



**Politecnico  
di Torino**

**Politecnico di Torino**

Master of Science in Engineering and Management

Academic year 2022/2023

December 2023

**DIGITAL ASSETS AND DIGITAL EURO:  
CAN THEIR STRUCTURES AND  
FUNCTIONALITIES REALLY REPLACE  
SWIFT?**

Supervisor:

Prof.ssa Anna D'Ambrosio

Candidate:

Giacomo Spiotta



# Index

<b>Introduction</b> .....	<b>5</b>
<b>Money</b> .....	<b>6</b>
History of money.....	7
Through the ages.....	9
Money's essence .....	11
<b>Blockchain</b> .....	<b>13</b>
<b>DLT vs Blockchain</b> .....	<b>13</b>
<b>Bitcoin</b> .....	<b>17</b>
How does Bitcoin work? .....	18
Account creation .....	18
Decentralization .....	19
Block: to prevent transaction ordering problems.....	20
Block Header .....	21
Blockchain characters .....	23
Proof-of-Work .....	24
Rewards .....	27
Longest chain rule.....	31
Double Spending Problem.....	32
Transactions .....	33
Governance.....	37
<b>Ethereum</b> .....	<b>39</b>
What is Ethereum? .....	39
Accounts.....	40
Gas.....	40
Ethereum blocks and mining time.....	41
ETH issuance.....	42
Governance.....	43
PoW vs PoS.....	43
Smart Contracts .....	43
DApps.....	45
Ethereum Virtual Machine .....	46
Oracles .....	47
AAVE .....	48
DAO hack .....	48
<b>International Payments</b> .....	<b>51</b>
SWIFT and Cryptocurrencies issues .....	54
<b>Central Bank Digital Currency (CBDC)</b> .....	<b>59</b>
<b>Overview</b> .....	<b>59</b>
Key drivers .....	61
Regulator's consideration .....	62

Technologies and access points .....	62
Retail vs Wholesale CBDCs .....	63
CBDCs distribution model .....	65
Interest bearing CBDC and non-interest bearing CBDC .....	67
<b>CBDCs around the world.....</b>	<b>67</b>
Sand Dollar: the Bahamas Digital Currency.....	69
DCash: the Eastern Caribbean Digital Currency .....	69
eNaira: the CBDC from Nigeria .....	69
China Digital Renminbi or Digital Yuan .....	70
Bakong project: the Cambodia National Currency.....	70
<b>Digital Euro .....</b>	<b>72</b>
Different visions between the founders .....	72
European CBDC approaches.....	73
Design .....	74
ECB constrained scenario .....	75
EU unconstrained scenario. ....	77
Geopolitical reason behind the Digital Euro .....	79
Future Perspective .....	79
<b>Cryptocurrencies, CBDCs and concluding remarks .....</b>	<b>81</b>
Cryptocurrency vs Central Bank Digital Currency .....	81
Concluding analysis .....	84
<b>References .....</b>	<b>86</b>

## **Introduction**

In the last years cryptocurrency and blockchain technology have captured attention and motivated many fintech and financial institutions to experiment how they could transform the financial services industry.

In addition to this, in recent years more and more CBDCs have begun to be talked about and many countries have started to develop their own, each with its own design but all with the same objective.

In response to the question "What is Bitcoin?" a comprehensive answer would span various fields, ranging from economics, computer science, law, history, geopolitics, and finance, likely leading to confusion for the interlocutor, as was the case for me when I first approached the subject more than a year ago. This thesis, for this reason, is born with the aim of simplifying these concepts, analyzing key steps to dispel the common feeling of uncertainty people, often experience and trying to give an application in our everyday lives.

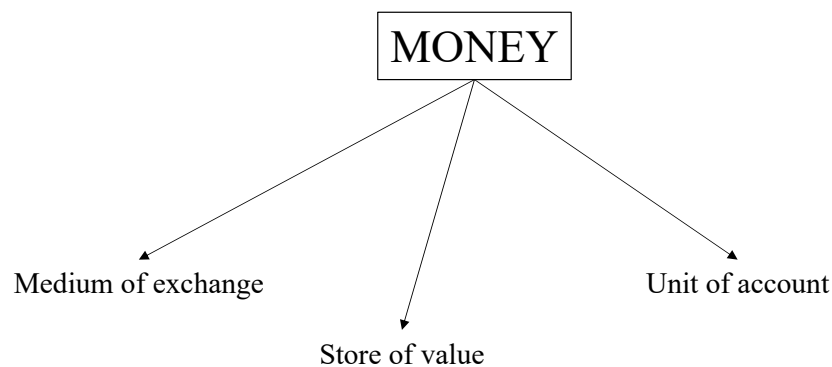
The work will be developed in multiple chapters, starting by introducing the concept of money, its various forms, and how it has originated and evolved over time. It will then move on to Blockchains and their digital assets, examining them from a more theoretical perspective. Finally, it will conclude with an analysis of the Digital Euro, a project still in its embryonic stage but on which Europe is spending high resources.

# Money

The coin history started more than ten thousands of years ago and in the ages it has evolved, because needs have changed over time and the money, as instrument, had to follow the updated requirements.

From an academic point of view the definition says that money must fulfil three functions<sup>i</sup>:

1. *Medium of exchange*, means that it is a payment mechanism, that does not need to be universally chosen but it should be widely accepted in the context of use.
2. *Store of value*, means you need to be reasonably confident that your money will buy you more or less the same amount of goods or services tomorrow or in the future.
3. *Unit of account*, means you can use to compare the value of two items.



According to these rules are today moneys good? Analyzing the U.S. Dollar, which is the most prominent form of money we have today, we can say:

1. it is a pretty good medium of exchange because it is widely accepted;
2. it is an excellent unit of account because goods, for example in the market, are priced in U.S. Dollar;
3. but about the storing value, we cannot say the same things since the introduction in 1913 by the FED it has lost the 96% of purchasing power<sup>ii</sup>.

