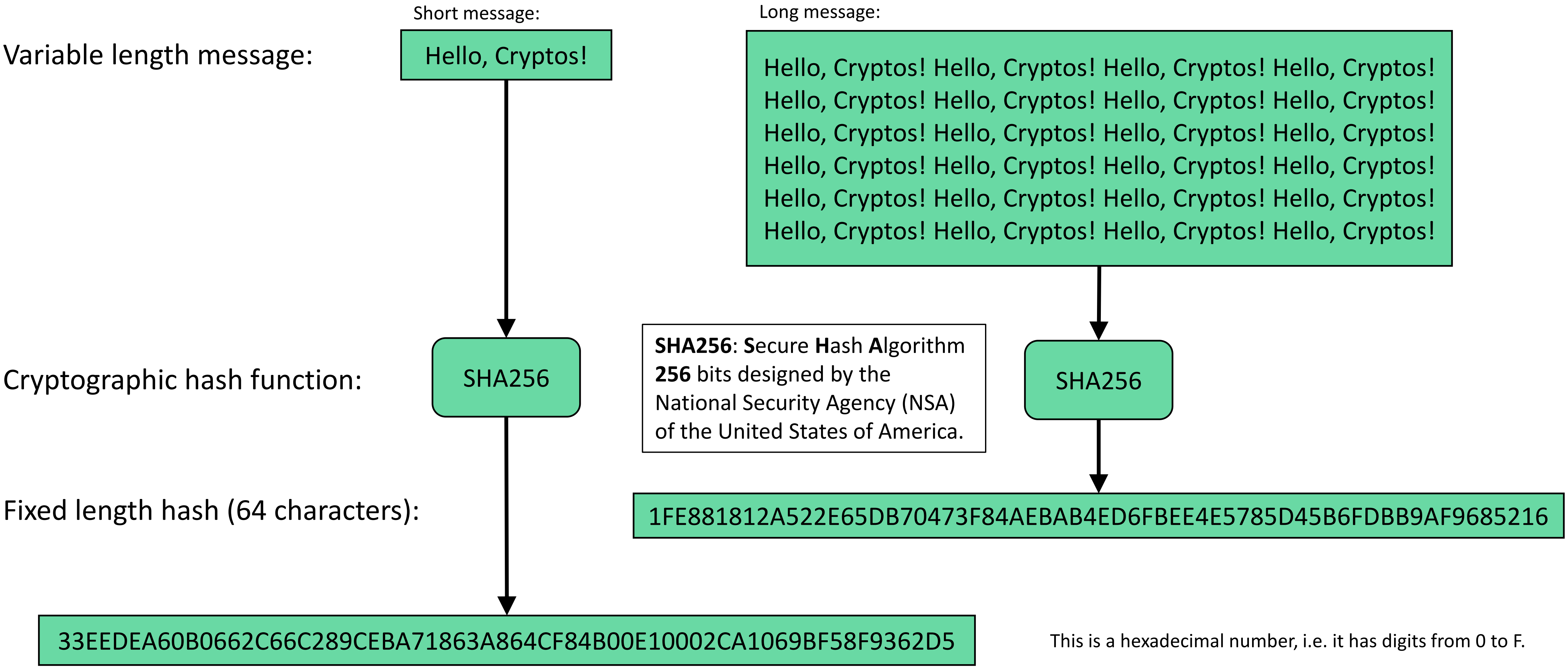


Proof of Work like proposed by Satoshi doesn't solve the *Two Generals Problem* or the more generic *Byzantine Generals Problem*. It's a probabilistic solution to the Byzantine Generals Problem, which means the confidence that a consensus is reached is growing with every block added to the chain, but it never reaches 100%.
https://ethereum.stackexchange.com/questions/40213/how-is-the-two-generals-problem-solved-with-proof-of-work

Hashing

Generates fixed length fingerprints of arbitrarily large messages.

An example



Variable length message:

Short message:

Hello, Cryptos!

Long message:

Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!
Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!
Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!
Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!
Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!
Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!

Cryptographic hash function:

SHA256: **S**ecure **H**ash **A**lgorithm **256** bits designed by the National Security Agency (NSA) of the United States of America.

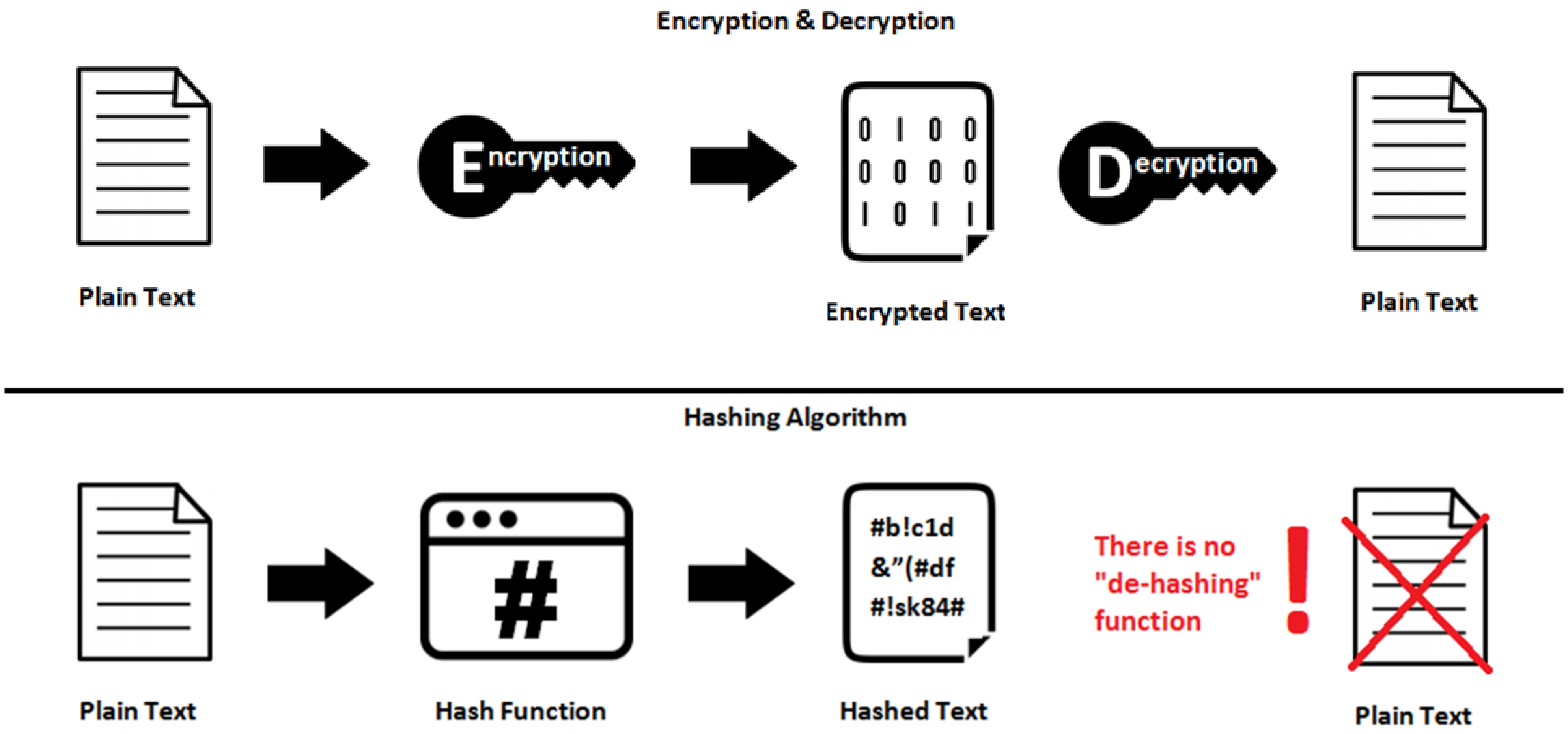
Fixed length hash (64 characters):

1FE881812A522E65DB70473F84AEBAB4ED6FBEE4E5785D45B6FDBB9AF9685216

33EEDEA60B0662C66C289CEBA71863A864CF84B00E10002CA1069BF58F9362D5

This is a hexadecimal number, i.e. it has digits from 0 to F.

