

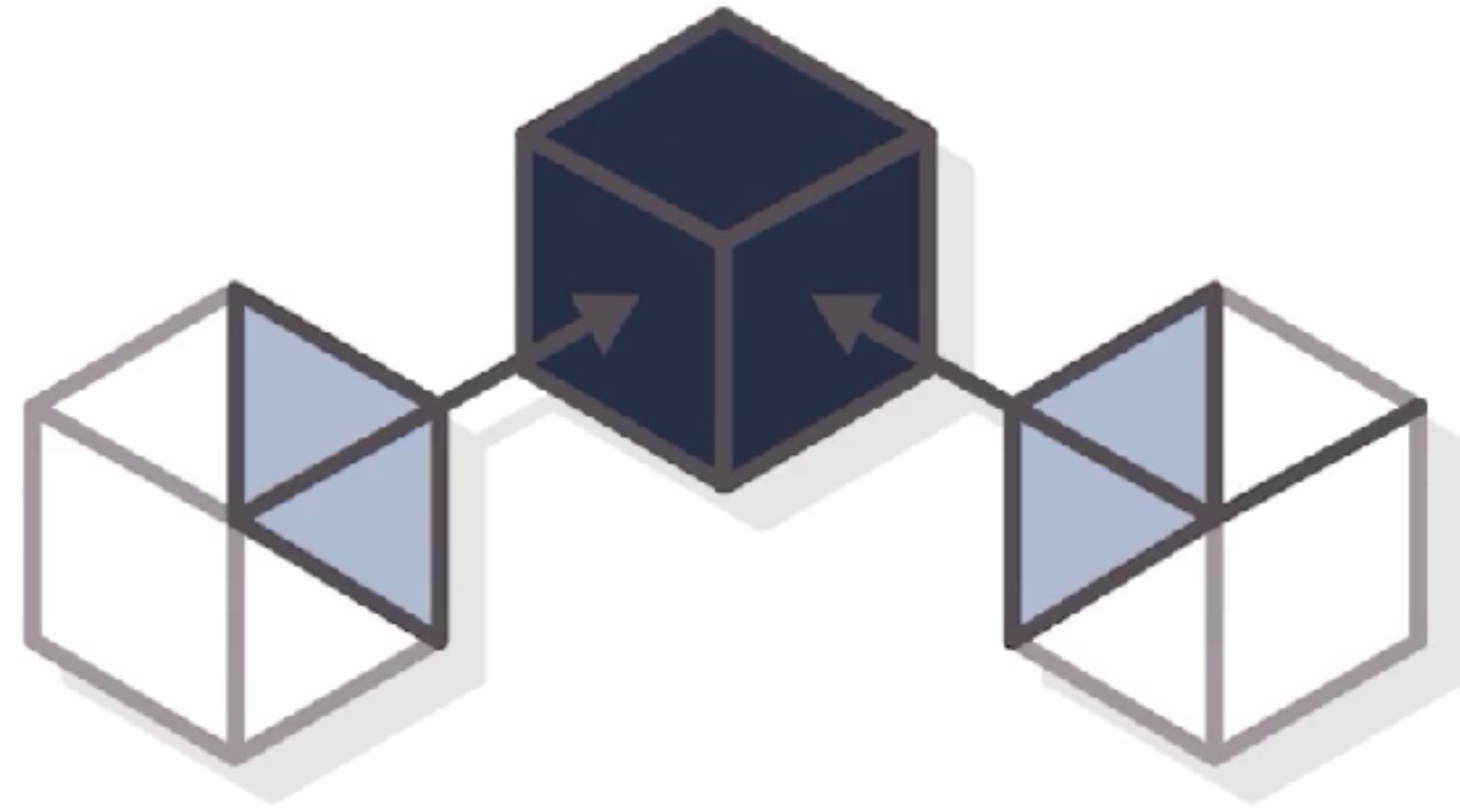
# Introduction To Blockchain

Distributed Systems

Faculty Of Information Systems



# WHAT IS BLOCKCHAIN?



Copyright © Blockchain Council

A graphic design for a presentation slide. At the top right is the Blockchain Council logo, which includes a blue cube icon and the text "Blockchain Council". Below the logo are several circular icons representing different cryptocurrencies: Bitcoin (top left), Litecoin (middle left), Ripple (top center), Cardano (bottom center), and Ethereum (middle right). A dark blue rectangular box with the text "Blockchain Technology" is positioned in the center. The background features a pattern of light blue and white triangles, creating a geometric, crystalline effect.

Blockchain is the technology which has gained popularity and huge interest from the advent of cryptocurrencies. Today, it is not only the backbone of the crypto industry, but is also growing in popularity, for storing, personal data, managing a digital asset, maintaining supply chain for enterprises and an empowering computer games in metaverse.



## Blockchain Technology

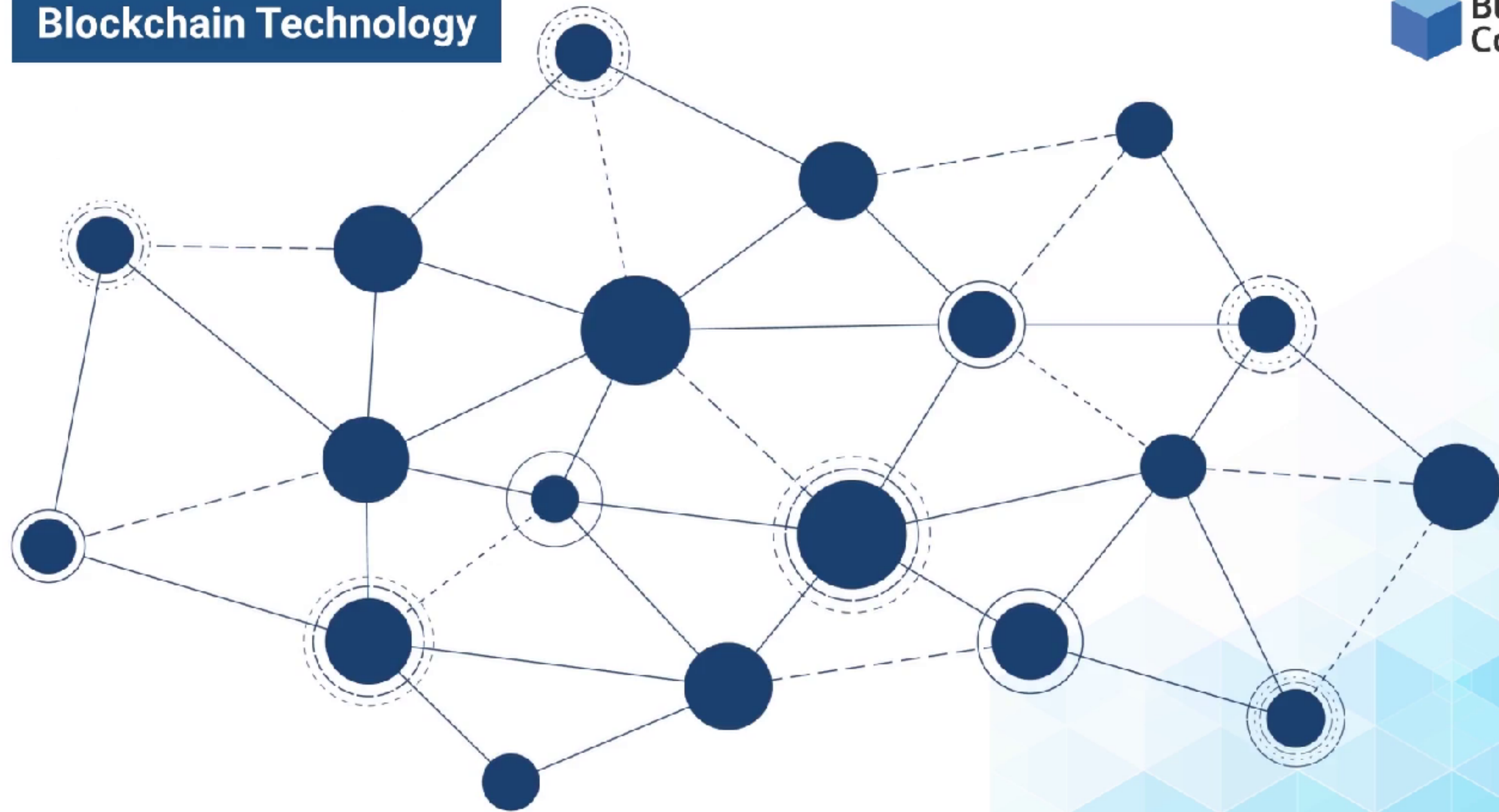
- Storing personal data
- Managing a digital asset
- Maintaining supply chain for enterprises
- Empowering computer games in Metaverse



But what is blockchain?

Let's discuss the technology in detail. As the name, suggests blockchain is a chain of data blocks. These blocks are stored on hundreds or thousands of computers distributed around the globe.

# Blockchain Technology



Copyright © Blockchain Council





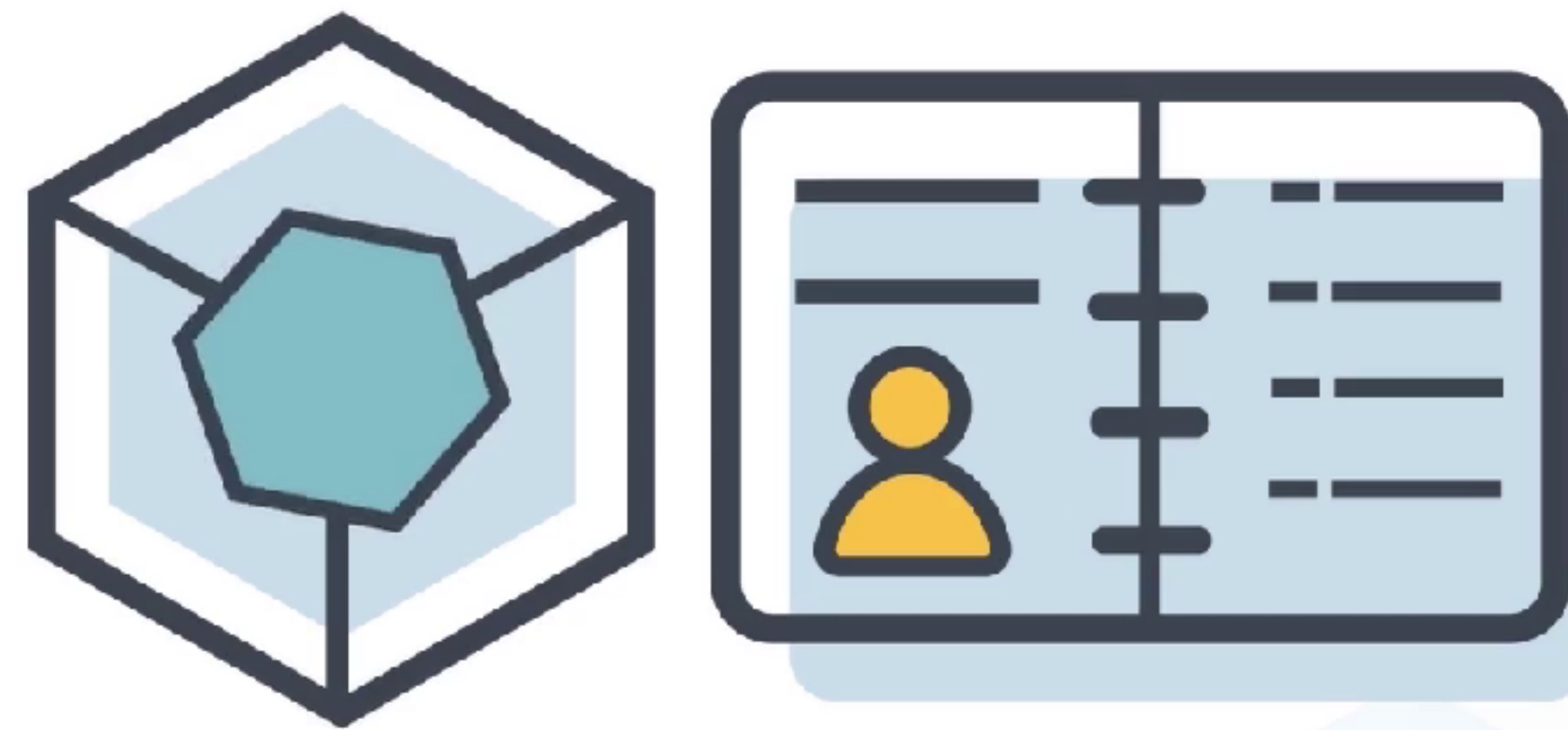


# Blockchain Technology



Basically blockchain is a digital Ledger which holds all the credits and debits of any digital asset.

# Blockchain Technology



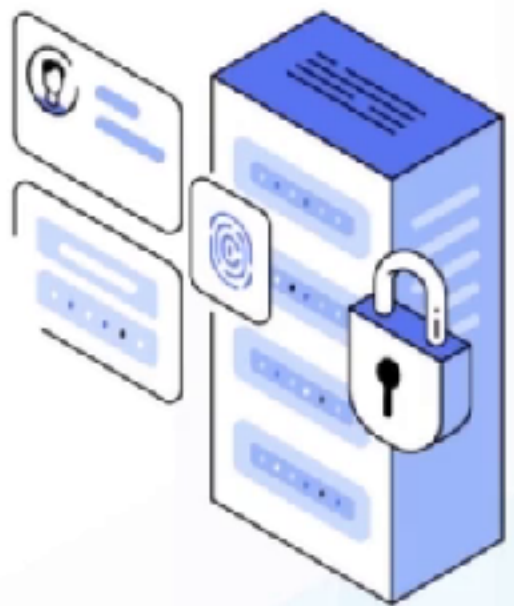


That digital asset can be a representation of any physical such as a pen, or a chair or digital such as virtual currency or data objects. Essentially all types of objects, be it physical, or synthetic, which have some value associated with them, can be represented as digital assets.

# Blockchain Technology



Physical Objects



Digital Objects

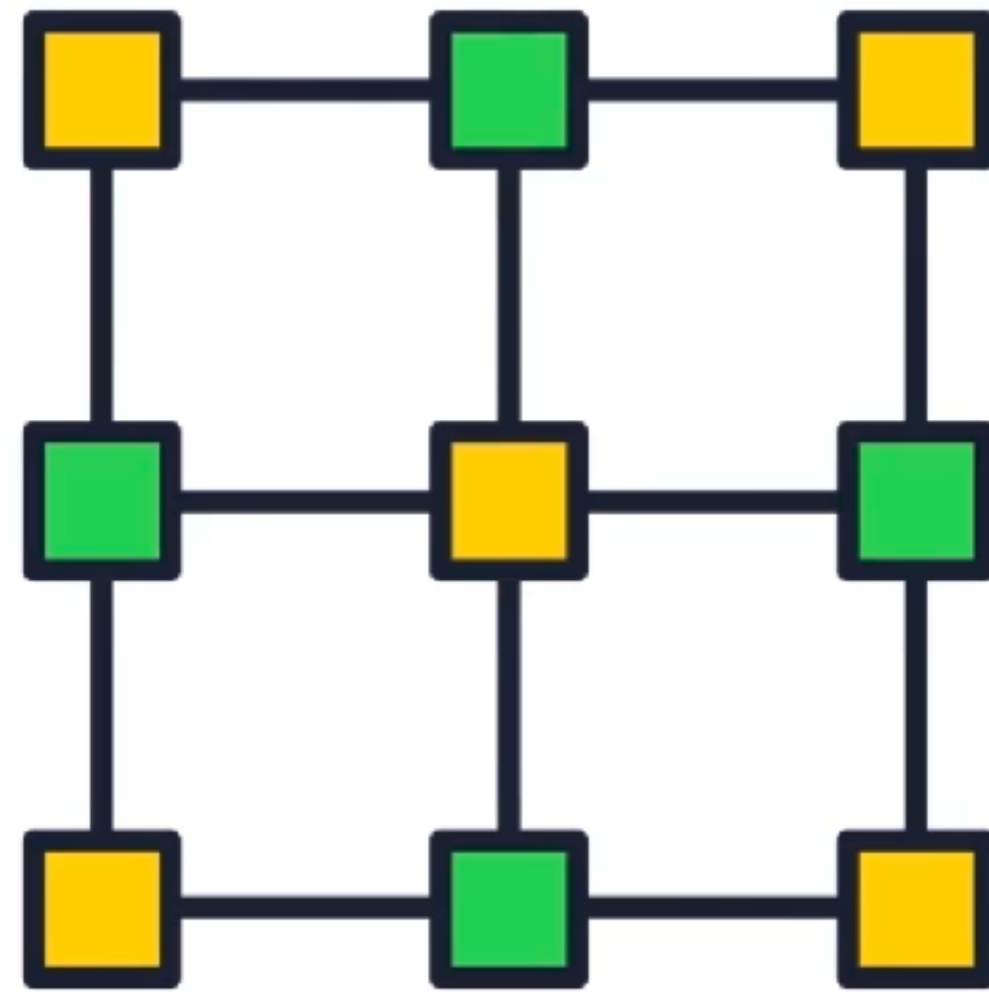
**Note** Whatever can be represented as a number can be treated as a digital asset.

Blockchain is a decentralised Ledger maintained and appeared as a peer to peer network that stores and tracks one or more digital assets. When we say a per to peer network, it means that decentralised network where all the network participants are connected in some way.

## Blockchain Technology



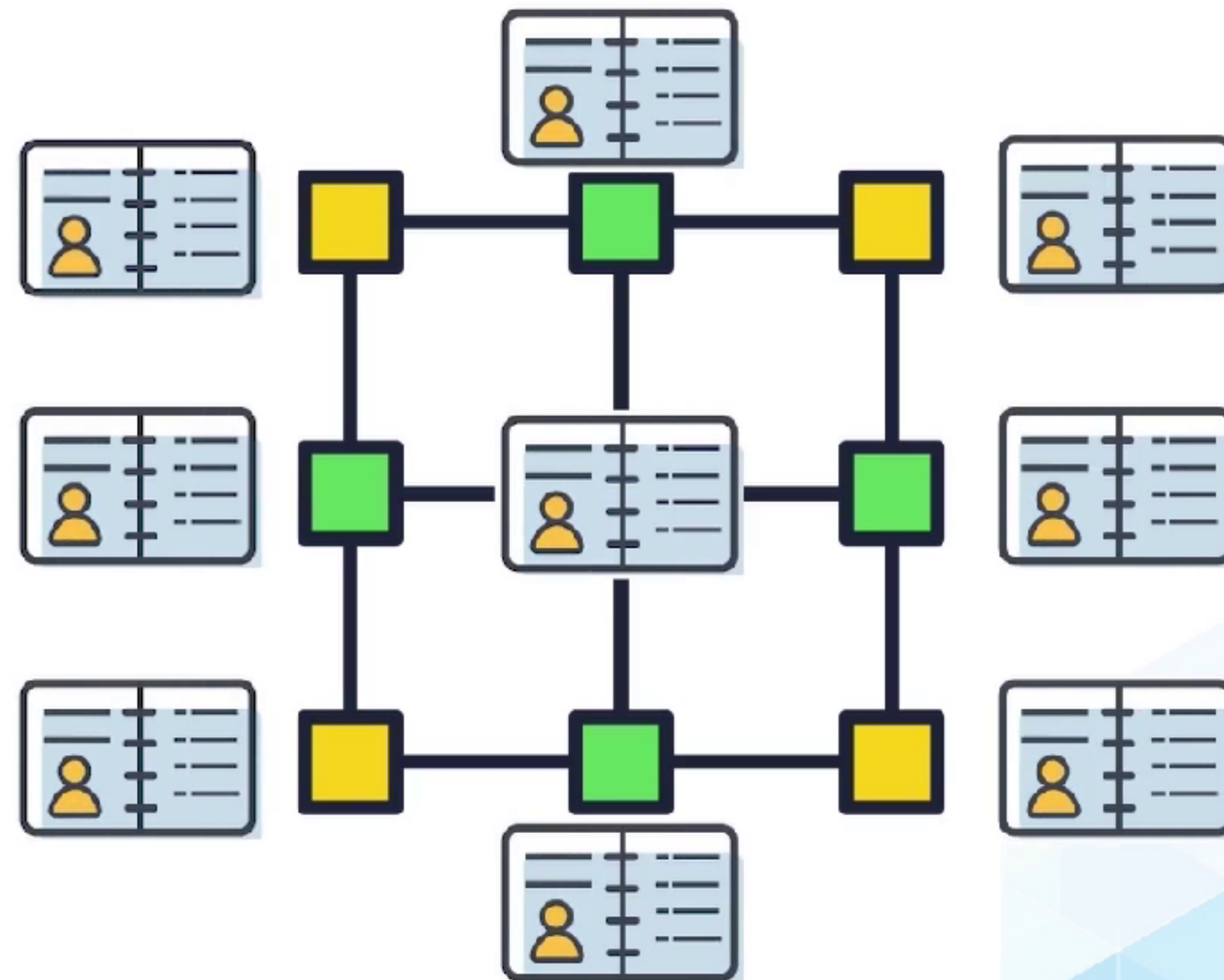
- Blockchain is based on decentralized technologies. This functions as a peer-to-peer (P2P) network.



In this network, each node maintains The Ledger. This Ledger can be compared to a bank account statement from Day Zero.

# Blockchain Technology

- Blockchain is based on decentralized technologies. This functions as a peer-to-peer (P2P) network.

