Scaling Blockchains: from Bitcoin to the Lightning Network

SPARC
Scheme for Promotion of Academic and Research Collaboration

Davide Patti
davide.patti@dieei.unict.it

SICILIAE STVDIVM GENERALE
· 1434 ·

Contacts

davide.patti@dieei.unict.it

https://github.com/davidepatti

https://www.davidepatti.it/

DISCLAIMER:
Science, Not Speculation

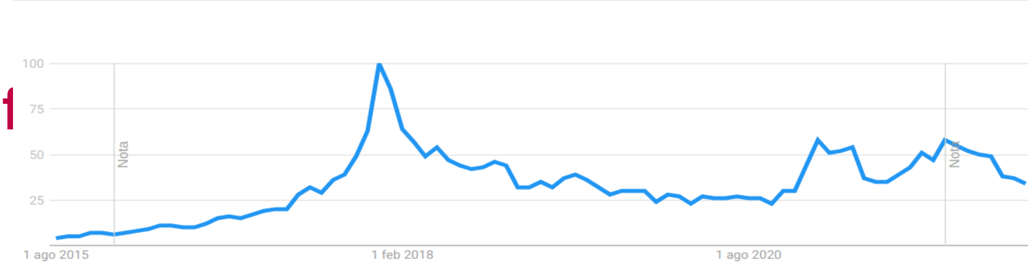
We will not discuss about prices, trading, speculation etc…

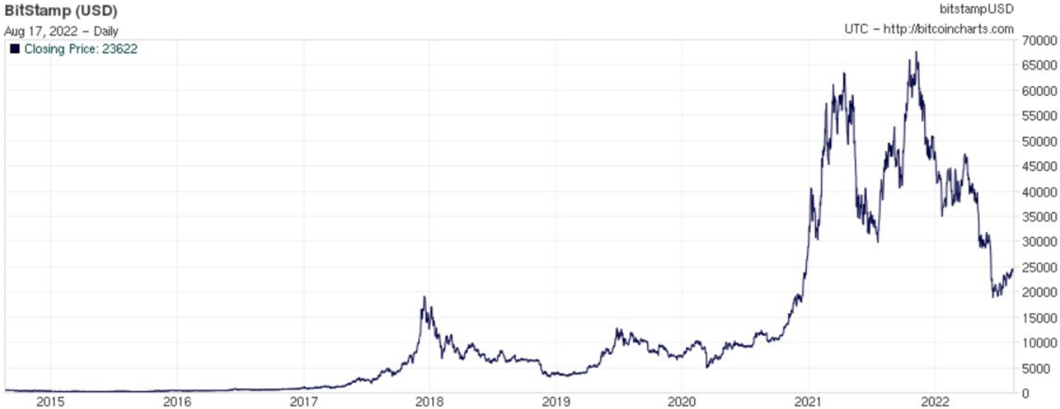
Price is only a consequence of the technology, not the origin

Look at recent past: why do we have the Web applications?

- *Because of an open TCP/IP protocol?*
- *...or because of Google and Apple stocks prices?*

“Blockchain” word seach (Google Trend)





“Blockchain”: Beyond the Hype

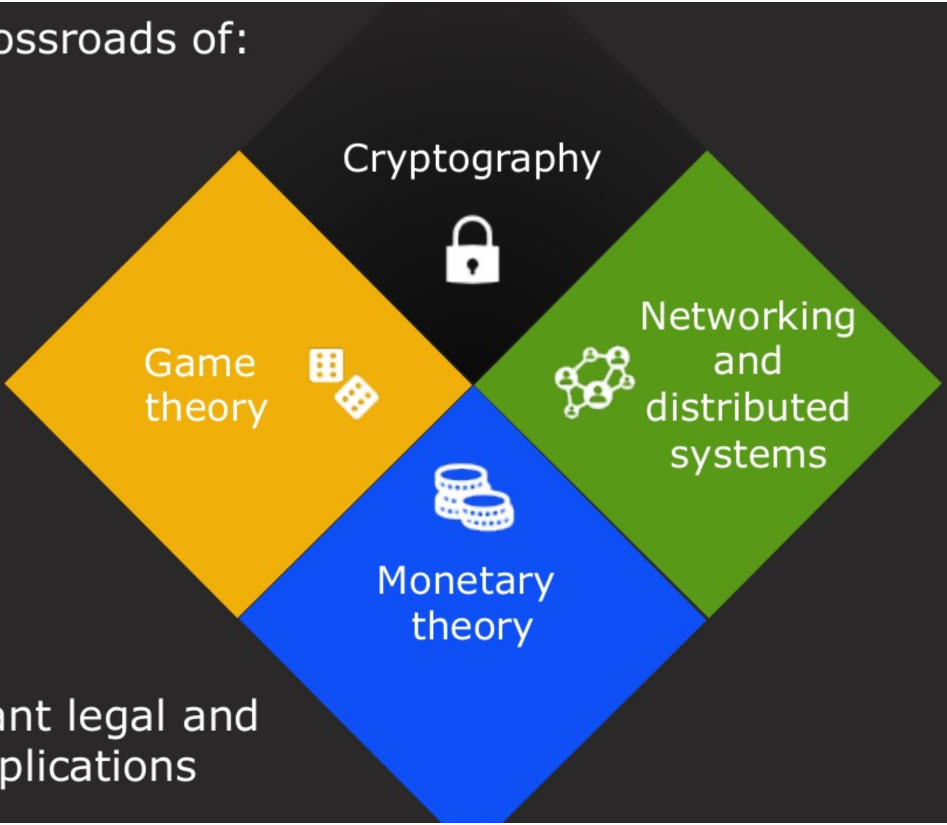
- Magic buzz-word for sounding “cool” (80% maybe non-sense)
- Potential revolutionary impact:
  - Understand when it makes sense
  - **...but EVEN MORE when it doesn’t**

Outline

- Physical VS Information Transfers
- Hash Functions, Proof-of-work, and Mining
- Asymmetric Cryptography
- Inside Blocks: Transactions
- Tools & Demo: Electrum
- Scaling Blockchains: The Trilemma
- Scaling to upper layers: The Lightning Network
- Open Research Topics and Challenges

Down to the “Rabbit hole”

At the crossroads of:



Cryptography

Game theory

Networking and distributed systems

Monetary theory

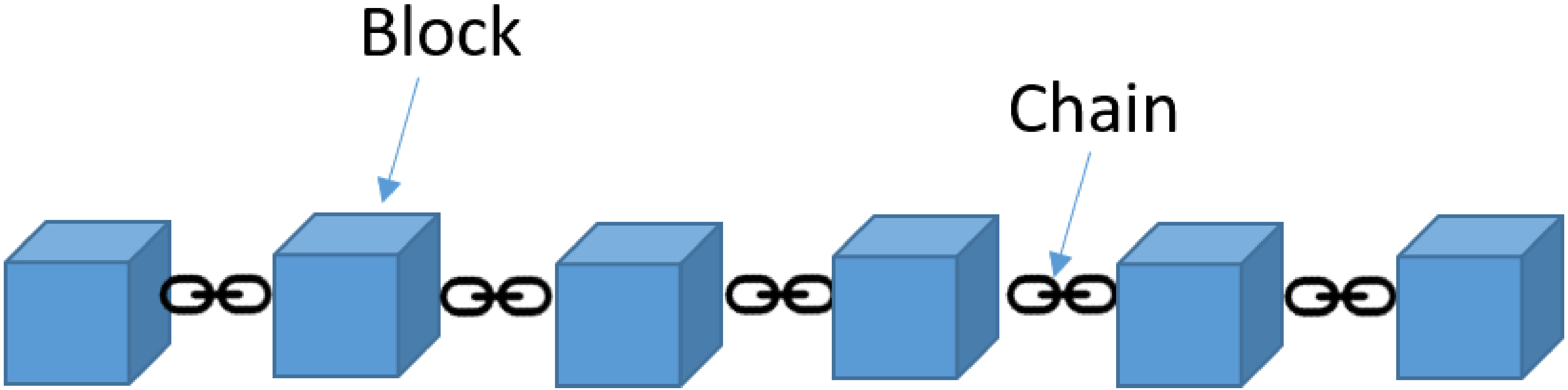
With relevant legal and political implications

Mainly not a technology,
a cultural paradigm shift
instead

It’s Time to Reveal The Truth:

It’s Time to Reveal The Truth:

A Blockchain is a Chain of Blocks



Sorry for the disappointment...

Some Questions Remain Open...

- *How are blocks chained?*
- *Why are blocks 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?*

Not a Good Term, after all

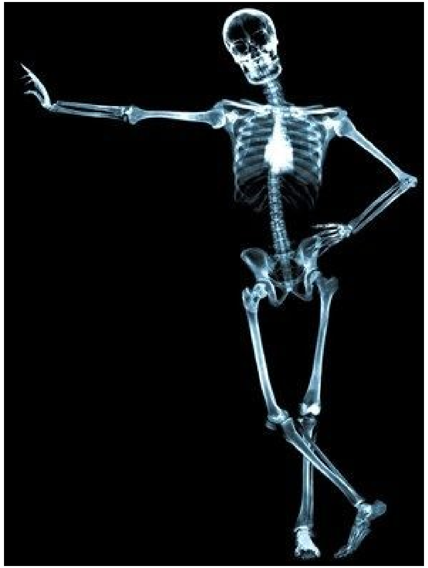
*“Bitcoin is a **blockchain** based technology”*

Not a Good Term, after all

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

is something like…

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



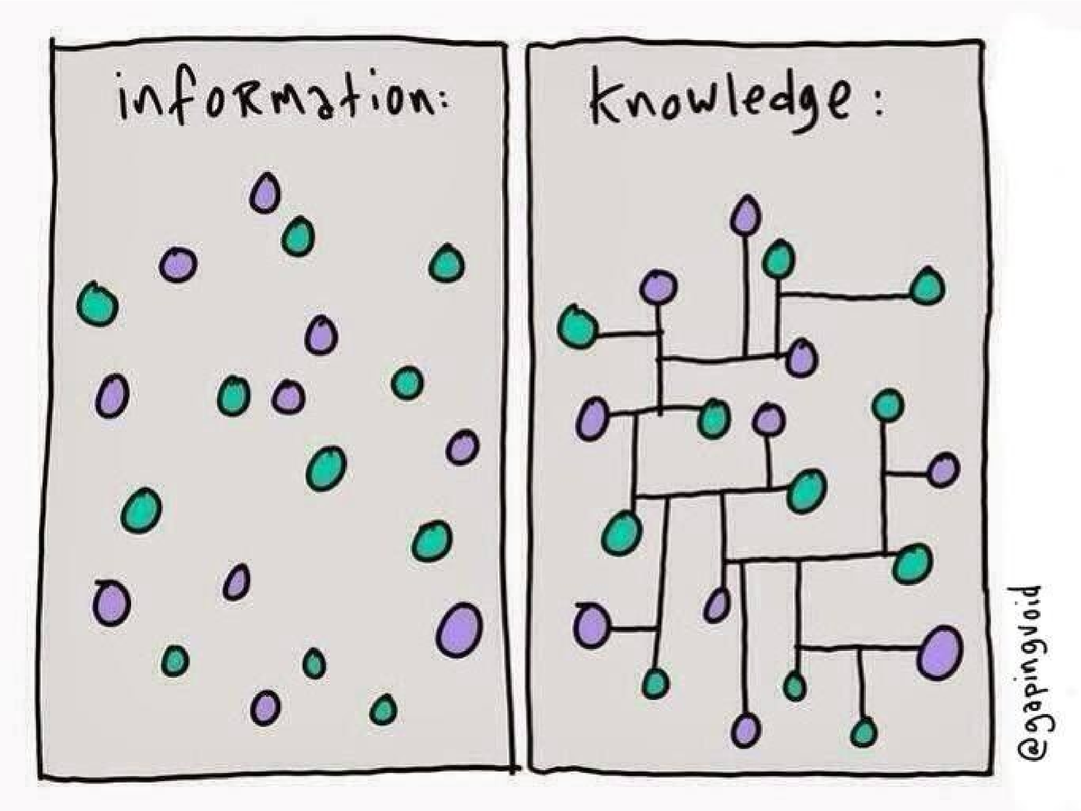
SAY BLOCKCHAIN
ONE MORE TIME
memegenerator.net

Enabling Key Concepts

Cannot understand blockchain without understanding:

- The origins and motivations behind **Bitcoin experiment**
- The mathematical ideas that makes it possible:
  - **Hash Functions, Asymmetric Cryptography**

….and how the different pieces related with each other



Outline

- **Physical VS Information Transfers**
- Hash Functions, Proof-of-work, and Mining
- Asymmetric Cryptography
- Inside Blocks: Transactions
- Tools & Demo: Electrum
- Scaling Blockchains: The Trilemma
- Scaling to upper layers: The Lightning Network
- Open Research Topics and Challenges

Let’s start from a Question

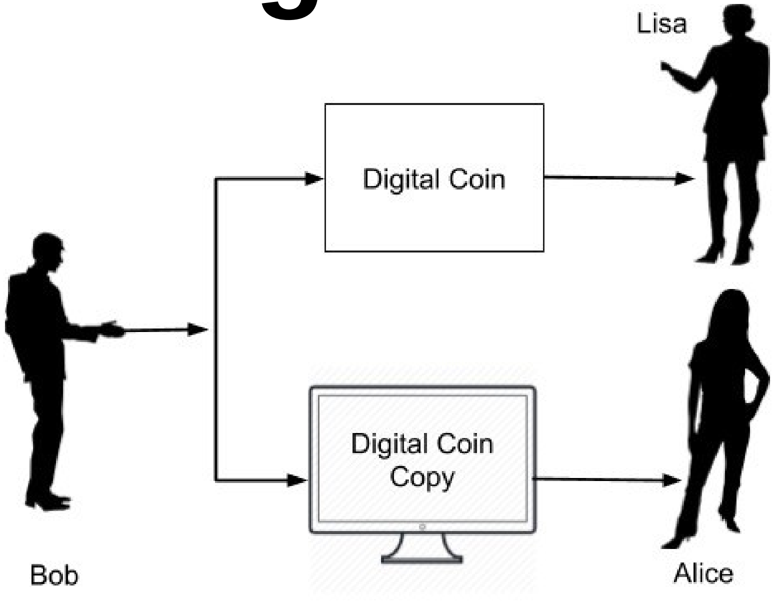
Is it possible to transfer something that is purely digital (information)?

Example: Some digital good, an asset...whatever can be assigned **an owner**

The Double Spending Problem

“Sending” digital content is actually ... **“sending a copy”**

Example:
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.