Hashing vs Encryption

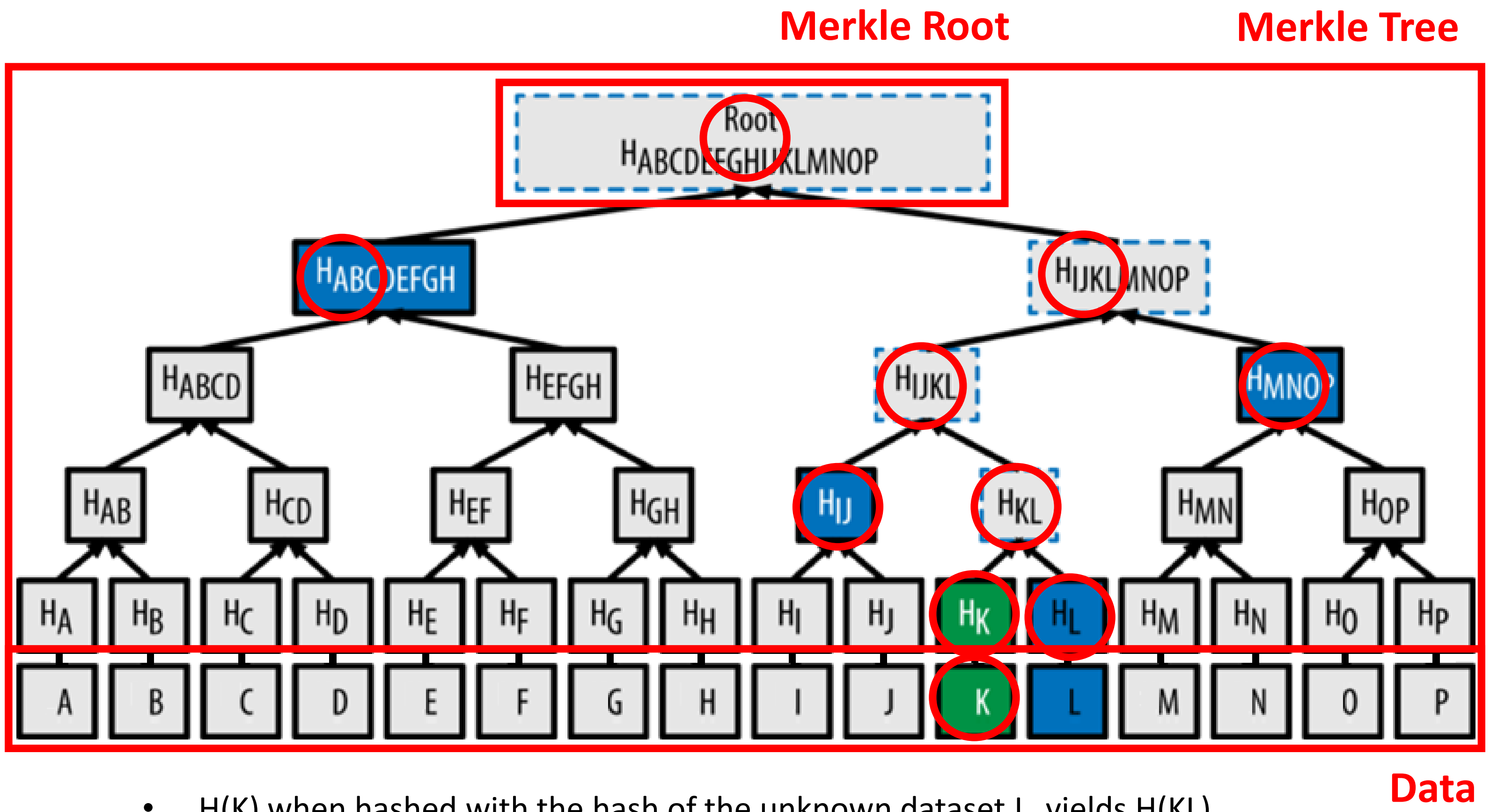


Encryption is a two-way function that includes encryption and decryption

Hashing is a one-way function that changes a plain text to a unique digest that is irreversible

https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption

Merkle Trees



Merkle trees are named after Ralph Merkle, who proposed them in a 1987 paper titled "A Digital Signature Based on a Conventional Encryption Function." Merkle also invented cryptographic hashing.

In order to verify the inclusion of data [K], in the merkle tree root, we use a one way function to hash [K] to obtain H(K).
In order to validate the inclusivity of K, K doesn't have to be revealed, similarly the hash of data L can be revealed without any implicit security repercussions and so on.

- H(K) when hashed with the hash of the unknown dataset L, yields H(KL)
- H(KL) hashed with H(IJ) leads to H(IJKL)
- H(IJKL) hashed with H(MNOP) leads to H(IJKLMNOP)
- H(IJKLMNOP) when hashed with H(ABCDEFGH) yields H(ABCDEFHGIJKLMNOP) - which happens to be our publically available merkle root

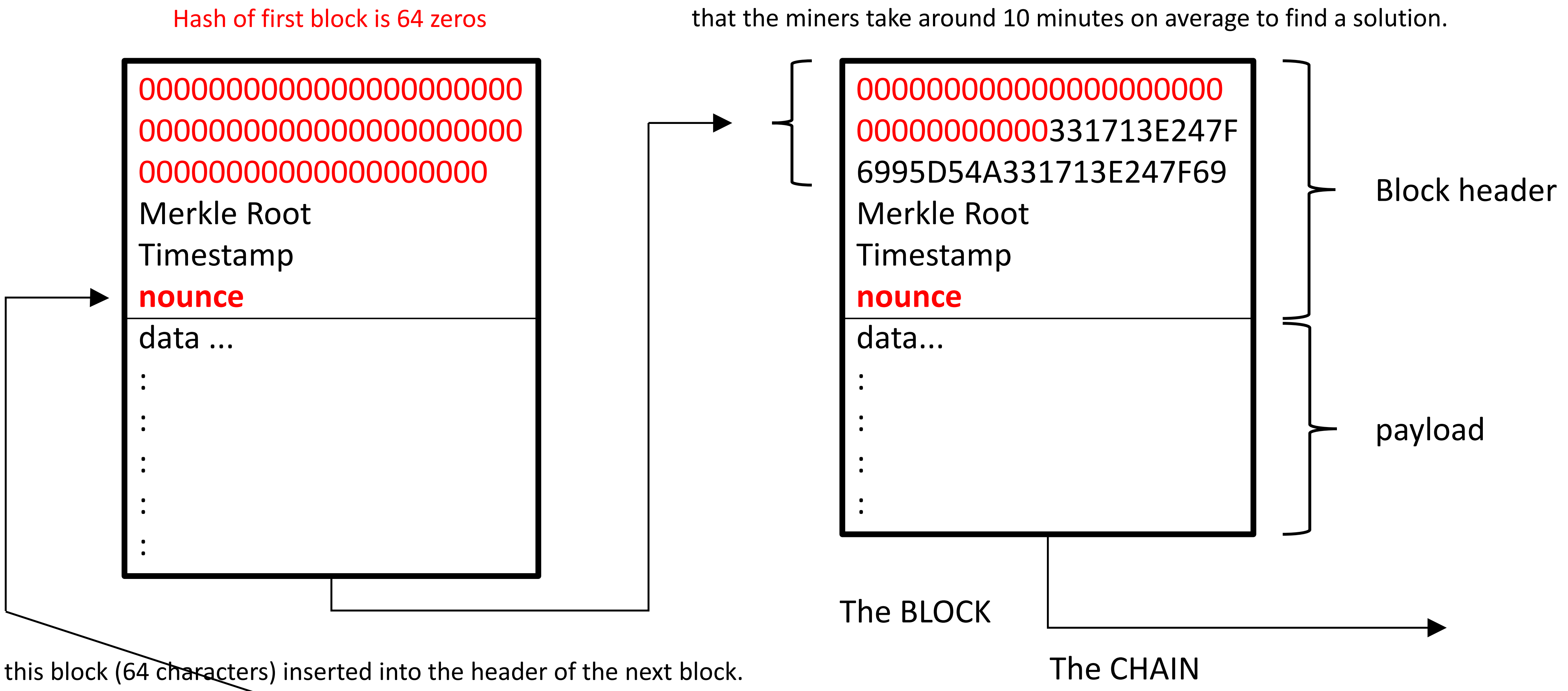
We've hence proven that the data set K is indeed present in our merkle tree by making use of H(L), H(IJ), H(MNOP) and H(ABCDEFGH) without having to reveal K or any of the data. In order to obtain a merkle proof of H, we need H(L), H(IJ), H(MNOP) and H(ABCDEFGH) with which we can together obtain H(ABCDEFHGIJKLMNOP) hence proving that H(K) was part of the merkle tree implying that data set K was indeed part of the universal dataset [A, B, C, … , N, O, P].

https://medium.com/crypto-0-nite/merkle-proofs-explained-6dd429623dc5

The golden nounce

A nonce (“number used once”) is a 32-bit (4-byte) unsigned integer (0 to 2^32-1 = 4,294,967,295)

Hash must start with certain number of zeroes (32 here).
This number of zeroes is the "difficulty" that is adjusted automatically so that the miners take around 10 minutes on average to find a solution.

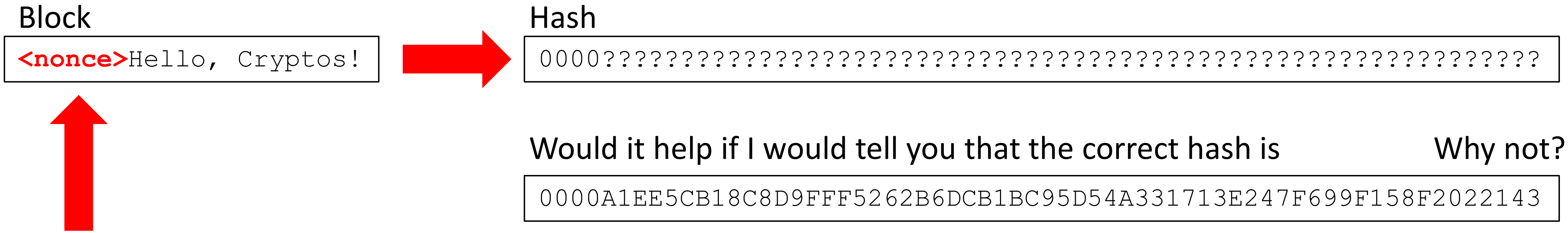


Hash of this block (64 characters) inserted into the header of the next block.
Miners must find a number (nounce) that, when inserted into this block, will create a hash that starts with a certain number of zeros - this is hard!

Try it yourself

Use the website https://passwordsgenerator.net/sha256-hash-generator/ to create a **SHA256** hash that has 4 zeroes at the beginning for the following block: "`Hello, Cryptos`!" by inserting a nonce before the text inside the block.

So, in different words, find a number that, followed by the text "Hello, Cryptos!" results in a hash that starts with "0000".



Block

`<nonce>Hello, Cryptos!`

Hash

`0000????????????????????????????????????????????????????????????`

Would it help if I would tell you that the correct hash is

`0000A1EE5CB18C8D9FFF5262B6DCB1BC95D54A331713E247F699F158F2022143`

Why not?

What is this number?

Try: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ... , 4294967294, 4294967295.

Solution:

26762Hello, Cryptos!

Now imagine doing this with 32 leading zeros!
That's why it's sometimes referred to as a "mathematical puzzle" and
this is **The Proof of Work**!

Proof of Work (PoW)

The essence of the proof of work consensus mechanism is to provide evidence that the majority of nodes agree and do not lie.

