Block

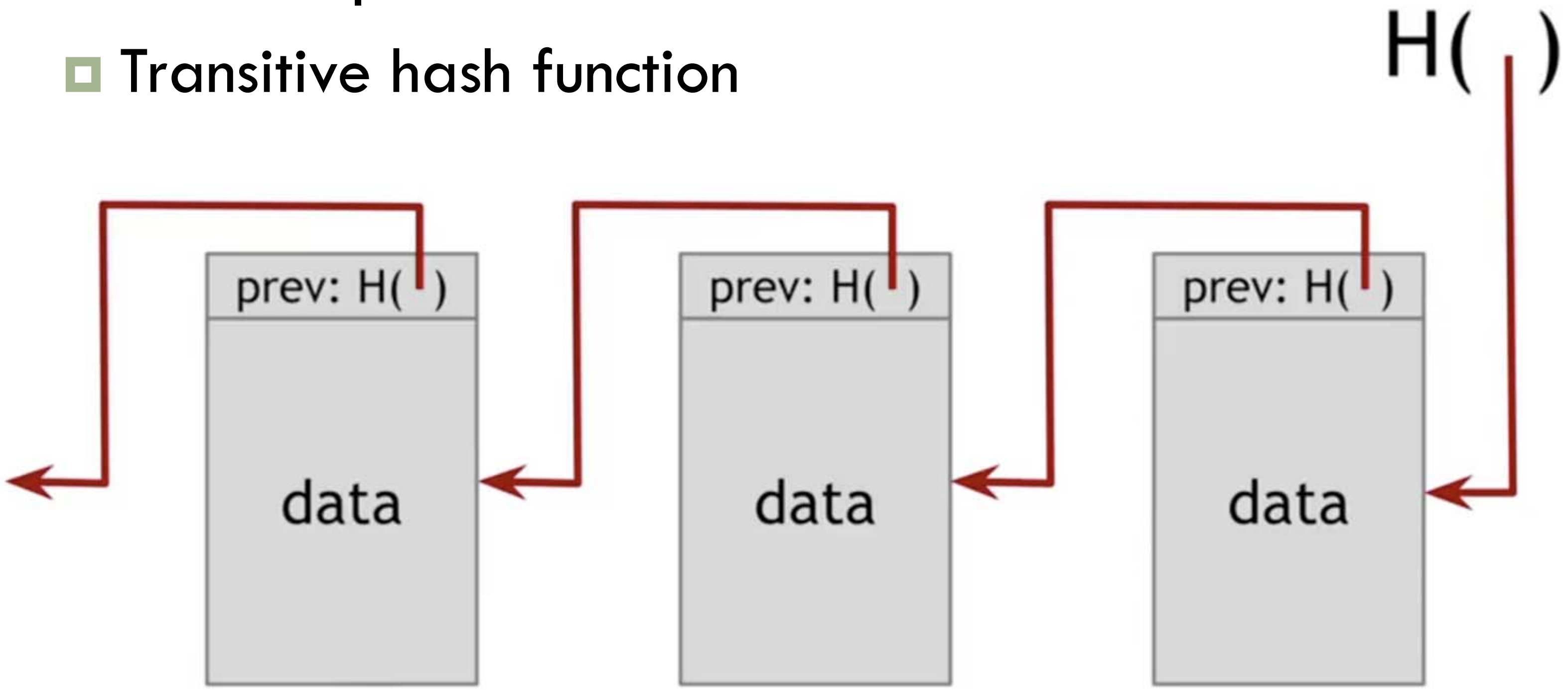
- The block may contain information about:
  - Transactions
    - P da *y* a Q
  - States
    - P has *n* instances of *x*
  - Conditions
    - Contracts
      - if < transaction> then < transaction>
    - Inferences
      - if < state> then < state>
- The block size is 1 MB of transactions.
  - Fixed in the initial version of the protocol.

Blockchain

- A blockchain (or *Blockchain*) is a linked list whose nodes link to its predecessor by **hashing** its contents.

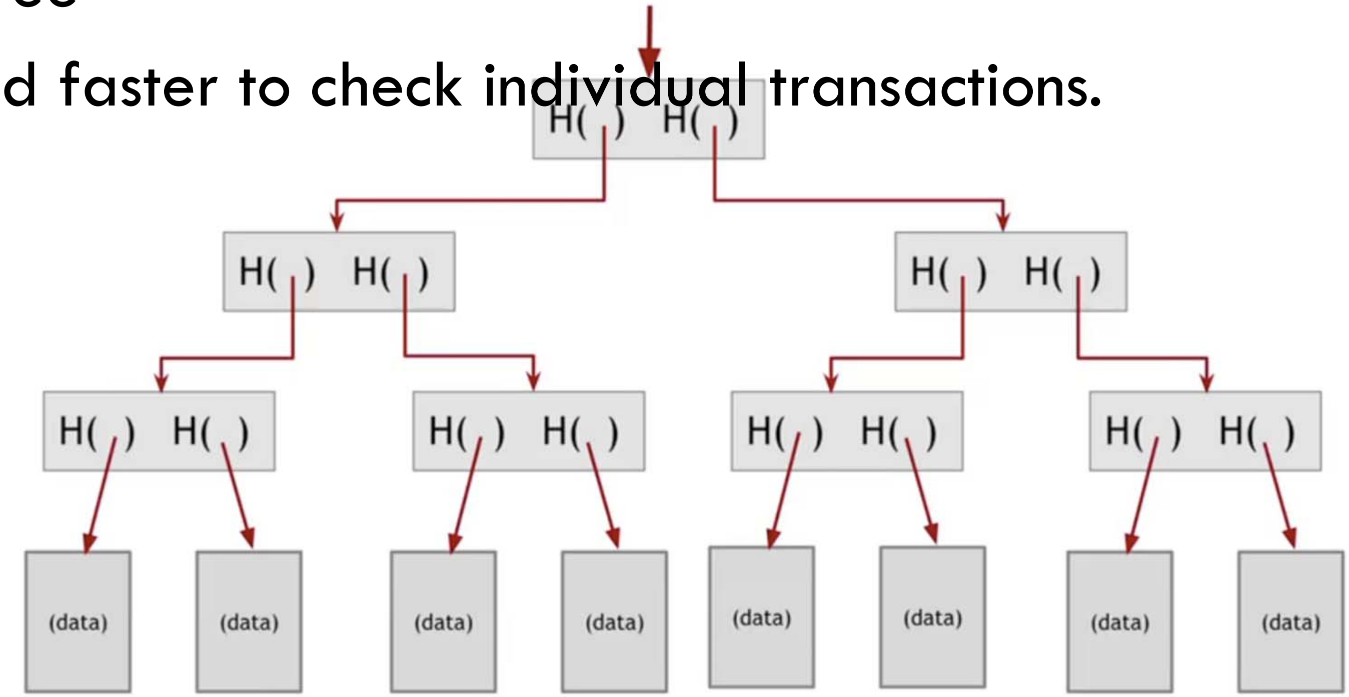
Blockchain structure (1/4)

- Linear sequence of data
  - Transitive hash function

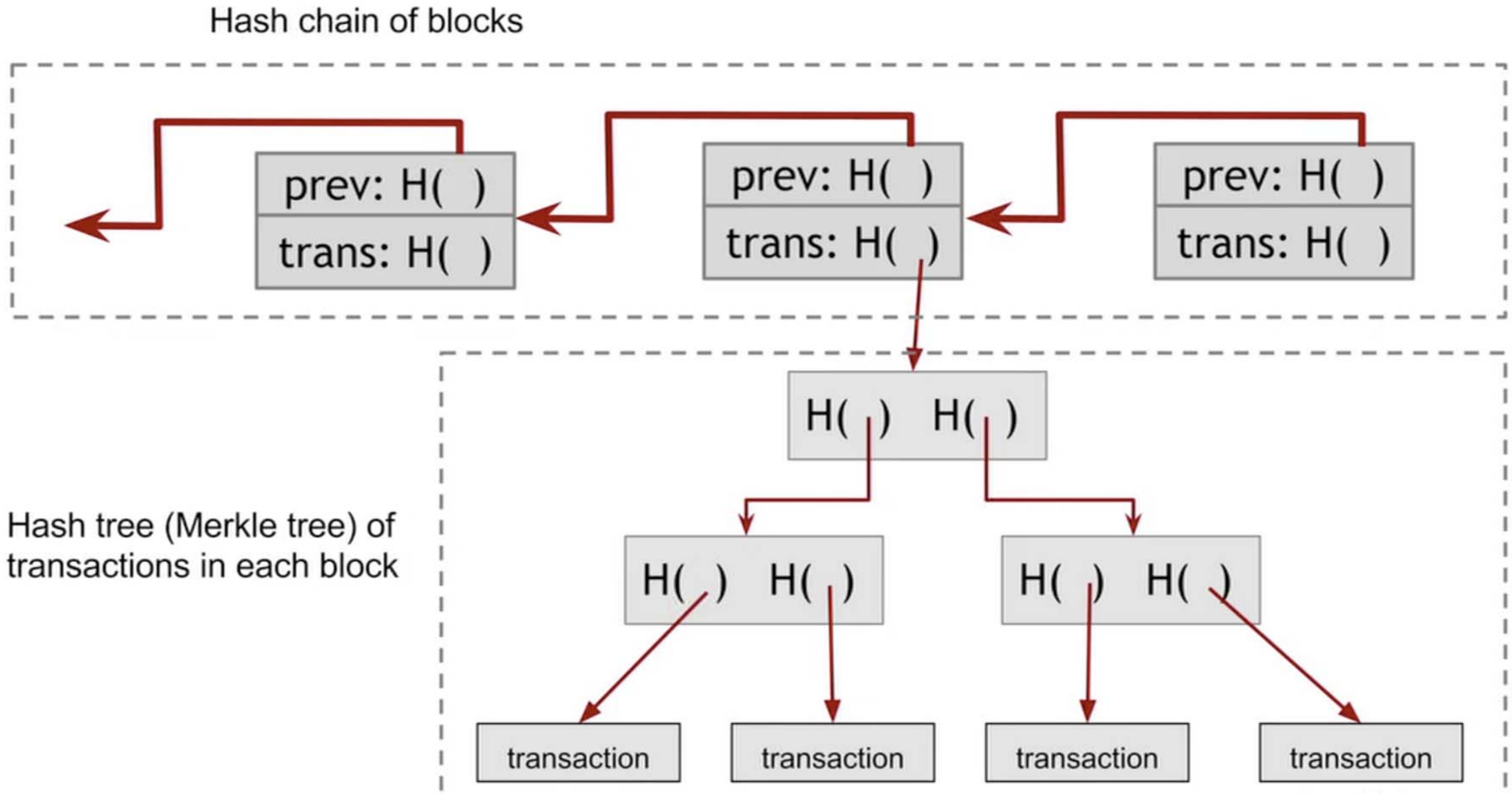


Blockchain structure (2/4)

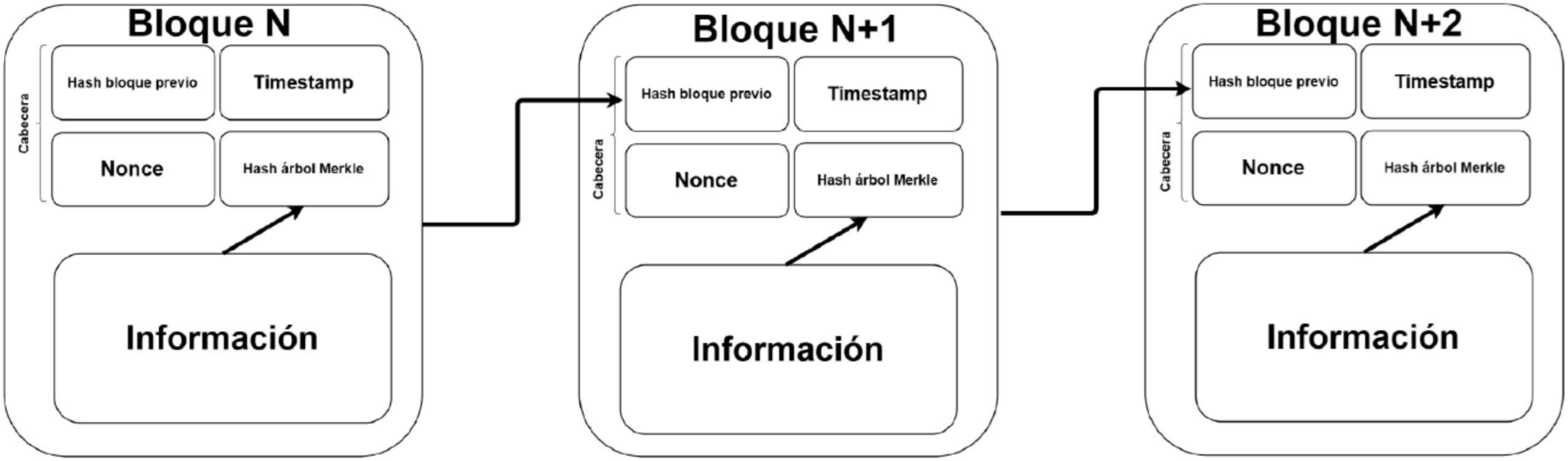
- Data sets
  - Merkle Tree
  - Easier and faster to check individual transactions.