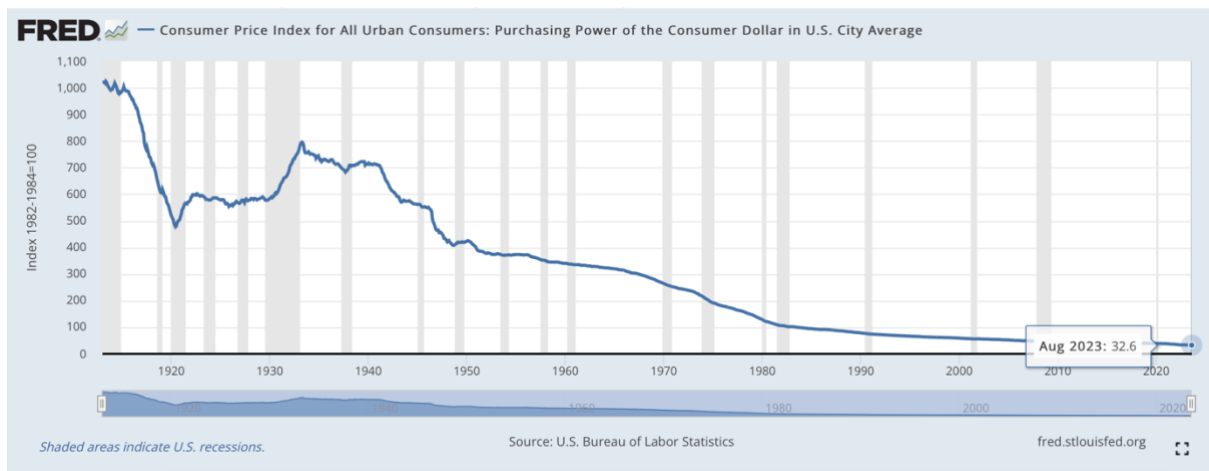


Figure 1. Consumer Price Index for All Urban Consumers: Purchasing Power of the Consumer Dollar in U.S. City Average<sup>iii</sup>

According to the graph it has been a poor store value over the long term, but this behavior is due to the inflation, introduced by the government, which reduces the purchasing power each year of small percentage.

Thus, according to the U.S. Dollar we can say it is a good kind of money but not perfect.

## History of money

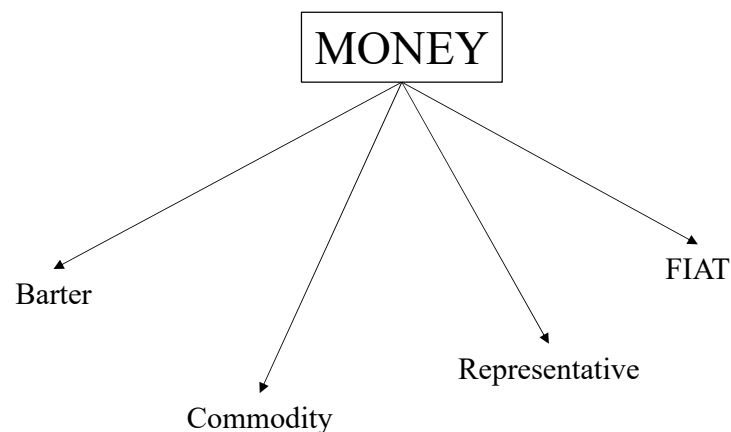
Money has not been always the same and to understand the innovative solution which we are facing now, I think it is useful to retrace the history, its successes, and failures.

Generalizing the concept there have been different moneys which were used in different ages and with different purpose<sup>iv</sup>:

1. *Barter*, before the money invention was highly common that transactions were carried by exchanging goods when both parties agreed on the deal. This kind of payment was extremely hard considering that two people must want something that the other person has but in that time. According to many theories it is probably the money was the invention that lubricate the transaction process.
2. *Commodity Money*, in which the token transacted is itself valuable, for example grain, which has intrinsic value, or precious metals, which has extrinsic value.

3. *Representative Money*, in which the token transacted is backed by the value of an underlying asset. This kind of money differs from the commodity one because it relies on third-party to be able to supply the underlying item.
4. *Fiat Currency*<sup>v</sup>, is a type of currency that is not backed by a commodity, such as gold or silver. It is typically designated and authorized by the issuing government to be legal tender, so debt repayment and tax payment have to be done with the currency declared by law. It can look like representative money, but the former has no backing, while the latter represents a claim on a commodity. Fiat money can be:

- Any money that is not backed by a commodity;
- Money declared by a person, institution or government to be legal tender meaning that it must be accepted in payment of a debt in specific circumstances;
- State-issued money which is neither convertible through a central bank to anything else nor fixed in value in terms of any objective standard;
- Money used because of government decree;
- An otherwise non-valuable object that serves as a medium of exchange (also known as fiduciary money).





## Through the ages

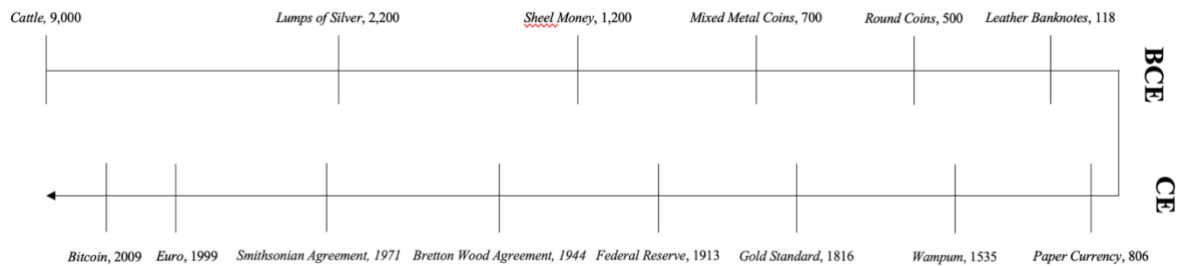


Figure 2. Money milestone timeline

Money has always been considered a tool and like all other objects it evolved to keep up with the needs in step with the time. After having taken a general look of the different typology of money let's recall which have been the exchange vehicle used in the past<sup>vi</sup>.

*Cattle, 9,000 BCE:* the earliest form of money (commodity to be more precise) were livestock, and then with the advent of agriculture also grain and vegetable plant started to be used. This is the most enduring form of money because it is still used today in some poor countries.

*Lumps of Silver, 2,200 BCE:* silver ingots started to be considered the Cappadocia's coin. This event was very important because there was the shift for the first time from using commodities that clearly have an intrinsic value to commodities that have an extrinsic value, because of their scarcity and durability.

