Subject A. Blockchain fundamentals – Blockchain architecture and principles.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

1.BLOCKCHAIN IN A NUTSHELL

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

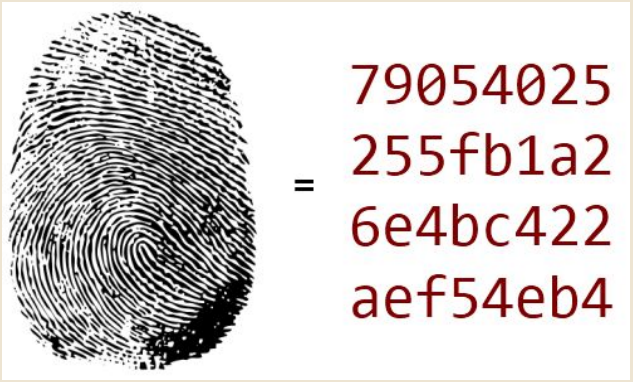
1. Blockchain in a nutshell

"an ever-growing list of records, called blocks, that are linked and protected using cryptography“

Fundamentals: Blocks and hash

A block is a record that has data inside. Two values correspond to each block: the so-called **previous hash** and the **hash**.

Digital hash: the fingerprint of the block that makes it much clearer. Data and the previous hash are represented, encrypted, in a number. This shortened version of the data is specifically sixty-four characters in length.



TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

1. Blockchain in a nutshell

What is Blockchain?

Blockchain is a shared, immutable **ledger** that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

1. Blockchain in a nutshell

Blockchain is important because business runs on information. The faster it's received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members.

https://hbr.org/sponsored/2017/10/how-blockchain-will-accelerate-business-performance-and-power-the-smart-economy

A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Key Elements of a Blockchain

- Distributed ledger technology
- Immutable records
- Smart contracts

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Key Elements of a Blockchain

Distributed ledger technology

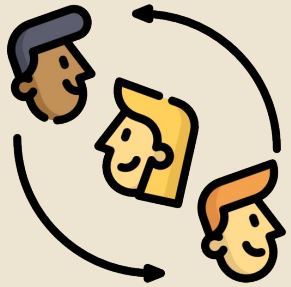
The distributed ledger and its immutable record of transactions are accessible to all network members. Transactions are only recorded once using this shared ledger, reducing the duplication of effort that is common in traditional corporate networks.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Key Elements of a Blockchain



Immutable records

After a transaction has been logged to the shared ledger, no participant may modify or tamper with it. If a mistake is found in a transaction record, a new transaction must be recorded to correct the problem, and both transactions must then be accessible.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Key Elements of a Blockchain

Smart contracts

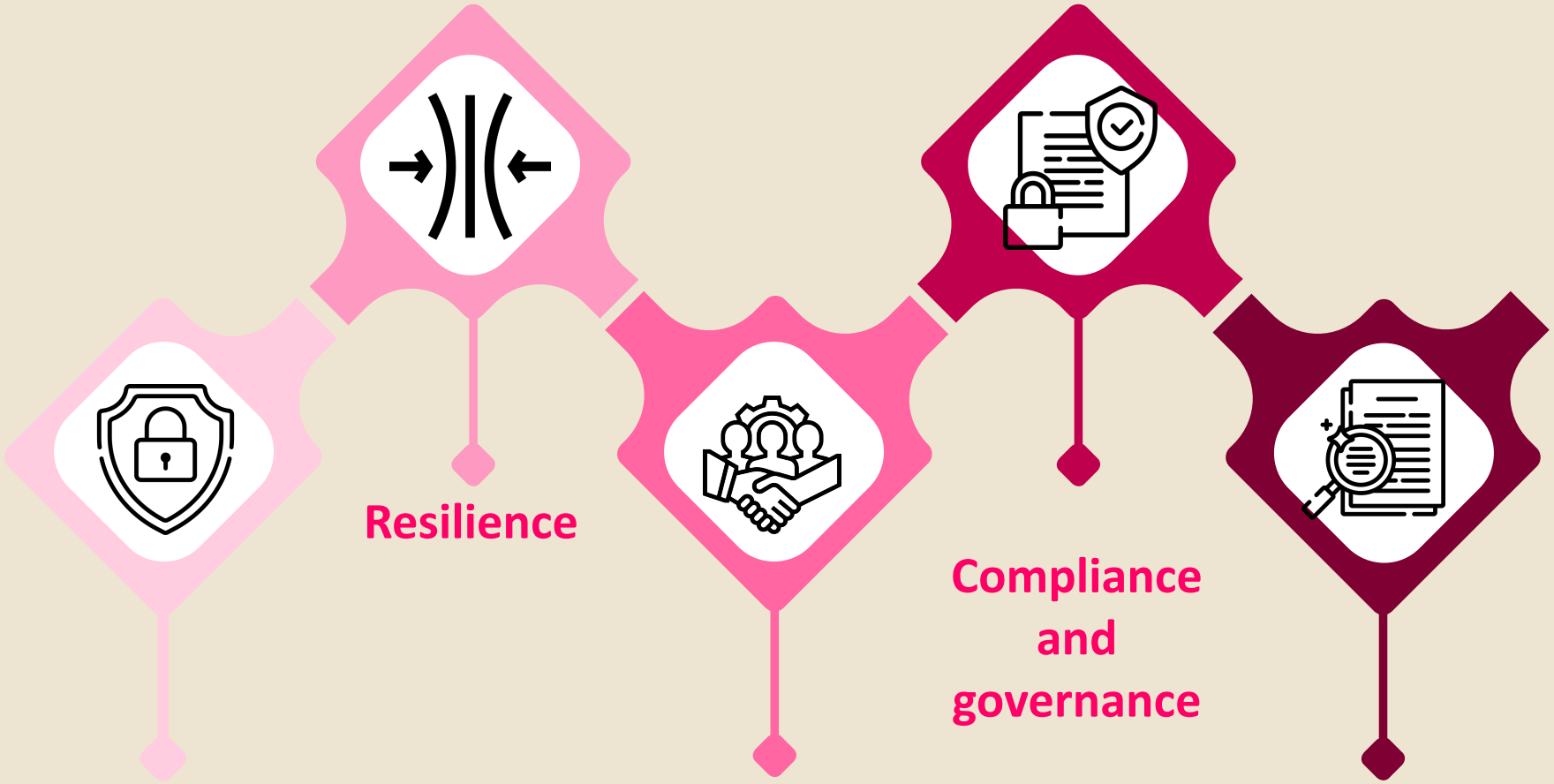
A collection of rules called a smart contract is recorded on the blockchain and performed automatically to speed up transactions. A smart contract can specify criteria for corporate bond transfers, as well as payment terms for trip insurance.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Blockchain Benefits

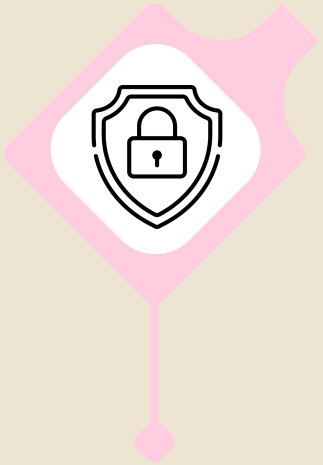


TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Security



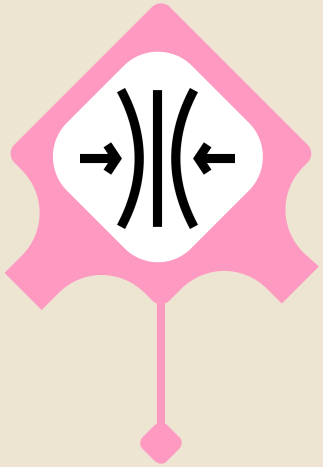
- The use of cryptography, immutability and distributed structure means that a blockchain database is virtually immune to hacking, fraud and other malfeasance. Illicit data changes are detected and rejected reliably.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Resilience



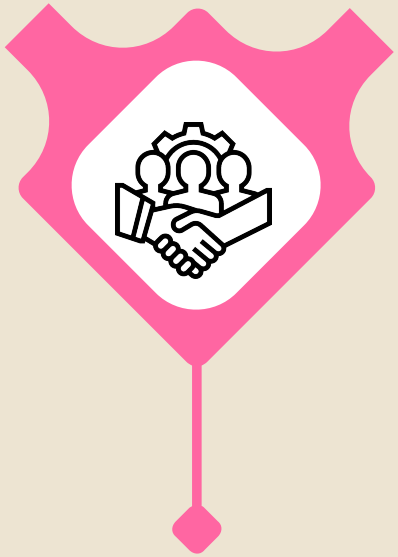
- Blockchain is a distributed technology: Every node that participates in the database shares a complete copy of the database and contributes consensus to the validation of each node as it changes. Not only does consensus enhance security, but if a node fails or falls under attack -- such as a distributed denial of service -- the remaining nodes continue to function. It is extremely difficult to attack and disable every node.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Faster Business



- As the common data set is available to all stakeholders with access to the ledger, a blockchain database can often eliminate traditional manual verifications and transaction settlement times that accompany business transactions. This can help to accelerate dramatically some financial and contractual business operations.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Compliance and governance

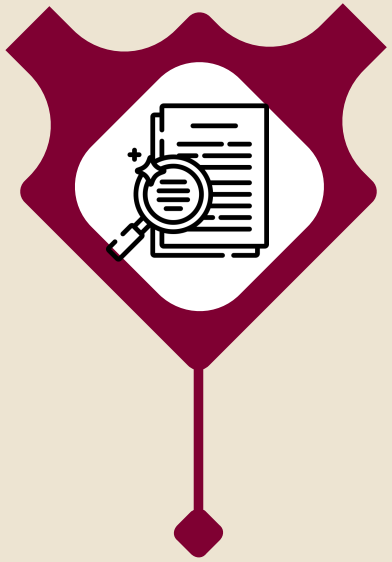
- The immutable and chronological nature of blockchain data can itself be audited to maintain business or industry compliance, as well as serve as a key element of governance across the business.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Transparency



- As the need for general trust increases with global business, the visibility and immutability of public blockchain transactions helps to build and ensure trust that data is fair and accurate.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

2. Fundamentals: blocks and hash:

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

2. Fundamentals: blocks and hash:

A block is a record that has data inside. Two values correspond to each block: the so-called previous hash and the hash.

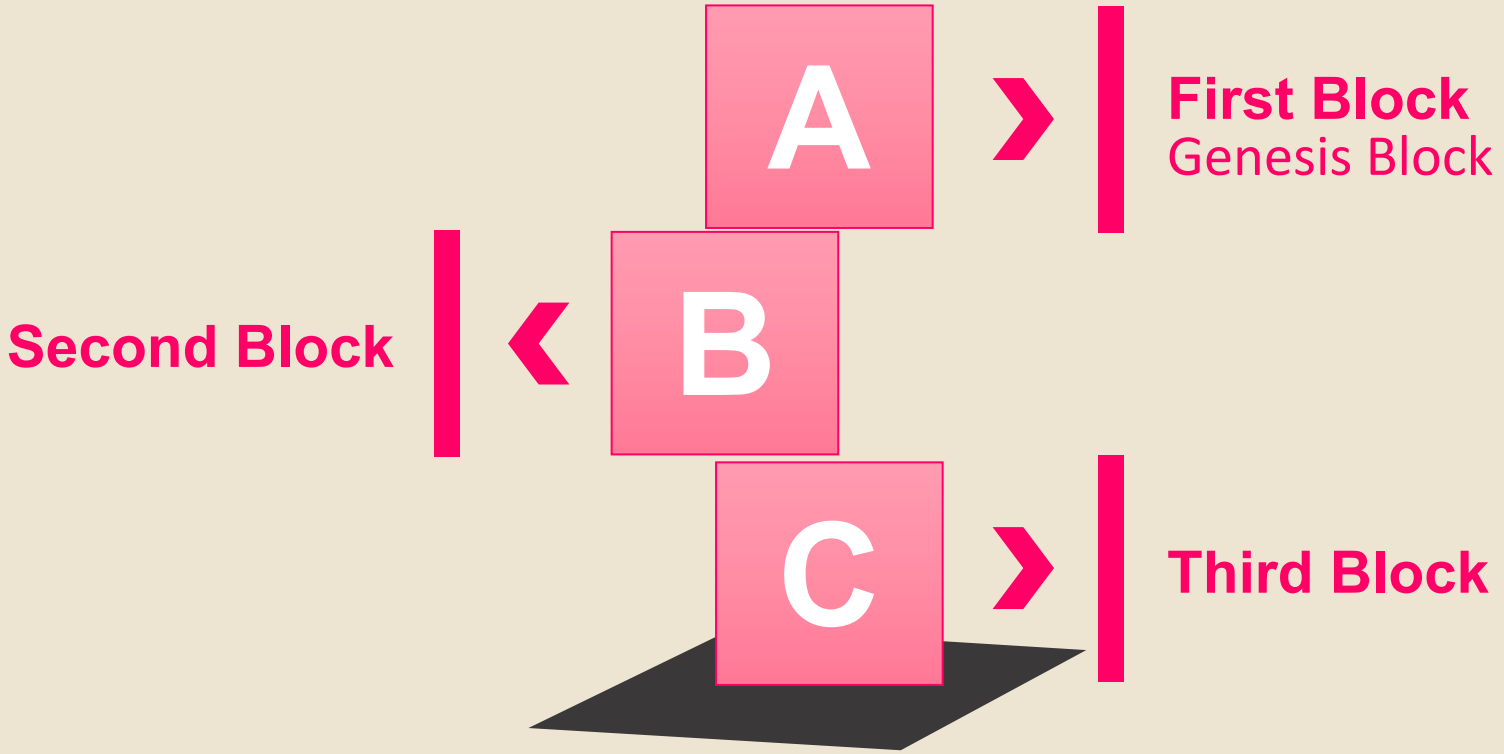
A digital hash can be defined as the fingerprint of the block that makes it much clearer. Data and the previous hash are represented, encrypted, in a number. This shortened version of the data is specifically sixty-four characters in length.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Three Different Blocks



TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Different blocks:

First Block

"genesis block"

Because it is the starting point of the chain. The genesis block will **always** be the first of the chain and cannot be substituted. Does not have a previous hash among its values because it is the first one. Therefore, in technical writing, the previous hash will be indicated as many zeros. Applied to cryptocurrencies, the genesis block is, for example, the first Bitcoin ever mined.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Different blocks:

Second Block

Contains data, previous hash, and hash.
The previous hash is the hash of the genesis block. The **blocks are cryptographically linked together through the hashes**.
So, if anything changed block number one, the next fingerprint would also change, and it would no longer match. The fingerprint of the block will then show that tampering happened.

TRANSITION

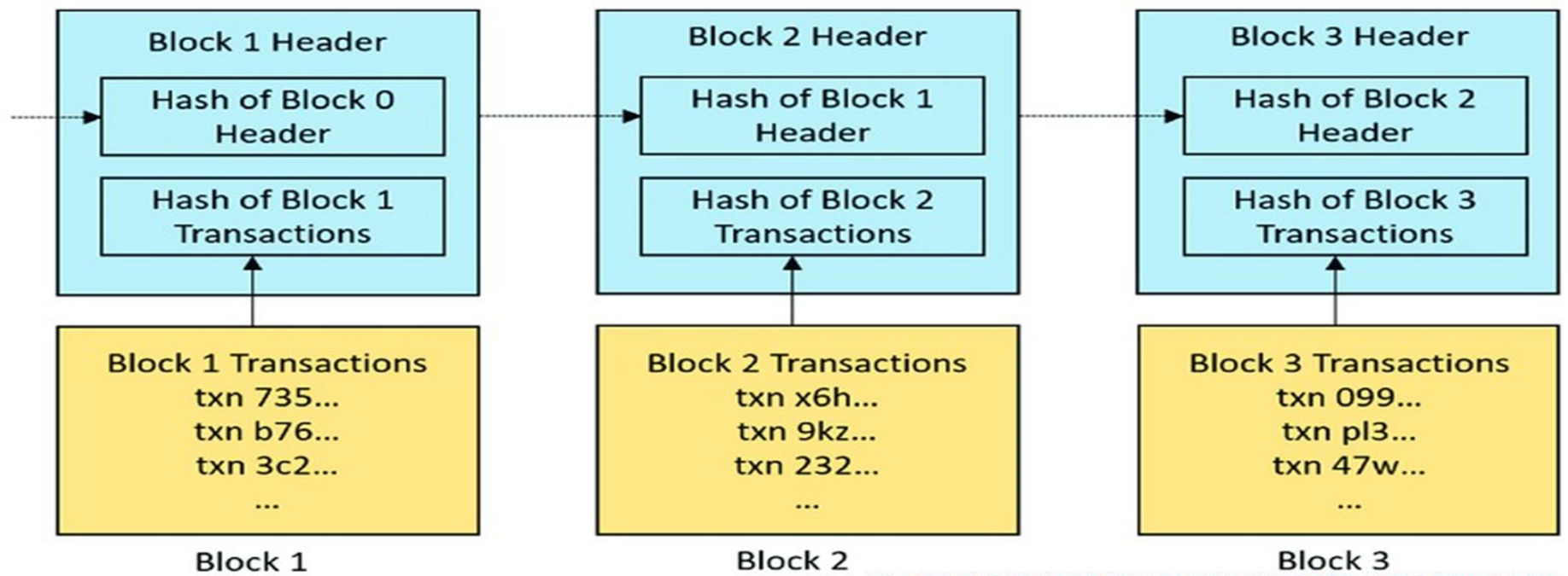
Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Different blocks:

Third Block

Will have the hash of block number 2 as its previous hash value, and so on.



1From: "Blockchain Technology in Healthcare: A Systematic Review" by 2019 C. Agbo, Q. H. Mahmoud, J. M. Eklund

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

3. Hash Cryptography

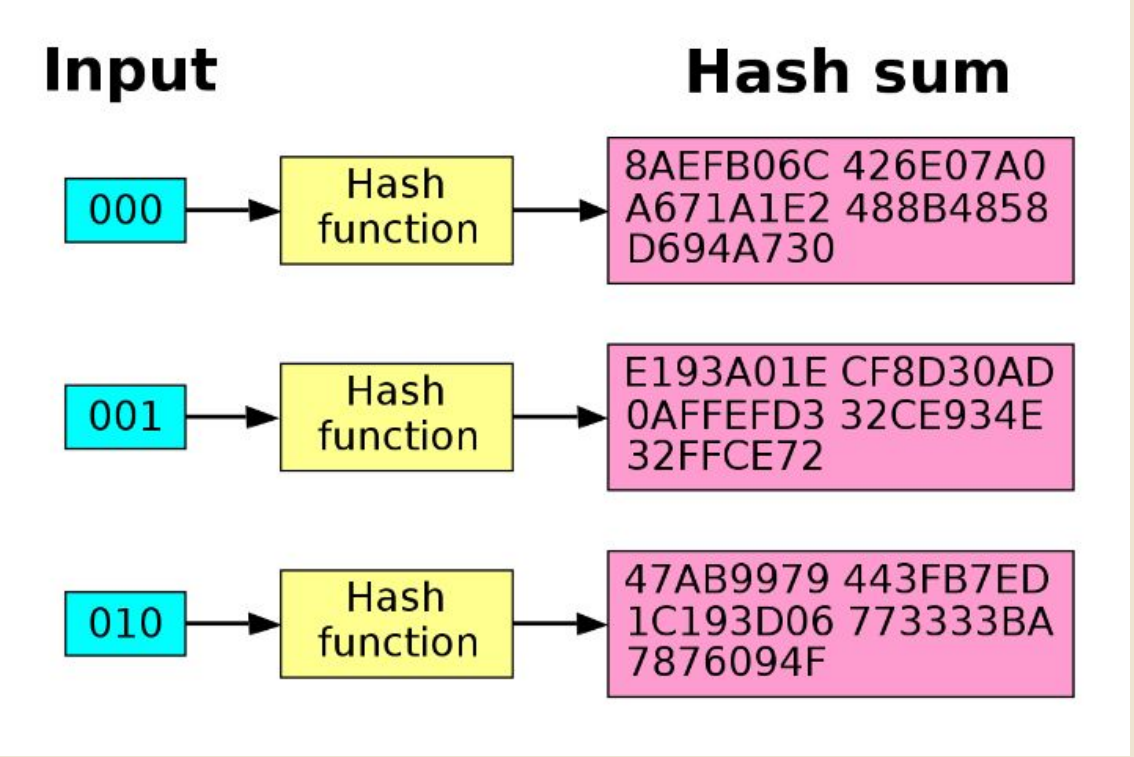
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

3. Hash Cryptography

- Cryptography codes **unique** markers for data.
- Can be equivalated to human fingerprints. Although there is a possibility that two people have the same fingerprint, it is a very unlikely (the probability is 1 in 60 million) event. In the same way in which the fingerprint identifies a person, hash identifies data.



TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

3. Hash Cryptography

- This technology is called **Shell 256 Hash,** developed by NSA.
- Shell stands for Secure Hash algorithm and 256 is the number of bits it occupies in memory.
- Hexadecimal (64 characters) :

0,1,2,3,4,5,6,7,8,9, a (10), b (11) ,c (12) , d (13) , e (14) ,f (15)

TRANSITION

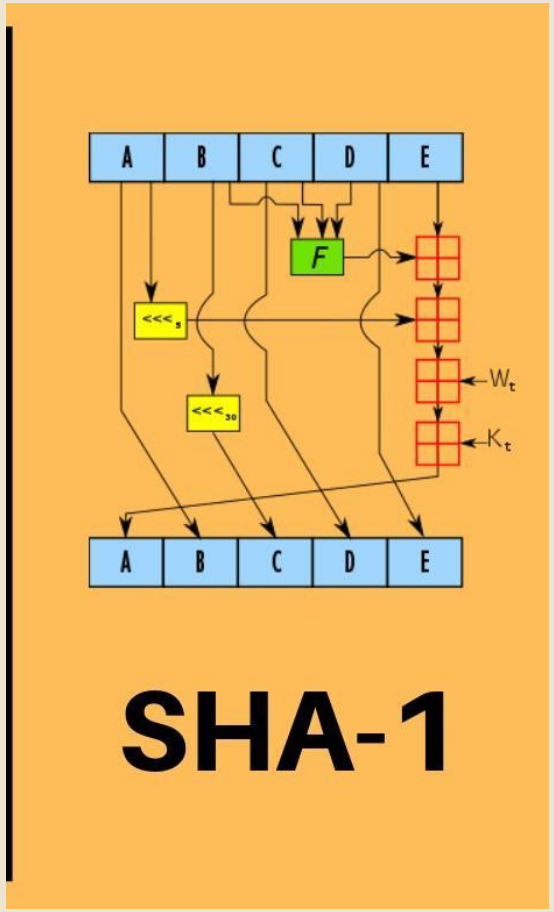
Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

5 requirements for hash cryptography

Secure Hash Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions.

A few algorithms of interest are SHA-1, SHA-2, and SHA-3, each of which was successively designed with increasingly stronger encryption in response to hacker attacks.



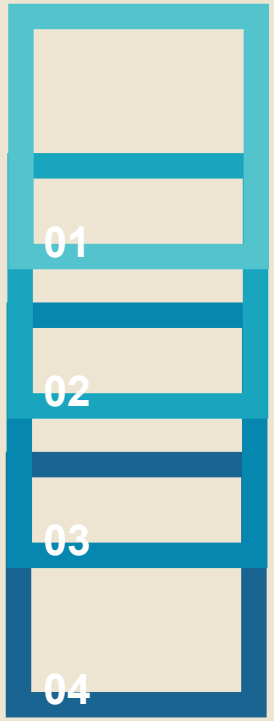
https://amythasneem.medium.com/secure-digest-functions-bb89d9d67b

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

4 requirements for hash cryptography



1. It has to go in one direction only ;
2. Must be deterministic;
3. The avalanche effect;
4. The algorithm needs to be able to withstand artificial collisions.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

3. Hash Cryptography

It's very secure, it is currently used to store passwords, to check digital documents, and in blockchain as well,

- **One direction:** The algorithm cannot be reversed, in other words once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data.

- **Second pre-image resistance**: Without this characteristic, two different passwords would yield the same hash value, deeming the original password unnecessary in order to access secured data.