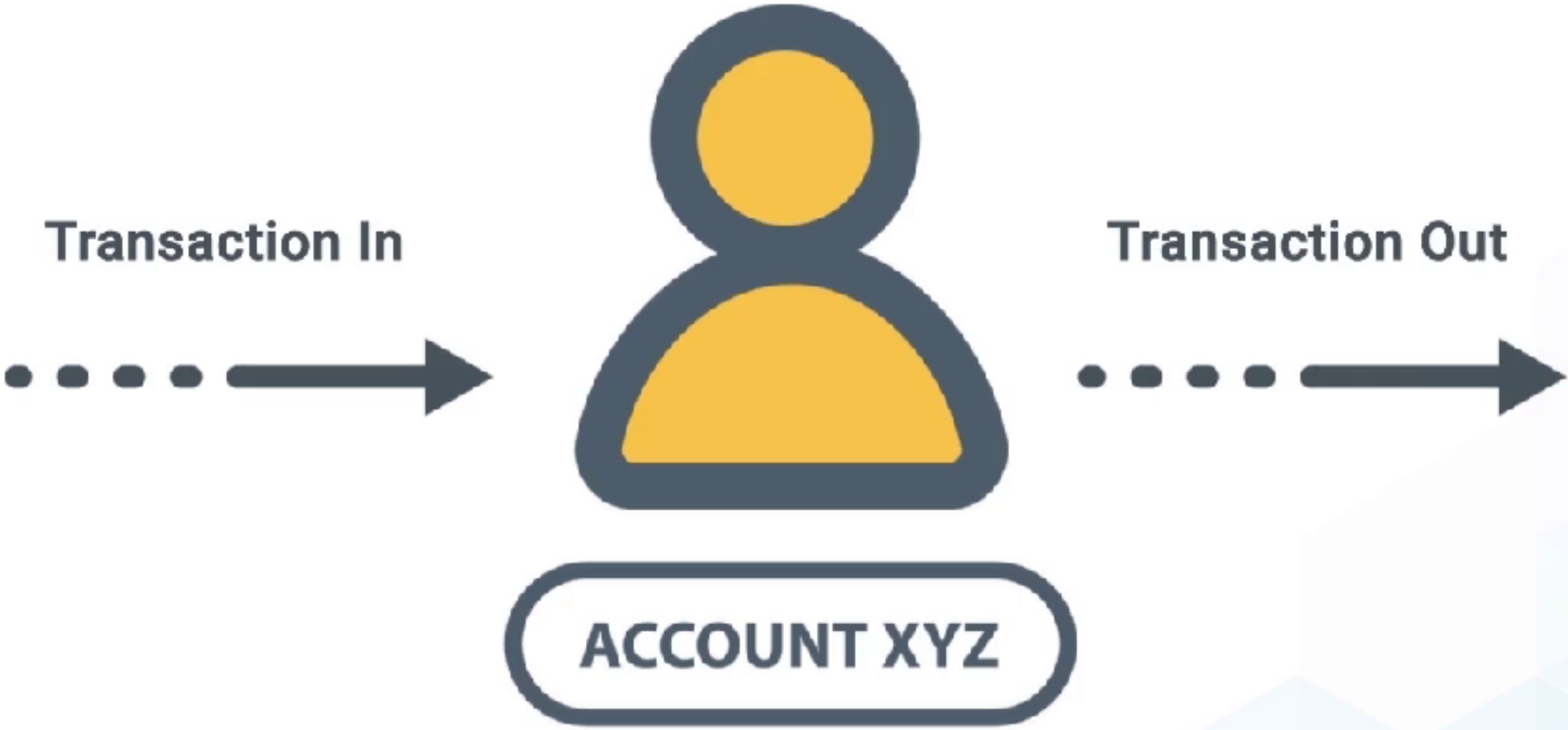




Let's say you open an account, then the ledger will keep track of every transaction in, and out of your account, from the day of the creation of the account.



# Blockchain Technology



Now, instead of storing this on a central server, the full ledger is saved to thousands of machines. Each transaction in this ledger can be verified at each machine independently and can be assessed if valid or not.

# Blockchain Technology

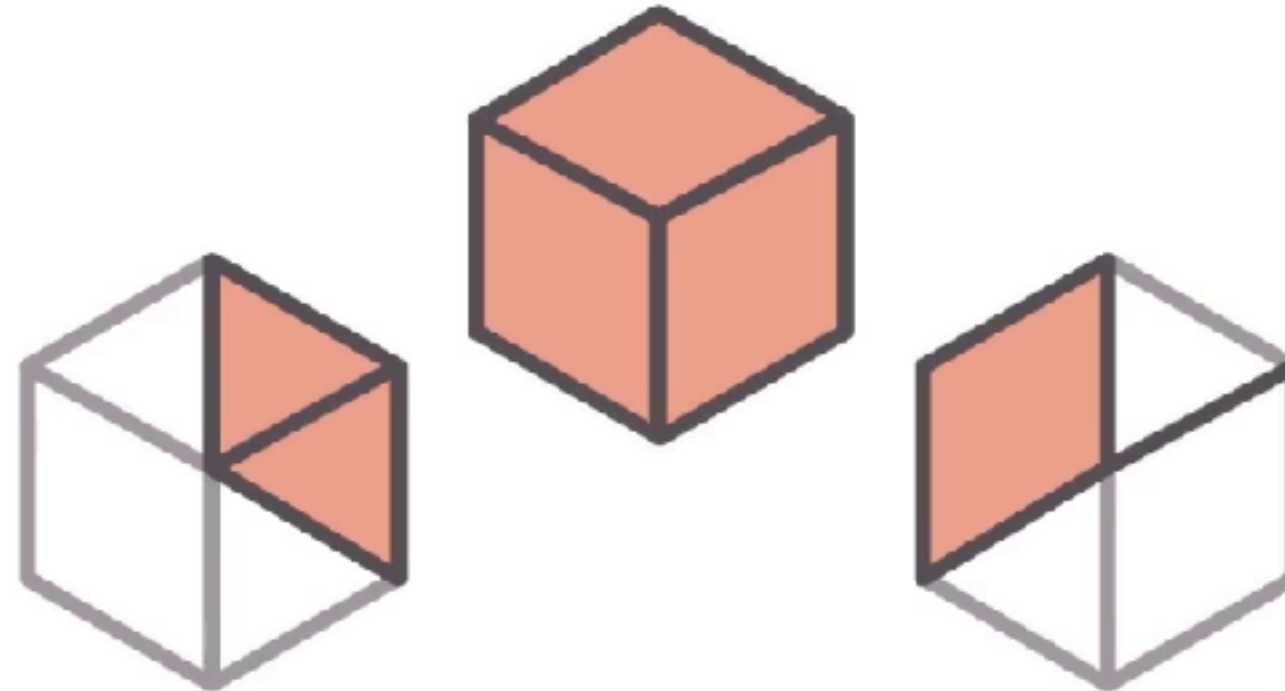


Each block in the blockchain stores information of all valid transactions like its date time, a month and accounts involved. Blocks, also consist of information about parties involved in transactions, and the information that distinguishes them from other blocks more like a unique code known as a hash that allows us to tell it apart from every other block, these hashes are cryptographic codes created by a special algorithms.

# Blockchain Technology

Hash: #####  
Date : 23-02-2021  
Time : 10:27  
Amount : xxx

Party Involved : y  
XXX934352DATA1



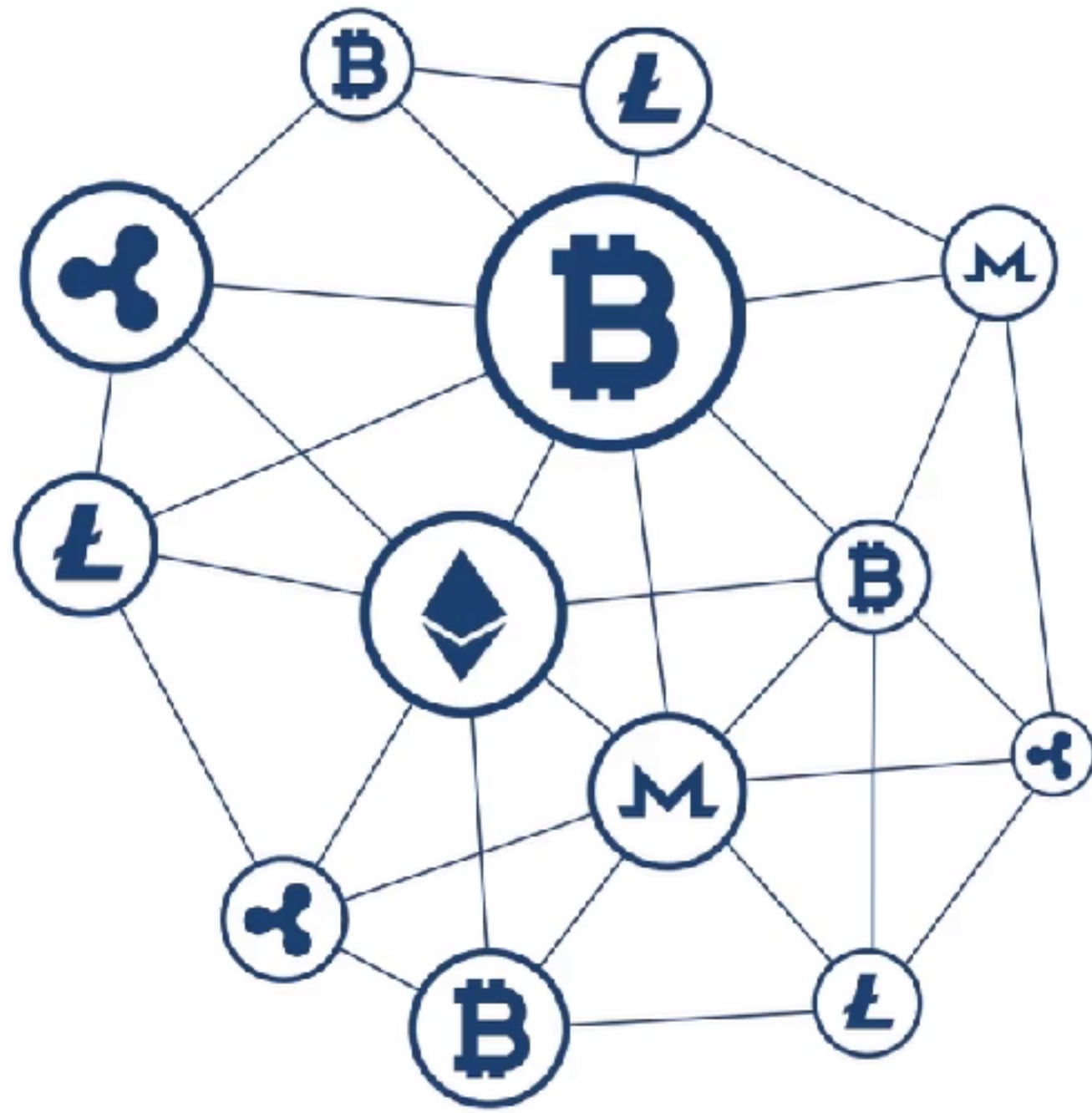
XXX9343GFGATA5  
Party Involved : x  
Hash: #####

Hash: #####  
XXXX96783GKGAFR9  
Date : 23-02-2021  
Time : 10:27  
Amount : xxx


You might be wondering what is the relation between blockchain and cryptocurrencies? Blockchain is related to cryptocurrency but it is not a cryptocurrency. In fact, cryptocurrencies are nothing but digital tokens to find as numbers in the blockchain which are tracked from Day Zero.



## Blockchain Technology



Copyright © Blockchain Council

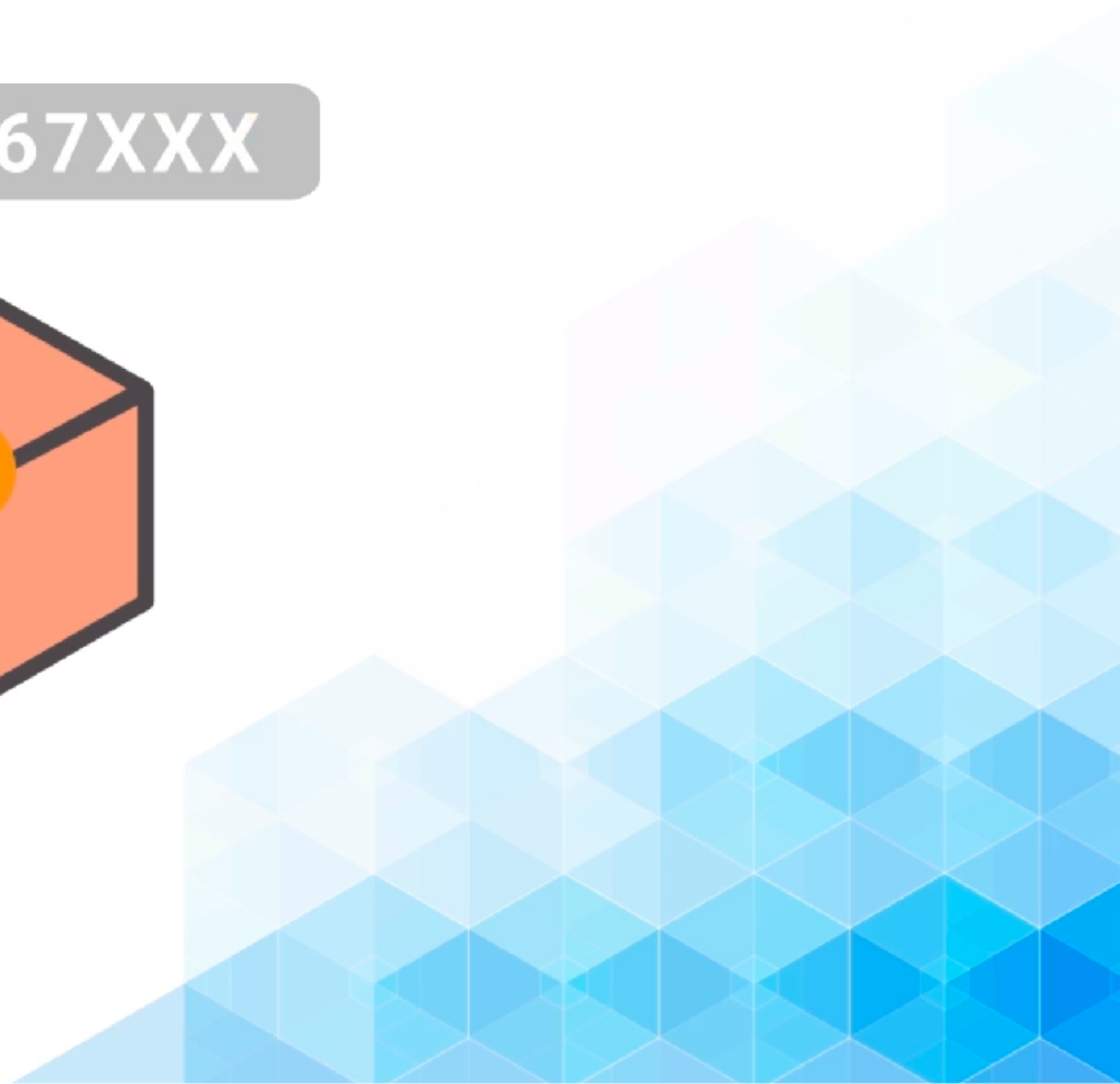
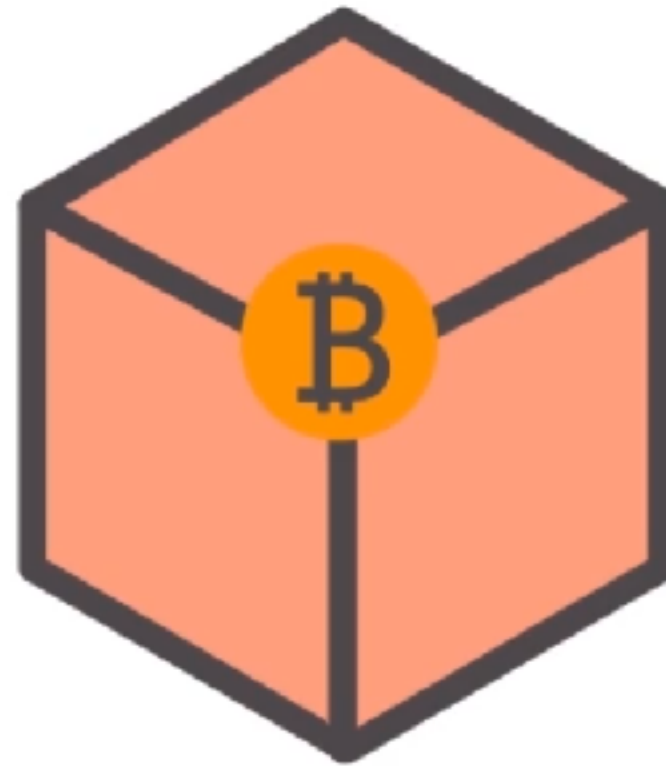
 Blockchain is related to cryptocurrency, but it is not a cryptocurrency.



To understand this, let's take Bitcoins for example, Bitcoins are just numbers which are stored in a blockchain Ledger in which have been tracked since day zero. People need that digital number because there can be only one copy of it which reflects the fundamental nature of the currency.

# Blockchain Technology

X1234567XXX



# What is the relation between blockchain and cryptocurrencies?

Let's say A has 100 Bitcoins, and B has zero. A transfers 50 Bitcoins to B then A no longer has 100 coins because the Ledger gets updated and it will remove 50 coins from A's balance and add 50 coins to B's balance creating a single secure copy.