*Sheel Money, 1,200 BCE:* it is a far example of fiat currency, they are cowry shell used for the first time in China but in some Africa's, regions survived until the mid of 1950s. They are widely available in the shallow water of the Pacific and Indian ocean.

*Mixed Metal Coins, 700 BCE:* Commodity money born in Turkey, place with a large gold supply, these are the first example of coins. They are made by a combination of gold and silver called electrum, and they are not consistently round but are created with different weights and for this reason they are not counted but are weighted.

*Round Coins, 500 BCE:* Commodity money born in China backed by the value of the base metal of which they are made, so it is extremely low.

*Leather Banknotes, 118 BCE:* First example of banknote documented in China made by deerskin leather with colorful borders.

*Paper Currency*, 806 CE<sup>vi</sup>: The first known paper banknotes appeared in China, it was used over 500 years, from the ninth through the fifteenth century. Over this period, too many paper notes were printed to the point that their value rapidly depreciated and inflation soared. Then beginning in 1455, the use of paper money in China disappeared for several hundred years. This was still many years before paper currency would reappear in Europe, and three centuries before it was considered common.

*Wampum*, 1535 CE: a monetary exchange method used by North American Indians made by strings of beads made from clam shells.

*Gold Standard*, 1816 CE<sup>vi</sup>: Representative Money, gold was officially made the standard of value in England in 1816. At this time, guidelines were made to allow for a non-inflationary production of standard banknotes which represented a certain amount of gold. Before Banknotes had been used for several hundred years but their worth had never been tied directly to gold.

*Federal Reserve*, 1913: the Federal Reserve Act was passed into law in the USA and created the FED the central banking system in USA. It has the mandate to maximize the employment and ensure price stability as today.

*Bretton Wood Agreement* 1944: In 1944, the Bretton Woods agreements were signed between the major industrialized countries of the western world. This project was a gold exchange standard, based on fixed exchange ratios between currencies, all pegged to the dollar, which in turn was pegged to gold, at \$35 per ounce (around 28 grams).

*Smithsonian Agreement* in 1971: the Smithsonian Agreement was signed by Nixon, ending the era of the gold-dollar standard. It was signed because it created monetary chaos between states and stopped converting dollars at the official exchange rate of \$35 per ounce, which had been decided in the 1944 agreements. The gold standard was abandoned, and Dollar became pure FIAT money.

*Euro*, 1999: On 1st January 1999, the Euro officially became the currency of the member states of European Union but in circulation came in 2002. This is the currency of nineteen of the current twenty-eight EU states.

*Bitcoin*, 2009: on 3<sup>rd</sup> January 2009 the first Bitcoin was mined into existence. Maybe it is premature classifying Bitcoin as a money standard but I think it is correct because shares some properties common associated with the money and so it can stay alongside the other forms.

*Digital Euro*, expected in next years: It would be a central bank digital currency, an electronic equivalent to cash and it would complement banknotes and coins, giving people an additional choice about how to pay<sup>vii</sup>.

## **Money's essence**

As seen, money has evolved enormously over the years, from instruments with very high intrinsic value (cattle's barter), to others with extrinsic value, to conclude with currencies (fiat one) which its value comes from only being declared "legal tender" by the government of the issuing country.

About this the European Central Bank says<sup>viii</sup>:

*"The nature of money has evolved over time. Early money was usually commodity money – an object made of something that had a market value, such as a gold coin. Later on, representative money consisted of banknotes that could be swapped against a certain amount of gold or silver. Modern economies, including the euro area, are based on fiat money. This is money that is declared legal tender and issued by a central bank but, unlike representative money, cannot be converted into, for example, a fixed weight of gold. It has no intrinsic value – the paper used for banknotes is in principle worthless – yet is still accepted in exchange for goods and services because people trust the central bank to keep the value of money stable over time. If central banks were to fail in this endeavour, fiat money would lose its general acceptability as a medium of exchange and its attractiveness as a store of value".*

Once familiarized with this concept, one of the great criticisms made of cryptocurrencies: "they have no intrinsic value" automatically loses sense because the intrinsic value does not make a currency important, but it is only its level of utility (in this case guaranteed by the legal tender) that really matters thus maybe if governments authorize blockchain digital assets to be legal tender would its use increase? Answer to this question is extremely complicated and perhaps premature but I hope in the future there will be the opportunity to test that.

In the next chapter I will analyze in a more technical way the two most famous digital assets: Bitcoin and Ethereum, comparing weakness, strengths and trying to explain which features could be extremely useful nowadays.

## **Blockchain**

In this chapter will be discussed about digital assets, mistakenly called cryptocurrencies. Since the concept is hard to understand, I think it is useful to start with a definition:

*“A cryptocurrency is a digital asset that is transactions are verified and records maintained by decentralized system using cryptography, rather than by a centralized authority”<sup>ix</sup>.*

If this definition does not give you further information is normal, but during this chapter will be explained the reason why this word is one of the most researched on Google in the last years, trying to give you some technical concepts useful to enter in the line of thinking of this technology.

There are so many Blockchains, around 1 million, each with different rules and mechanisms and for this reason it is not easy to generalize exactly.

Bitcoin, the most widespread and the first to be analyzed, was born in the 10s and from that event hundreds of users started to fond with this which is interesting and at the same time difficult to understand.

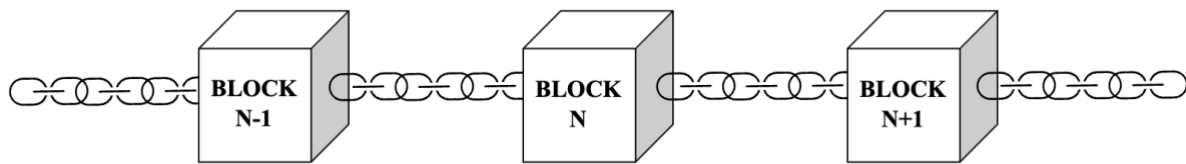
The second one under our magnifying glass is Ethereum which enter in the market in 20s, it shakes up the concept of digital assets introducing the ‘‘Smart Contract’’ which gives the possibility to use the Blockchain technology to execute contract without the need of judges or other kind of third parties, but only with a program.

## **DLT vs Blockchain**

Many times, one hears about DLT and Blockchain and often these two terms are interchanged. In reality, they have two different but close meanings and before introducing digital assets, it is important to clarify this.