Map

Relates to reality (if accurate)

Territory

Reality (by definition)

Information vs Physical Transfers

- **Physical Transfers don’t have this problem:**

  Representation = Reality

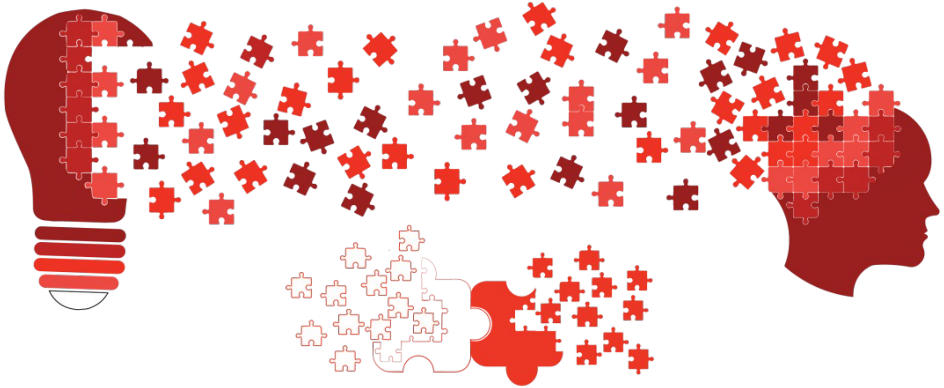
  - *Example: A physical apple*
- I can actually move a physical apple from A to B:
  - the apple is “represented” by the group of atoms

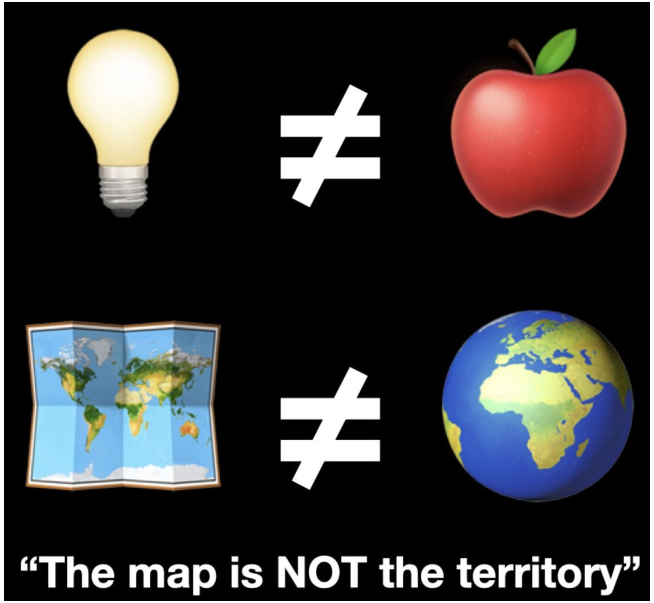
    ...but it also IS the the group of atoms

    Map and Territory are the same

Information Realm is different:

- If you can read the information, you can also copy it perfectly.
- There is no way to “hand over” information





*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)

Why bother? just exchange physical objects

- Historically known as “barter”,i.e., 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?

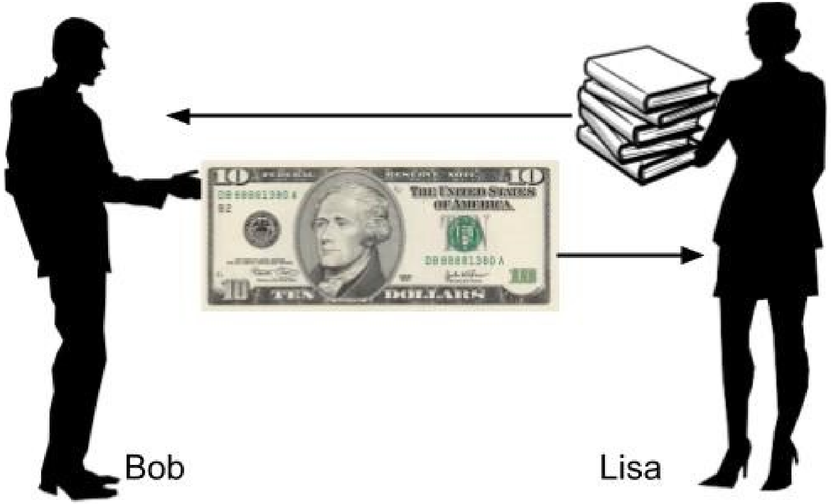
We need a way to make an “Indirect Exchange” of things, something that acts as a “medium”, as “store of value”

How to avoid direct exchange?

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

MONEY

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.

Let’s talk about money.

20
FEDERAL RESERVE NOTE
20
THE UNITED STATES OF AMERICA
C 159
ID228 [redacted] 60B
D4
UNITED STATES FEDERAL RESERVE SYSTEM
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
Anna Escobedo Cabral
Treasurer of the United States.
C3
ID228 [redacted] 60B
SERIES 2006
Secretary of the Treasury.
20
20
JACKSON
TWENTY DOLLARS

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

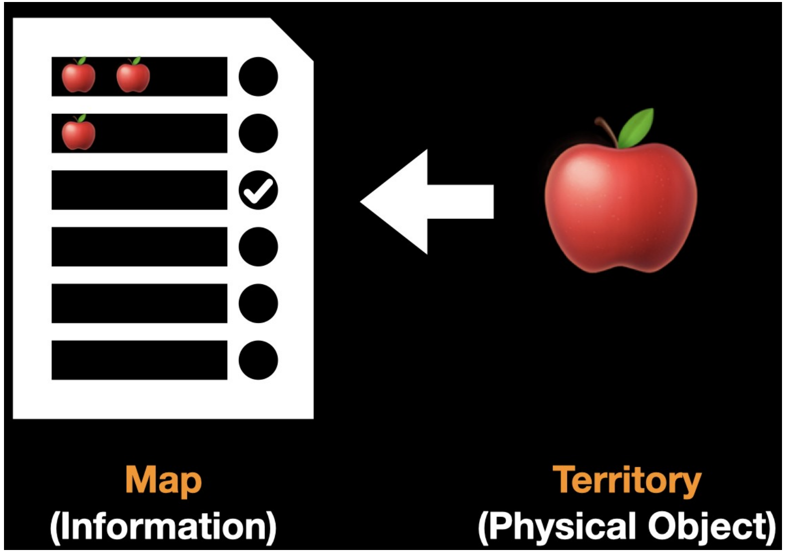
Gold: still used today. Notably as store of wealth for nation states.

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...)

From Physical Exchange to Ledgers

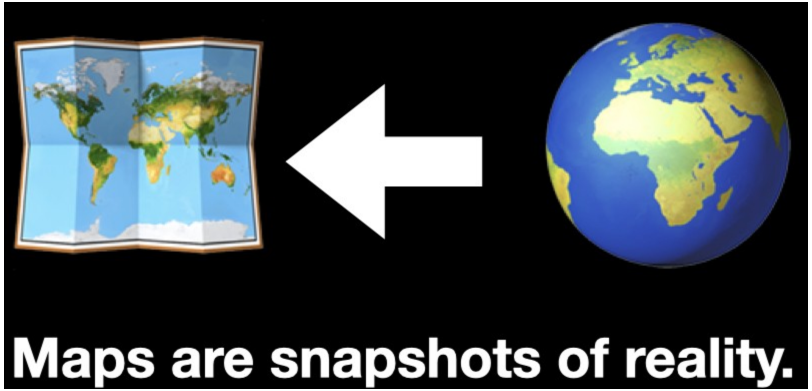
- You can either exchange physical objects/money directly
- ...or you can replicate the state of the world by writing down what "happened"



NOTICE: Tokens are inherently trustless; ledgers are not.

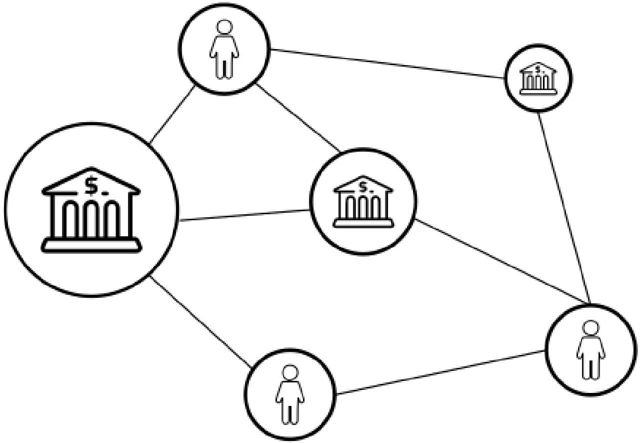
The Oracle Problem

- Every time you represent a real-world object as information, you run into **the oracle problem**: you need to trust someone so that the information reflects reality accurately.



Maps are snapshots of reality.

Traditional Exchange of Value



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?

Short Recap of Transfer

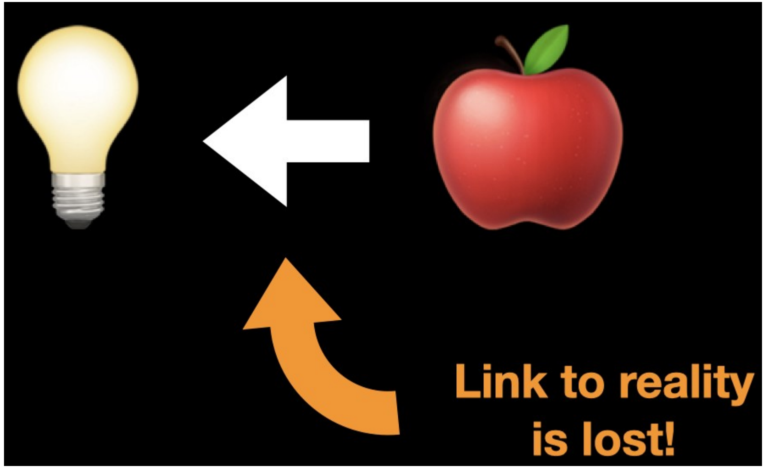
- Direct exchange of physical goods is ok (no trust required)
- ...but barter became unpractical
- Exchange of physical object used as “store of value” (money) was the solution
- ...but eventually the use of “ledgers” is needed in world-wide economy → trusted authorities

Let’s go back to Pure Information

It’s like having the Map(information) without having the Territory (physical object)

Same “trust” problems of ledgers...but even worse!

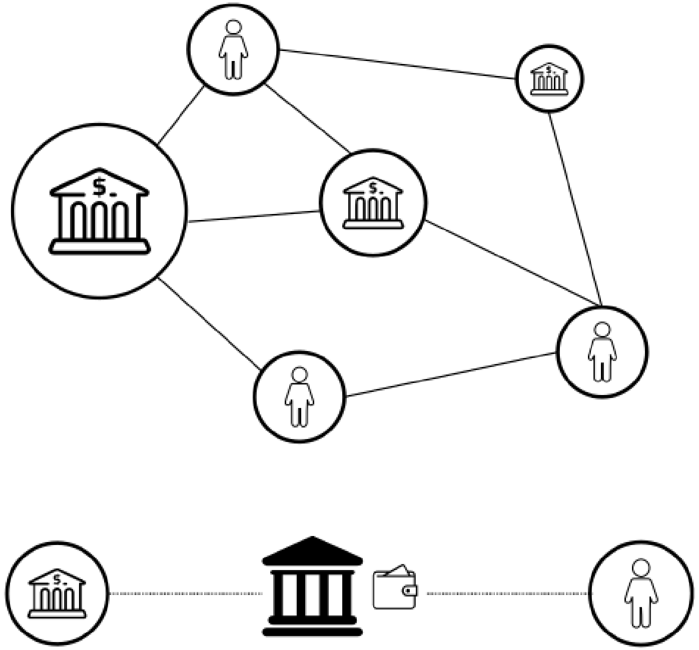
- Censorship/Reversal of events, there’s no physical “checkpoint”
- No replication cost!



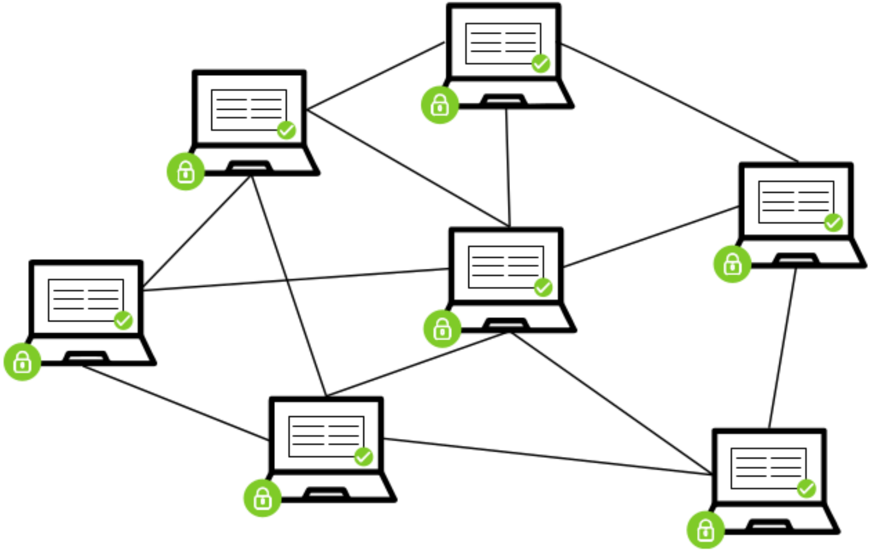
Main Question (revised version)

Is it possible to represent and transfer a purely digital asset **without requiring Trusted Authorities?**

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



- 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



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

Transaction data is immutable

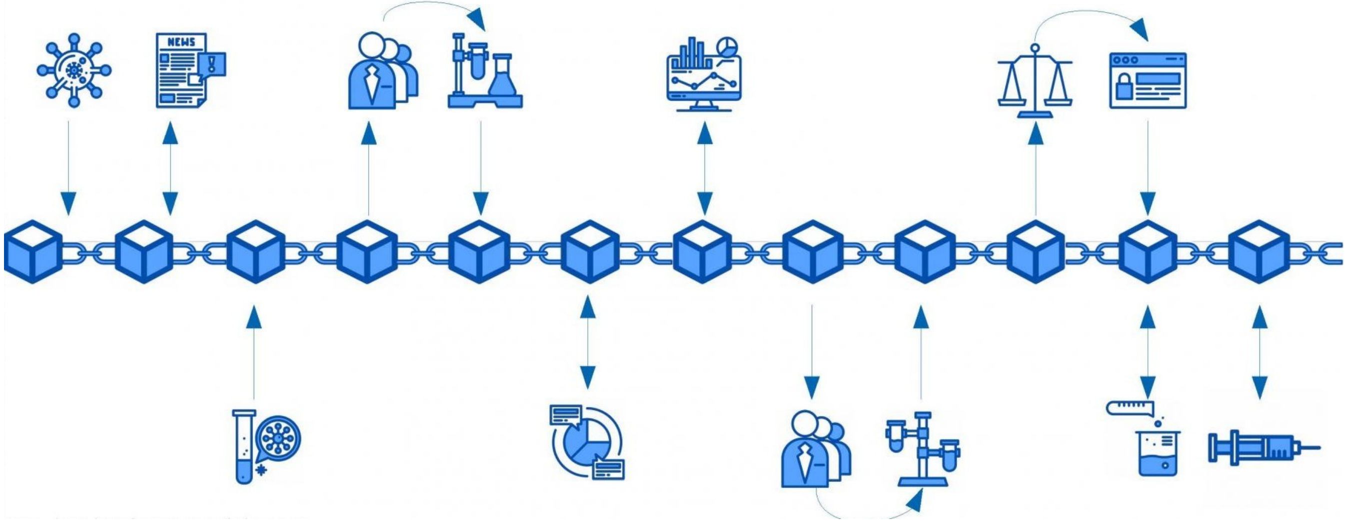
Peer to Peer transactions using digital tokens to represent assets and value

Mission (Impossible?)

