MAY 24th 2022

Online • 10h Lisbon time (UTC)

INTERNATIONAL WEBINAR

BLOCKCHAIN & CRYPTOCURRENCIES

SUPPORT TECHNOLOGIES AND FUTURE TRENDS OF BLOCKCHAIN AND CRYPTOCURRENCIES

Mário Marques da Silva – Chairman

Universidade Autónoma de Lisboa & Instituto de Telecomunicações

CRYPTOCURRENCIES OR CRYPTOASSETS

João Duque

Instituto Superior de Economia e Gestão

VALUE CHAIN TRANSPARENCY ENABLED BY BLOCKCHAIN

Nuno Almeida

Ernest & Young

LAW ENFORCEMENT TRAINING ON CRYPTOCURRENCIES

Ionut Stoica

European Union Agency for Law Enforcement Training

UAL - Dep. de Engenharias e de Ciências da Computação

THE CONFERENCE WILL ONLY BE AVAILABLE UPON REGISTRATION AT AUTONOMA.PT

Support Technologies and Future Trends of Blockchain and Cryptocurrencies

Mário Marques da Silva

Professor at Universidade Autónoma de Lisboa

Director of the Department of Engineering and Computer Sciences

Researcher at Instituto de Telecomunicações

mmsilva@autonoma.pt

UAL

Autónoma TECHLAB
Centro de Investigação em Tecnologias

MAY 24th 2022
Online • 10h Lisbon time (UTC)

INTERNATIONAL WEBINAR
BLOCKCHAIN
&
CRYPTOCURRENCIES

SUPPORT TECHNOLOGIES AND FUTURE TRENDS OF BLOCKCHAIN AND CRYPTOCURRENCIES
Mário Marques da Silva – Chairman
Universidade Autónoma de Lisboa & Instituto de Telecomunicações

CRYPTOCURRENCIES OR CRYPTOASSETS
João Duque
Instituto Superior de Economia e Gestão

VALUE CHAIN TRANSPARENCY ENABLED BY BLOCKCHAIN
Nuno Almeida
Ernest & Young

LAW ENFORCEMENT TRAINING ON CRYPTOCURRENCIES
Ionut Stoica
European Union Agency for Law Enforcement Training

UAL - Dep. de Engenharias e de Ciências da Computação

THE CONFERENCE WILL ONLY BE AVAILABLE UPON REGISTRATION AT AUTONOMA.PT

Agenda

1. Introduction

2. Bitcoin

3. Blockchain

4. Mining

Agenda

1. **Introduction**

2. Bitcoin

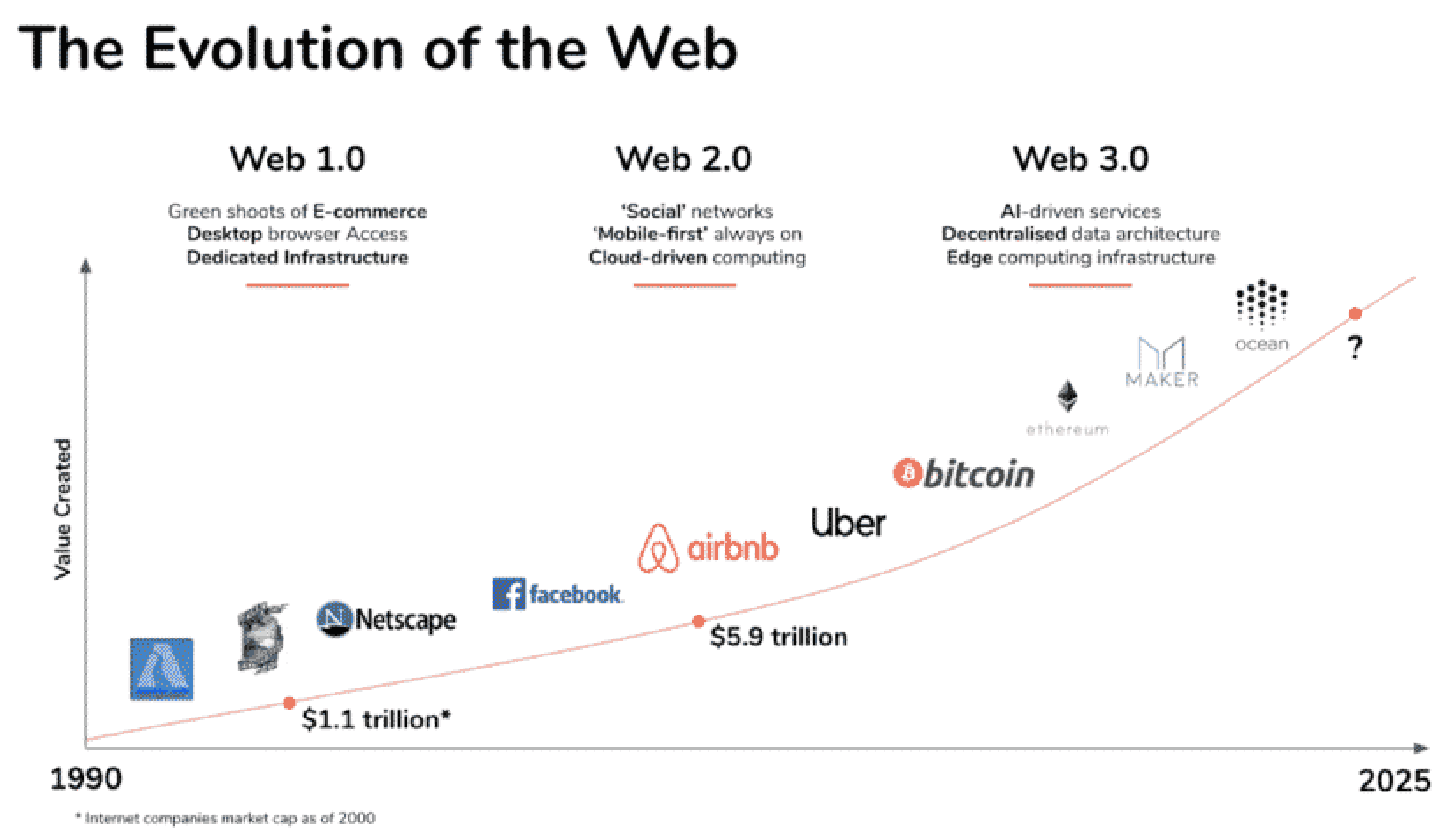
3. Blockchain

4. Mining

1. Introduction

With the massive use of the Internet, there is a need for a Currency with the same requirements: **Global** and **Instantaneous**.

Moreover, cryptocurrencies are **Decentralized** and **Secure**.



Web3.0
Internet
wires, network
Web 1.0
read-only
static
Web 2.0
read-write
dynamic
Web 3.0
read-write-trust
verifiable
NULL SIMPLY

Agenda

1. Introduction

2. Bitcoin

3. Blockchain

4. Mining

2. Bitcoin

*“Bitcoin is a smart currency, designed to be evolved by smart engineers. It **eliminates the need for banks**, frees you from credit card fees, **exchange fees**, wire transfer fees, and **reduces the need for “lawyers” or “juries”** in transactions… all good things.”*

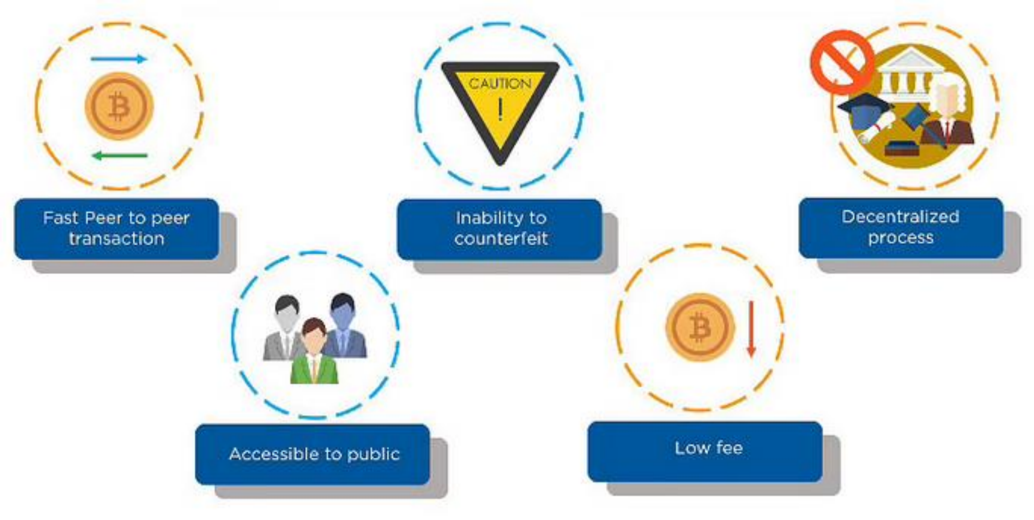
Peter Diamondis, Founder & President of X Prize Foundation

- Currency without governance, without intermediaries, without borders, decentralized and secure.
- As is the Internet (except decentralized and secure [Web 3.0])

Owning US$ 96 Billions, CEO of Binance, Changpeng Zhao, is the 11nd Richest in the World

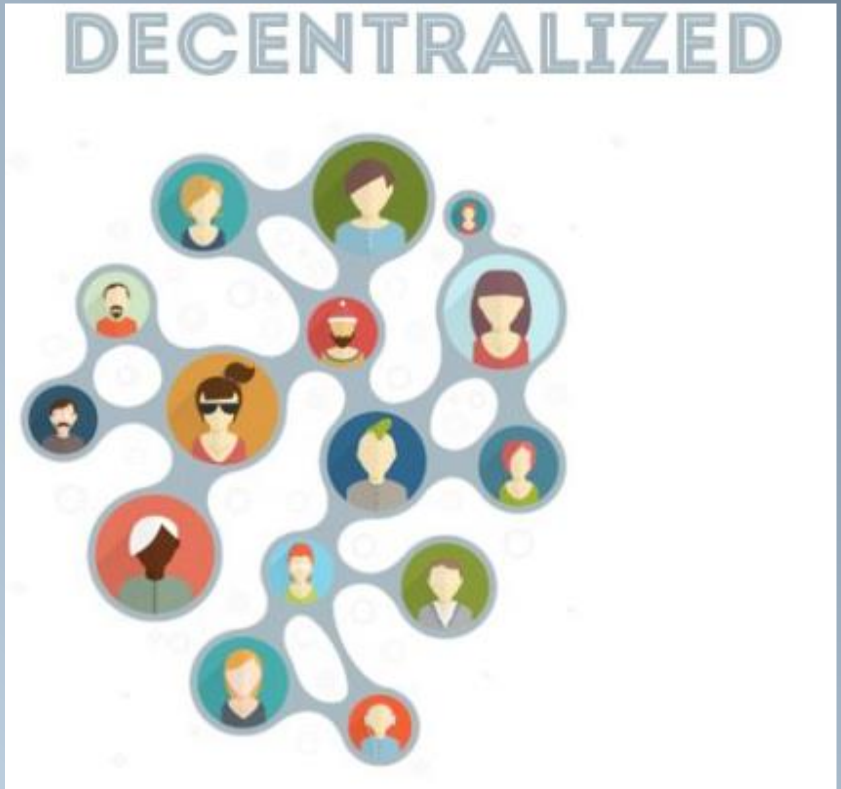
2. Bitcoin

- Bitcoin is the mostly known cryptocurrency (the first):
  - Created in 2009 by Satoshi Nakamoto
  - **Descentralized and without intermediaries** (not controlled by governaments and banks)
  - **Global**
  - **Secure / Trustable**
  - Without intermediaries (faster, cheaper and more private than fiat currency)
  - Used for shopping, investment, payments, etc. [although some only see it as an investment of "stock market" type]
  - Uses Blockchain Technology, allowing peer-to-peer transfers [based on secure criptography]: utilizes the computer networks of users (instead of a central server)