# Blockchain Technology



₿ 100



₿ 0

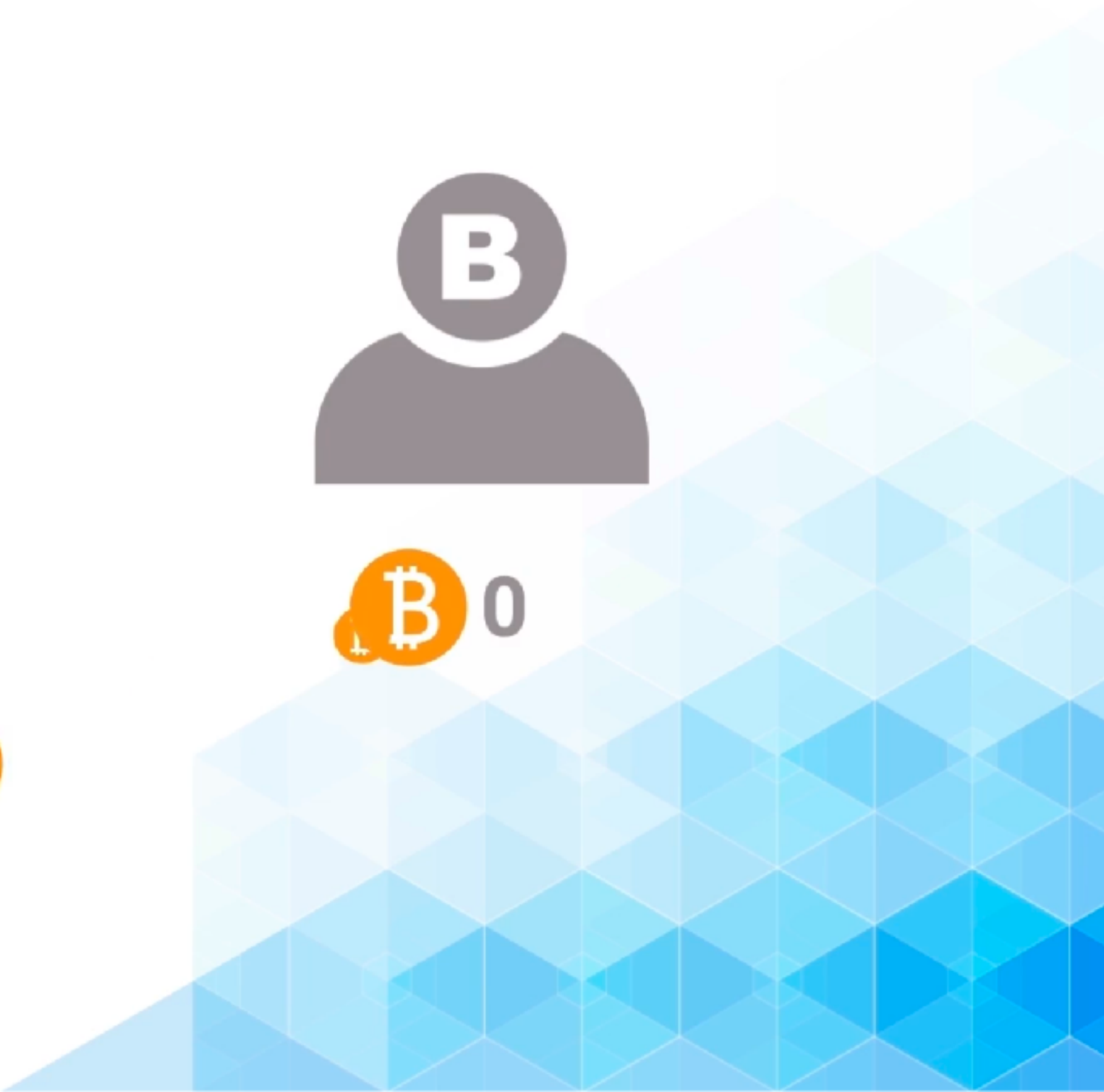
# Blockchain Technology



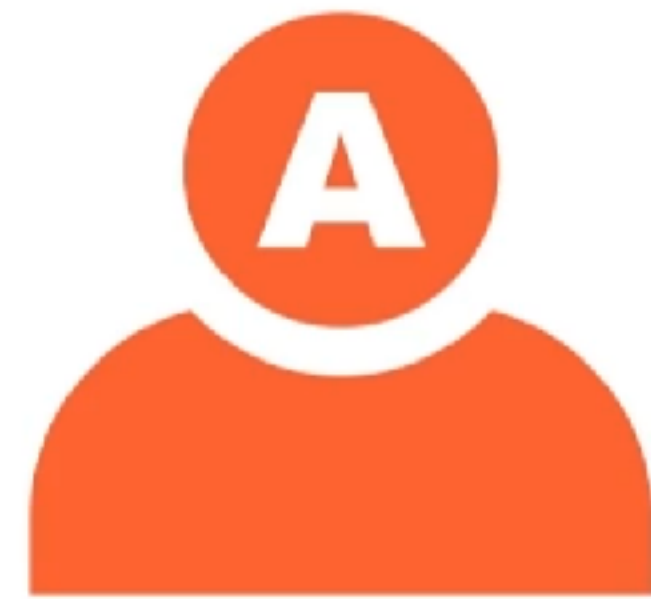
₿ 100



₿ 0



# Blockchain Technology



₿ 50



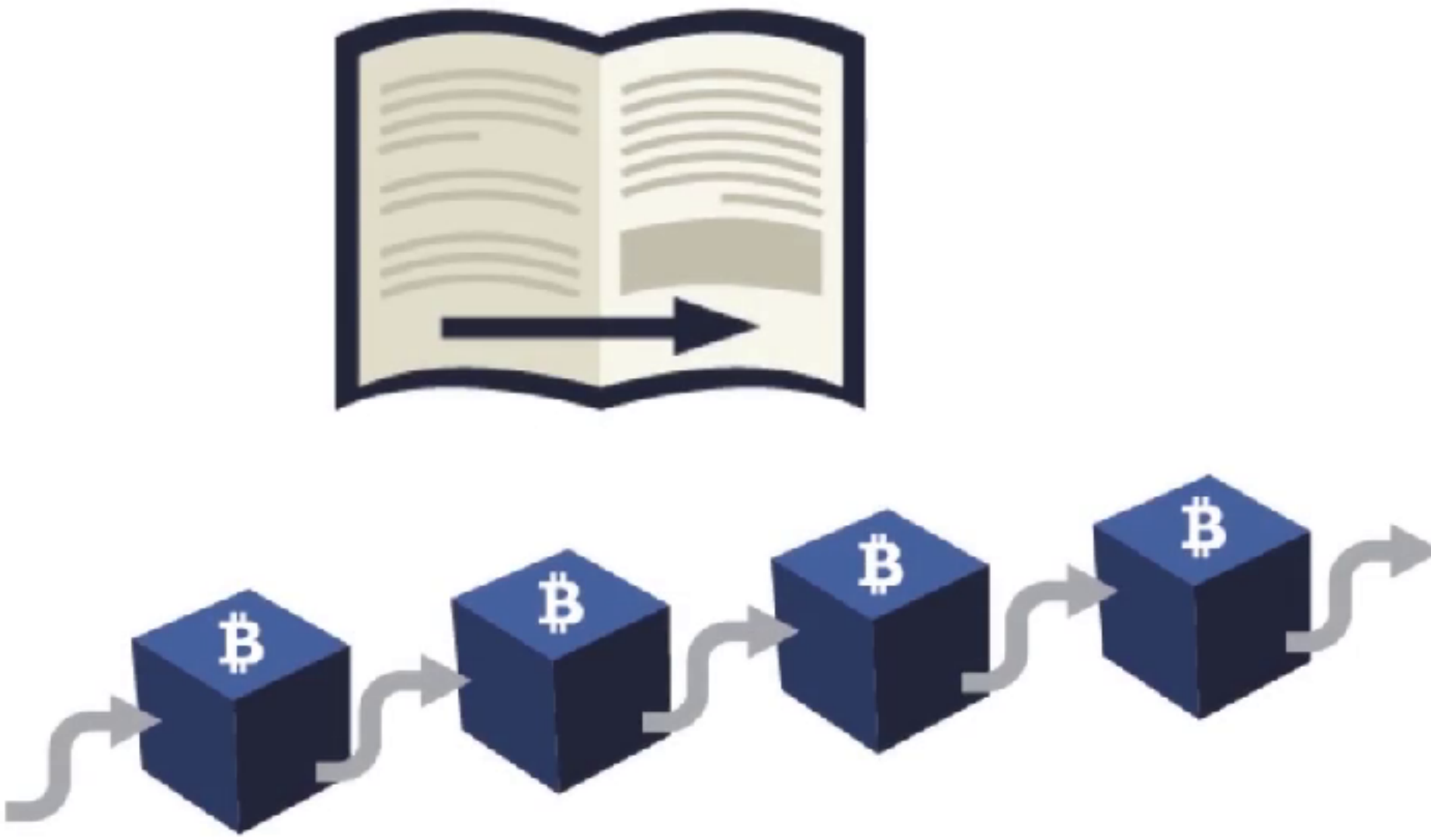
₿ 50



# Blockchain Technology



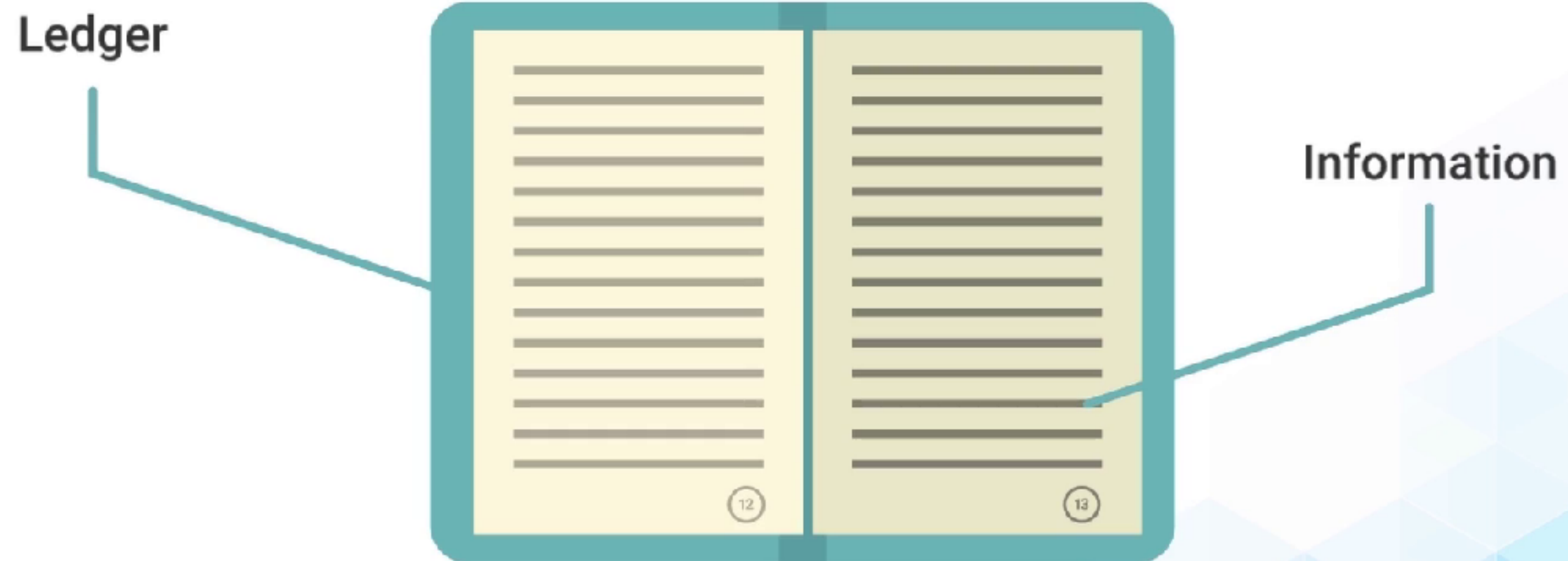




## Understanding the Book Analogy

In a traditional system, a physical Ledger is in the form of a book where each page contains the information as lines on pages. Likewise, let's imagine a book as a kind of rudimentary blockchain where the pages represent, blocks in each page is connected to every other page through a page number.

# Understanding the Book Analogy



# Understanding the Book Analogy



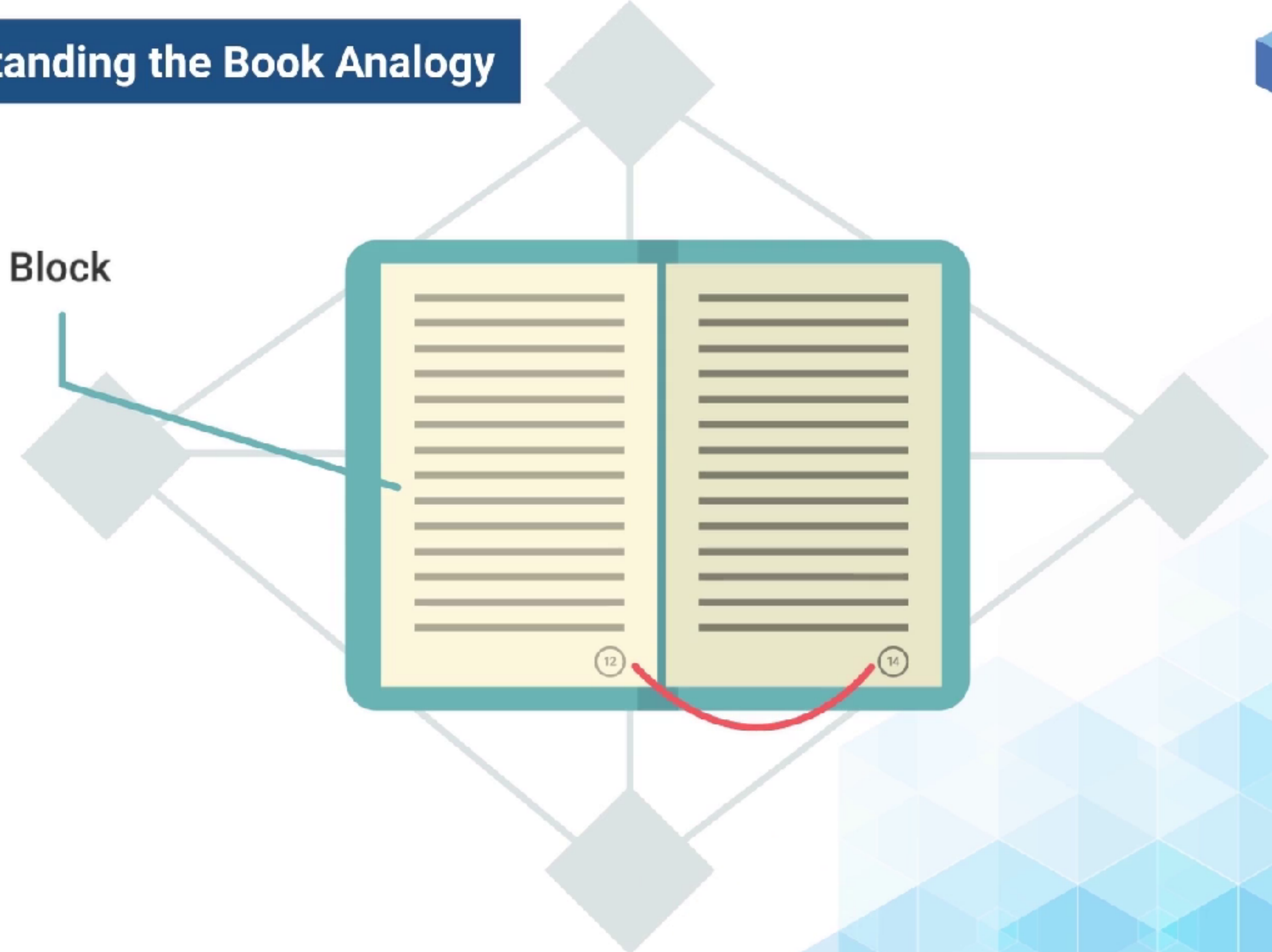
In a book, all pages are in a particular order. That's why if someone tampers with a specific page or removes any page, it can easily be noted since the pages are numbered and are connected to each other in a particular order.

# Understanding the Book Analogy





# Understanding the Book Analogy



Copyright © Blockchain Council



## Understanding the Book Analogy

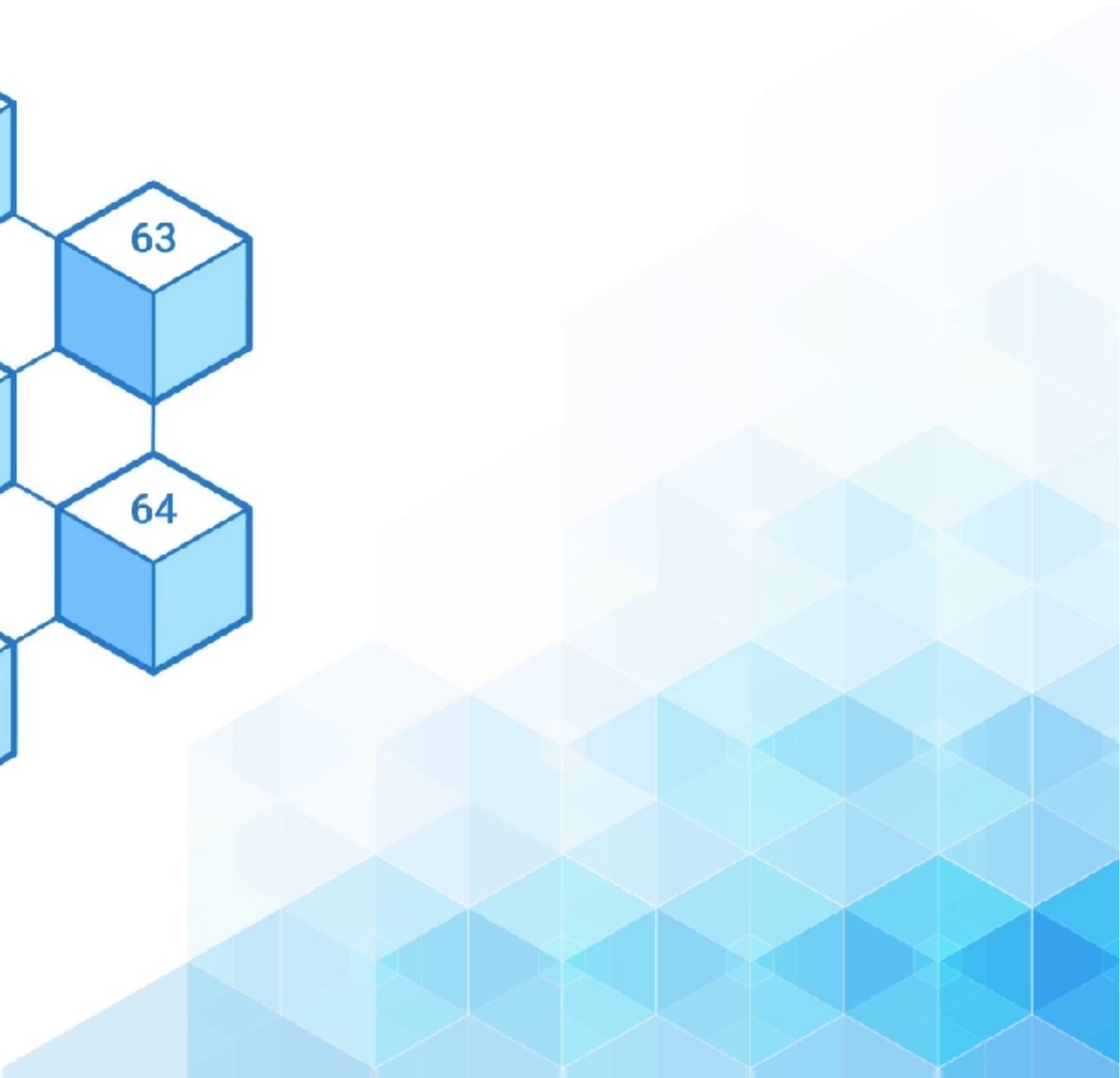
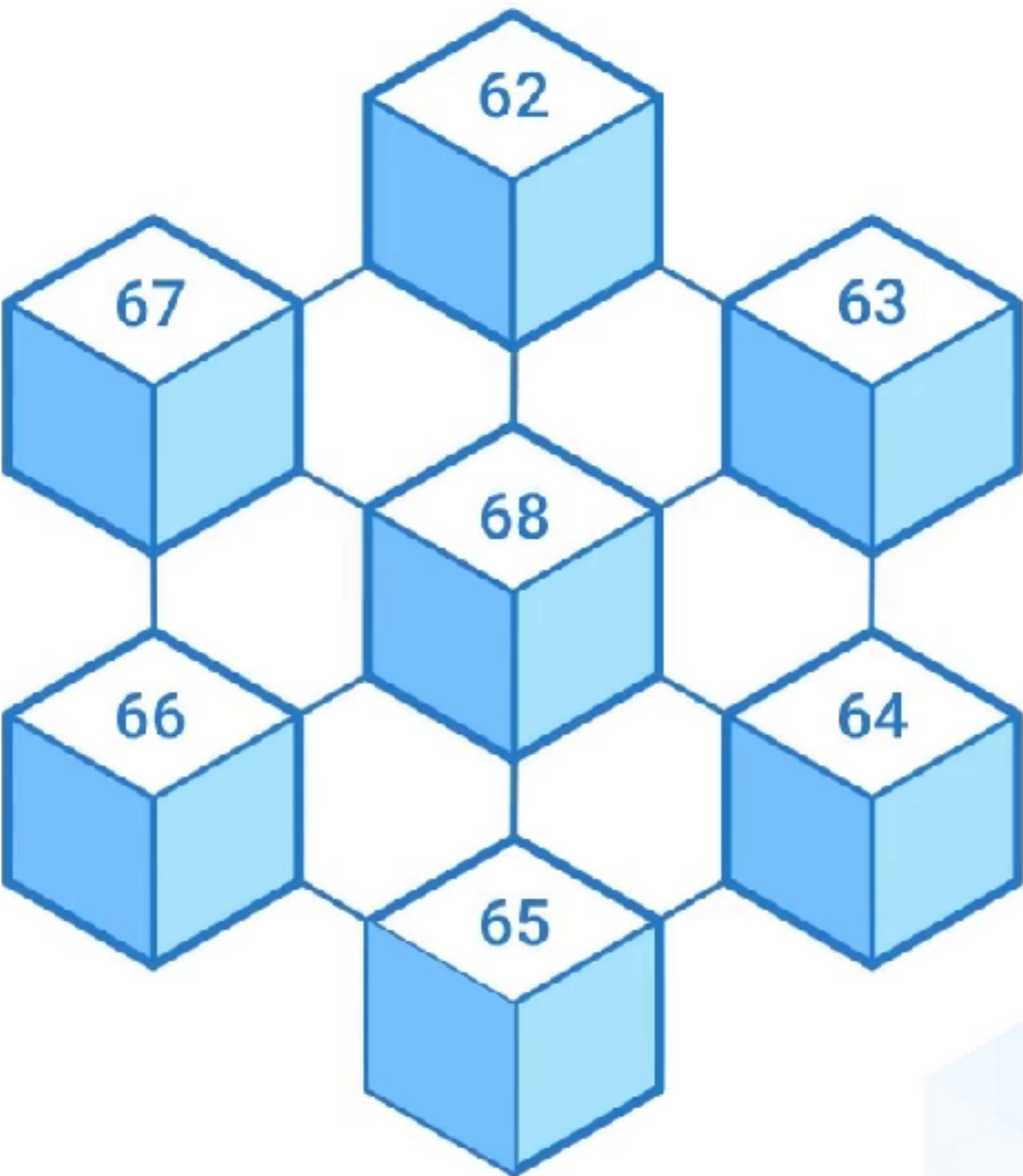


12

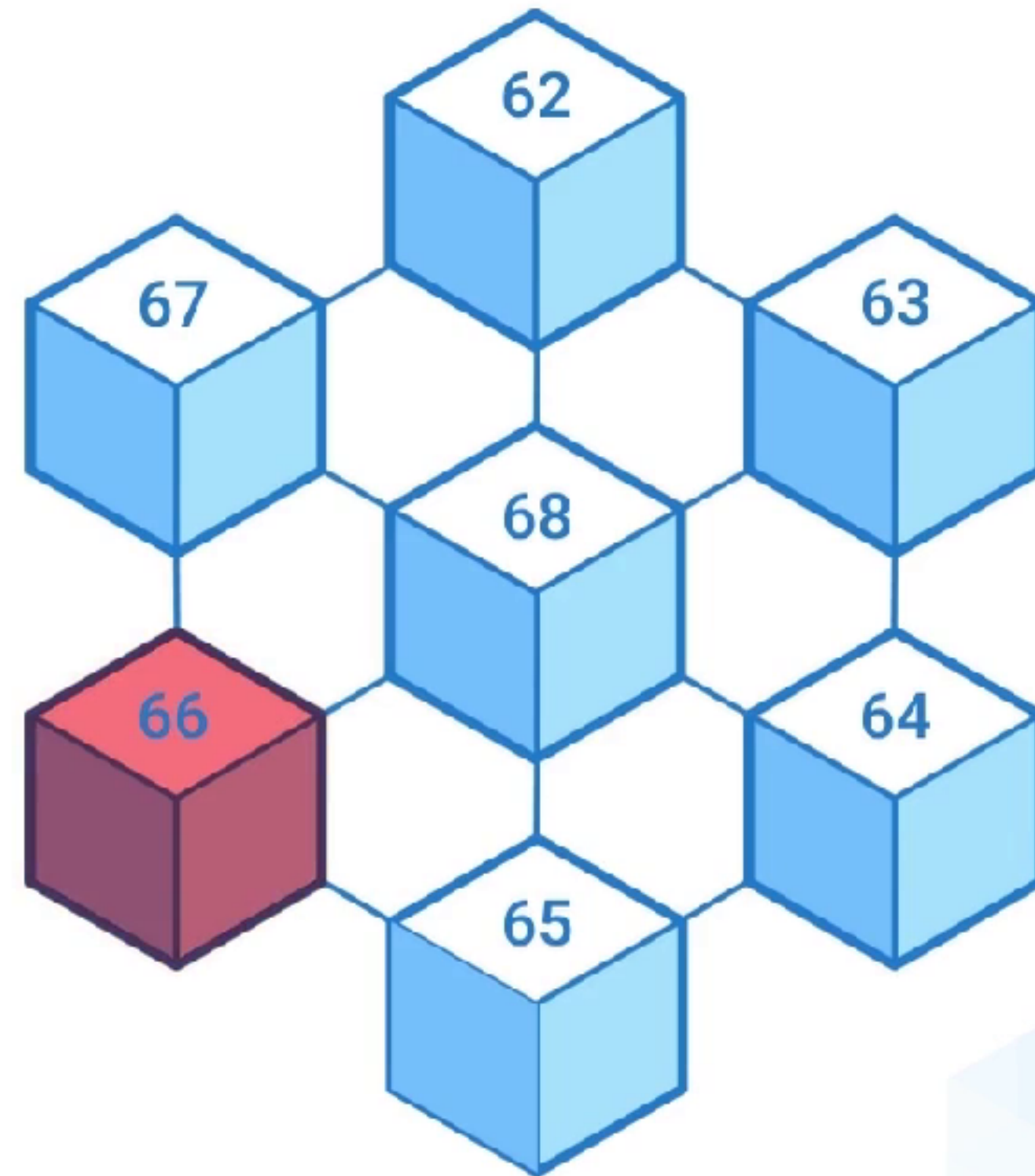
14

It is also easy to arrange the pages or the blocks in order, and then identify any suspicious activity. This makes page number significant in a legal agreement or in an MOU as it helps the reader to understand if there is a page missing in the entire agreement. It is obvious that changing or removing a page can change the meaning of the whole agreement. And this is very important in a ledger, as well. Removal of a page in a ledger can corrupt the entire Ledger very easily.