1) No need for trusted source, not even a global notion of time

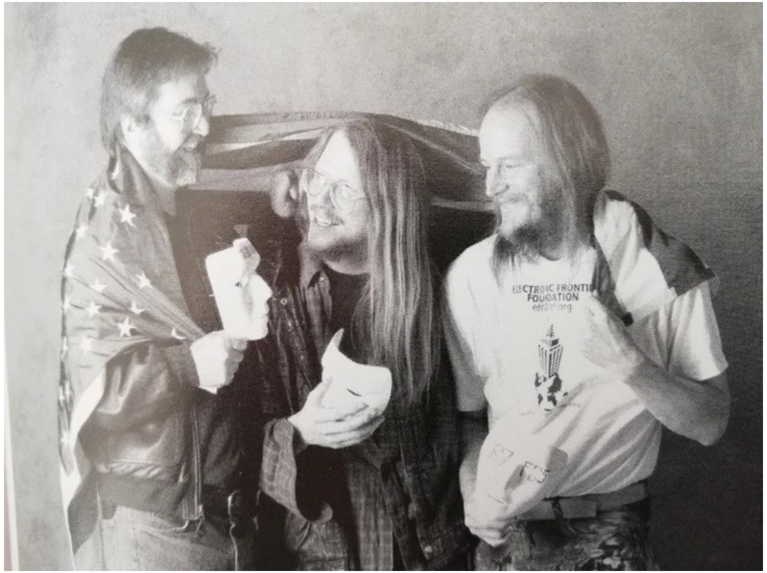
2) Agree on sender and receiver without trusted sources

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

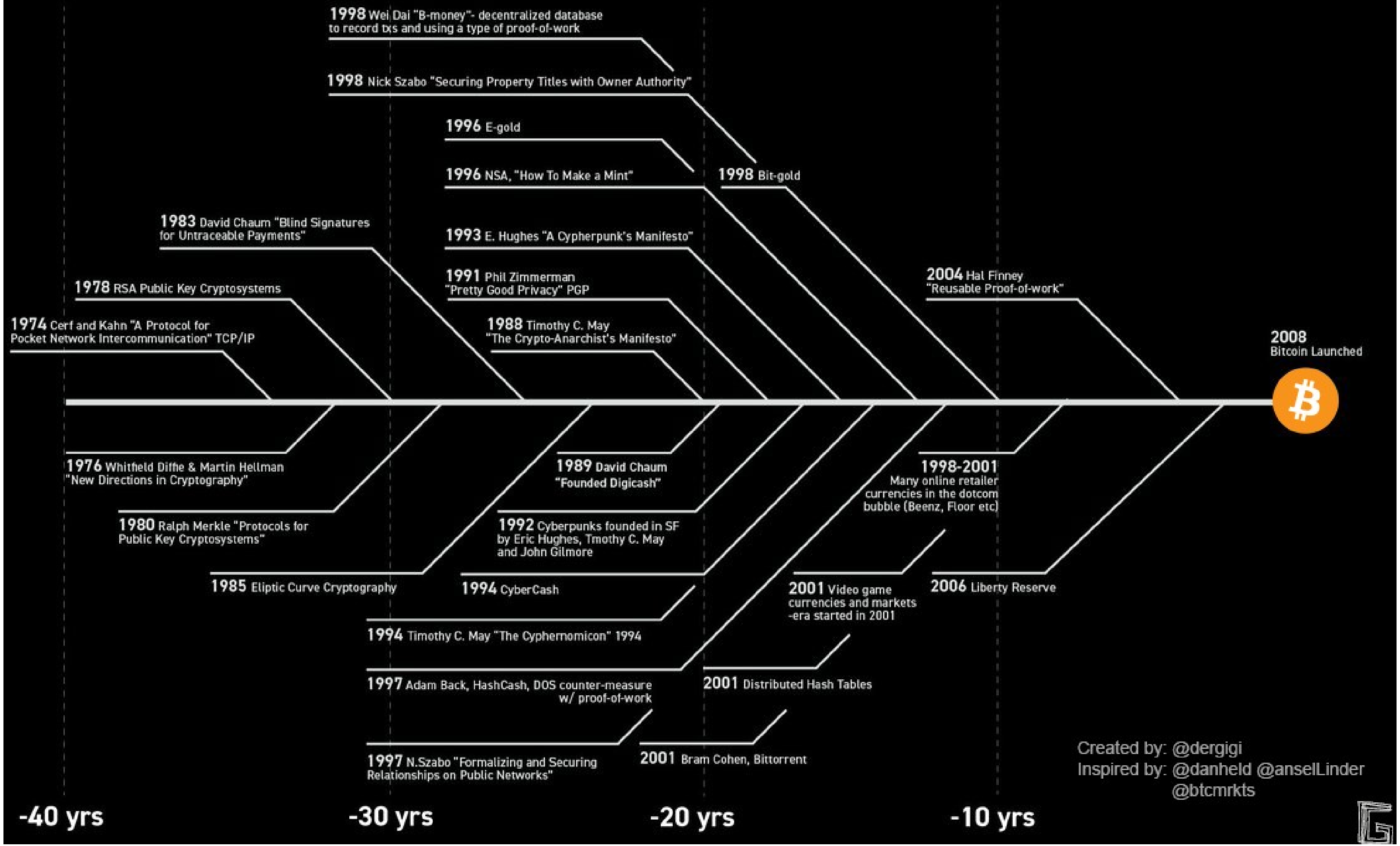


The CypherPunk Movement

- In 1992, three Bay Area computer scientists launched a new mailing list “**cypherpunks**” for discussing cryptography, mathematics, politics, and philosophy.
- The shared a core conviction: the Internet would soon become an important battleground for human freedom.
- Use cryptography to enable digital freedom and censorship-resistance



Bitcoin prehistory - It's the result of 40 years of research, development and demand



1998 Wei Dai "B-money"- decentralized database to record txs and using a type of proof-of-work

1998 Nick Szabo "Securing Property Titles with Owner Authority"

1996 E-gold

1996 NSA, "How To Make a Mint"

1998 Bit-gold

1983 David Chaum "Blind Signatures for Untraceable Payments"

1993 E. Hughes "A Cypherpunk's Manifesto"

1978 RSA Public Key Cryptosystems

1991 Phil Zimmerman "Pretty Good Privacy" PGP

2004 Hal Finney "Reusable Proof-of-work"

1974 Cerf and Kahn "A Protocol for Pocket Network Intercommunication" TCP/IP

1988 Timothy C. May "The Crypto-Anarchist's Manifesto"

2008 Bitcoin Launched

1976 Whitfield Diffie & Martin Hellman "New Directions in Cryptography"

1989 David Chaum "Founded Digicash"

1998-2001 Many online retailer currencies in the dotcom bubble (Beenz, Floor etc)

1980 Ralph Merkle "Protocols for Public Key Cryptosystems"

1992 Cyberpunks founded in SF by Eric Hughes, Tmothy C. May and John Gilmore

1985 Eliptic Curve Cryptography

1994 CyberCash

2001 Video game currencies and markets -era started in 2001

2006 Liberty Reserve

1994 Timothy C. May "The Cyphernomicon" 1994

1997 Adam Back, HashCash, DOS counter-measure w/ proof-of-work

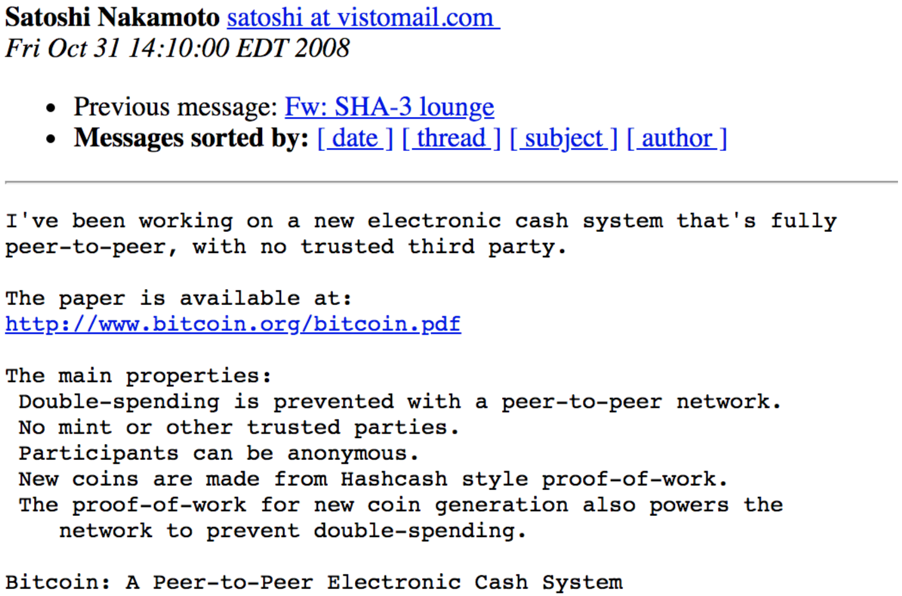
2001 Distributed Hash Tables

1997 N.Szabo "Formalizing and Securing Relationships on Public Networks"

2001 Bram Cohen, Bittorrent

Created by: @dergigi
Inspired by: @danheld @anselLinder @btcmrkts

- Years of failed attempts, mainly due to centralizalization points
- On Oct 31, 2008, an unknown user (Satoshi Nakamoto) posted a message with a paper



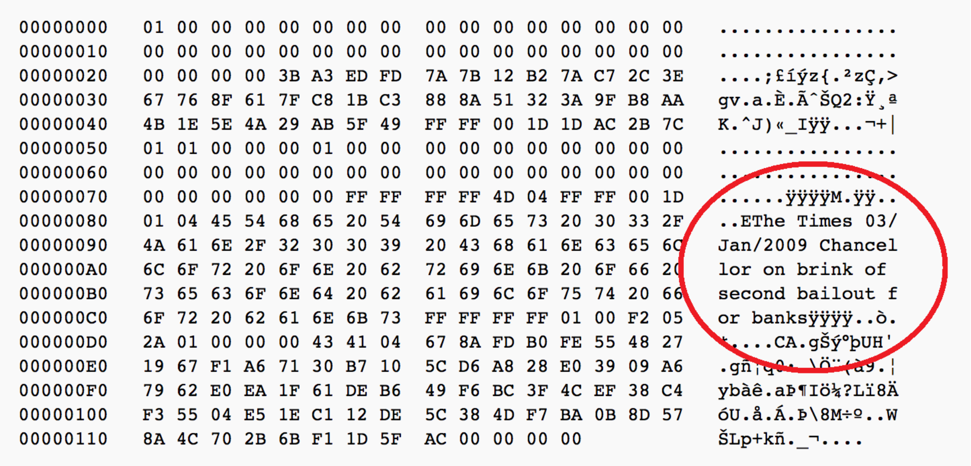
Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System
```

https://bitcoin.org/bitcoin.pdf

An opensource implementation was released and on Jan 3d, 2009, the first genesis block was mined

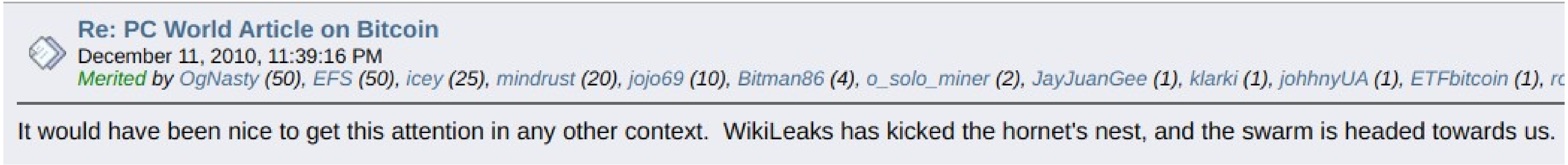


```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

THE TIMES
£1.50
Eat Out from £5
More than 900 great restaurants, including four Gordon Ramsay favourites from £15
Chancellor on brink of second bailout for banks
Salman Rushdie I won't marry again

- In the next months, cypherpunks, hackers, scientist become interested and joined the network
- On Dec 2nd, 2010, Satoshi made a last post, disappearing since then:

https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280



Re: PC World Article on Bitcoin

December 11, 2010, 11:39:16 PM

Merited by OgNasty (50), EFS (50), icey (25), mindrust (20), jojo69 (10), Bitman86 (4), o_solo_miner (2), JayJuanGee (1), klarki (1), johhnyUA (1), ETFbitcoin (1), r

It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us.