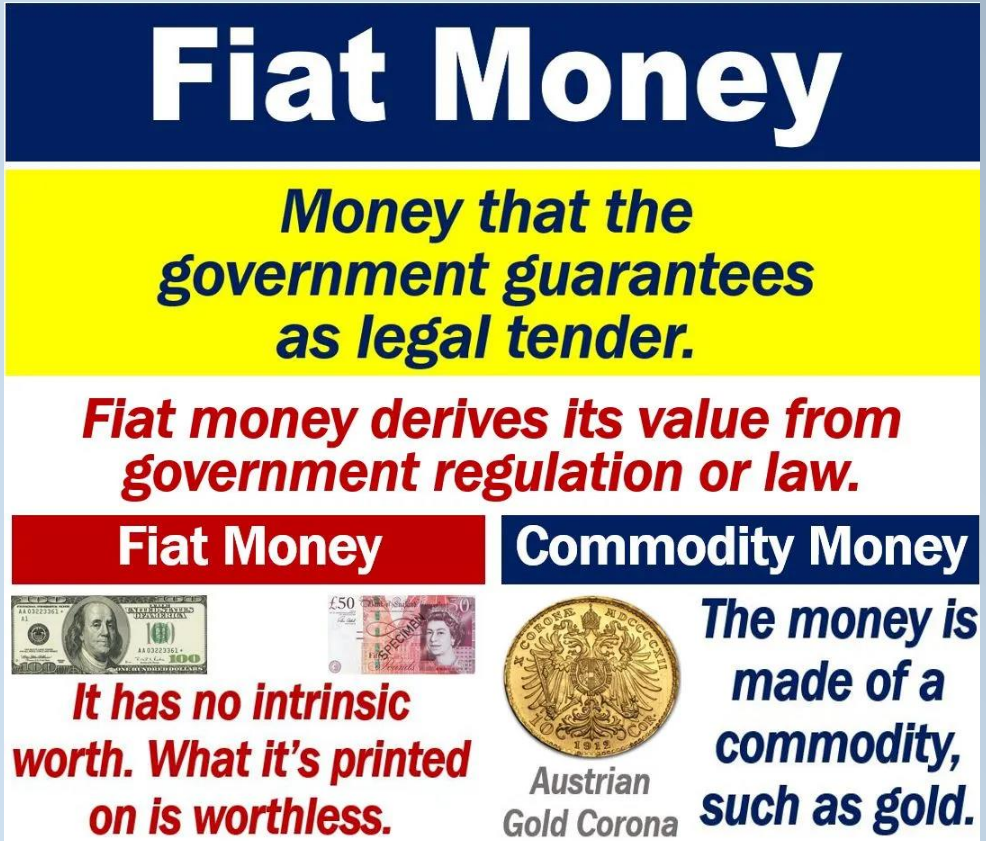
2. Bitcoin

- Bitcoin is the mostly known cryptocurrency (cont.):
    - Limited to 21 Millions
    - More **secure** and **less charges** than conventional online transfers
    - More secure than fiat currencies (cash - €€€ $$$) → easy to be counterfeit
    - Transfers realized 24/7, processed rapidly.
    - Transactions are Pseudonyms (not anonymous)
        - Each person has a wallet with a public address (Bitcoin Address):
            - Wallets are visible in the blockchain, as well as the transfers from A to B, with value X.
    - Around 30% of the persons worldwide are unable to have a conventional bank account.



2. Bitcoin

- Fiat money is a government-issued currency that is not defined by a physical commodity, such as gold or silver.
  - Subject to printing, to mitigate economical factors or bank failures, governments, etc., causing inflation/devaluation, with implications over peoples' savings.



Fiat Money

Money that the government guarantees as legal tender.

Fiat money derives its value from government regulation or law.

Fiat Money

It has no intrinsic worth. What it's printed on is worthless.

Commodity Money

Austrian Gold Corona

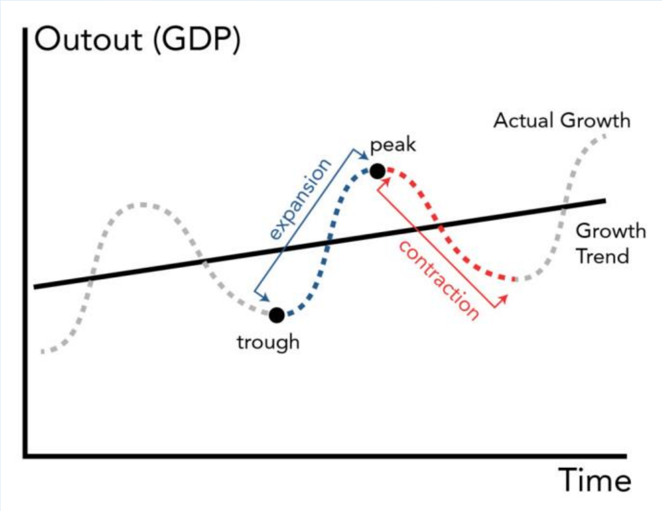
The money is made of a commodity, such as gold.

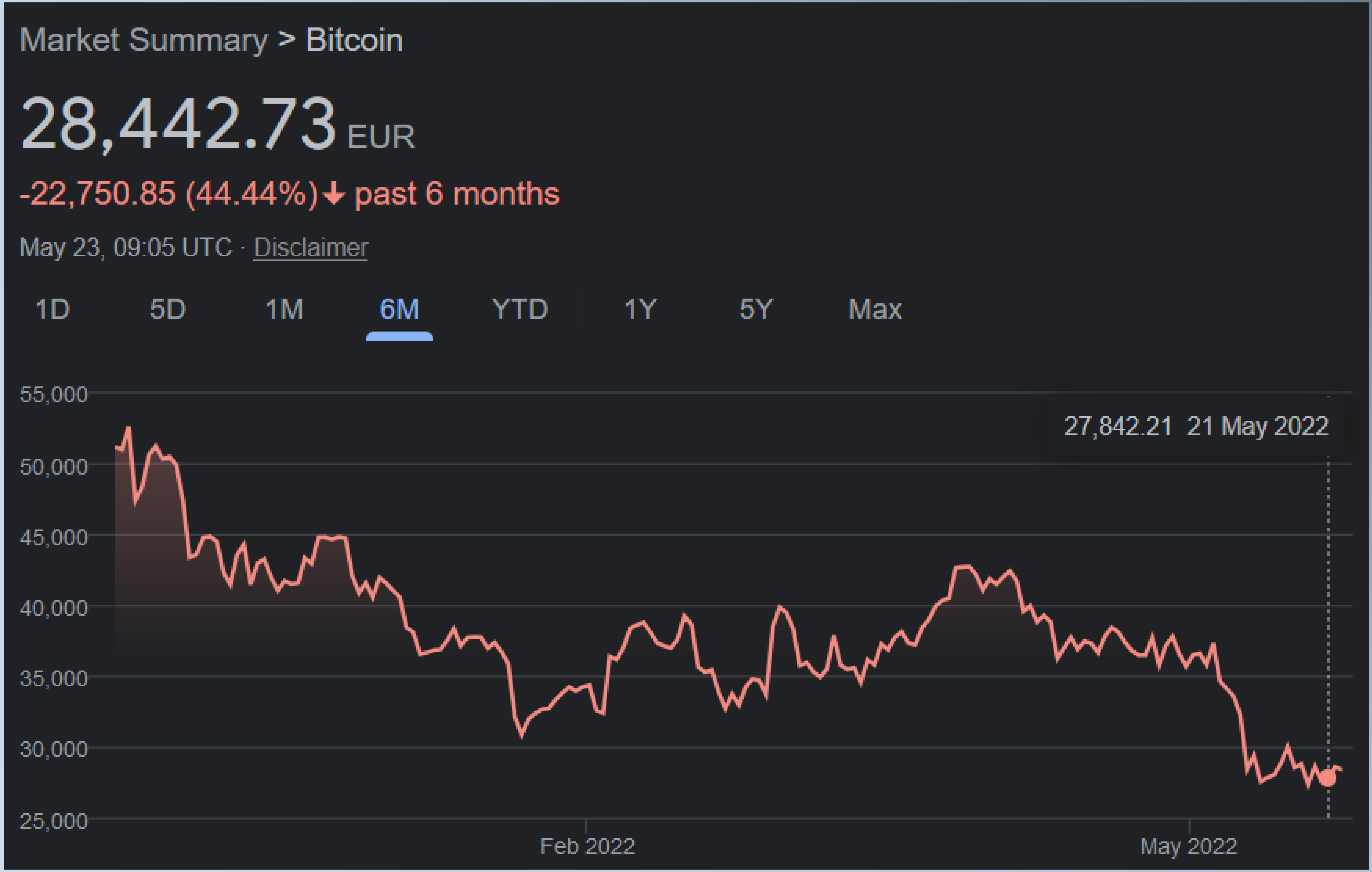
2. Bitcoin

FIAT	BITCOIN
Unlimited reserve of value. More can be printed at any time.	**Limited** value reserve. There is a maximum limit of 21 million Bitcoins in the world.
Currency value **influenced by the interests of specific Stakeholders** – Governments and Banks (there are **privileged customers**).	Democratic currency – Nobody has absolute control. **All stakeholders are equal**.
Expensive transfers that require a third party to process them: Banks.	**Low-cost, direct** person-to-person transfers (without intermediaries).
Slow and bureaucratic **transfer process**. 48 hours or more for international transfers. Only 5 days a week.	**Instant transfers** – speed of the Blockchain network that processes them 24/7.

2. Bitcoin

- There are 3 ways to acquire Bitcoins:
  - **Buying Bitcoins** through an Exchange (ex: Coinbase, Binance, Webull or eToro, etc.).
  - **Accepting Bitcoins** in the Sale of Products and Services
  - **Mining Bitcoins** (implies investment in Hardware and energy, for Mathematical processing called "Proof of Work")