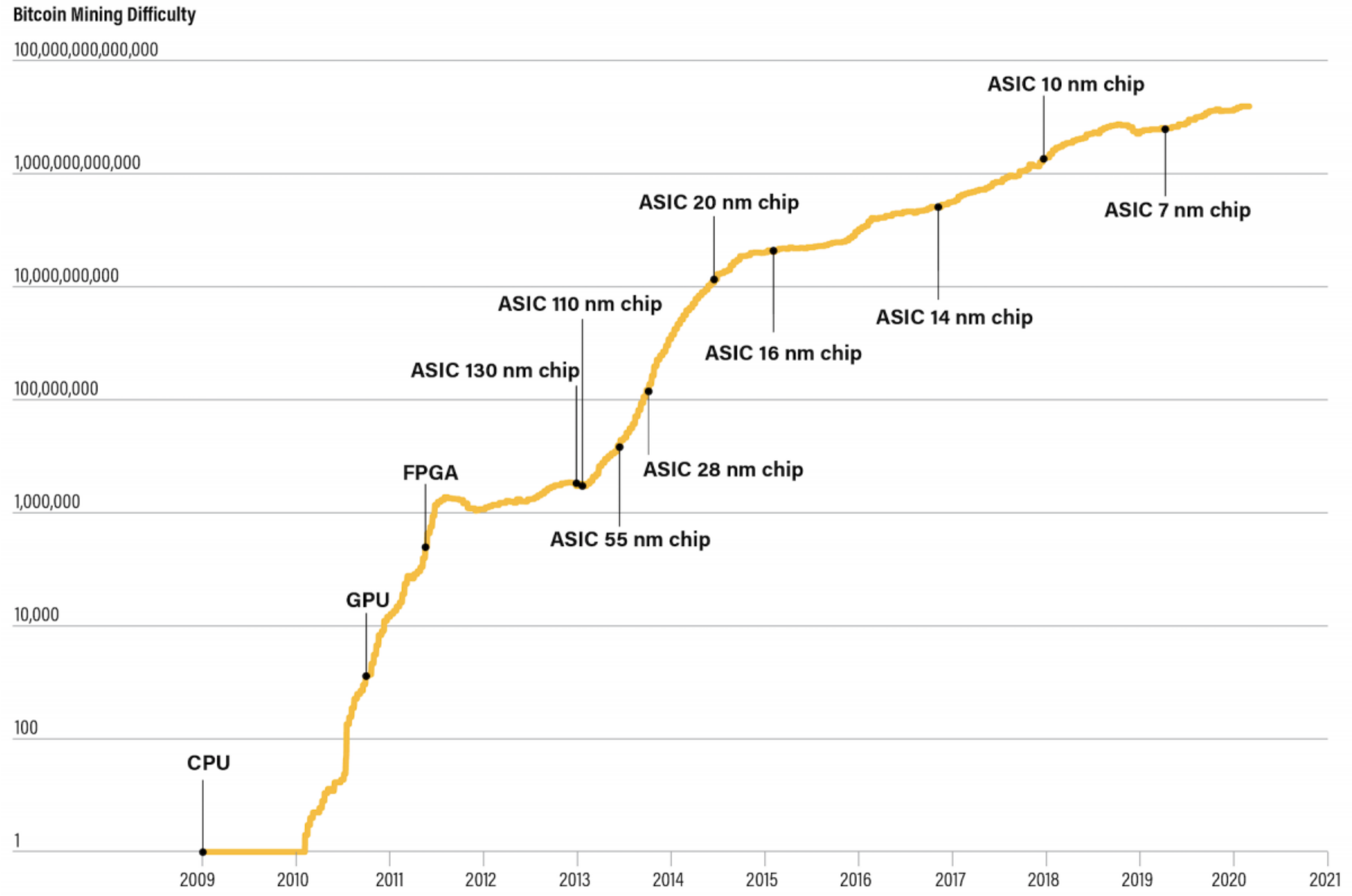
A proof of work verification is difficult, costly, and time-consuming to create, but easy to verify. Bitcoin is secure because it is computationally infeasible to attack the network. Requiring Proof of Work for participation is central to this property. Hence Bitcoin relies on **computational work** on **cryptographic challenges** as the **basis for trust**.

The difficulty is adjusted every 2,016 blocks (two weeks) to keep each miner’s probability of solving the block within the ten-minute interval. This decentralises the verification process across the entire network. This adjustment occurs by the protocol automatically increasing or decreasing the target based on the number of miners.

new_difficulty = old_difficulty * (2016 blocks * 10 minutes) / (the time took in minutes to mine the last 2016 blocks)

https://medium.com/coinmonks/simply-explained-why-is-proof-of-work-required-in-bitcoin-611b143fc3e0

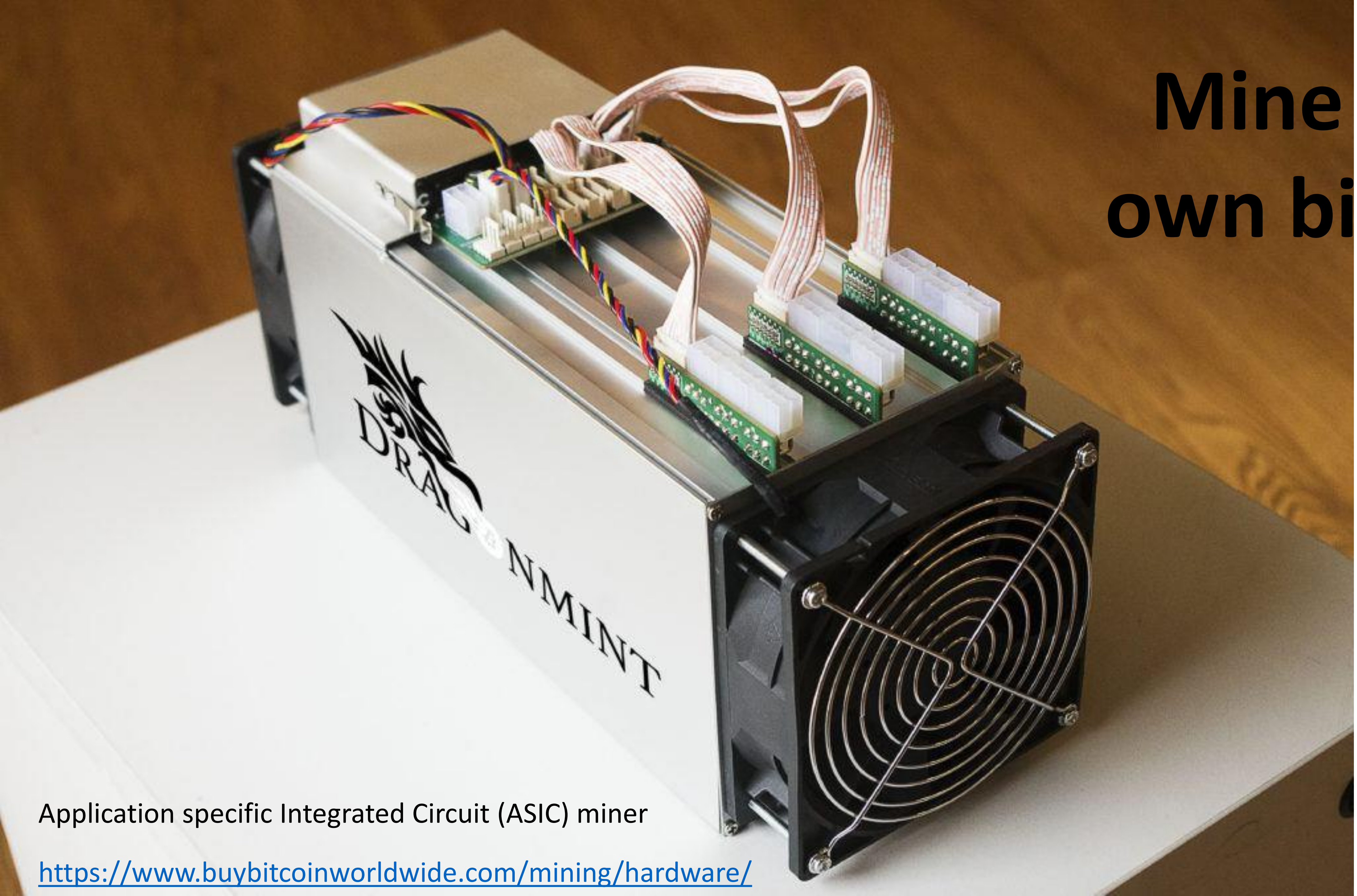
Increase of Difficulty over Time



CPU (central processing unit)
GPU (graphics processor)
FPGA (Field Programmable Gate Arrays)
ASIC (specialized hardware)