...after 13 years, the Bitcoin experiment
it’s still running

https://www.bitcoinisdead.org/

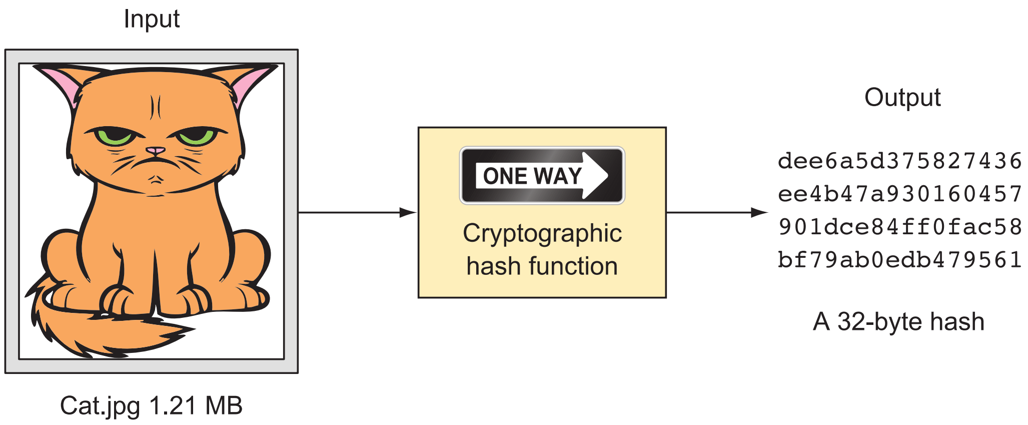
https://99bitcoins.com/bitcoin-obituaries/

Outline

- Physical VS Information Transfers
- **Hash Functions**, Proof-of-work, and Mining
- Asymmetric Cryptography
- Inside Blocks: Transactions
- Tools & Demo: Electrum
- Scaling Blockchains: The Trilemma
- Scaling to upper layers: The Lightning Network
- Open Research Topics and Challenges

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)



Input

Cat.jpg 1.21 MB

Cryptographic hash function

Output

dee6a5d375827436
ee4b47a930160457
901dce84ff0fac58
bf79ab0edb479561

A 32-byte hash

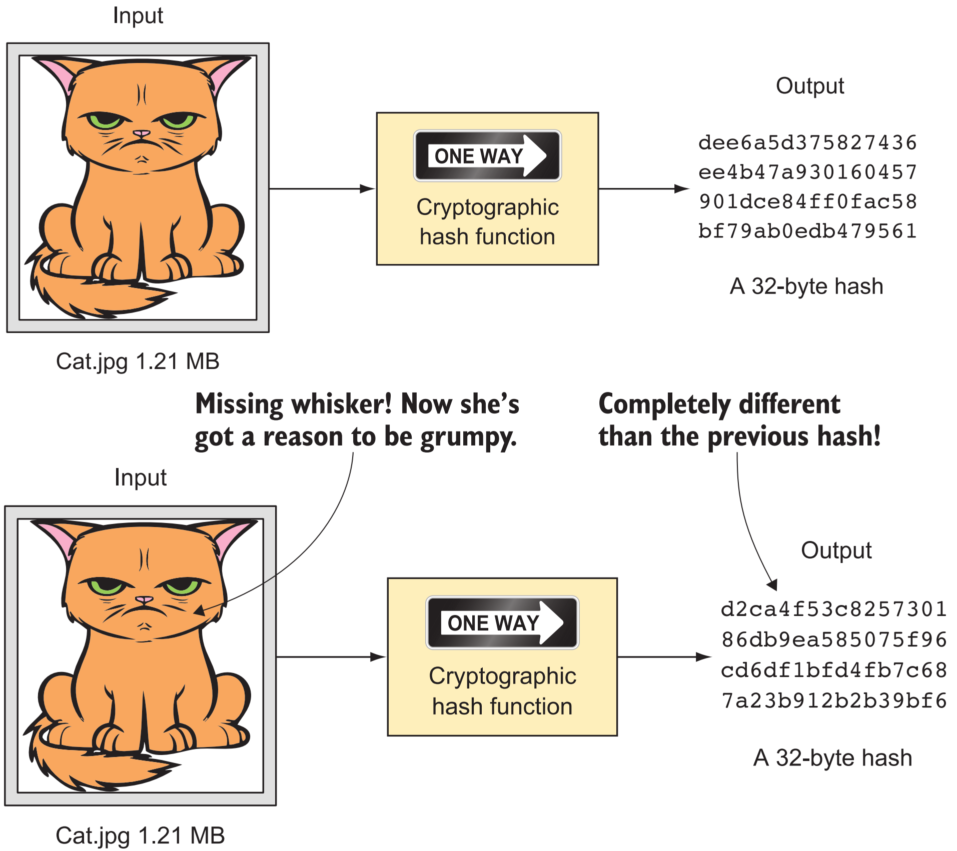
Key Concept: Hashes

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

6d02cc6fef85fb4ccdc4a0435f8c9458ffde5ad99af11878de0940236d7a300b

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

- What happens when you change, even just a little, the input?



Input

Cat.jpg 1.21 MB

Cryptographic hash function

Output

```
dee6a5d375827436
ee4b47a930160457
901dce84ff0fac58
bf79ab0edb479561
```

A 32-byte hash

Missing whisker! Now she's got a reason to be grumpy.

Completely different than the previous hash!

Input

Cat.jpg 1.21 MB

Cryptographic hash function

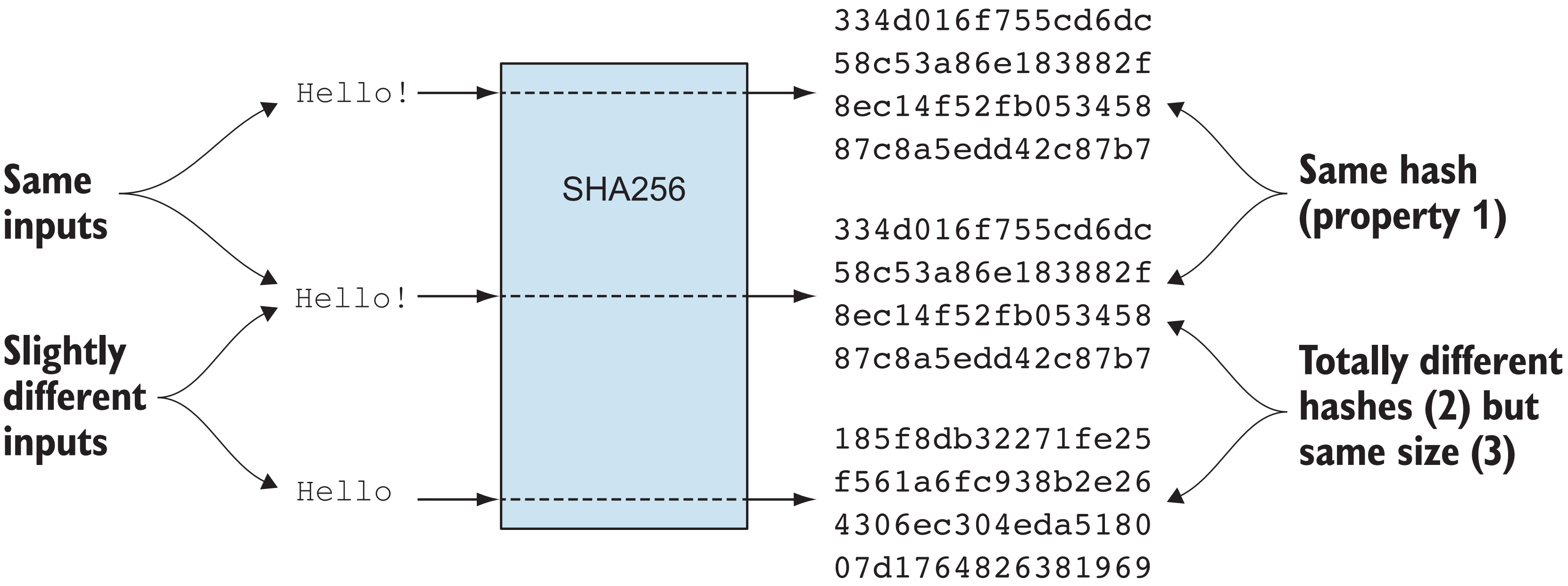
Output

```
d2ca4f53c8257301
86db9ea585075f96
cd6df1bfd4fb7c68
7a23b912b2b39bf6
```

A 32-byte hash

Hash Properties

Deterministic(1) Random oracle(2) Fixed size(3)



Same inputs

Slightly different inputs

Hello!

Hello!

Hello

SHA256

334d016f755cd6dc 58c53a86e183882f 8ec14f52fb053458 87c8a5edd42c87b7

334d016f755cd6dc 58c53a86e183882f 8ec14f52fb053458 87c8a5edd42c87b7

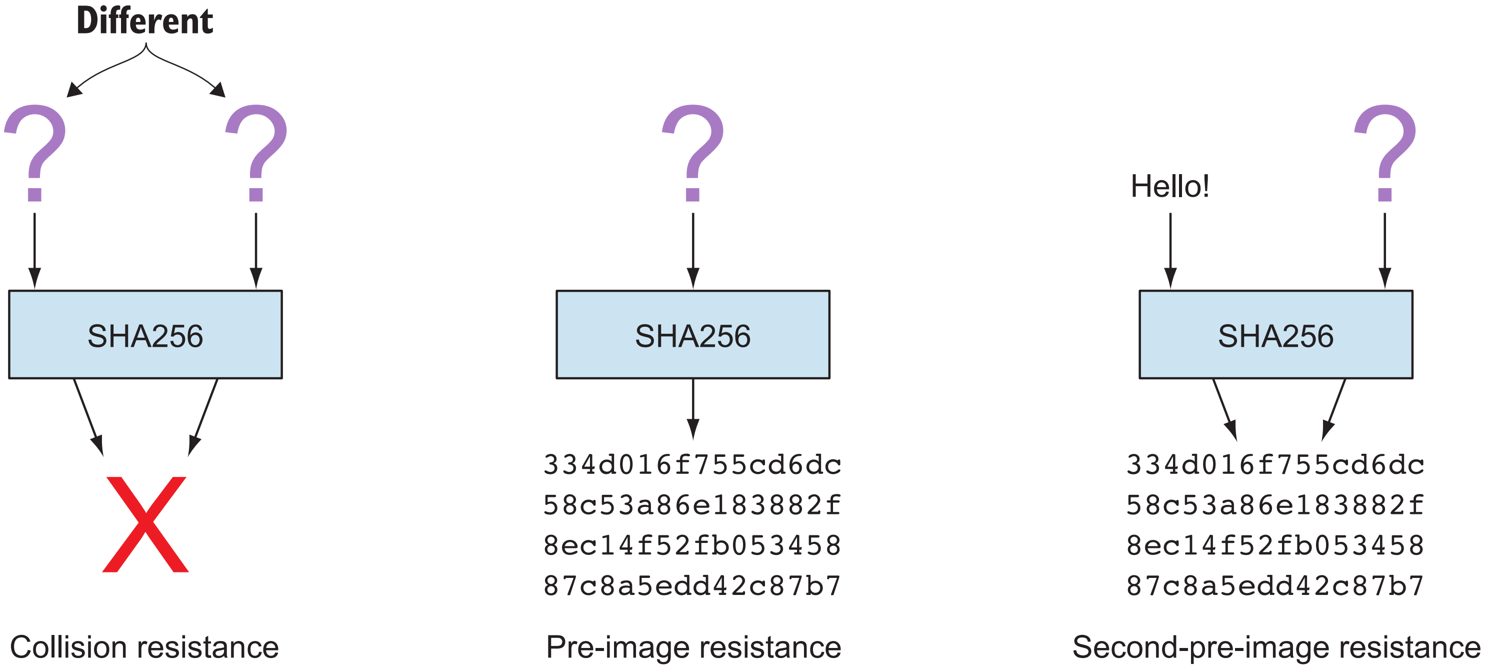
185f8db32271fe25 f561a6fc938b2e26 4306ec304eda5180 07d1764826381969

Same hash (property 1)

Totally different hashes (2) but same size (3)

Hash Properties

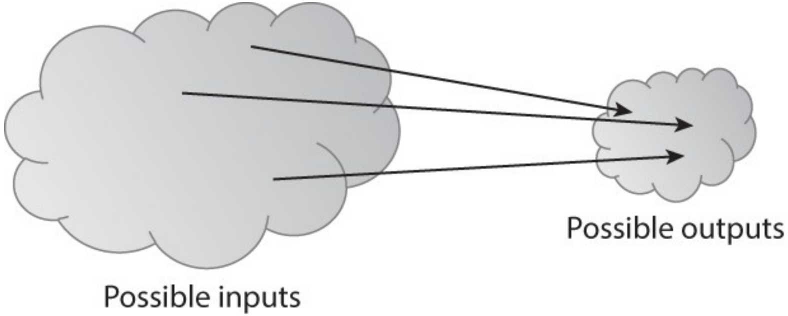
Collision resistance, Irreversibility (pre-image resistance)



Properties of Hash Functions

- **Deterministic:** given an input x, the resulting H(x) is always the same
- **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



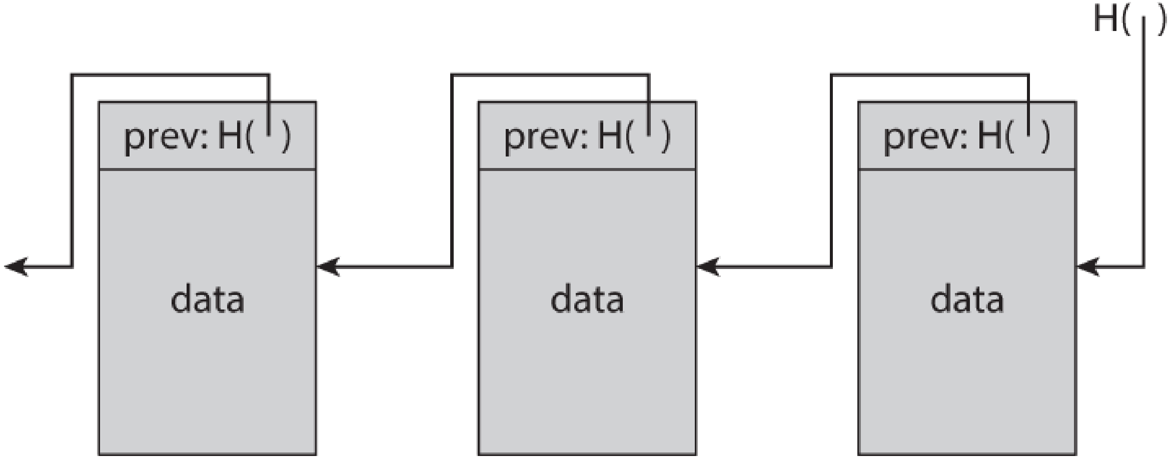
Hash Functions are One-way

- Counterintuitive: 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

https://github.com/B-Con/crypto-algorithms/blob/master/sha256.c

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



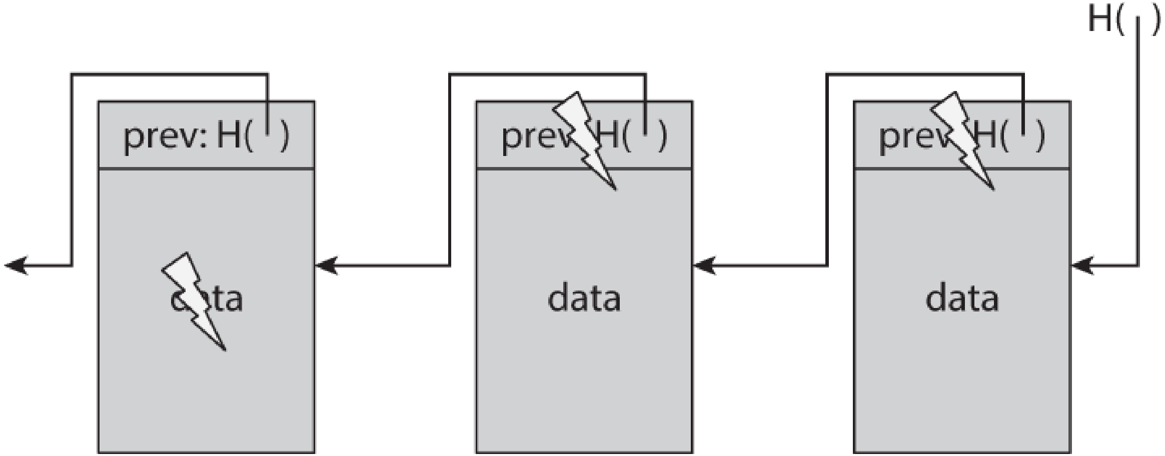
Counter example: Book Analogy

What happens to pages 44 and 46 if you change a single word in the page 45 of a book?