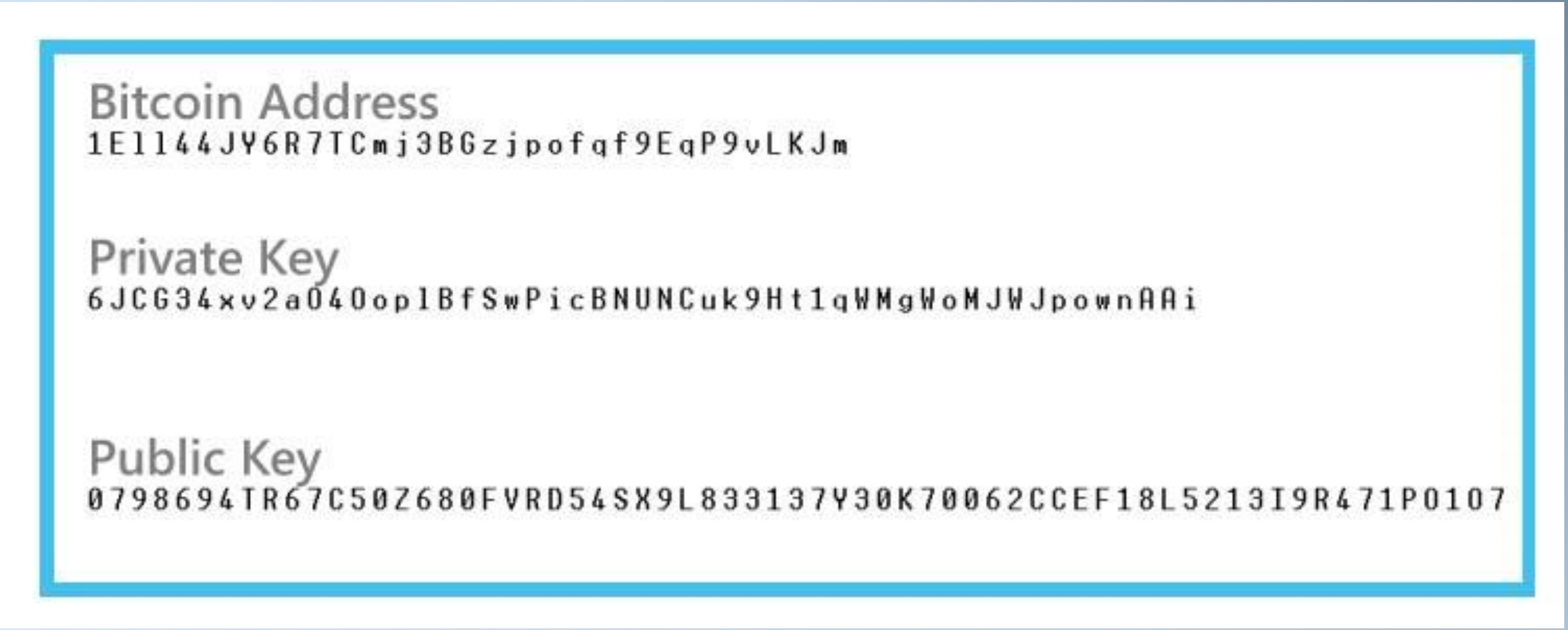

Market Summary > Bitcoin

28,442.73 EUR

-22,750.85 (44.44%)↓ past 6 months

May 23, 09:05 UTC · Disclaimer

2. Bitcoin



Bitcoin Address

1E1144JY6R7TCmj3BGzjpofqf9EqP9vLKJm

Private Key

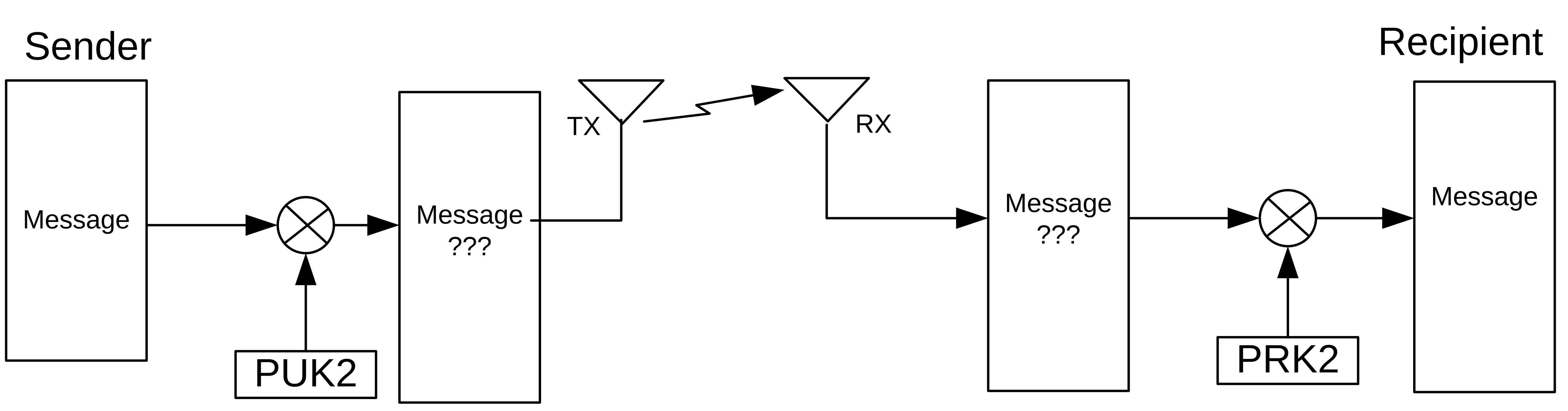
6JCG34xv2a040op1BfSwPicBNUNCuk9Ht1qWMgWoMJWJpownAAi

Public Key

0798694TR67C50Z680FVRD54SX9L833137Y30K70062CCEF18L5213I9R471P0107

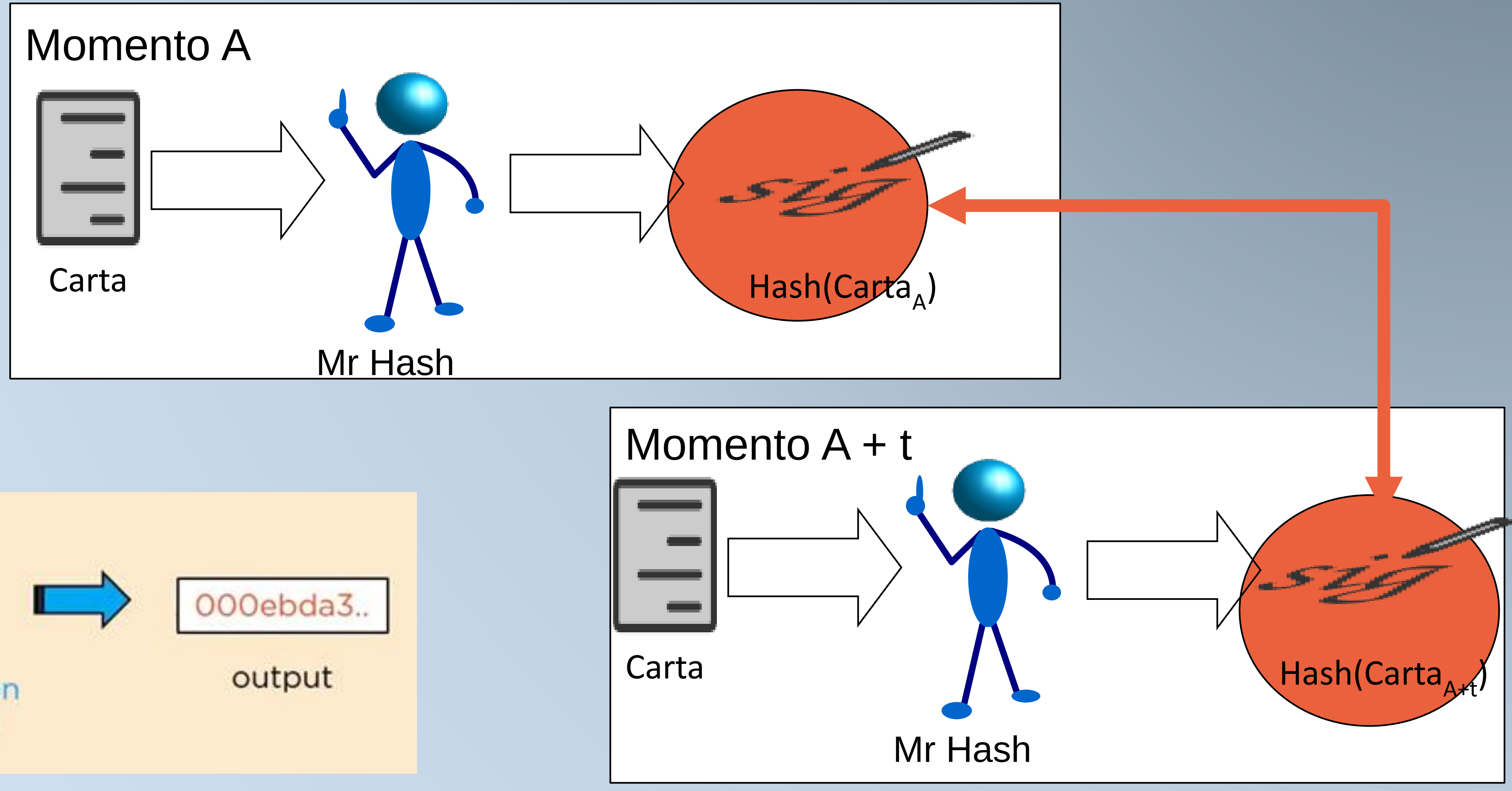
2. Bitcoin

- Symmetric encryption (same key to encrypt and decrypt) has vulnerabilities associated with its prior distribution
- In asymmetric encryption: The confidentiality of the private key must be ensured, that is, it must be kept secret by its legitimate user.
  - The public key is freely distributed to all users.



2. Bitcoin

- Hash function is used as “signature”
- A cryptographic function that performs a checksum
- Bitcoin Blockchain uses SHA-256, generating 256-bits from any string
- One-way function: From Hash sum it is impossible to get the block of data.
- **But what if a Hacker accesses the content and its Hash, modifying both?**
    - Solution?



Momento A

Carta

Mr Hash

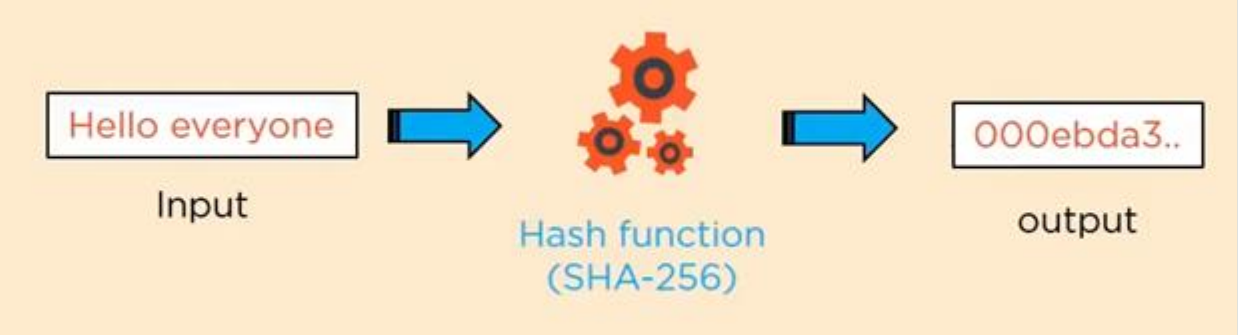
$\text{Hash}(\text{Carta}_{A})$

Momento A + t

Carta

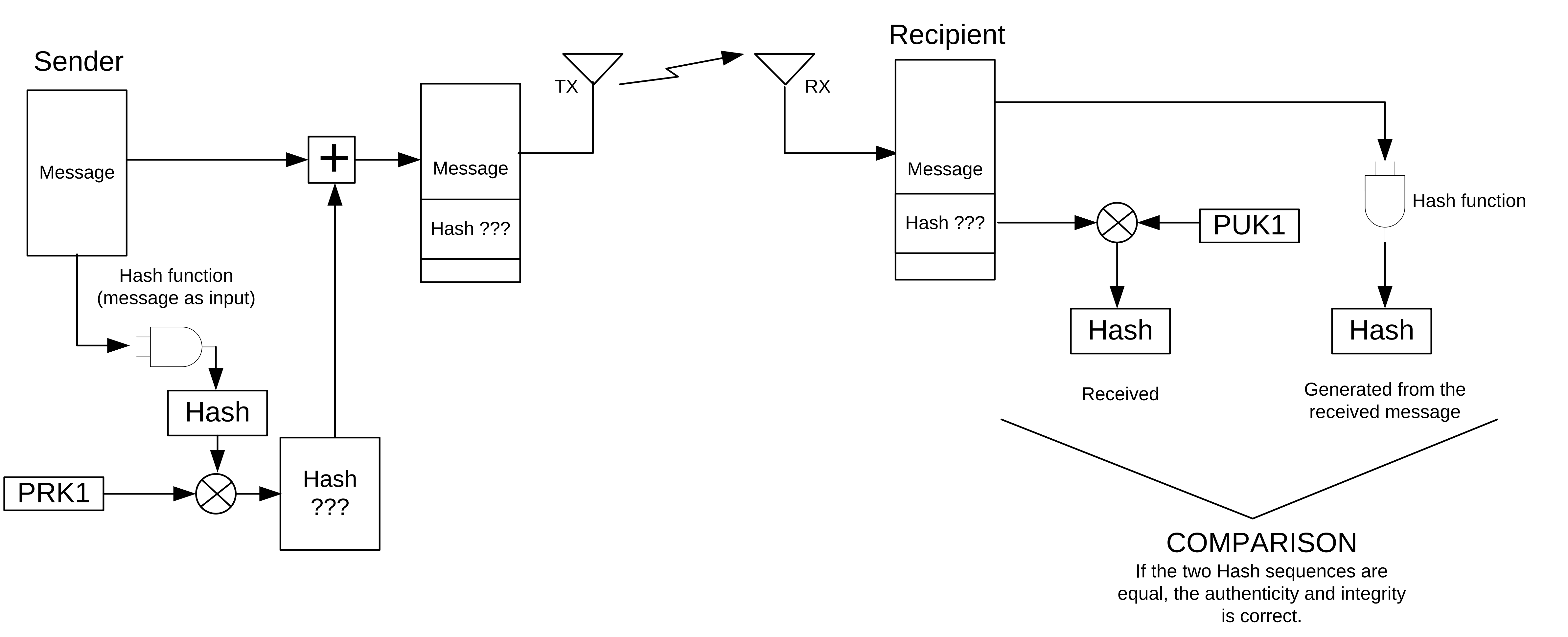
Mr Hash

$\text{Hash}(\text{Carta}_{A+t})$



2. Bitcoin

Blockchain also uses **Digital Signature** to verify the **integrity**, **authenticity** and to avoid **non-repudiation** of data.