# Understanding the Book Analogy



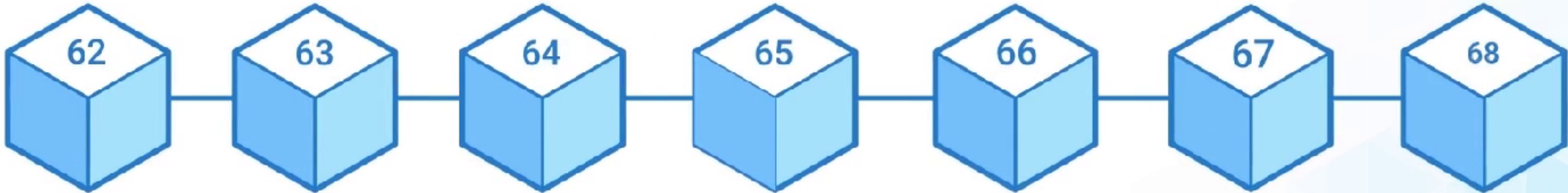
# Understanding the Book Analogy



If we have an account statement that has 100 Pages, and if someone removes page number, let's say 65 then, we can quickly identify this because the record will not be complete.



# Understanding the Book Analogy





# Understanding the Book Analogy



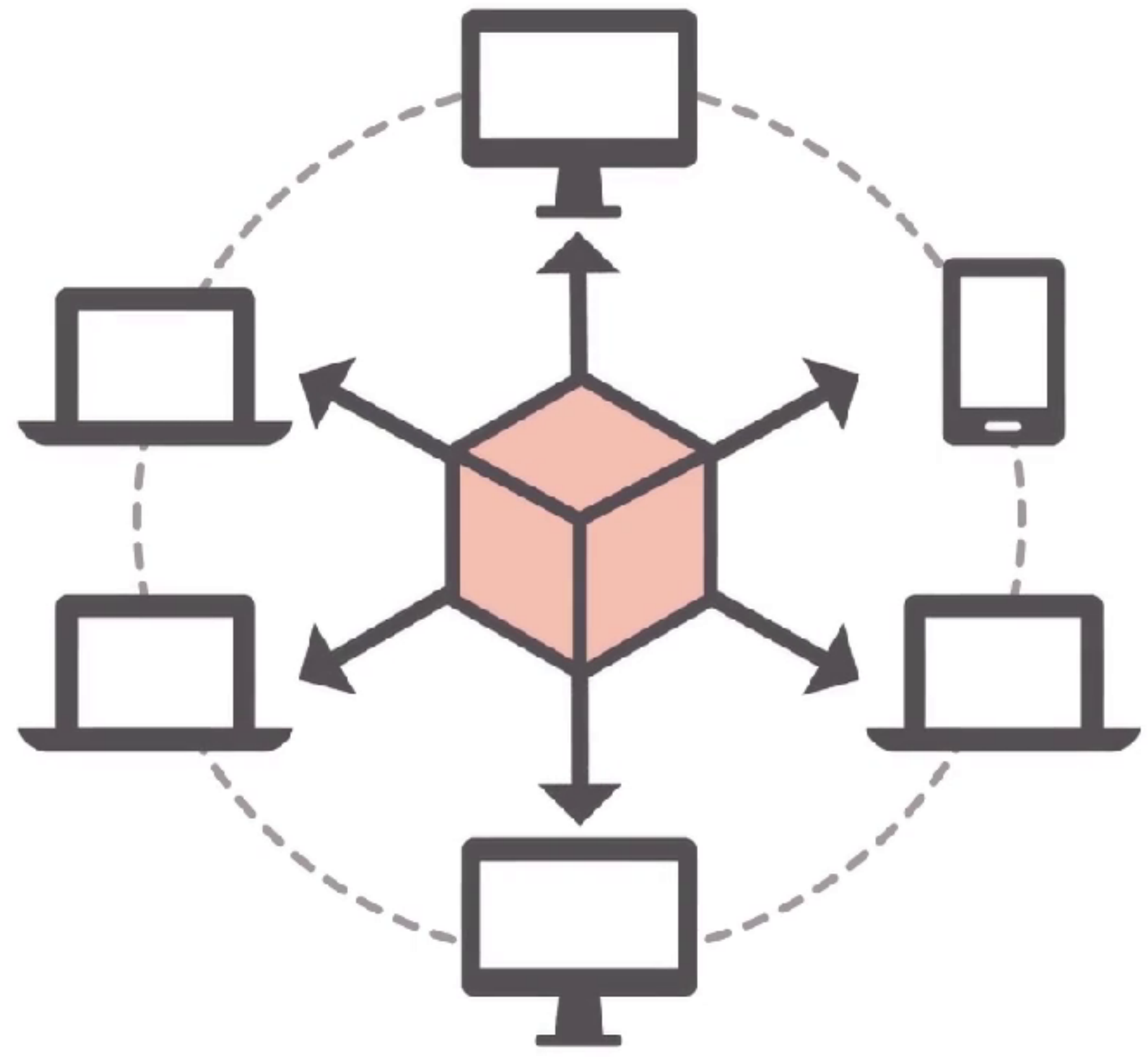
If you compare blockchain to a book, you can find that the whole blockchain is equivalent to the book of which each block is the same as a page, and each transaction in a block, is the same as an entry on each page of the book. Blockchains record every credit and debit of the asset in the form of transactions and store a set of these transactions in a block such that any detail once approved cannot be altered without informing every one of the network. This is made possible by connecting each block to the previous block.

## Understanding the Book Analogy



**"Book = Blockchain, Page = Block, An entry in page = Blockchain Transaction"**

- Each page refers to a block connected to the previous page through a page number.
- It is easy to detect if a page/block has been removed or deleted.
- It is easy to arrange the pages/blocks and identify suspicious activity, because of the page number.
- It is impossible to tamper a previous entry in the ledger without someone noticing it, as the pages/blocks are built tightly on top of each other.



## History of Blockchain

Blockchain was invented by a pseudonym person or a group of people known as a Satoshi Nakamoto, when he released the white paper of Bitcoin named Bitcoin a peer to peer electronic cash system.

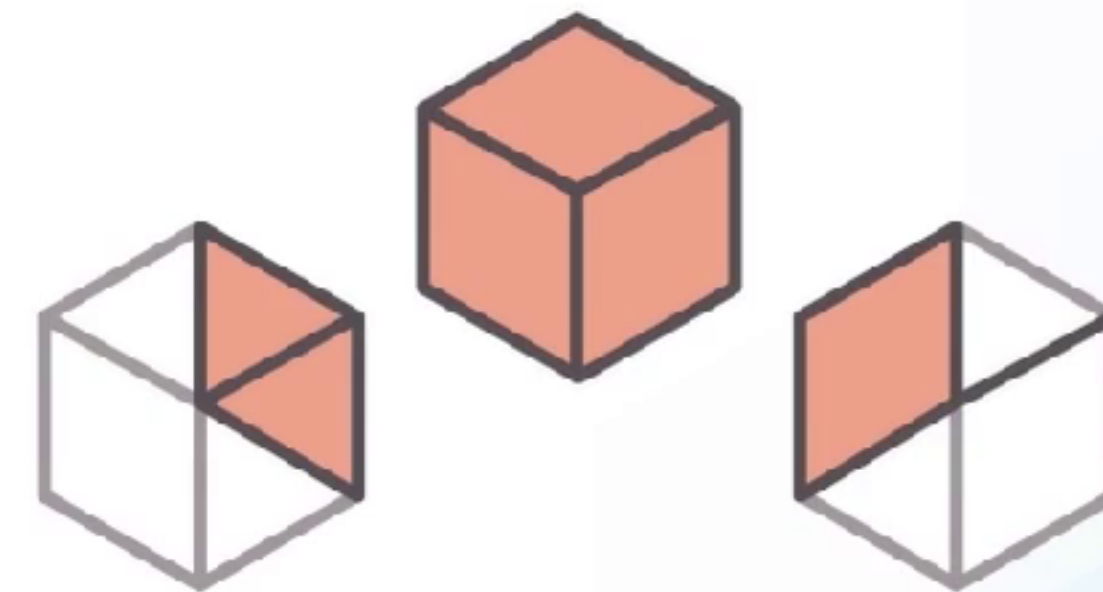


## History of Blockchain

- In 2008, the blockchain system was conceptualized and introduced by an individual or a community known by the name 'Satoshi Nakamoto.'



**Satoshi Nakamoto**

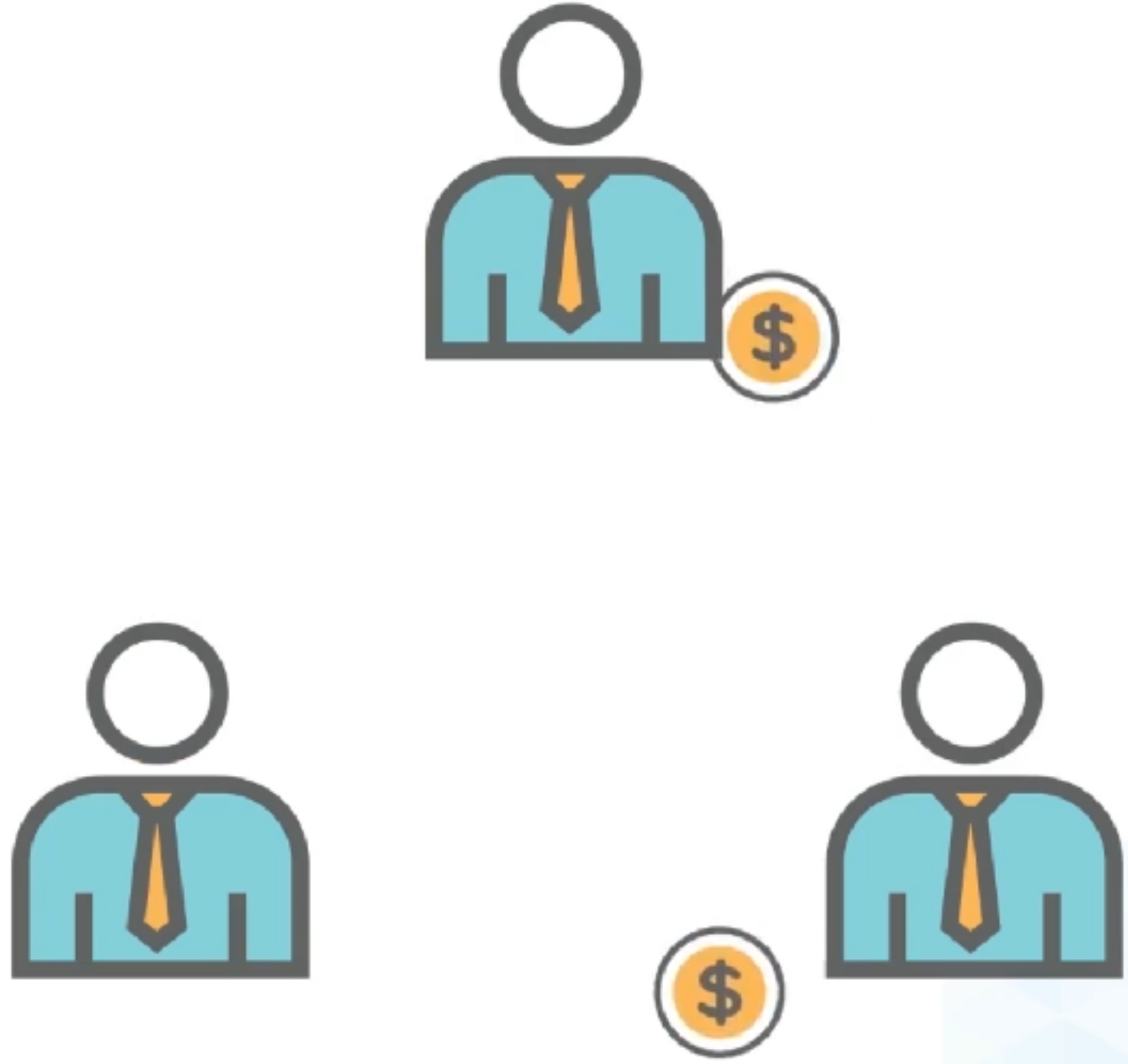


**Bitcoin: A Peer-to-Peer Electronic Cash System**



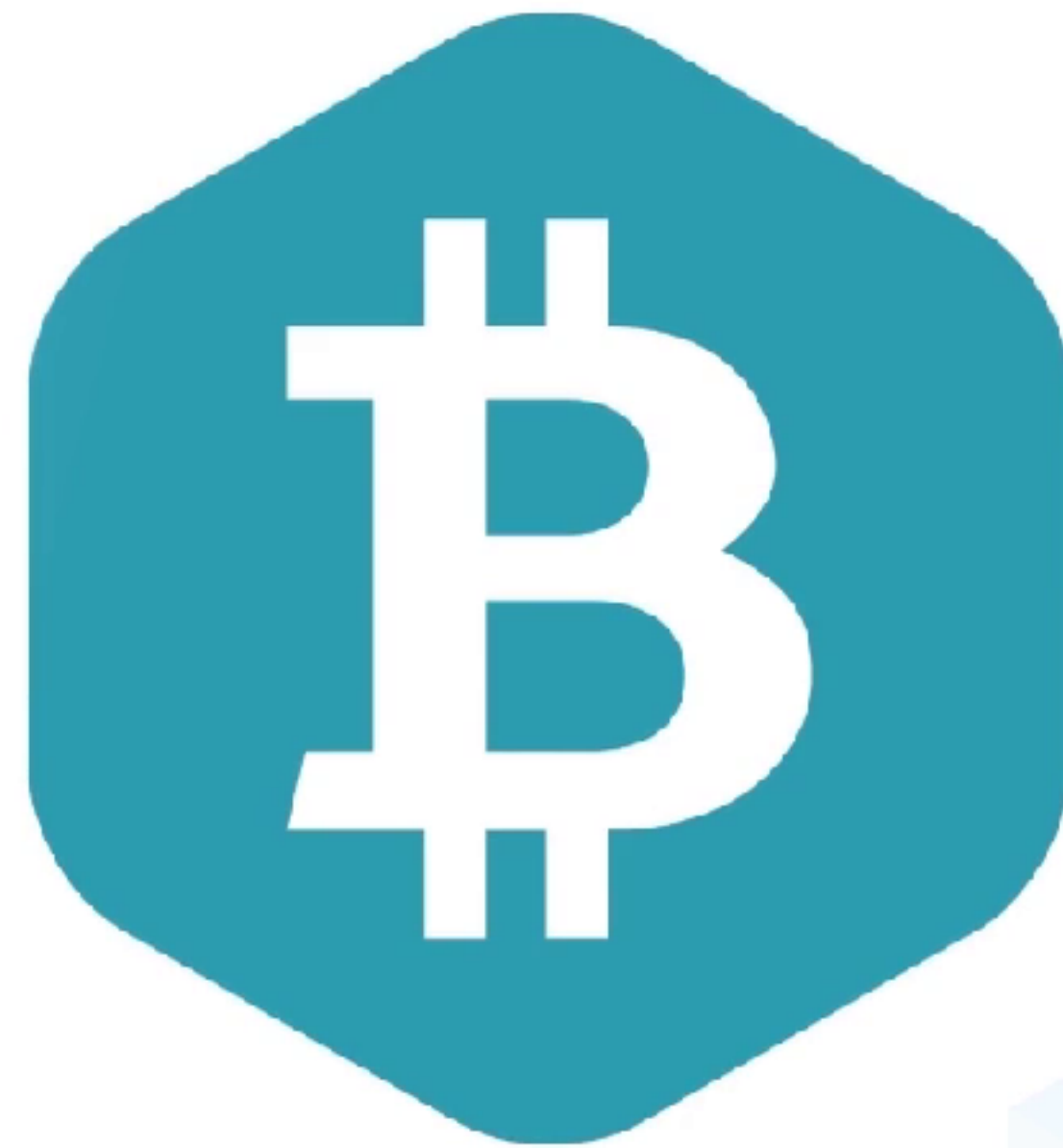
It was then everyone came to know about the form of cash that could be sent on a decentralised peer-to-peer Network without the need for any Central Bank or other authority to operate and maintain the Ledger, much as how physical cash can be.

# History of Blockchain



Although it was not the first decentralised currency that was proposed. This proposal solves several problems that this field was already facing in the past, and it is safe to say that Bitcoin is the most successful digital currency till now.

# History of Blockchain



Let us quickly go through some of the alternatives proposed in the past. First in 1991, two cryptographers named Stuart Haber and W. Scott Stornetta proposed the secured chain of blocks. After a few years in 1998, a computer scientist, Nick Szabo proposed the first digital currency BitGold, which used cryptography and hashing to store transactions digitally. Later in 2008 Nakamoto introduced hashing in blockchain, keeping the system secure and immutable data on the blockchain then was impossible to alter.



## History of Blockchain

- W. Scott Stornetta and Stuart Haber in 1991, proposed the concept of a secured chain of blocks (set of records).



**Nick Szabo**

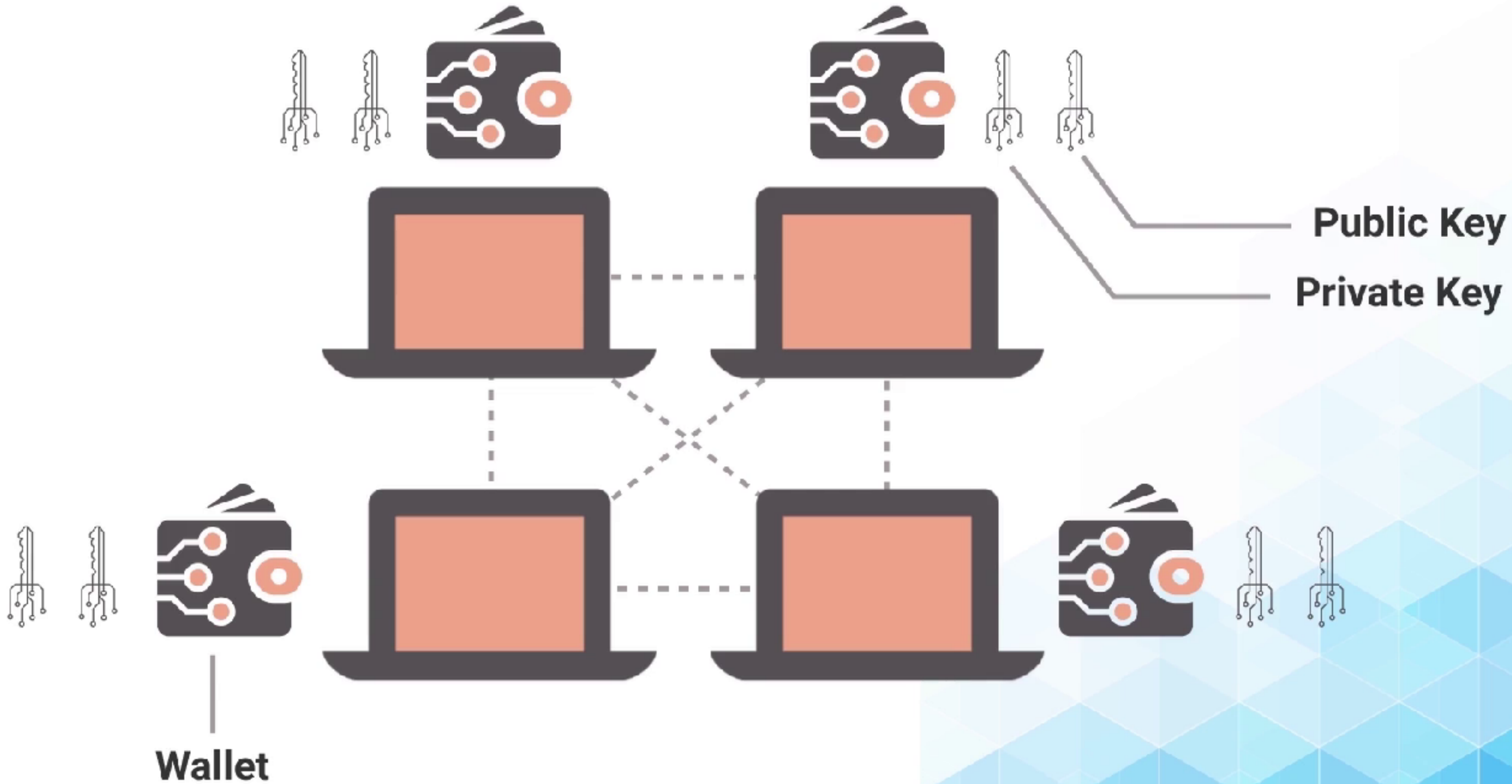
 BitGold<sup>™</sup>

- Satoshi Nakamoto implemented the idea of using hashing in the blockchain framework to make it so safe that once saved in the blockchain, no one can make modifications or erase the data.

# How does Blockchain works?

We can define the blockchain as a system that allows a group of connected computers to maintain a single updated and secure Ledger. Now, if users want to send or receive any asset on the network, they will require a wallet. It is a software that saved your private keys and lets you store send and receive Bitcoins. Each user has a unique pair of cryptographically generated, and connected Keys to private in a public key. While the public key is known in the network, the private key is stored in the wallet, it allows only the user to be able to spend their Bitcoins.