...nothing!

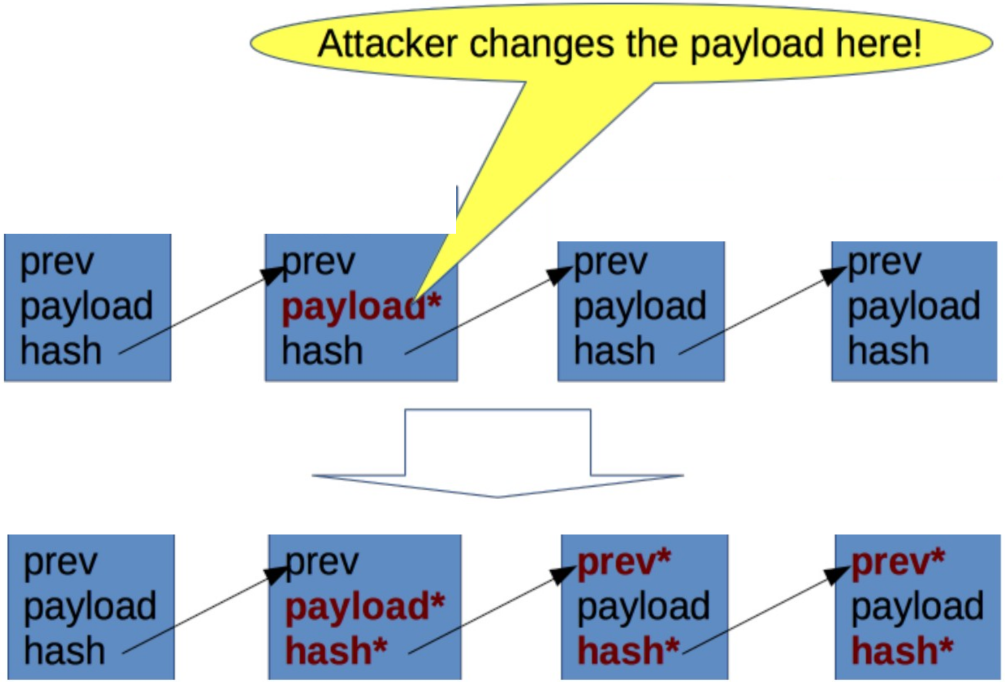
Tamper-proof Structure

- 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



Attacking the Chain

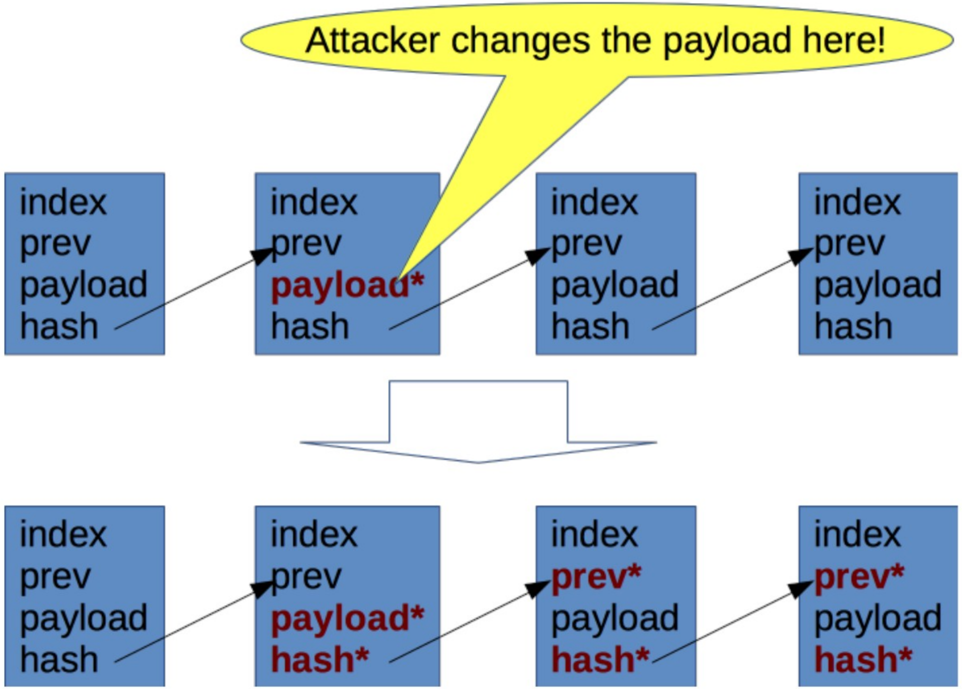
The modification of a block would require the recomputation of the all the hashes for the subsequent blocks...



Wait a Moment….

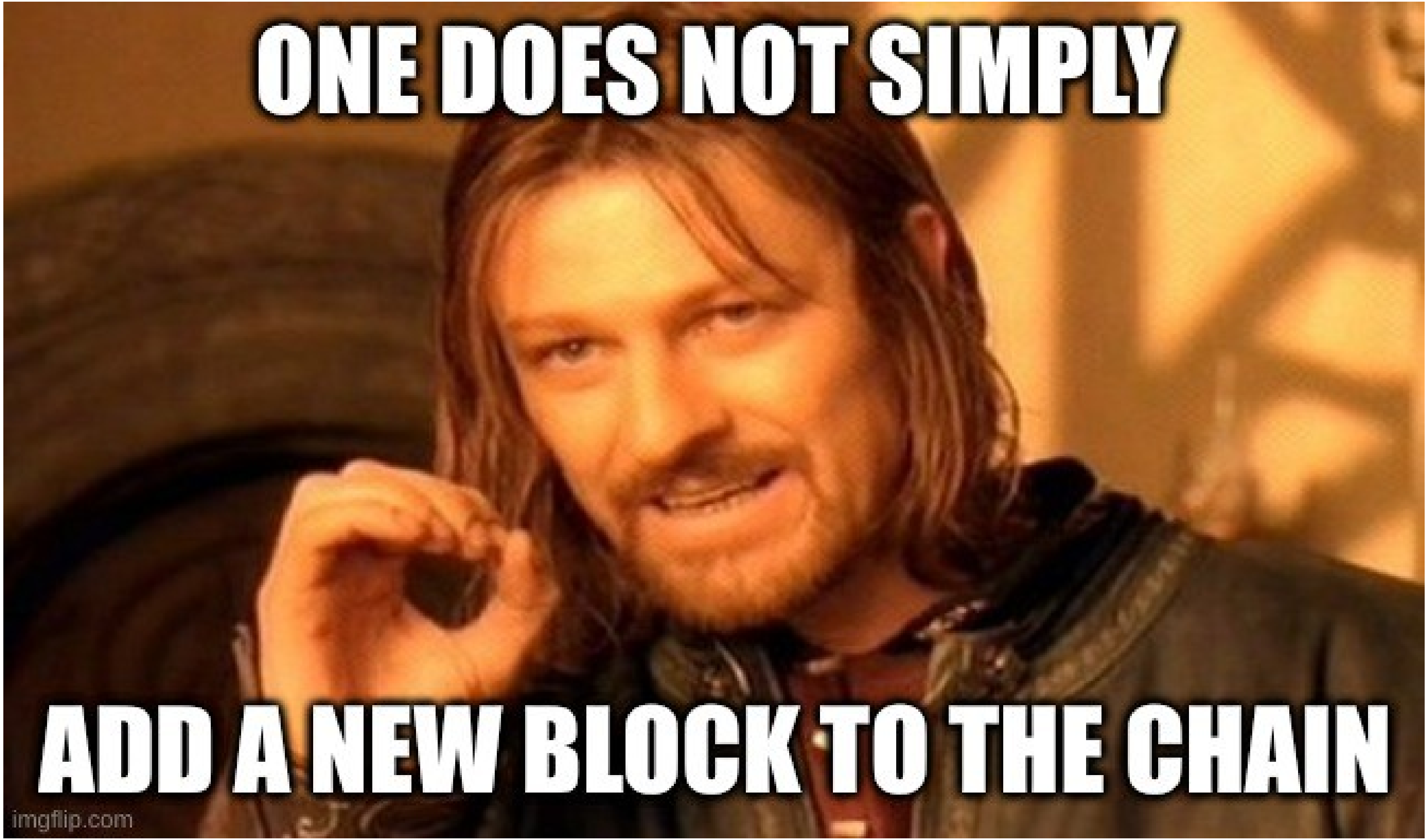
…we just said before block, **hashes are easy to compute in the x → H(x) direction**

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



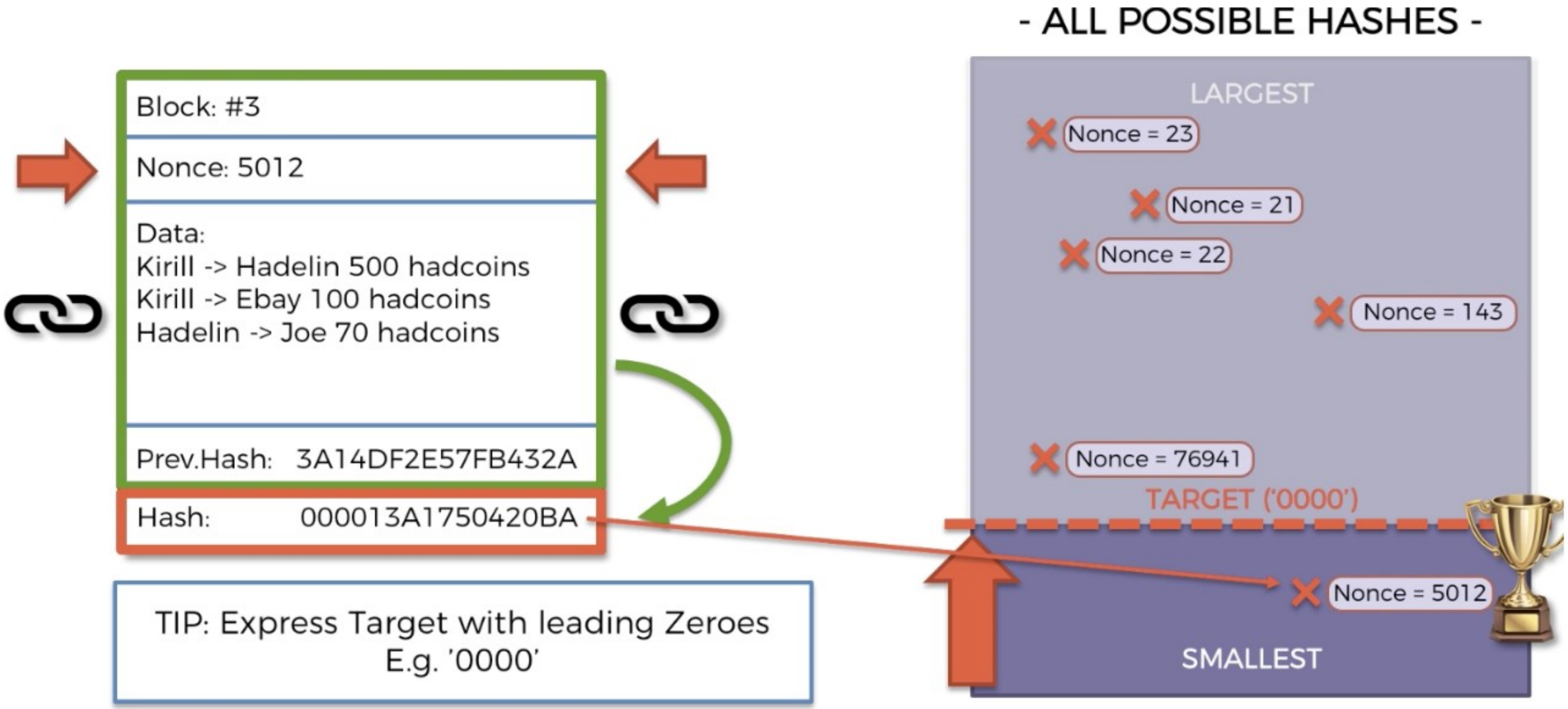
Outline

- Physical VS Information Transfers
- Hash Functions, **Proof-of-work**, and Mining
- Asymmetric Cryptography
- Inside Blocks: Transactions
- Tools & Demo: Electrum
- Scaling Blockchains: The Trilemma
- Scaling to upper layers: The Lightning Network
- Open Research Topics and Challenges


ONE DOES NOT SIMPLY
ADD A NEW BLOCK TO THE CHAIN
imgflip.com

Proof-of-Work

The hash of a new block MUST BE lower than a target→NOT EASY!