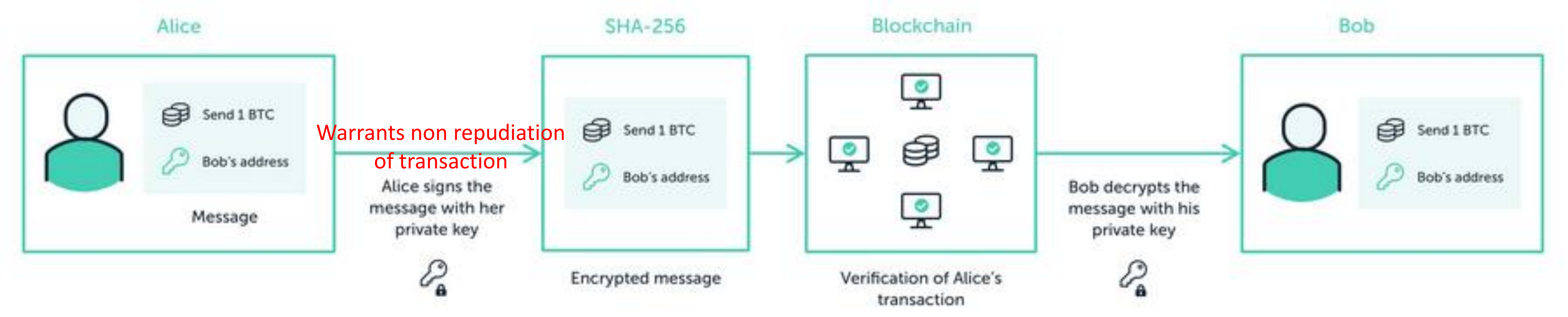


COMPARISON

If the two Hash sequences are equal, the authenticity and integrity is correct.

2. Bitcoin

- To perform a transaction, 3 elements are invoked:
  - Transaction sender's Private Key (stored in Wallet)
  - Public key of the recipient of the transaction (as if it were the recipient's IBAN)
  - The transaction amount
  - Still exists:
    - The **Bitcoin Address**: Corresponds to a shortened version of the Public Key but cannot be generated from it.
    - 12 Word Phrase (Seed Phrase): Allows retrieval of Wallet Private Key and Bitcoin Address. Allows recovery of access to funds even in the event of losing access to the original Wallet.
- The Private Key, 12-word phrase, and the Password to access the Wallet must be kept (paper). If you lose, the cryptocurrencies are lost.


Alice
Send 1 BTC
Bob's address
Message
Warrants non repudiation of transaction
Alice signs the message with her private key
SHA-256
Send 1 BTC
Bob's address
Encrypted message
Blockchain
Verification of Alice's transaction
Bob decrypts the message with his private key
Bob
Send 1 BTC
Bob's address

Agenda

1. Introduction

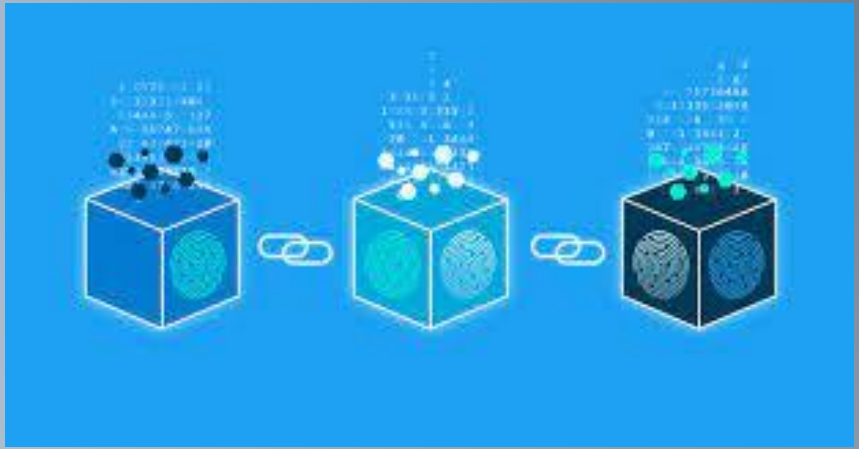
2. Bitcoin

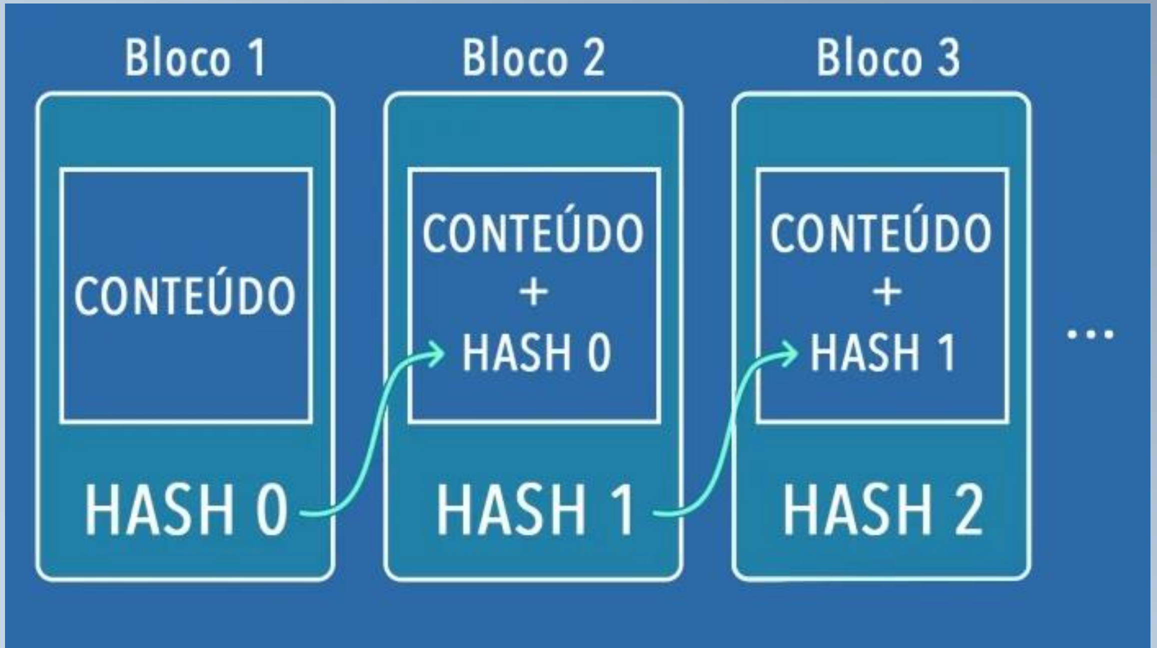
3. **Blockchain**

4. Mining

3. Blockchain

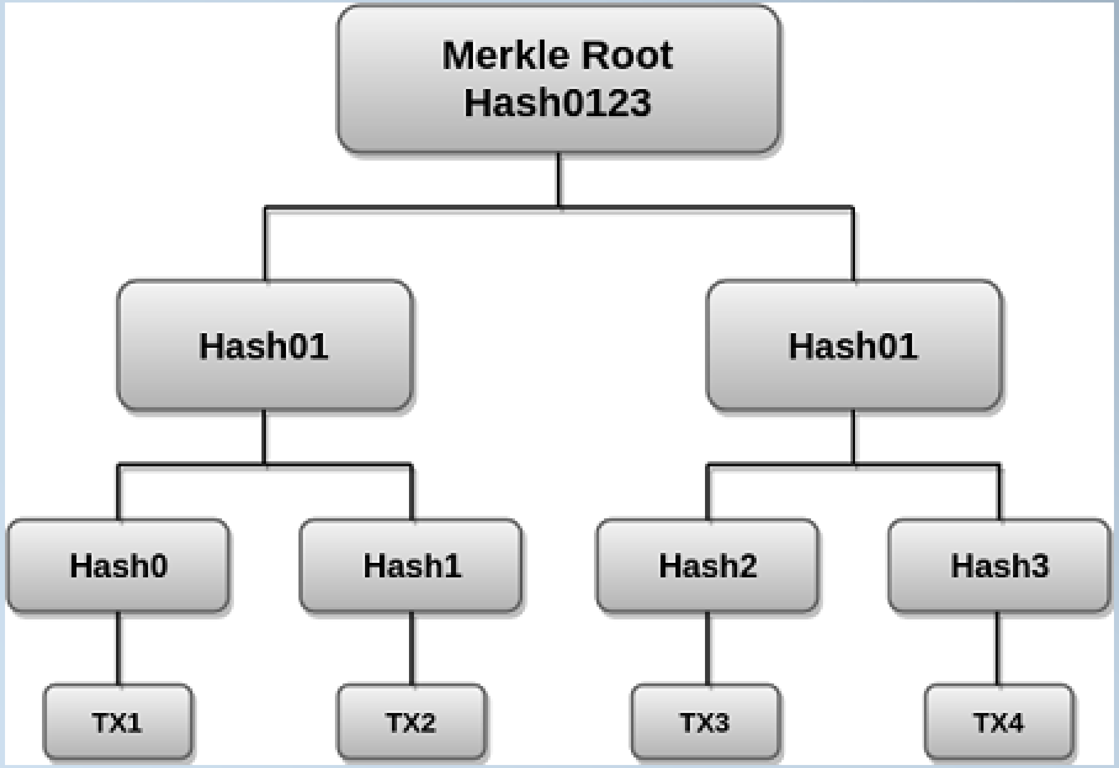
- Chain of Blocks
  - **Secure** and **Decentralized** (peer-to-peer, rather than centralized on a bank's central computer - server)
- Blockchain is an event **registration/recording system**, with applications in various sectors, not being specific to Cryptocurrencies
- **Secure infrastructure that allows all events, data, and documents to be digitally stored, with integrity, authenticity, and without the possibility of non-repudiation (digitally signed).**
- Each block stores details about a set of **transactions carried out in the last 10 minutes** (approx.), with the origin, destination, value, and "timestamp"
- Contains the Distributed Ledger (i.e., events logbook): Distributed database where digital currency **transactions are recorded in chronological order**
- **Mining**: consists of **processing/validating each block**, done in a **decentralized** way (instead of being done by a centralized server)





3. Blockchain

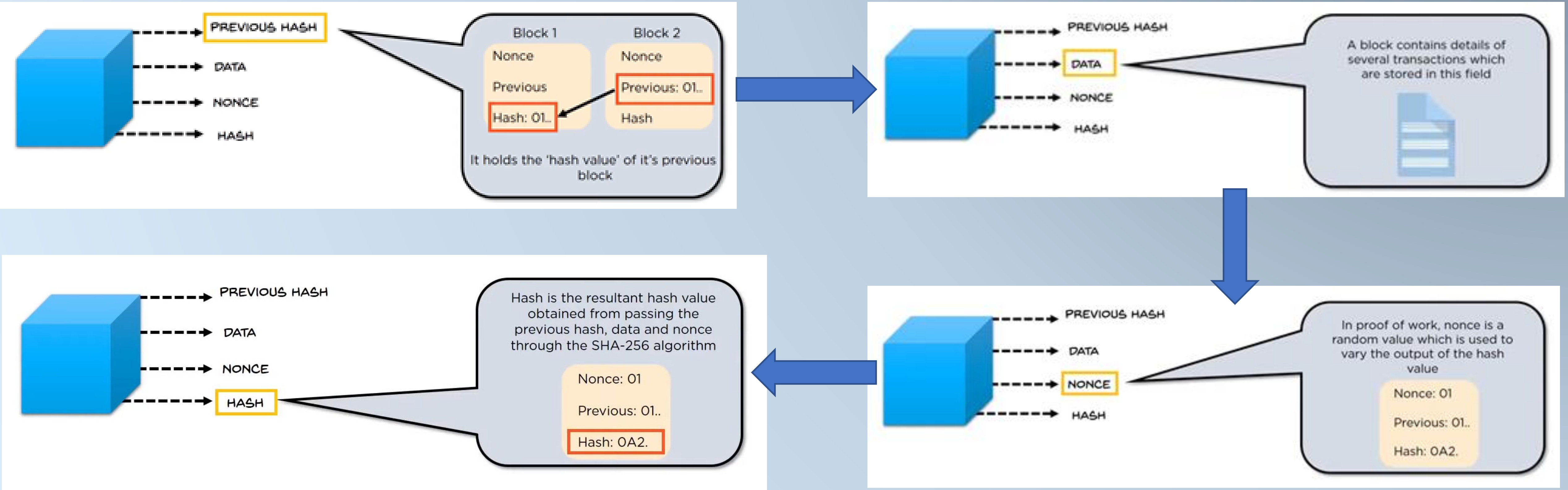
- Merkle Tree aims to verify individual transactions on the network.
- In the Merkle Tree, the **Hashes of individual transactions**, known as **Transaction IDs**, are grouped repeatedly using the SHA-256 algorithm, until a Hash identifies the entire tree.
- This **last Hash is known as Merkle Root** or Root Hash. The Merkle Root, the Merkle Tree identifier, is **part of the block header**.