https://www.coindesk.com/rise-of-asics-bitcoin-mining-history

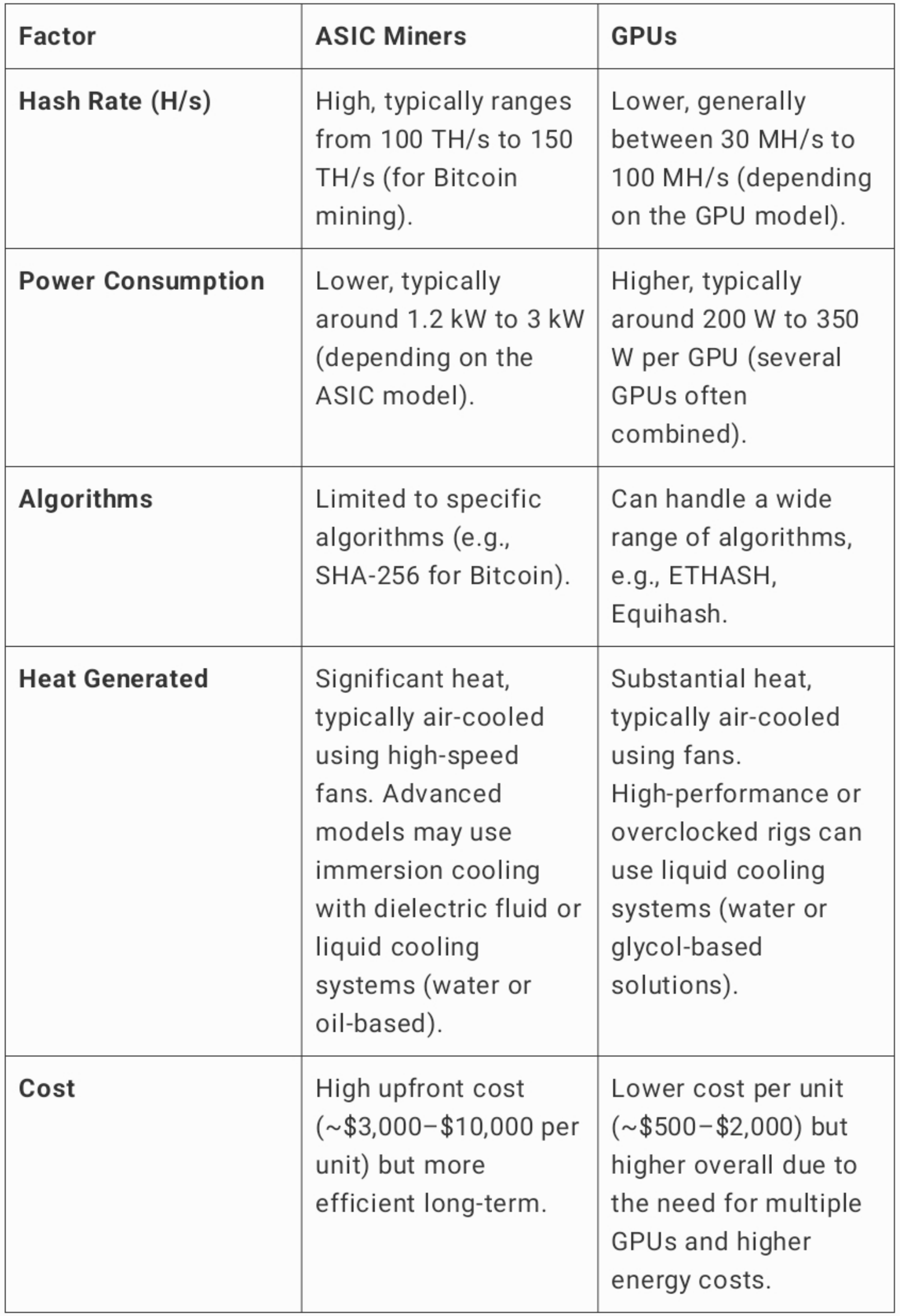
Mine your own bitcoins



Application specific Integrated Circuit (ASIC) miner

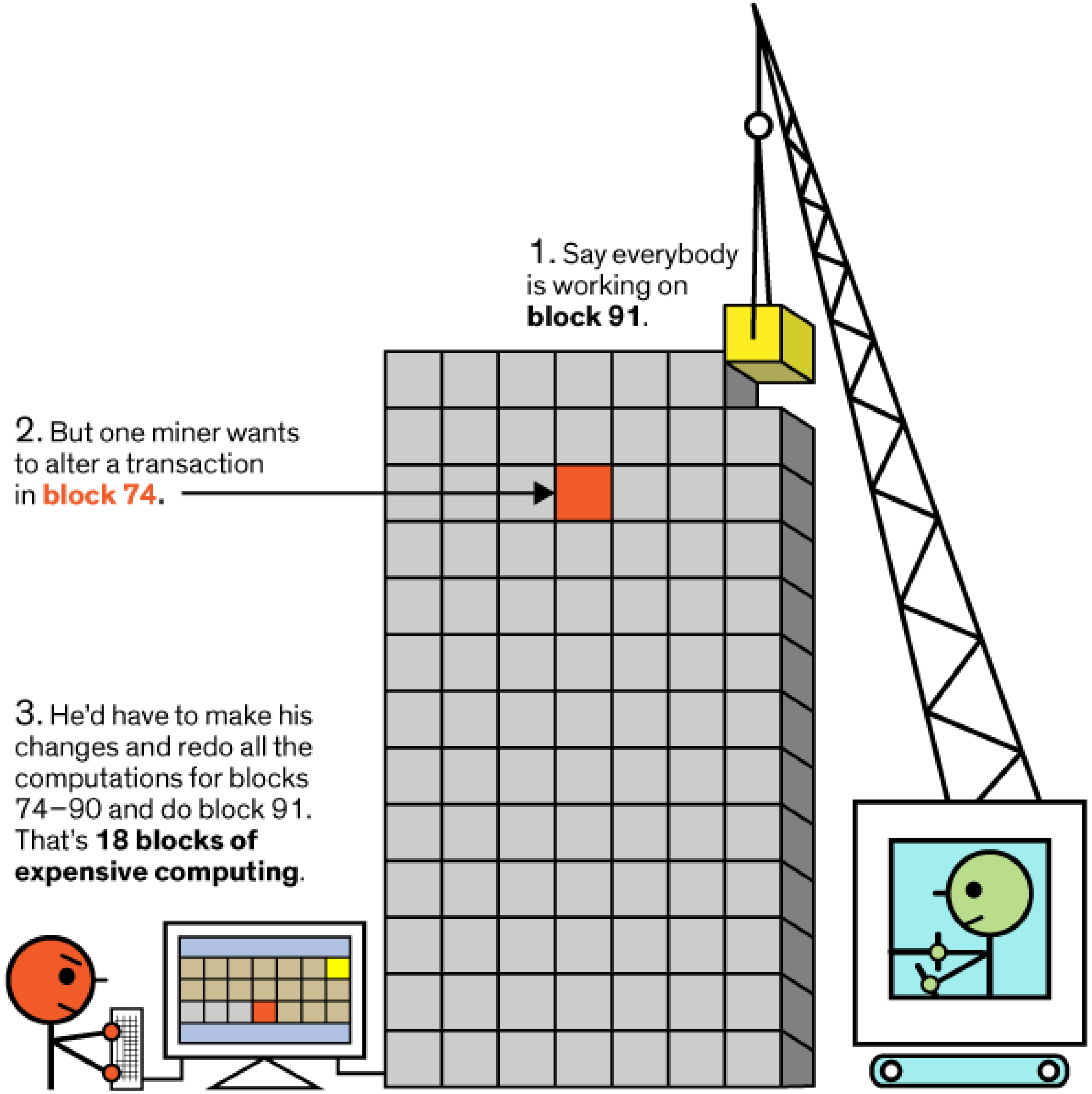
https://www.buybitcoinworldwide.com/mining/hardware/

ASIC vs GPU miners



Factor	ASIC Miners	GPUs
Hash Rate (H/s)	High, typically ranges from 100 TH/s to 150 TH/s (for Bitcoin mining).	Lower, generally between 30 MH/s to 100 MH/s (depending on the GPU model).
Power Consumption	Lower, typically around 1.2 kW to 3 kW (depending on the ASIC model).	Higher, typically around 200 W to 350 W per GPU (several GPUs often combined).
Algorithms	Limited to specific algorithms (e.g., SHA-256 for Bitcoin).	Can handle a wide range of algorithms, e.g., ETHASH, Equihash.
Heat Generated	Significant heat, typically air-cooled using high-speed fans. Advanced models may use immersion cooling with dielectric fluid or liquid cooling systems (water or oil-based).	Substantial heat, typically air-cooled using fans. High-performance or overclocked rigs can use liquid cooling systems (water or glycol-based solutions).
Cost	High upfront cost (~$3,000–$10,000 per unit) but more efficient long-term.	Lower cost per unit (~$500–$2,000) but higher overall due to the need for multiple GPUs and higher energy costs.

Why you can't cheat a bitcoin



1. Say everybody is working on **block 91**.

2. But one miner wants to alter a transaction in **block 74**.

3. He'd have to make his changes and redo all the computations for blocks 74–90 and do block 91. That's **18 blocks of expensive computing**.

4. What's worse, he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they're working on.

ockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb

What is the reward?

The winning miner claims a **block** reward by adding it as a first transaction on the **block**. At inception, each bitcoin **block** reward was worth 50 BTC. The **block** reward is halved after the discovery of every 210,000 **blocks**, which takes around four years to complete. As of February 2019, one **block** reward was worth 12.5 BTC.

In November of 2019, the price of Bitcoin was about $9,300 per bitcoin, which means you'd earn
12.5BTC * $9,300/BTC = **$116,250** for completing a block.

In May 2020, the number of bitcoins (BTC) entering circulation every 10 minutes dropped by half again from 12.5 to 6.25. The next halving will likely occur in 2024.