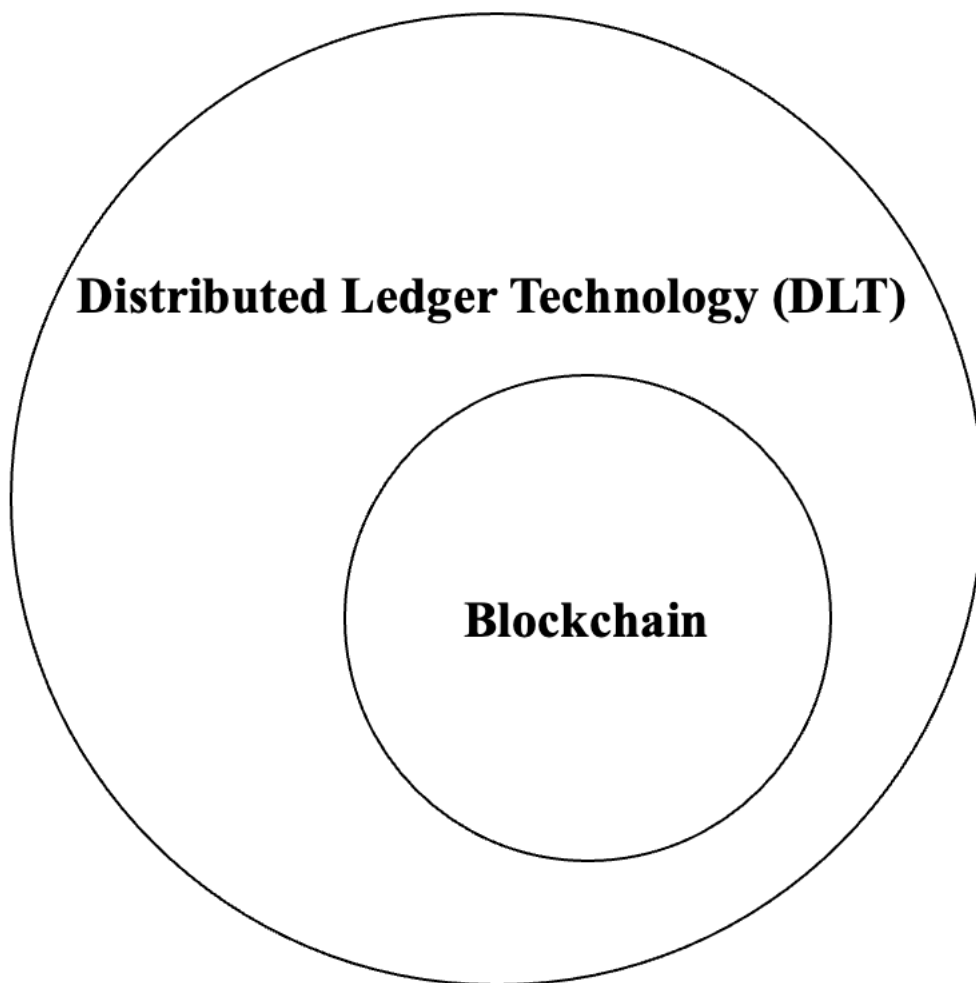
DLT, *Distributed Ledger Technology*, is a database that exists in duplicate across multiple points of a network. It is shared, replicated, and synchronized between many participants that are spread across geography. On the other hand, Blockchain essentially is a kind of DLT where

data are stored in blocks and arranged on a chain, ensuring greater security through a more complex sorting method.



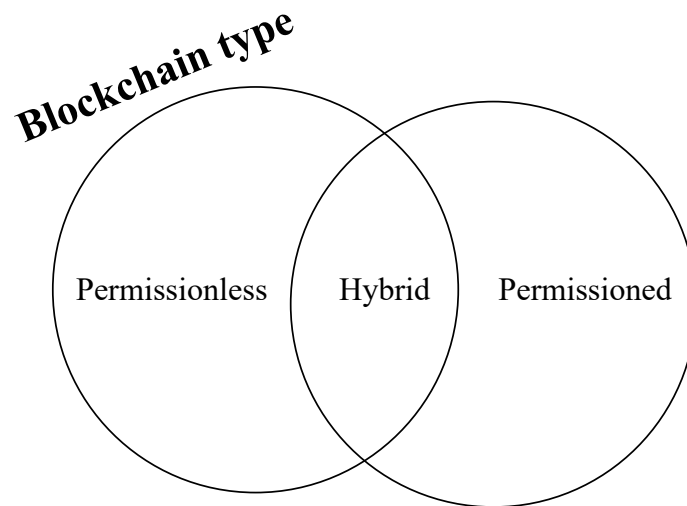
*Figure 3. Blockchain*

Thus, DLT is a tree and the blockchain is a branch of this tree, because all blockchains are DLTs but the contrary, it is not guaranteed.



*Figure 4. DLT vs Blockchain*

Getting slightly more specific within them, blockchains are divided into permissionless and permissioned by type of access, which in the latter case are regulated, often by consortia or individual entities, and only those with access privileges can participate in the network. Then there are some hybrid forms in which there is a single authority with some permissionless processes.



*Figure 5. Blockchain types*

In our case, however, the permissioned forms do not interest us, and we are going to study architectures where everyone can become an active and integrated part of the processes.

## **Before 2008**

The development of digital money is closely linked to cryptography developments, as it provides the basis for trusting the legitimacy of a user's claim to value, because is used as digital signatures to complete and validate transactions.

In the late 80s, researchers began building digital assets, often backed by a national currency or precious metal, as an innovative representative money. These early digital currencies were centralized and easy to attack by governments and hackers and to avoid that, a decentralized digital currency, which is free from central authority, was started to be studied... From that Bitcoin or Ethereum were born.

Before we begin, it is worth pointing out a lexical caveat: “Bitcoin” refers to infrastructure while “bitcoin” to its digital assets.



## Bitcoin

*“A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.<sup>x</sup>”*

People think bitcoin as a digital currency, but it may be easier to consider it as an electronic asset. The term currency often side-tracks people when they are trying to understand Bitcoin because they are often too bound with aspects of conventional currency which do not apply to Bitcoin (what backs it or who sets the interest rate), despite that its purpose is to replace the national currencies during the financial crisis of 2008 an outdated digital payments technology, but during that years the development and studies lead to consider it an electronic resource.