TRANSITION

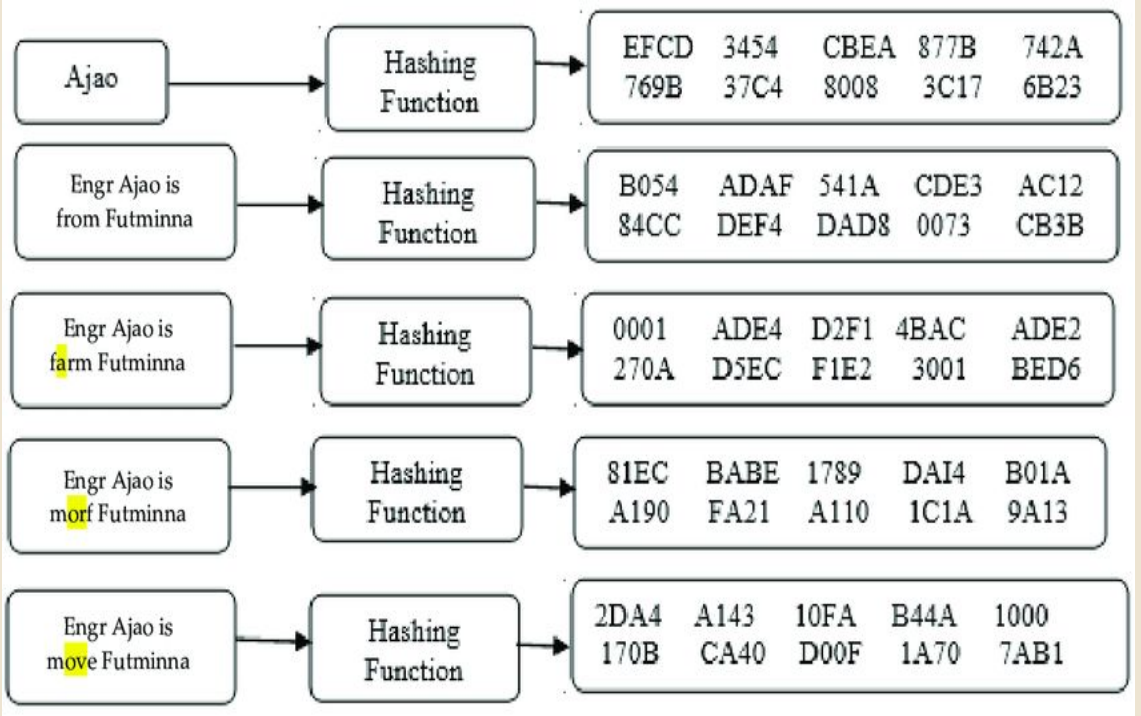
Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

The Avalanche effect

If you take exactly the same document and you slightly change it .

One small change triggers a few changes and they, in turn, trigger more dramatic changes.



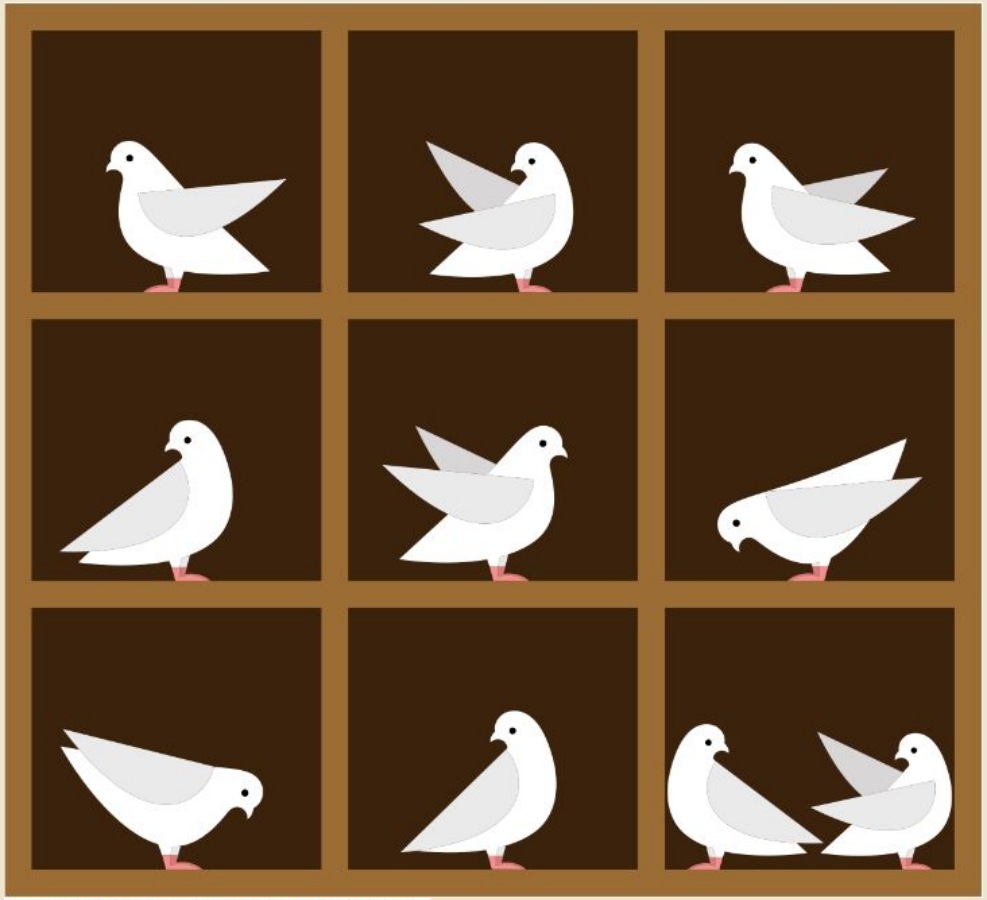
https://www.researchgate.net/figure/Crypto-hash-function_fig1_335055783

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Collisions



3Source: "THINKING LIKE A MATHEMATICIAN: The Pigeonhole principle The quintessential counting argument" by Jørgen Veisdal 2019

There may be **two** people with the same fingerprint, even if the probability is negligible, in the same way, it is possible for the hashing algorithm.

The principle states that if there are 10 pigeons and only 9 holes, two pigeons will have to share one of those holes. So, if there is more quantity A than there are slots of quantity B, then inevitably **there will be what we call collisions**.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

4. Immutable Ledger

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

4. Immutable Ledger

- Immutable Ledger simply means a record that cannot be changed.
- If someone tries to tamper with the data in that specific block, the hash for this block will change. So that cryptographic link will no longer work because the hash is different from the hash recorded here for the previous block. The previous hash will no longer match this one. It would then be necessary to would have to change the block as well.

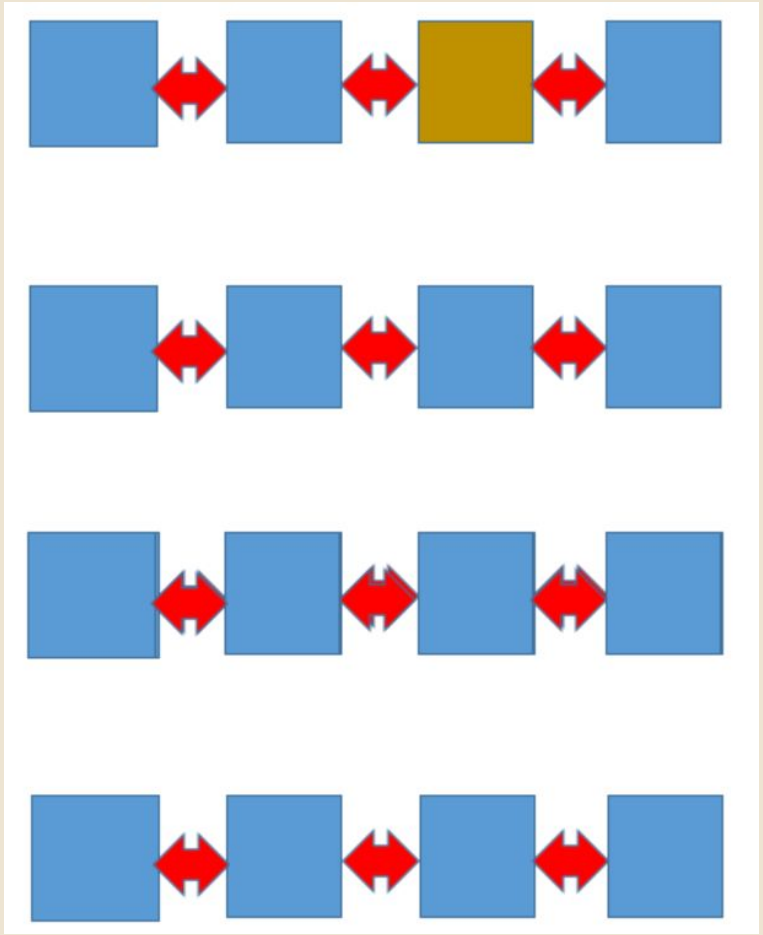
https://analytics4all.org/2018/04/09/blockchain-immutable-ledger/

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

4. Immutable Ledger



https://analytics4all.org/2018/04/09/blockchain-immutable-ledger/comment-page-1/

- Due to the cryptographic link, as soon as they change one block, all the subsequent blocks will no longer be valid. They will no longer be linked to the chain and it will be very easy to tell and very difficult for the person to tamper with the record.

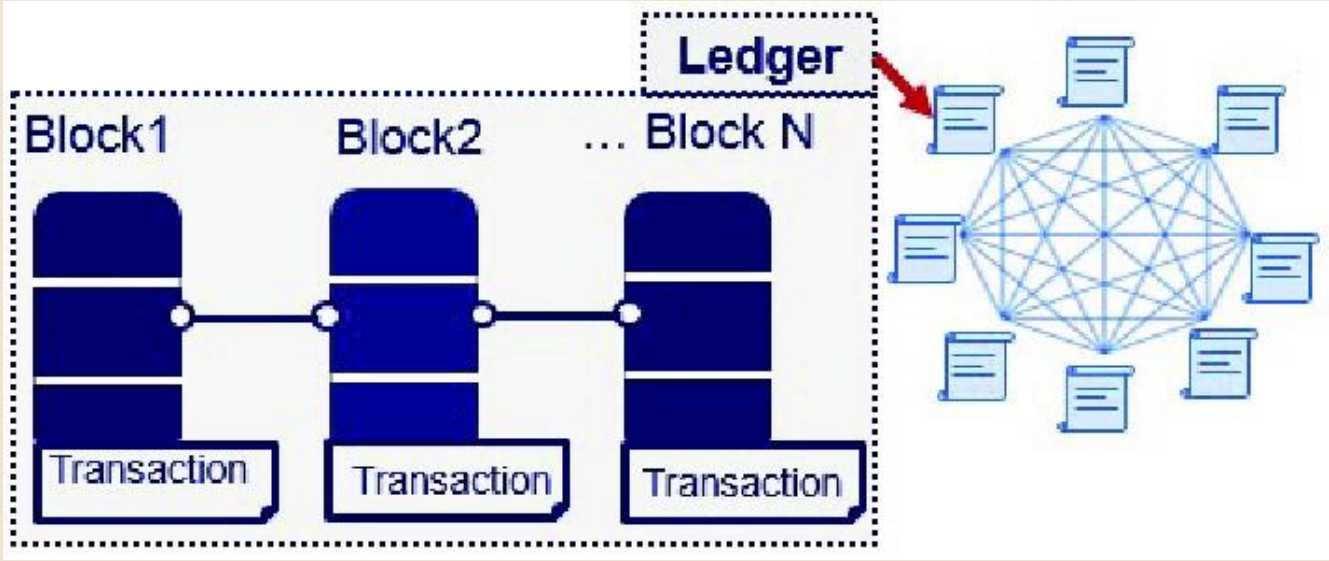
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

4. Immutable Ledger

- Unlike a physical ledger where you can only change one entry, here you would need to change all subsequent entries. This is what is meant by an immutable ledger: you cannot change entries as soon as they enter the block.
- Property Ledgers is one of the biggest examples when talking about blockchain outside of finance, Bitcoin, etc,



TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

5. Peer to Peer Network

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

5. Peer to Peer Network

Using the blockchain allows the immutable ledger to be protected, preventing forgeries that could be facilitated by traditional means. However, two questions remain:

If the 'scam' is potentially worth a lot of money and you have enough time, someone could make the effort to change all the blocks and hashes: what would prevent them from doing so?