Blockchain structure (3/4)

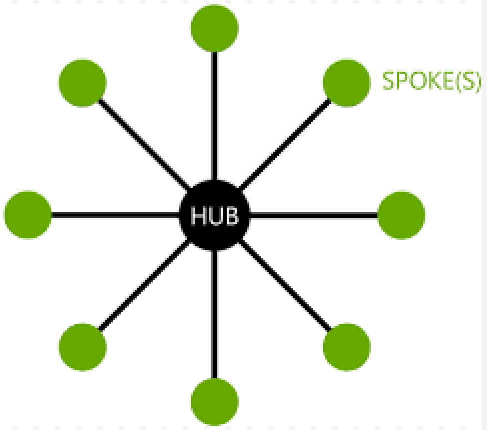


Blockchain structure (4/4)

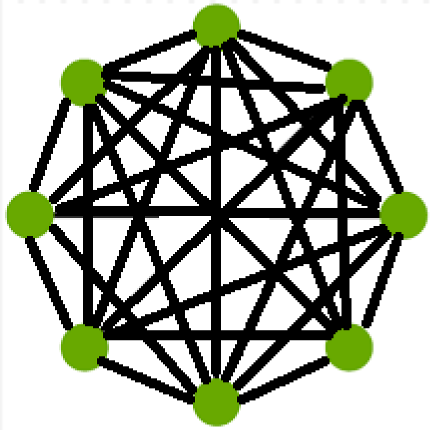


Decentralization

- Blockchain is a decentralized P2P network.
- Each *node* has a copy of the *ledger*.



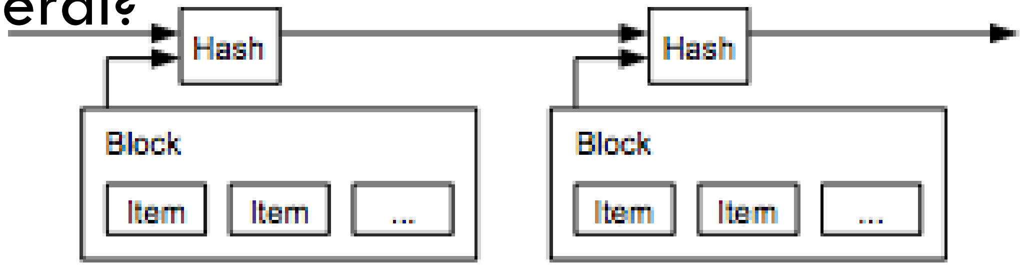
Traditional "Hub and Spoke" scheme with centralized BD



Blockchain network with decentralized *ledgers*

Avoiding the problem of double spending

- The usual solution is a central authority to verify this.
  - And if not?
- Time stamp servers (*timestamp*)
  - Generate the *timestamp* of a block and publish it
    - Proof that the data existed at that time.
    - The timestamp of the block includes the timestamp of the previous blocks.
  - What if there are several?
    - Consensus mechanisms

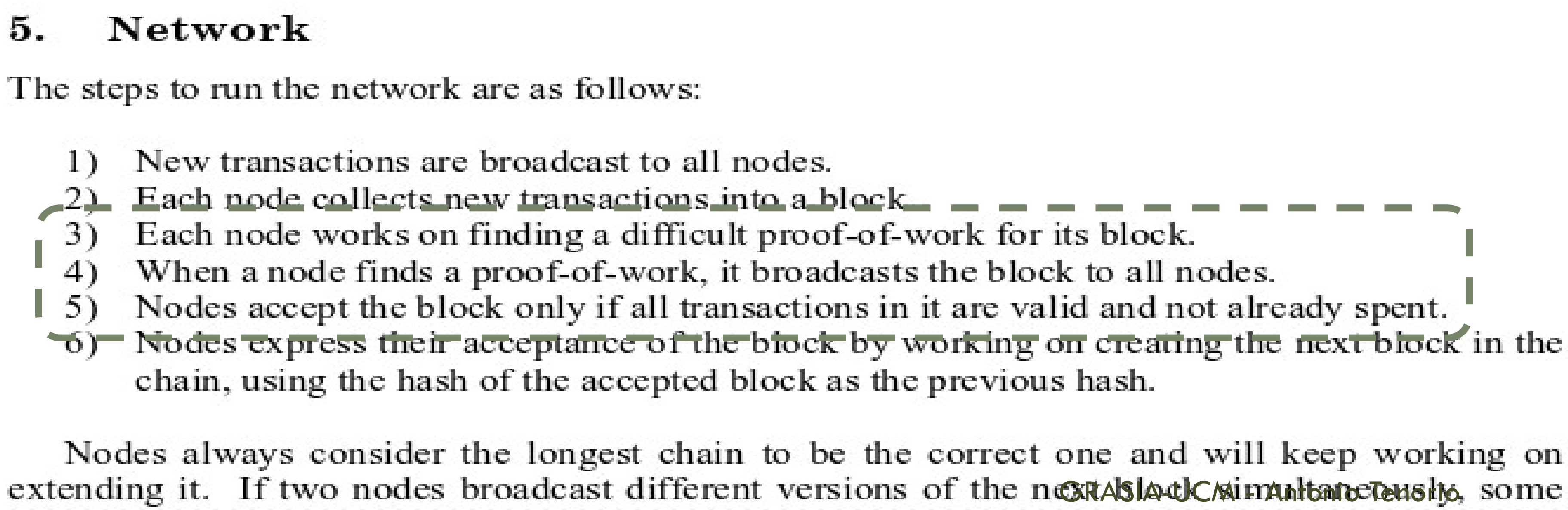


Consensus mechanisms

- □ They ensure that the next block added to a blockchain is the only authentic version.
- □ It prevents powerful participants (adversaries) from corrupting the system and successfully forking the chain.

Proof of work

- Nakamoto's article sets out how to secure a Blockchain against attacks through a proof of work.
    - It is the great novelty of his work



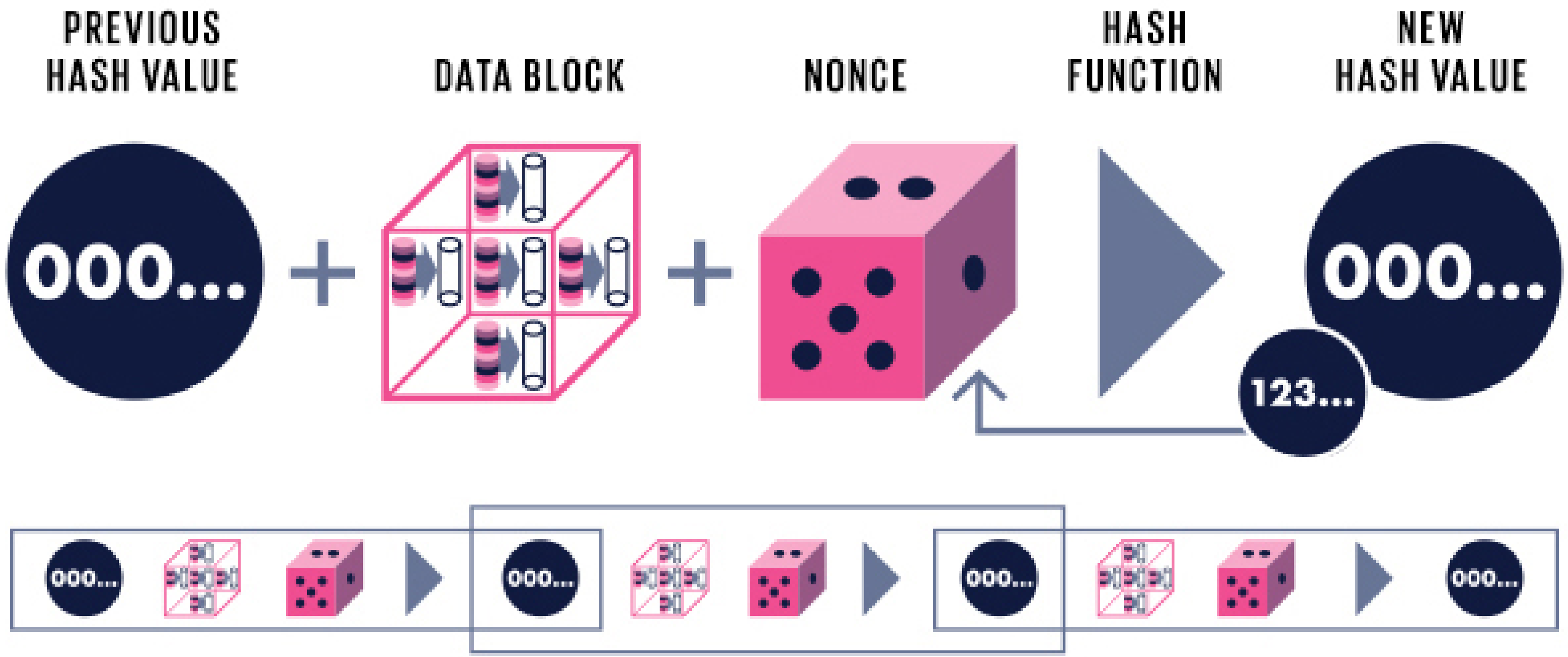
5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some

Proof of work



- PoW involves looking for a "*nonce*" value that, when combined with a combined hash of all transactions in a block, the resulting hash starts with a certain number of zero bits.

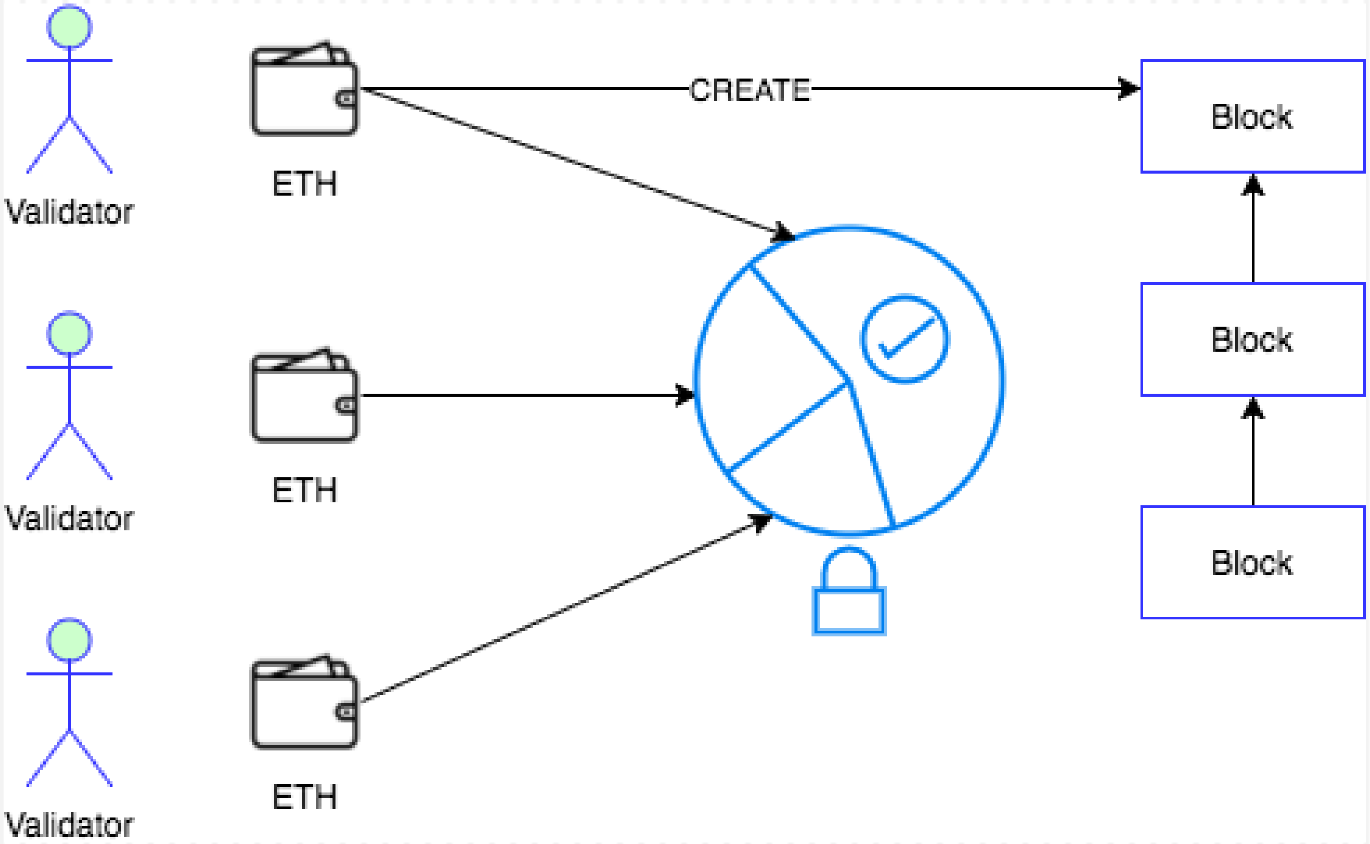
Proof of work

- It is essentially a voting mechanism.
  - 1 CPU = 1 vote.
- The majority decision is represented by the longest blockchain.
  - In which PoW has invested the most effort.
- If most of the CPU power is controlled by honest nodes, the honest chain will grow faster and outperform competing chains.
  - Modifying a past block would require redoing the PoW of the block and all subsequent blocks, until the chain of honest nodes is exceeded.
  - 51% attack