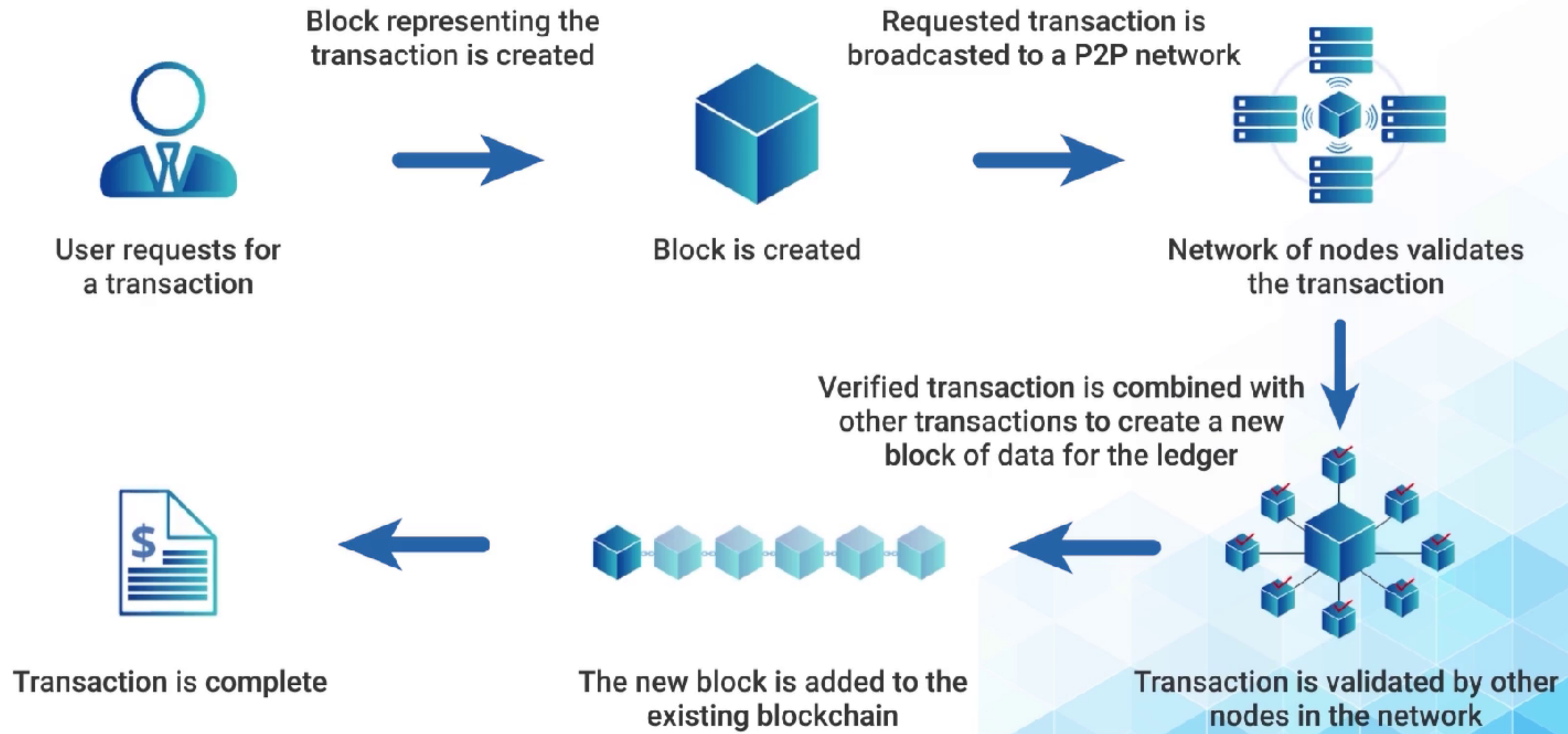
# How does Blockchain works?



Now, users will create transactions. A block is created that stores these transactions. Each of these blocks of data is cryptographically secured and linked to the previous ones. Once the block is created, it is broadcasted in the peer to peer network to other nodes. Nodes present in the network then validate the block along with all the transactions it holds. Once it is verified, it is appended on top of the existing Blockchain. A transaction is thus made permanent and unalterable in the Blockchain. A transaction can be a simple transfer of cryptocurrency from one user to another. It can also be creating a new contract to ensure some rules.



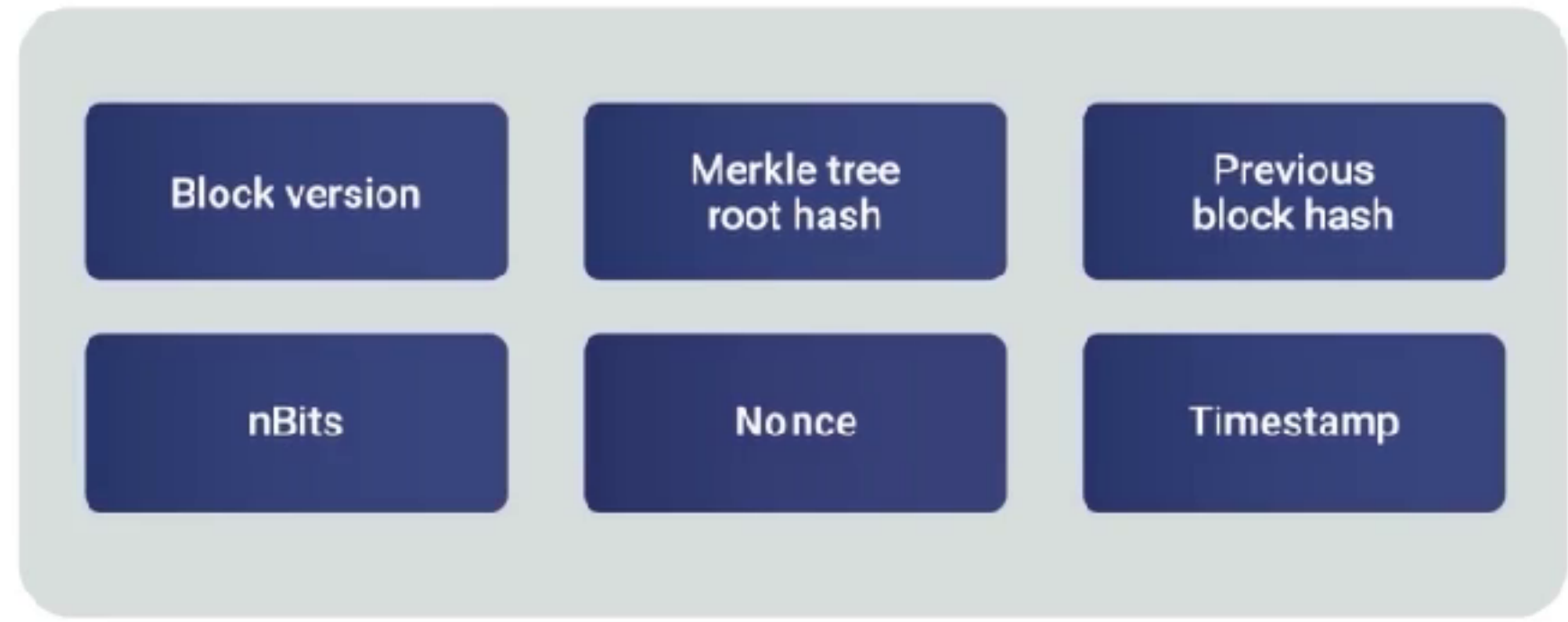
# How does Blockchain works?



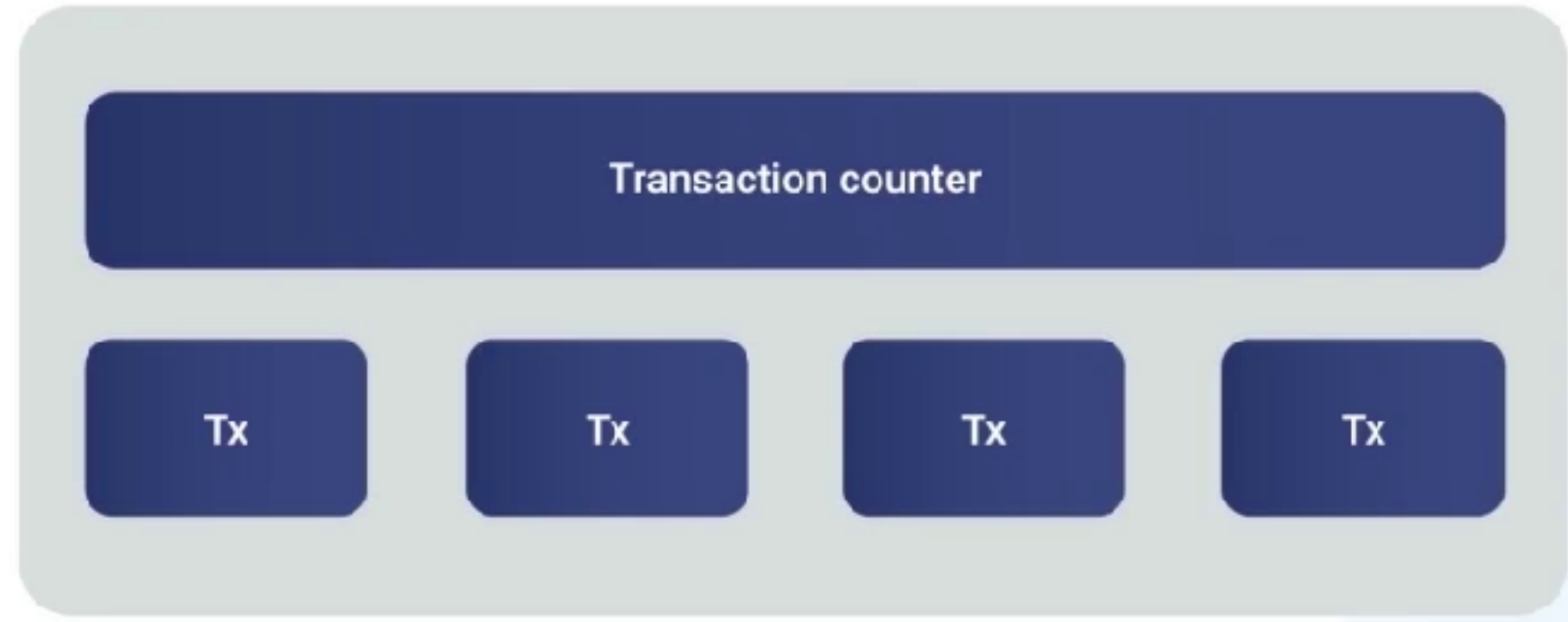
Blockchain is a chain of blocks and a ledgers. Each individual block is uniquely identified by its block header. Transaction Data is stored in the block body.

# Block Overview

Block



Block Header

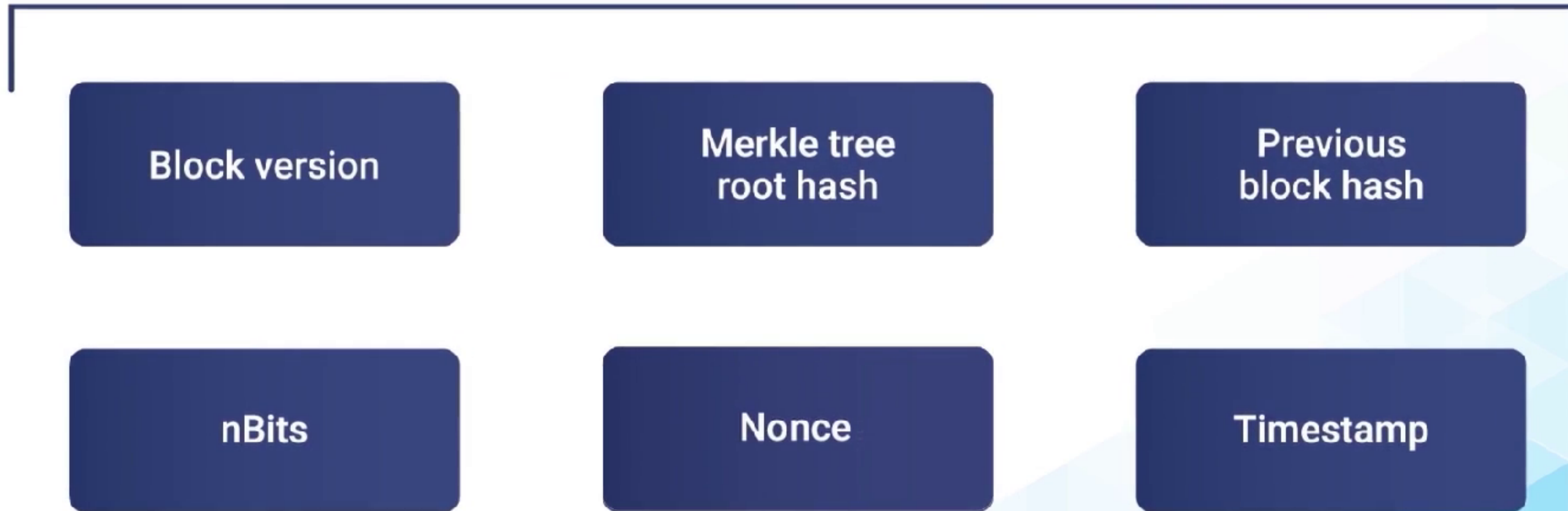


Block Body

The block header has the following components: Version Number of the block, signifies the Blockchain protocol incorporated in the block. Then is the Merkel tree root hash, transactions are arranged as a Merkel tree to encode them, securely and efficiently. Each transaction in the block is hashed and stored in a tree-like structure such that each hash is linked to its parent. Next is the hash of the previous block in the Blockchain, this component makes a block connected to the previous blocks on the chain, having them all build on top of each other, this brings the connection and chronology between each block. Next component is the nBits, it is an encoding of the block target. For a block, a target is the threshold hash value determining the block validity. A block will be valid only if the hash of its header is below the target value. Then there is nonce stored in the block header, it is a variable decided by the Miner creating the block. In order to keep the block hash under target value, the Miner guesses the nonce value, This is the work the Miner has to do to produce a valid block, the process is called Proof of Work. Block header also has a Unix time timestamp value, it serves as a source of variation for the block hash.



## Block Header

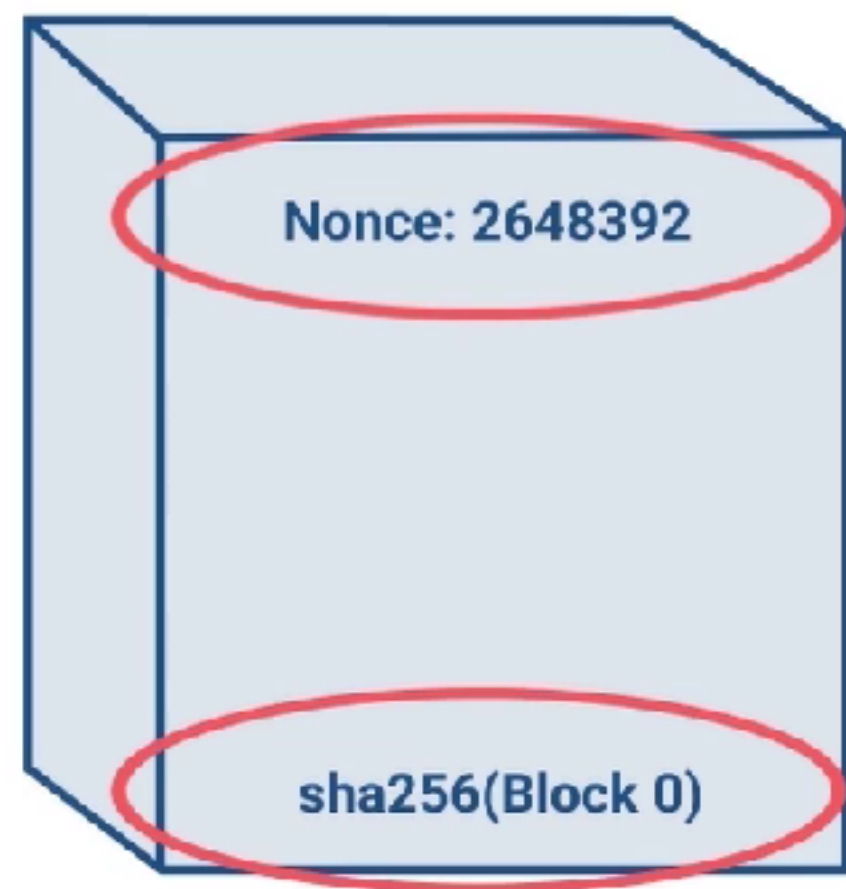






The first block of a Blockchain is its genesis block. The Genesis block is called the day zero block or block zero. It is the block that will contain the starting balance, which can even be zero. If a Blockchain is not minting new tokens or new balances every single block. Then the Genesis block, must have an initial balance, Otherwise there will be no way to introduce the new balance. As you can see, in the Genesis block, there is something called a nonce, which is a small string base number. Here, SHA-256 previous underscore block, or block zero represents the signature of the previous block, and Since this is a Genesis block, we are not keeping the signature of the previous block.

# How Blockchain looks like?



**Genesis Block 0**

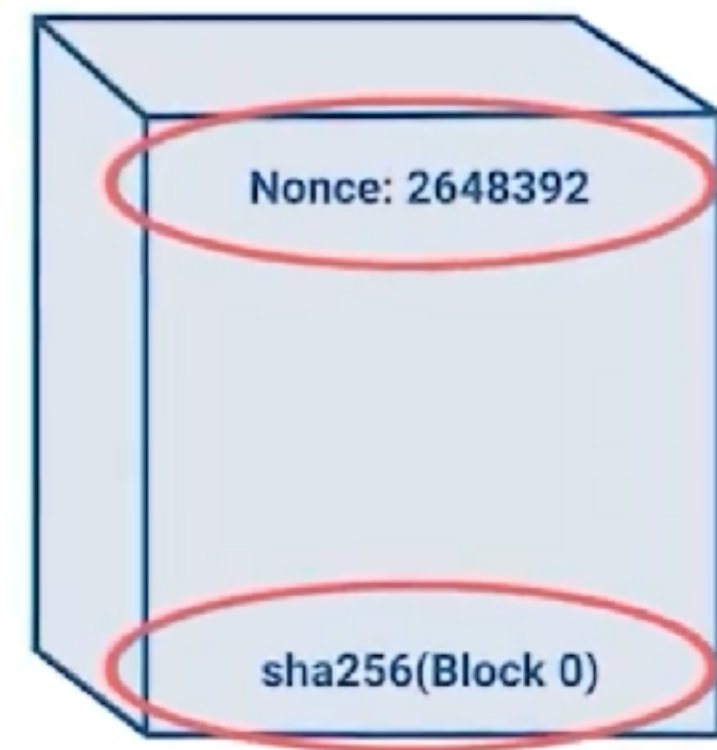
Copyright © Blockchain Council



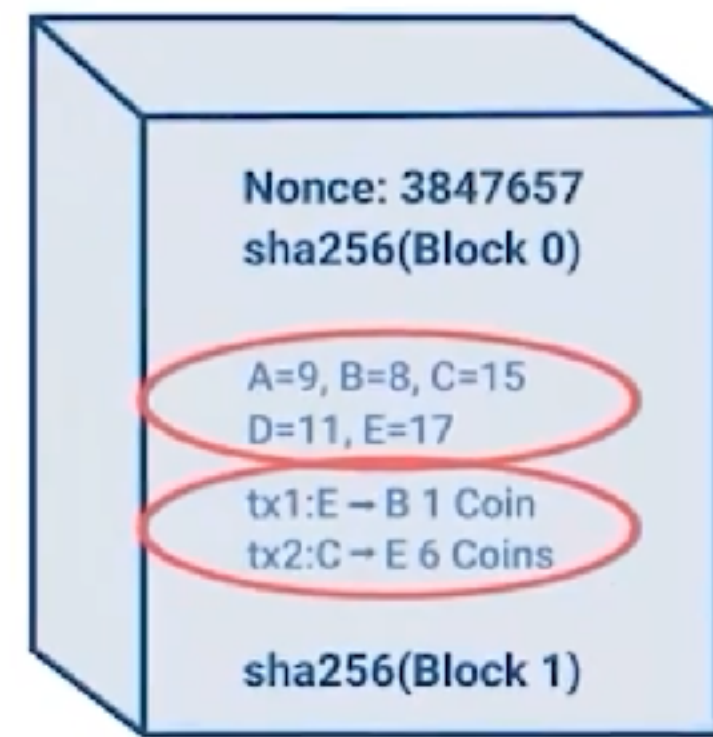
Imagine in block one that A's Balance is nine tokens, B's Balance is 8. C's balances 15, D's balance is 11, and E balance is 17. In this block, there are two transactions that are initiated where E transfers one coin to B, C transfer 6 coins to E.



# How Blockchain looks like?



**Genesis Block 0**



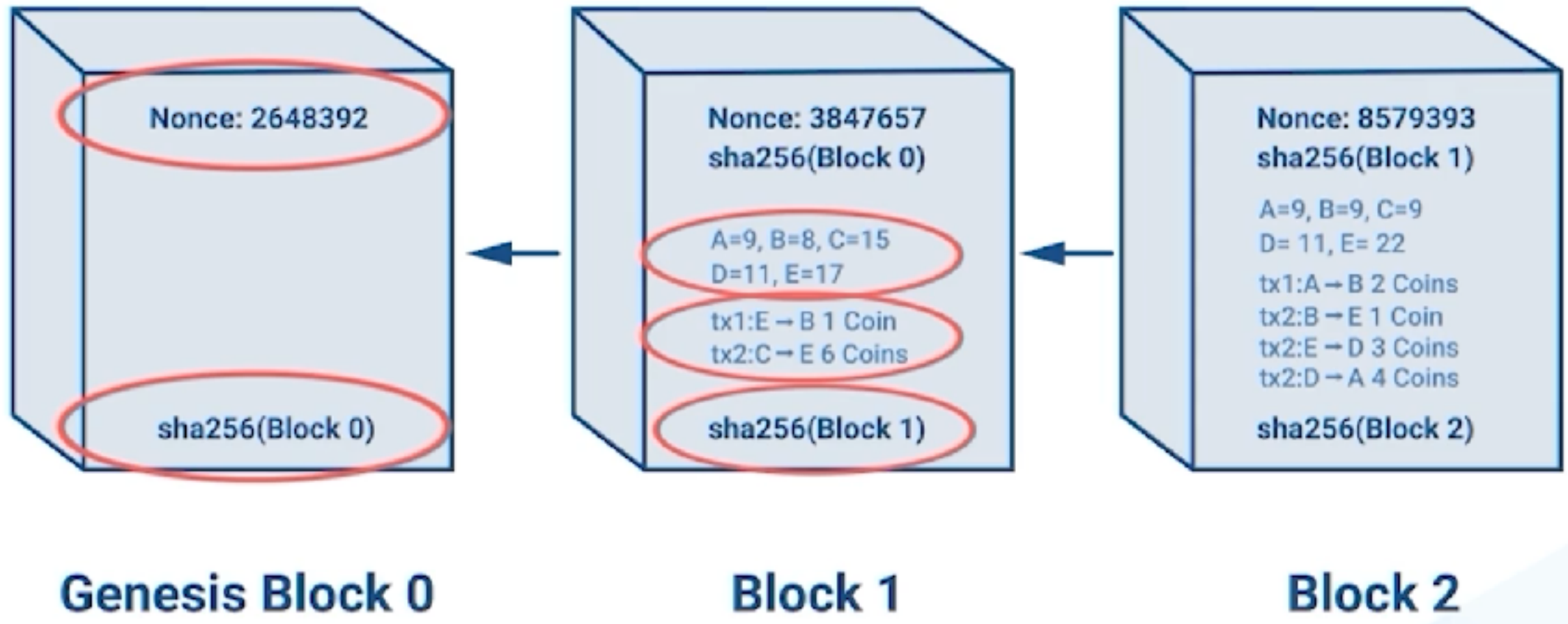
**Block 1**



As you know, these transactions have happened, the new block, that is blocked 2, must accurately reflect the new balances in line with these transactions. A new block that is block 1, is then added to the Blockchain and you will notice that there is a sha256 or this underscore block, which is the signature of this whole current block. As you can see this signature block number zero or sign and is being generated by the digest of the full block.