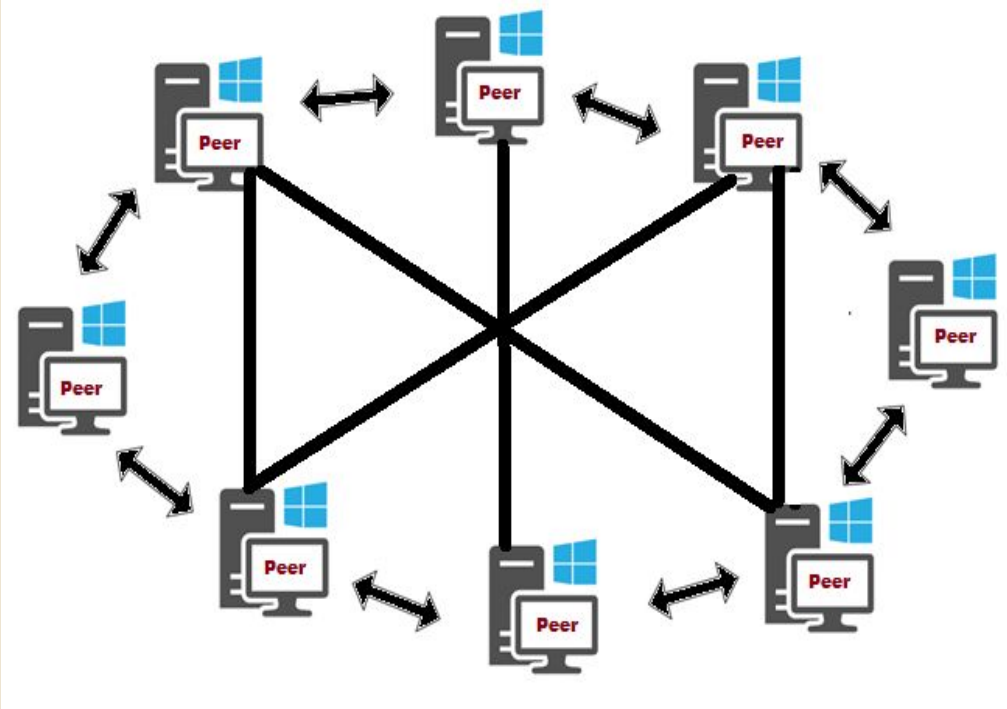
If a system or input error occurs and the changes cause the data to be lost? how can this be remedied?

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Distributed peer-to-peer (P2P) networks.



- In a distributed P2P System there are lots of computers, all interconnected. Ideally, the more they're connected, the better. The blockchain is copied across all of those computers.
- The problem occurs when someone tries to hack into the system or there is a technical problem.

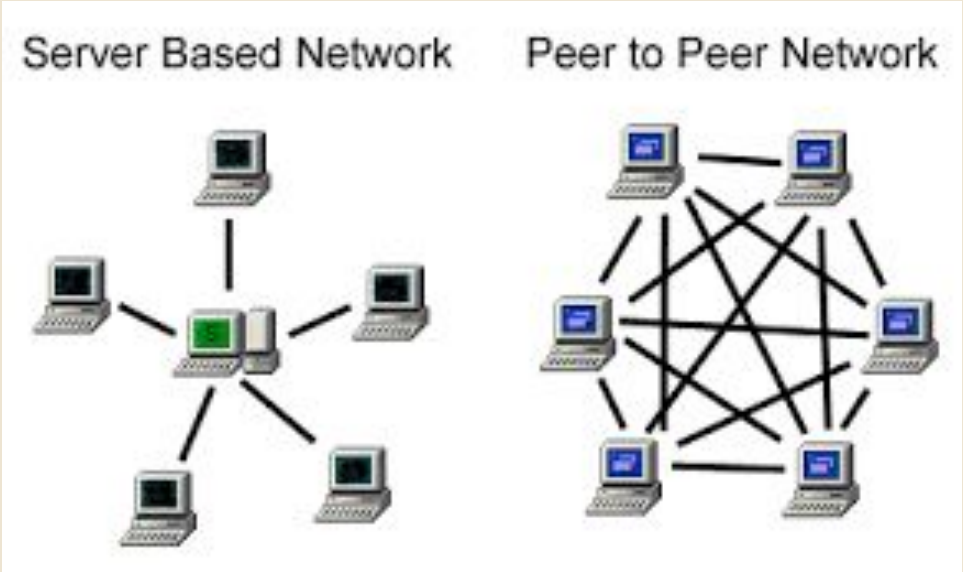
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Distributed peer-to-peer (P2P) networks.

The attack takes place on a block, the data of which is changed. As said before, it is possible to change all the other blocks following the attacked block, modifying the chain, especially if it is a worthwhile operation. But the situation changes in the P2P Network context. The network constantly checks peers to see if their blocks match, so any changes or problems are immediately reported.



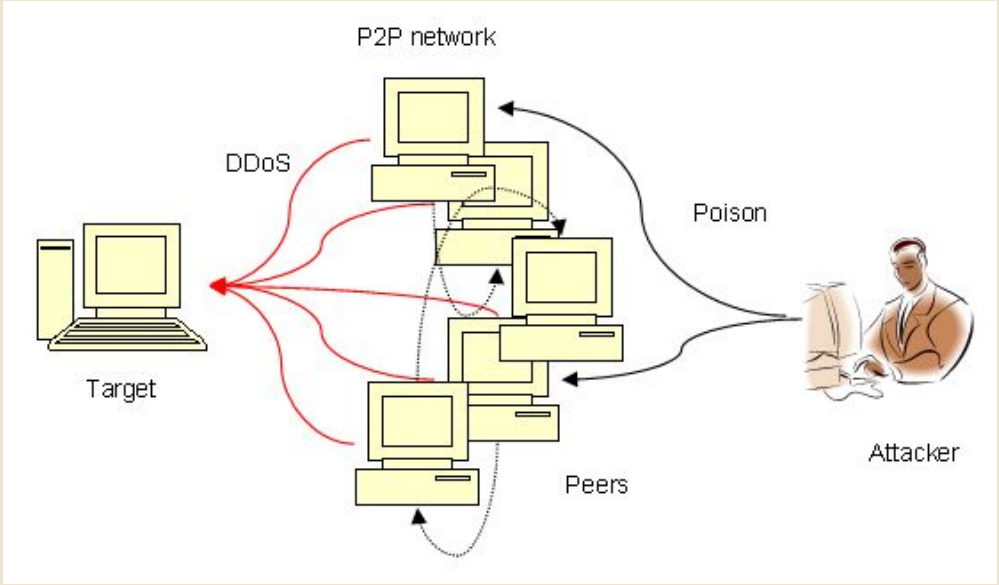
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Distributed peer-to-peer (P2P) networks.

The rest of the computers know there has been an attack because the encrypted chains no longer match. In this way the anomalous values are immediately recognized, the system, therefore, replaces them with the original values on the other computers. For the attack to be successful, the hacker would have to take down more than 50 percent of the computers at the same time to successfully replace the chain.



https://www.cse.wustl.edu/~jain/cse571-07/ftp/p2p/

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

6. How mining works

TRANSITION

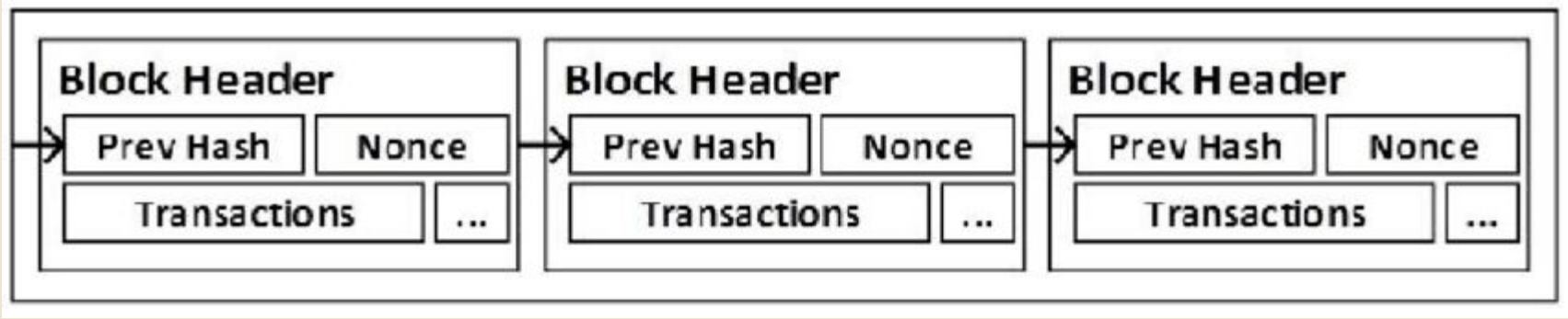
Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

How Mining works – The Nonce

There is, in fact, another element within the block: the field is called **Nonce** (number used only once). This is what mining is all about.

- **This value**, together with the data and the previous hash, combined with the algorithm **defines the hash of the block** and thus determines the chain.
- By changing the nonce, which is a number, the **hash changes substantially**. **This is due to the avalanche effect**.



TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

The Nonce

The **nonce** provides extra control and flexibility: you can manipulate the hash value by controlling the nonce. We must not forget that:

- ✔ The block number cannot be changed
- ✔ You cannot change the hash directly, because it would invalidate the chain
- ✔ You cannot change the previous hash because it is defined by the previous block
- ✔ You cannot change the data because it would mean tampering with it, which would defeat the purpose of a block change (It has to be an immutable ledger, to prevent tampering)

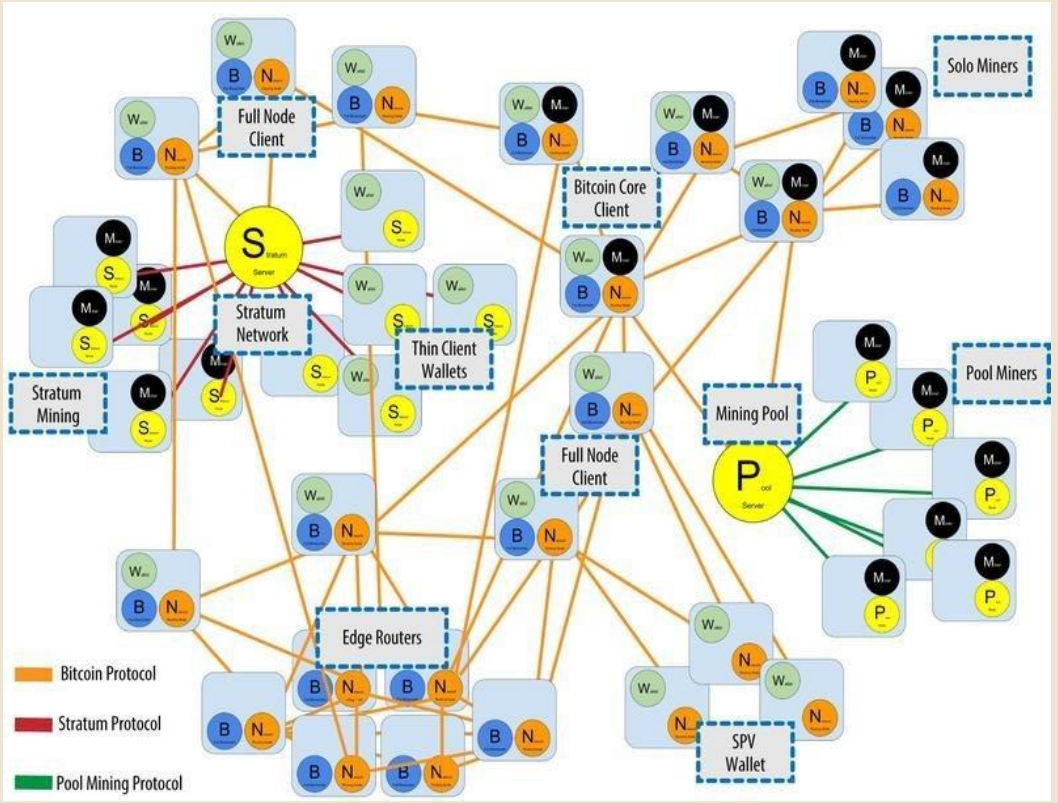
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

How Mining works – The Cryptographic Puzzle

The blockchain system or the algorithm will set a target for miners to accomplish a certain hash. The target is set arbitrarily, without economic or other reasons. The hash must meet this target and be below the set limit. A good way of thinking about the target is in terms of leading zeros: the lower it is, the smaller the number and therefore more leading zeros there will be.