Consensus methods

- *Proof of Work* (Nakamoto consensus)
- *Proof of State*
- *Proof of Elapsed Time*
- *Proof of Burn*
- *Proof of Capacity*
- *Proof of Importance*
- *Proof of Stake (proof of* participation)
  - Ex. PeerCoin, https://peercoin.net/
- *Proof of Replication*
  - E.g. Filecoin, https://filecoin.io/
- …

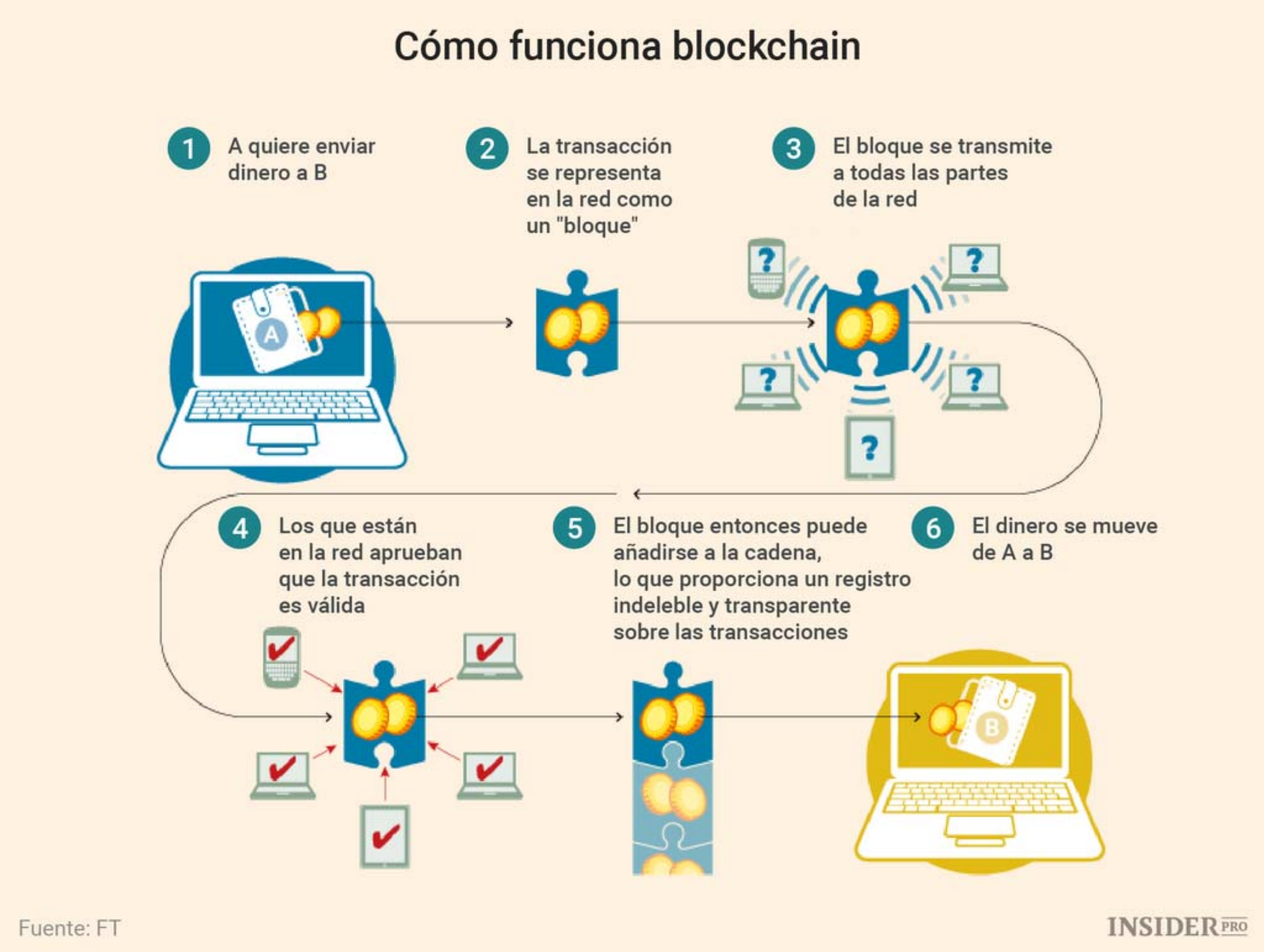
Participation test



Participation test

- *Proof of Stake* (*PoS*) is a category of consensus algorithms.
  - For public blockchains.
  - They depend on the economic participation of a validator in the network.
- It is not necessary to consume large resources to secure a blockchain.
  - Resource = Computation and energy
- Therefore, it is not necessary to issue so many new coins to motivate participants to continue participating in the network.
  - Game theory mechanisms to discourage centralized cartels.
- Ability to use economic sanctions to make 51% attacks much more expensive to carry out.

Networking



Cómo funciona blockchain

1. A quiere enviar dinero a B
2. La transacción se representa en la red como un "bloque"
3. El bloque se transmite a todas las partes de la red
4. Los que están en la red aprueban que la transacción es válida
5. El bloque entonces puede añadirse a la cadena, lo que proporciona un registro indeleble y transparente sobre las transacciones
6. El dinero se mueve de A a B

Fuente: FT

INSIDER PRO

Networking

1. New transactions are transmitted to all nodes.
2. Each node collects and verifies new transactions in a block.
3. Each node works to find a difficult proof of work for its block.
4. When a node finds a proof of work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and have not been spent.
6. Nodes express their acceptance of the block by working to create the next block in the chain, using the hash of the accepted block as the previous hash.

Here

Node = Miner

But they are different

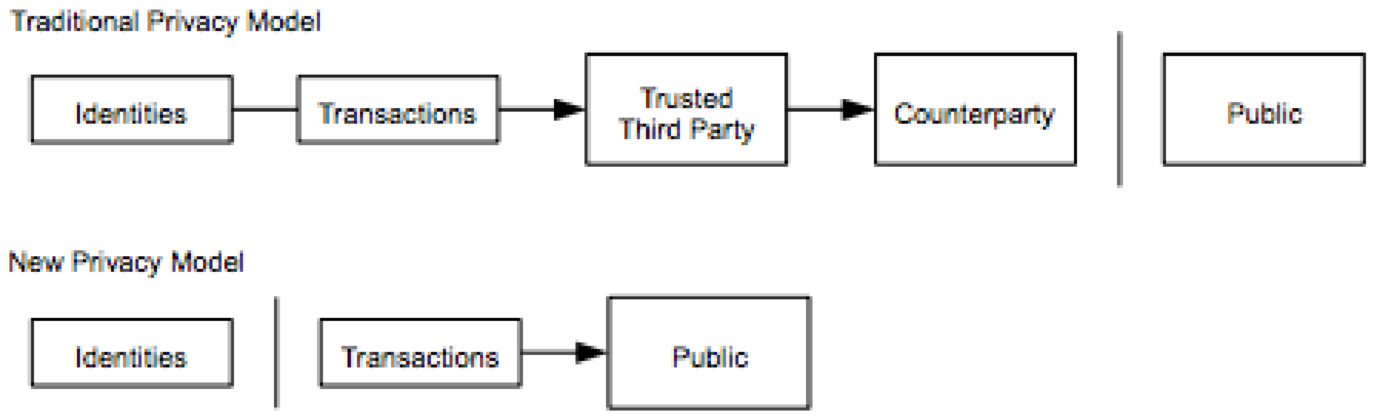
Watching Bitcoin mining

Node logic

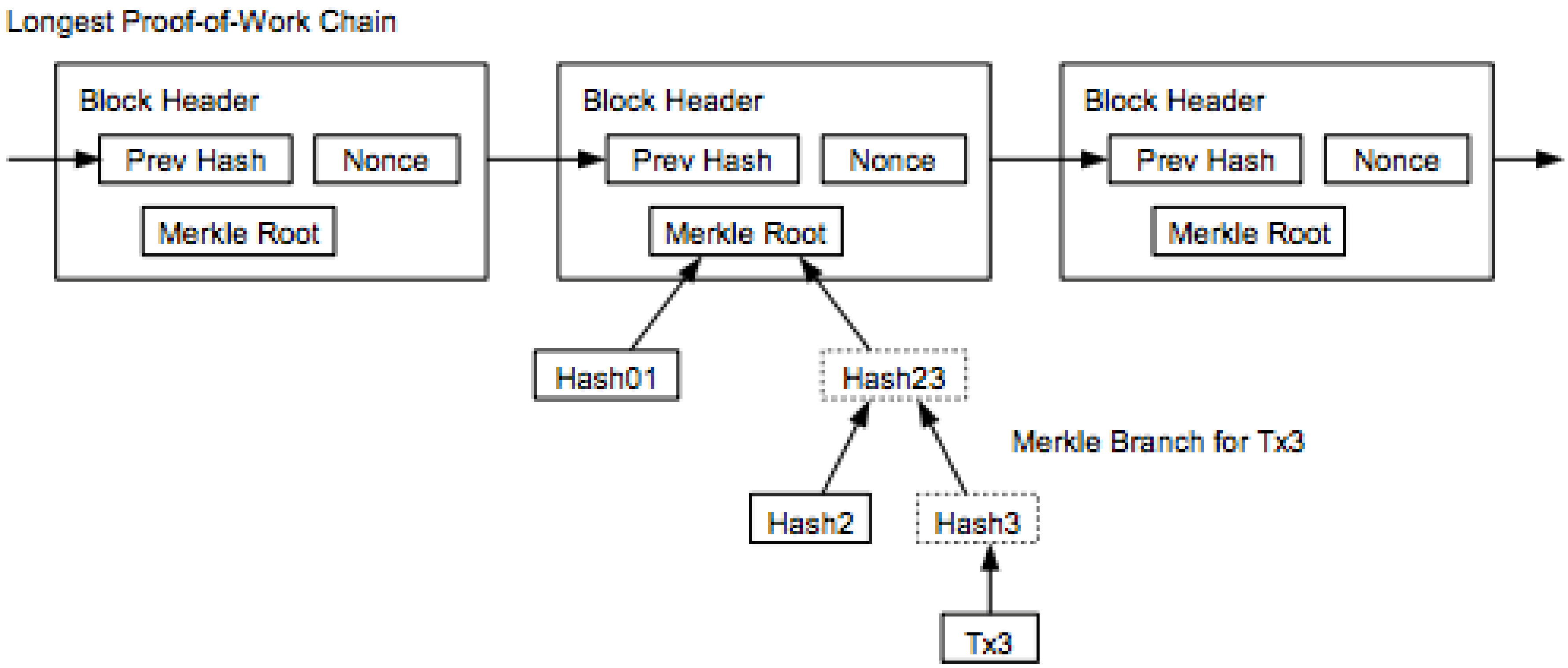
- Nodes always consider the longest string to be the correct one.
  - And they work on it to extend it.
- If two nodes transmit different versions of the next block simultaneously, some nodes may receive one or the other first.
  - They work on the first version they received, but keep the other branch in case it turns out to be the longer one.
- The tie is broken when the next working test is encountered and one branch becomes longer.
  - The nodes that were working on the other branch switch to the longer branch.

Privacy

- Traditional model, limiting access to information.
  - Parties involved and trusted third party.
- The need to publicly announce all transactions precludes this method.
  - Privacy by keeping public keys anonymous.



Transaction Verification



Transaction Verification

- A user only needs to keep a copy of the block headers of the longest string.
  - Which you can get by querying network nodes until you are convinced you have it.
  - *Full* vs *light* vs *lightning* nodes
- You can't verify the transaction yourself, but by linking it to a place on the chain, you can see that a network node has accepted it and the blocks added after you further confirm that the network has accepted it.