3. Blockchain

Blockchain is a chain of blocks. **Each block has 4 fields**:

- **Data**: The set of transactions included in this block (last 10 minutes) – after being mined and validated, they are included in the block.
- **Hash**: It is the Hash Sum value, obtained by passing the fields of the “Previous Hash”, “Data” & “Nonce” block through the SHA-256 algorithm, corresponding to the digital signature of the block.
- **Previous hash**: Hash value of the previous block. This way, the blocks are interconnected, avoiding fraud, and **creating the CHAIN OF BLOCKS**.
- **Nonce**: Corresponds to a random value used to vary the Hash Sum output.
    - In the “proof of work” validation algorithm (verification of the transaction in the block), performed during Mining, this **random value is validated** so that the **Hash Sum is less than a certain value**.



It holds the ‘hash value’ of it’s previous block

A block contains details of several transactions which are stored in this field

In proof of work, nonce is a random value which is used to vary the output of the hash value

Hash is the resultant hash value obtained from passing the previous hash, data and nonce through the SHA-256 algorithm

3. Blockchain

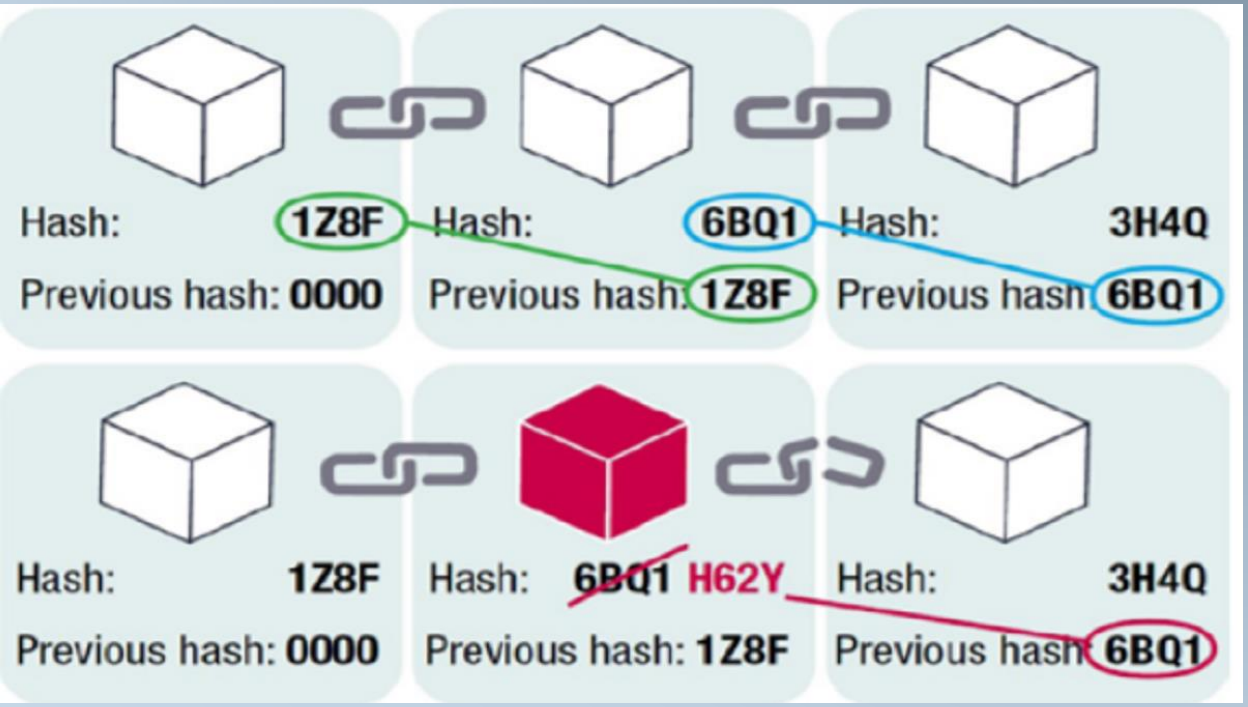
- Blockchain was not created with BTC but rather, in 1991, in order to have **data organized in a sequential way to prevent alteration of documents or events, or modification of data**.
- In the context of Bitcoin, Blockchain was adapted by Satoshi Nakamoto (2009) to function as a "Distributed Ledger".
- With blockchain, **everything you do is recorded**. Hence, it is possible to make all types of contracts without the possibility of **non-repudiation** (smart contracts). It **opens up disruptive prospects for the future**.
- Blockchain can be **used in the business world** (e.g., **insurance** or **aviation** to allow **audits** to be carried out after an accident to determine its causes)
- **Reliable Electronic Voting** must be implemented using Blockchain.
- It is anticipated that **Web 3.0 will be based on Blockchain** Technology, due to its **Decentralized and Trusted approach** (as opposed to Server Oriented approach)
- Blockchain has advantages in terms of protection from computer attacks. It is secure (encryption), distributed and identifies what was done, when and by whom.

Corporations are still only just figuring out the potential applications of blockchain technology, but its use is already growing more quickly than anyone could have predicted

(Lex Sokolin, head economist for Consensys)

3. Blockchain

- For a Hacker to change a block, he would have to change the Hash value of all the following blocks, which would require a very high processing power (close to impossible), and which would have to be validated by more than half of the network computers.
  - Blockchain is resistant to data modification (no one has succeeded, until today).



Agenda

1. Introduction

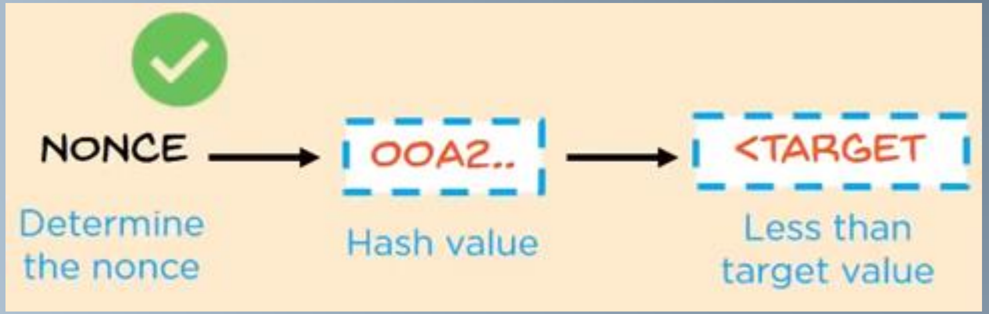
2. Bitcoin

3. Blockchain

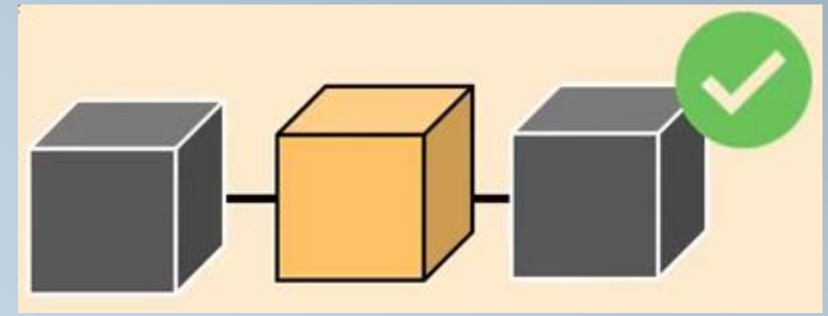
4. Mining

4. Mining

- **Mining is validation processing called Proof-of-Work** (PoW). It is through PoW that cryptocurrency transactions are digitally validated and added to the “blockchain ledger” (record of all transactions on the network).
- **PoW**: is performed through a **puzzle, which consists of the calculation of successive Hash functions** (encryption), used to verify the block transactions that are updated in the “Distributed Ledger” network.
- The **computer protection of PoW** (decentralized versus Server) lies in the **validation difficulty associated with Mining** and in the approval of more than half of the network users.
  - If processing were easy, modifying the data would also be easier
- This processing requires Great Processing Power.
- As a reward, the miner(s) receive 6.25 BTC (started at 50 BTC), after finding the solution (first to go).
- This mathematical process must be carried out in a maximum time of 10 minutes.
- The reward is halved every 210,000 blocks (approximately 4 years).
- In this way, **the number of BTC in circulation increases up to the limit of 21 Million**.
  - In the end, miners will only be rewarded through transaction costs.

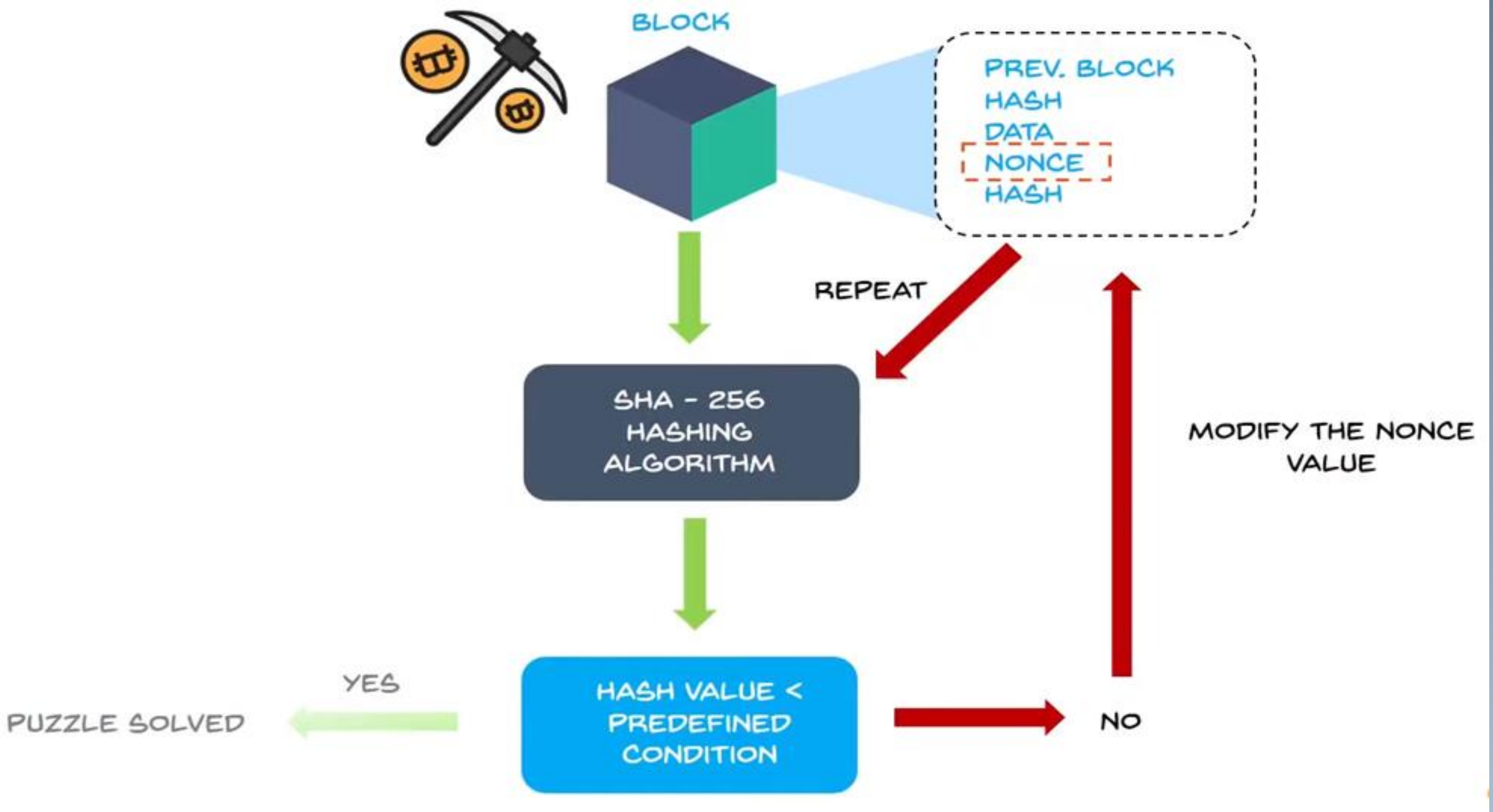


The puzzle is solved by varying a nonce which produces a hash value lower than a predefined condition