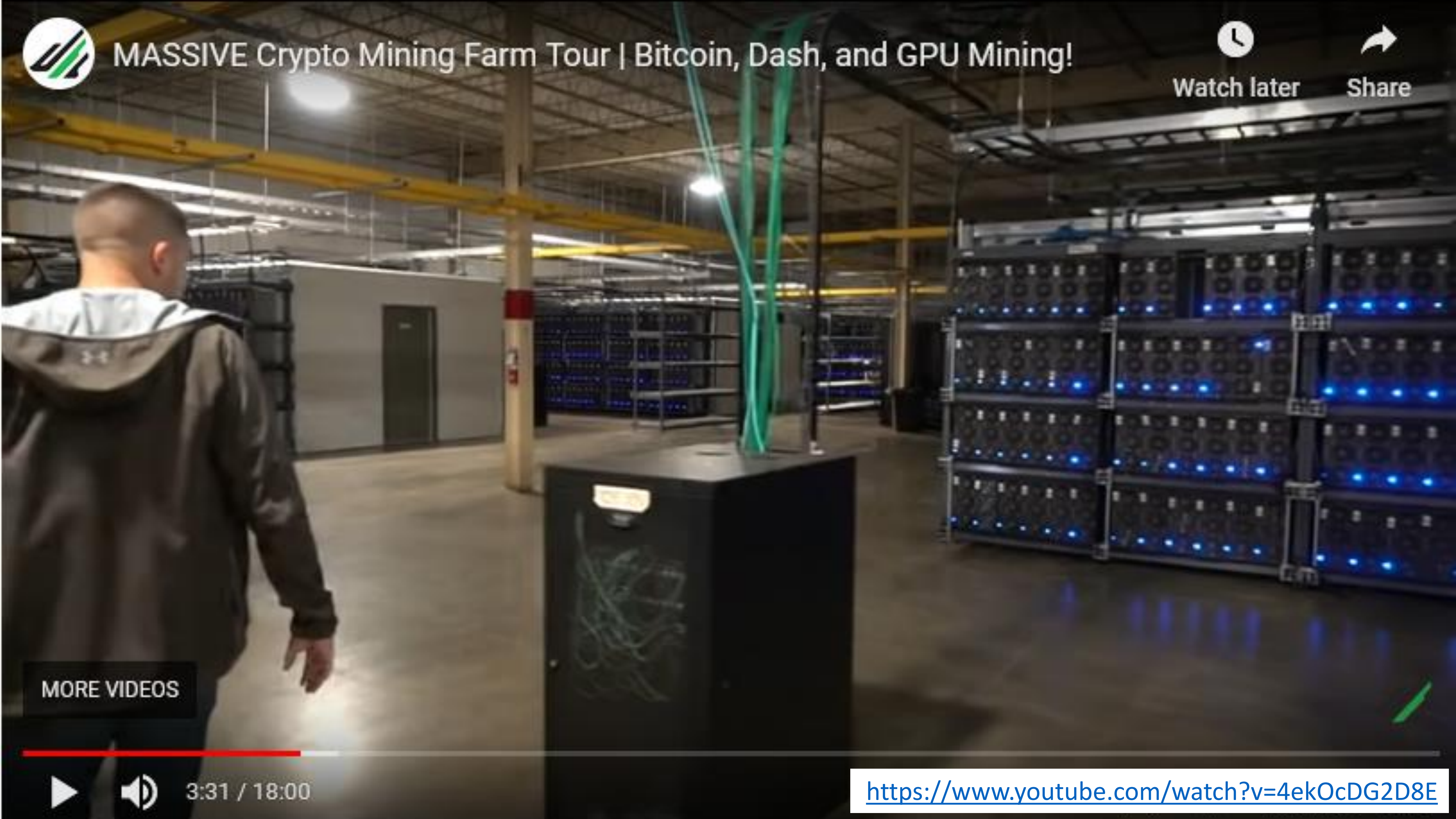
The maximum and total amount of bitcoins that can ever exist is 21 million.

There are 2,512,225.0 bitcoins left to be mined.
When all 21 million bitcoins are mined, there won't be a block reward to pay to miners.

When a Bitcoin user sends a BTC transaction, a small fee is attached. These fees go to miners and this is what will be used to pay miners instead of the block reward.

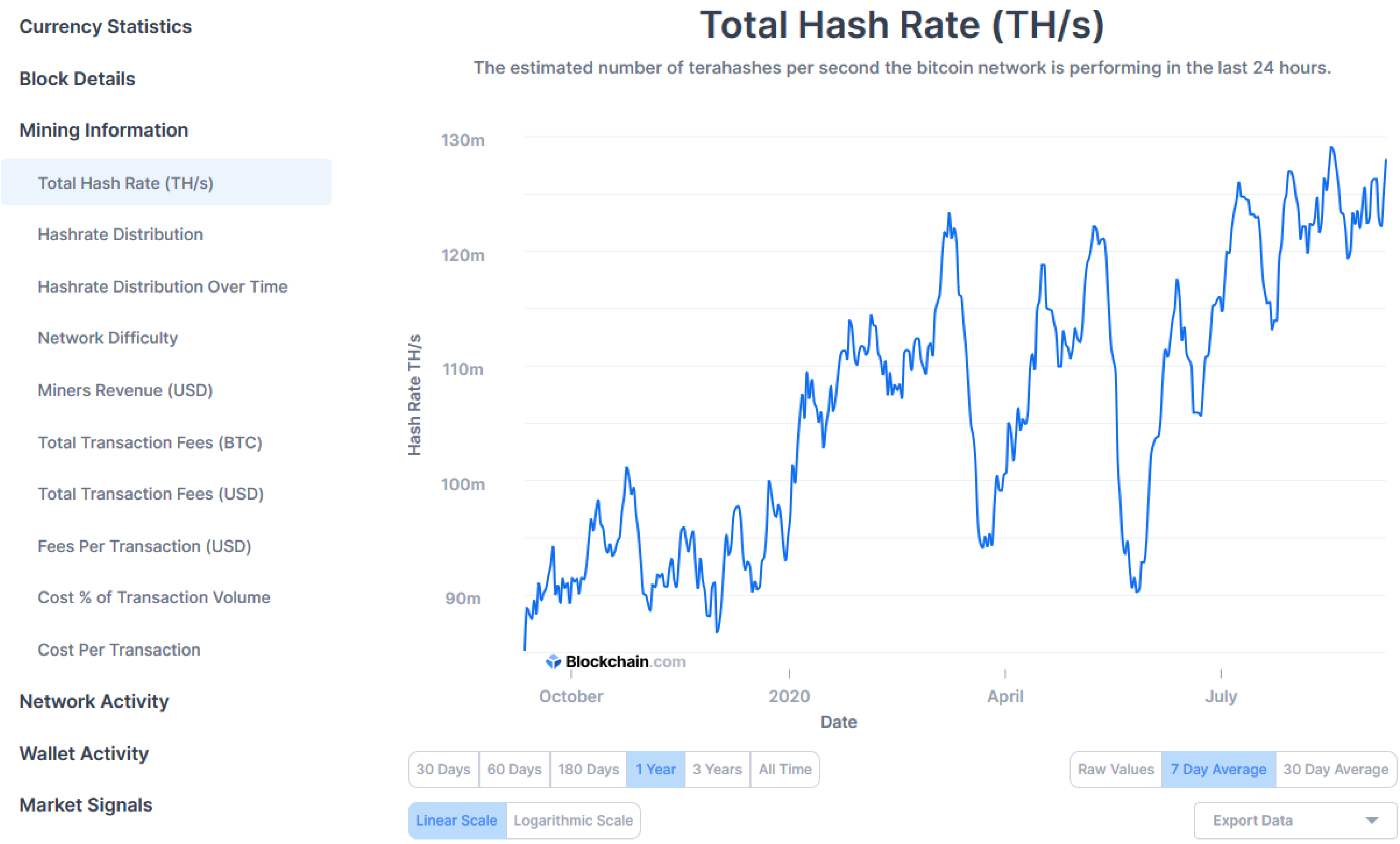
https://www.coindesk.com/bitcoin-halving-explainer

https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/


MASSIVE Crypto Mining Farm Tour | Bitcoin, Dash, and GPU Mining!
Watch later
Share
MORE VIDEOS
3:31 / 18:00

https://www.youtube.com/watch?v=4ekOcDG2D8E

Live Mining Statistics



Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.

https://www.blockchain.com/charts/hash-rate

BLOCKCHAIN
TECHNOLO
CO2
LOCKC

Is it worth it?

Here are some websites that might help you to answer this question.
However, you will need a big computer! How about the CSIRO supercomputer?

https://www.cryptocompare.com/mining/calculator/btc

https://www.buybitcoinworldwide.com/bitcoin-clock/

https://www.bitcoinprice.com/btc/aud/

CSIRO IT contractor spared jail for mining Monero on supercomputer

Intensive correction order imposed for 15 months.

A former CSIRO IT contractor has escaped jail time for using the country’s peak science and research organisation’s supercomputer to mine cryptocurrency.

Jonathon Khoo was sentenced to a 15-month intensive correction order at Sydney’s Downing Centre Local Court on Friday after pleading guilty to the charges.

Khoo was charged by the Australian Federal Police in May 2019 for modifying the computer systems of CSIRO without authorisation to access the processing power.

The charges included unauthorised modification of data to cause impairment and unauthorised modification of restricted data. Magistrate Erin Kennedy on Friday said Khoo had installed and run 2903 command scripts into CSIRO’s two high performance computers (HPC) and the Claymore Dual Miner software.

In doing so, Khoo generated $9,422 worth of cryptocurrency mining proceeds in the form of Ethereum and Monero.

While there was no “impairment to the CSIROs” operations, Kennedy said the use of the systems for period of just over a month in duration reduced the performance of the HPC. She said the HPC was also used by the Royal Australian Navy and Victor Chang Cardiac Research Institute.

CSIRO put the total cost of the HPCs reduced capacity at $76,668, including hardware and software.

Kennedy described the offence as "reckless" with "some level of planning", but acknowledged Khoo's remorse. She also noted that Khoo had admitted his guilt to police almost immediately after a search warrant was executed in 2019.

Khoo was handed a 15-month intensive correction order - a custodial sentence served in the community - with 300 hours of community service.

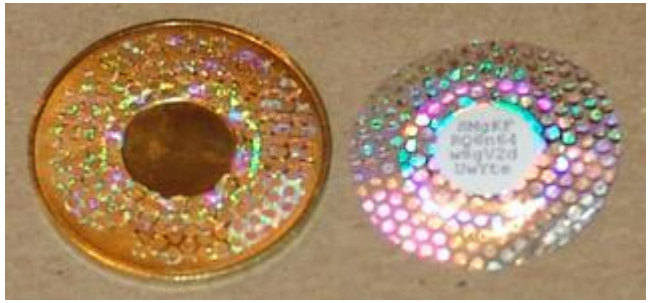
By Justin Hendry
Sep 18 2020 1:15PM
https://www.itnews.com.au/news/csiro-it-contractor-spared-jail-for-mining-monero-on-supercomputer-553535

'Mining' for cryptocurrencies involves solving a complex mathematical problem that requires large amounts of processing power.

Physical Bitcoins?

Casascius physical bitcoins, also called **Casascius coins**, are physical metal coins created by Bitcoin user Casascius (Mike Caldwell, Sandy, Utah, USA) and sold until Nov 26, 2013, that contain an embedded piece of paper with digital Bitcoin value, covered by a tamper-resistant hologram. The coins are designed such that they could be circulated in face-to-face transactions. The first person to redeem its private key gets the value on the coin, and afterwards, the coin no longer has any Bitcoin value. It is difficult or impossible to read the private key on the coin without damaging or destroying the hologram, which exposes a honeycomb-like tamper-evidence pattern when peeled.
https://en.bitcoin.it/wiki/Casascius_physical_bitcoins

Casascius



Redeemed Casascius coin

Mike Caldwell and his Casascius coin. Caldwell started minting his coins a couple of years ago, but late last year he was banned from selling pre-funded coins.