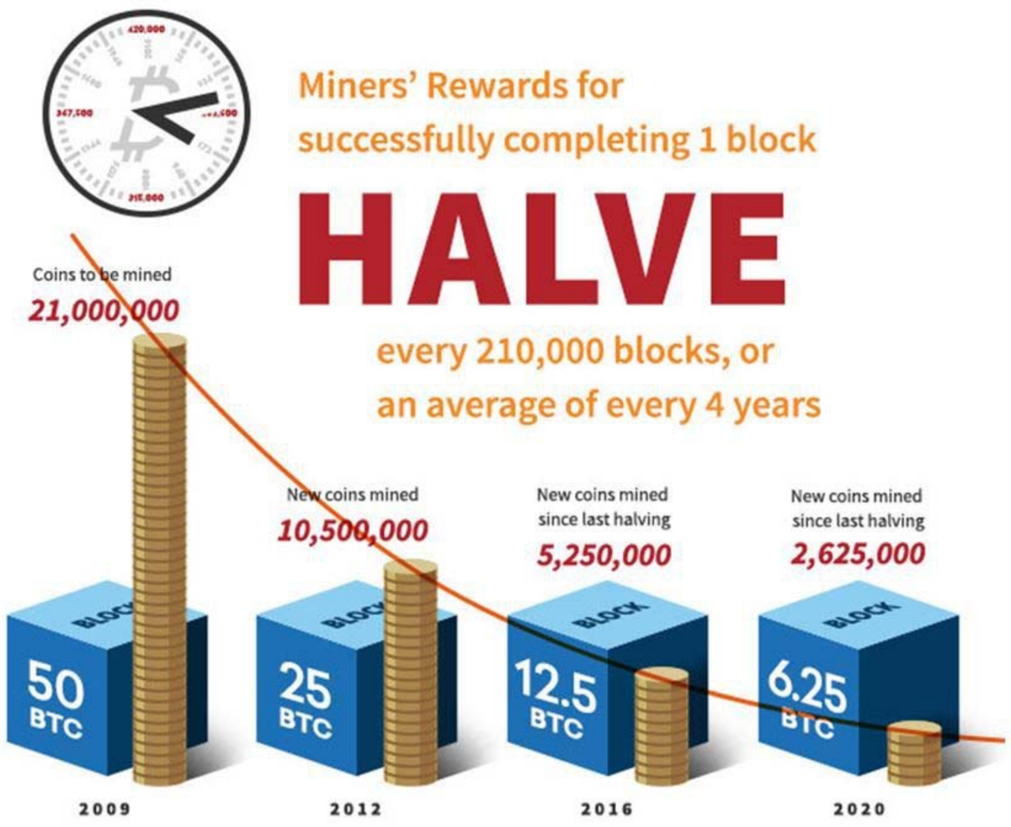
Distributed and immutable registry

- Blockchain retains data across transactions.
  - As in conventional databases.
- In Blockchain it is "almost impossible" to change the data once it is written in the chain.
  - Blocks can be changed, but it is extremely difficult to do so.
  - Requires rework in all blocks subsequent to the modified and consensus of each.
- So, in general, the transaction is immutable or indelible.
  - In terms of DB, blockchains are write and read only.
  - Like an accounting ledger written in ink, an error would be resolved with another entry.

Incentives

- By convention, the first transaction in a block is a special transaction that initiates a new coin owned by the block creator.
  - Incentive for nodes to work for the network
  - Mechanism for the initial distribution of coins in circulation
    - Since there is no central authority to issue them.
- The continued addition of a constant quantity of new coins is analogous to gold **miners** expending resources to add gold to circulation.
  - Here CPU and electricity what is spent.

Incentives



Updated information at

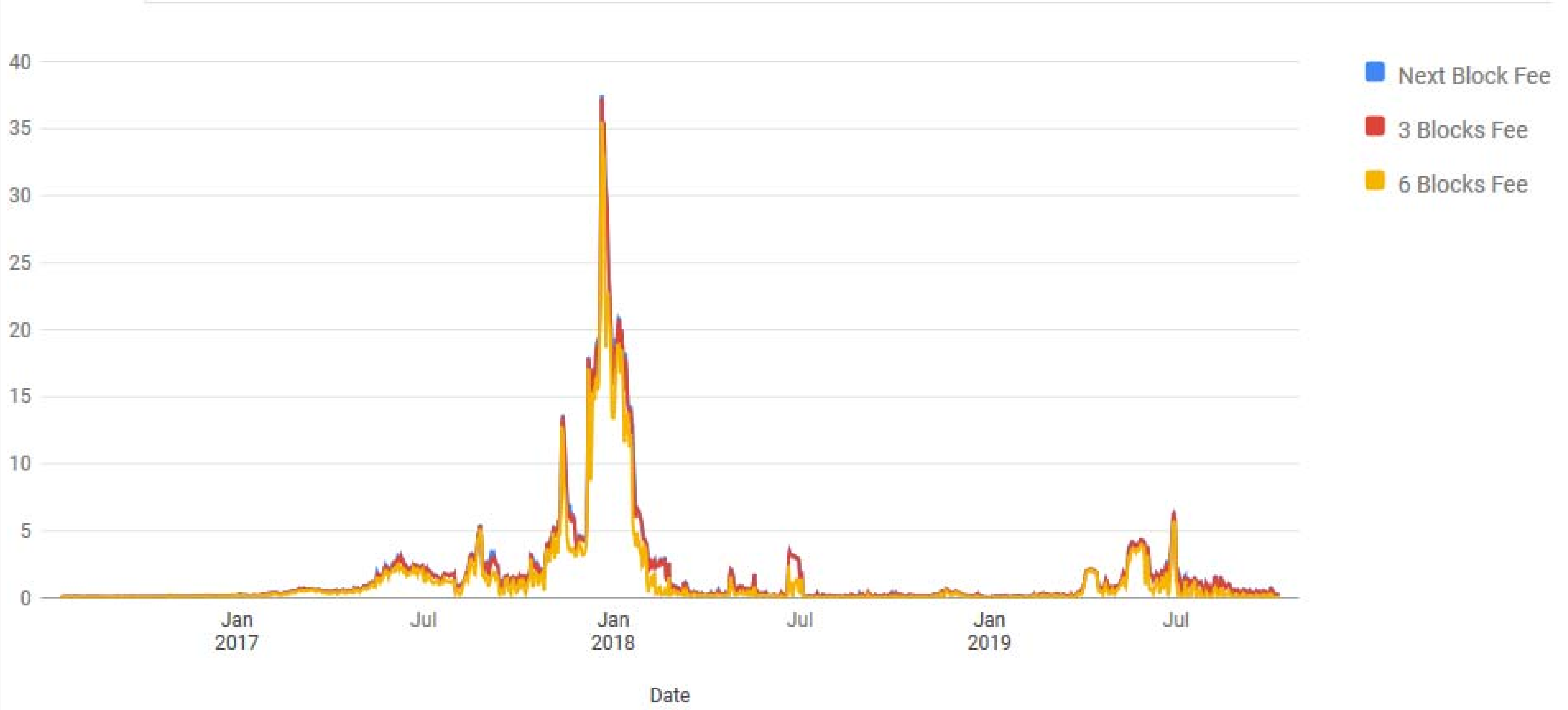
Incentives

- Can it be profitable for me?
  - Crypto Compare
  - Coin Warz
  - What to Mine
  - …

Incentives

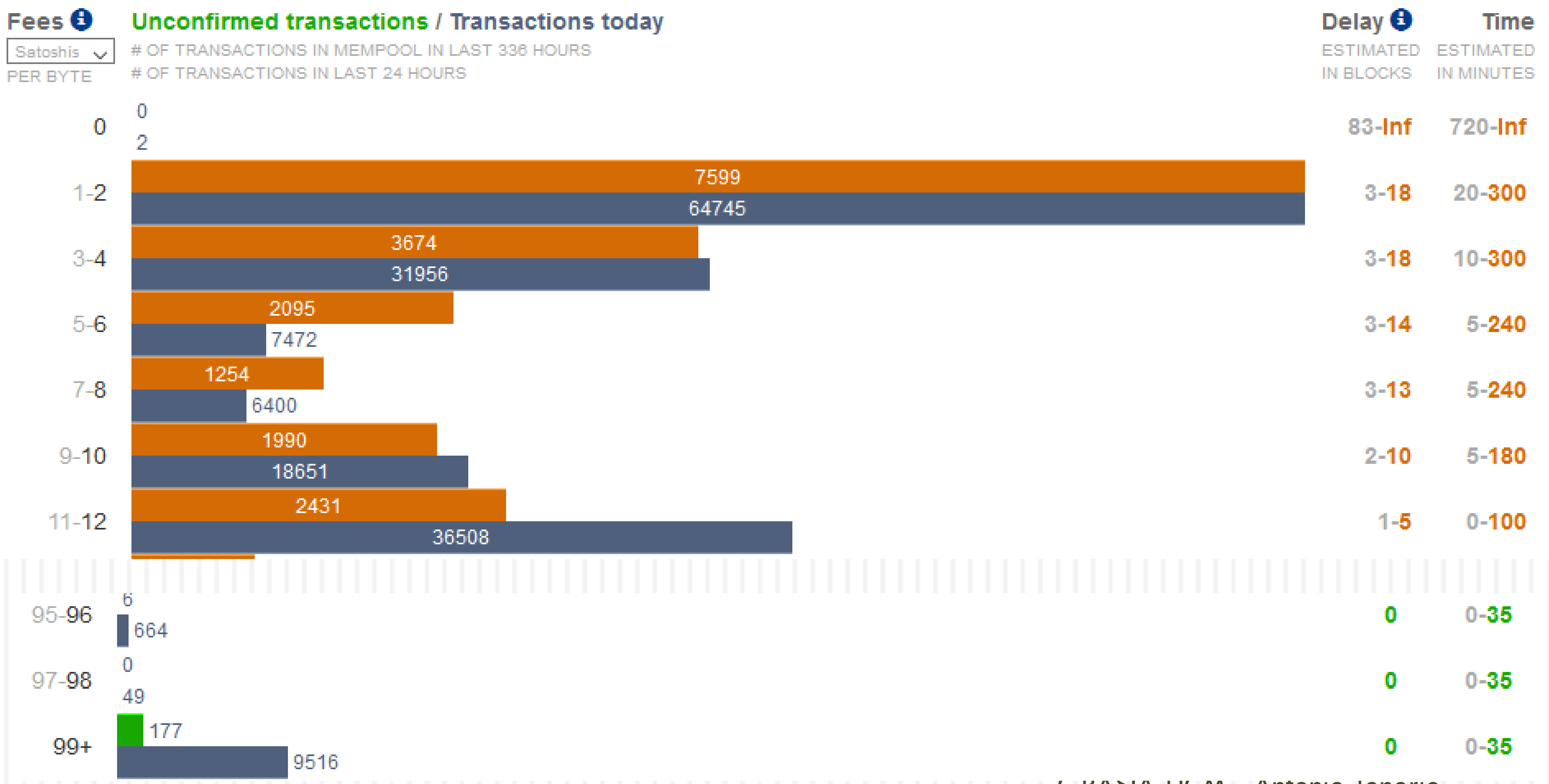
- Miners can choose the transactions they work on.
  - Those that add to the blocks.
- They may charge a transaction fee.
  - Next rate, 3 or 6 blocks
- Without a fee the transaction may be delayed.
  - Days, weeks or be rejected