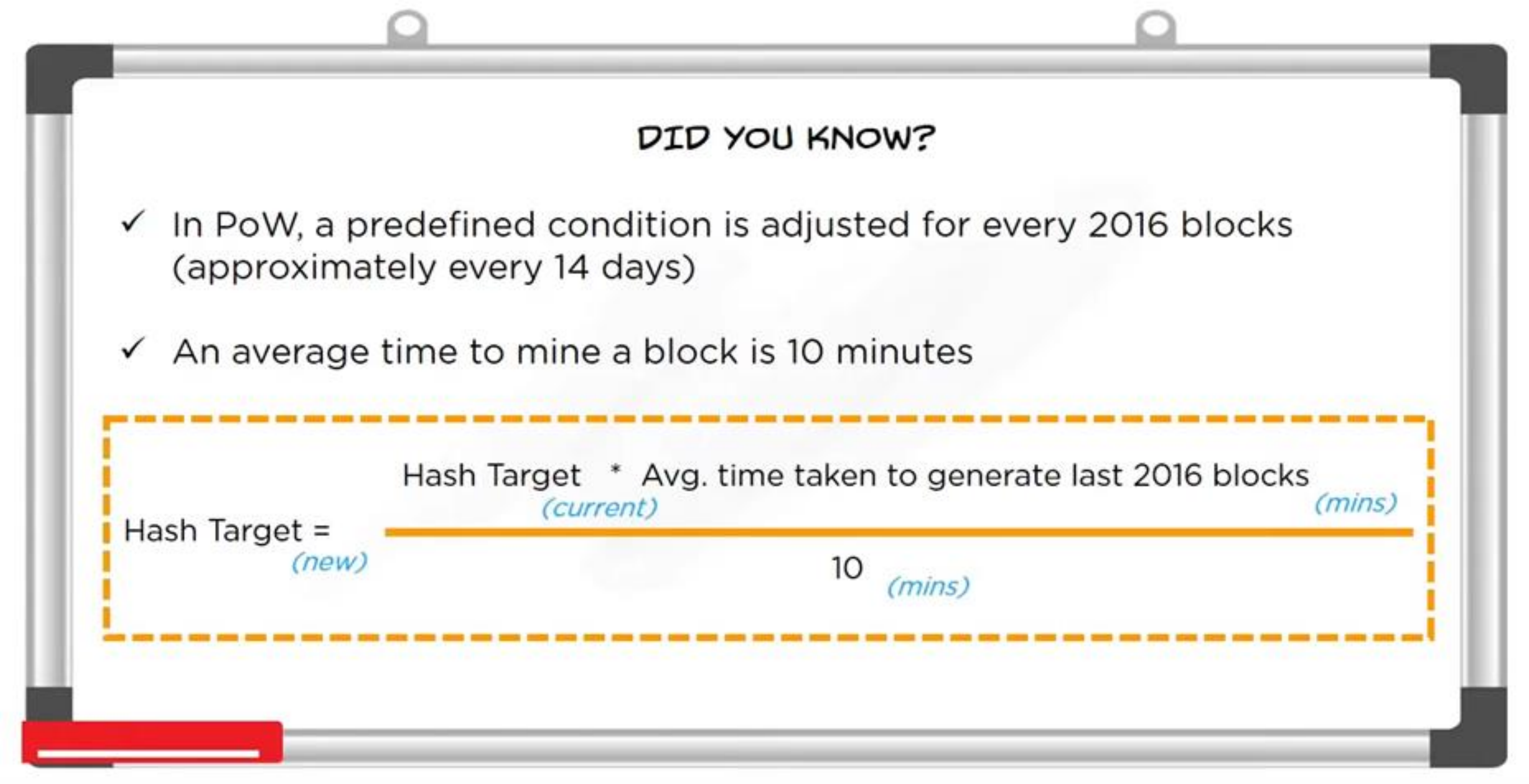


4. Mining

- The "predefined condition", or "Hash Target", is found in the header, being expressed as a 67-digit number that determines the Mining difficulty.
- This difficulty is calculated based on the number of miners competing to find the Hash function, being adjusted every 2016 blocks (based on the time it took previous miners to solve the equation).
- The "predefined condition" aims to keep the block validation to a maximum of 10 minutes.



4. Mining

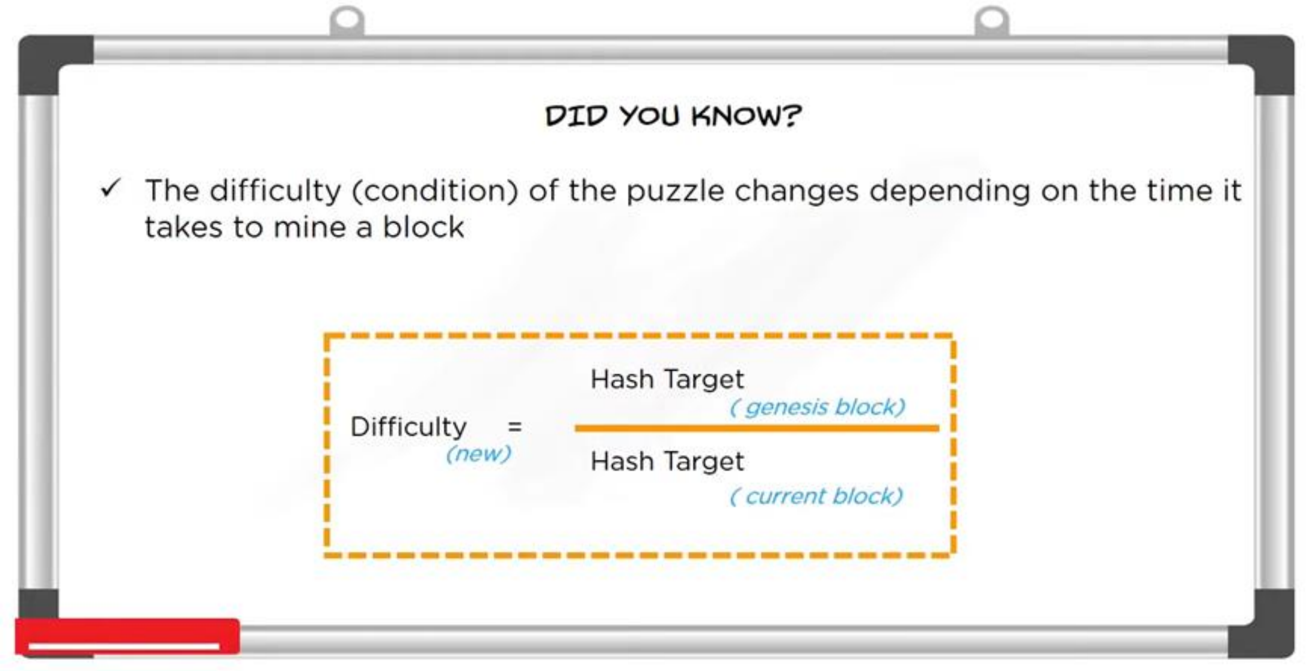


DID YOU KNOW?

- ✓ In PoW, a predefined condition is adjusted for every 2016 blocks (approximately every 14 days)
- ✓ An average time to mine a block is 10 minutes

$$\underset{(new)}{\text{Hash Target}} = \frac{\underset{(current)}{\text{Hash Target}} \; * \; \underset{(mins)}{\text{Avg. time taken to generate last 2016 blocks}}}{\underset{(mins)}{10}}$$

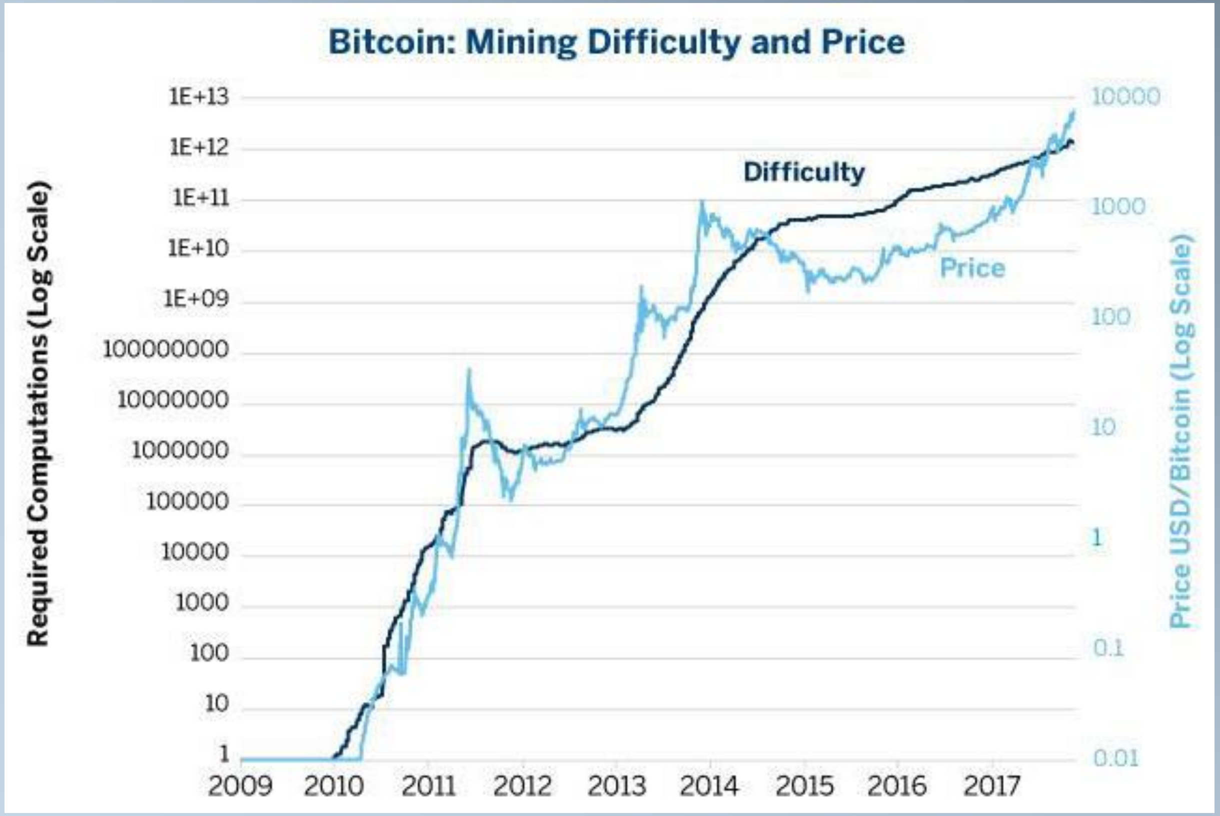
4. Mining



DID YOU KNOW?