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'

Key Concept: Proof-of-Work

- The number of zeros represents a “difficulty”
- 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**
- **The Nonce has no particular meaning, just to have a different hash (Nonce = number to use “once”)**

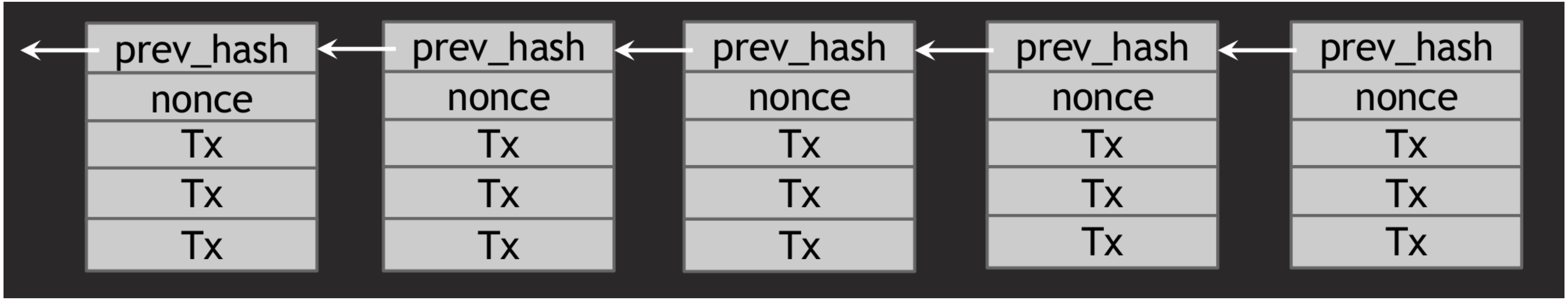
DEMO: Find the Nonce

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

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

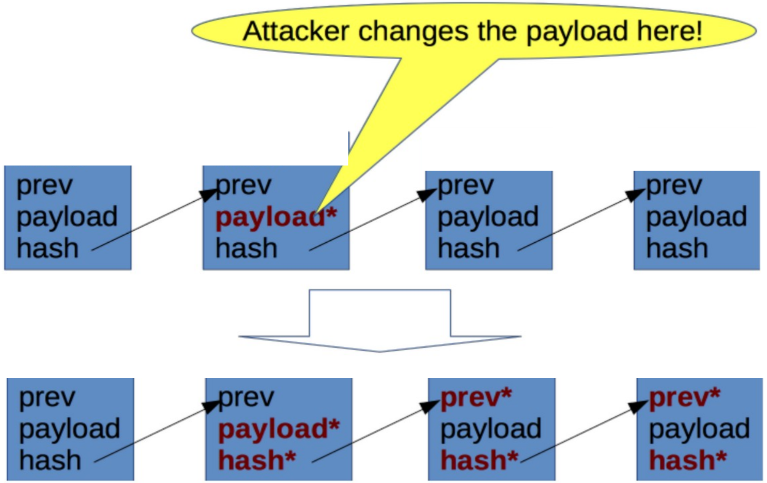
Accepting a new Block

- 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

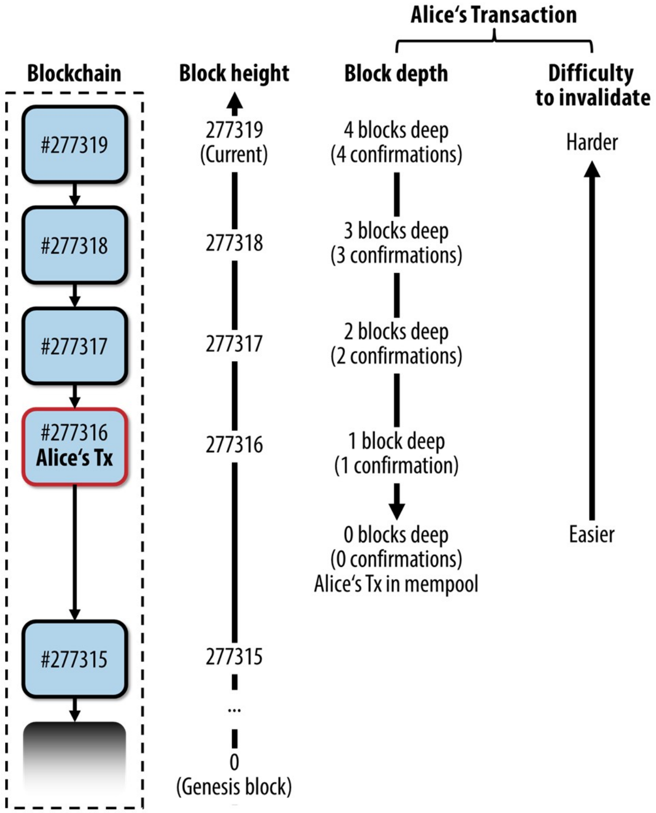


Chain Security: 51% Attack

- An attacker should not only find the hash for the block to be altered, but also for all the next blocks
- **The longest chain is the real one:** the attacker should be faster than the sum of all the other computing nodes in the world (51% attack)
- This would require an incredible computational and economic effort, which would be noticed very quickly.
- The result would be only to create an alternative chain of poor value, thus make useless that effort of the attacker



Security & Finality

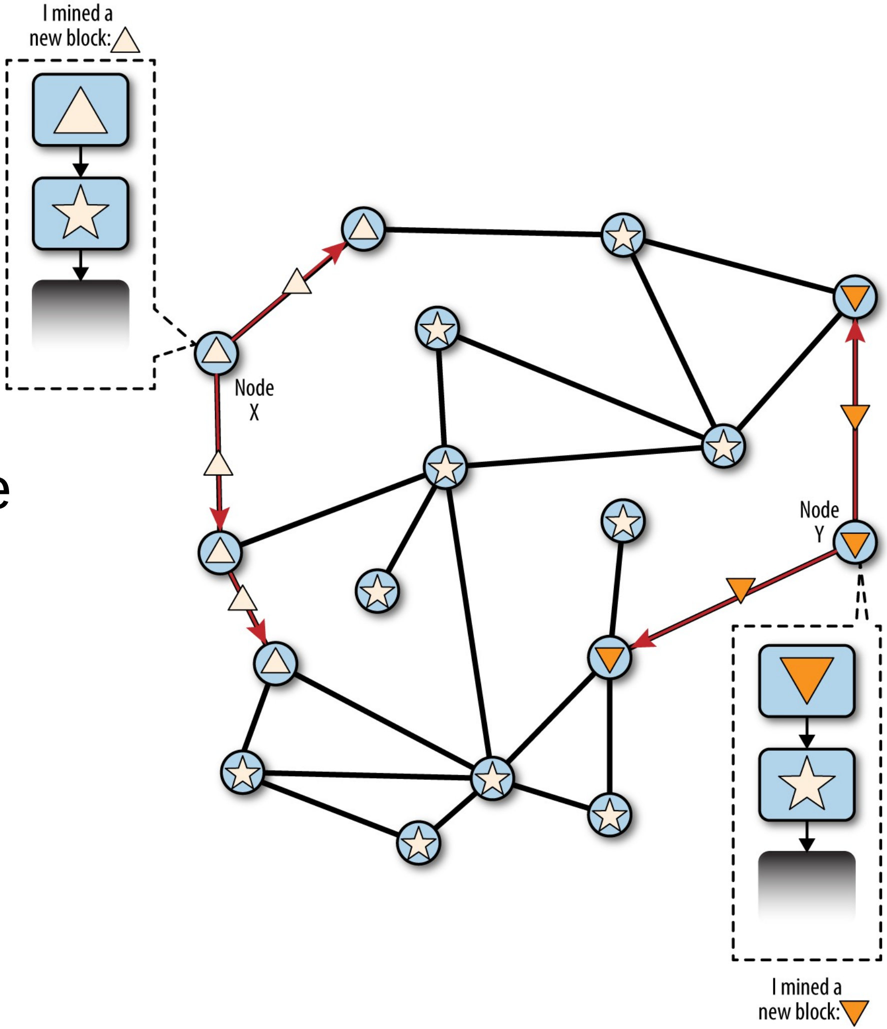


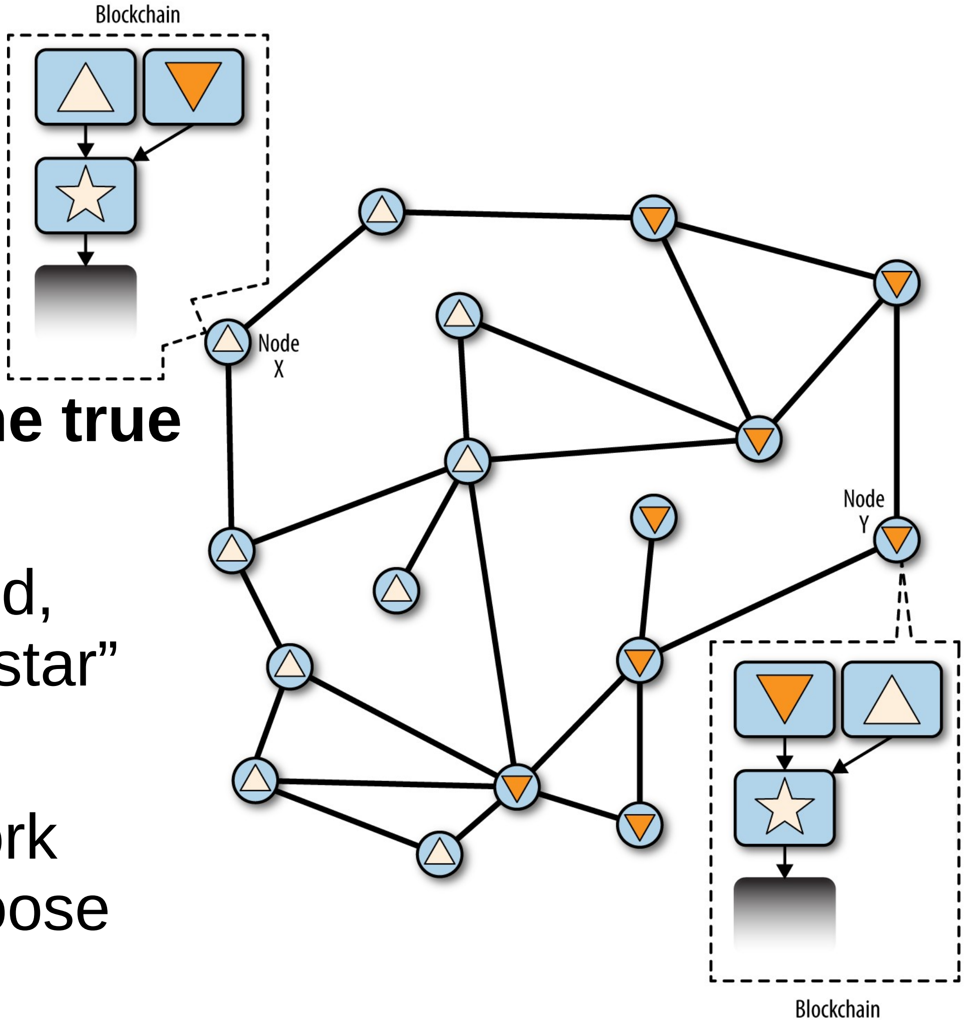
- Because of the proof-of-work, the chances of a block being altered decrease exponentially with the number of blocks chained after it
- The chain of blocks is a history of transactions resilient to network attackers because it cannot be altered without huge resources
- The number of confirmations an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

In rare case, particular situations can occur:

- While searching for the next block, 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

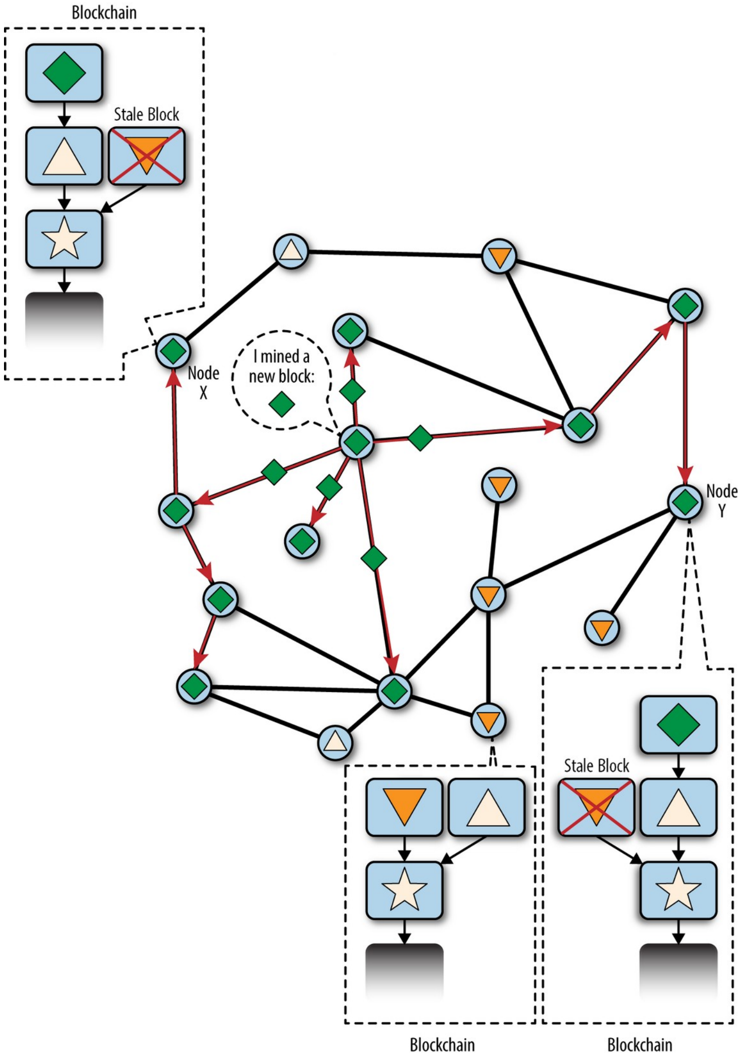




We cannot say that one is the true one, and the other is false:

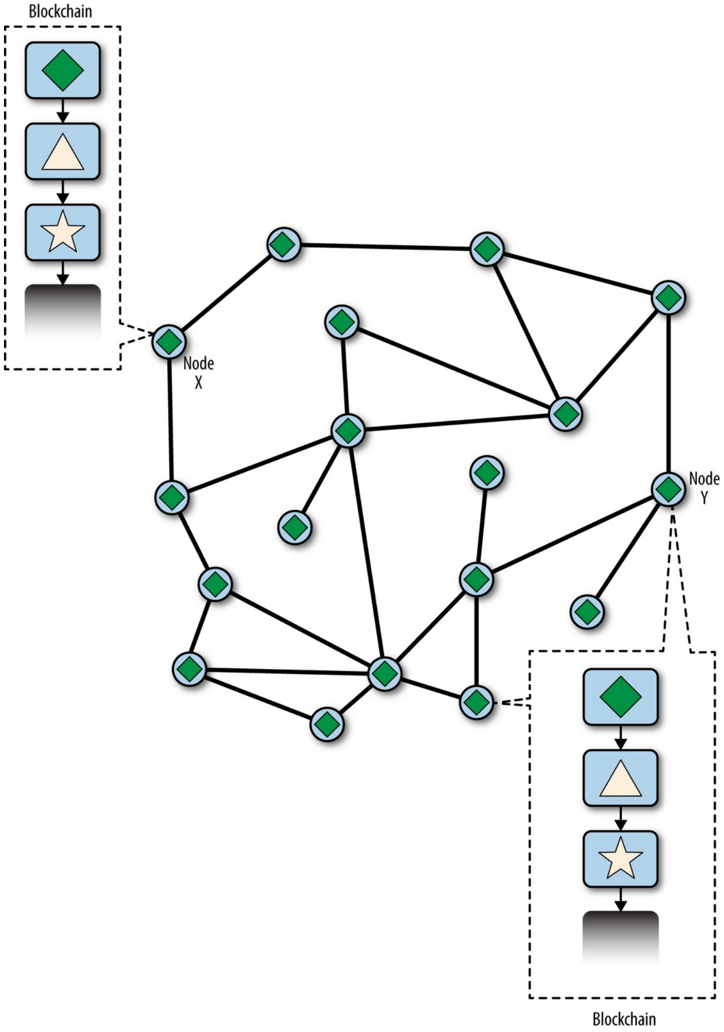
- They are both correctly mined, using the hash of the “white star” block.
- But, depending on the network condition, each node will choose the first received

- 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**)



Outline

- Physical VS Information Transfers
- Hash Functions, Proof-of-work, and Mining
- Asymmetric Cryptography
- Inside Blocks: Transactions
- Tools & Demo: Electrum
- Scaling Blockchains: The Trilemma
- Scaling to upper layers: The Lightning Network
- Open Research Topics and Challenges