Incentives



Rate in dollars per transaction

Delays



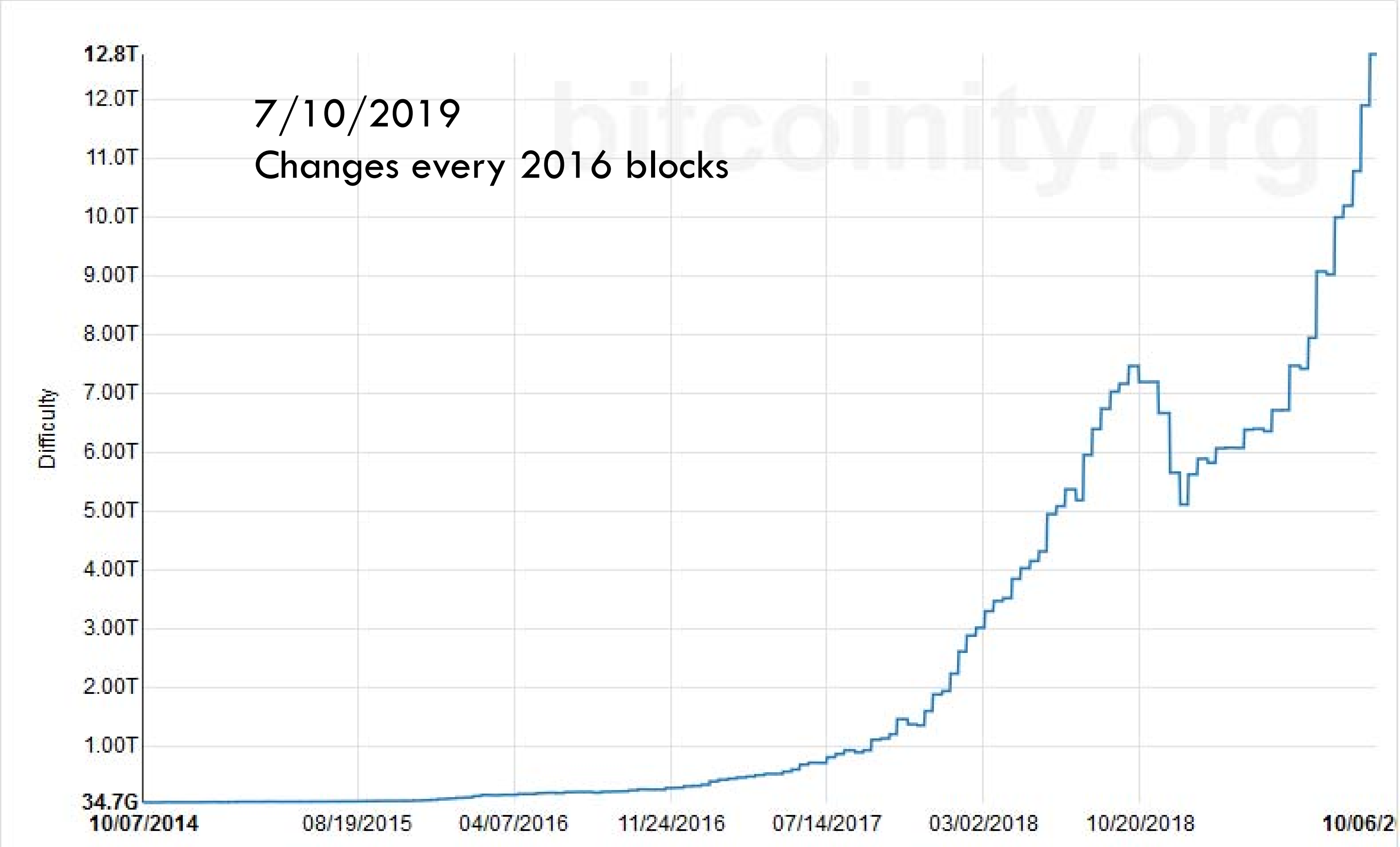
Fees Satoshis PER BYTE	Unconfirmed transactions # OF TRANSACTIONS IN MEMPOOL IN LAST 336 HOURS	Transactions today # OF TRANSACTIONS IN LAST 24 HOURS	Delay ESTIMATED IN BLOCKS	Time ESTIMATED IN MINUTES
0	0	2	83-Inf	720-Inf
1-2	7599	64745	3-18	20-300
3-4	3674	31956	3-18	10-300
5-6	2095	7472	3-14	5-240
7-8	1254	6400	3-13	5-240
9-10	1990	18651	2-10	5-180
11-12	2431	36508	1-5	0-100
95-96	6	664	0	0-35
97-98	0	49	0	0-35
99+	177	9516	0	0-35

Incentives

- Miners have a vote in the future of the network.
  - Change the block size?
  - Make a *fork*?
    - *Hard vs soft*
  - Allow more Bitcoins?

