Blockchain Technologies and Decentralized Computing

Davide Patti
davide.patti@dieei.unict.it

About me

Assistant Professor @ University of Catania (Italy)

davide.patti@dieei.unict.it

https://github.com/davidepatti

https://www.davidepatti.it/

Blockchain: Beyond the Hype

- Magic buzz-word for sounding “cool” (80% maybe non-sense)
- Potential revolutionary impact of blockchain:
  - Understand when it makes sense
  - ….but EVEN MORE when it doesn’t

Outline Day 1

- Physical vs Digital Assets
- Exchange of Value in Human history
- Hash Functions
- Proof-of-Work
- Mining

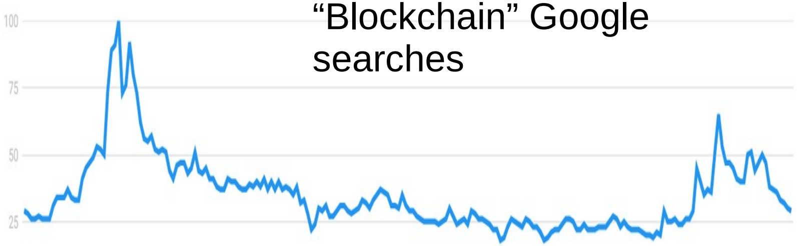
DISCLAIMER:
Technology, Not Speculation

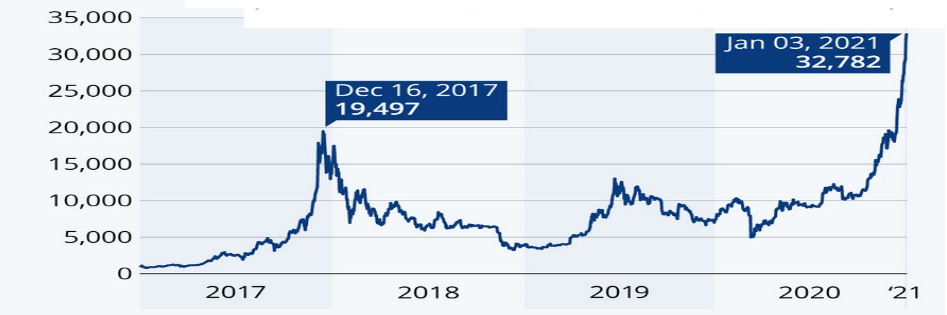
We will not discuss about prices, trading, speculation etc…

Price is only a consequence of the technology, not the origin

Looking at recent past, why do we have the Web applications?

- *World-wide Internet open TCP/IP protocol*
- *...or Google and Apple stocks prices?*


“Blockchain” Google searches



* Closing price (latest data in range, UTC time)
Source: Coin Market Cap

Terminology & Goals

Bitcoin: the decentralized protocol, aka, the “blockchain”

bitcoin (or **BTC**): the underlying digital asset exchanged between nodes using the blockchain

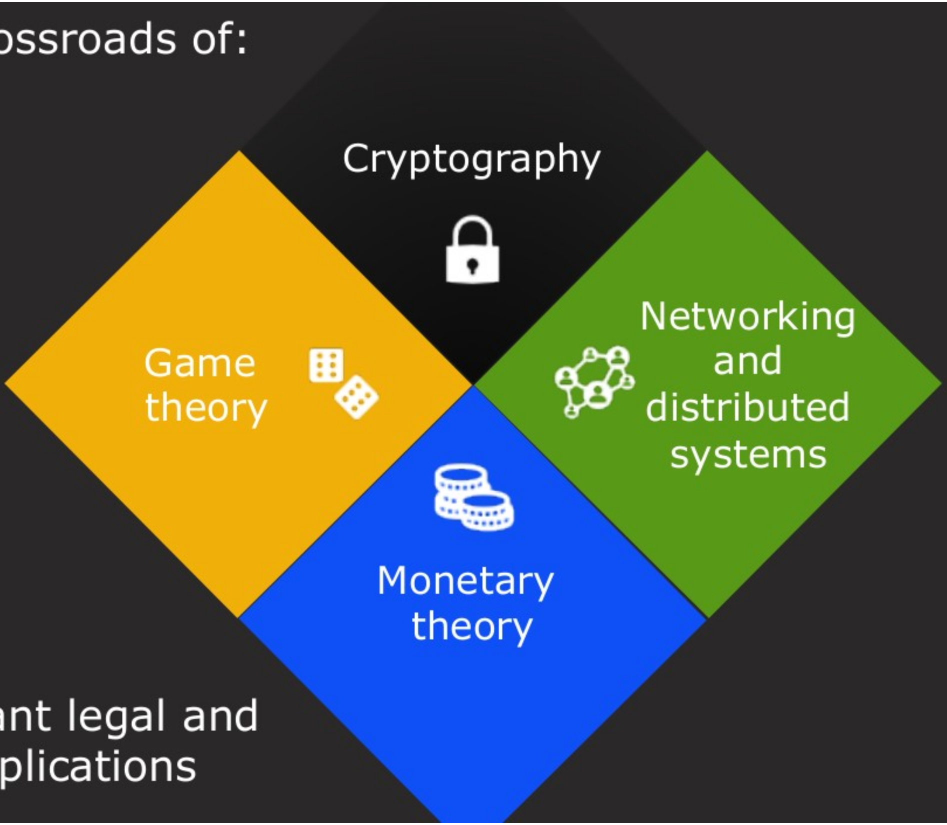
GOALS

1)Understanding that a blockchain is an **“open and decentralized platform of trust”**, NOT a distributed database

2)Understanding that digital assets (e.g.,money) are only a first application of the **“trustless digital reality”** created at layer 1

Down to the “Rabbit hole”

At the crossroads of:



Cryptography

Game theory

Networking and distributed systems

Monetary theory

With relevant legal and political implications

Mainly not a technology, a cultural paradigm shift instead

(c) 2021 Digital Gold Institute

It’s time to reveal the Truth:

A Blockchain is a Chain of Blocks

It’s time to reveal the Truth:

A Blockchain is a Chain of Blocks

Sorry for the disappointment…

Some Questions Remain Open

- How are they chained?
- Why are they chained?
- What’s inside the blocks?
- Why can’t we have only a single block?
- This “chaining” is still in progress in this moment?
- How this started? How can stop?
- Who chains these blocks?
- *“I’m not scared: I studied Computer Science 27 years ago, I know what a linked list is...”*

Not a Good Term, after all

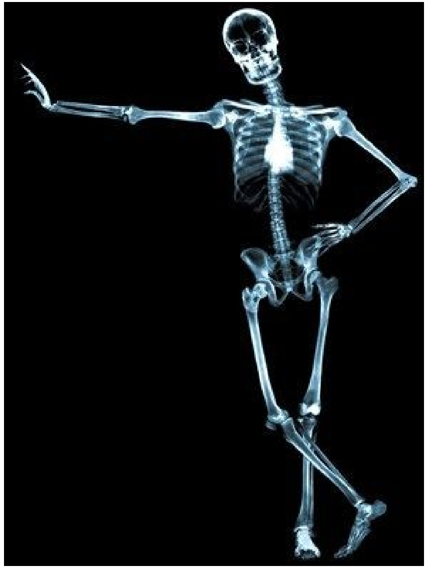
“Bitcoin is a ***blockchain*** *based technology”*

Not a Good Term, after all

*“Bitcoin is a **blockchain** based technology”*

is something like…

*“Humanity is a **skeleton** based biotechnology”*



Enabling Key Concepts

Cannot understand blockchain without understanding:

- The philosophical and economic vision behind **Bitcoin**
- The mathematical concepts that make it possible:
  - **Hash Functions**
  - **Asymmetric Cryptography**

Outline Day 1

- **Physical vs Digital Assets**
- Exchange of Value in Human history
- Hash Functions
- Proof-of-Work
- Mining

Let’s start from a Question

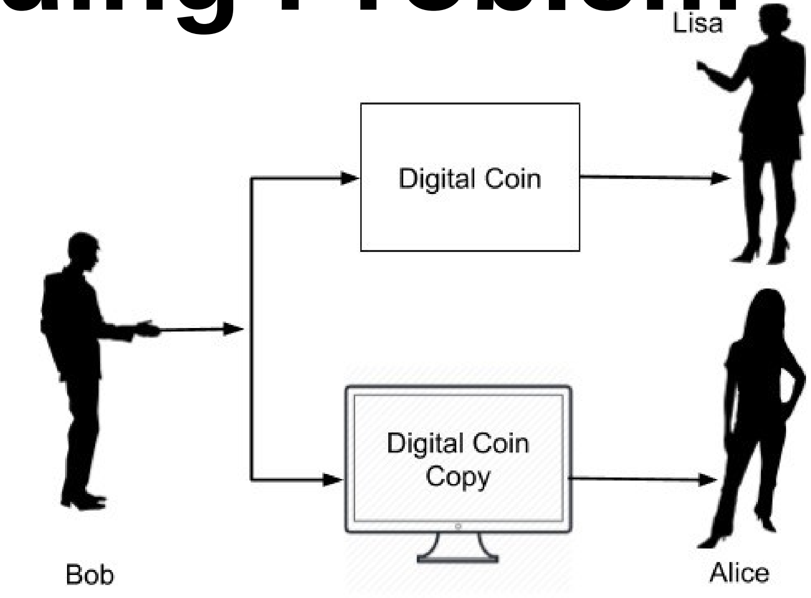
Is it possible to exchange/transfer something that is purely digital?

Example: Some digital good, an asset, a file, some form of money….whatever can be assigned **a value and an owner**

Double Spending Problem

Sending digital content means actually “sending a copy”
→ I could send another copy!

What happens when I “send” an image to someone?



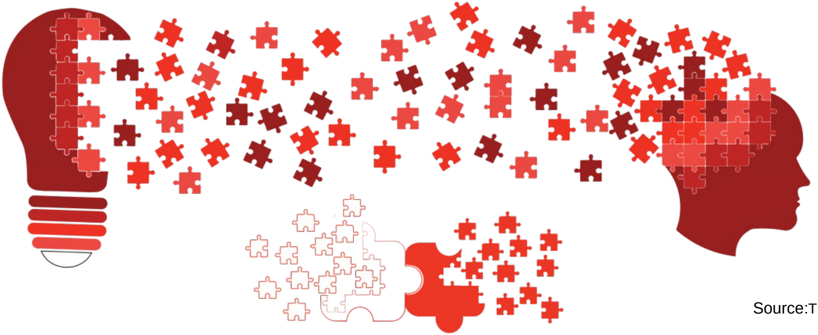
After Bob gives his digital asset to Lisa, he can also a give a copy of the file to Alice.

Information vs Physical Assets

- **Information never represents the state of the world directly.**
  - A physical apple vs a computer file.
- In the physical realm, we can actually move things from A to B.
- Physical tokens are unique composites of atoms whose assembly is not easily replicable

Pure information does not have this property:

- **If you can read the information, you can also copy it perfectly.**
- There is no way to “hand over” information, you can never be sure if the original owner destroyed the infor mation on his end.



Source:TEDxYouth

Digital assets, like all information, can only be spread, like an idea.

… if you have an apple and I have an apple, and we swap apples — we each end up with only one apple.

But if you have an idea and I have an idea and we swap ideas — we each end up with two ideas.

Charles F. Brannan (1949)

Physical Double Spending

- A lot harder, if not impossible

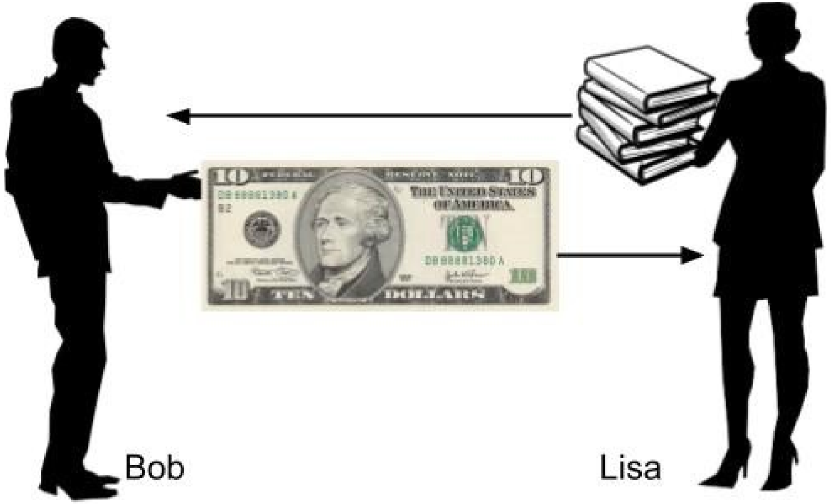
  Totò selling “his own” historical Fontana di Trevi, in Rome

https://www.youtube.com/watch?v=KNYVuxva1IM&ab_channel=italfilmsubs

Outline Day 1

- Physical vs Digital Assets
- **Exchange of Value in Human history**
- Hash Functions
- Proof-of-Work
- Mining

Traditional Transfer of Value: Money



Once the Lisa receives this physical $10 bill, there is no way for Bob to re-use this money for some other transaction, as the physical currency is now in Lisa’s possession.

Why don’t just exchange physical objects?

- Historically known as “barter”: direct exchange of goods
  - Lack of ***“Coincidence of scales”:*** can you buy a home with shoes?
  - Lack of ***“Coincidence of time frames”***: accumulate fishes to buy a car? What happens?
  - Lack of ***“Coincidence of locations”***: I want to sell a house to buy in another location, but you can’t transport the house

How to avoid direct exchange?

We need a way to make an “Indirect Exchange” of things, something that acts as a “medium”….

We need a way to make an “Indirect Exchange” of things, something that acts as a “medium”….

MONEY

Let’s talk about money.

Money has evolved, since forever.

Rai stones, used in Micronesia 500AD - present day.

Cowrie Shell Money. Some shell money in use up until late 1800s

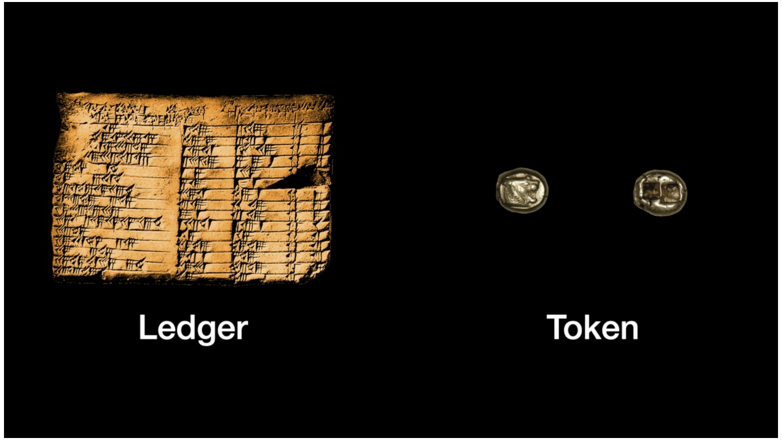
Gold: still used today. Notably as store of wealth for nation states.

What makes good money? Bad money?

- **Durable**: doesn’t perish
- **Portable**: easy to transport
- **Fungible**: one is interchangeable with another
- **Verifiable**: easy to check authenticity
- **Divisible**: support exchange of small amounts
- **Scarce**: can’t be abundant or easy to produce (iron is an useful metal...but..)

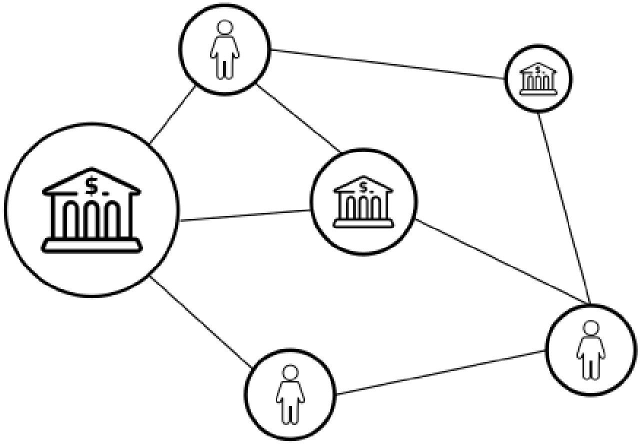
Physical Tokens → Ledgers

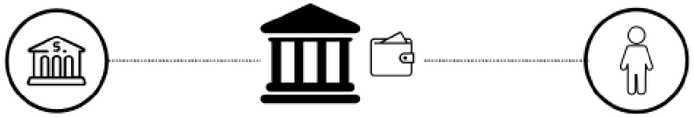
- You can either use real-world artifacts directly, e.g., give someone a sea shell, a coin, or some other tangible thing
- or you can replicate the state of the world by writing down what happened on a piece of paper.
- The first method — **a physical token** — directly represents the state of things.
- The second one — **a ledger** — indirectly reflects the state of things.