Miners

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

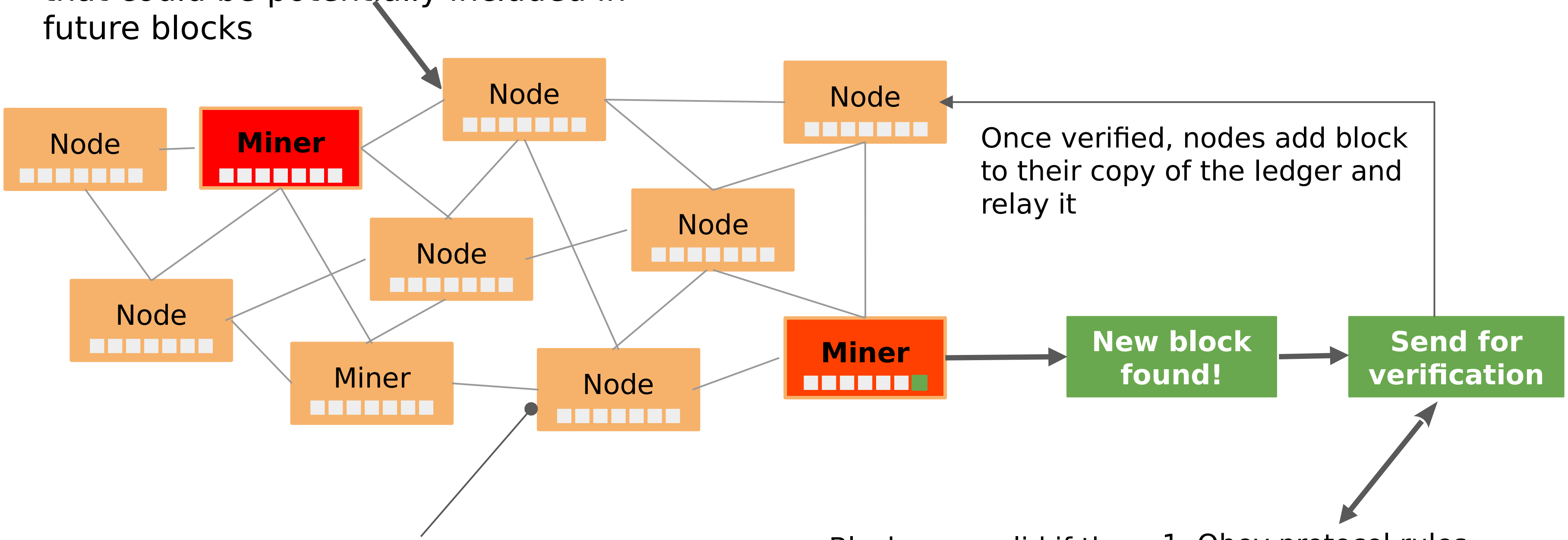
The search for the next “0000xxxx” hash is called “Mining”.

- When a node finds the new block, it is entitle of a piece of digital asset
- Analogy: like “miners” finding gold, searching for rare numbers

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

Miners & Nodes

Nodes collect and broadcast events that could be potentially included in future blocks



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

Verification remain a decentralized process to keep miners honest

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

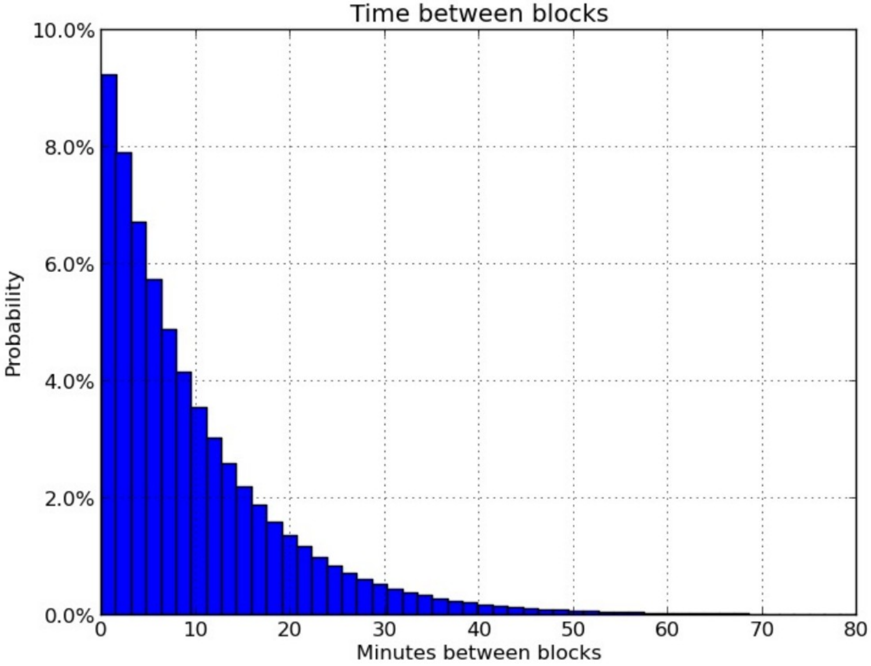
For a single miner:

- Probability of solving next block:

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

- Mean time to find a block:

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

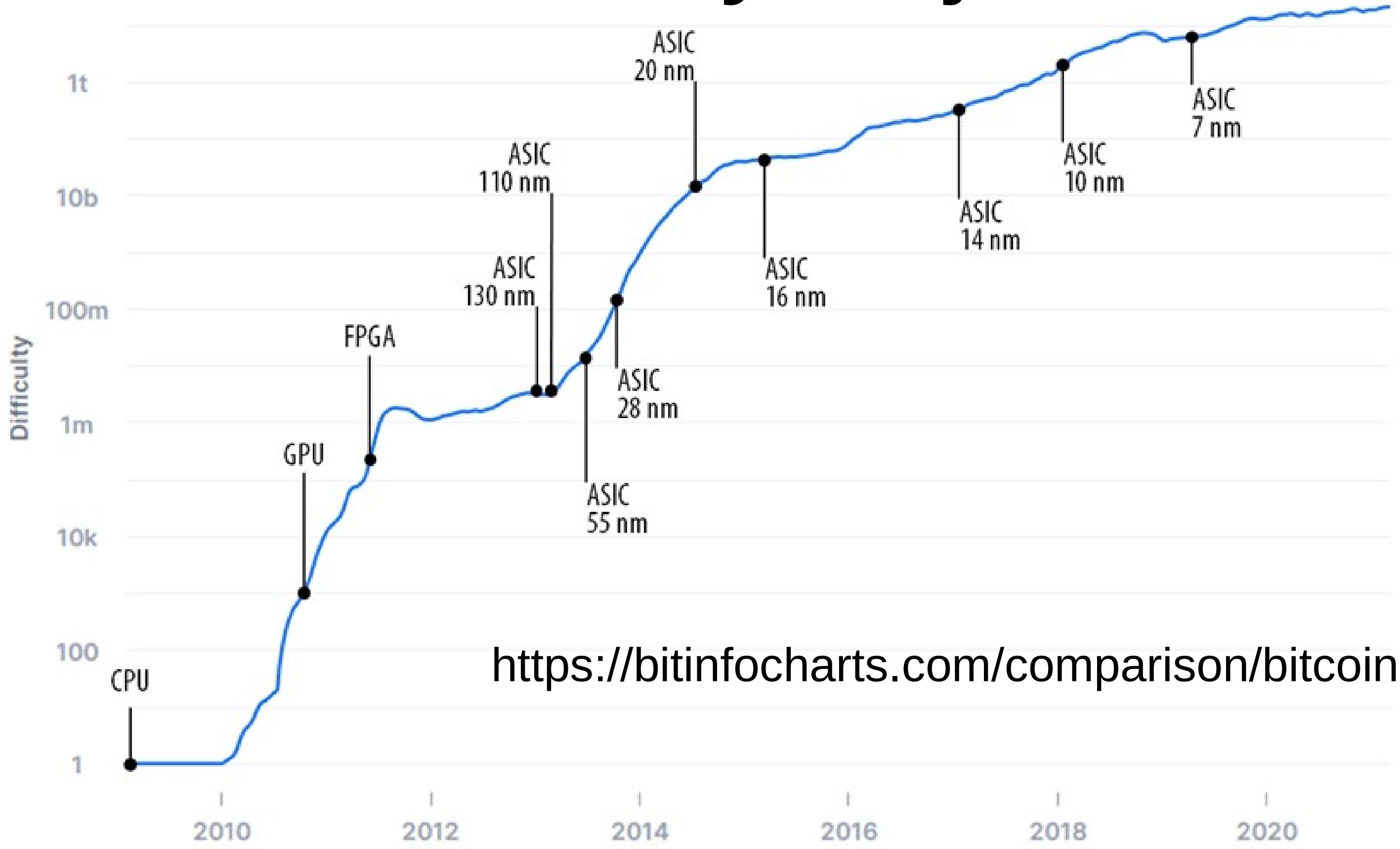


- 0.01% of the hash rate → one block every 69 days

Key Idea: Difficulty Adjustment

- The number of zeros required in the resulting block hash represents a “difficulty”
- Bitcoin protocol updates automatically 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).

Difficulty Adjustment

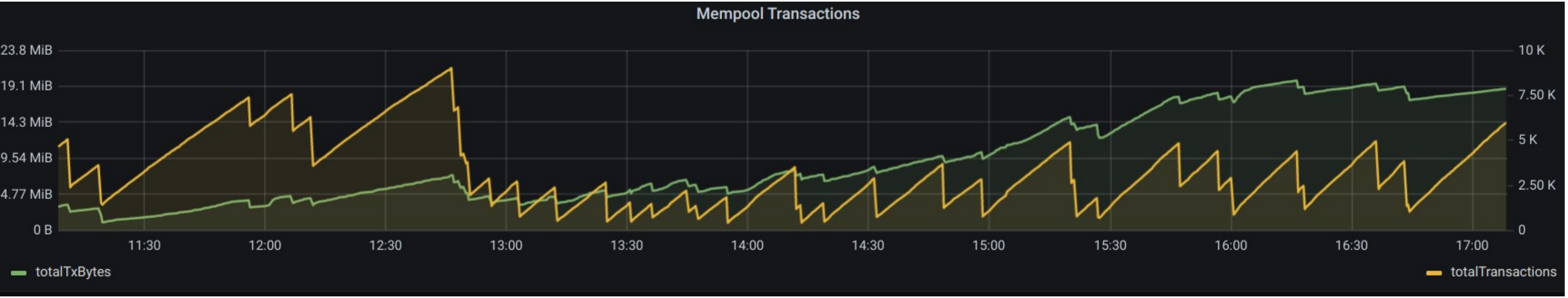


https://bitinfocharts.com/comparison/bitcoin-hashrate.html#3y

- Checkout the current memory pool at:

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

  https://txstreet.com/v/btc



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**

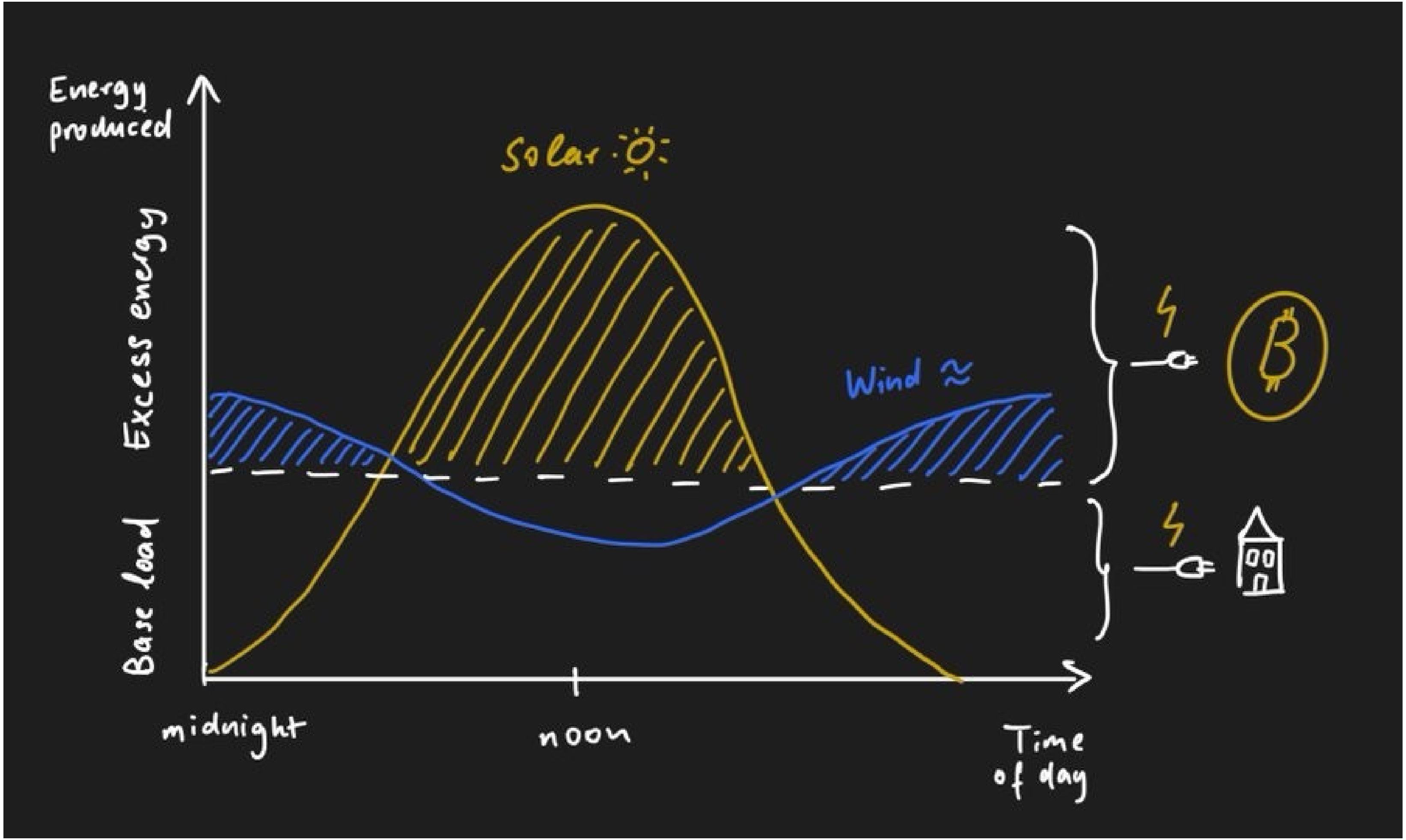
Bitcoin network provides a cross-country, censorship-resistant, trustless digital asset

- 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”