Evolution

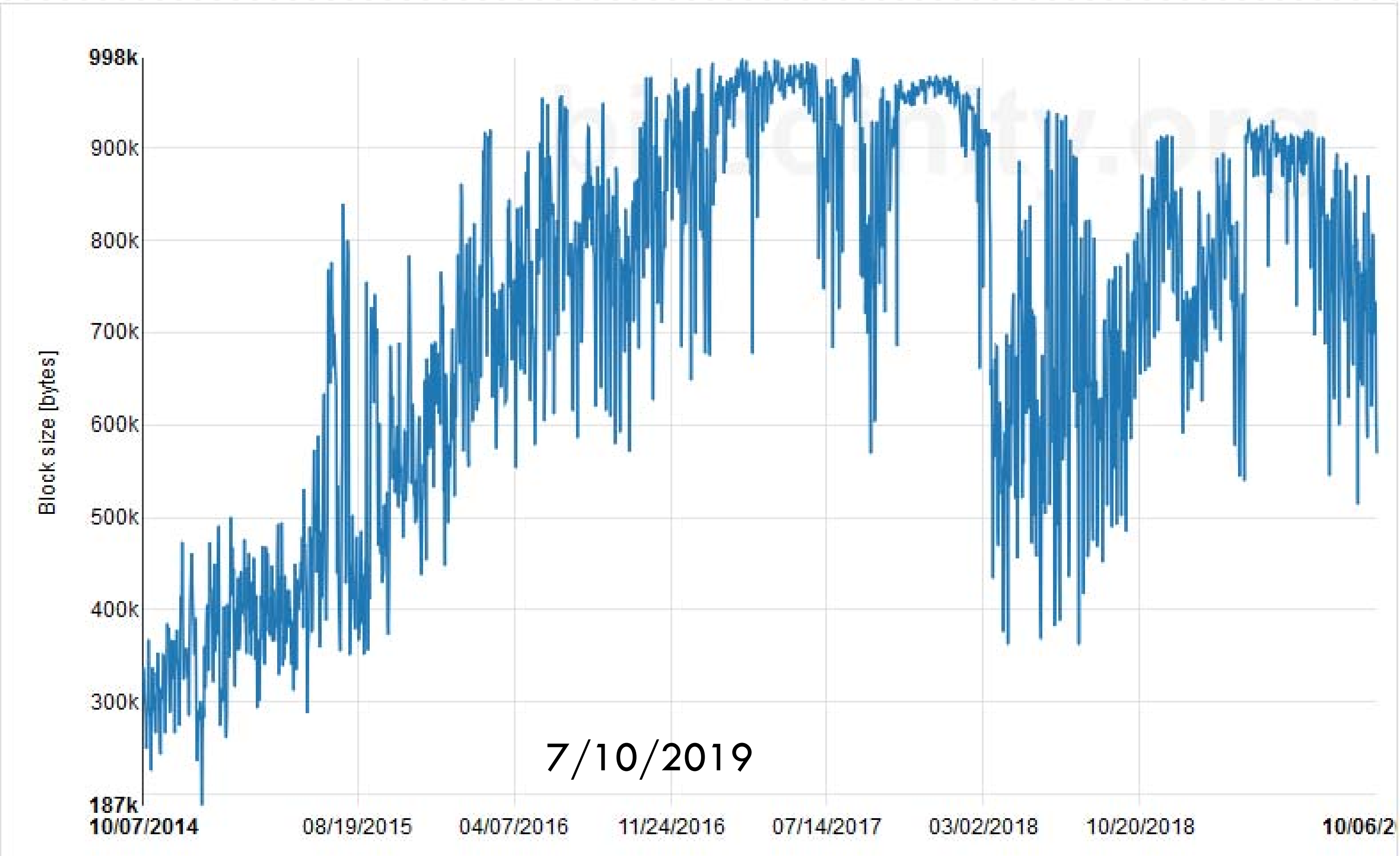
Hash difficulty - Bitcoin



7/10/2019

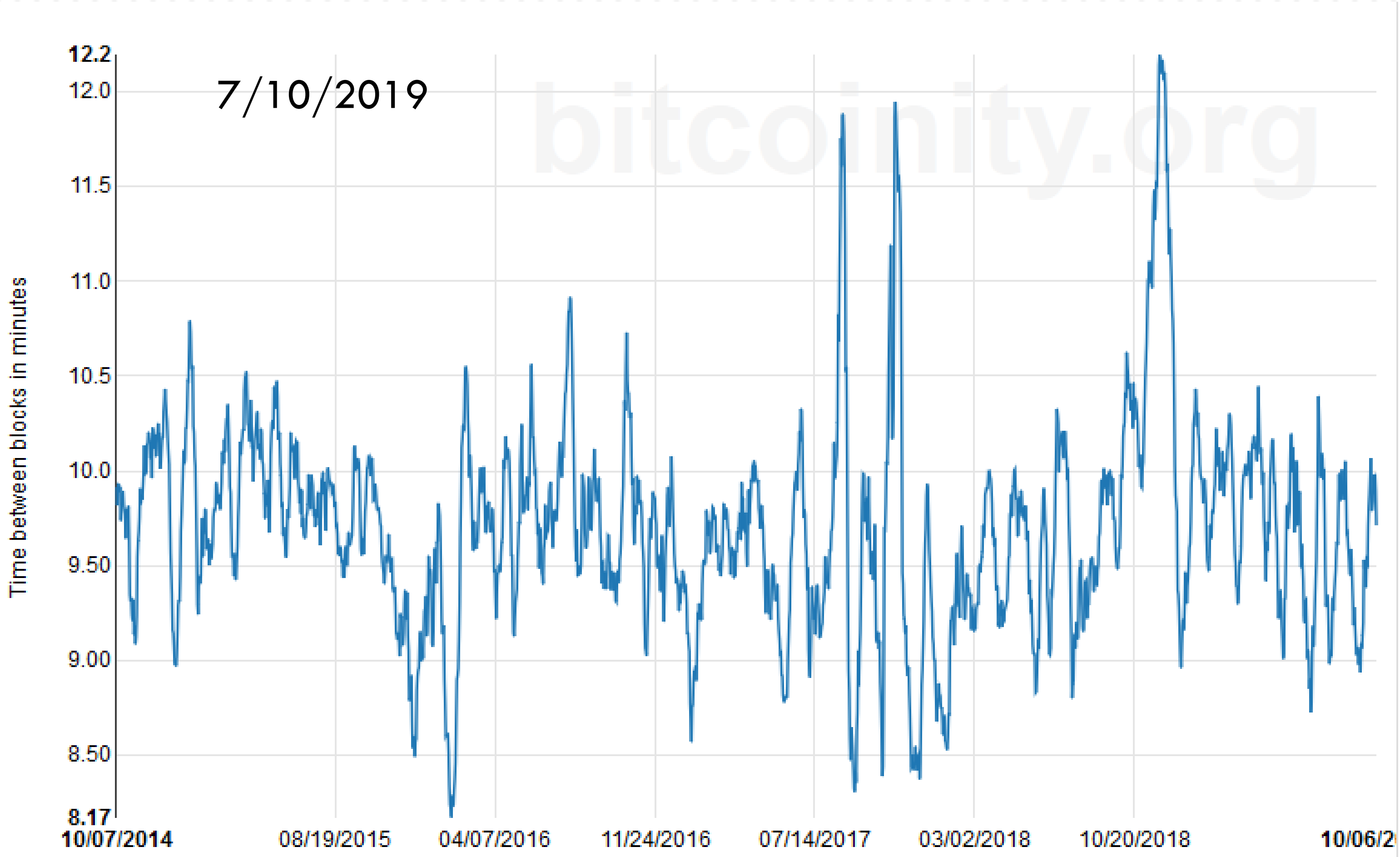
Changes every 2016 blocks

Block size - Bitcoin



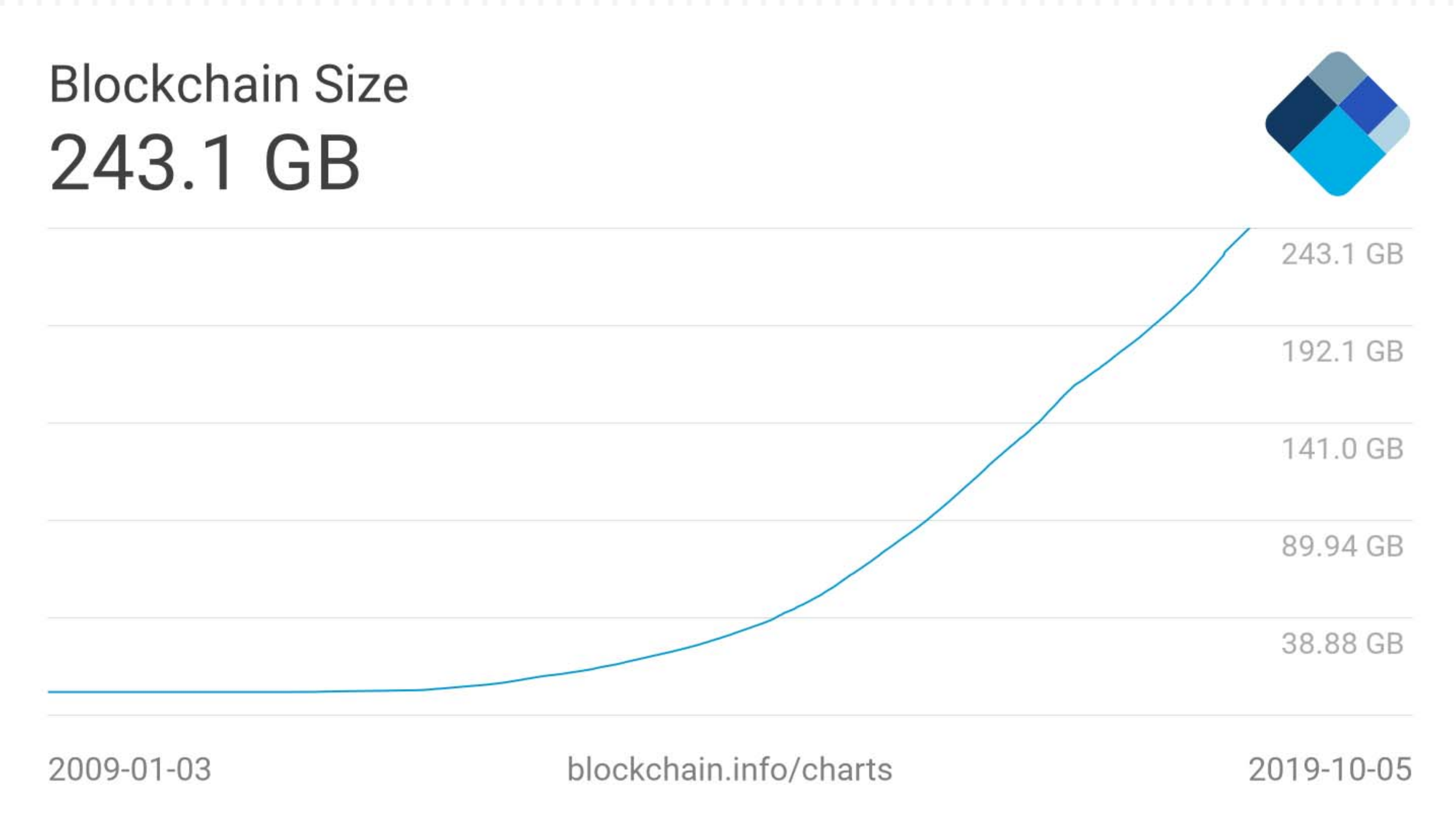
7/10/2019

Time between blocks - Bitcoin



7/10/2019

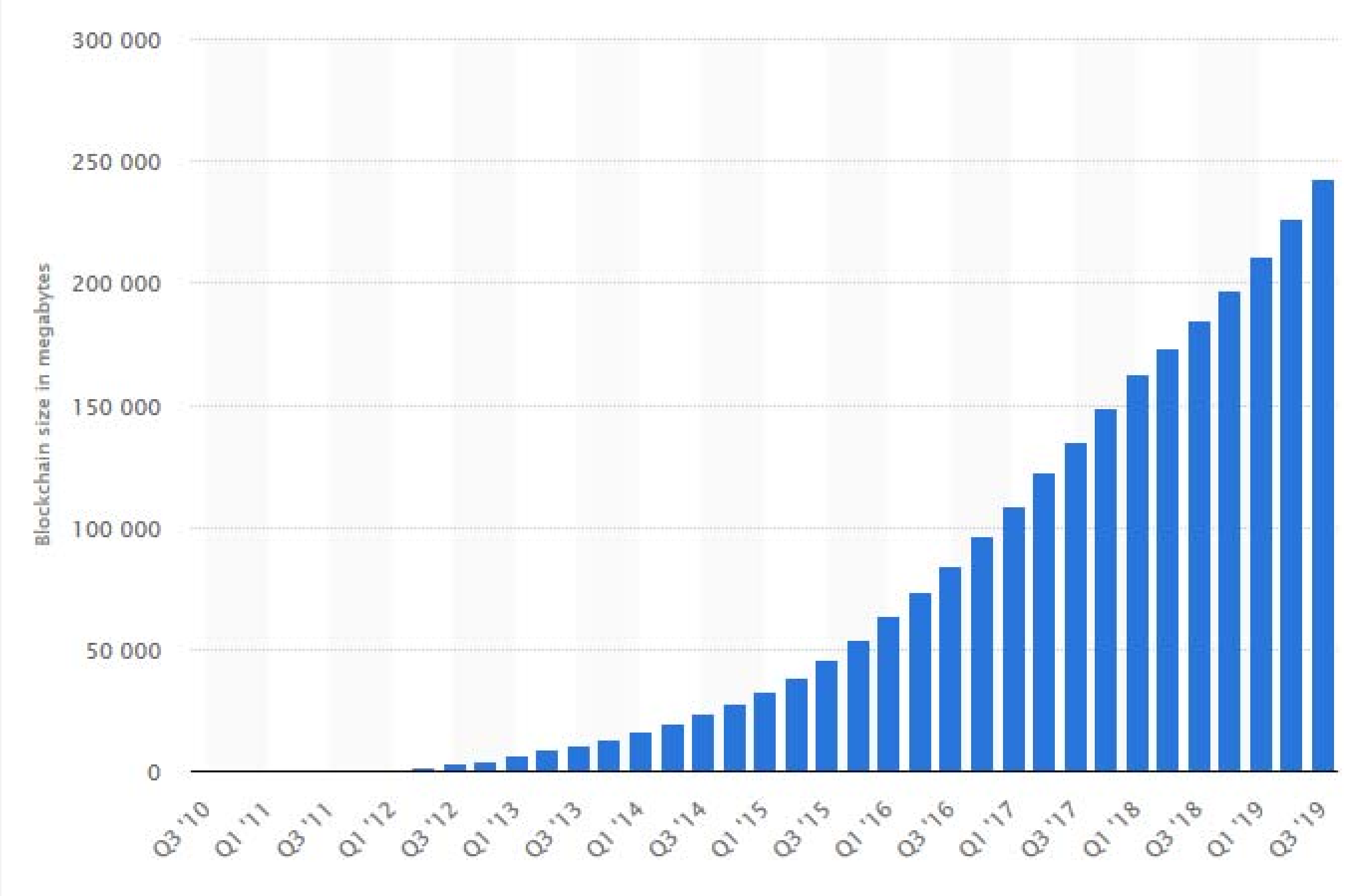
Ledger size - Bitcoin



Blockchain Size

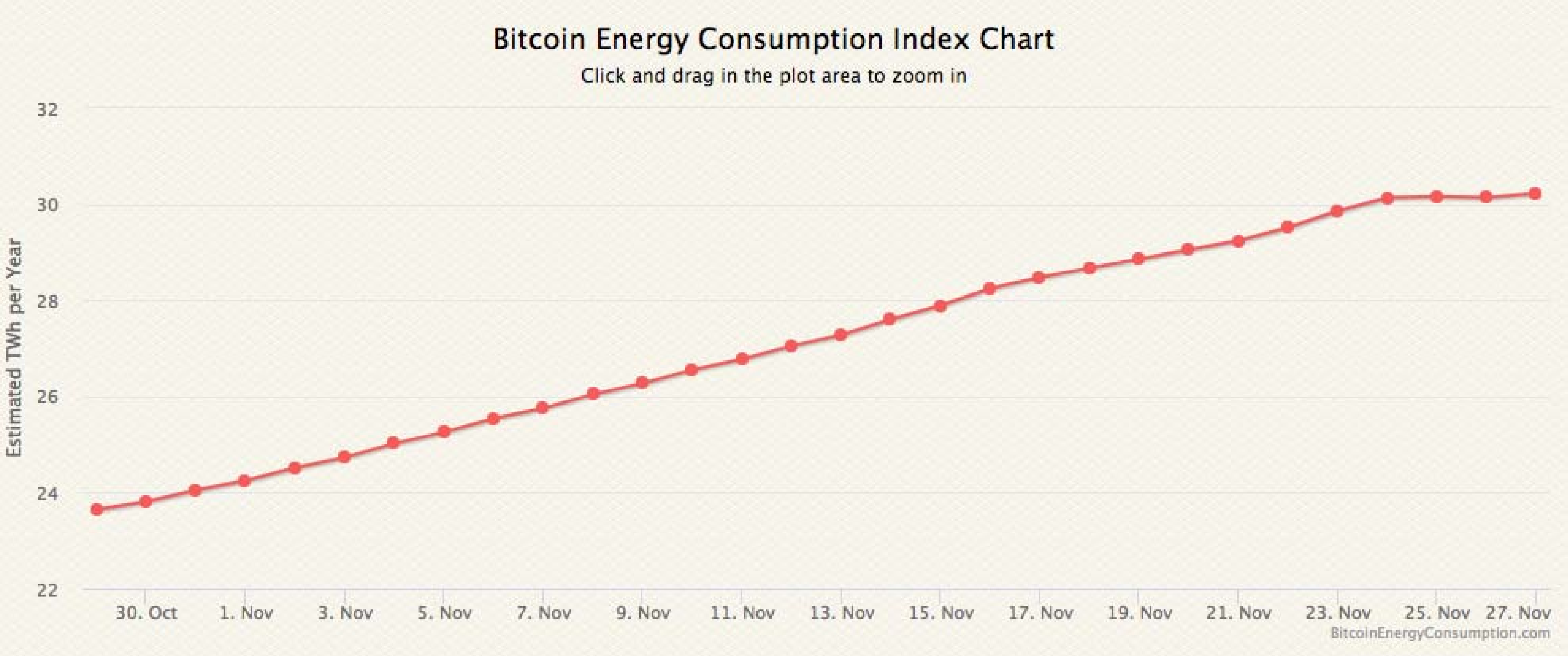
243.1 GB

Ledger size - Bitcoin

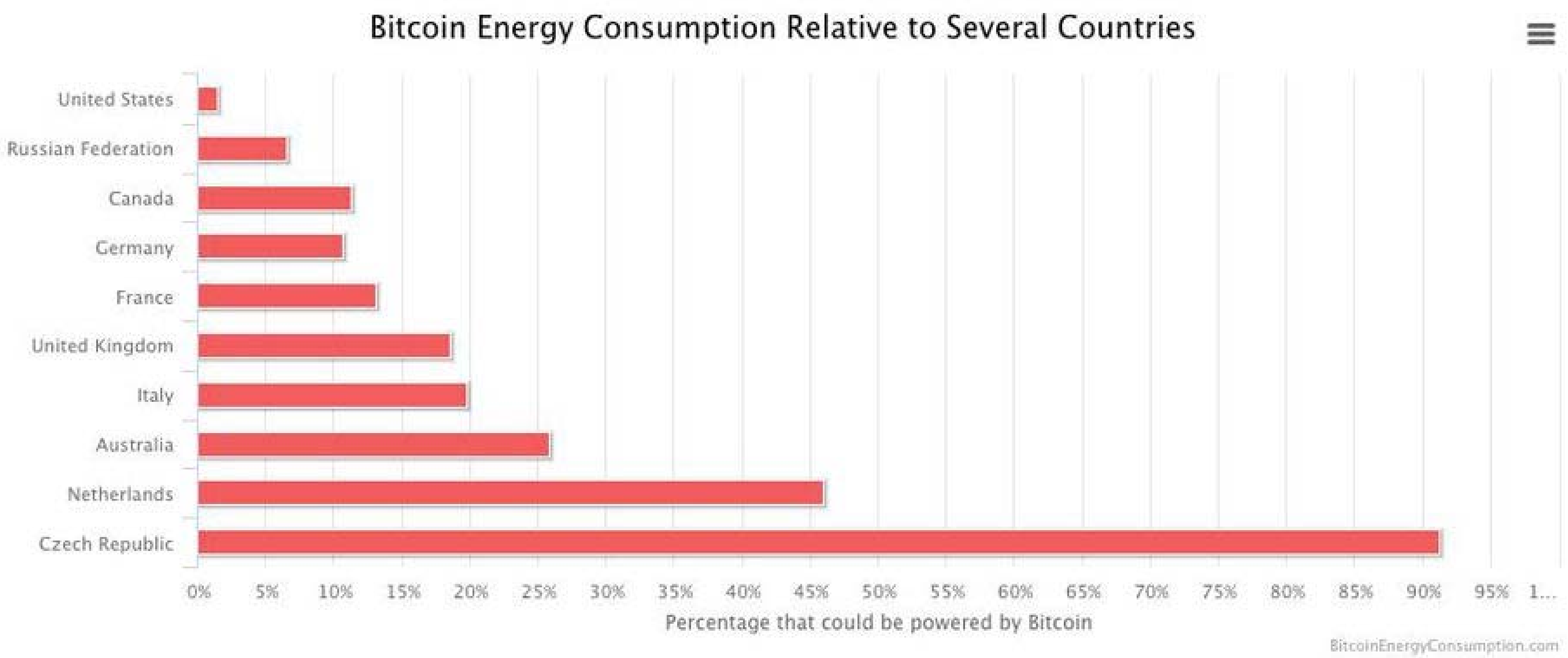


Transaction costs - Bitcoin

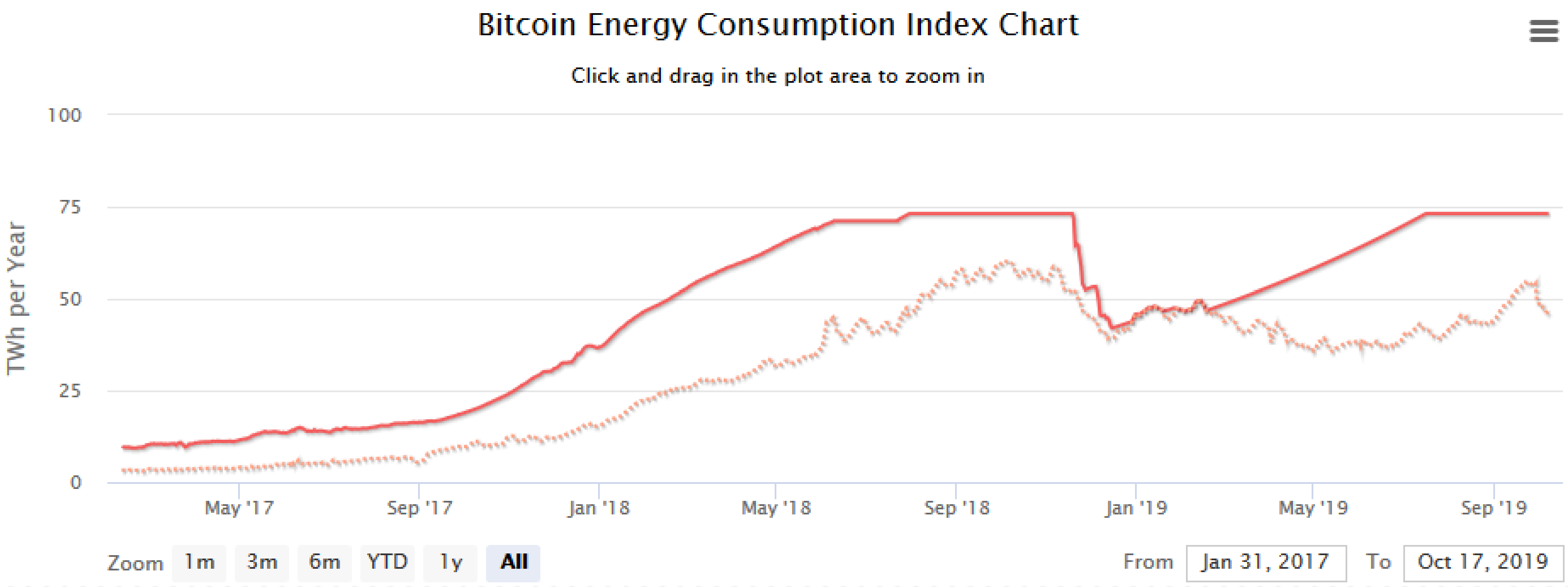
- □ Computationally and energy expensive