NOTICE: Tokens are inherently trustless; ledgers are not.

Current Financial System





- Central authorities (bank, fed, notary, escrow, etc.) transfer actual value between two parties

- Multiple intermediaries and record-keeping are required to facilitate transfer of assets and create trust

- It’s not always feasible to carry around physical money

- Nowadays traditional exchange of value is performed on ledgers managed by trusted third-parties

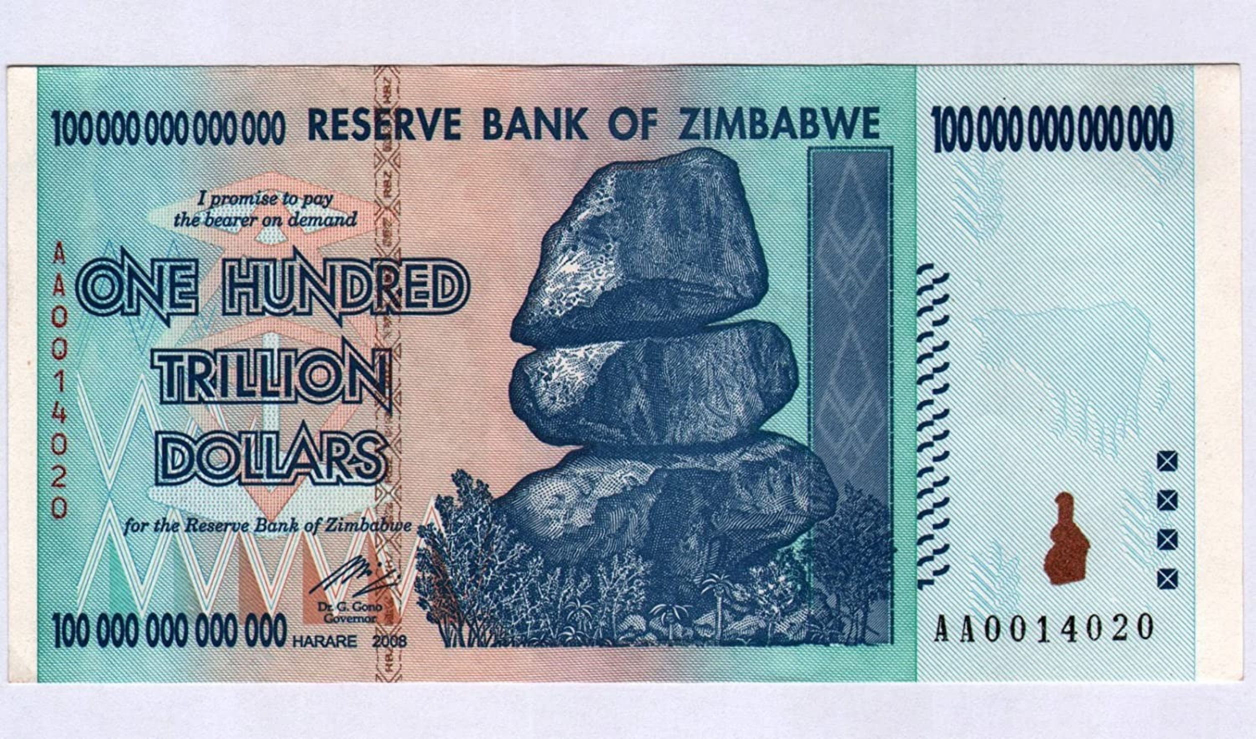
- **This comes with pros and cons**

How does where you live change your view?

Unlimited money printing

Unlimited money printing

Runaway inflation



Unlimited money printing

Runaway inflation

Negative interest rates

Unlimited money printing

Runaway inflation

Negative interest rates

Savers forced to take risks

Unlimited money printing

Runaway inflation

Negative interest rates

Savers forced to take risks

Authoritarianism on the rise

Unlimited money printing

Runaway inflation

Negative interest rates

Savers forced to take risks

Authoritarianism on the rise

Refugees facing capital controls

Unlimited money printing

Runaway inflation

Negative interest rates

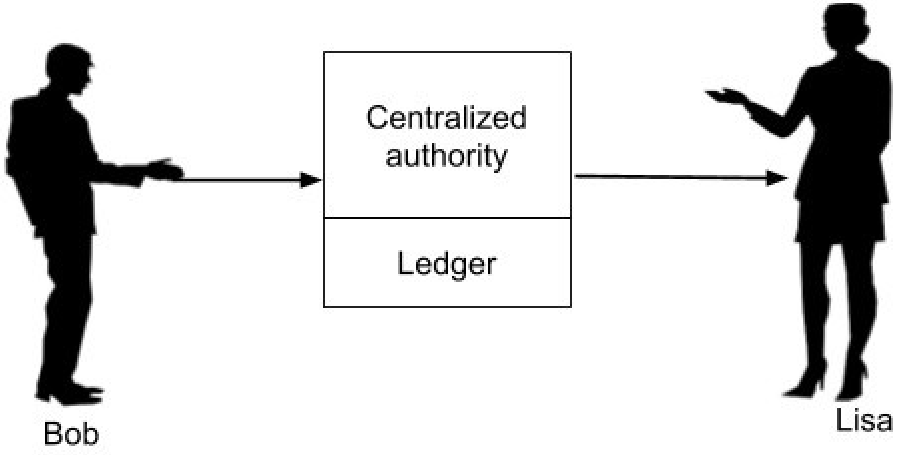
Savers forced to take risks

Authoritarianism on the rise

Refugees facing capital controls

Lack of access to banking

...and in the Digital World?



- We need ledgers to solve the problem of double-spending
- Need a **centralized authority** to track all the transactions?

Centralized... in Internet?

Same problems of physical world...
...**but Internet makes things even worse for centralization:**

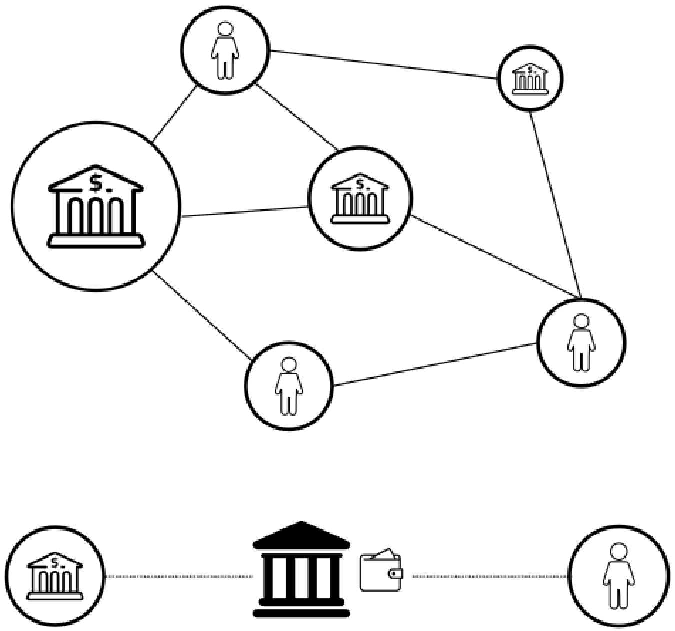
- **Single point of failure:** If it goes down, the system stops working!
- **Concentration of power:**
  - It can censor transactions or impose restrictions
  - Change the rules, modify the history
  - Alter the amount of digital assets (no replication cost!)
- Maybe there’s **nobody we all trust:**
  - Internet is a world-wide entity that crosses the national borders

Main Question (revised version)

Is it possible to represent and transfer purely Digital Assets without requiring a Centralized Authority?

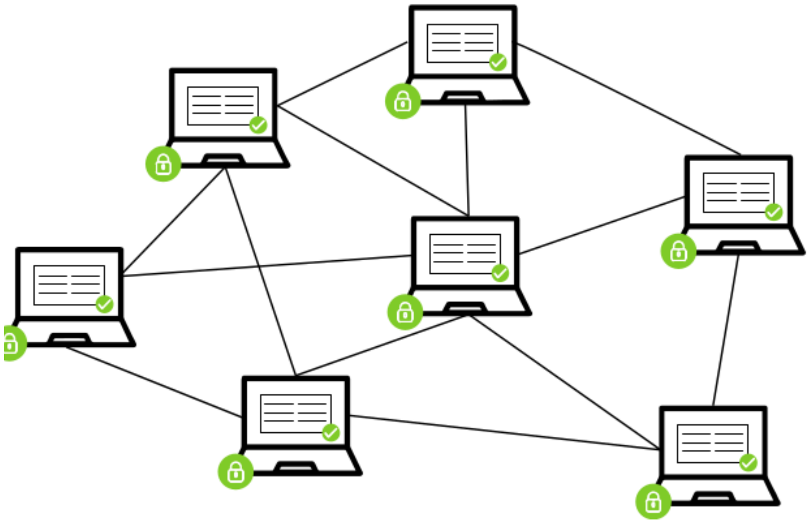
Is it possible that a set of Internet entities agree on some “digital reality” **without trusting each other**?

Current Financial System



- Central authorities (bank, fed, notary, escrow, etc.) transfer actual value between two parties
- Multiple intermediaries and record-keeping are required to facilitate transfer of assets and create trust

BlockChain System



Distributed network of computers (nodes) that maintain a shared source of information

Transaction data is immutable

Peer to Peer transactions using digital tokens to represent assets and value

Agree on What? A Chess Analogy

Alice and Bob want to play chess by mail

- Alice sends Bob “1 e4”
- Bob sends back “1 ... e5”
- Alice sends Bob “2 Nf3”
- ...
- Each of these messages is one move in the game

What’s necessary for them to be able to play the game?

On What Do they Need to Agree?

They have to agree on the state of the board

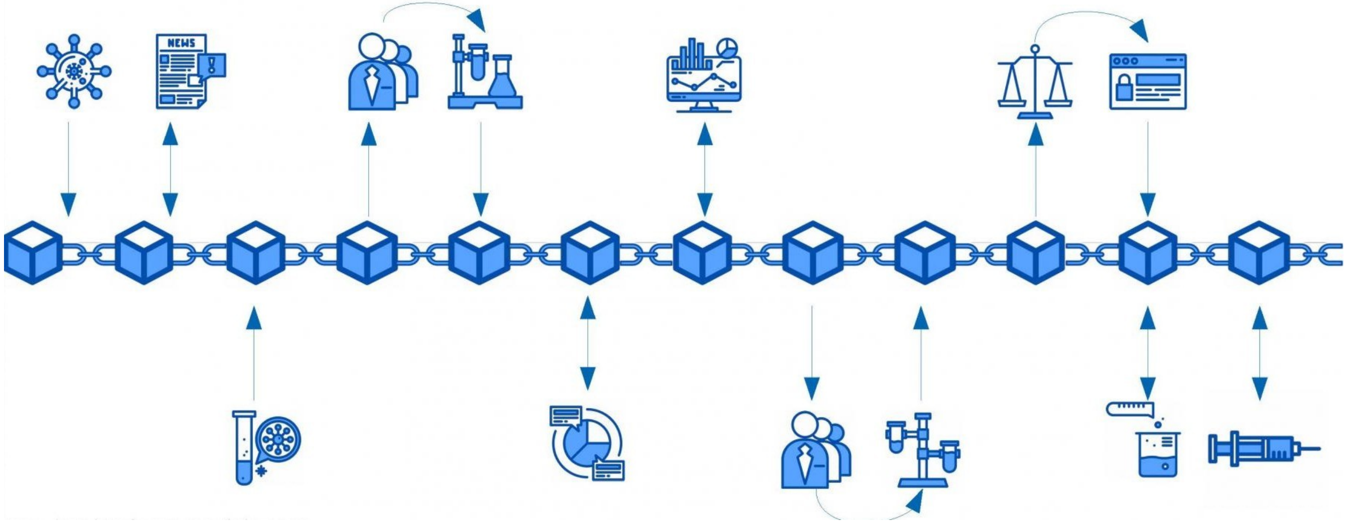
1. Both know the starting positions of the board.
2. Both know the sequence of messages so far (transcript of the game)
3. Thus, they can reconstruct the state of the board.

If we agree on history, we agree on the present state of the world

Block chain (of events)

- All entities agree some initial state of the system (genesis block)
- Each block contains events where (eg, some value transfer)
- A sequence of blocks represents the history of events

→ **We can all agree on the current state of the system**

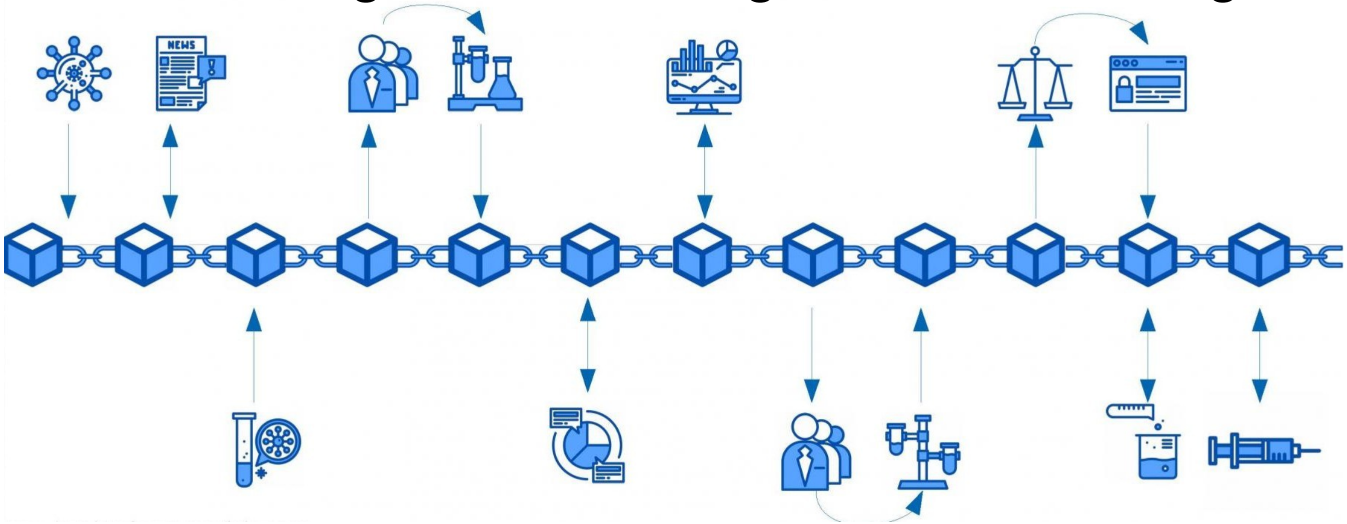


Impossibile Mission?