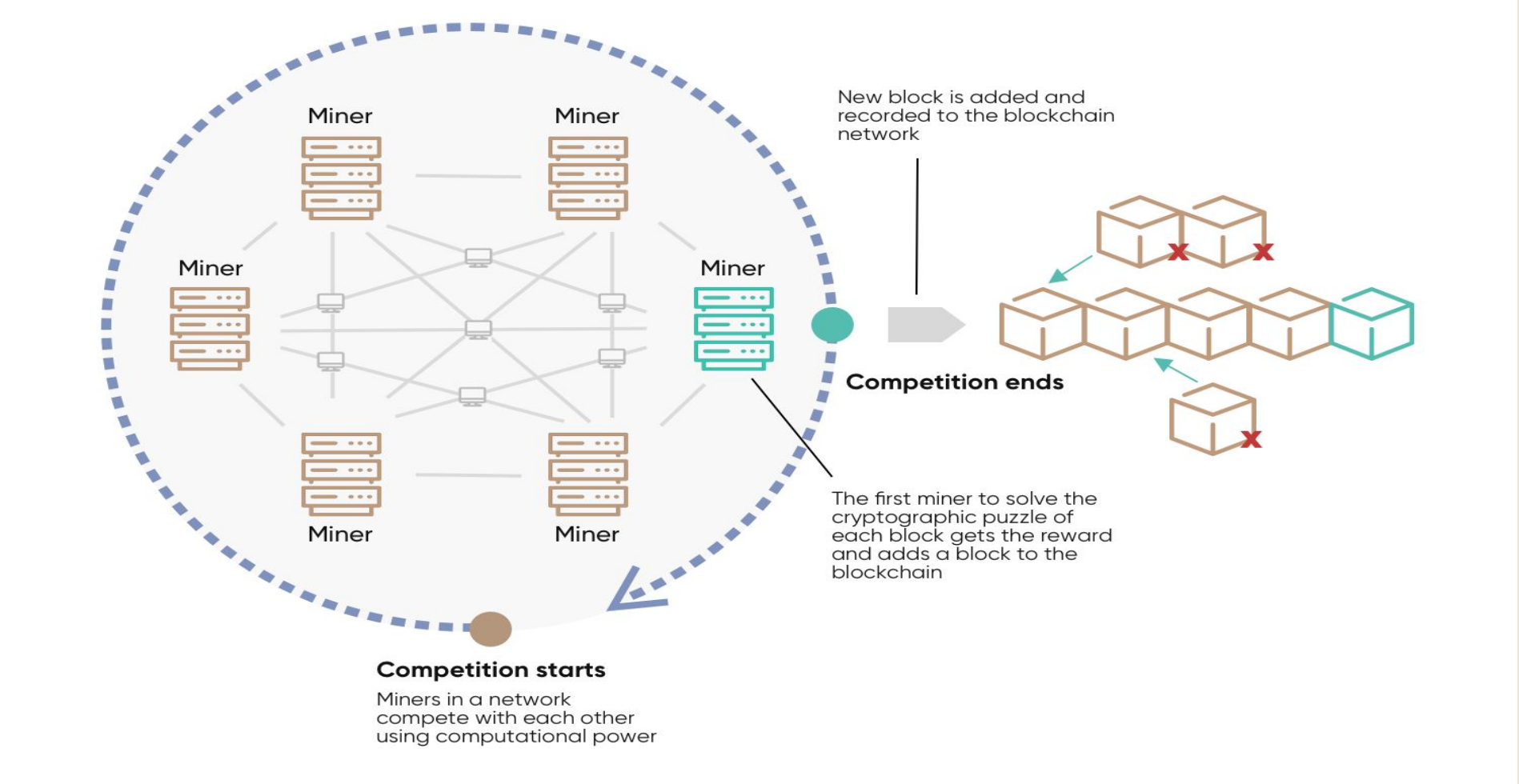
https://steemit.com/bitcoin/@cryptovest/bitcoin-and-blockchain-what-math-puzzle-do-miners-actually-solve

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

The Cryptographic Puzzle



TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

The Cryptographic Puzzle

- Miners change the nonce in order to try to guess a value of the nonce that will generate a hash **below the target**. When, by trial and error, they find the nonce that allows the hash to be placed below the target (and therefore to have a certain number of zeros) they call it **Golden Hash**.
- Once defined, they can create a new block to add to the blockchain. The block is accepted by the blockchain **only when the hash is below the target.**

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

The Cryptographic Puzzle

To define a hash that satisfies the required characteristics, there is no linear process: it is completely unpredictable and that is a very important feature. The process you need to follow to find the hash is called **Cryptographic Puzzle.**

Without the avalanche effect, which substantially modifies the hash by making very small changes, **this puzzle would not exist**. It would be enough to decrease or increase the Nonce number to be sure of meeting the target. However, precisely because of this effect, the search requires attempts and not defined and unambiguous steps**.**

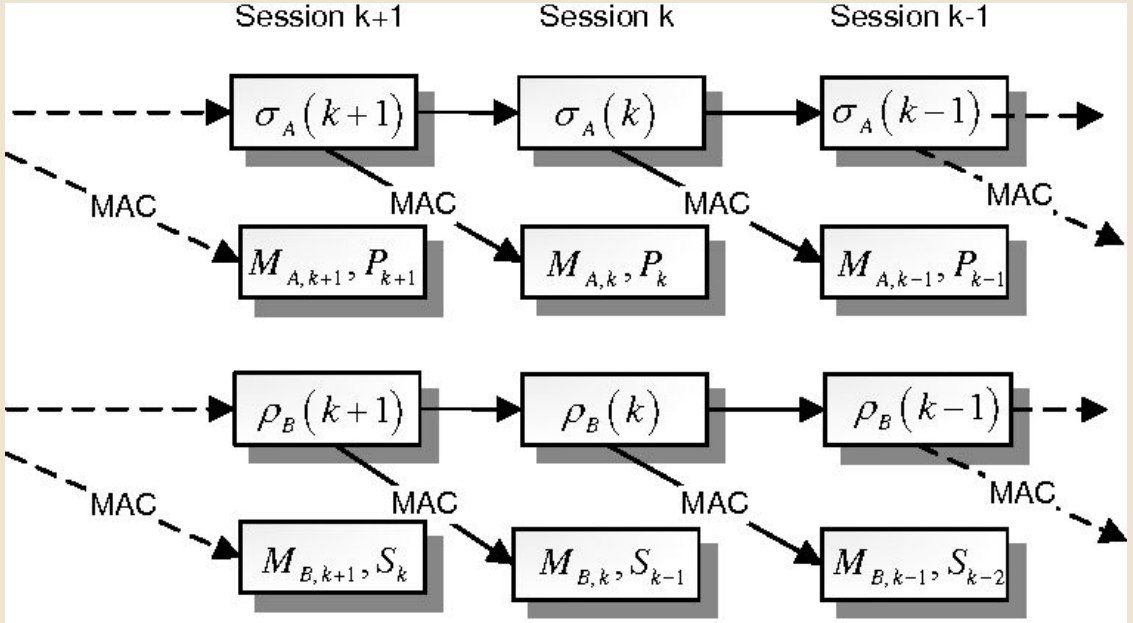


Figure 2

The connection between the keys and the puzzles from each session of the DeMA protocol

https://www.semanticscholar.org/paper/On-Chained-Cryptographic-Puzzles-Groza-Petrica/ac8b958df1b1839a7f7478bea407bf2a2fc57ce5

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

8. Byzantine Fault Tolerance

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

8. Byzantine Fault Tolerance

It is a very important characteristic, not only for blockchain but also for any type of decentralized system. To explain the concept there is a story.

- 4 Byzantine generals surround a castle and want to conquer it.

They can only win if the majority of them come to a **consensus** of what to do. Whether they attack or retreat, the majority of these generals have to come to an agreement:

- ✔If three out of four say "we are attacking" and they attack, they will win;
- ✔If three or four out of four say "we are retreating" and they retreat, they'll be all safe and fight;
- ✔ However, if they don't come to a consensus, they will be destroyed by the enemy.

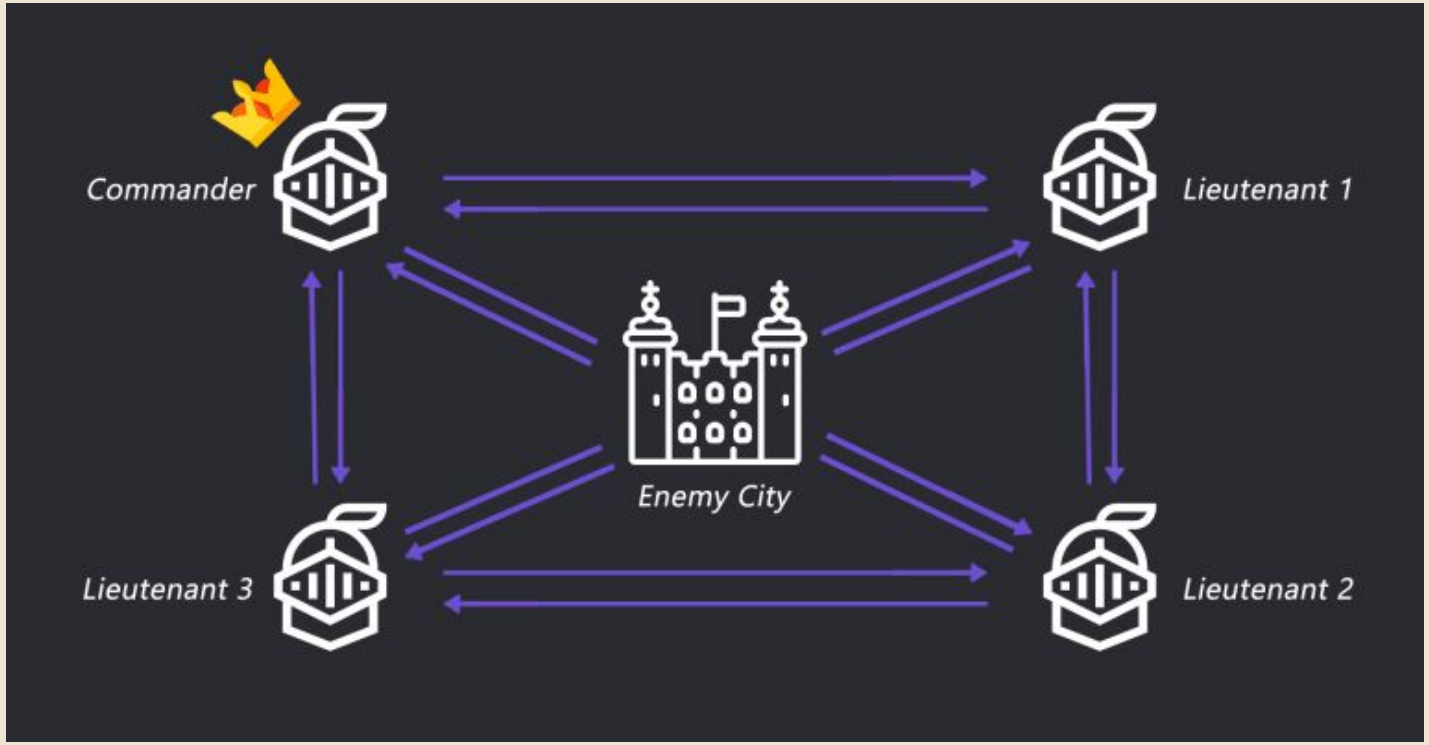
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

8. Byzantine Fault Tolerance

- Between them there are 3 figures:
  - ✔ the supreme commander
  - ✔ a probable traitor (but the commander himself may be the traitor)
  - ✔ The other Liutenants