Power consumption



Power consumption

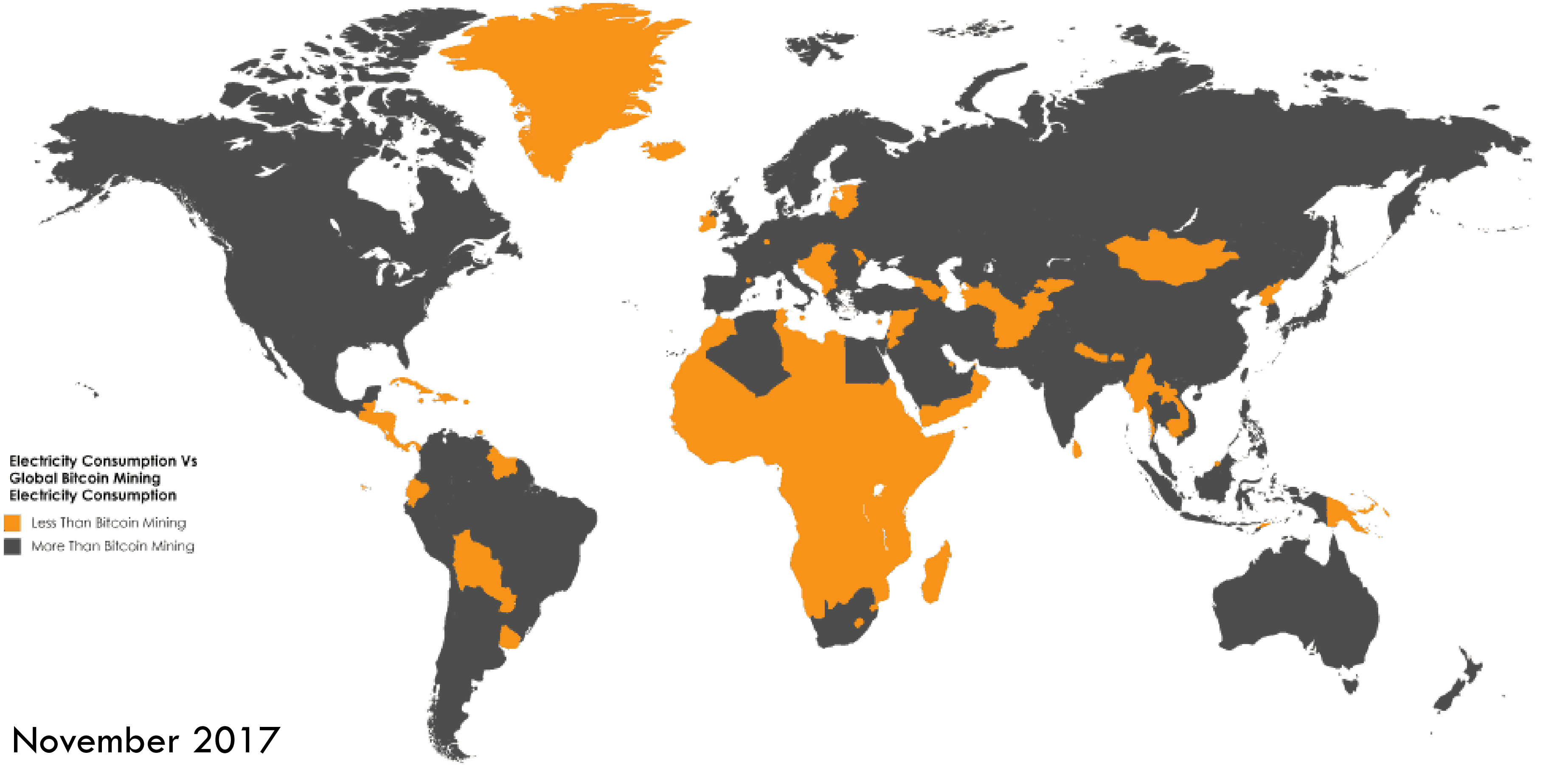


Bitcoin Energy Consumption Index Chart

Click and drag in the plot area to zoom in

From Jan 31, 2017 To Oct 17, 2019

Power consumption

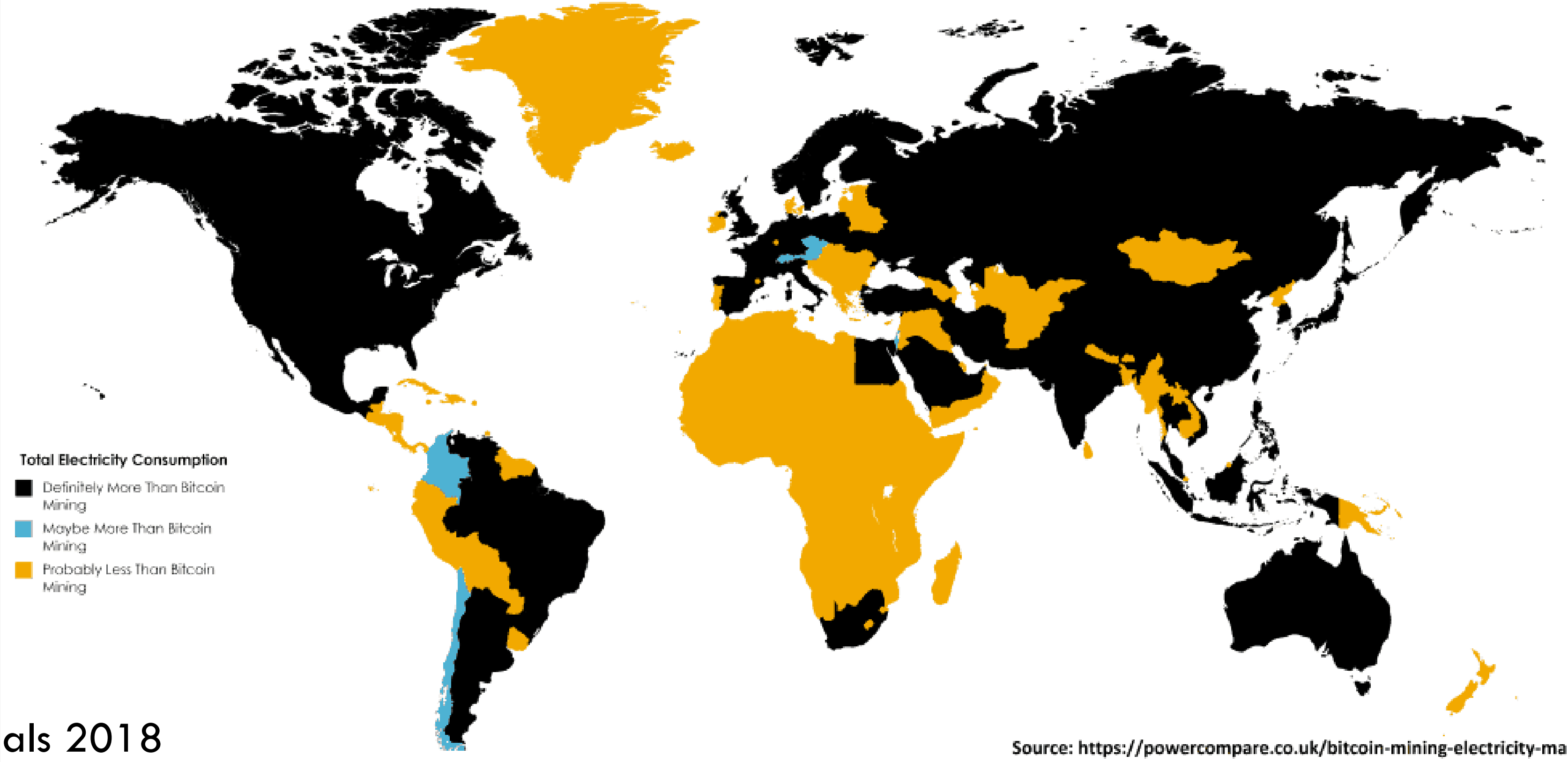

Electricity Consumption Vs
Global Bitcoin Mining
Electricity Consumption
🟧 Less Than Bitcoin Mining
⬛ More Than Bitcoin Mining

November 2017

Source: https://powercompare.co.uk/bitcoin/

Power consumption

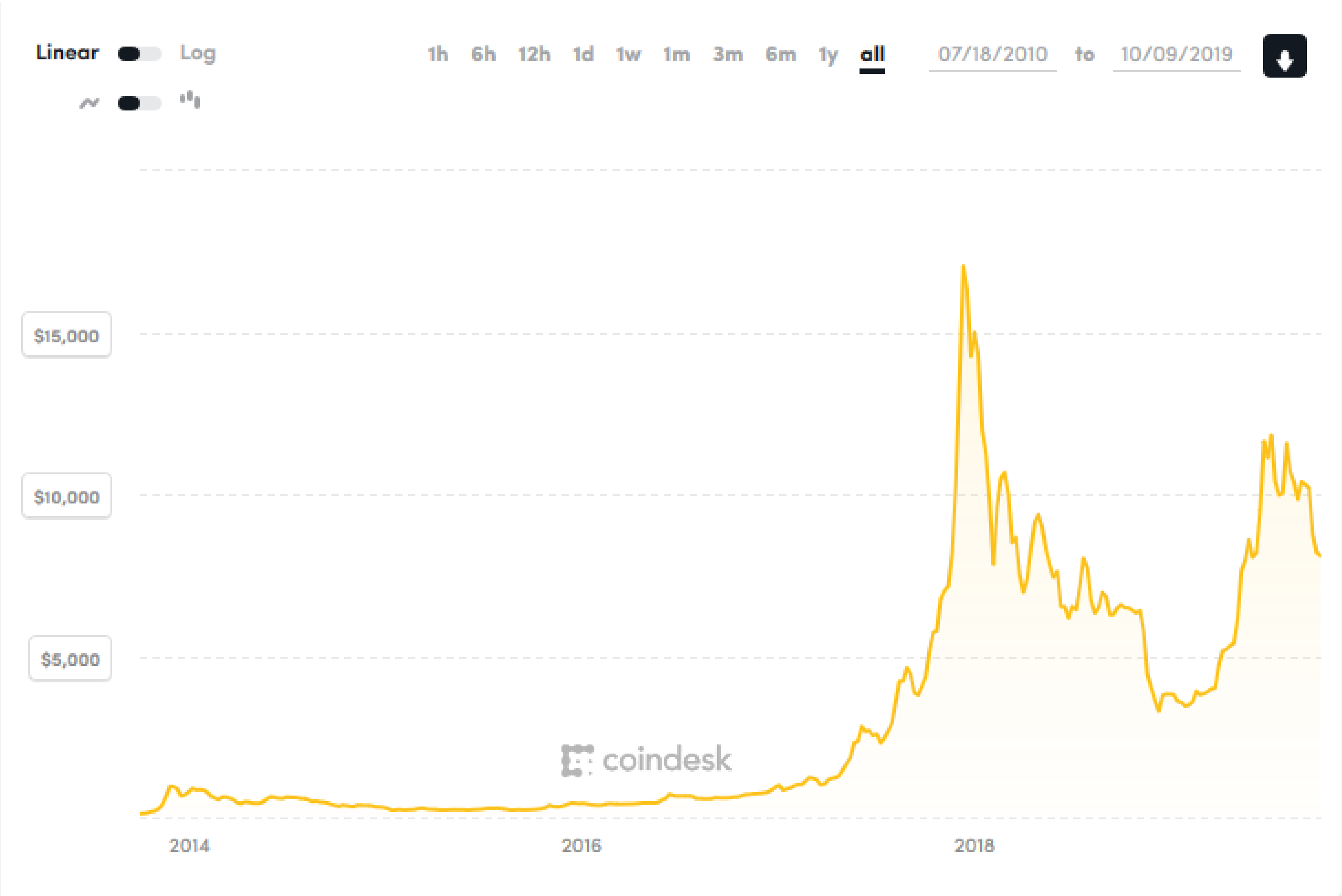
Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018