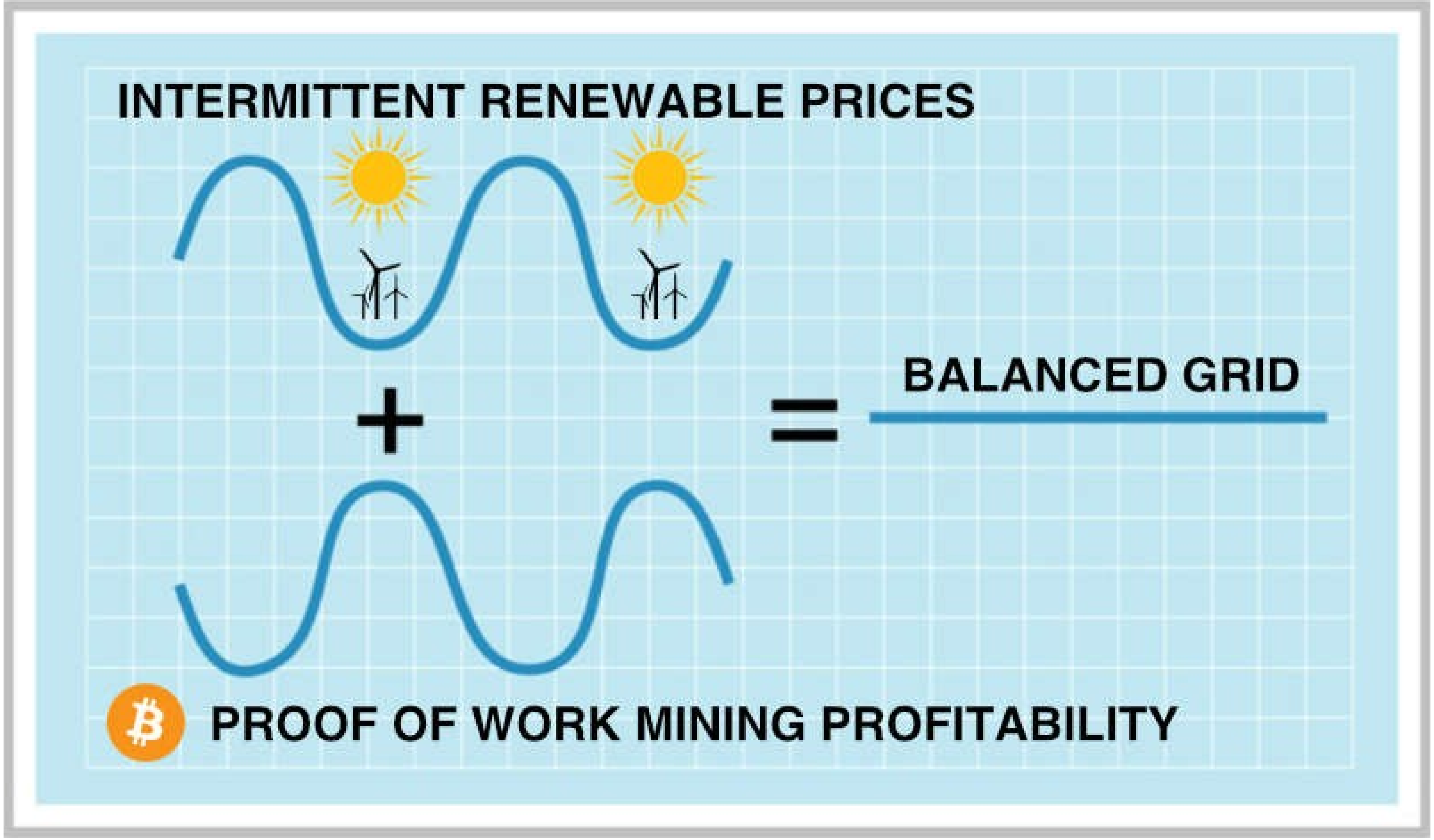
https://bitcoinminingcouncil.com/wp-content/uploads/2021/07/2021.07.01-BMC-Q2-2021-Materials.pdf

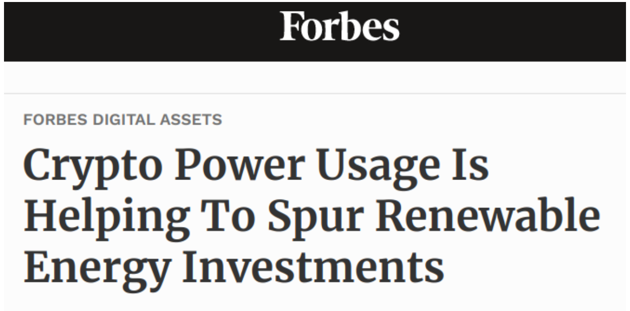
...But also mining has a unique features that differs from other industry energy use cases:

- **Location Agnostic:** mining hardware can move in different places
- **Memory-less/Interruptible:** the mining can be turned off/on, no continuity is required for the completion of a production task
- Due to the above peculiar features, **bitcoin mining is gaining traction as a solution to incentivize green energy production**



https://twitter.com/callebtc

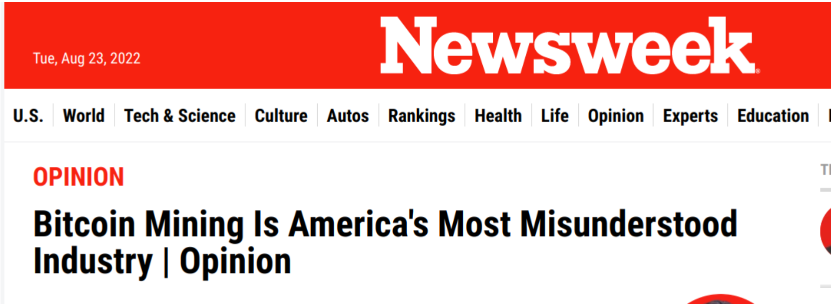

INTERMITTENT RENEWABLE PRICES
+
=
BALANCED GRID
PROOF OF WORK MINING PROFITABILITY



Forbes

FORBES DIGITAL ASSETS

Crypto Power Usage Is Helping To Spur Renewable Energy Investments



Tue, Aug 23, 2022

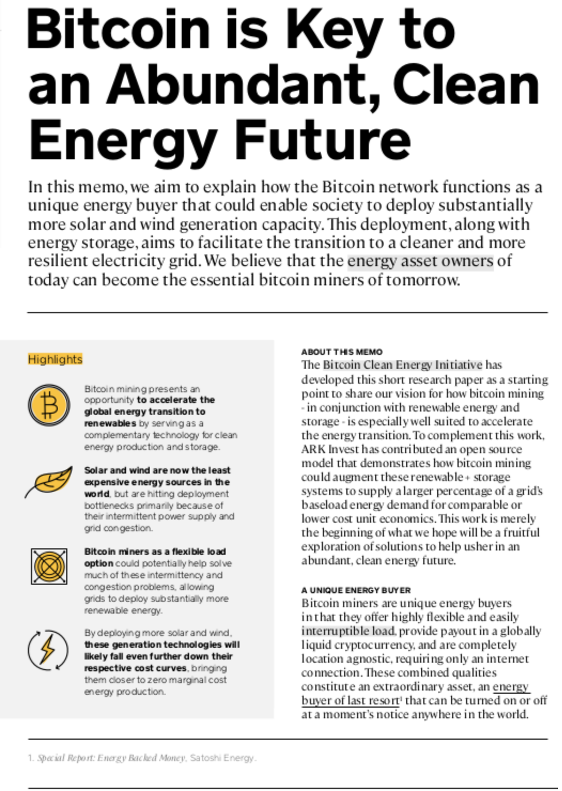
Newsweek

U.S. | World | Tech & Science | Culture | Autos | Rankings | Health | Life | Opinion | Experts | Education | I

OPINION

Bitcoin Mining Is America's Most Misunderstood Industry | Opinion

TI



Bitcoin is Key to an Abundant, Clean Energy Future

In this memo, we aim to explain how the Bitcoin network functions as a unique energy buyer that could enable society to deploy substantially more solar and wind generation capacity. This deployment, along with energy storage, aims to facilitate the transition to a cleaner and more resilient electricity grid. We believe that the energy asset owners of today can become the essential bitcoin miners of tomorrow.

Highlights

Bitcoin mining presents an opportunity **to accelerate the global energy transition to renewables** by serving as a complementary technology for clean energy production and storage.

Solar and wind are now the least expensive energy sources in the world, but are hitting deployment bottlenecks primarily because of their intermittent power supply and grid congestion.

Bitcoin miners as a flexible load option could potentially help solve much of these intermittency and congestion problems, allowing grids to deploy substantially more renewable energy.

By deploying more solar and wind, **these generation technologies will likely fall even further down their respective cost curves**, bringing them closer to zero marginal cost energy production.

ABOUT THIS MEMO

The Bitcoin Clean Energy Initiative has developed this short research paper as a starting point to share our vision for how bitcoin mining - in conjunction with renewable energy and storage - is especially well suited to accelerate the energy transition. To complement this work, ARK Invest has contributed an open source model that demonstrates how bitcoin mining could augment these renewable + storage systems to supply a larger percentage of a grid's baseload energy demand for comparable or lower cost unit economics. This work is merely the beginning of what we hope will be a fruitful exploration of solutions to help usher in an abundant, clean energy future.

A UNIQUE ENERGY BUYER

Bitcoin miners are unique energy buyers in that they offer highly flexible and easily interruptible load, provide payout in a globally liquid cryptocurrency, and are completely location agnostic, requiring only an internet connection. These combined qualities constitute an extraordinary asset, an energy buyer of last resort[1] that can be turned on or off at a moment's notice anywhere in the world.

[1] *Special Report: Energy Backed Money*, Satoshi Energy.

http://squ.re/BCEI-whitepaper

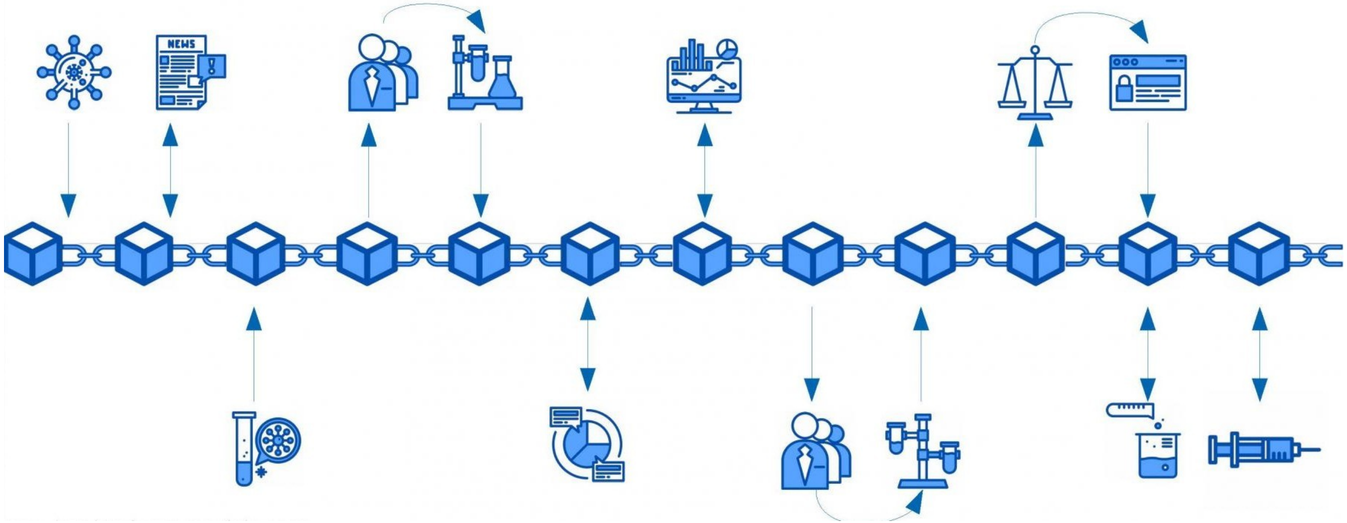
https://www.newsweek.com/bitcoin-mining-americas-most-misunderstood-industry-opinion-1669892

Impossible Mission?

1)**We must guarantee the order of events**

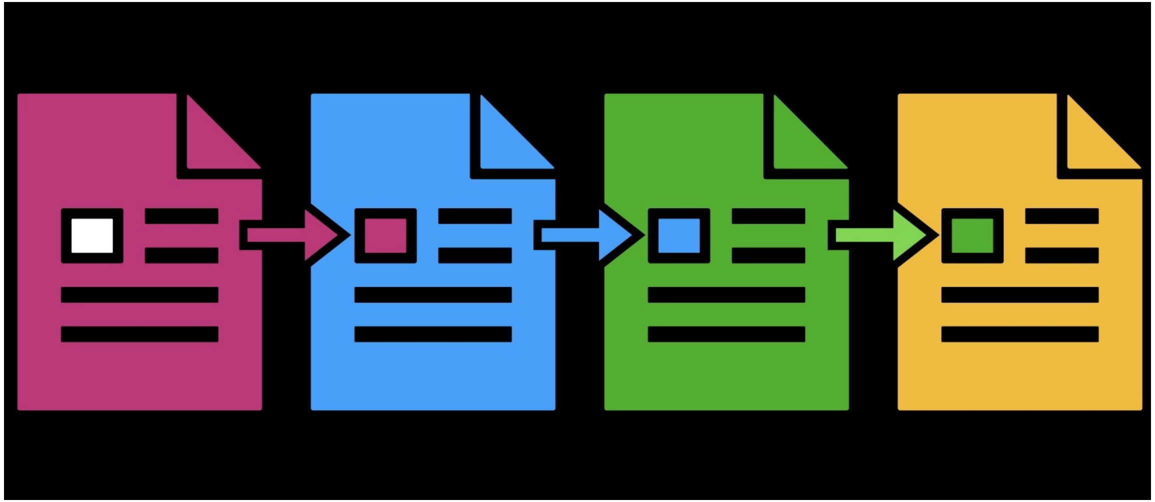
2)Ensure that sender and receiver are the correct ones

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

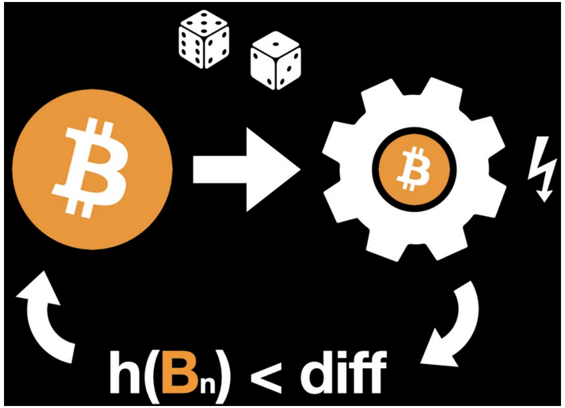


Blockchain = Timechain

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



- **Proof-of-work is the anchor between informational realm and physical world,** because computation requires real-world energy
- **Blocks cannot be produced with “fake” energy**, the block itself is the proof of the negative entropy generated (hash 00000000xxxxxx)



A block not only describes “what happened”...but it also IS “what happened”