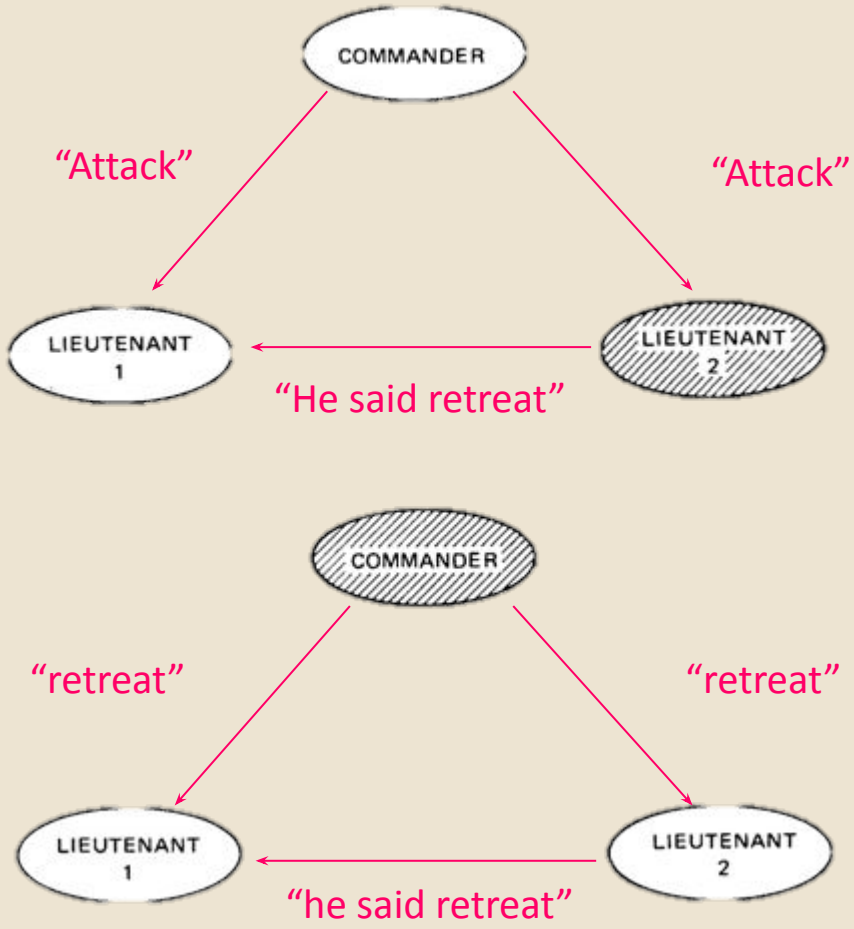
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

For example:

1. **The commander orders each one separately to attack**, but the three generals do not know whether he is the traitor. Then they will have to look at the majority in the content of what the commander said. The traitor will tell the other two that he received the order to retreat, lying. The other two will tell the truth, saying that the commander ordered each of them to attack.



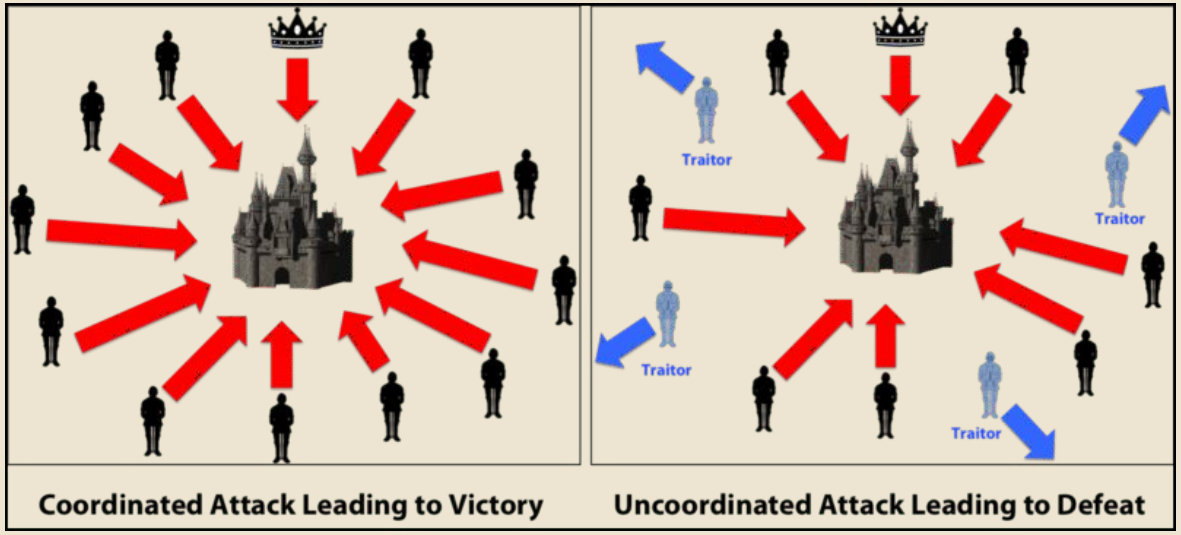
6"The Byzantine Generals' Problem" by Ashwin Kumar R (2019) blogpost

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

8. Byzantine Fault Tolerance



2. Can consensus be reached?

- The commander will attack because he ordered it.
- General 1 has two positive responses for the attack (commander and general 2)
- General 2 has two positive responses for the attack (commander and general 1)

So the majority reaches an agreement and attacks.

TRANSITION

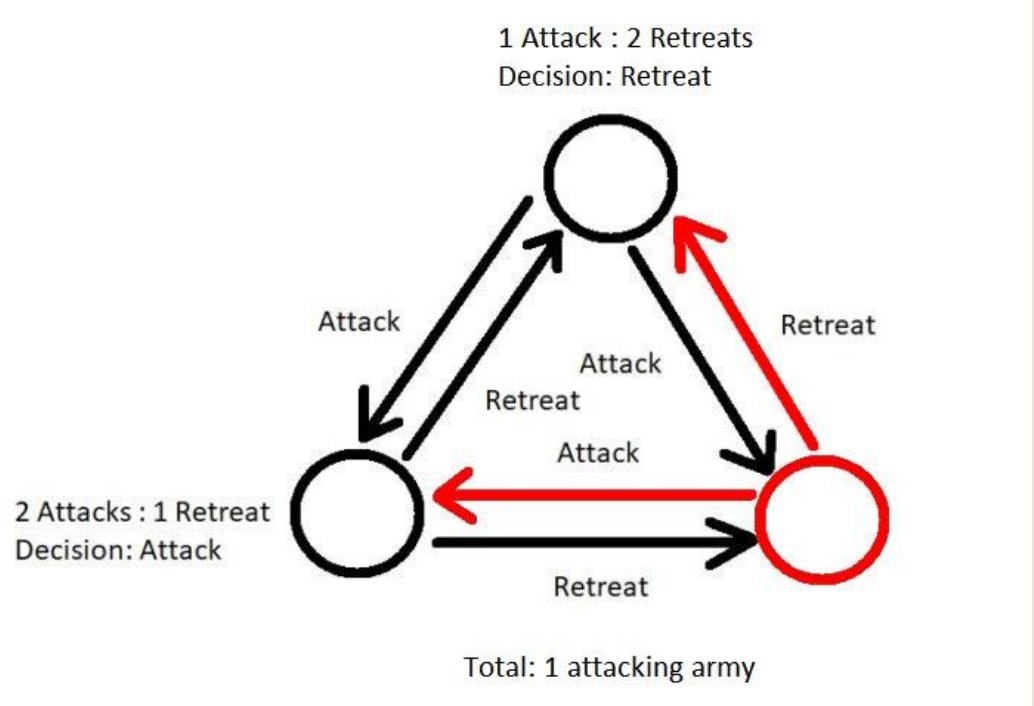
Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

8. Byzantine Fault Tolerance

3. What happens if the commander is also the traitor?

- If he told everyone to attack it would be pretty stupid of him because then they would tell each other to attack and they would attack and take the castle
- The same for retreating



TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

8. Byzantine Fault Tolerance

- **Deciding based on the majority of information is the algorithm and it is Byzantine fault-tolerant.** The question is to what level is it tolerant or to what level is intolerant? If there were two traitors, the mechanism could not work. For instance, for this algorithm to work, you have to have no more than 33% traitors: if there are four traitors out of ten generals, it will not work.

- That is the level of tolerance of this system in the sense of traitors. How does this go back to blockchain or like other systems that are decentralized or more technological?

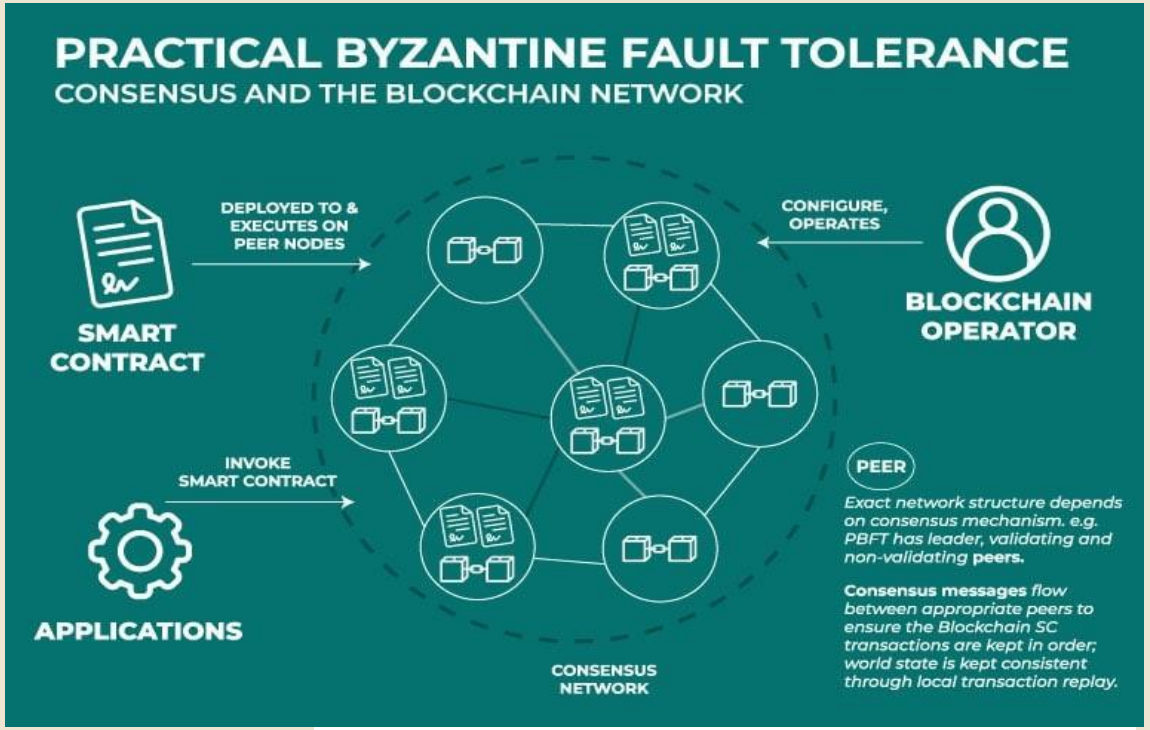
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

8. Byzantine Fault Tolerance

What happens in the blockchain? If anyone tries to attack the system, it is necessary to put in place a consensus protocol that will allow to protect the system and to make it as tolerant as possible. That's the whole concept of Byzantine fault tolerance.



7"What is Byzantine Fault Tolerance?" A quick guide (2021) blogpost

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

8. Byzantine Fault Tolerance

Overall, the Byzantine fault tolerance is considered an attractive alternative to other algorithms such as PoS (proof of stake), PoW (Proof of Work) consensus and PoI (Proof of Importance).

Pros

- The network does not need multiple confirmations, nor a waiting period to ensure that a transaction is secure or valid after it is included in a block
- Consensus can be reached without requiring excessive energy usage for miners.