Behind the scenes, Bitcoin is also the name of a protocol, and its currency is only the first application of the present invention. The culmination of decades of research in cryptography and distributed systems, Bitcoin includes his four major innovations brought together:

1. *Decentralized peer-to-peer network* (Bitcoin protocol);
2. *Public ledger* (Blockchain);
3. A set of rules (*consensus rules*) for independent transaction validation and currency issuance;
4. Mechanisms for achieving global decentralized consensus on valid blockchains (*proof-of-work algorithms*).

## **How does Bitcoin work?**

Bitcoin is developed by an open community of volunteers. At first, that community consisted of only Satoshi Nakamoto, instead now Bitcoin's source code had more than 600 contributors.

The software used to run the blockchain is "Bitcoin Core" and it includes various functions such as wallet management, transaction verification, mining support, network communication, consensus protocol, security, and privacy but these topics will be discussed later because they are too hefty to be analyzed in few lines.

*"Create a worldwide electronic payment system that cannot be censored, and to allow anyone the ability to send payments"*<sup>x</sup>, this is the objective to keep in mind to understand Bitcoin. As we can imagine a lot of constraints derive from the sentence and thus, an analysis will be provided here.

### **Account creation**

Applications around the world works with an administrator who provide the service and manage the new membership. He must set up an account and assign it to you when you ask for the creation. This structure goes against the privacy policy desired by the community and thus, it cannot be taken in consideration by Nakamoto.

They want a way to open account without ask permission and it can only be possible with the implementation of cryptography, which is a branch of mathematics used in computer security to prove the authenticity and the knowledge of data without revealing it.

Bitcoin ownership is established through a private key composed by numbers and letters picked randomly that allows you to access your wallet in. From that is derived firstly the public key and then the addresses through a hash function. The addresses are like an email and identify a specific destination for transactions instead the public key is more like a Name or Surname which enables you to make different addresses that gives you the Bitcoin control.



Figure 6. Private key, public key, and bitcoin address

The useful property of asymmetric cryptography is the ability to generate digital signatures. From a private key can be possible to produce a numerical signature which can only be produced by someone with knowledge of the private key. This useful property of asymmetric cryptography makes it possible for anyone to verify every signature on every transaction, while ensuring that only the owners of private keys can produce valid signatures.

## Decentralization

Once the third-party administrator in creating account has been eliminated, he still has the role of central bookkeepers, the coordinator who maintains the list of transactions you request against some business and technical rules. It can be thought as a financial institution which manage the inflow and outflow of cash. So, for a digital cash system the control and censorship provided by this third party must be removed.

The most people you share a secure system and its information, the less vulnerable is to manipulation, so the solution is to remove hierarchy and enlarge the possibility to everyone to became bookkeepers by broadcasting all new transactions to all active actors via gossip network (in which each actor relays new payment to as many others as they are connected to).

In this new protocol if someone is forced to stop work, the other can continue, thus it is also more resilient.

**Block: to prevent transaction ordering problems<sup>xi</sup>**

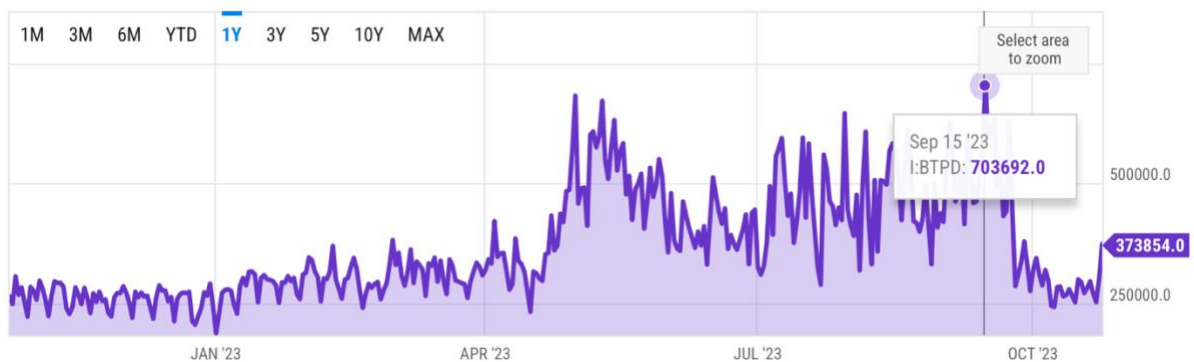


Figure 7. Bitcoin transactions per day.

Now as I am writing there are hundreds of transactions on the blockchain, on average Bitcoin handles 400 thousand, and since bookkeepers stays around the world what happens if a Chinese node receive transaction A before B and instead an Italian one receives the B before the A? There are many different factors which influenced the transmission of a message around the net and the solution is to create block, a container of transactions, which dimension is around 1 MB. It is composed by block size, block header, the transactions counter and transactions their selves.

Dimensions in bytes	Field	Representation
4	Block Size	Block dimension.
80	Block Header	Block title
5	Transaction counter	Transactions number
It depends	Transactions	The block heart, with the transaction inside

They are created less frequently than transaction, on average every 10 minutes, (but different cryptocurrencies have different mining time, as we will see, due to the difficulty and the

composition of the block) and it is more likely that when created it reaches the other bookkeepers before another one is created.