The US Financial Crimes Enforcement Network (FinCEN) classified his activities as ‘money transmitting’ and Caldwell was forced to start selling empty coins. Sales resumed earlier this year and Casascius is currently listing three coins, along with a gold-plated savings bar. However, none of them are priced and it is unclear whether or not Casascius simply ran out of stock or stopped selling them directly altogether.

In addition to these silver, brass and gold-plated products, Casascius also sells aluminium promo coins. A bag of 500 costs 0.39 BTC.

Some additional Facts

- **Bitcoin’s blockchain began in January 2009**, when the mysterious Satoshi Nakamoto mined the first block of bitcoins (known as the “genesis block”).

- Currently, Bitcoin has the capacity to handle between **4-7 transactions per second** (tps), which pales in comparison to systems like VISA and Paypal. VISA can handle on average around 1,700 tps and PayPal an average of 193 tps.

- Currently, each block on the Bitcoin blockchain is able to contain 1mb of data, meaning that the **block size of bitcoin is 1 megabyte**.

- If you become a full node for the Bitcoin blockchain, meaning you help validate ongoing transactions, you basically have to download the entire database first. The **Bitcoin blockchain is currently 5450 GB (2024)**. This represents “the total size of all block headers and transactions” since January 2009.

- The **difficulty** is **adjusted** every 2016 blocks (every 2 weeks approximately) so that the average time between each block remains 10 minutes. The **difficulty** comes directly from the confirmed blocks data in the Bitcoin network.

Visual intros to Blockchain

Blockchain 101 - Part 1 - A Visual Demo
This is a very basic visual introduction to the concepts behind a blockchain.

https://www.youtube.com/watch?v=_160oMzblY8

Blockchain 101 - Part 2 - Public / Private Keys and Signing
How public/private key pairs are used to make sure that the transaction was posed by the person who had the money.

https://www.youtube.com/watch?v=xIDL_akeras

Summary

Definition
A blockchain is a digital database, a record of transactions
in which individual records, called blocks,
are linked together in a single list, called a chain.

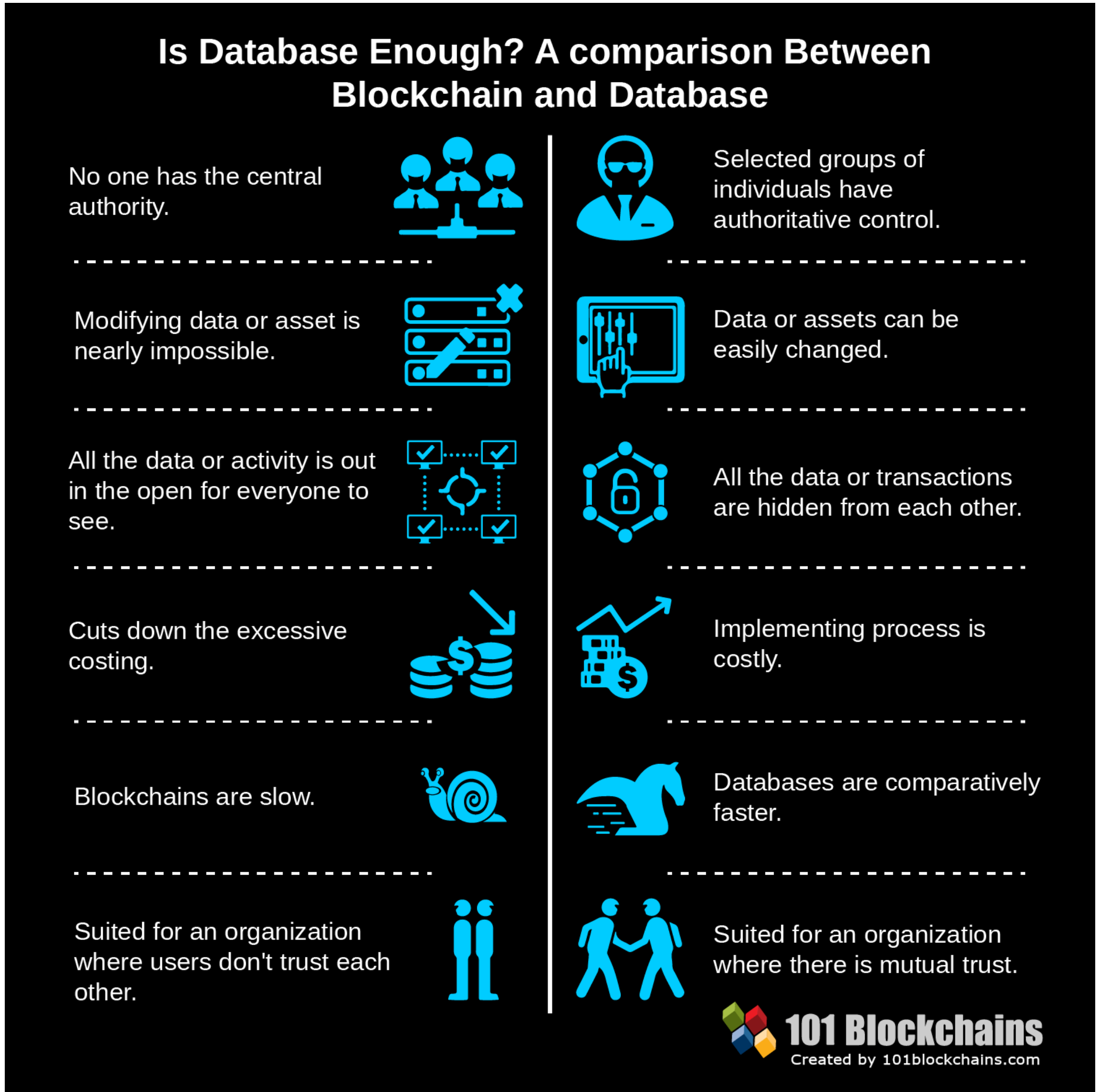
Summary

History

Based on Stuart Haber's theory, the Blockchain was first proposed by "Satoshi Nakamoto" (an unknown person/group) in 2008 in the context of bitcoin, a peer-to-peer version of electronic cash

Blockchain vs Database

Summary



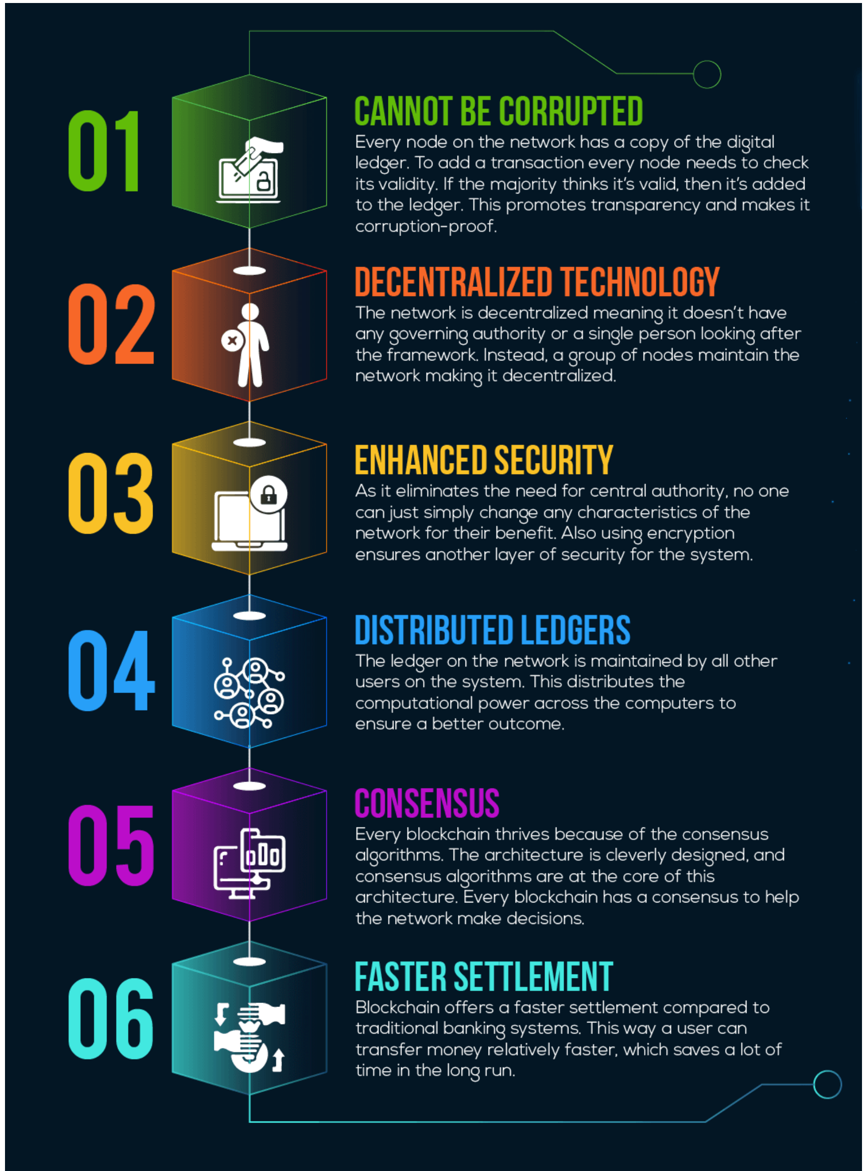
Is Database Enough? A comparison Between Blockchain and Database

No one has the central authority.	Selected groups of individuals have authoritative control.
Modifying data or asset is nearly impossible.	Data or assets can be easily changed.
All the data or activity is out in the open for everyone to see.	All the data or transactions are hidden from each other.
Cuts down the excessive costing.	Implementing process is costly.
Blockchains are slow.	Databases are comparatively faster.
Suited for an organization where users don't trust each other.	Suited for an organization where there is mutual trust.