Total Electricity Consumption
⬛ Definitely More Than Bitcoin Mining
🟦 Maybe More Than Bitcoin Mining
🟧 Probably Less Than Bitcoin Mining

Finals 2018

Source: https://powercompare.co.uk/bitcoin-mining-electricity-map/

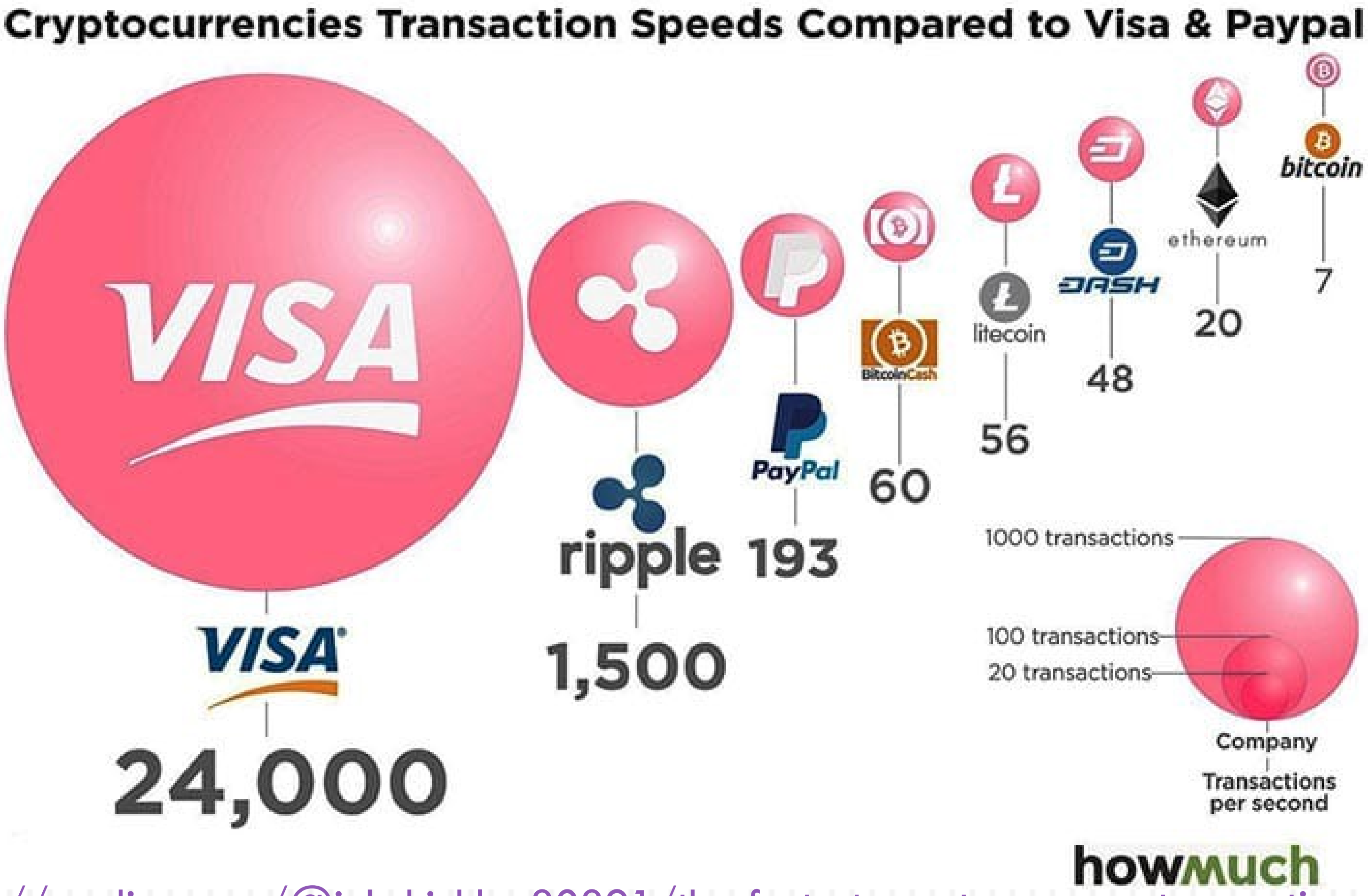
Price - Bitcoin



And when the Bitcoins run out?

- A maximum of 21 million bitcoins can be generated.
- It is not known when it will arrive.
  - Currently 75% has been mined but it is becoming increasingly difficult.
  - In 2009 you could mine 200 Bitcoins with a PC
  - In 2015 it would have taken 98 years to mine just 1 Bitcoin.
- Transaction fees
  - Will it be enough?

Speed of transactions



https://medium.com/@johnhinkle_80891/the-fastest-cryptocurrency-transaction-speeds-for-2018-4

Public vs. private blockchains

- Public Blockchains are encrypted but visible to the public.
  - E.g. https://www.blocktrail.com/BTC
- Private ones employ user rights for visibility.
  - Ex. permissions
    - Client: write and display all data
    - Auditors: view all transactions
    - Vendor A: writes and displays the data of partner A
    - Vendor B: writes and displays the data of partner B

Other applications

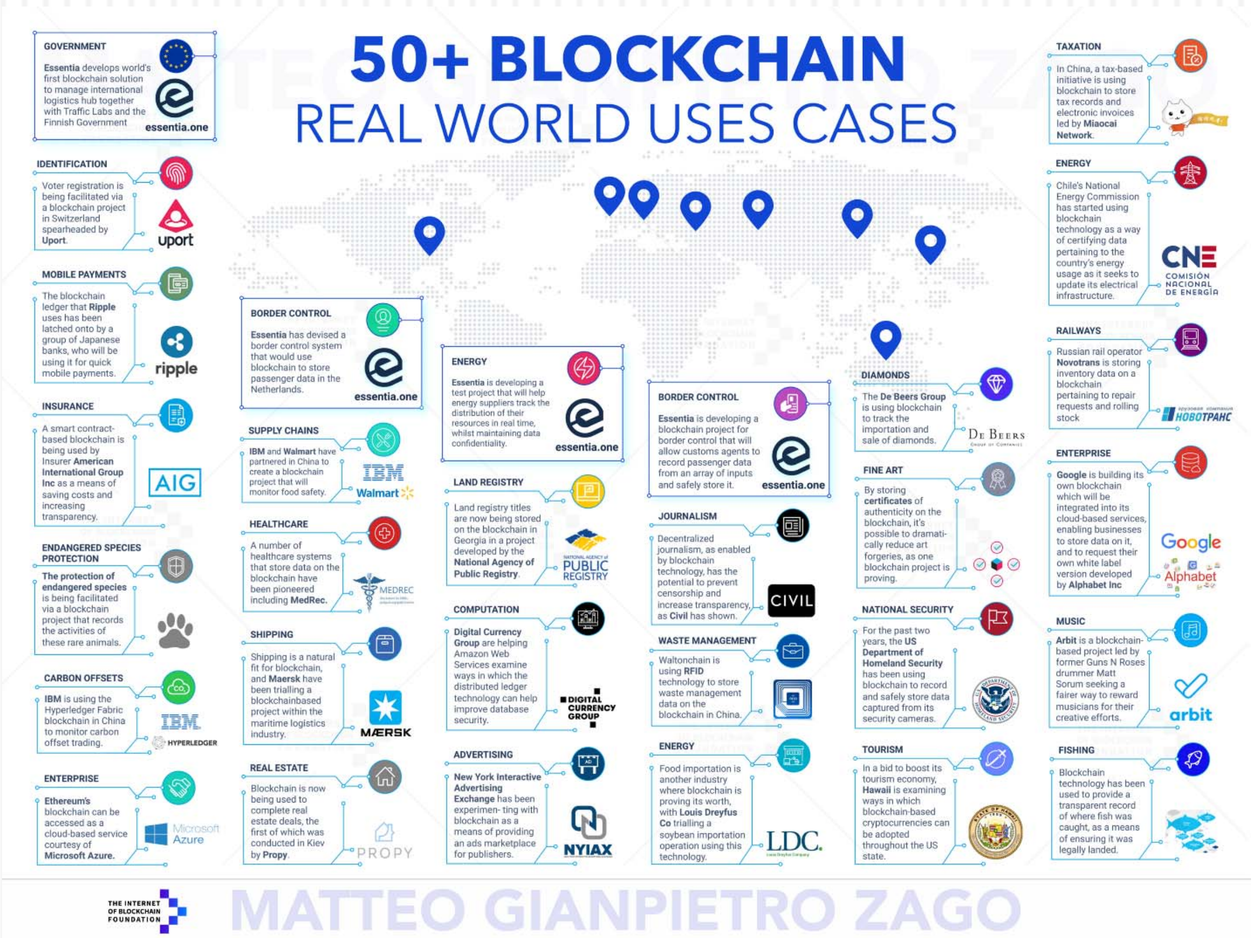
- Alternative altcoins to Bitcoin

- Tokens on the Bitcoin Blockchain
  - ColoredCoins (https://coloredcoins.org/)
  - CounterParty (https://counterparty.io/)
- Decentralized DNS
  - NameCoin (https://www.namecoin.org/)
- Storage
  - Storj (https://storj.io/)
  - Filecoin (https://filecoin.io/)
- Computing
  - Golem (https://golem.network/)

Other applications: currency and financial

- Payments
  - Square (https://www.coindesk.com/square-gets-a-bitlicense-new-york-crypto/)
- Gift Cards
  - Gyft (https://www.gyft.com/bitcoin/)
  - eGifter (https://www.egifter.com/)
- Financial Services
  - Banks (https://www.ethnews.com/gmo-internet-group-creates-a-bank)
  - *Hedge funds* (https://www.bitwiseinvestments.com/fund)
  - Bonds and liquidity (https://ripple.com/solutions/source-liquidity/)
  - Crowdfunding (https://www.idgconnect.com/blog-abstract/30700/blockchain-africa)

Other applications



50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT

Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION

Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

MOBILE PAYMENTS

The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

INSURANCE

A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

ENDANGERED SPECIES PROTECTION

The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS

IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

ENTERPRISE

Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

BORDER CONTROL

Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS

IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

HEALTHCARE

A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

SHIPPING

Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

REAL ESTATE

Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.

ENERGY

Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY

Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

COMPUTATION

Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

ADVERTISING

New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

BORDER CONTROL

Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM

Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

WASTE MANAGEMENT

Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY

Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

DIAMONDS

The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

FINE ART

By storing **certificates** of authenticity on the blockchain, it's possible to dramati-cally reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY

For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM

In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION

In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY

Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

RAILWAYS

Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

ENTERPRISE

Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

MUSIC

Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

FISHING

Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

THE INTERNET OF BLOCKCHAIN FOUNDATION

MATTEO GIANPIETRO ZAGO

https://medium.com/@matteozago/50-examples-of-how-blockchains-are-taking-over-the-world-4

Ethereum and smart contracts

Smart contracts

Encoding clauses into source code in a manner which is automatically self-enforced and executed without the need for a central authority, in the form of smart contracts (Szabo, 1997).

- Emulates traditional contract (voluntary agreement between parties)
- Trustless
- Automatic application (*self-enforcement*)

Smart contracts on the Blockchain

- *Smart Contracts*:
  - small programs
  - that are deployed on the blockchain
  - are executed by the nodes of the network.
  - operate autonomously:
    - independent of "third parties" to operate
    - potentially uncontrollable

- Provides a layer of business logic prior to sending blocks.