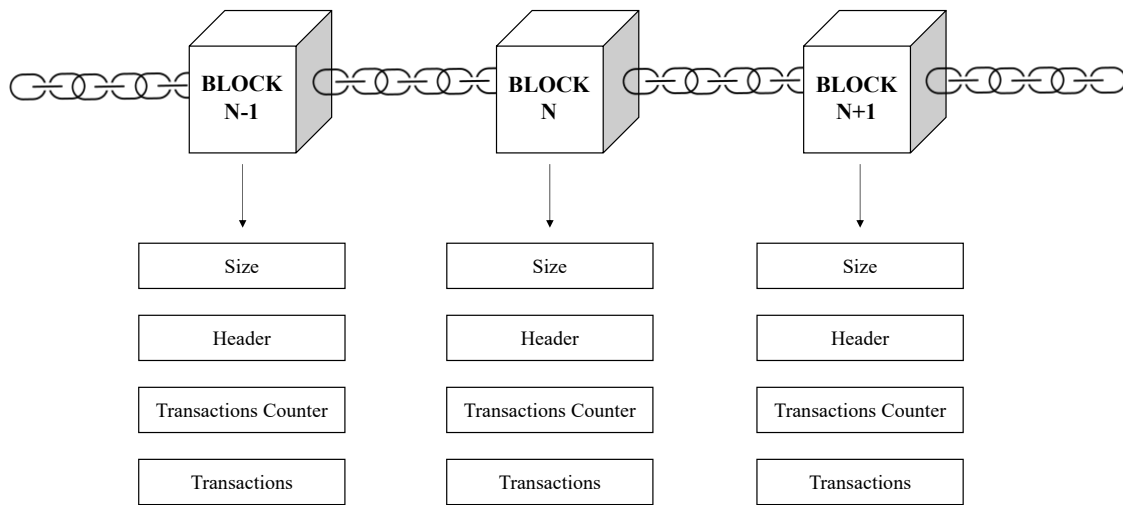


Figure 8. Block composition

## Block Header

Going more deeply in the analysis of the block header

Dimensions in bytes	Field	Representation
4	Version	Version number
32	Previous Block Hash	Previous Hash of the chain
32	Merkle Root	Merkle tree's hash root
4	Timestamp	Creation time approximated
4	Difficulty target	Target for the PoW
4	Nonce	Counter of the PoW

First, we have a reference to the previous block hash that connects this block to the previous in the blockchain. His second set of metadata, namely difficulty, timestamp and nonce, are related to the mining competition which will be discussed later on. The third piece is the “*Merkle Tree*

*Root*”, it acts as an overview of all the data in the tree. It represents the entire dataset without revealing the underlying details of each leaf node. It works by pairing two hashed transactions two by two and then recursively hashed until there is only one hash called *root*. Merkle roots are important for efficient and secure verification of data integrity because it enables efficient validation and consistency checking of large datasets.

Rather than comparing all the data individually, participants can simply compare a small number of hashes to Merkle roots, to verify that they contain specific data. This reduces the computing and memory requirements for checking data integrity.

A total of 2,330.65 BTC (\$62,694,876) were sent in the block with the average transaction being 0.9909 BTC (\$26,655.36). AntPool earned a total reward of 6.25 BTC \$168,125. The reward consisted of a base reward of 6.25 BTC \$168,125 with an additional 0.3051 BTC (\$8,207.24) reward paid as fees of the 2,352 transactions which were included in the block.

Details	Mined on September 19, 2023 10:15:40		
Hash	00000-c73ef	Depth	1
Capacity	139.12%	Size	1,458,829
Distance	7m 51s	Version	0x20400000
BTC	2,330.6516	Merkle Root	2a-60
Value	\$62,694,876	Difficulty	54,150,142,369,480.00
Value Today	\$62,705,807	Nonce	359,936,336
Average Value	0.9909232819 BTC	Bits	386,216,622
Median Value	0.01550875 BTC	Weight	3,993,625 WU
Input Value	2,330.96 BTC	Minted	6.25 BTC
Output Value	2,337.21 BTC	Reward	6.55509756 BTC
Transactions	2,352	Mined on	19 Sep 2023 at 10:15:40
Witness Tx's	2,011	Height	808,408
Inputs	6,620	Confirmations	1
Outputs	8,836	Fee Range	0-331 sat/vByte
Fees	0.30509756 BTC	Average Fee	0.00012972
Fees Kb	0.0002091 BTC	Median Fee	0.00005224
Fees kWU	0.0000764 BTC	Miner	AntPool

Figure 9. <https://www.blockchain.com/explorer/blocks/btc/808408>, Bitcoin Block 808,408.

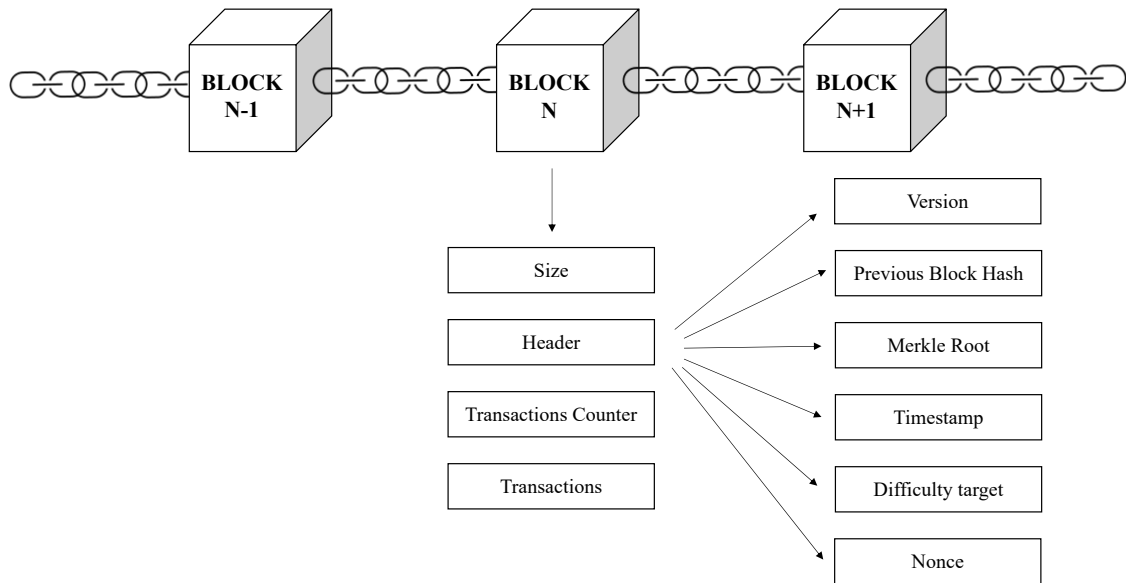


Figure 10. Block header composition

## Blockchain characters

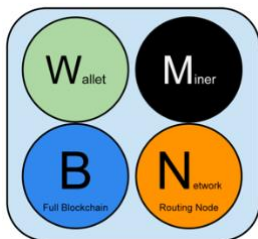


Figure 11. A Bitcoin node with all four functions<sup>31</sup>.

In the network every node is peer to the other, but it can have different roles depending on the functionality supported. These are four: routing (which is required to participate the network), the blockchain database, mining and wallet services.