Cons

- The system is vulnerable to Sybil attacks, that are executed by the same entity that controls the network entities and therefore corrupt the system.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

9. Consensus Protocol - Defense Against Attackers

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

9. Consensus Protocol - Defense Against Attackers

The consensus protocol for a blockchain needs to reach **two main** objectives:

1. **Protect the network from attackers**
2. **The challenge of competing chains**

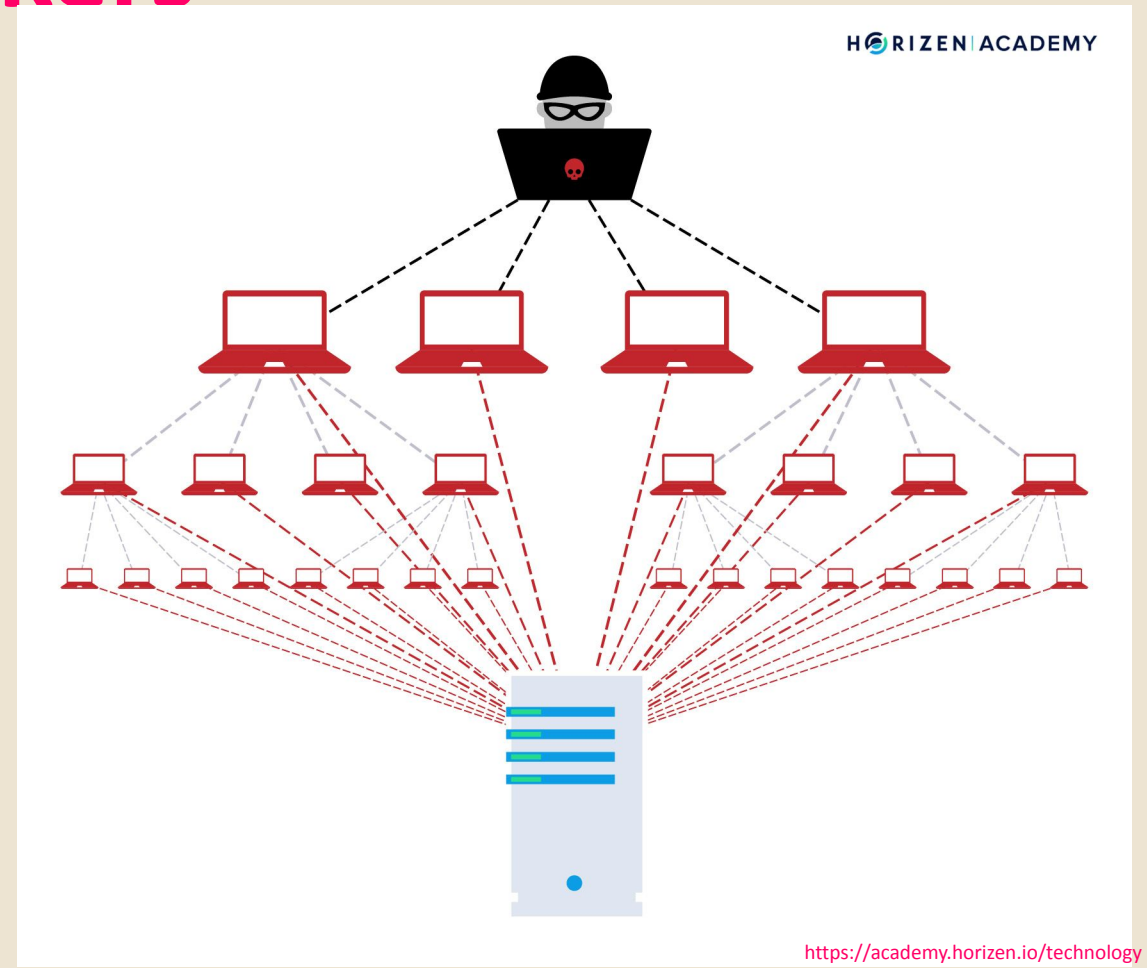
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

9. Consensus Protocol - Defense Against Attackers

- In a large blockchain, because it is distributed across the world, a lag between nodes can happen, especially those that are far away from each other. It could also happen that two nodes that are far away from each other can successfully find a block at the same time. This is not an attack, but a delay of information that arrives just after the creation of the block.



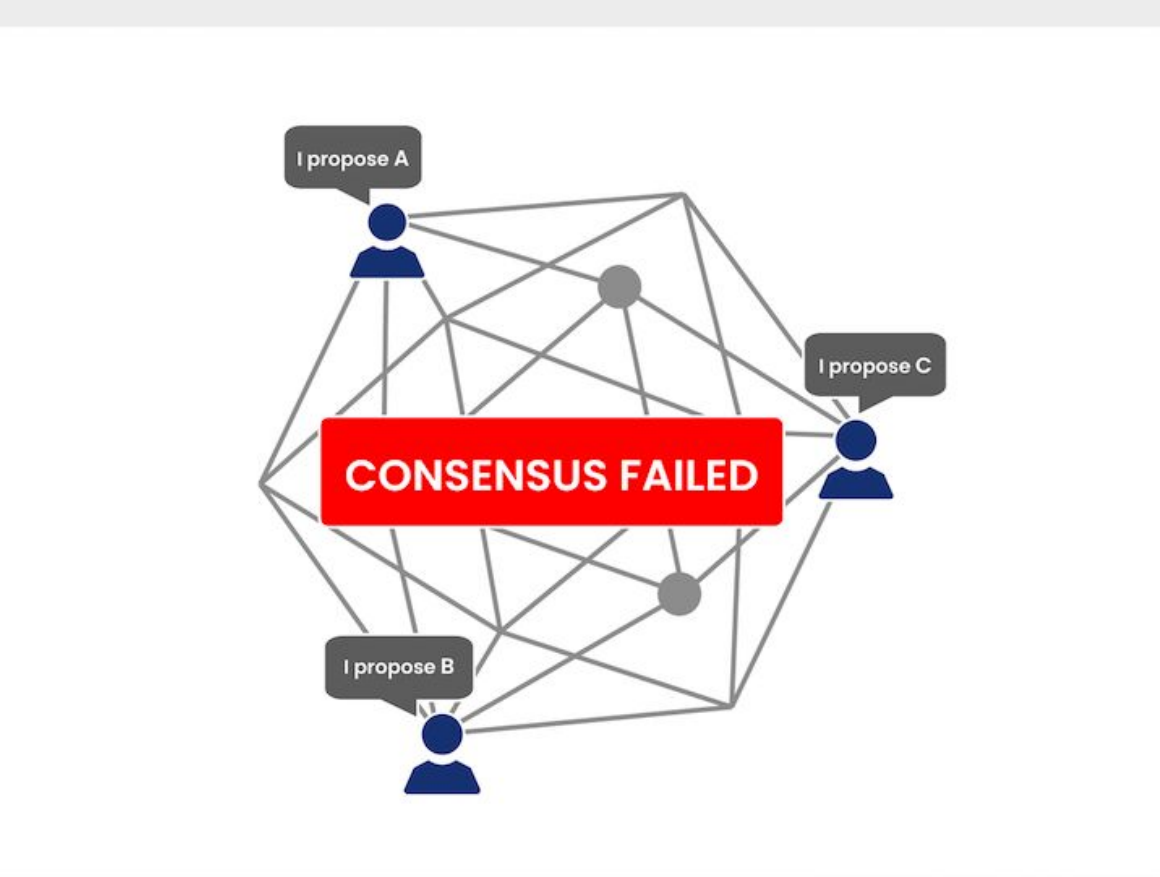
https://academy.horizen.io/technology/advanced/attacks-on-blockchain/

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

9. Consensus Protocol - Defense Against Attackers



https://analyticsindiamag.com/blockchain-consensus-algorithms/

Although it does not represent an attack, this is a problem because it needs to be in consensus on how to keep growing. If there is no consensus, there will be conflicts and then they will split up into two and then later on the block channel split up into four and eight and so on.

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

9. Consensus Protocol - Defense Against Attackers

At this point is important to note that there are **multiple types** of consensus protocols, that we mentioned before:

TRANSITION

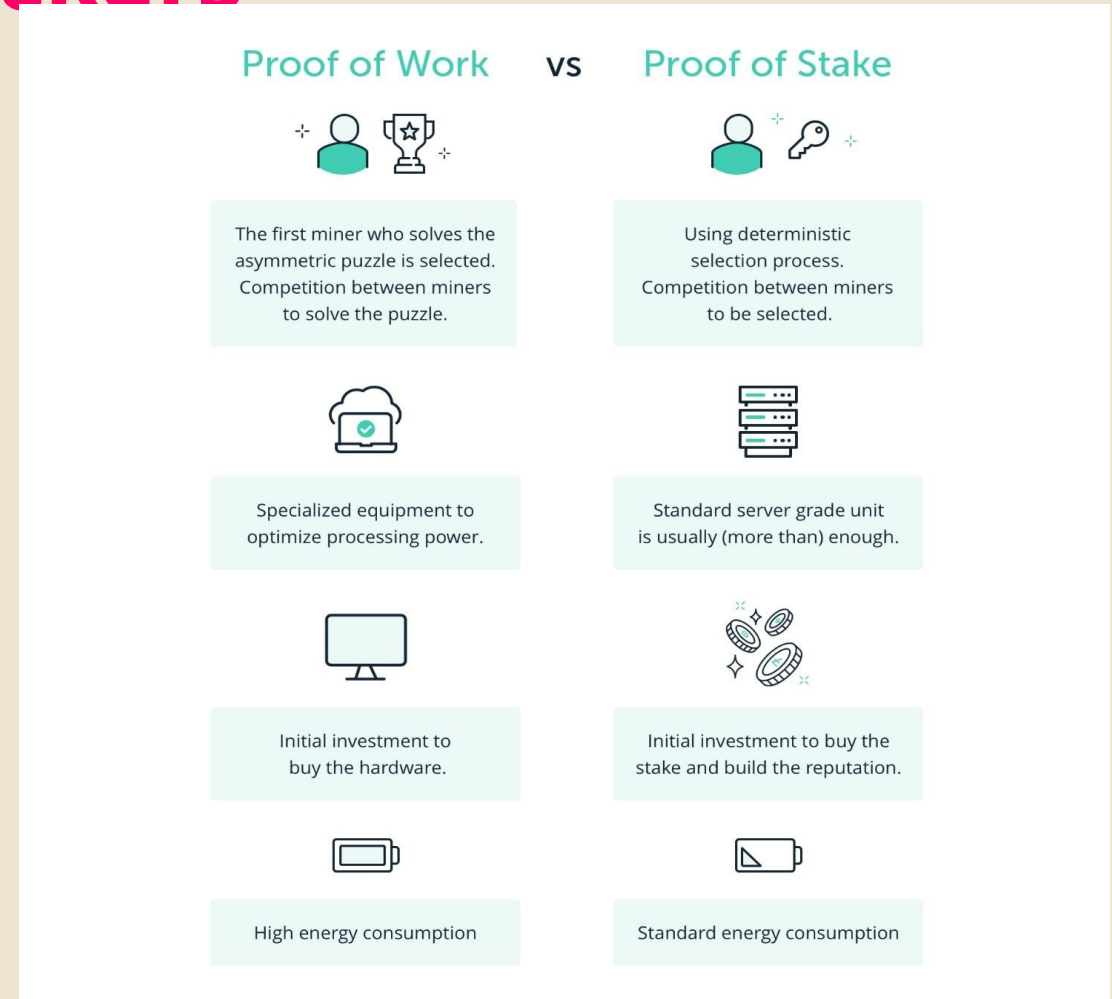
Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

9. Consensus Protocol - Defense Against Attackers

Proof-of-work (PoW)

- Is the original algorithm, and it is currently used, among others, by Bitcoins.
- Where does the term come from? Finding the correct hash, the one that meets the target, requires a lot of work, many hours, and therefore a lot of electricity. The final hash is **proof of the work** that went into finding it, proof that the search had a purpose and that it achieved it.