- ✓ The difficulty (condition) of the puzzle changes depending on the time it takes to mine a block

$$\underset{(new)}{\text{Difficulty}} = \frac{\text{Hash Target } _{(\textit{genesis block})}}{\text{Hash Target } _{(\textit{current block})}}$$



Bitcoin: Mining Difficulty and Price

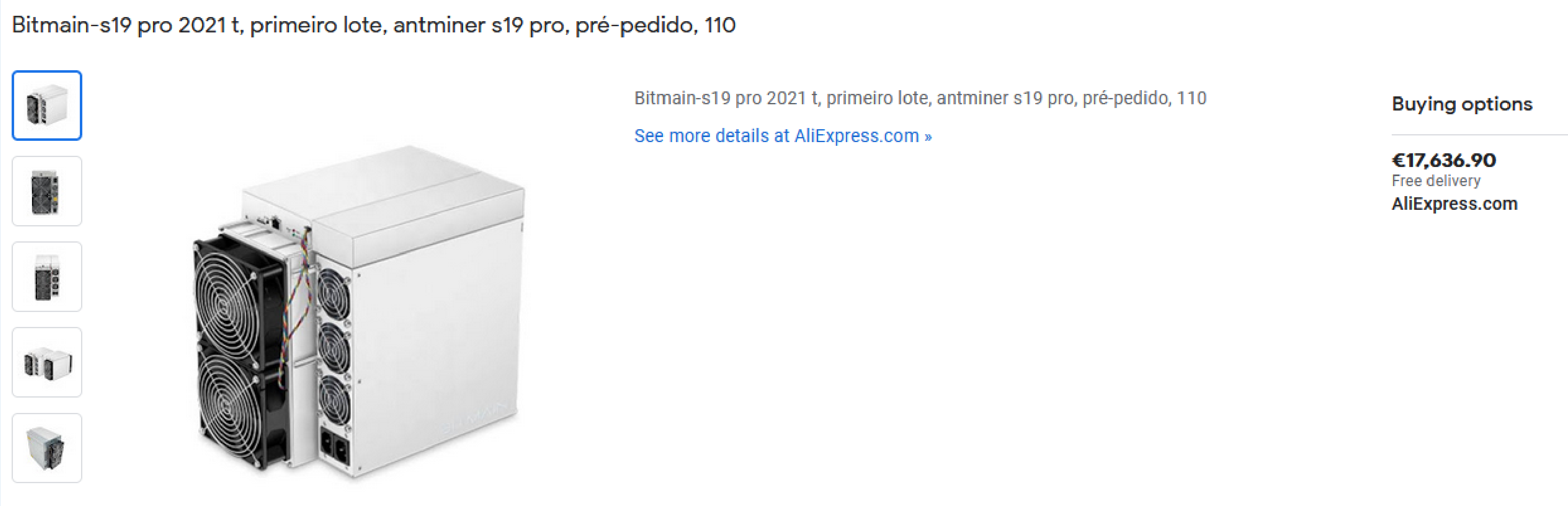
4. Mining

- Initially, mining was performed with CPUs. As the difficulty level increased, the CPUs became inefficient.
- They started using GPUs (faster).
- However, **energy consumption** has increased (became exaggerated).

- **Solution: use ASIC (Application Specific Integrated Circuit)**. They are "chips" designed for specific functions, instead of "Multi-Purpose", so they are much more efficient (**consumes less power and are faster for Mining**) -> But a lot of **Noise** and **Heating** (choose the appropriate location for ASIC).
  - This solution allowed Mining to be profitable.
- Mining a block (many transactions carried out in about 10 minutes) costs about 200 Euros of Electricity.
- To mine, you still need **Software** (ECOS, BeMine, or Kryptex Miner) and a **Wallet**.

4. Mining

Antminer S19 Pro	M30 S++	Antminer T19
Manufacturer: Bitmain	MicroBT	Bitmain
Hashrate: 110 TH/s [TH/s - trillions Hash per second]	Hashrate: 112 TH/s	Hashrate: 84 TH/s
Energy Consumption: 3250 W	3472 W	3150 W



Bitmain-s19 pro 2021 t, primeiro lote, antminer s19 pro, pré-pedido, 110

Bitmain-s19 pro 2021 t, primeiro lote, antminer s19 pro, pré-pedido, 110

See more details at AliExpress.com »

Buying options

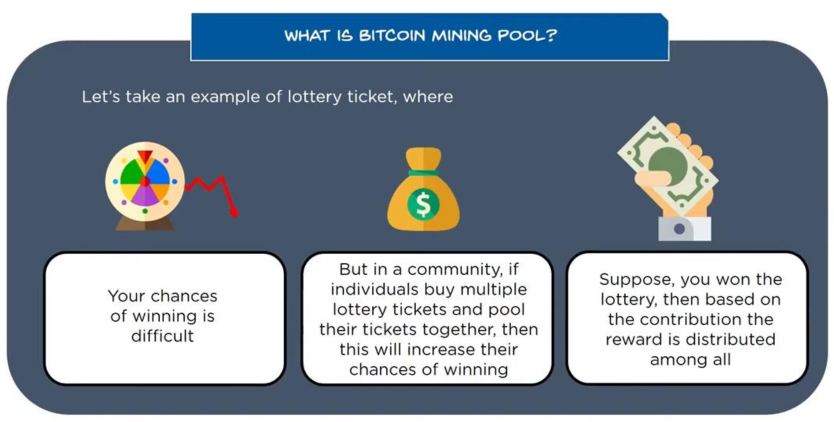
€17,636.90

Free delivery

AliExpress.com

4. Mining

- Mining can be done in 2 ways:
  - Individually. The probability of success, i.e., of being able to perform the Proof of Work in a maximum of 10 minutes, is reduced. In addition, it requires a lot of processing power.



WHAT IS BITCOIN MINING POOL?

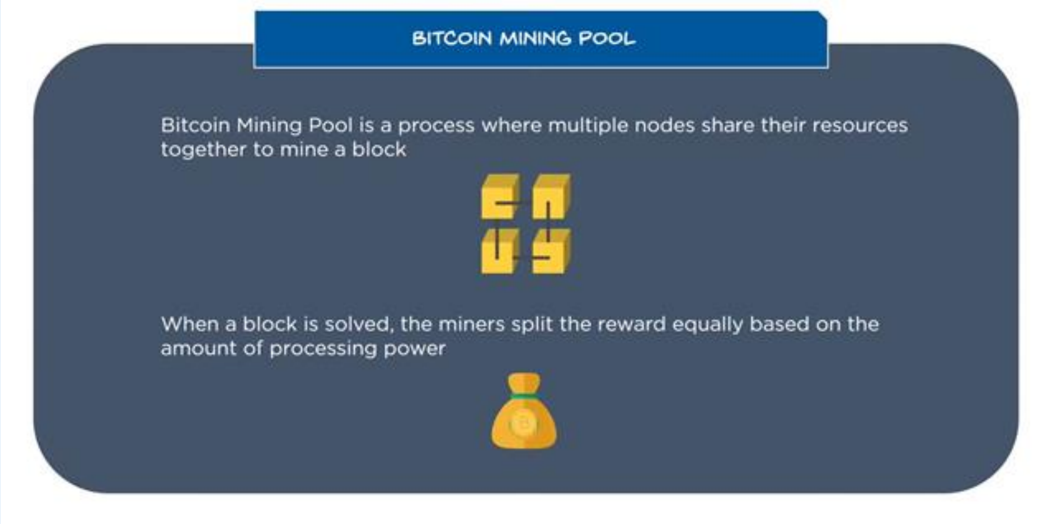
Let's take an example of lottery ticket, where

Your chances of winning is difficult

But in a community, if individuals buy multiple lottery tickets and pool their tickets together, then this will increase their chances of winning

Suppose, you won the lottery, then based on the contribution the reward is distributed among all

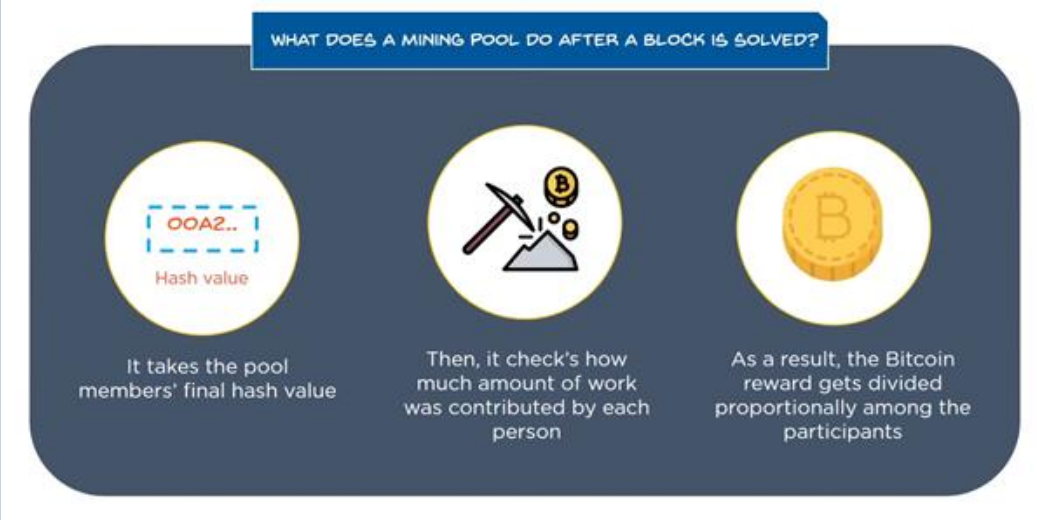
  - In Pool (group): Increases the probability of success, using Distributed Computing.



BITCOIN MINING POOL

Bitcoin Mining Pool is a process where multiple nodes share their resources together to mine a block

When a block is solved, the miners split the reward equally based on the amount of processing power



WHAT DOES A MINING POOL DO AFTER A BLOCK IS SOLVED?

It takes the pool members' final hash value

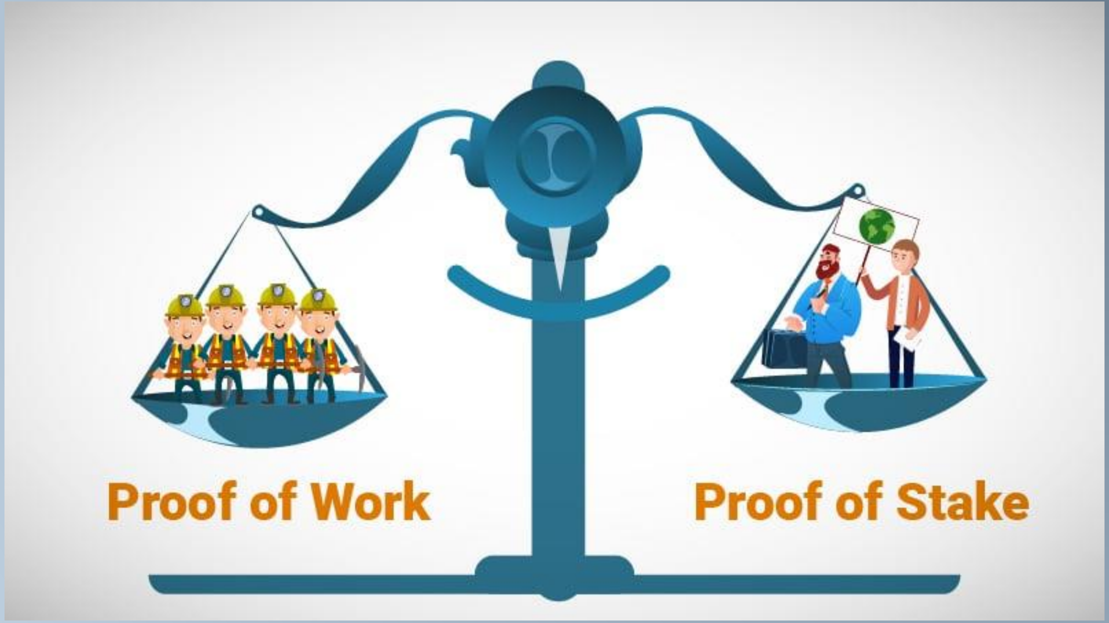
Then, it check's how much amount of work was contributed by each person

As a result, the Bitcoin reward gets divided proportionally among the participants

4. Mining

Alternative to PoW (mining): Proof of Stake (PoS):