1)We must guarantee the order of events

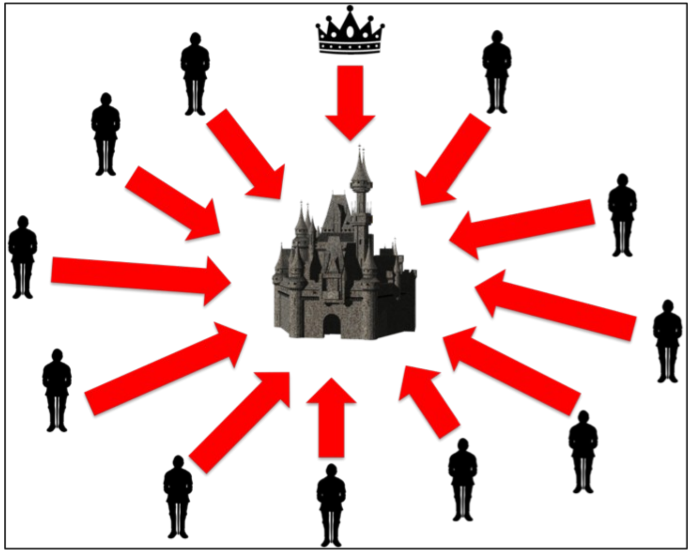
2)Ensure that sender and receiver are the correct ones

3)Entities not trusting each other agree on some “digital reality”

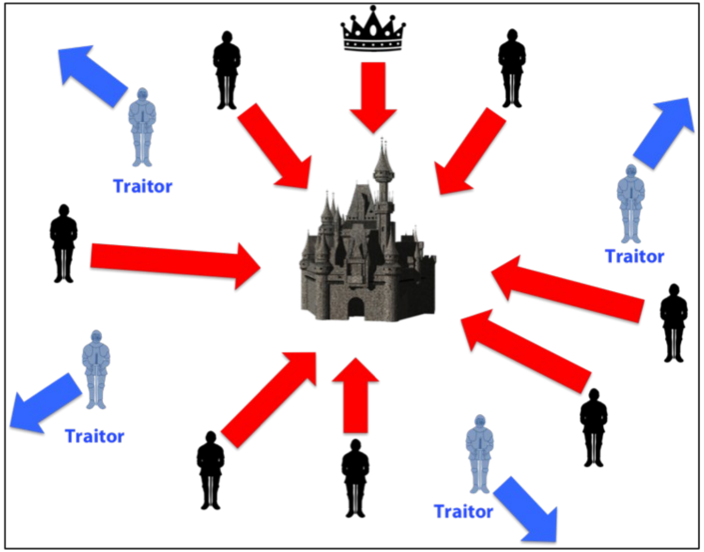


Consensus in distributed systems is hard because:

- Computer nodes may be faulty for technical malfunction (crash failure) or arbitrary malicious activity (Byzantine failure)
- There is latency in communication between nodes
- There is no notion of global time



Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

Thought Experiment

- Room full of people (nodes) that can only talk one-to-one (asynchronous network)
- Try to reach (distributed) consensus about the smaller possible bit of information: a logical variable TRUE/FALSE
- Assume at least one person is severely hear-impaired (faulty) or deceptively untrustworthy (malicious)

Key Concepts to understand BlockChain

Hash Functions

Asymmetric Cryptography

Outline Day 1

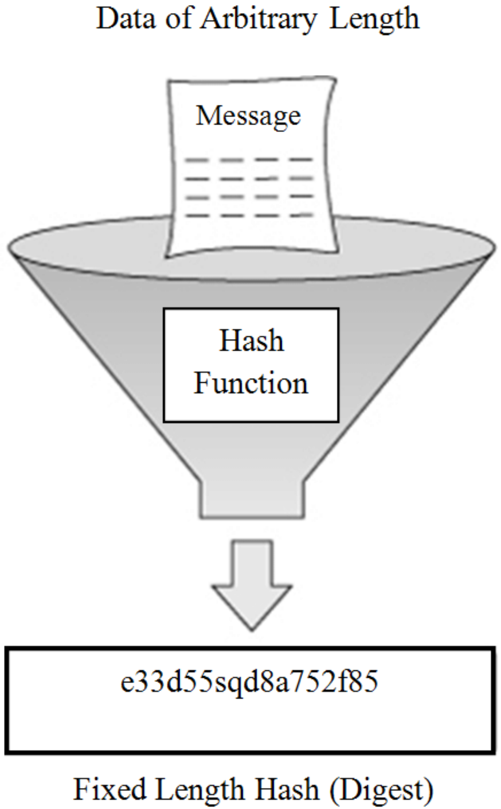
- Physical vs Digital Assets
- Exchange of Value in Human history
- **Hash Functions**
- Proof-of-Work
- Mining

Key Concept: Hashes

- A hash function is a type of mathematical function which turns data into a fingerprint of that data called a hash.

- It's like a mathematical mixing algorithm which takes the input data and turns it into an **output of a fixed length,** which represents the fingerprint of the data.

- Bitcoin uses SHA256, which produces an output of 32 bytes (256 bits)

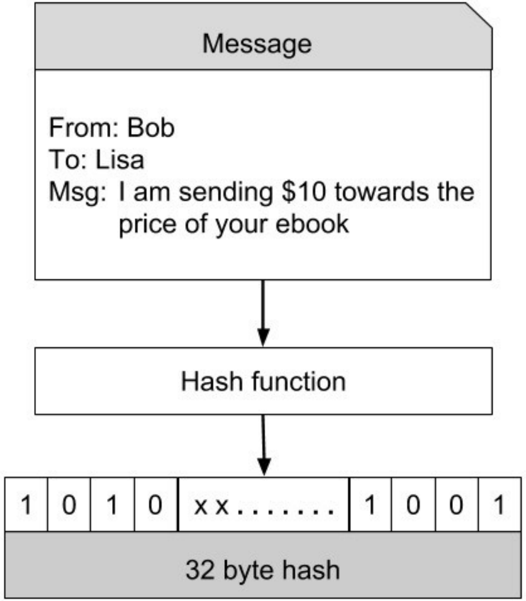


Key Concept: Hashes

When you mash the phrase:
“**hello SPARC students**”
you get this fingerprint (shown in hexadecimal):

e2ba86c5bbcb251fe957ba5cf0e7659ec54df94b8e8c229eda4d1a4edd595395

DEMO: Check it out at:
https://emn178.github.io/online-tools/sha256.html


Message
From: Bob
To: Lisa
Msg: I am sending $10 towards the price of your ebook
Hash function
1 0 1 0 x x 1 0 0 1
32 byte hash

Hash Functions are One-way

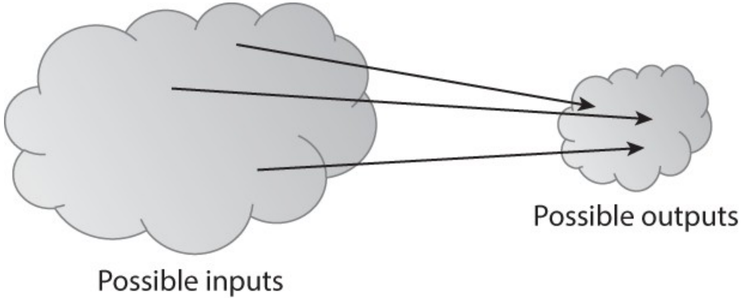
- Counterintuitive: Even simple instructions can generate **irreversibility**
  - Rotate that egg three times on the table (**ok, easily reversible**)
  - Drop that egg on the floor (**irreversible**!)
- **One-way functions:** They are easy to do in one direction...But reversing them it's practically impossible
- Just like it is practically impossible to unscramble an egg, it is practically impossible to unscramble a hash

Properties of Hash Functions

- **One-way (irreversibility):** If you have x, It’s easy to calculate H(x)

  ...but if you have only H(x), It’s unfeasible to back-calculate the original data x from the hash.

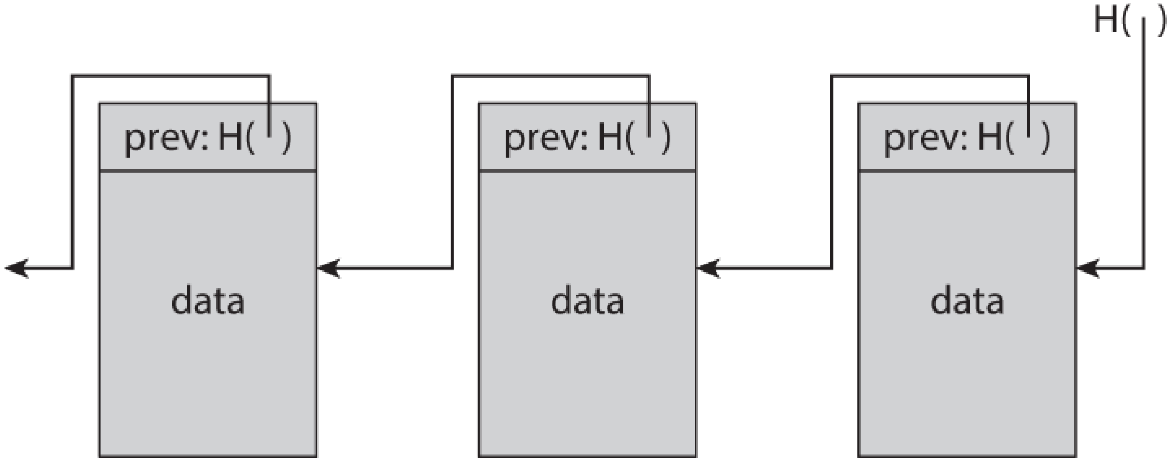
- **Collision Resistance:** you cannot find two different x and y so that H(x) = H(y)



- **Random Oracle:** If the input data changes in the slightest, the hash changes in an unpredictable way

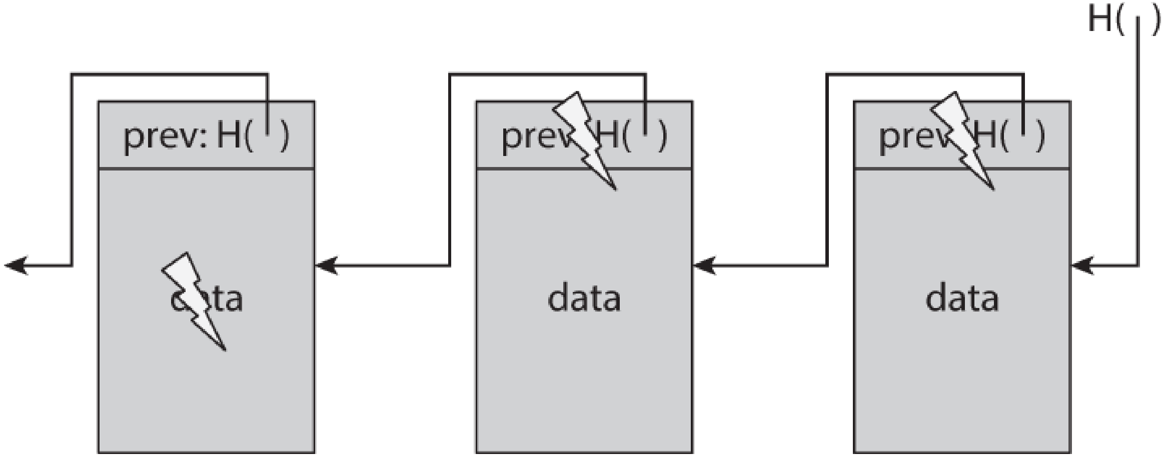
Key Concept: Use Hashes to Chain Blocks

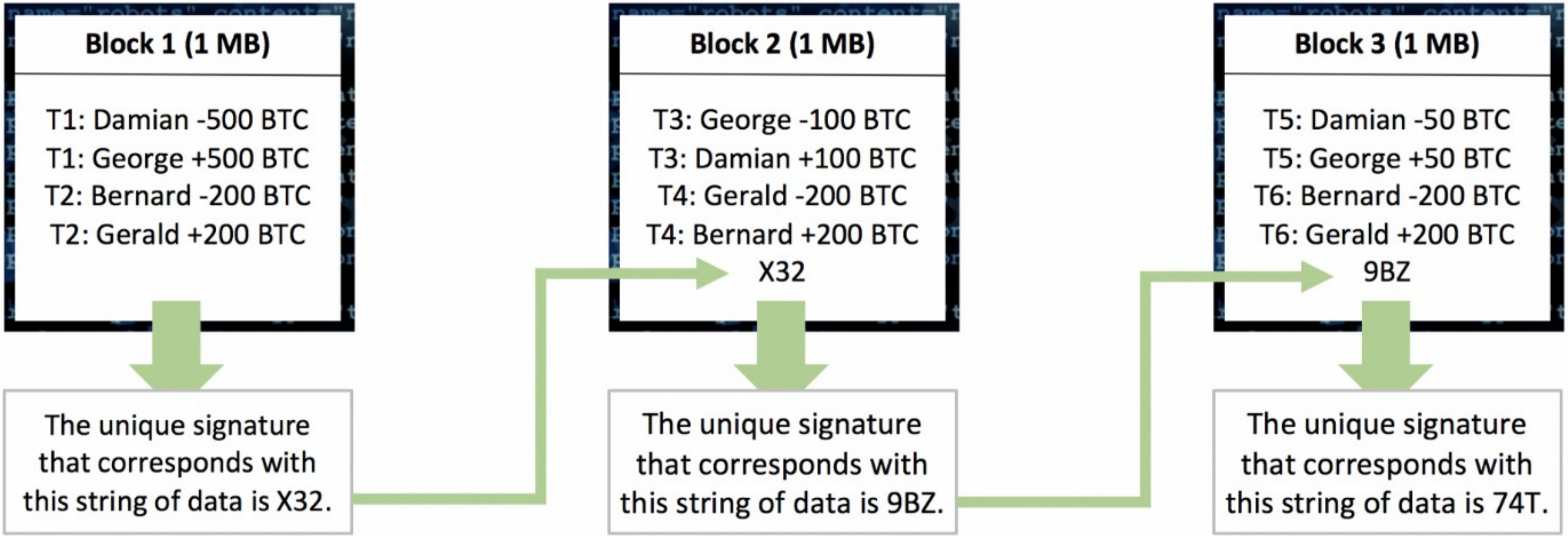
- Each block collects a list of “events” (transactions)
- Not using incremental numbers to order the blocks (e.g., book style)
- Instead, we put additional data, containing the hash of the previous block



Tamper-proof Structure

- Hashes are simple to compute x → H(x), thus each node can quickly verify that each block is connected to the right one!
- **Hash is computed on (data+previous_hash)**
- If data of block “n” is alterered, all subsequent blocks will have wrong hashes





Block 1 (1 MB)

T1: Damian -500 BTC
T1: George +500 BTC
T2: Bernard -200 BTC
T2: Gerald +200 BTC

The unique signature that corresponds with this string of data is X32.

Block 2 (1 MB)

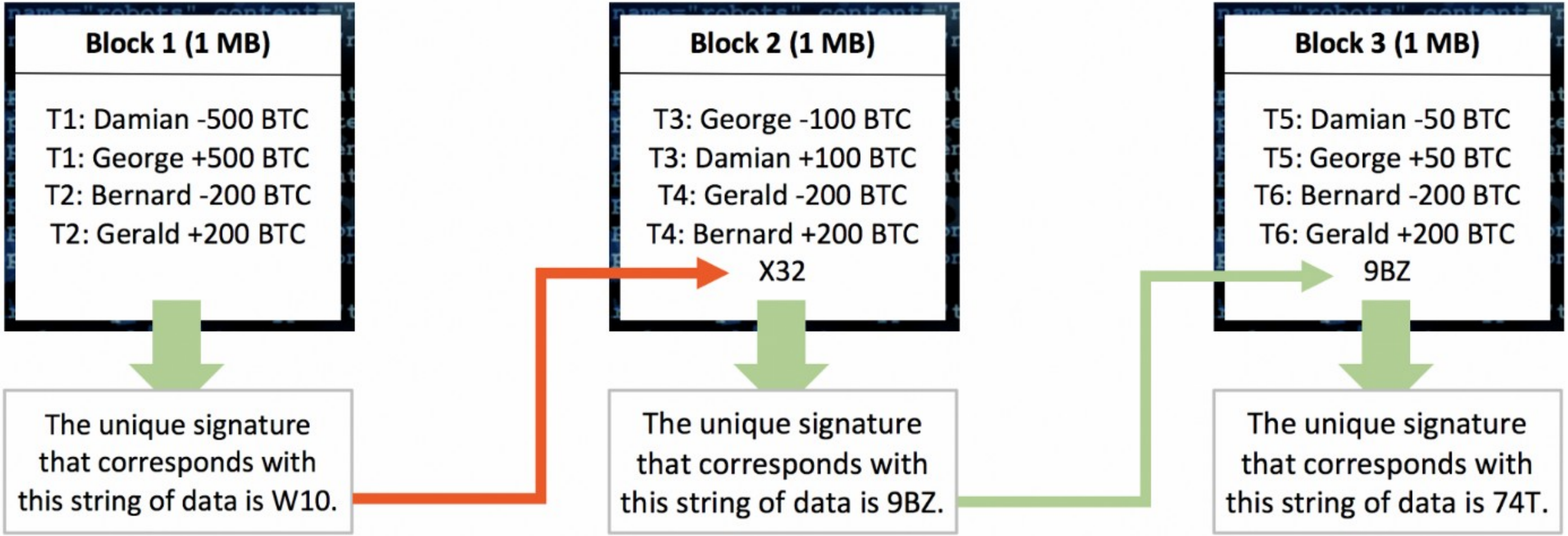
T3: George -100 BTC
T3: Damian +100 BTC
T4: Gerald -200 BTC
T4: Bernard +200 BTC
X32

The unique signature that corresponds with this string of data is 9BZ.