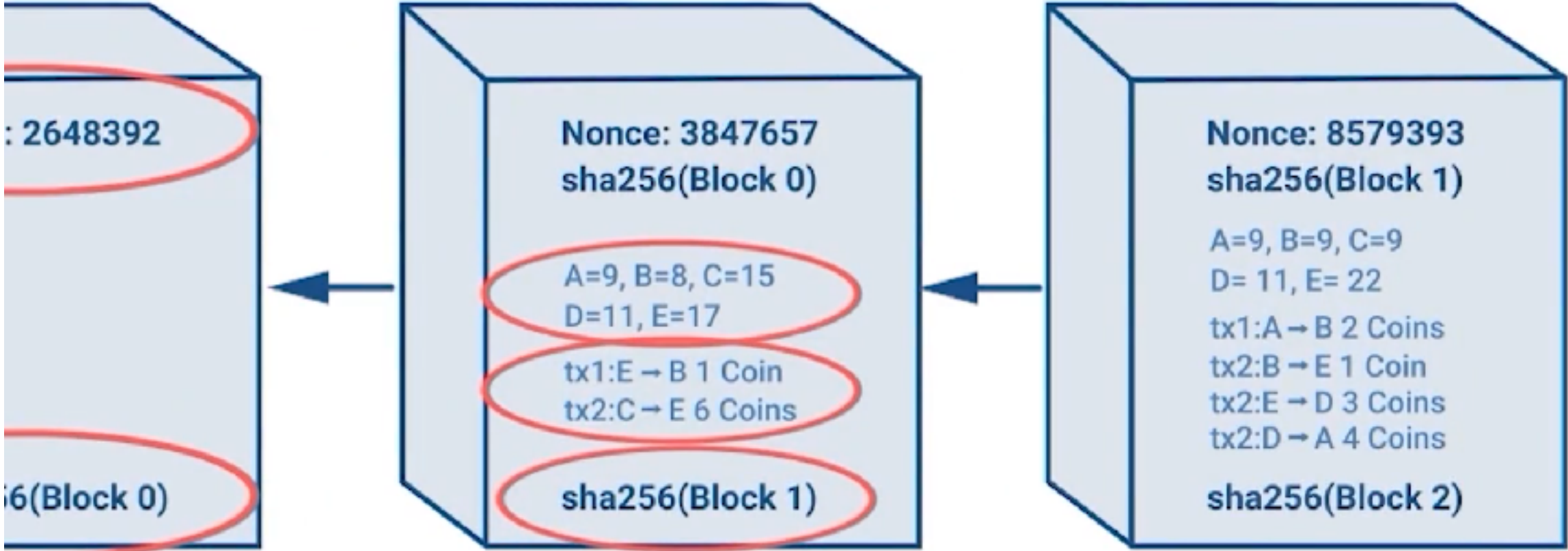
This is the signature of the full block, which is being calculated by SHA-256 of the current block. Sha256 is a simple hash algorithm which is a crunch of any length of data into a unique string of a fixed length. This way, if any single digit or letter is tampered within this block, the signature will completely change. It is not possible to reverse the digest or signature to the original input data or original data. This is always one way crunching. So, this way the SHA-256 has crunched the entire block into a unique fixed length string and we call it the signature of the block.

# How Blockchain looks like?



Next, if a new block has been added, the signature of the previous block will go to the sign-end one into the new block as a header. The nonce will be created that will be guessed by a minor who can be a person computer or server where the process which is confirming the block. The minor will figure out this number and will update the balances of all the addresses.

# How Blockchain looks like?



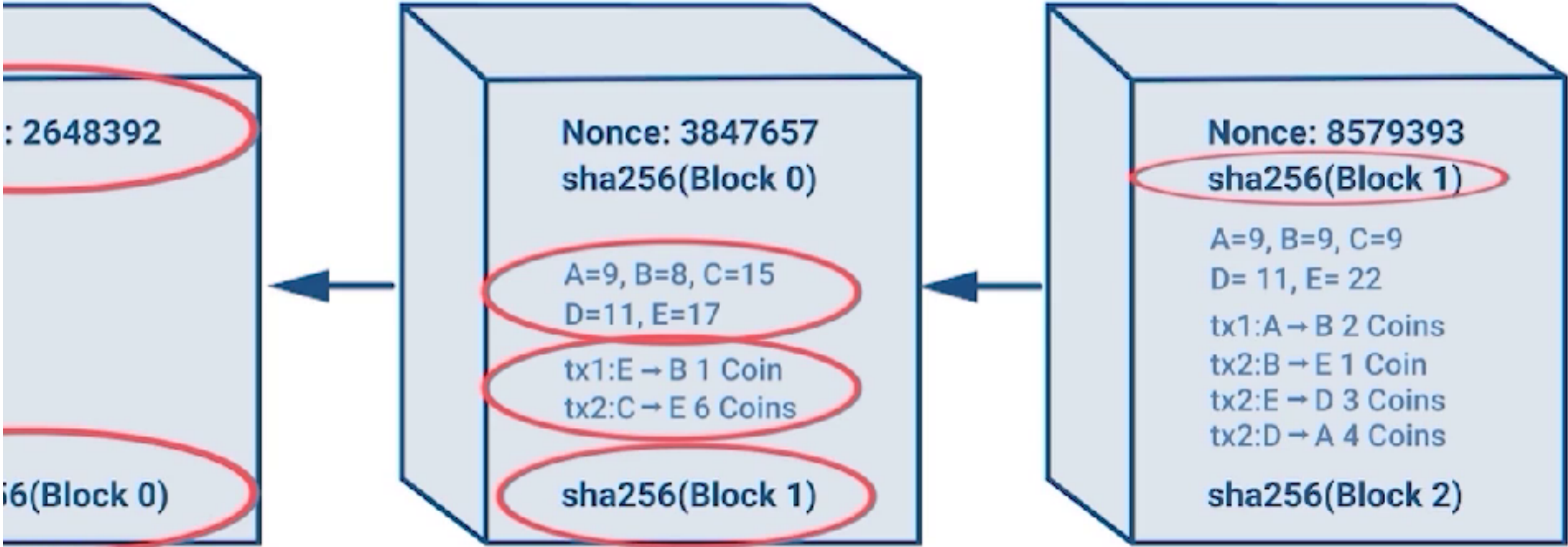
Block 0

Block 1

Block 2



# How Blockchain looks like?



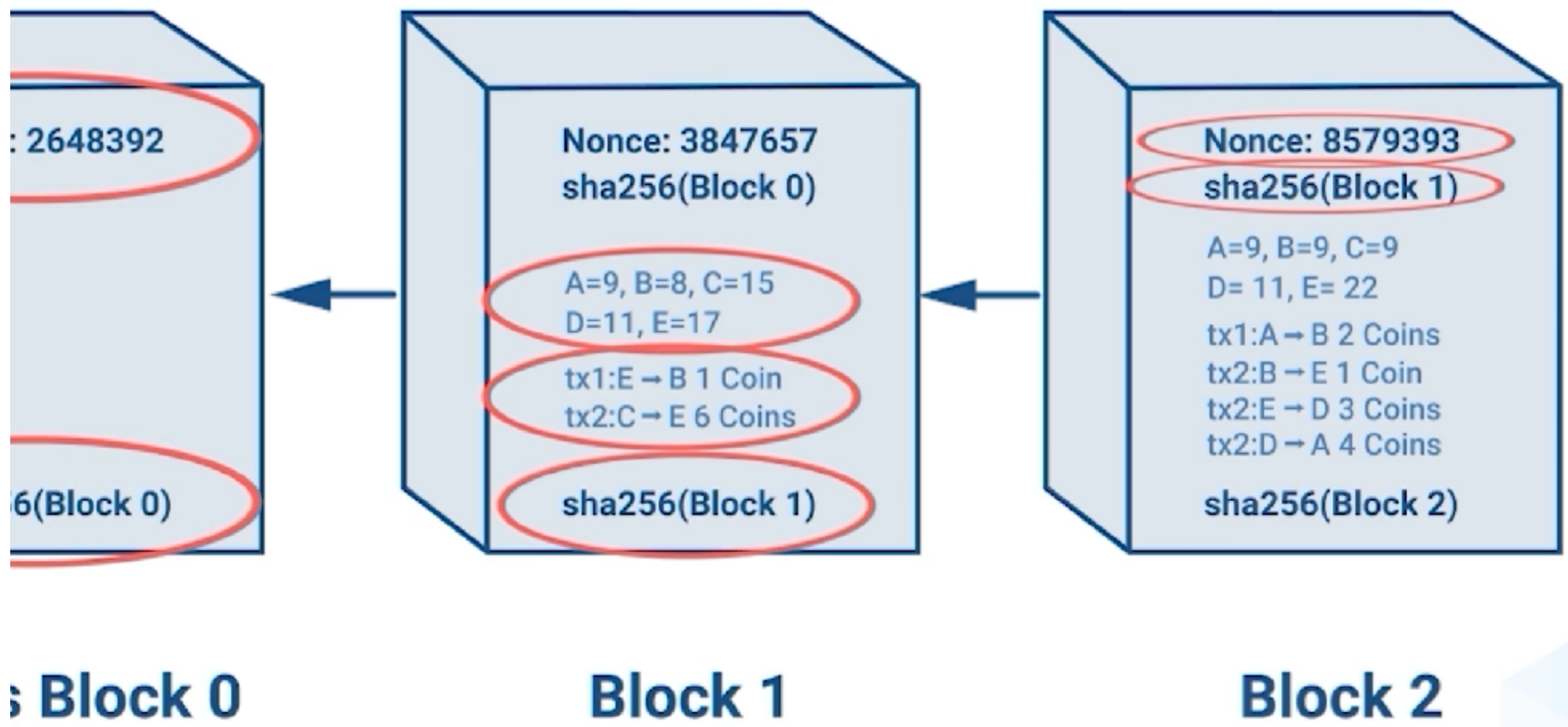
Block 0

Block 1

Block 2

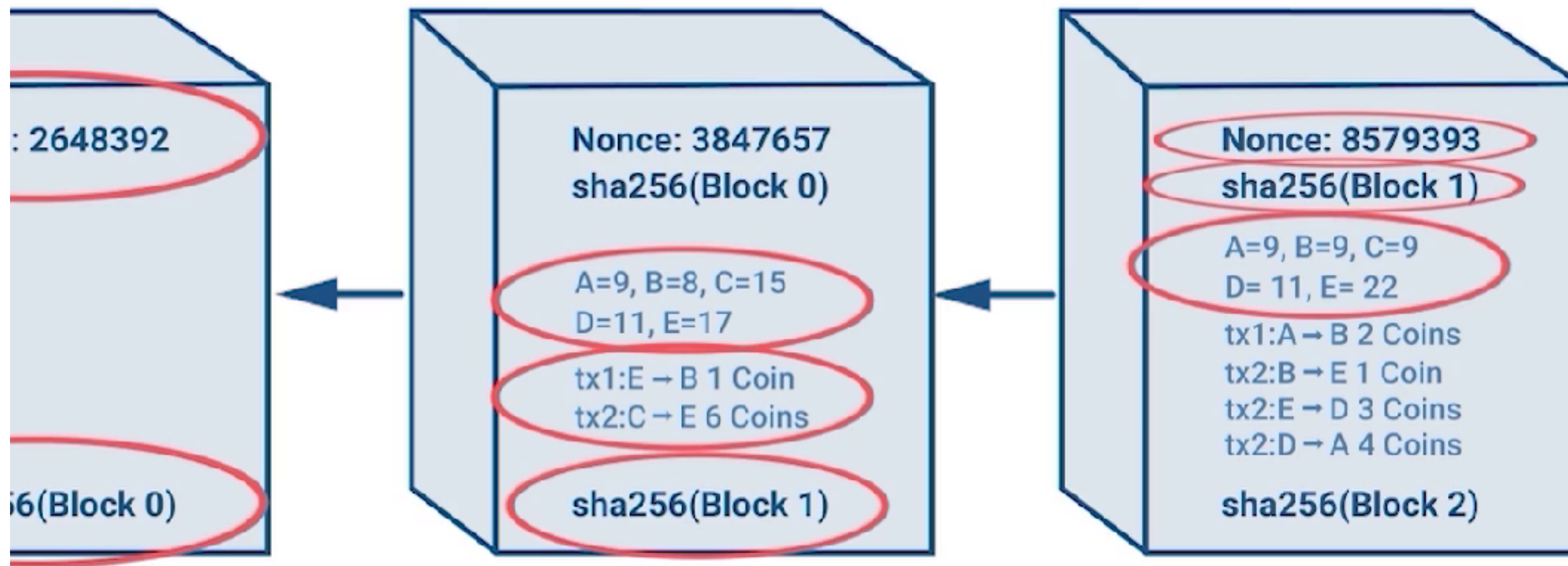


# How Blockchain looks like?



So let's say in block 2 and now A has nine tokens, B has nine tokens, C has nine tokens, D has 11 and E has 22 tokens. A has transferred two tokens to B, So B has 11 tokens now. Similarly, the balance of C, D and D will be updated. And there are only two transactions which are new. Also, for the second transaction, B sends one token to E, and E sends three tokens to D. And lastly D sends four tokens to A.

# How Blockchain looks like?



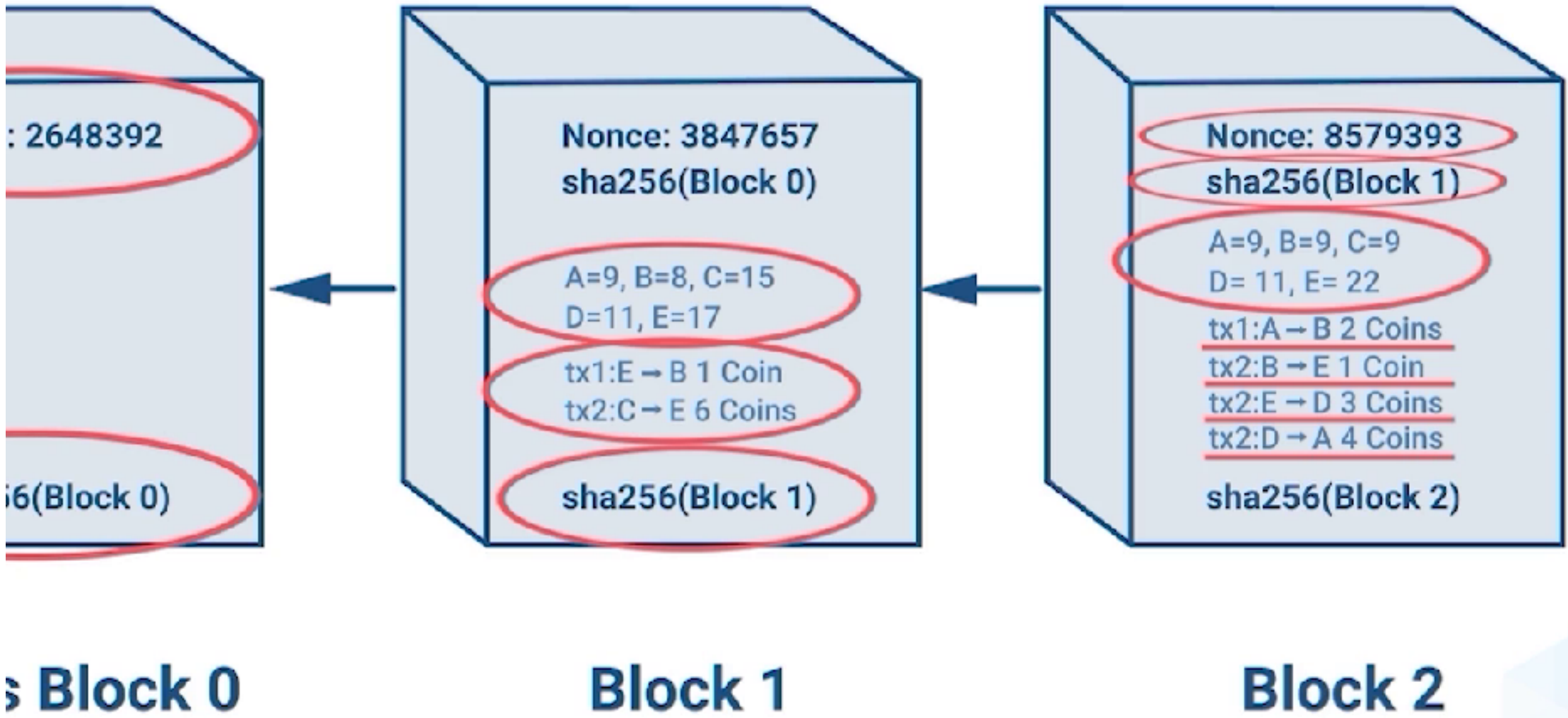
Block 0

Block 1

Block 2



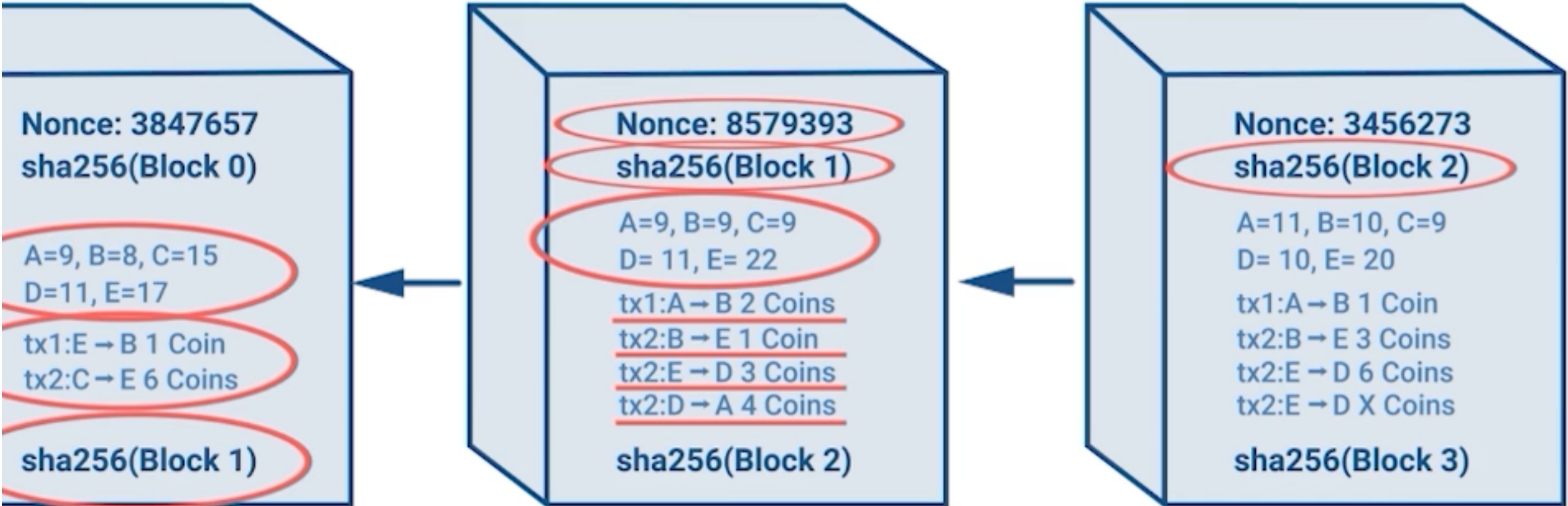
# How Blockchain looks like?



Here, the signature of the previous block which goes here



# How Blockchain looks like?



Block 1

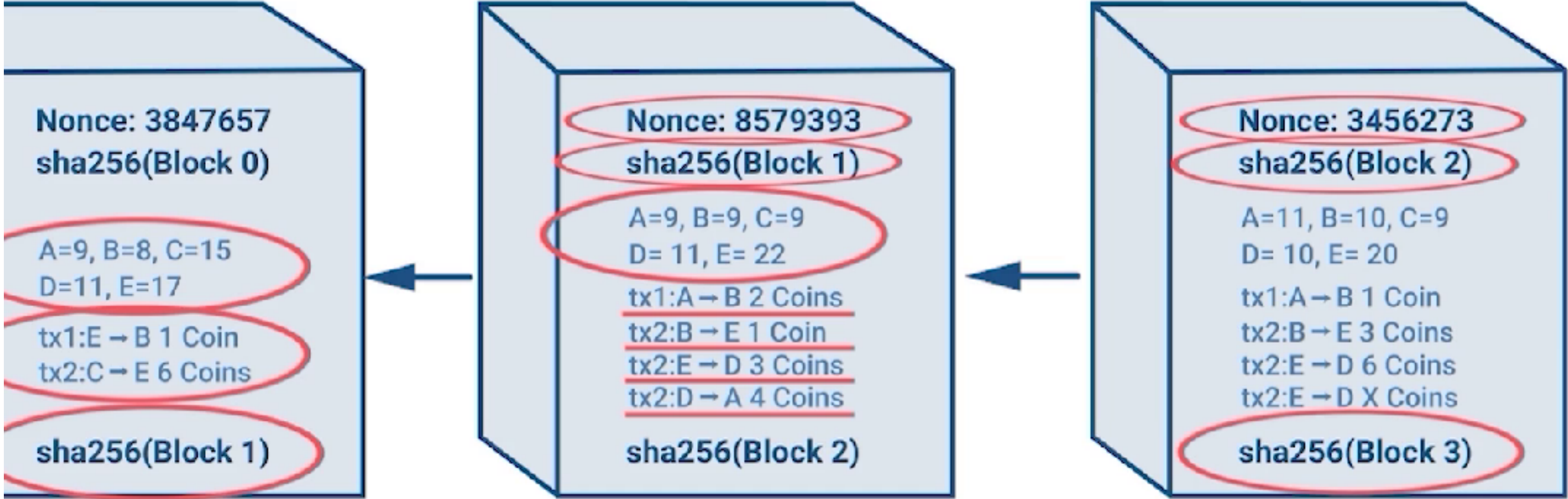
Block 2

Block 3

The signature of the whole new block is created through this process which will again go back to the previous block as a header, here, the nonce is the number which is being generated by the miners. These numbers or the nonces should be generated in a particular way through the mining algorithms.