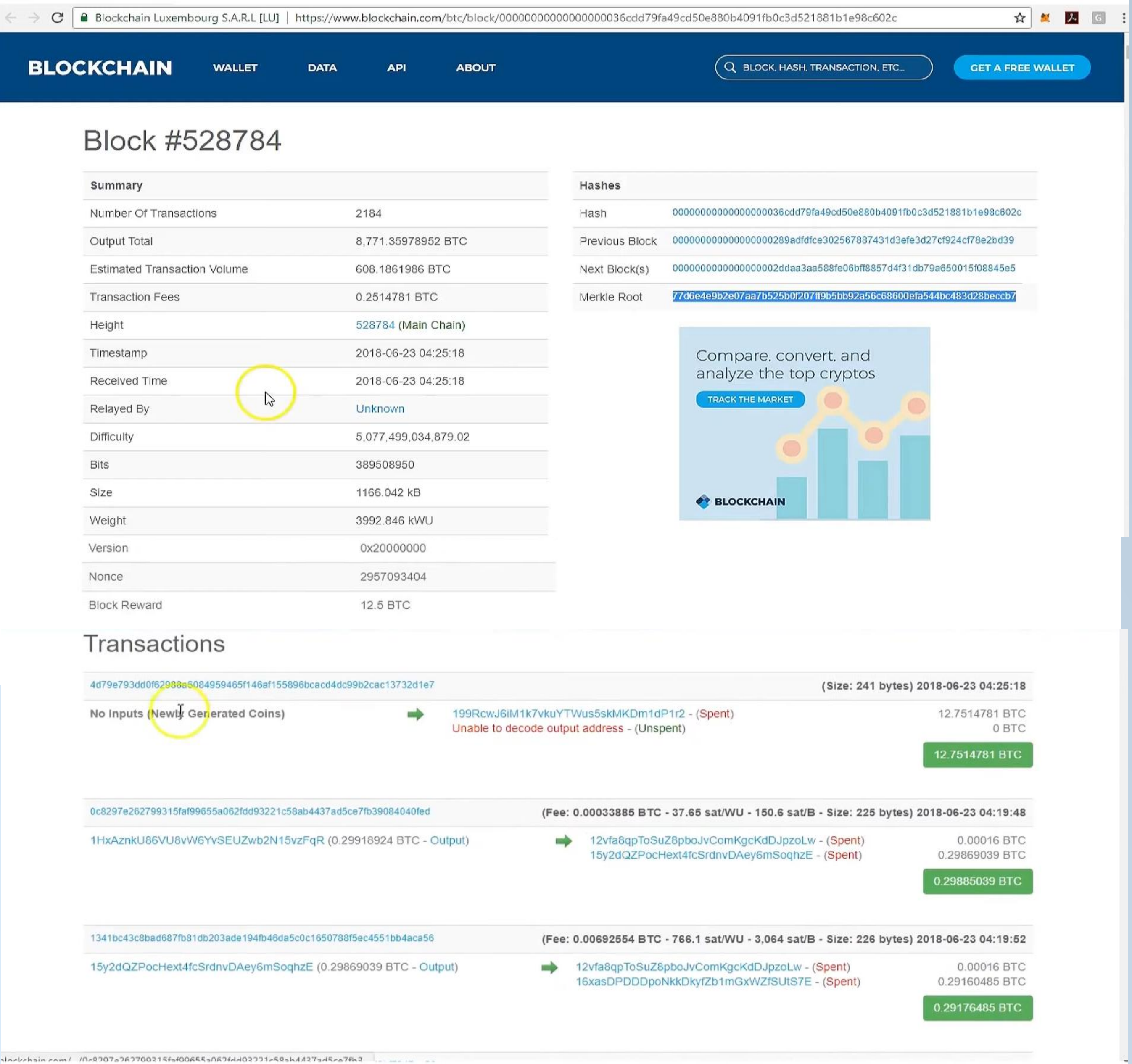
- In order to make **validation more efficient and cheaper (avoiding extensive electrical consumption)**, several currencies (eg **Ethereum**) are **migrating from Proof of Work to Proof of Stake**.
- They are **machines (software) selected at random to work as validators of the blocks of transactions** on the network, interconnecting the various blocks of the Blockchain.
- PoS consists of a validation process of a block, whose responsible is determined by the PoS algorithm.
  - At the very least, voting shares must be distributed properly to avoid becoming a



Alternative to PoW (mining): Proof of Stake Authority (PoA):

- PoA: Transactions and blocks are **validated by authorized accounts, known as validators (supernodes with special privileges)**. Validators run software to allow the block of transactions. The process is **automated by the software** without human intervention.
- In PoA, individuals earn the right to become validators, so there is an incentive to maintain the position they have earned. By assigning a reputation to the identity, validators are encouraged to maintain the transaction process as they do not want to have their identities associated with a negative reputation. This is considered more robust than PoS (proof of stake).
  - It has the inconvenience of **being able to have an agreement between Stakeholders acting as PoA, approaching the centralized system.**
  - In **PoS the validators are all the same** (selected randomly). In the **PoA they are users with additional privileges**.

A block of a blockchain



Blockchain Luxembourg S.A.R.L [LU] | https://www.blockchain.com/btc/block/00000000000000000036cdd79fa49cd50e880b4091fb0c3d521881b1e98c602c
BLOCKCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE WALLET

Block #528784

Summary	
Number Of Transactions	2184
Output Total	8,771.35978952 BTC
Estimated Transaction Volume	608.1861986 BTC
Transaction Fees	0.2514781 BTC
Height	528784 (Main Chain)
Timestamp	2018-06-23 04:25:18
Received Time	2018-06-23 04:25:18
Relayed By	Unknown
Difficulty	5,077,499,034,879.02
Bits	389508950
Size	1166.042 kB
Weight	3992.846 kWU
Version	0x20000000
Nonce	2957093404
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000036cdd79fa49cd50e880b4091fb0c3d521881b1e98c602c
Previous Block	00000000000000000289adfdfce302567887431d3efe3d27cf924cf78e2bd39
Next Block(s)	0000000000000000002ddaa3aa588fe06bff8857d4f31db79a650015f08845e5
Merkle Root	77d6e4e9b2e07aa7b525b0f207ff9b5bb92a56c68600efa544bc483d28beccb7

Transactions

4d79e793dd0f62988a6084959465f146af155896bcacd4dc99b2cac13732d1e7 (Size: 241 bytes) 2018-06-23 04:25:18

No Inputs (Newly Generated Coins) → 199RcwJ6iM1k7vkuYTWus5skMKDm1dP1r2 - (Spent) 12.7514781 BTC
Unable to decode output address - (Unspent) 0 BTC
12.7514781 BTC

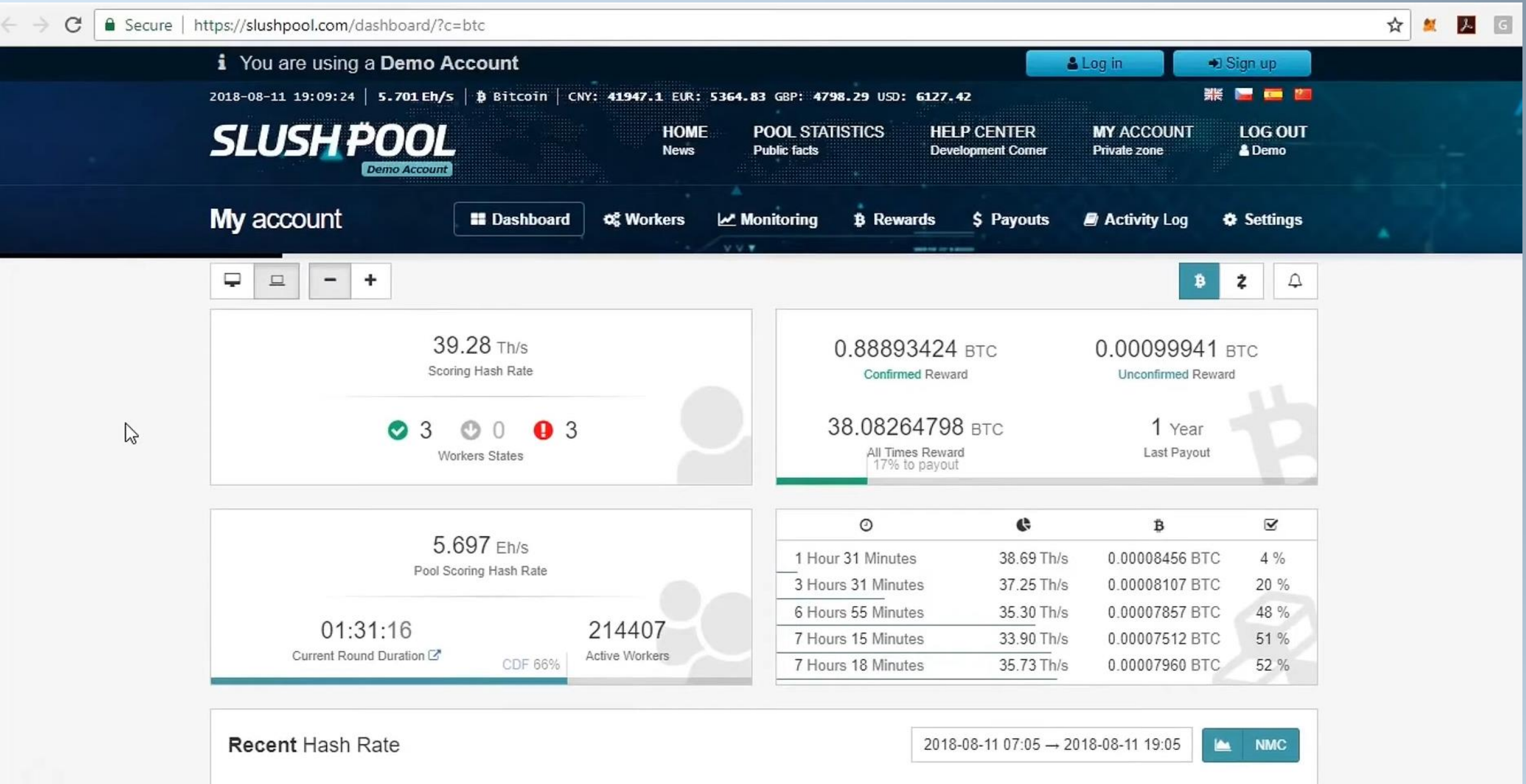
0c8297e262799315faf99655a062fdd93221c58ab4437ad5ce7fb39084040fed (Fee: 0.00033885 BTC - 37.65 sat/WU - 150.6 sat/B - Size: 225 bytes) 2018-06-23 04:19:48

1HxAznkU86VU8vW6YvSEUZwb2N15vzFqR (0.29918924 BTC - Output) → 12vfa8qpToSuZ8pboJvComKgcKdDJpzoLw - (Spent) 0.00016 BTC
15y2dQZPocHext4fcSrdnvDAey6mSoqhzE - (Spent) 0.29869039 BTC
0.29885039 BTC

1341bc43c8bad687fb81db203ade194fb46da5c0c1650788f5ec4551bb4aca56 (Fee: 0.00692554 BTC - 766.1 sat/WU - 3,064 sat/B - Size: 226 bytes) 2018-06-23 04:19:52

15y2dQZPocHext4fcSrdnvDAey6mSoqhzE (0.29869039 BTC - Output) → 12vfa8qpToSuZ8pboJvComKgcKdDJpzoLw - (Spent) 0.00016 BTC
16xasDPDDDpoNkkDkyfZb1mGxWZfSUtS7E - (Spent) 0.29160485 BTC
0.29176485 BTC

- Mining Pool



You are using a **Demo Account**

2018-08-11 19:09:24 | 5.701 Eh/s | ₿ Bitcoin | CNY: 41947.1 EUR: 5364.83 GBP: 4798.29 USD: 6127.42

39.28 Th/s
Scoring Hash Rate

✓ 3 ⊙ 0 ❗ 3
Workers States

0.88893424 BTC
Confirmed Reward

0.00099941 BTC
Unconfirmed Reward

38.08264798 BTC
All Times Reward
17% to payout

1 Year
Last Payout

5.697 Eh/s
Pool Scoring Hash Rate

01:31:16
Current Round Duration

CDF 66%

214407
Active Workers

⊙	◔	₿	☑
1 Hour 31 Minutes	38.69 Th/s	0.00008456 BTC	4 %
3 Hours 31 Minutes	37.25 Th/s	0.00008107 BTC	20 %
6 Hours 55 Minutes	35.30 Th/s	0.00007857 BTC	48 %
7 Hours 15 Minutes	33.90 Th/s	0.00007512 BTC	51 %
7 Hours 18 Minutes	35.73 Th/s	0.00007960 BTC	52 %

Recent Hash Rate

2018-08-11 07:05 → 2018-08-11 19:05

Agenda

1. Introduction

2. Bitcoin

3. Blockchain

4. Mining

THANK YOU