Block 3 (1 MB)

T5: Damian -50 BTC
T5: George +50 BTC
T6: Bernard -200 BTC
T6: Gerald +200 BTC
9BZ

The unique signature that corresponds with this string of data is 74T.



Block 1 (1 MB)

T1: Damian -500 BTC
T1: George +500 BTC
T2: Bernard -200 BTC
T2: Gerald +200 BTC

The unique signature that corresponds with this string of data is W10.

Block 2 (1 MB)

T3: George -100 BTC
T3: Damian +100 BTC
T4: Gerald -200 BTC
T4: Bernard +200 BTC
X32

The unique signature that corresponds with this string of data is 9BZ.

Block 3 (1 MB)

T5: Damian -50 BTC
T5: George +50 BTC
T6: Bernard -200 BTC
T6: Gerald +200 BTC
9BZ

The unique signature that corresponds with this string of data is 74T.

Attacking the Chain

The modification of a block would require the recomputation of the all the hashes for the subsequent blocks….

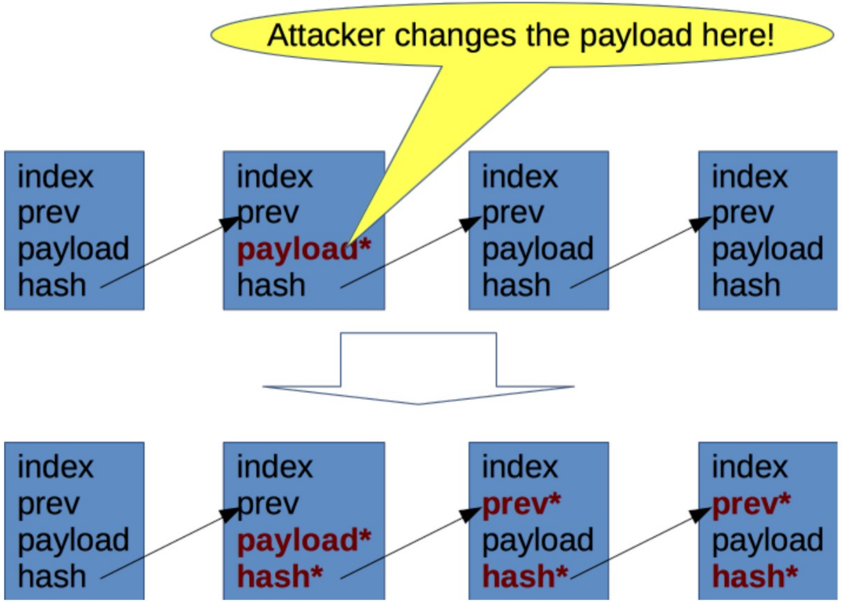
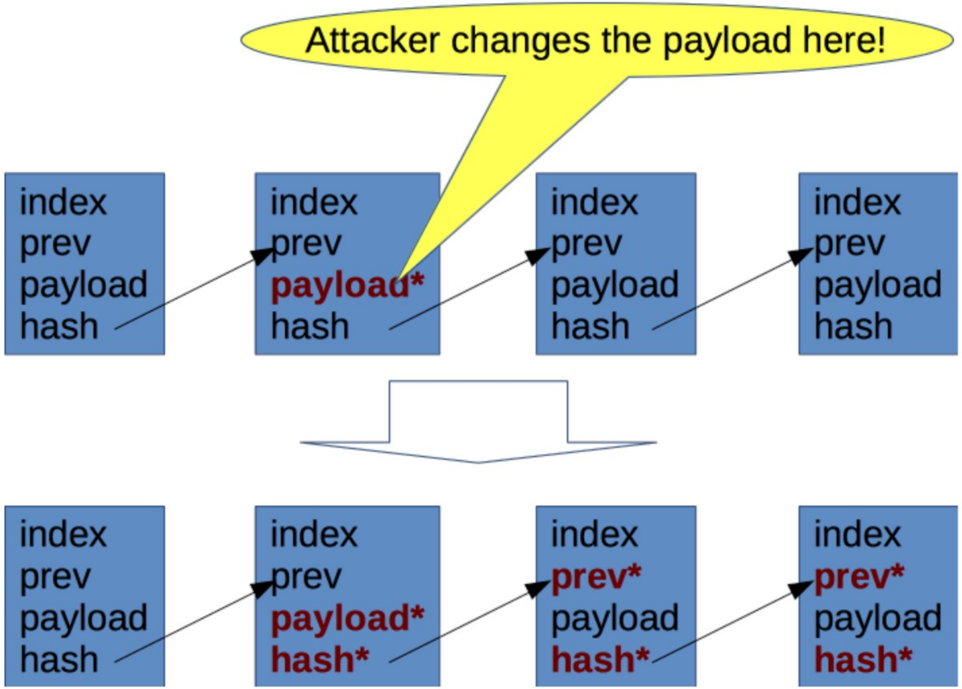


Figure: A change in one record in the hash chain propagates forward to change the hashes in all future records.

Wait a Moment….

…we just said before block, **hashes are easy to compute in the x → H(x) direction**

Thus, a malicious attacker could still want to use its computing power to **recompute all hashes trying to rewrite an “alternative reality”** of blockchain!

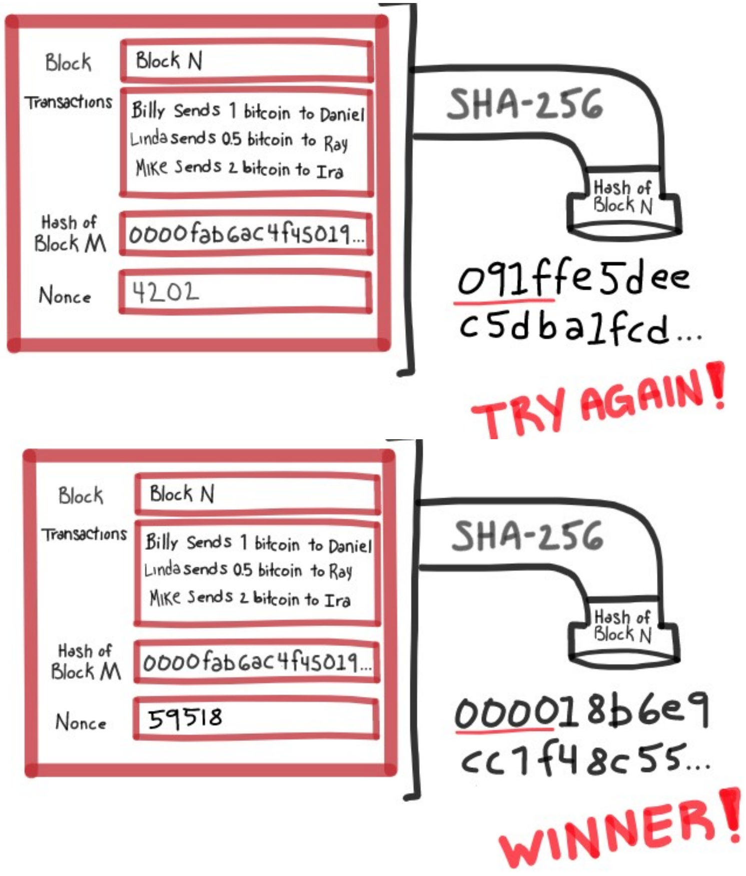


Outline

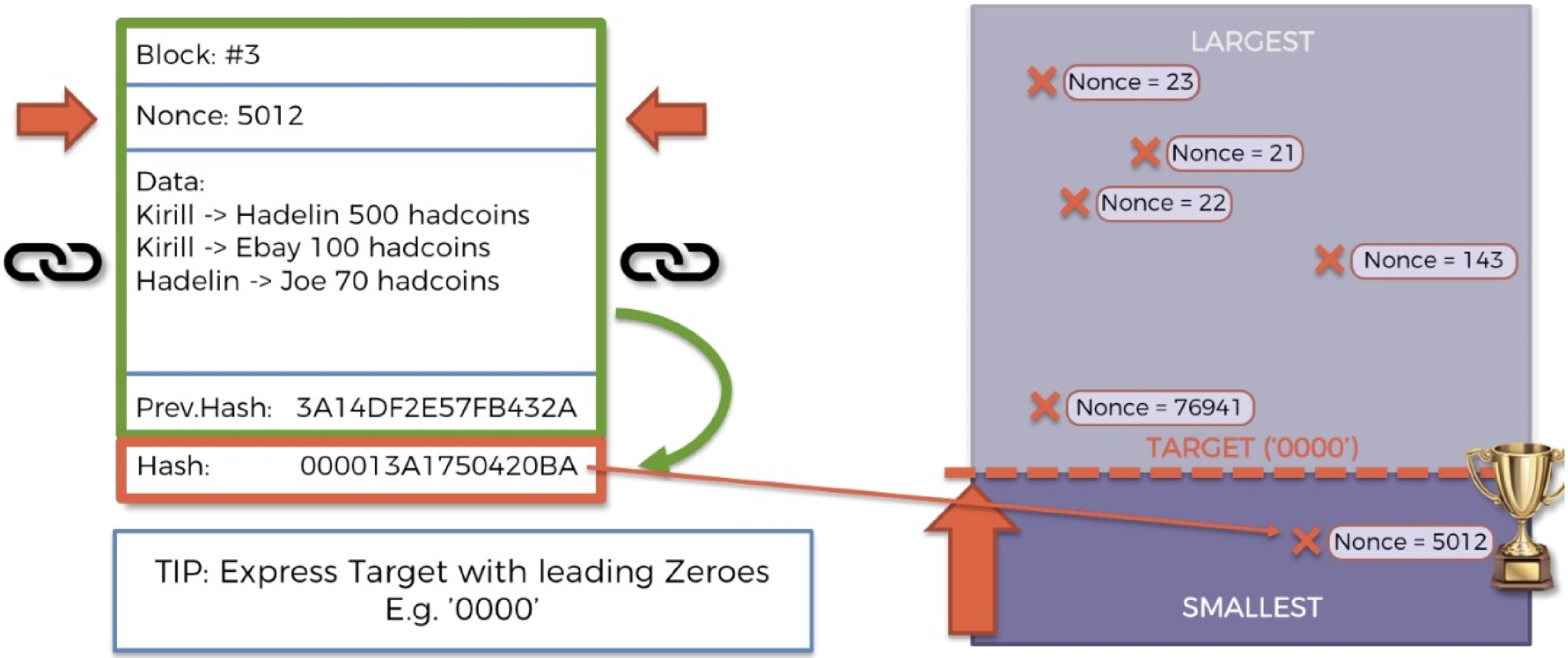
- Physical vs Digital Assets
- Exchange of Value in Human history
- Hash Functions
- **Proof-of-Work**
- Mining
- Asymmetric Cryptography
- Transactions on Chain

Key Concept: Proof-of-Work

- A new block can be added at the end of the chain **only if its hash** starts with a given number of zeros at the beginning (e.g,0000xyzetc…)
- To propose a block, a node assembles the data of transaction and then tries to change several times an additional numeric field called Nonce
- For every Nonce tried, the resulting hash would be very different



- ALL POSSIBLE HASHES -



Block: #3

Nonce: 5012

Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins

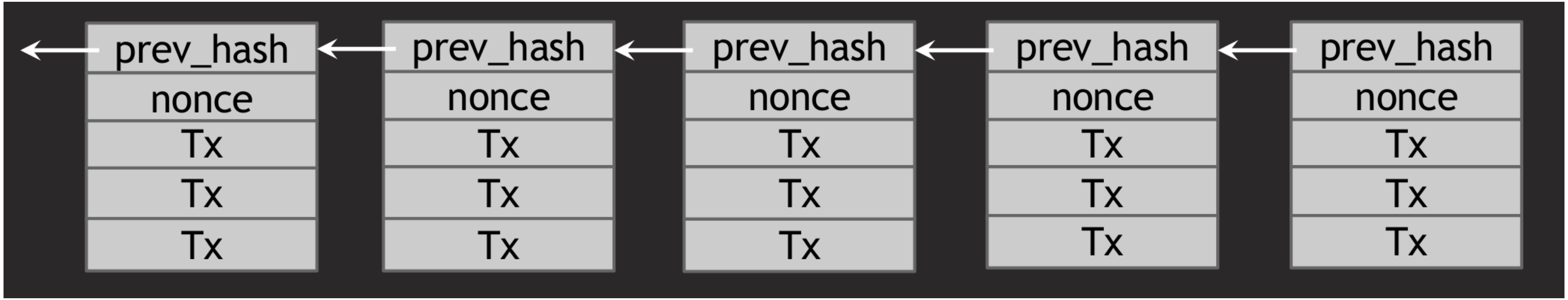
Prev.Hash: 3A14DF2E57FB432A

Hash: 000013A1750420BA

TIP: Express Target with leading Zeroes
E.g. '0000'

Accepting a new Block

- Nodes trying to find the next Nonce are called **Miners**
- Every node can easily verify that the new block hash computed of the whole block (data+nonce+prev_hash) is correct



DEMO: Find the Nonce

TRY the Luck!
Try to produce an hash beginning with one or more zeros at:

https://emn178.github.io/online-tools/sha256.html

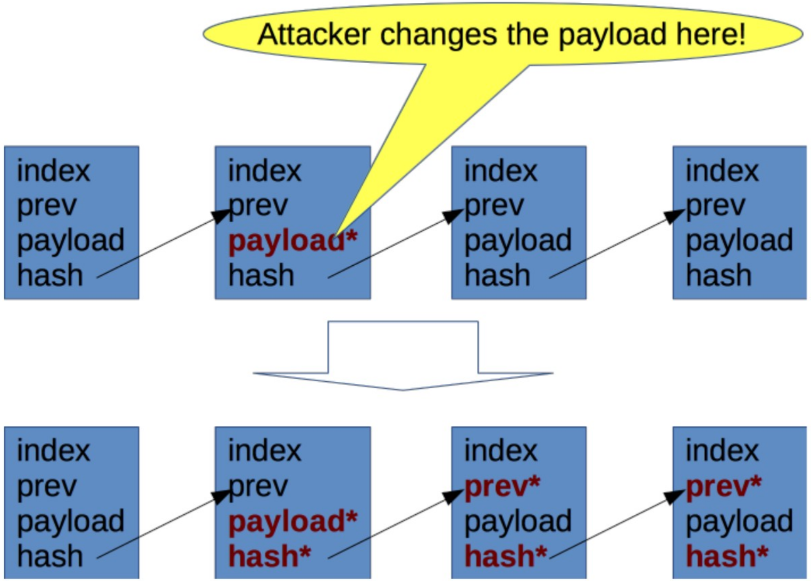
A Game-Theory problem

- An attacker should not only find the Nonce for the block to be altered, but also for all the blocks until the most recent

- **The longest Blockchain is considered the rea one:** so, the attacker should be **faster than the sum of all the other computing nodes in the world (51% attack)**

- This would require an unthinkable economic effort, which would be noticed very quickly.