101 Blockchains
Created by 101blockchains.com

Key Features of Blockchain Technology

Summary



01
CANNOT BE CORRUPTED
Every node on the network has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof.

02
DECENTRALIZED TECHNOLOGY
The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework. Instead, a group of nodes maintain the network making it decentralized.

03
ENHANCED SECURITY
As it eliminates the need for central authority, no one can just simply change any characteristics of the network for their benefit. Also using encryption ensures another layer of security for the system.

04
DISTRIBUTED LEDGERS
The ledger on the network is maintained by all other users on the system. This distributes the computational power across the computers to ensure a better outcome.

05
CONSENSUS
Every blockchain thrives because of the consensus algorithms. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.

06
FASTER SETTLEMENT
Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster, which saves a lot of time in the long run.

Summary

Applications

Blockchain is starting to disrupt many industries in the next 5 to 10 years

Banking and payments

Cyber Security

Supply Chain

Management

Forecasting

Networking and IoT

Insurance

Private Tansport and

Ride Sharing

Cloud Storage

Charity

Voting

Government

Public Benefits

Healthcare

Energy

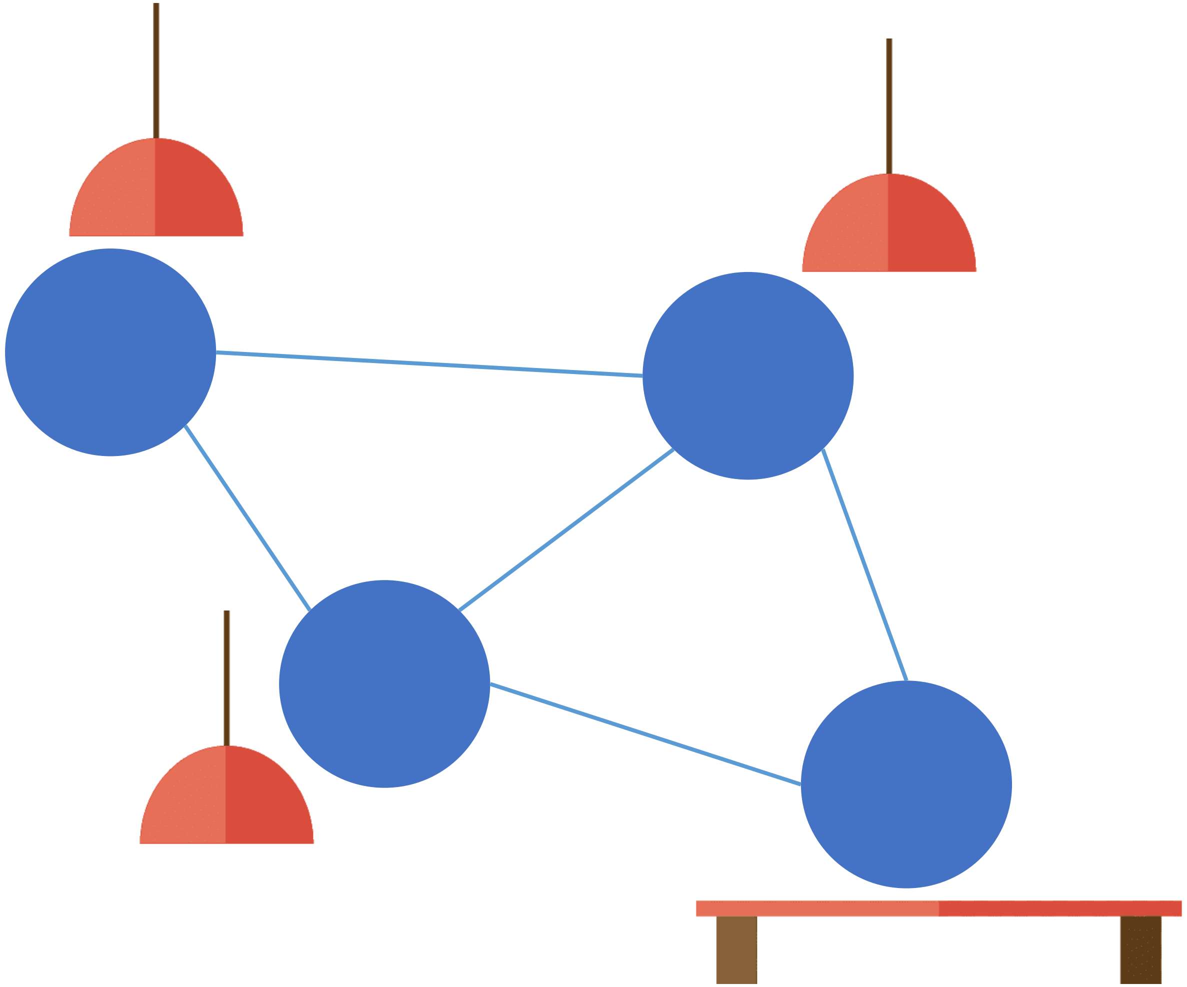
Management

Online Music

Retail

Real Estate

Summary

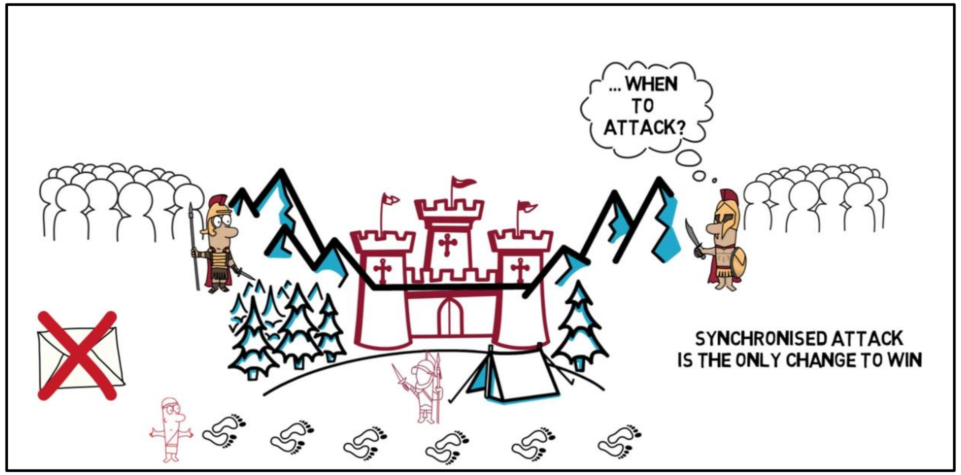


Double Spending Problem

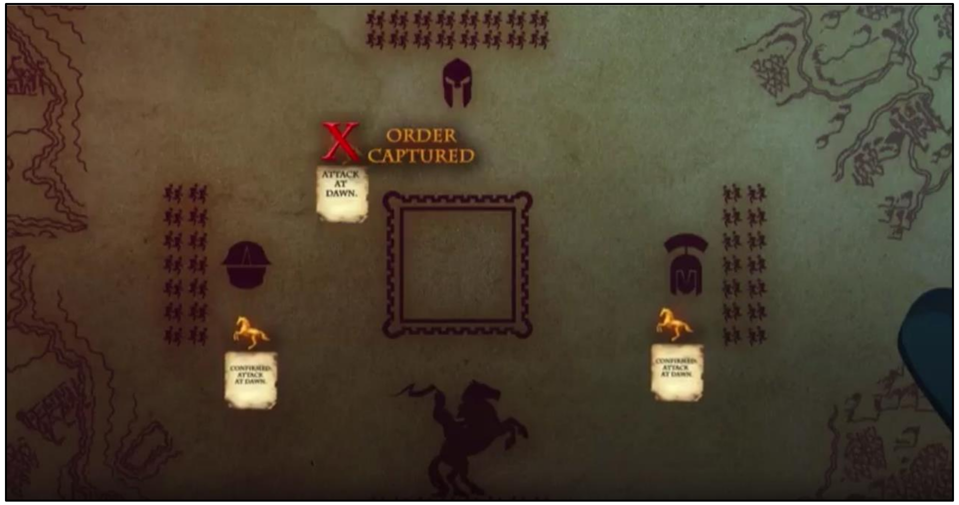
How to Trust the Data

Summary

Two Generals Problem

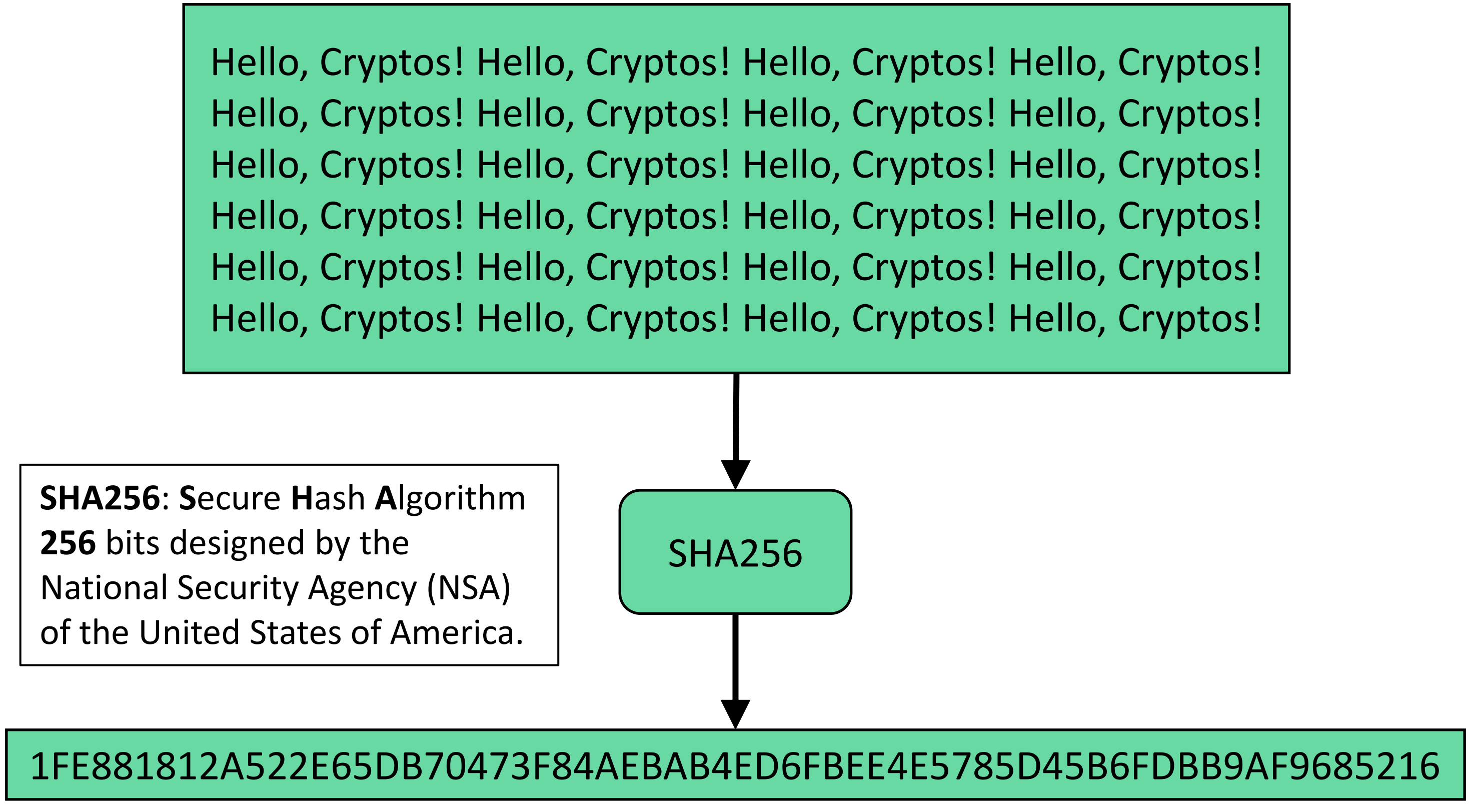


Byzantine Generals Problem



What is a *hash*?

Summary



Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!
Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!
Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!
Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!
Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!
Hello, Cryptos! Hello, Cryptos! Hello, Cryptos! Hello, Cryptos!