Mining nodes compete to create new blocks by running specialized hardware to solve the Proof-of-Work algorithm. Some mining nodes are also full nodes, maintaining a full copy of the blockchain, while others are lightweight nodes participating in pool mining and depending on a pool server to maintain a full node.

There are 4 types of nodes:

1. *Bitcoin Core*: it is also called “full node” and maintains a complete and up-to-date copy of the Bitcoin with all the transactions, which they independently build and verify, starting with the very first block, *genesis block*;
2. *Full Block Chain Node*: it contains the full blockchain database and the network routing node (no wallet and mining functions), it works as a transactions recorder;

3. *Solo Miner*: it is a “full block chain node” but with the mining function;
4. *Lightweight Wallet*: it contains a wallet and a network node without a blockchain.

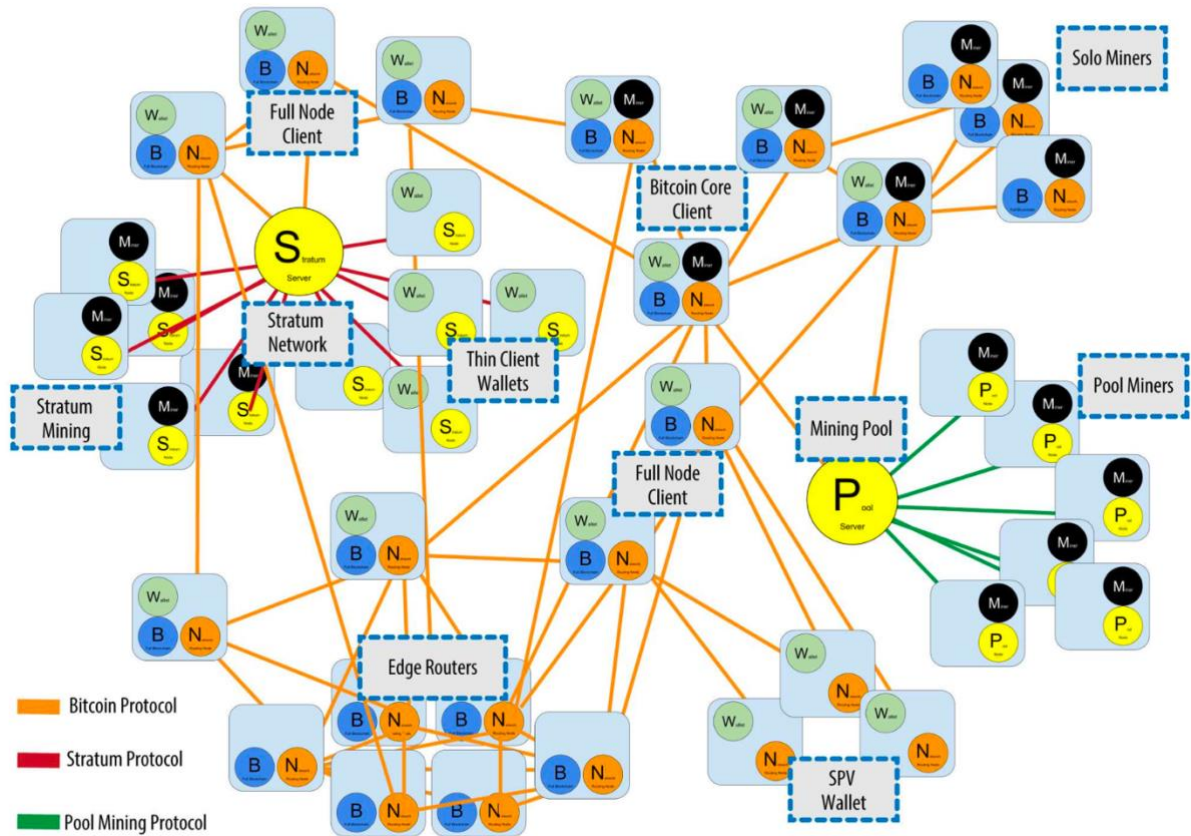


Figure 12. The extended bitcoin network showing various node types, gateways, and protocols<sup>xi</sup>.

In the figure the Bitcoin protocol, which is run by the nodes with inside the Network routing node, is followed by Stratum and Pool Mining protocol which are both strategies to facilitate the expensive mining task by dividing the efforts and the hardware between a pool of nodes.

### Proof-of-Work

As said before, we know blocks are created every 10 minutes but is there a special rule to make pointless for someone to try to create blocks at a more frequent interval? The answer is given by the Proof-of-Work algorithm.

Miners participate in this game in which the “only” constraint is to find an output which is smaller than the target, as seen in the figure 5 under the field “*Difficulty*”.



Before explaining the process, I think, it is better to give a definition of what hash is.

*“Hash is an irreversible math function which produce a sequence of bits, called a digest, closely correlated with the input data.”*

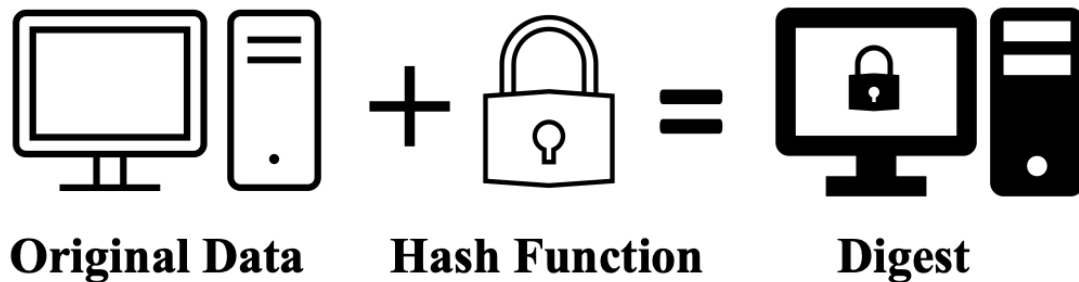


Figure 13. Process of hashing easily explained

In the big family of hash function, we will find the SHA-256 (Secure Hash Algorithm) which is used by Bitcoin in the Proof-of-Work algorithm (and in the creation of addresses). The main feature of this algorithm is that it is practically impossible to find two distinct input that generate the identical output because a small difference in the data means a large change in the result.