- The result would be only to create an alternative bitcoin chain of poor value, thus make useless that effort of the attacker



Outline Day 1

- Physical vs Digital Assets
- Exchange of Value in Human history
- Hash Functions
- Proof-of-Work
- **Mining**

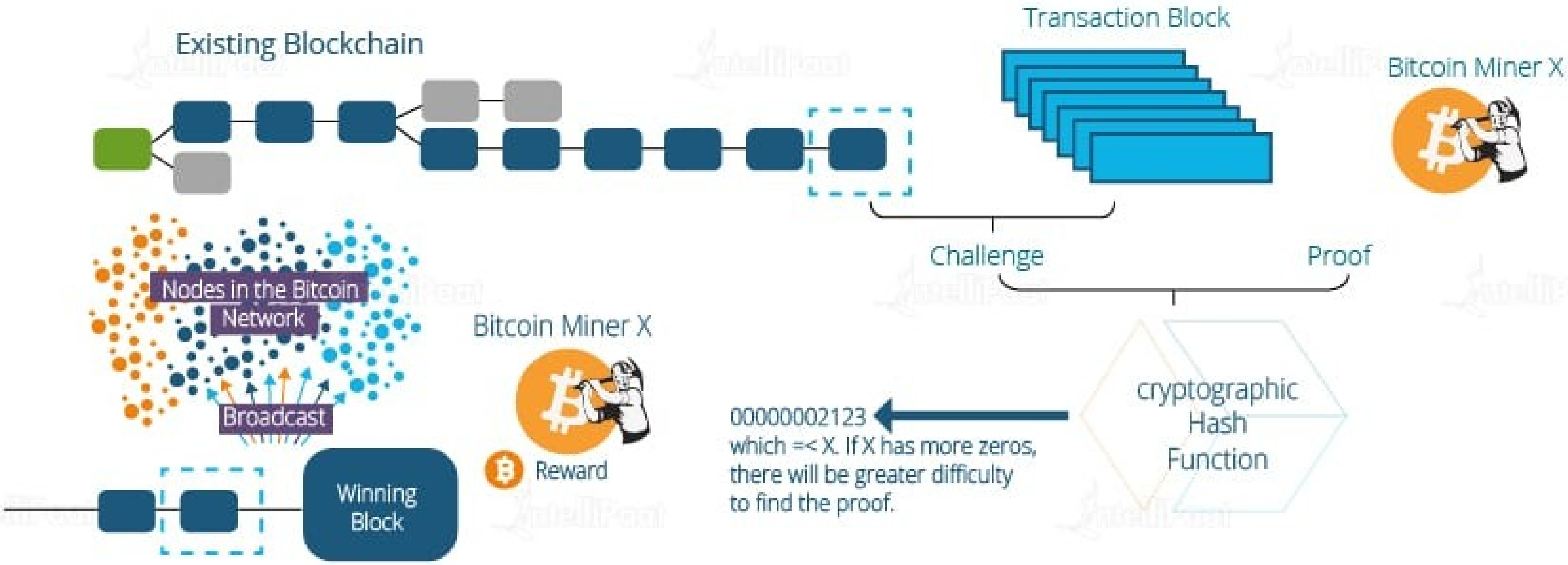
Miners

Why would a node ever want to participate in this research?

- The partecipating nodes are called “miners”.
- The search for the “next Nonce” is called “Mining”. When a node finds the new block, it receives a reward in bitcoin.
- Analogy: like “miners” finding gold

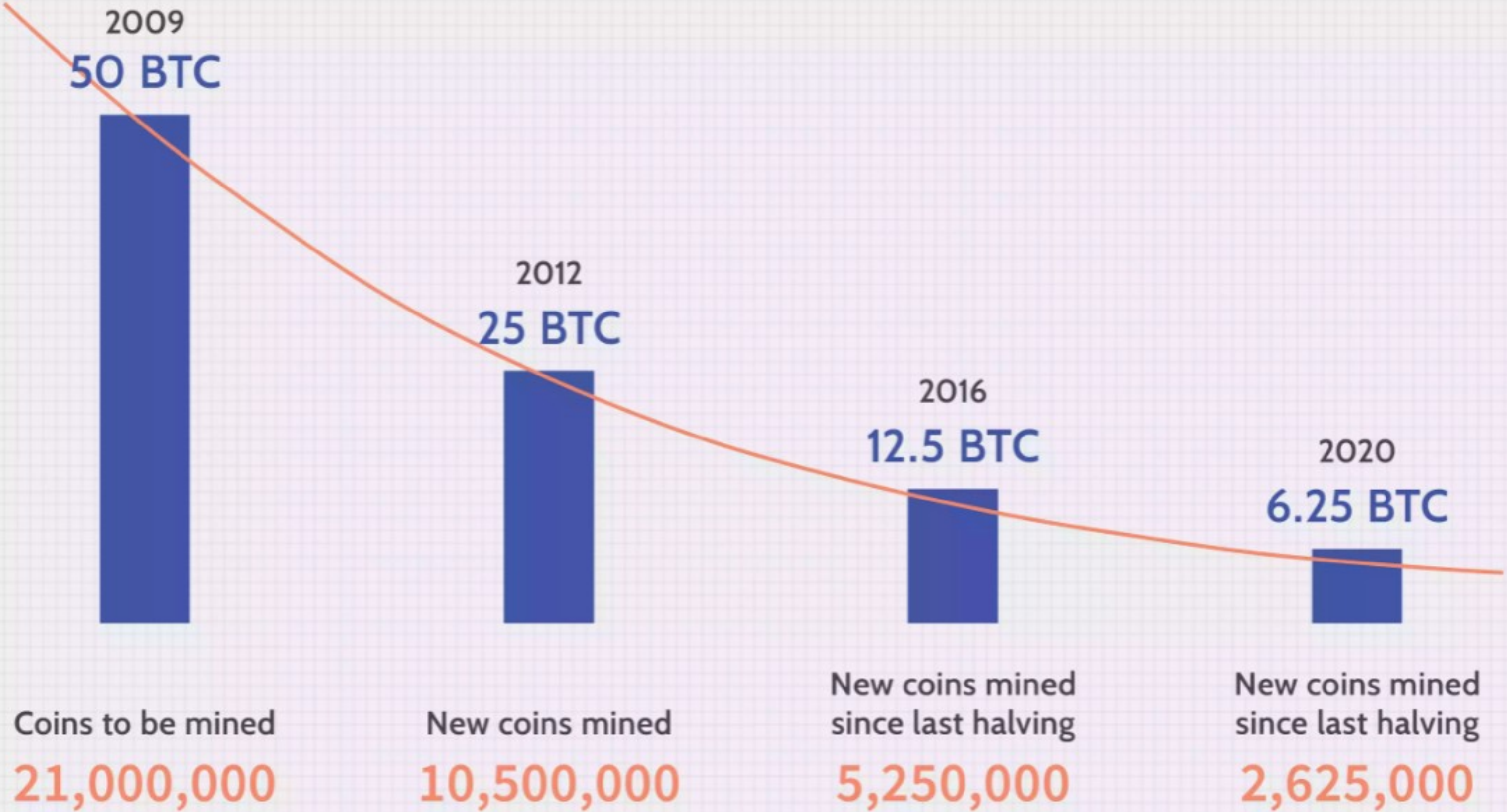
Profit = block reward + Tx fees – costs (electricity, hardware,labor)

Proof of Work

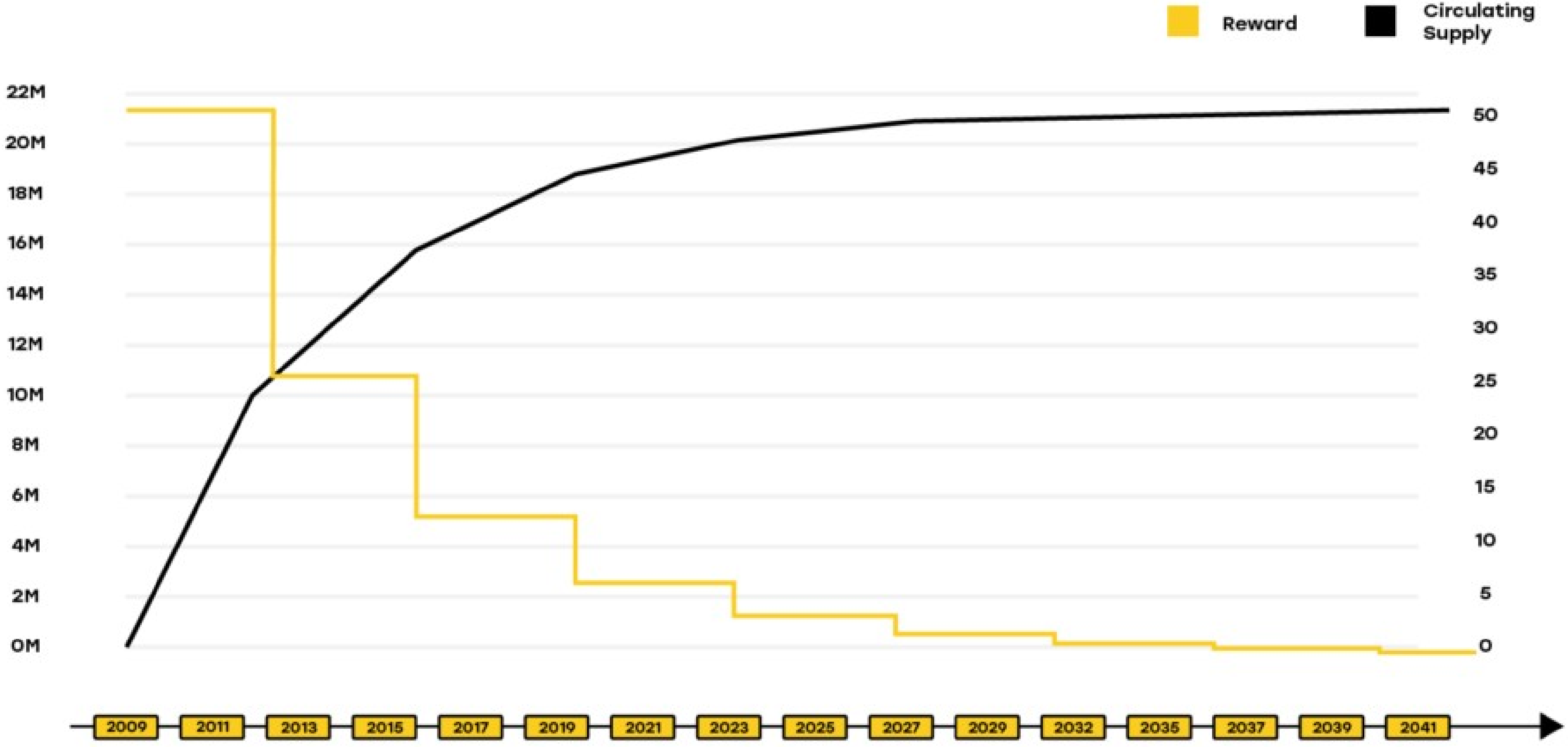


00000002123 which =< X. If X has more zeros, there will be greater difficulty to find the proof.

Miners' Rewards for successfully completing 1 block halve every 210,000 blocks, or an average of every 4 years



Bitcoins in circulation and block reward per year



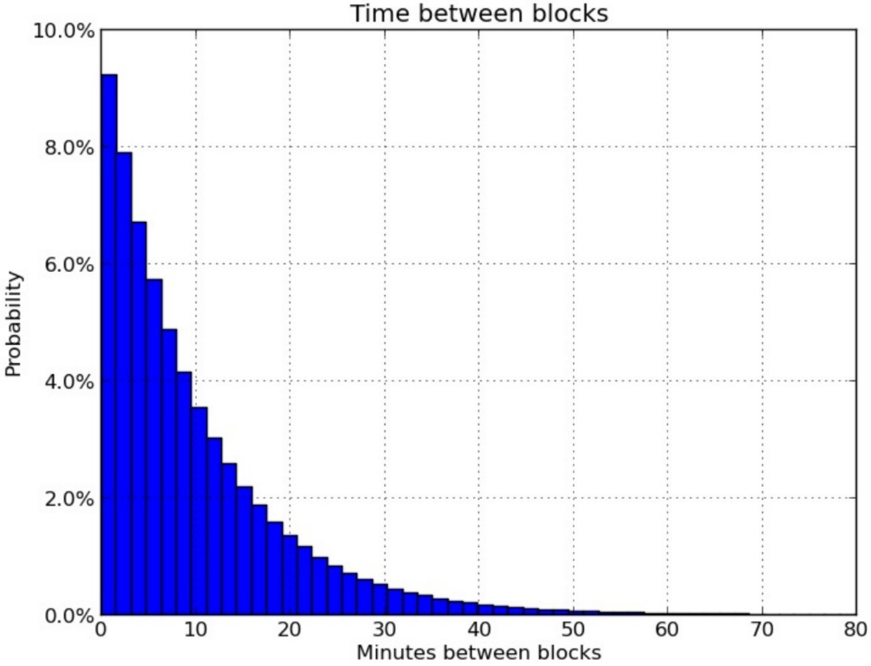
For a single miner:

- Probability of solving next block:

$$P = \frac{hash\ power}{global\ hash\ power}$$

- Mean time to find a block:

$$\frac{10\ minutes}{P}$$



- 0.01% of the hash rate → one block every 69 days

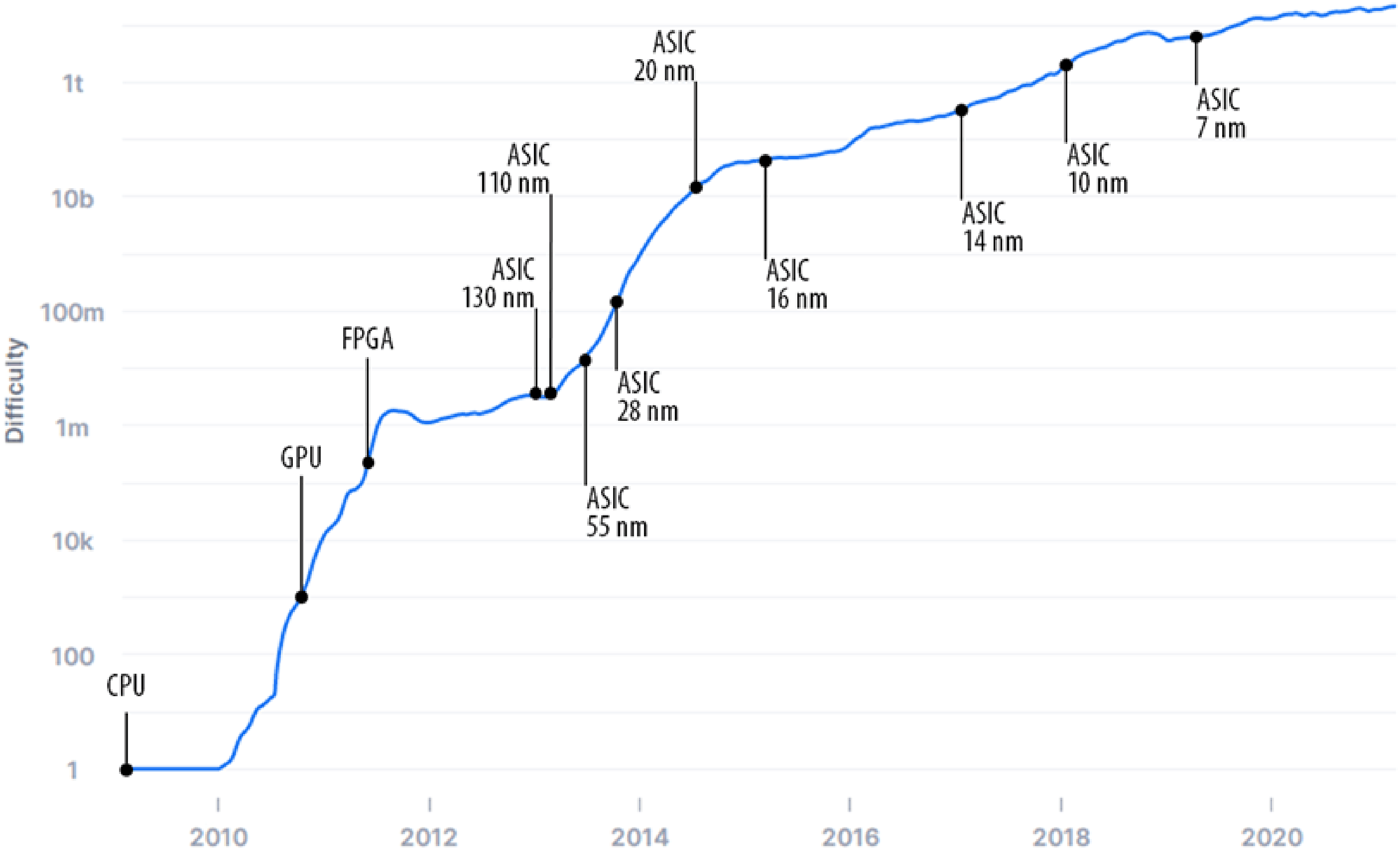
Key Idea: Difficulty Adjustment

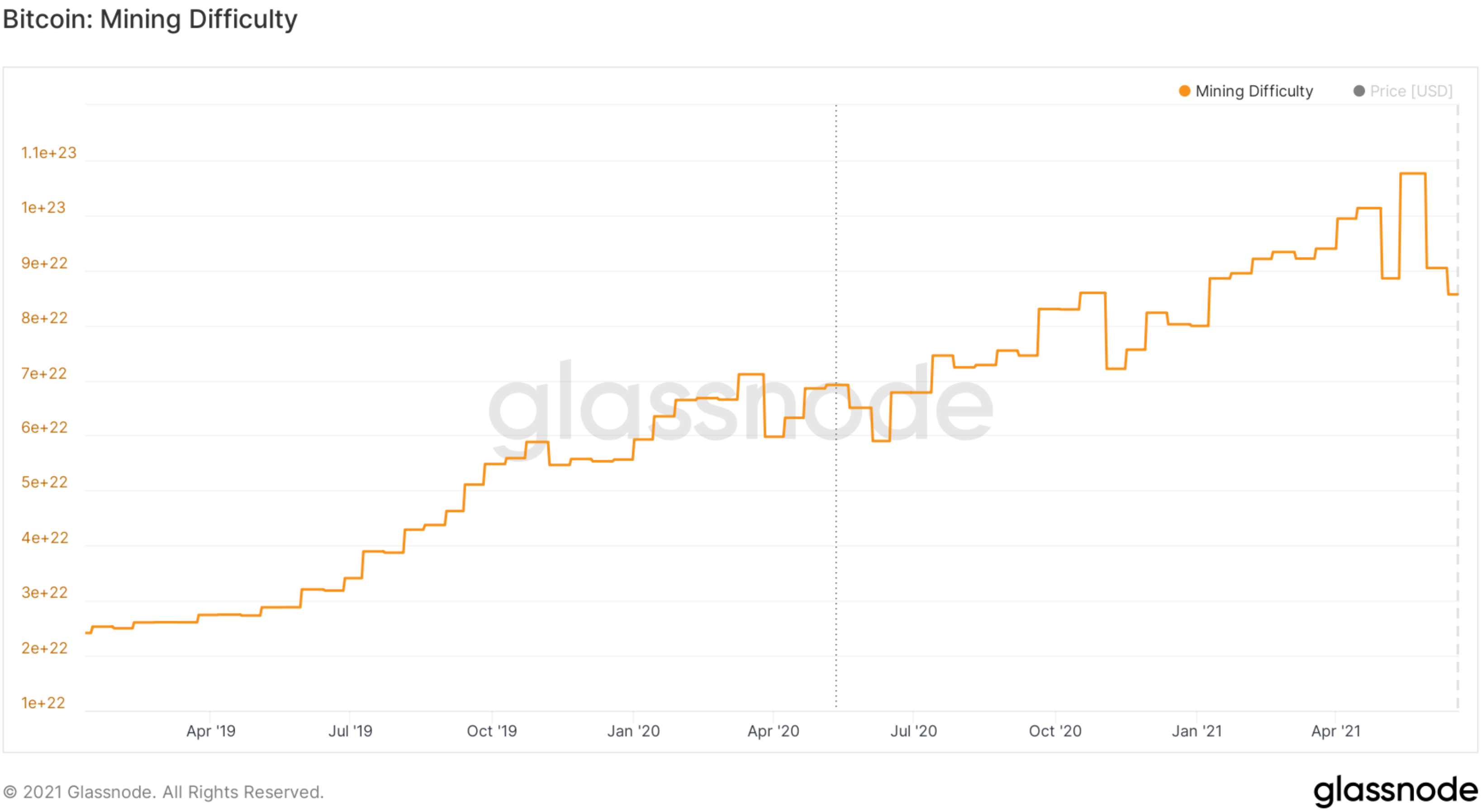
- The number of zeros required in the resulting block hash represents a “difficulty”
- Bitcoin protocol updates it periodically so that a new block is created on average every 10 minutes
- If more nodes add computing power, the number of zeros required is **automatically updated** by the protocol (more zeros → more difficulty).

Network Difficulty

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

Source: Blockchain.com / "The Evolution of Bitcoin Hardware" by Michael Bedford Taylor (University of Washington) / CoinDesk Research





Bitcoin: Mining Difficulty

© 2021 Glassnode. All Rights Reserved.

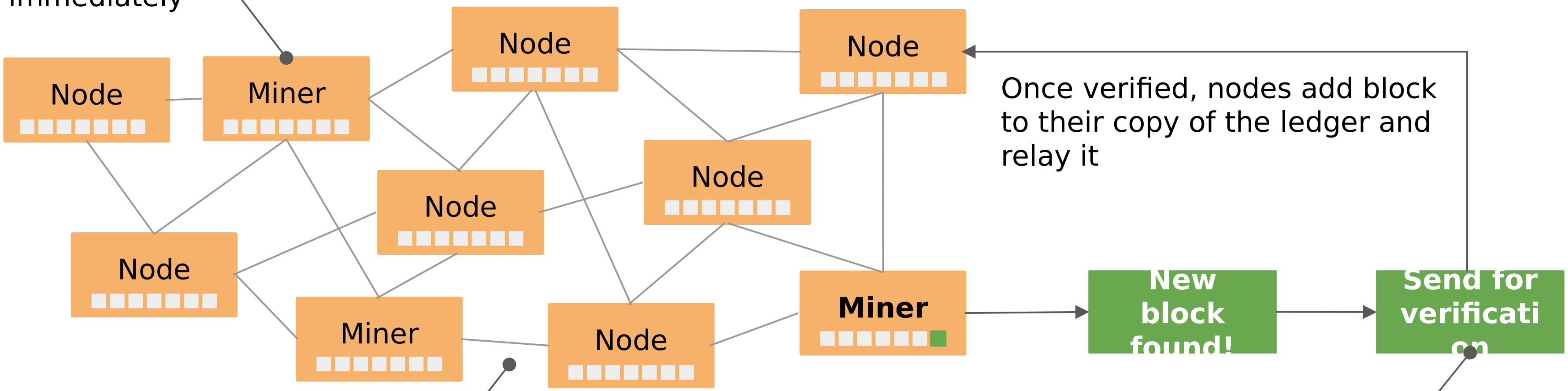
https://studio.glassnode.com/metrics

Miner Logic

Strategic issues	Default behavior
transactions to include in the next block	any transaction above minimum fee; if block is full, then prioritize transactions with higher fees
block to mine on top of	head of the valid chain with higher cumulated difficulty
criteria for choosing between equivalent valid blocks	first block heard
when to announce a new just-finalized block	immediately after finding it, to maximize the chance of entering the reference chain

Nodes verify the validity of newly mined blocks

Game theory suggests that miners begin mining next block immediately



Once verified, nodes add block to their copy of the ledger and relay it

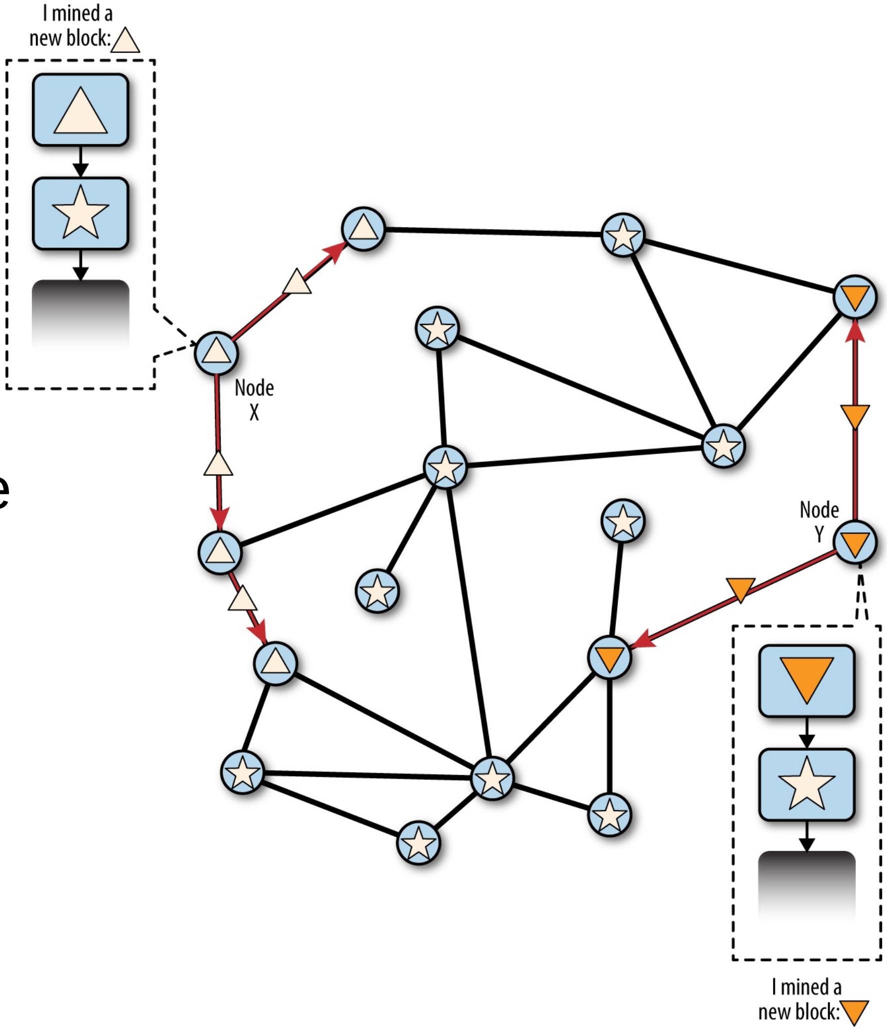
Critical that verification remain a decentralized process to keep miners honest

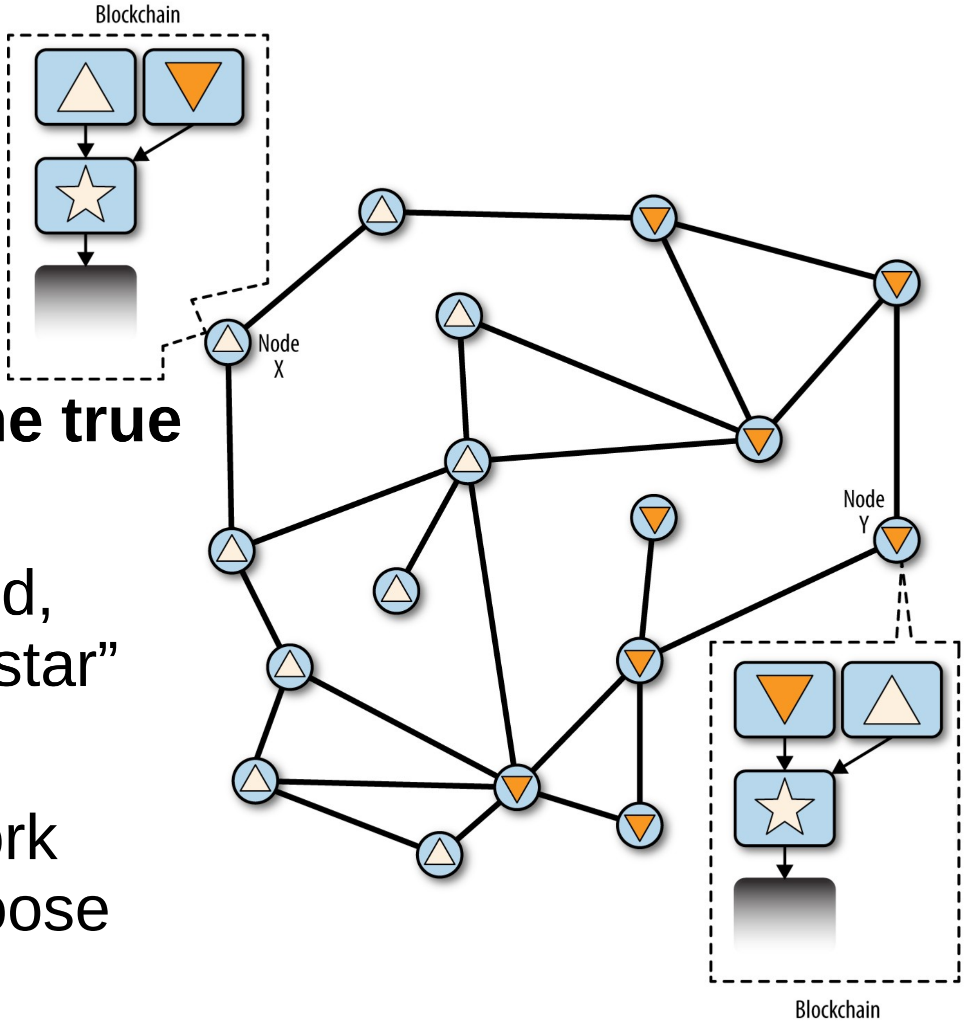
Blocks are valid if they:
1. Obey protocol rules
2. Meet PoW requirements

In rare case, particular situations can occur:

- While searching for the next Nonce, using the hash of the last block (white star) two miners find two different blocks with an hash that satisfies the current required difficulty

- Each of them will start broadcasting its own “vision” of the current blockchain status

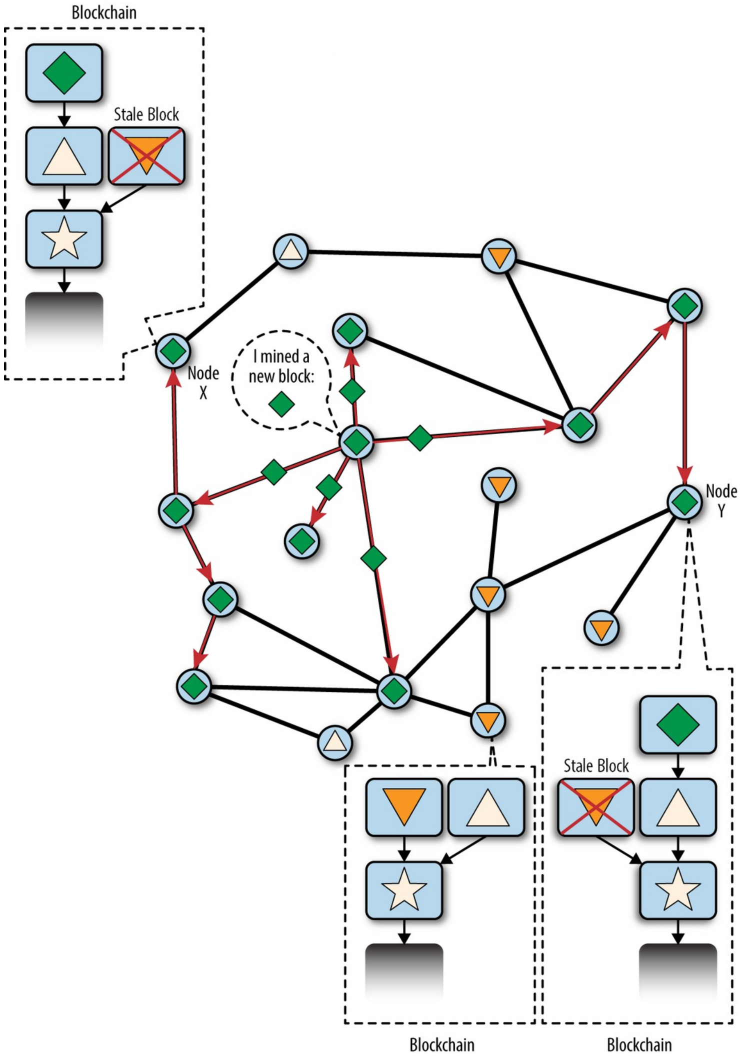




We cannot say that one is the true one, and the other is false:

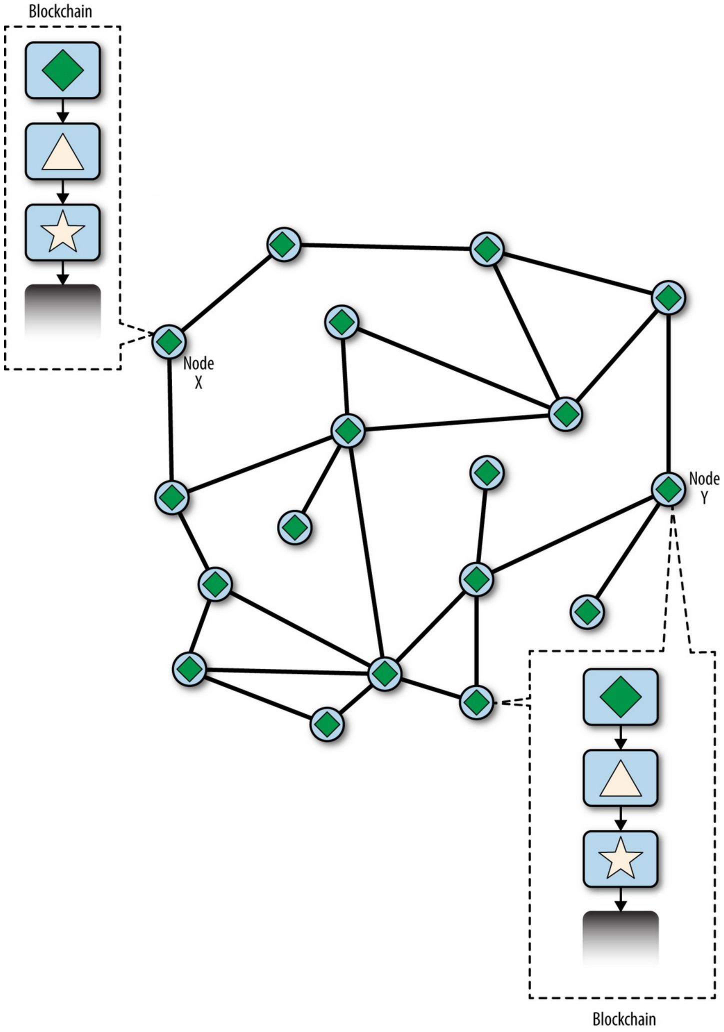
- They are both correctly mined, using the hash of the “white star” block.
- But, depending on the network condition, each node will choose the first received

- Suppose a miner belonging to the “white triangle” branch of the chain finds the next block (green square), it will add to that chain
- Now, the “green square” chain, based on the “white triangle”, is the longest chain
- Notice: we are still not 100% sure that this will be the block sequence, because the other is only one block shorter
- In theory, another “coincidence” could happen, and a node of the “orange” side could find a block and make the chains of the same length



There are 10 mins on average between blocks, and new blocks are propagated very quickly, so eventually one of the will prevail as the longest.

Notice: all the transactions that were included in the “orange triangle” but NOT in the “white triangle”, will be put again in the waiting list (**memory pool**)



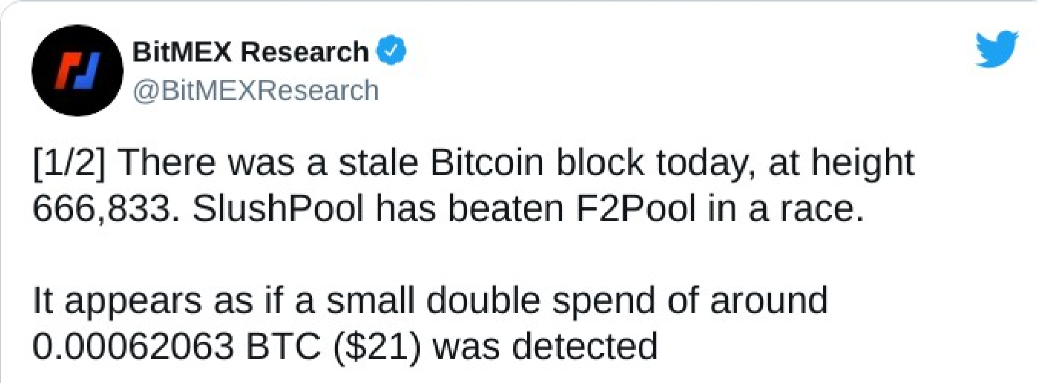
The double spend saga

Bitmex Research first reported a small double spend detected on the blockchain.

No, actually never happened...

More study about Bitcoin suggested ;)

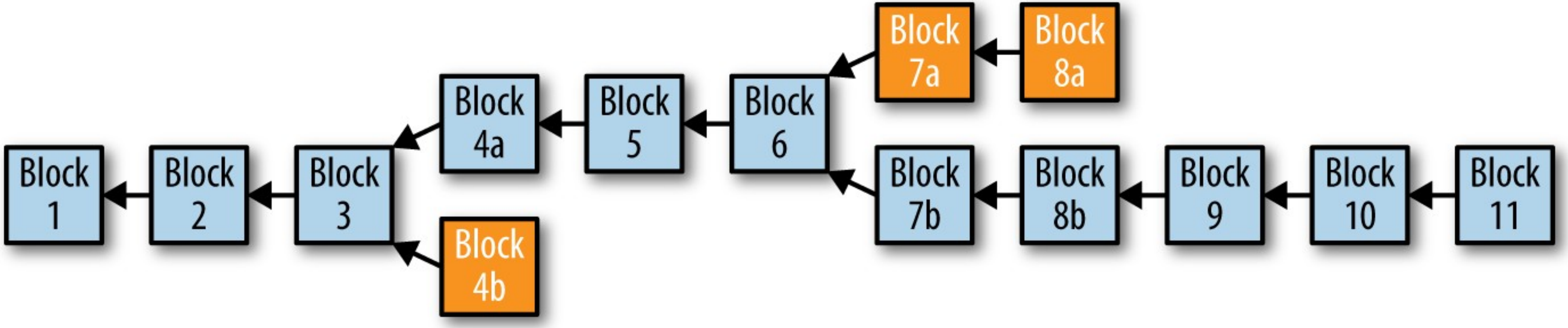
=========================>

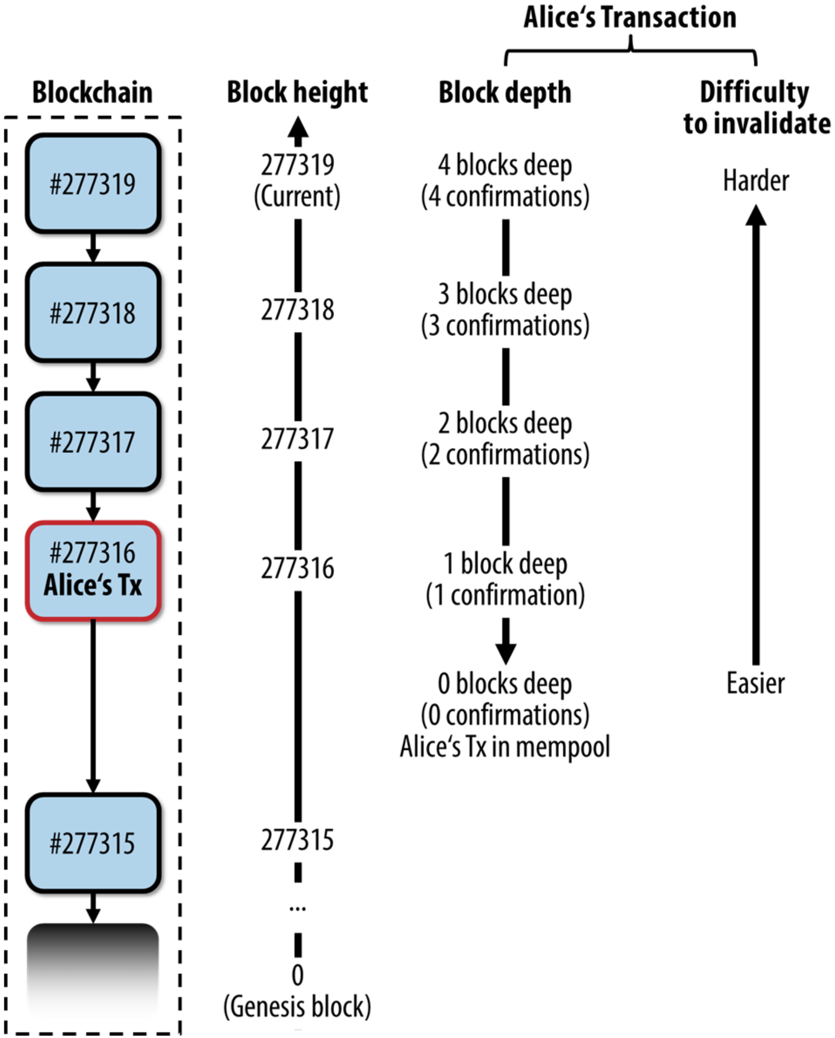


BitMEX Research
@BitMEXResearch

[1/2] There was a stale Bitcoin block today, at height 666,833. SlushPool has beaten F2Pool in a race.

It appears as if a small double spend of around 0.00062063 BTC ($21) was detected



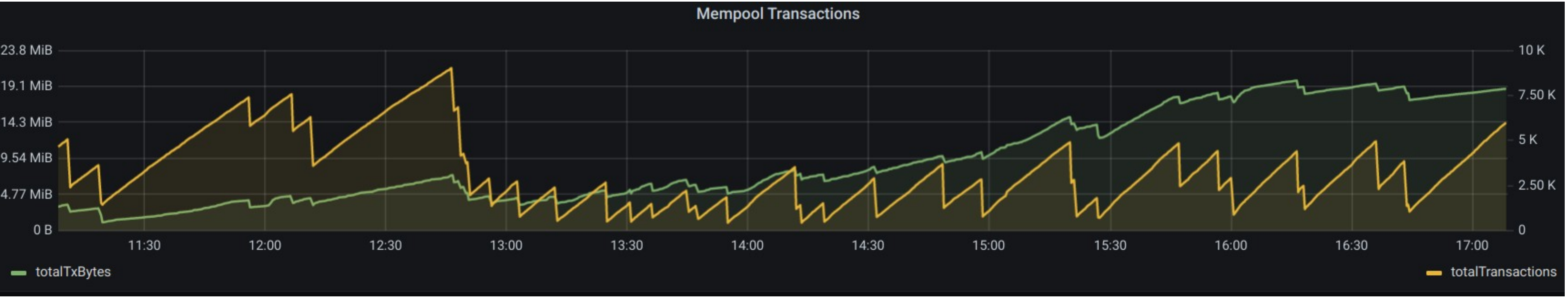


- Because of the proof-of-work, the chances of a block being altered decrease exponentially with the number of blocks chained after it
- The chain of blocks is a history of transactions resilient to network attackers because it cannot be altered without huge resources
- The number of confirmations an user should wait depend on relevance of the transaction

- Checkout the current memory pool at:

  statoshi.info
- Empty pool → less competition for being included in the next block → good moments for moving
- Funny, but real:

  https://txstreet.com/v/btc



Mining Alone…it's so sad

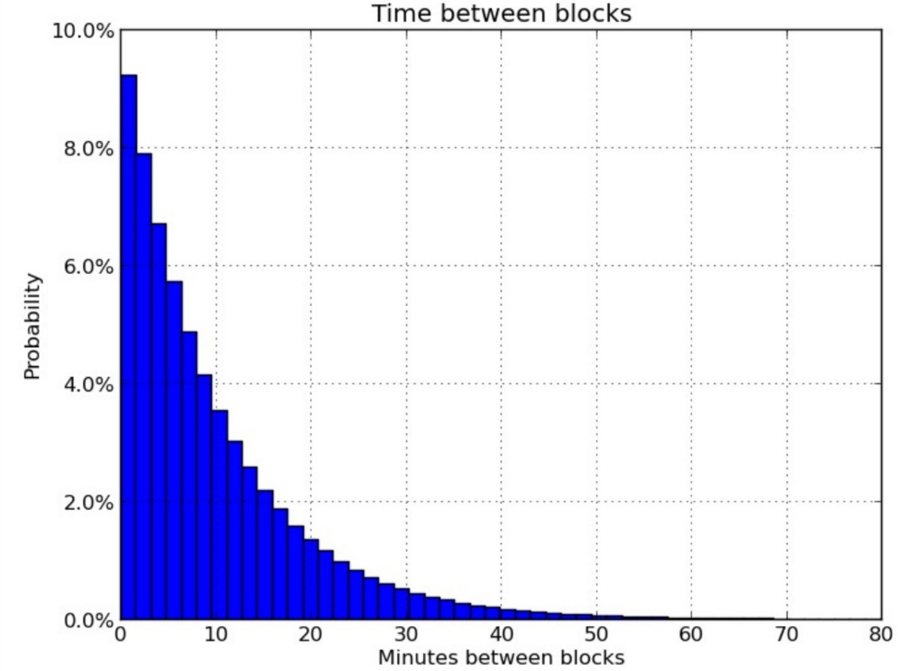
For a single miner:

- Probability of solving next block:

$$P = \frac{hash\ power}{global\ hash\ power}$$

- Mean time to find a block:

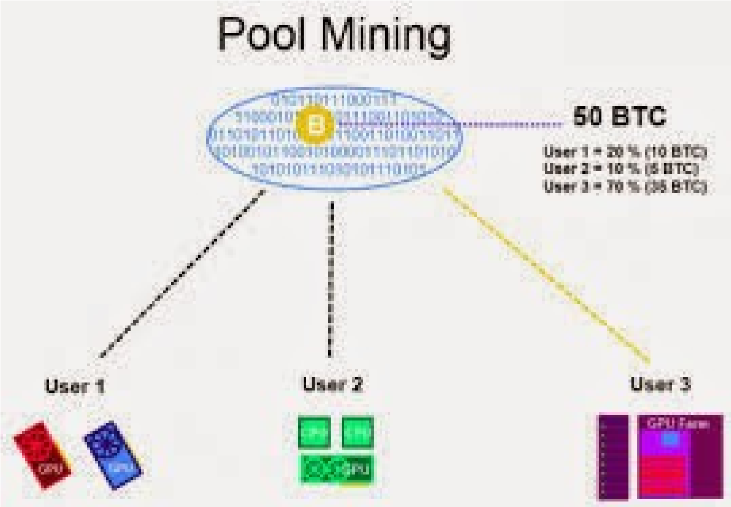
$$\frac{10\ minutes}{P}$$

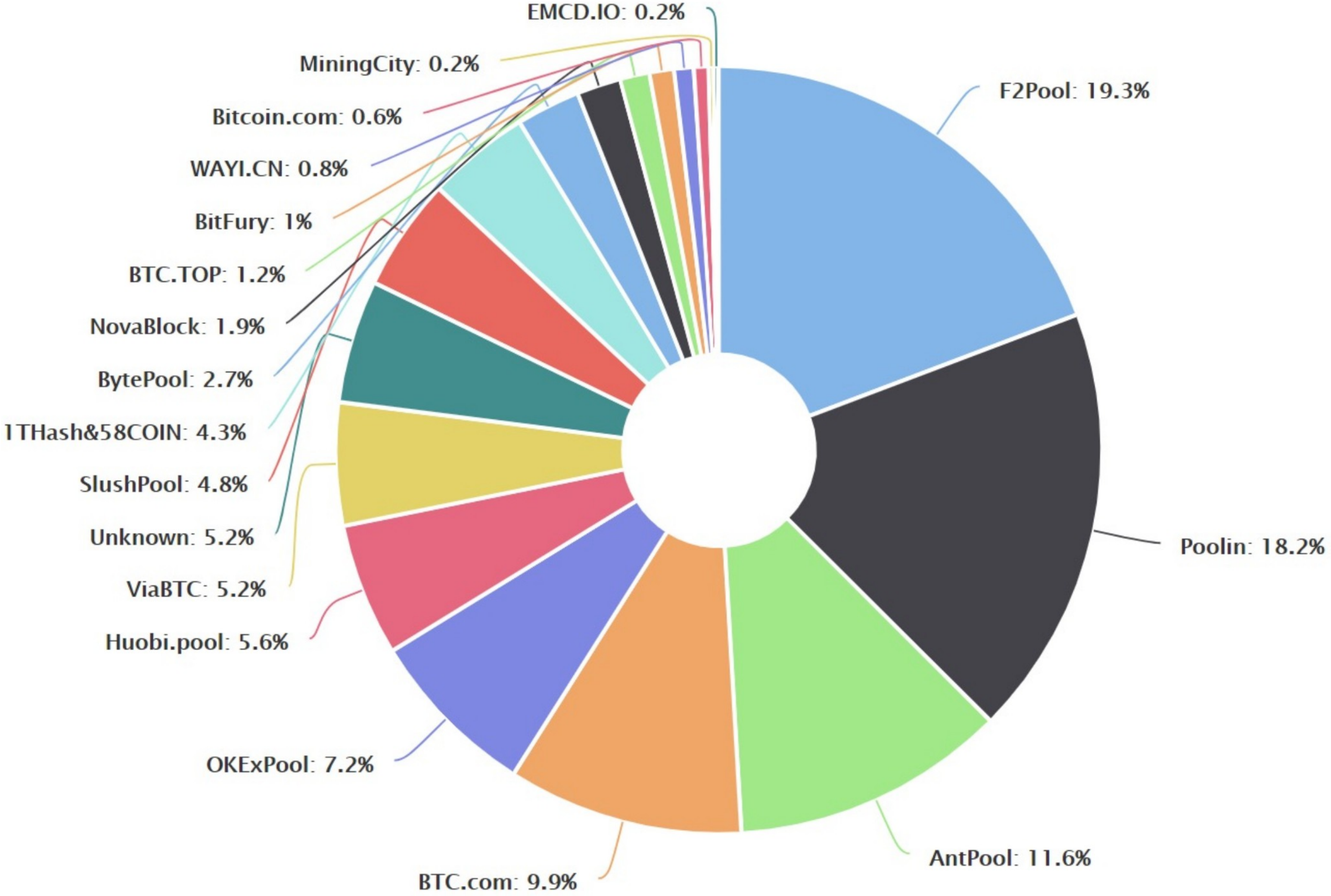


- 0.01% of the hash rate → one block every 69 days

Mining Pools

- Statistical variance kills small miners
- Stratum mining pool protocol https://slushpool.com/help/stratum-protocol/
- Pool manager creates the block template to be mined by pool members, with the reward going to a pool-controlled address
- Pool members all attempt to finalize the same block (with different nonces)
- Pool manager distributes revenues based on mining share




EMCD.IO: 0.2%
MiningCity: 0.2%
Bitcoin.com: 0.6%
WAYI.CN: 0.8%
BitFury: 1%
BTC.TOP: 1.2%
NovaBlock: 1.9%
BytePool: 2.7%
1THash&58COIN: 4.3%
SlushPool: 4.8%
Unknown: 5.2%
ViaBTC: 5.2%
Huobi.pool: 5.6%
OKExPool: 7.2%
BTC.com: 9.9%
AntPool: 11.6%
Poolin: 18.2%
F2Pool: 19.3%

FUD Questions

- **FUD**: *fear, uncertainity, doubt*
- Some recurrent topics seems among people outside the technology
- **Not necessarily unmotivated:** It happens for every disrupting tech (e.g., internet, electricity)
- FUD has a positive side anyway: **motivating yourself towards a better understanding**

FUD Classics: *“Mining is a waste of energy”*

Energy usage cannot be discussed **ignoring the purpose of its usage:**

*“All Washing machines of the world globally consume **XYZ** ”*

- It’s always a trade-off, you don’t clean clothes, you have more free time, etc…
- Pushing towards clean energy production (carbon free) & more efficient Washing Machines, **NOT just discussing XYZ**

Bitcoin network provides a cross-country, open and trustless way to transfer digital value with near-zero fees in a few minutes

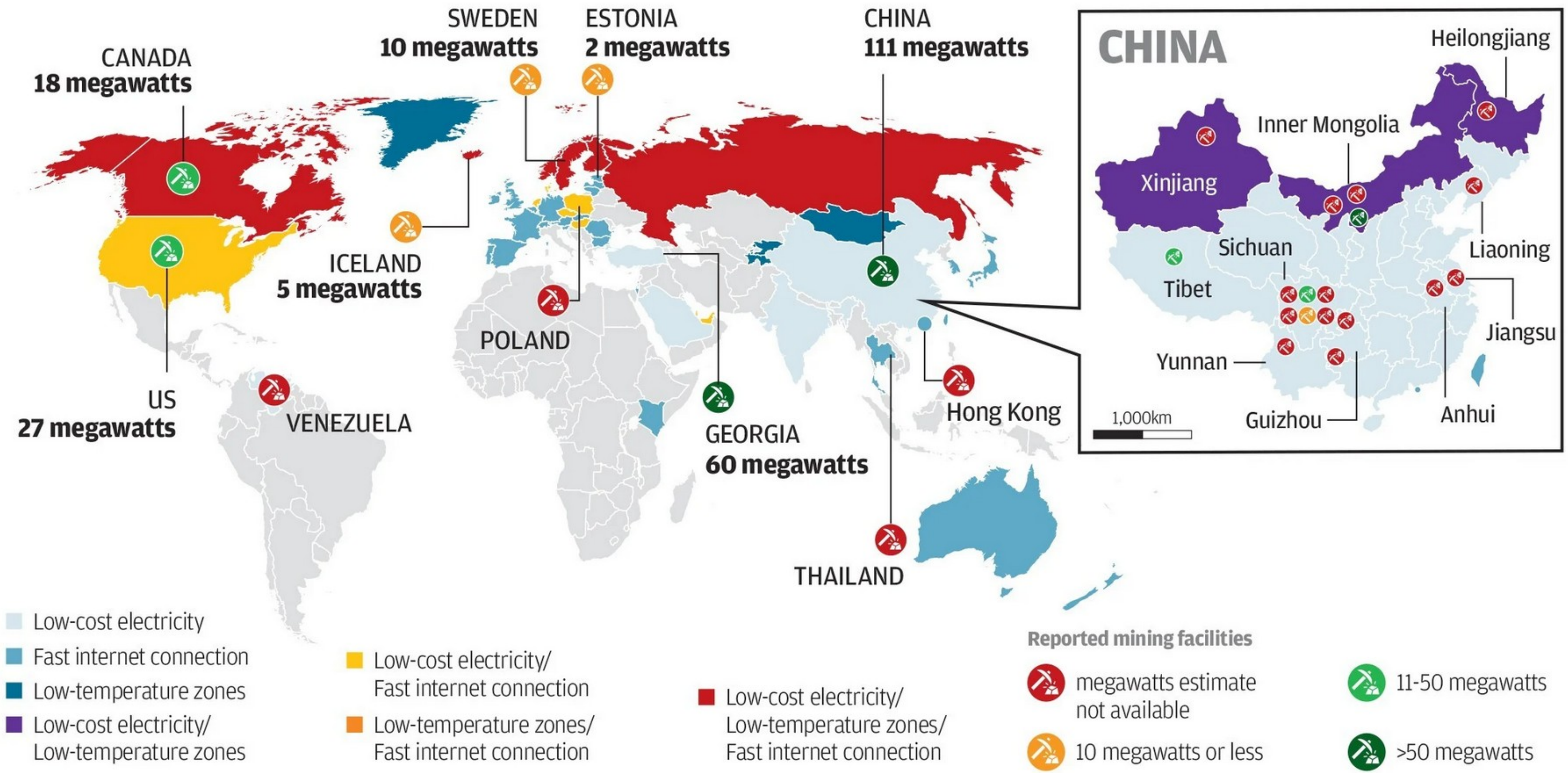
- a more appropriate comparison should be against the total energy usage of the entire international wire transfer/ cash system *(offices, people using cars to go to such offices, servers, ATM etc...)*
- ...or against gold mining, if we think BTC asset as a “store of value”

https://bitcoinminingcouncil.com/wp-content/uploads/2021/07/2021.07.01-BMC-Q2-2021-Materials.pdf

...But also mining has a unique feature that differs from other industry energy use cases:

- It **doesn’t care about the place** (mining hardware can move)
- The gain margin is on the cost of the energy, so **miners will to the push for the cheapest energy on the market**
- Since carbon taxes are going to be applied globally to energy production, **the cheapest for of energy is the renewable energy, especially the one wasted when cannot be consumed locally**

Global cryptocurrency mining sites



Source: University of Cambridge

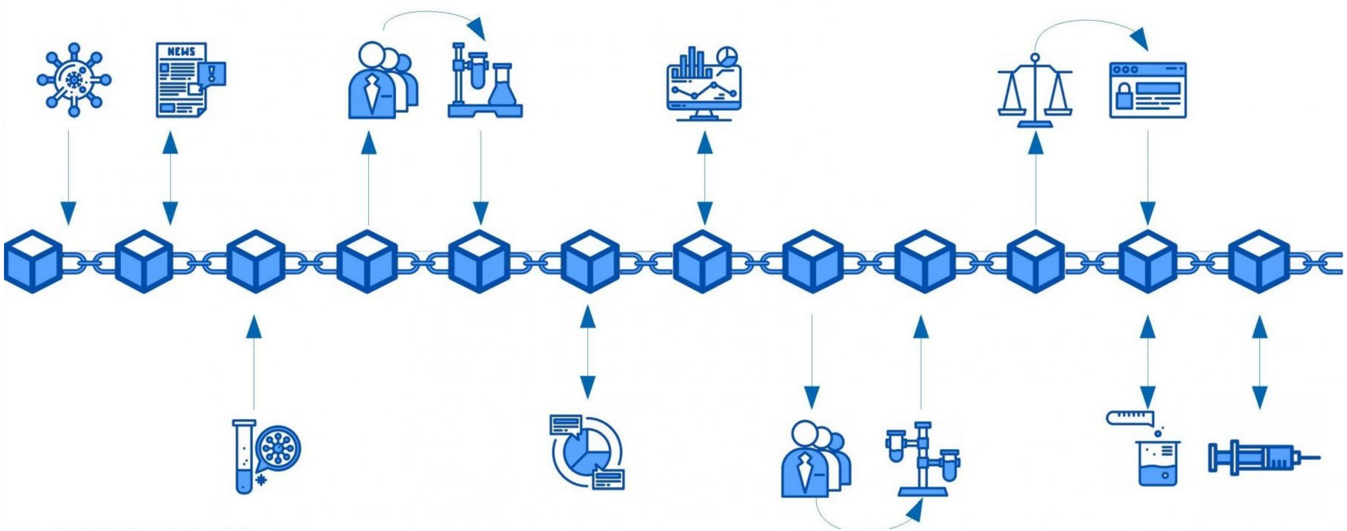
SCMP

Impossible Mission?

1)We must guarantee the order of events

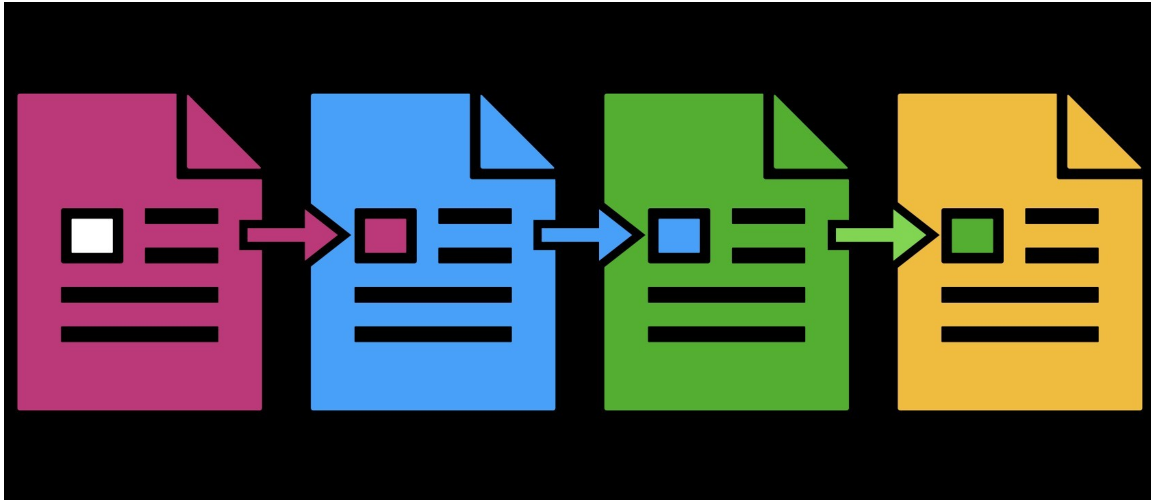
2)Ensure that sender and receiver are the correct ones

3)Entities not trusting each other agree on some “digital reality”



Blockchain = Timechain

Causality: it’s impossible to calculate the hash a block before the previous

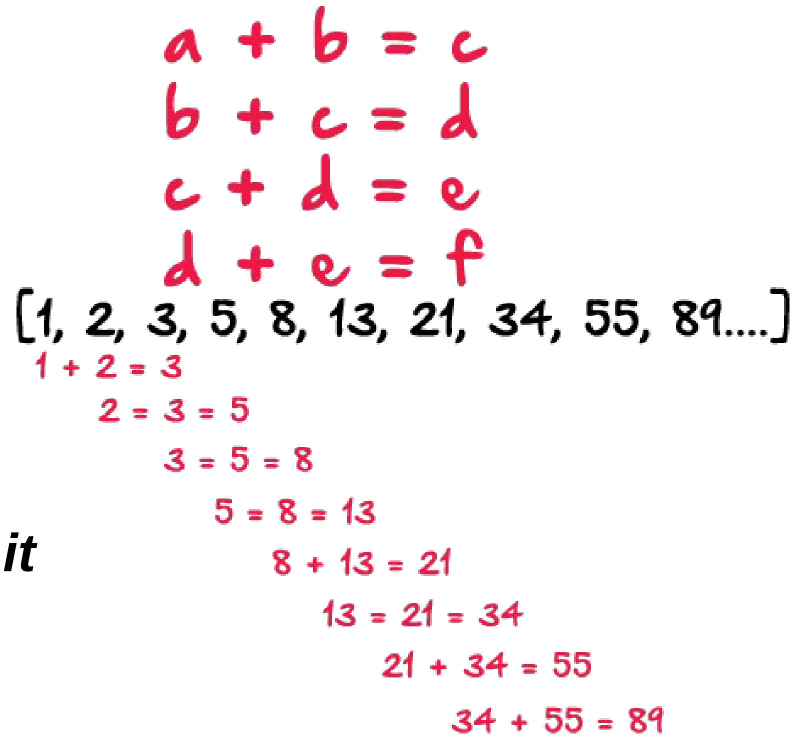


Causality is not sufficient...

Without this increase in entropy, we could go forward and backward in time.

The sequence of Fibonacci Numbers, for example, is causal but not entropic. Every number in the sequence is caused by the two numbers that came before it.

*In that sense, **it is a causal chain. However, it is not useful to tell the time because it is entirely predictable.***



a + b = c
b + c = d
c + d = e
d + e = f

[1, 2, 3, 5, 8, 13, 21, 34, 55, 89....]

1 + 2 = 3
2 = 3 = 5
3 = 5 = 8
5 = 8 = 13
8 + 13 = 21
13 = 21 = 34
21 + 34 = 55
34 + 55 = 89

https://dergigi.com/2021/01/14/bitcoin-is-time/

Blockchain = Timechain

Unpredictability: it’s not possible which transaction events will be submitted to the next blocks → you cannot go forward into a future that still not happened