TRANSITION

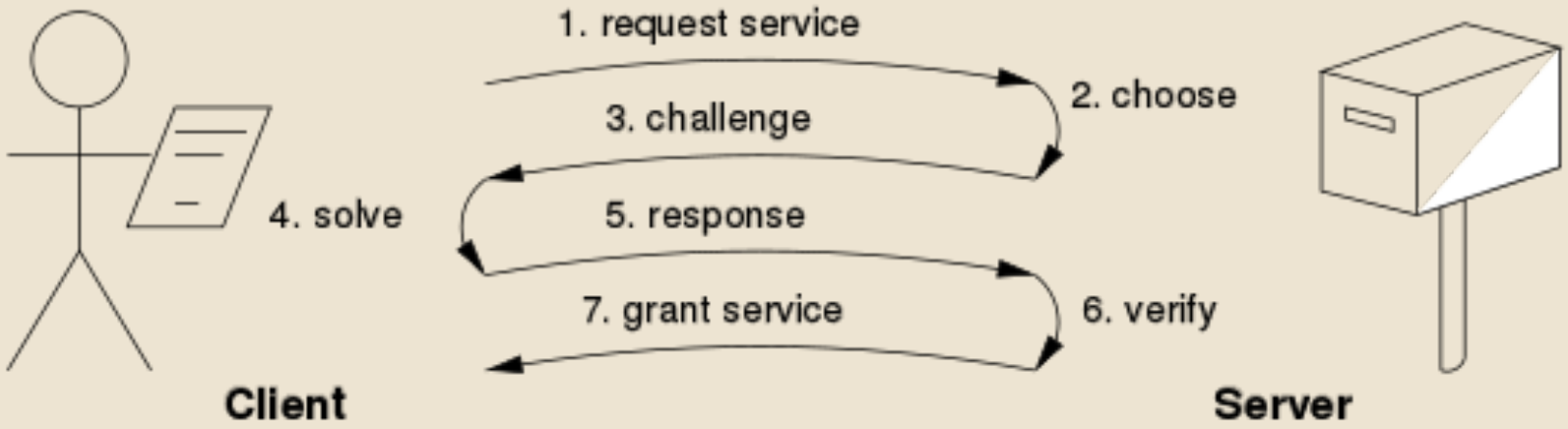
Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

9. Consensus Protocol - Defense Against Attackers

Proof-of-work (PoW)

When a miner adds a new block, there comes there is a new block. The network or the blockchain will reward the miners for mining and they also will get the fees associated with the transactions that are included in that block: so there is a monetary incentive, but they have to play fair.



Challenge response http://www.coelho.net/

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

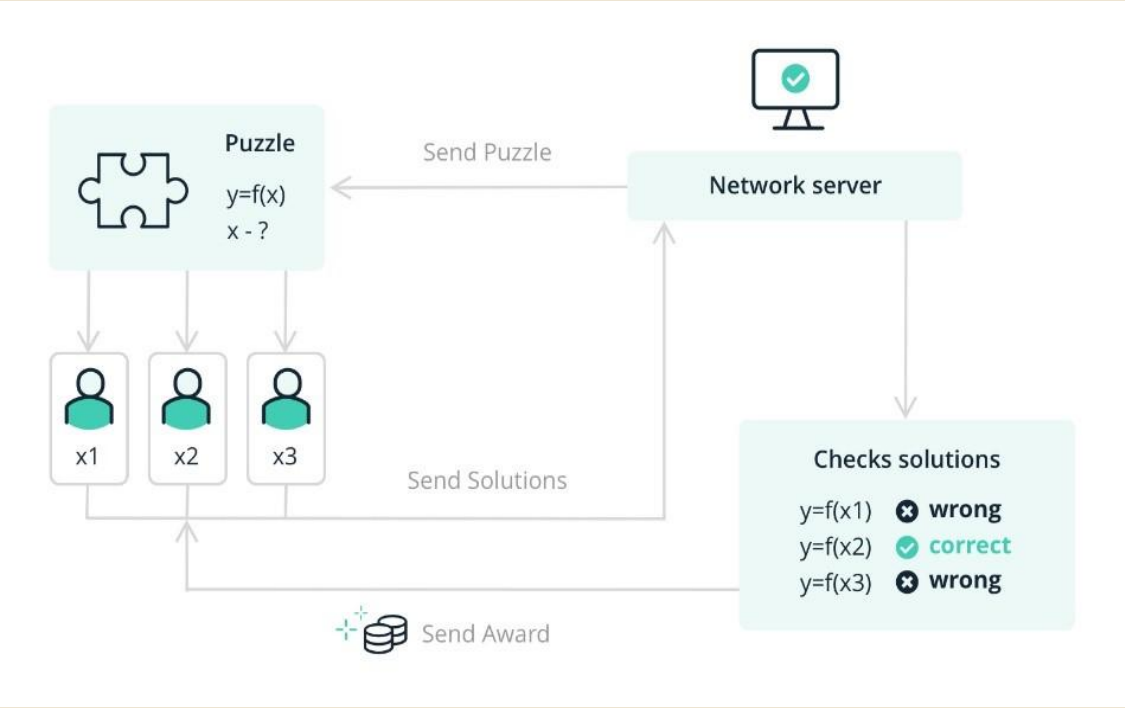
9. Consensus Protocol – Proof of Work (PoW)

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

9. Consensus Protocol – Proof of Work (PoW)



9"What is Proof-of-Work" Ledger Academy (2019)

How will the network know if they're adding a malicious block?

Every single note before the block is propagated to the network will conduct a series of checks and this series of checks is very rigorous. If a check does not go through, then they reject the block and so basically, at the end of the day, the network will not allow malicious blocks to be added to the chain. That is why there is a financial incentive to play according to the rules.

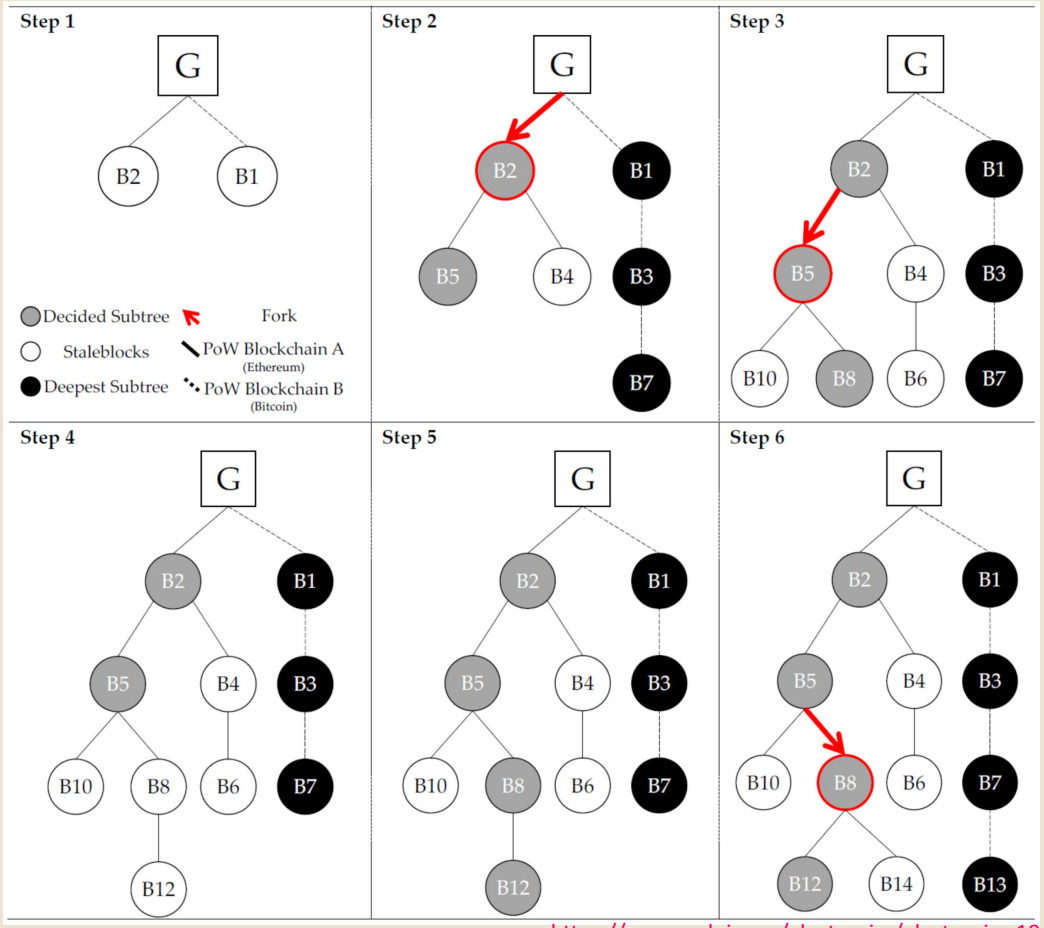
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Conflict between blocks:

When a new block, free of malicious intent, is created, it is attached to the blockchain. The information may propagate at different speeds and does not reach all nodes immediately. Another block may be generated at the same time.



https://www.mdpi.com/electronics/electronics-10-02135/article_deploy/html/images/electronics-10-02135-g008.png

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

How do we proceed?

We wait for another block to be added. Once that block is added, then we will see which of the two chains is longer: which chain basically adds a block first wins.

Whichever chain has the most blocks will eventually win and replace the other chain. **The part of the network that has the highest hashing power will eventually generate the longest chain. Hashing power is measured by how many hashes can be checked per second.**

https://www.mdpi.com/electronics/electronics-10-02135/article_deploy/html/images/electronics-10-02135-g008.png

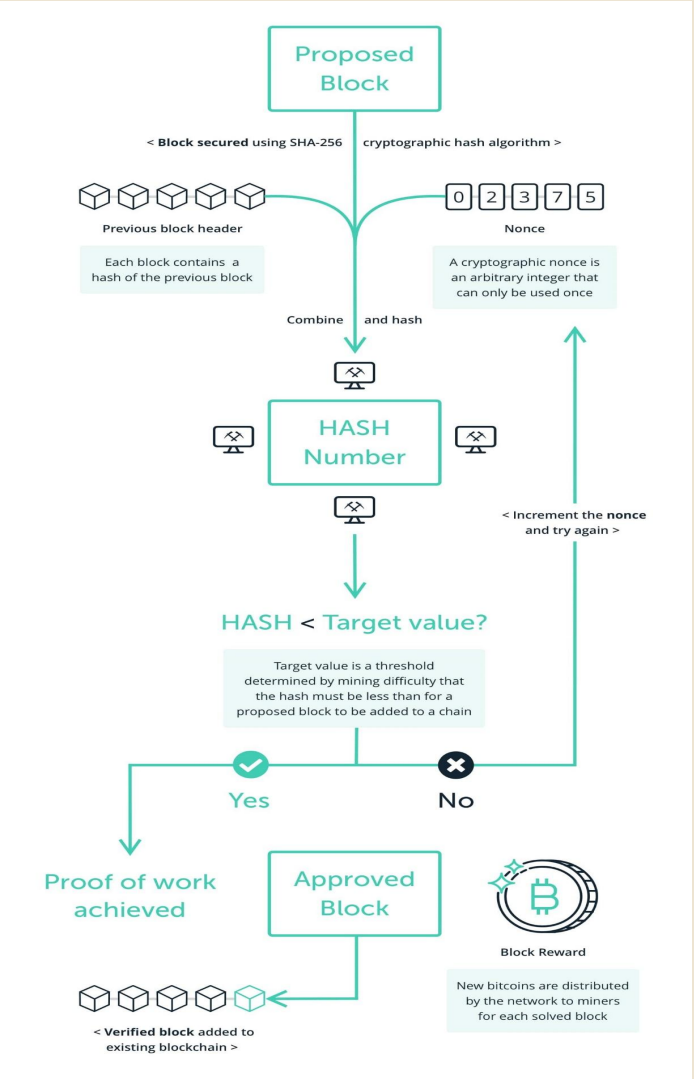
TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

In a blockchain, the consensus protocol predicts that 50 of those with 51% of the hashing power, or more than 50% of the hashing power, will win.

When the conflict is resolved, the "losing" block is "detached" and becomes an "**orphan block**".



Since the remuneration is contained within the block, the creator will lose the transaction. When a conflict appears, it is always better to wait for other blocks to be added, to make sure you add your own to the winning chain and don't lose the reward.

10"What is Proof of Work" Ledger Acedemy (2019)

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.

Thank you for the atention!

TRANSITION

Funded by the Erasmus+ Programme of the European Union

TRANSITION – Project Reference: 2019-1-MT01-KA202-051255
This project is funded by the European Union ERASMUS+ Program – Key Action 2 Cooperation for innovation and the exchange of good practices.