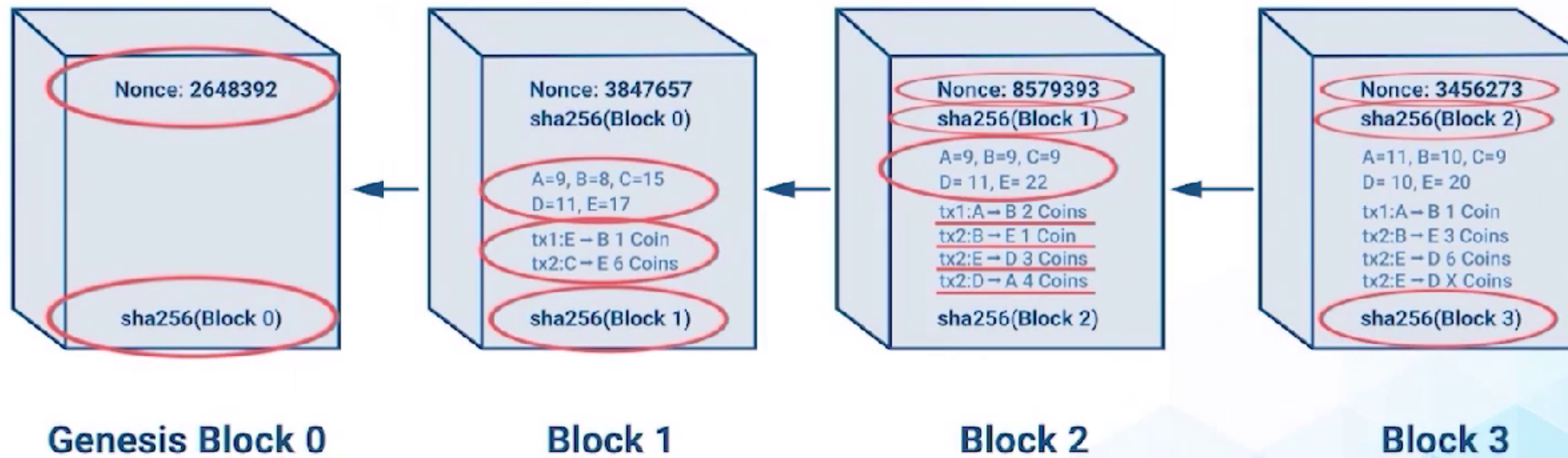
It depends on each particular blockchain, but in a general sense, the nonces should be generated in such a way that it's truly random and directly proportional to the difficulty of the blockchain.

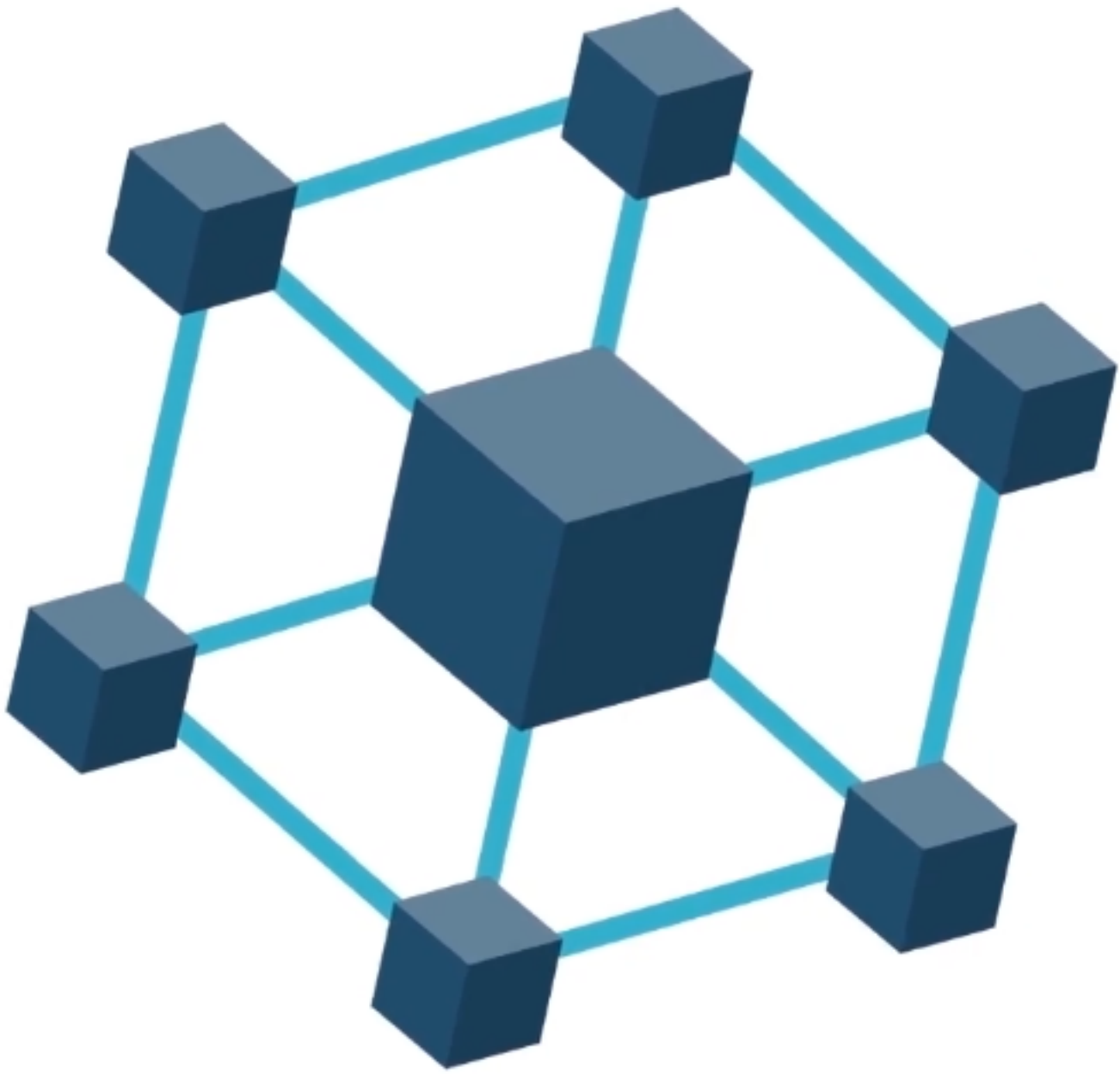
# How Blockchain looks like?





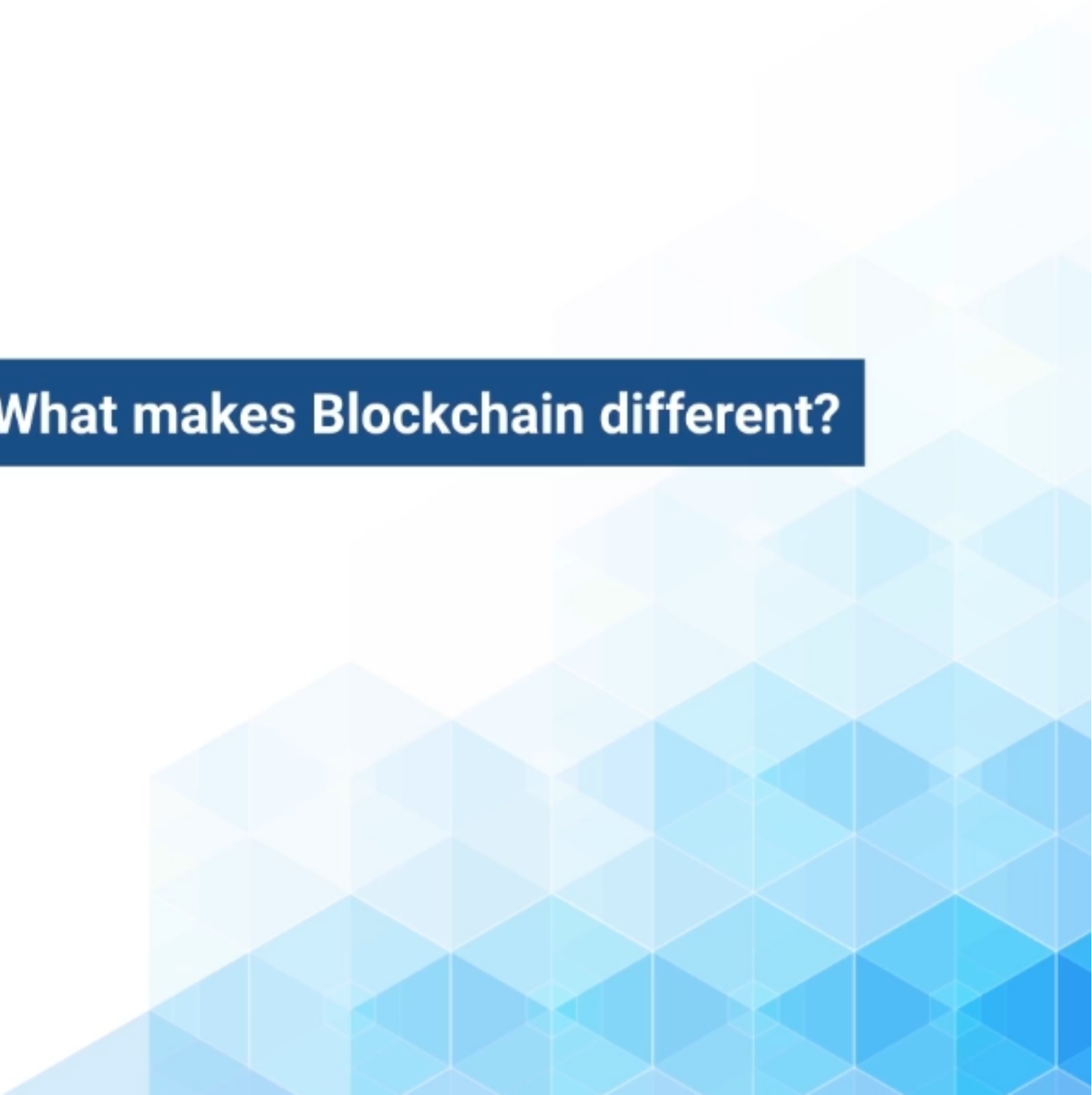
# How Blockchain looks like?





Copyright © Blockchain Council

**What makes Blockchain different?**





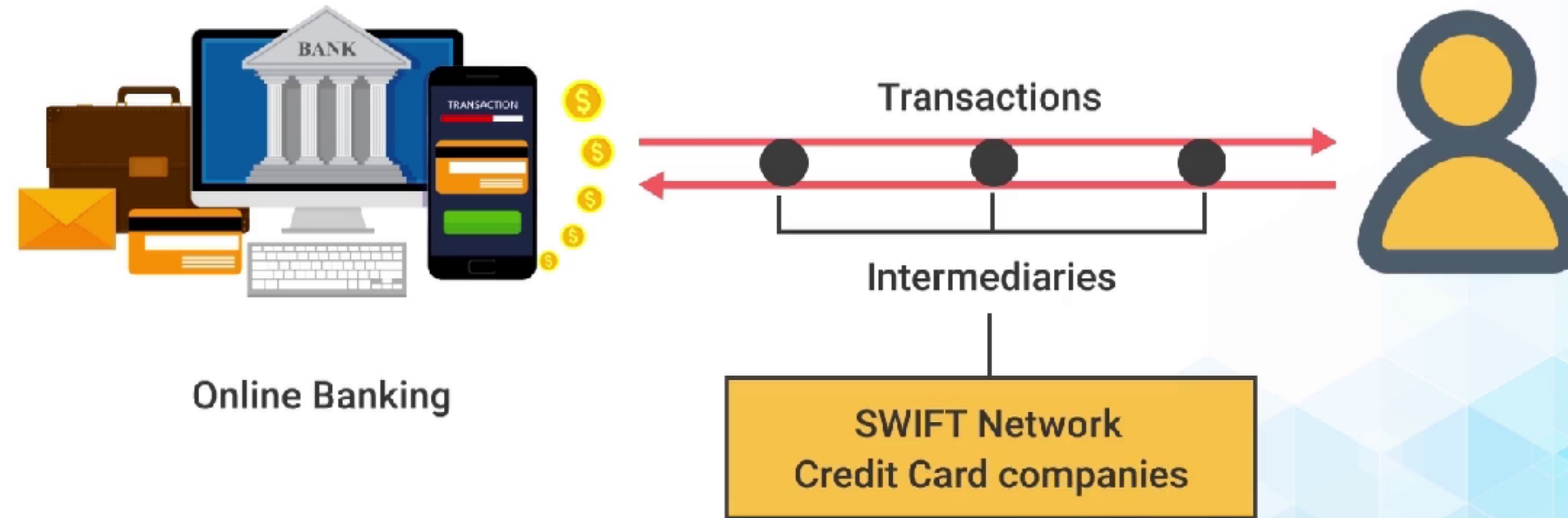
## What makes Blockchain different?

- 01 No Central Authority
- 02 Verifiability and Auditability
- 03 Disintermediation
- 04 Confidentiality and Integrity
- 05 Robustness

First, it's no Central Authority or third-party intermediators. The emergence of online banking has made doing transactions straightforward and less time-consuming process for the end users. But behind the scenes, there are many intermediaries involved in the process that played critical roles as trusted and reliable third-party structures. Involvement of these parties in the transaction flow results in high costs, which the payee and payer have to bear.

## What makes Blockchain different?

- No central authority or third party intermediaries

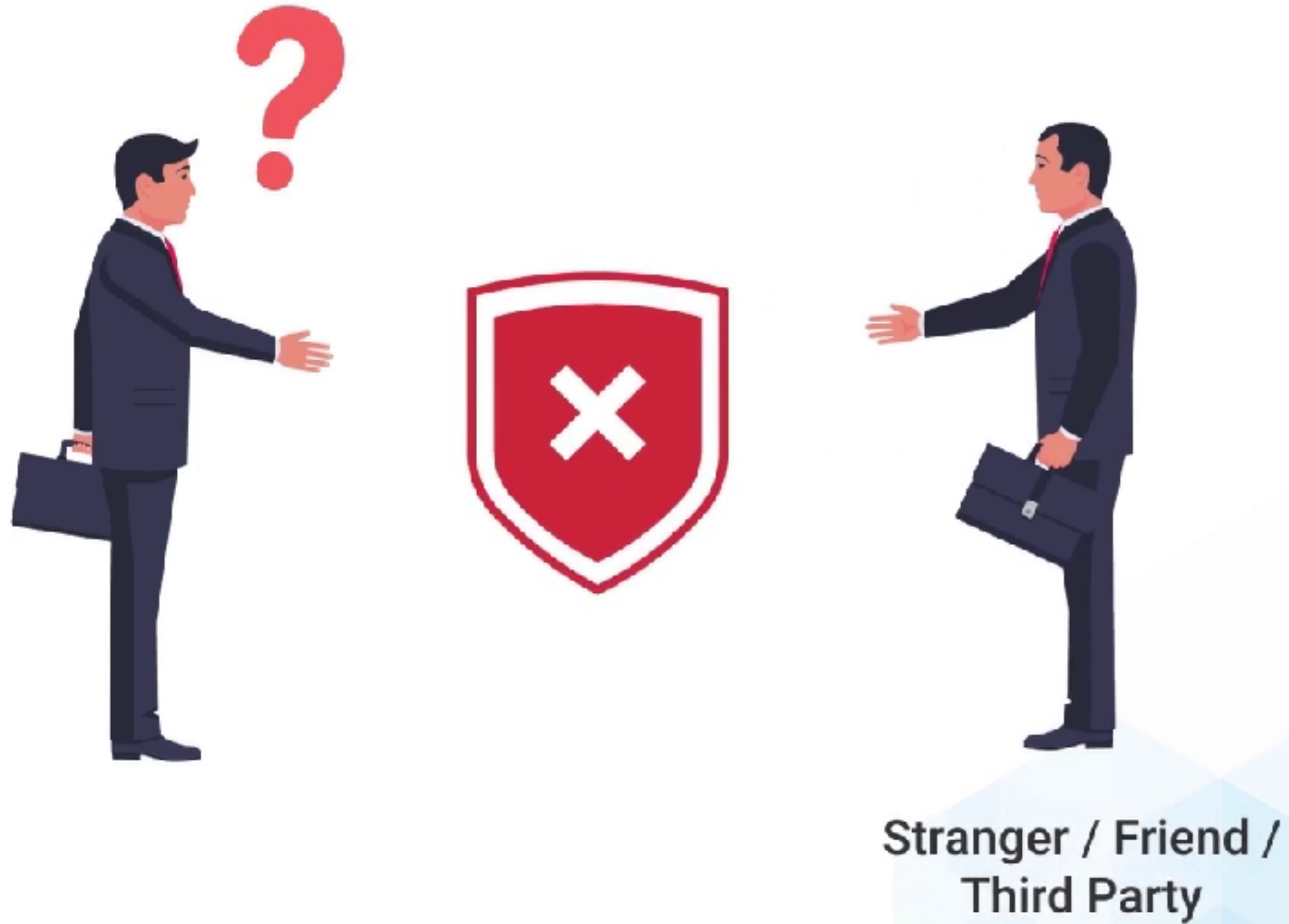


It is human nature, not to trust strangers, or even our friends, so it is the major point that Blockchain is adhering to, It is removing the need to trust third party. The cryptographic algorithms used in Blockchain eliminate, the need to trusting third-party. For example, you have the referees in a soccer game or you have banks who are helping you to make the online transactions, and eBanking or internet banking.

Third parties help in maintaining trust. But there is always a possibility that they can tamper with the data. This is the main issue Blockchain is trying to solve.



# What makes Blockchain different?



# What makes Blockchain different?

```
if (n > 0 && t < 1){  
v = drtovAtTimekey  
thisblock.Duration  
gffg = .05;  
yrnc = 2.0;  
cryp = 8.0
```

Cryptographic Algorithms



Stranger / Friend /  
Third Party

In a Blockchain, transactions are verified by nodes distributed globally in a peer to peer network. Anyone can join or leave this network without disrupting the network's ability to form consensus on the state of the Blockchain. It is unlike a central server in which a single computer is used to manage transactions. Instead distributed computation from anywhere in the world can be leveraged.

## What makes Blockchain different?

- In a blockchain, transactions are verified by distributed nodes





Bitcoin and Ethereum are excellent examples of Blockchain which are used to communicate value globally without any trust in any party and without any middlemen.

## What makes Blockchain different?

- In a blockchain, transactions are verified by distributed nodes



Bitcoin



Ethereum

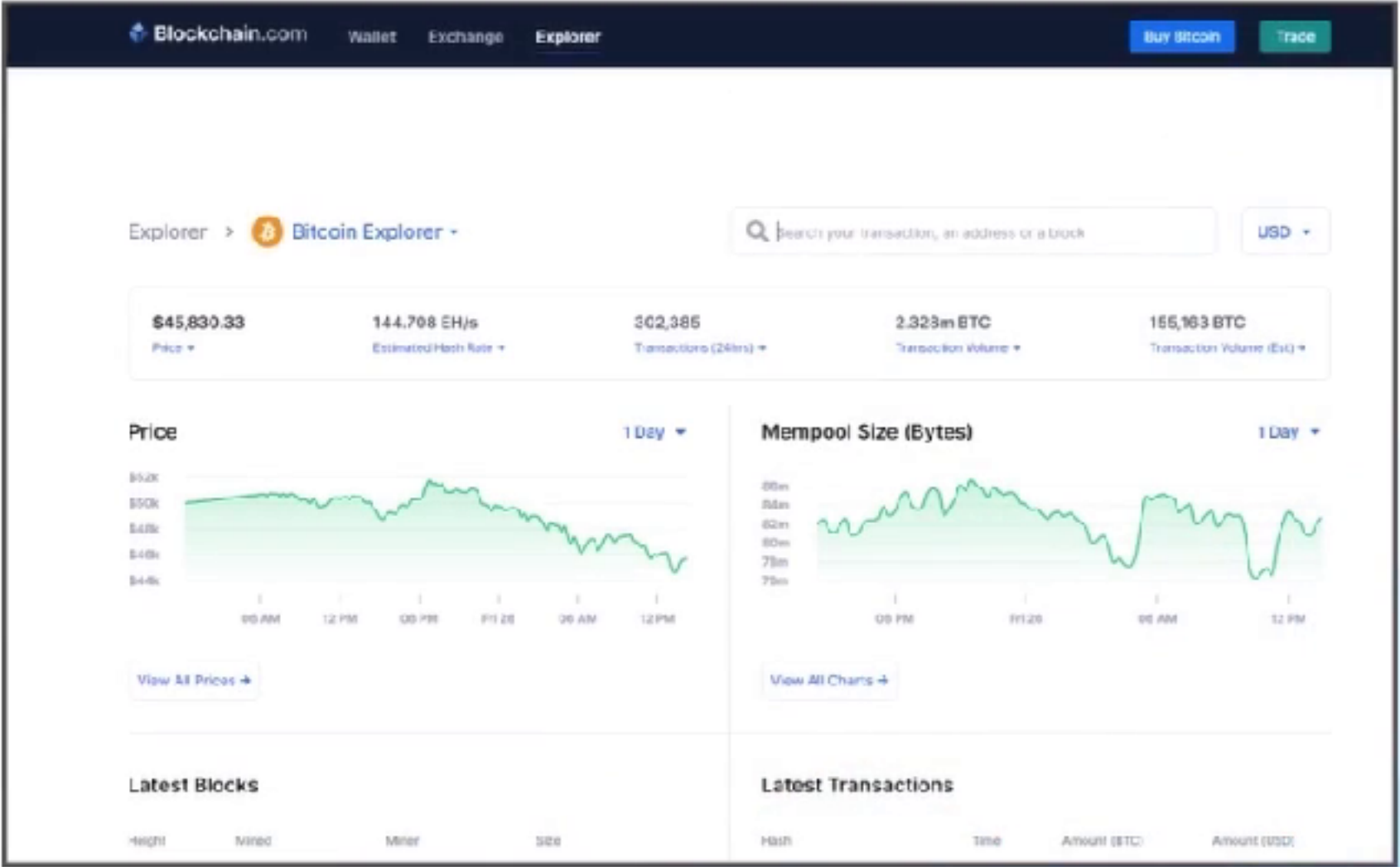
Now, let us understand how Blockchain provides you with a verifiability and auditability? Any record of the transaction on the Blockchain is verifiable by anyone. So if you are using the public Blockchain like Bitcoin or Ethereum, all the transactions happening can be verified by anyone. For example, there is the Bitcoin Explorer that are the web applications built upon the blockchain itself, where you can go and see how the transactions had happened. How much Bitcoin was sent to the person. What was the different period where transactions happened? So everything is verifiable and transparent with the public Blockchain and these records are openly accessible.