SHA256: **S**ecure **H**ash **A**lgorithm **256** bits designed by the National Security Agency (NSA) of the United States of America.

SHA256

1FE881812A522E65DB70473F84AEBAB4ED6FBEE4E5785D45B6FDBB9AF9685216

What is a *nonce*?

Summary

What is Proof of Work (PoW)?

Summary

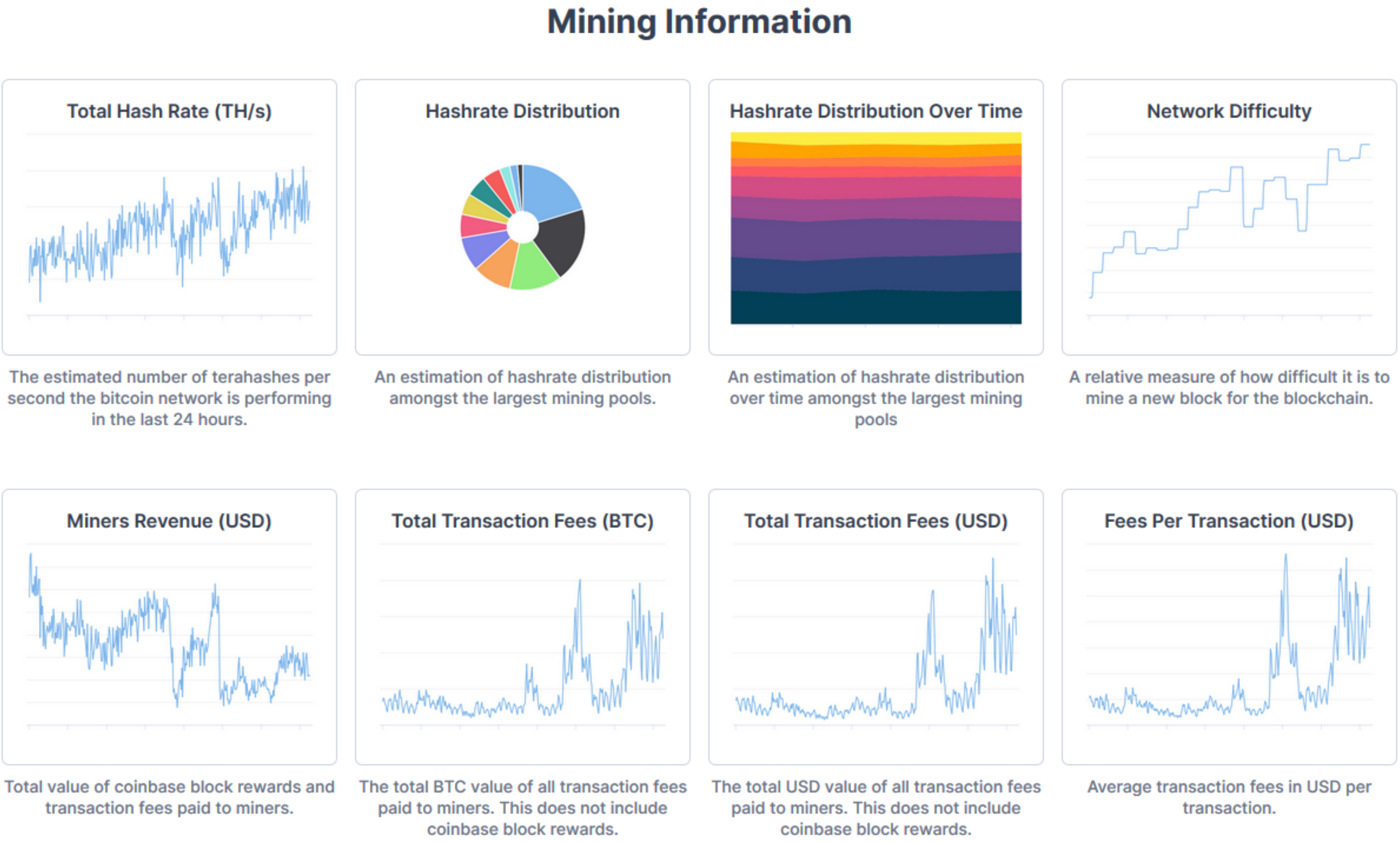
Only one member of the network, chosen based on solving a puzzle (that takes on average 10 minutes to solve) is allowed to decide if the transaction is valid or not, and this decision is then agreed to by all on the network.

The purpose of this consensus algorithms is not to ascertain the “truth” as to which is the “correct” transaction between two conflicting transactions, it is merely a mechanism to prevent the double spending problem in distributed networks.

The truth is simply what everyone agrees on!

Putting it all together

Summary



Mining Information

Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.

Hashrate Distribution

An estimation of hashrate distribution amongst the largest mining pools.

Hashrate Distribution Over Time

An estimation of hashrate distribution over time amongst the largest mining pools

Network Difficulty

A relative measure of how difficult it is to mine a new block for the blockchain.

Miners Revenue (USD)

Total value of coinbase block rewards and transaction fees paid to miners.

Total Transaction Fees (BTC)

The total BTC value of all transaction fees paid to miners. This does not include coinbase block rewards.

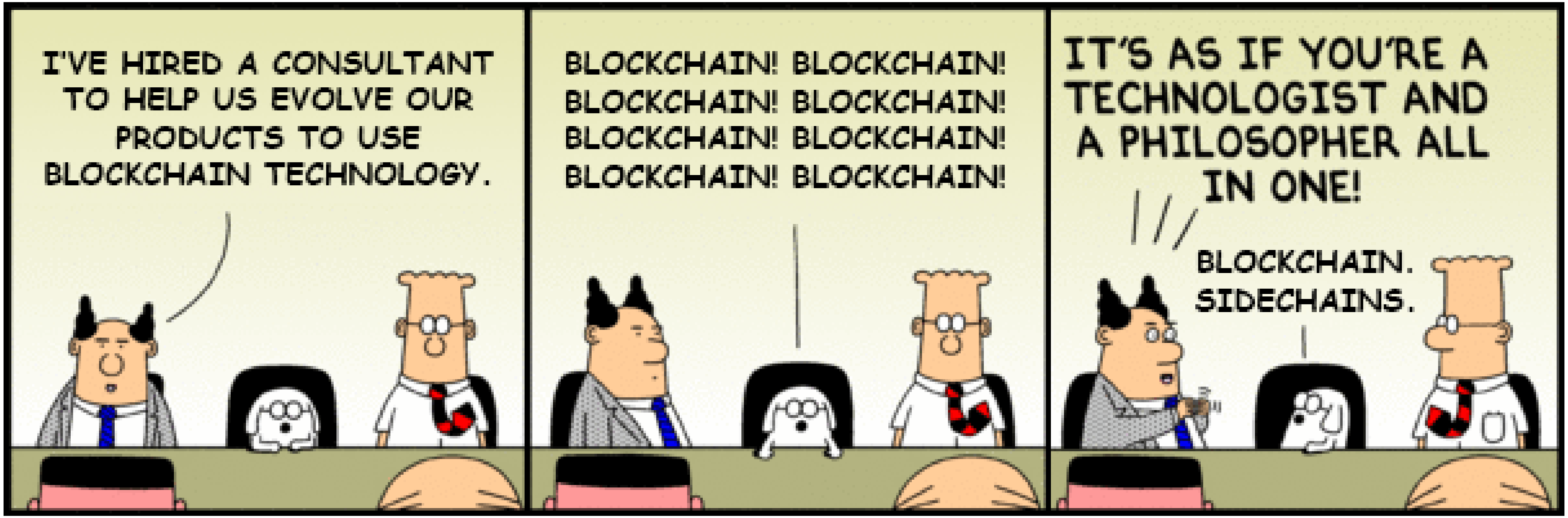
Total Transaction Fees (USD)

The total USD value of all transaction fees paid to miners. This does not include coinbase block rewards.

Fees Per Transaction (USD)

Average transaction fees in USD per transaction.

https://www.blockchain.com/charts


I'VE HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO USE BLOCKCHAIN TECHNOLOGY.
BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN!
IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!
BLOCKCHAIN. SIDECHAINS.