# What makes Blockchain different?

Verifiability and Auditability



Public Blockchain



Bitcoin Explorer

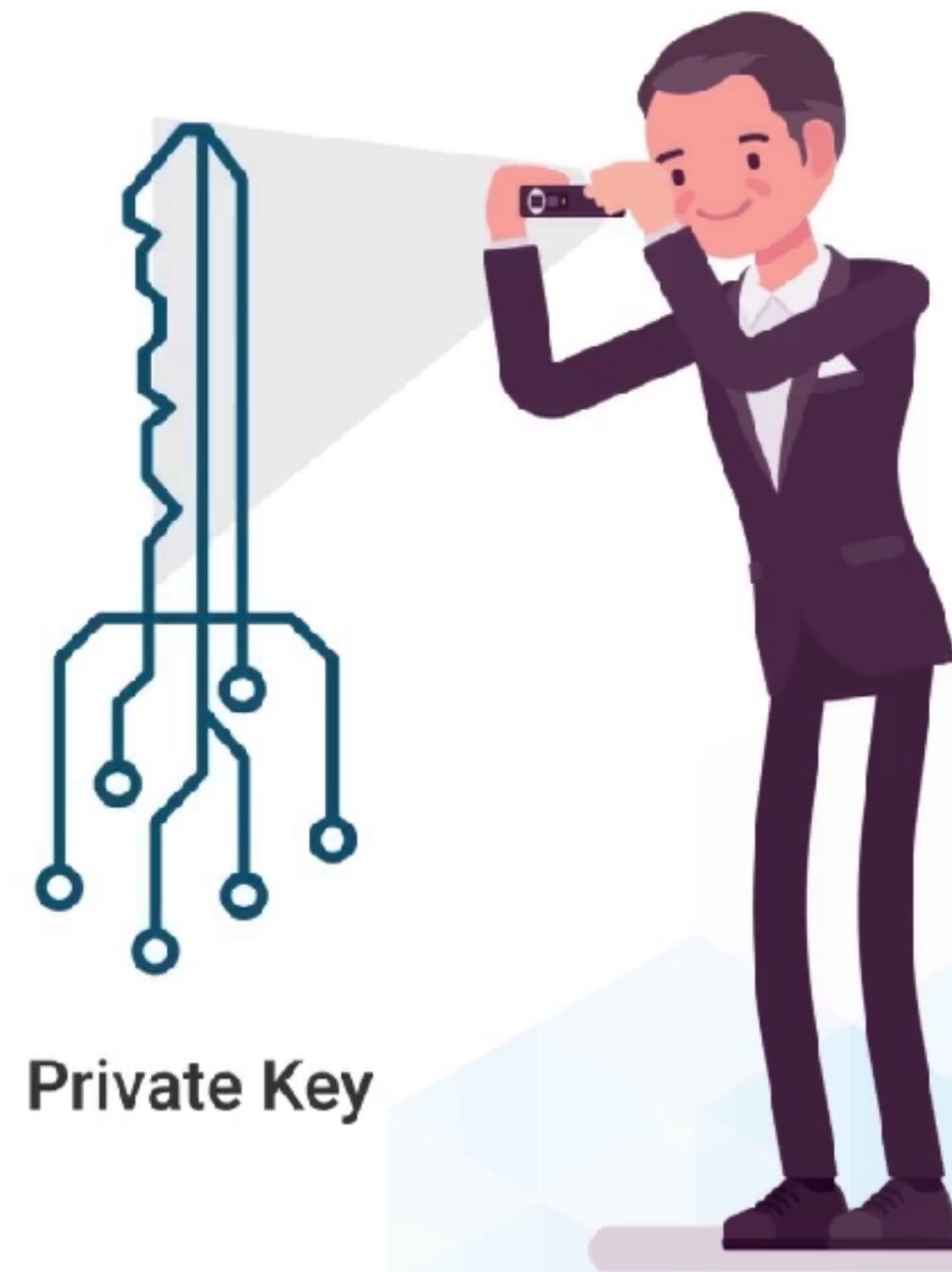
Suppose you want to upload some data over Bitcoin Blockchain? And you know, now that when you are uploading the data over the blockchain, it can be seen by anyone, But to make sure that nobody can see your transaction or data, what you can do is to use your account private key to encrypt your data if you have an account over the network, and then you can use the private key of that account or even if you have the understanding about the cryptography, then you can create your key pair and then use that private key to encrypt the data and uploaded over the Bitcoin Blockchain.



## What makes Blockchain different?



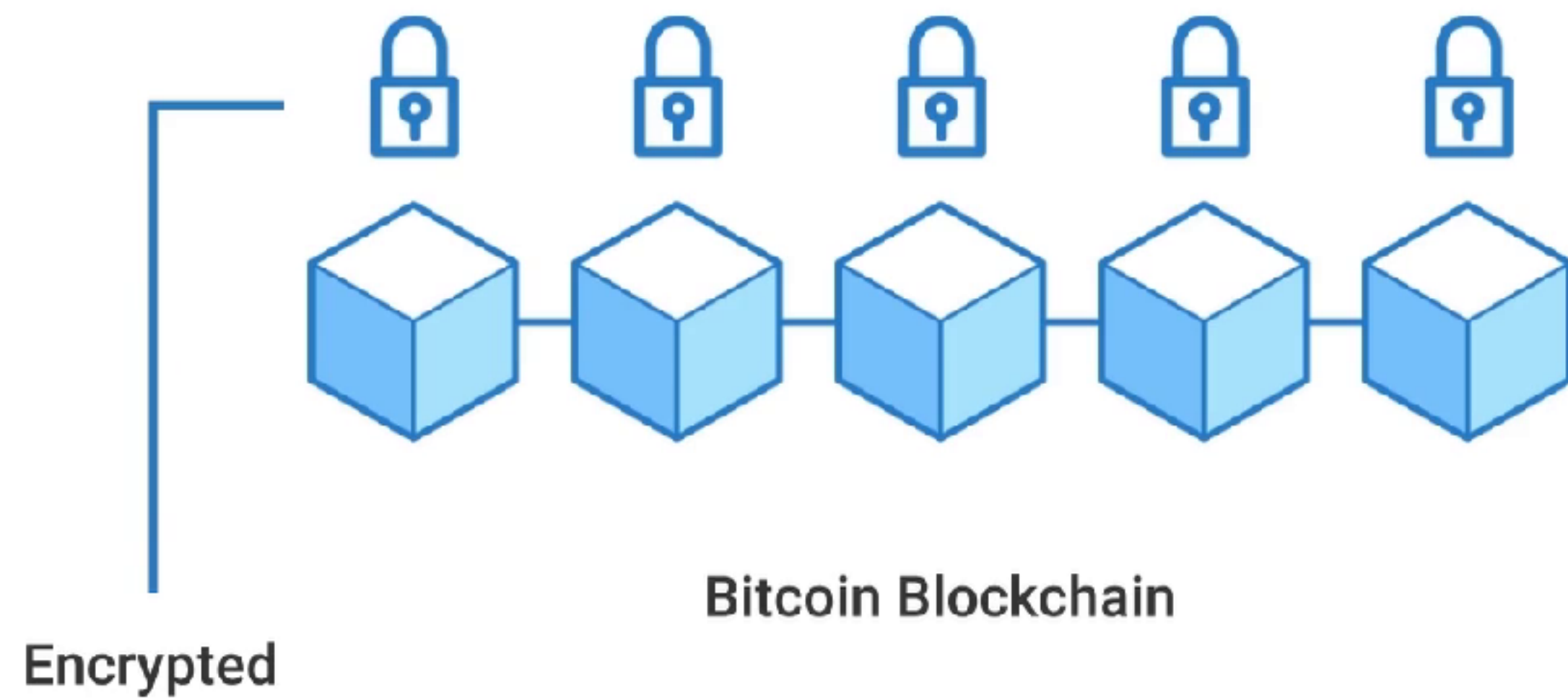
## What makes Blockchain different?



So it's like whenever you upload the data over the Bitcoin blockchain, it's going to be accessible by everyone but it's going to be encrypted. So only the person or the group of the people who have your public Keys will be able to take that data and see the data that you have uploaded. So that's one of the ways to upload data on bitcoin blockchain or Ethereum blockchain.

## What makes Blockchain different?

- Everyone can access the data in Bitcoin blockchain.



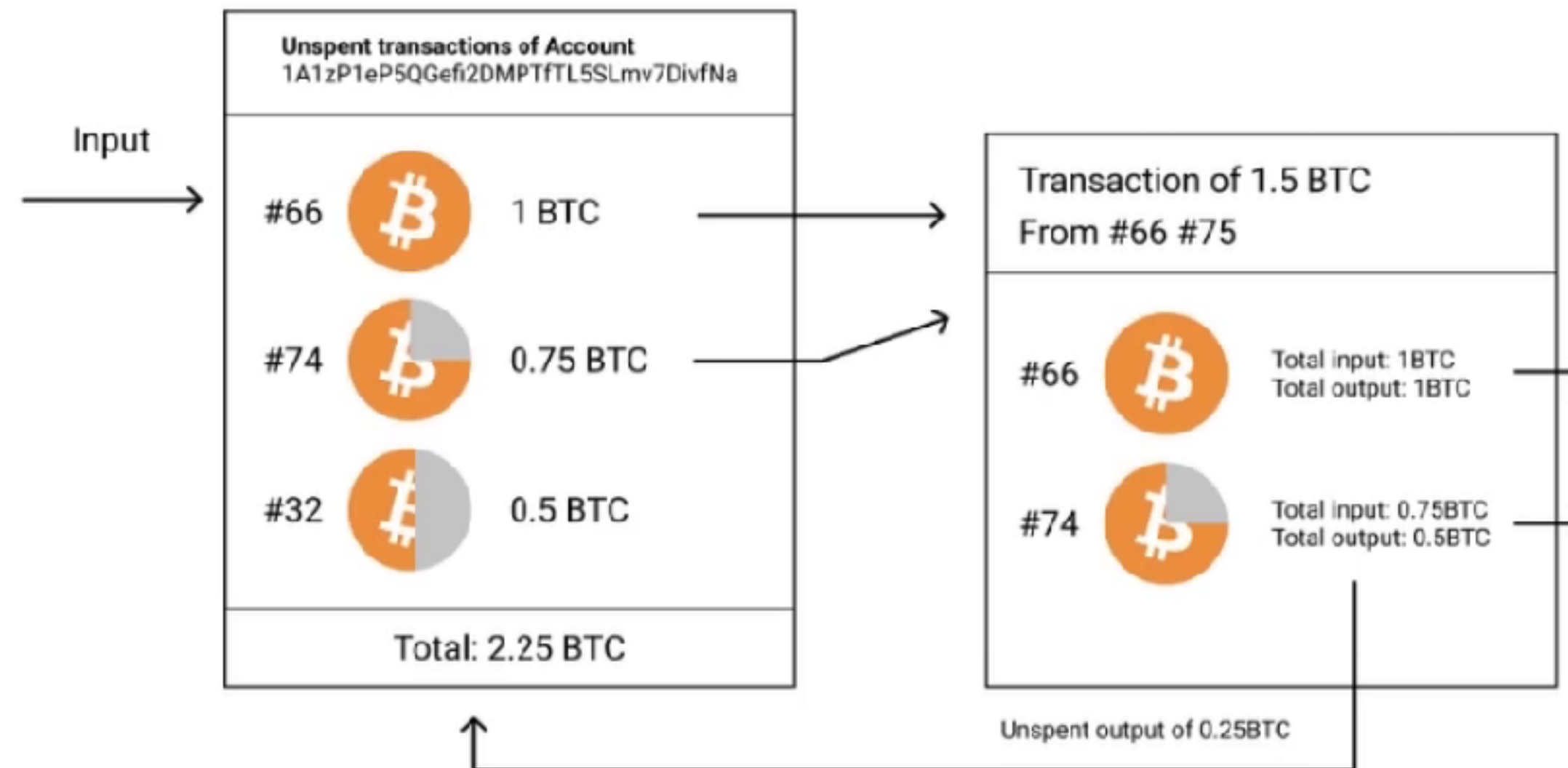
Then it's easy to audit any transaction and its Trail is every transaction is interlink to the previous one. Since Bitcoin works on the UTXO principle where every input in a Bitcoin transaction comes from the unspent output of some previous transaction.



## What makes Blockchain different?

- Bitcoin works on the UTXO principle where every input in a bitcoin transaction comes from the unspent output of some previous transaction.

**UTXO** Amount of digital currency someone has left remaining after executing a cryptocurrency transaction.



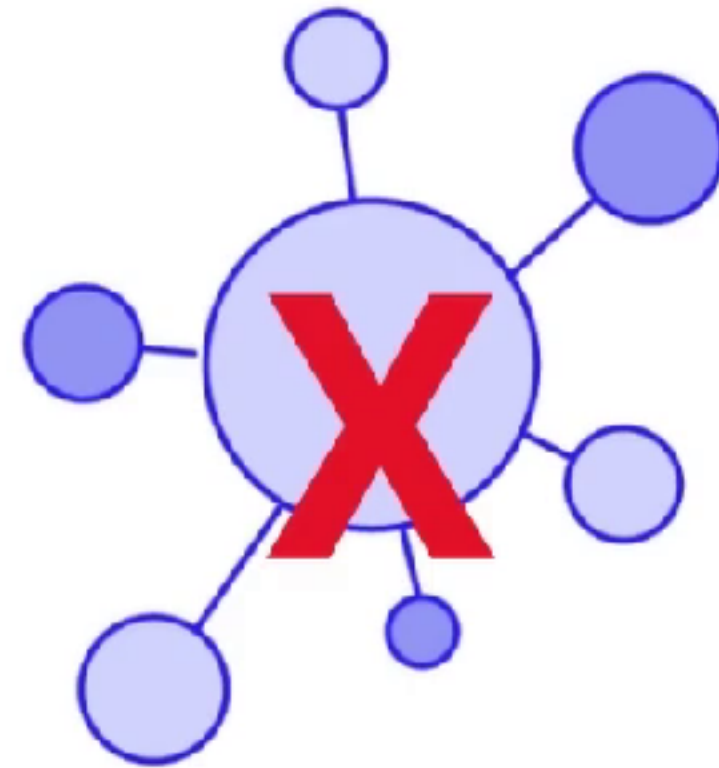
Then we have to intermediation. Now, in order to verify any transaction on blockchain, you do not need a third party or a mediator or you do not have to depend on any Centralised administrator. All the records stored in the blockchain are verifiable anytime by any peer. For example to verify the college degree, you have to trust the college servers or the college email it which is responding to the enquiry. This is not required, if the college degrees are verified by the blockchain based ledger.

# What makes Blockchain different?

 Disintermediation



Mediator



Centralized administrator



Trusted third party

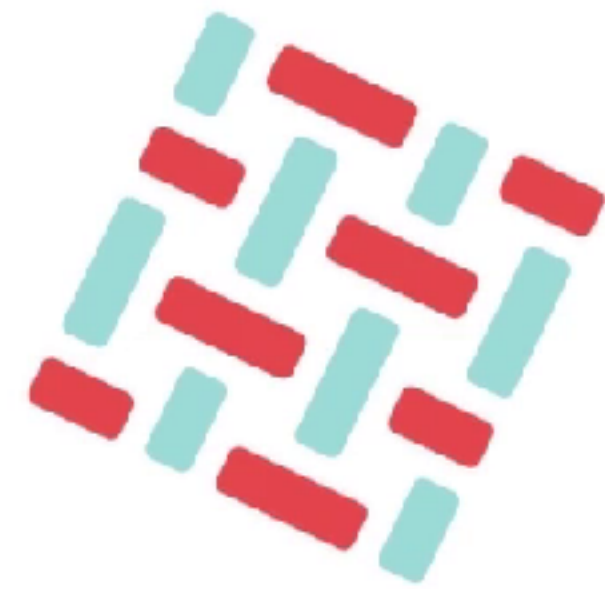
Next is confidentiality and integrity. The blockchain is an openly distributed Ledger yet a private system, due to encryption. Many Technologies have options to restrict the certain records access based on the user's public key or the permission set by the creator of the files. Hyperledger fabric blockchain offers tons of private and confidentiality features using the certificate authority or CA server.



## What makes Blockchain different?



- Confidentiality and Integrity



# HYPERLEDGER FABRIC

- Hyperledger Fabric Blockchain offers private & confidentiality features using the Certificate Authority (CA) Server.



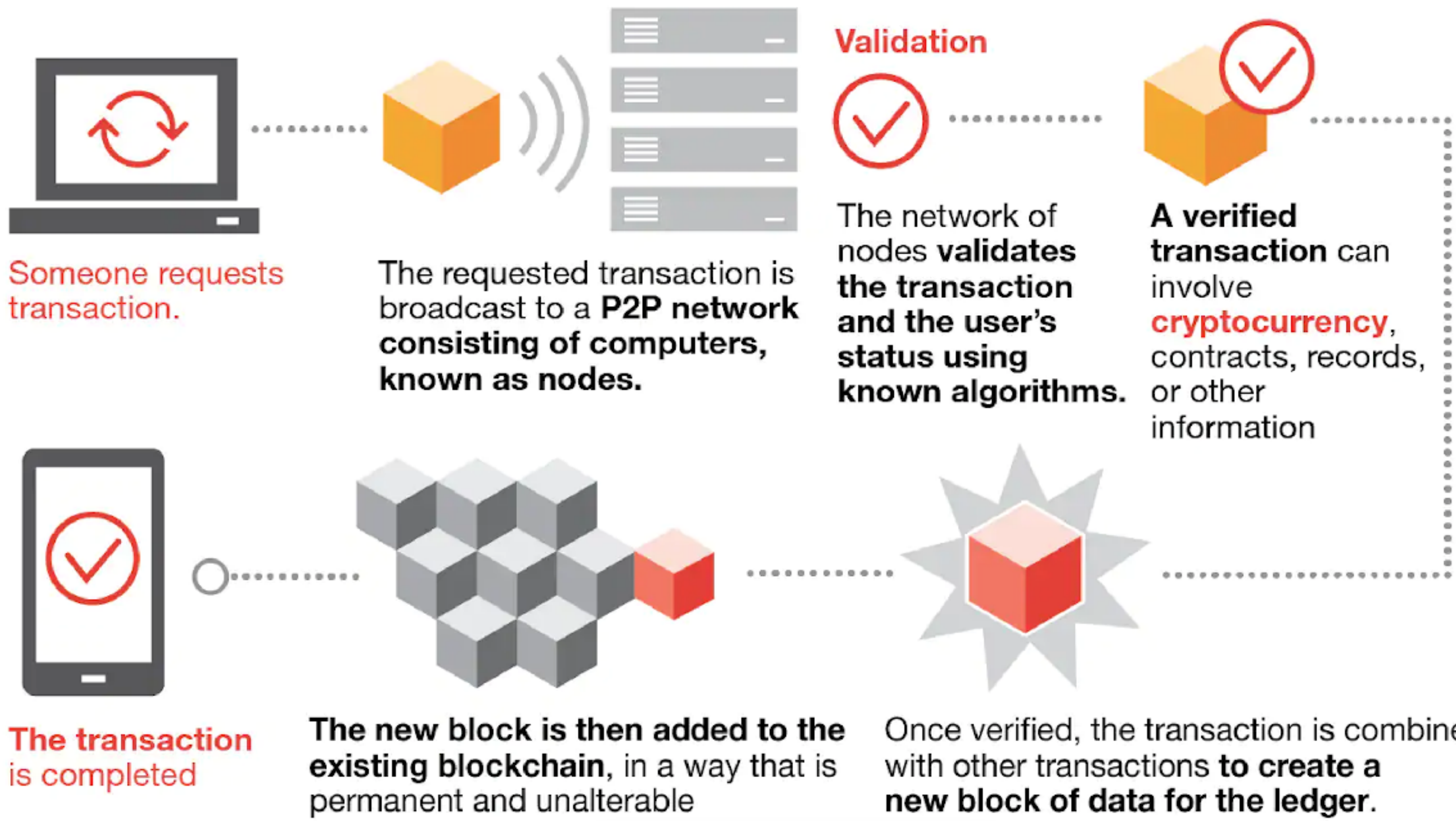
And last is robustness.

Extreme Fault tolerance is been built redundancy and decentralisation. In the blockchain network, any server or machine can come and go at any time without informing any of the other nodes.

## What makes Blockchain different?



- Robustness
- Blockchain is extreme fault tolerance is due to inbuilt redundancy & decentralization.





## Potential applications



### Automotive

Consumers could use the **blockchain** to manage fractional ownership in autonomous cars.



### Financial services

**Faster, cheaper settlements** could shave billions of dollars from transaction costs while improving transparency.



### Voting

Using a blockchain code, constituents could cast votes via smartphone, tablet or computer, **resulting in immediately verifiable results.**



### Healthcare

**Patients' encrypted health information** could be shared with multiple providers without the risk of privacy breaches.