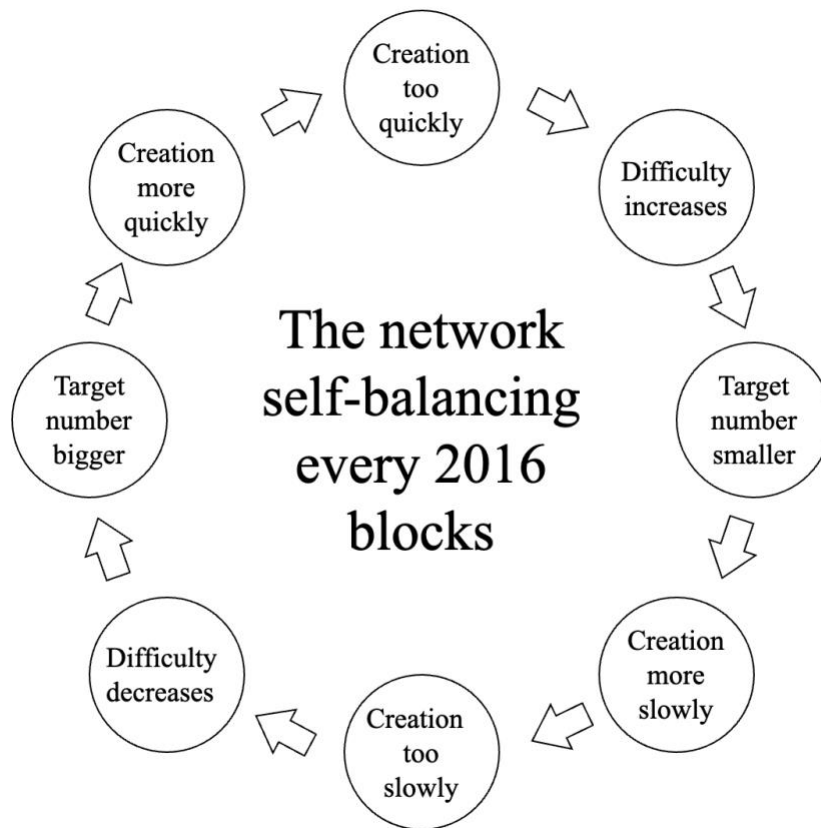
The input in the PoW is the block header and the game is to find a digest lower than the target.

This is done by many attempts and if the result does not satisfy the requirement the miner will adjust the nonce (typically by incrementing it by one) and re-execute the SHA algorithm. So, the probability of successfully mining a block increase in proportion to the amount of hashing power you possess.

As computers improve, they will be able to solve these puzzles faster and to compensate that, the difficulty of the blockchain is periodically increased, on average every 2 weeks.

$$\text{New Target} = \text{Old Target} * \left( \frac{\text{Actual Time of Last 2016 Blocks}}{20160 \text{ minutes}} \right)$$

This is the function run every 2 weeks to check if the difficulty must be increased, decreased or keep the same.



This is an example of Proof-of-Work algorithm implementation. As we can see the nonce, property of the block, is fundamental for the implementation of the algorithm because is the only input which is incremented to loop run the “while cycle” until the hash target is reached.<sup>xiii</sup>

```

class Block{
    constructor (index, timestamp, data, previousHash = ''){

        //we keep track of our properties here
        this.index = index;
        this.timestamp = timestamp;
        this.data = data;
        this.previousHash = previousHash;
        this.hash = this.calculateHash();

        //nonce property
        this.nonce = 0;
    }

    //calculating the hash value with the nonce property
    calculateHash(){
        return SHA256(this.index + this.previousHash +
this.timestamp + JSON.stringify(this.data) +
this.nonce).toString();
    }
}
  
```

```

//Method to mine a block
mineBlock(difficulty){
    //while loop conditional used is a quick trick to make
the substring of hash values exactly the lenght of difficulty
    while(this.hash.substring(0, difficulty) !==
Array(difficulty + 1).join("0"))
    {
        //incrementing the nonce value everytime the loop
runs.
        this.nonce++;

        //recalculating the hash value
        this.hash = this.calculateHash();
    }

    //logging when a block is created
    console.log("Block mined: " + this.hash);
}

```

## Rewards

This tedious procedure needs resources which are expensive as computers and electricity. In exchange for their mining efforts, miners receive rewards in the form of newly coins, with each block and transaction fees collected from the transactions included in the block.

In the latter block-creator gets a commission equal to the small percentage from each transaction and thanks to this the ones with the highest fees are prioritize over those with lower fees. As all Market-Based approach, fees tend to go up in times where there are many transactions and down when queues are emptier.

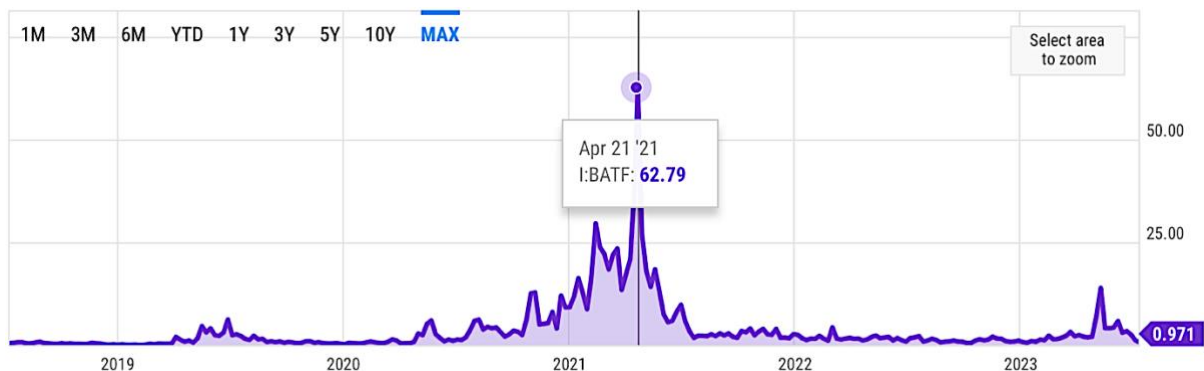


Figure 14. The graph shows how transaction fees are varied during the years.<sup>xiii</sup>

The second payment received is called Block Reward which is the primary means of introducing new coins into circulation. When miners successfully mine a new block, they

receive an amount of cryptocurrency as a reward which is determined by the protocol and undergoes periodic halving to regulate the pace of coin creation. For instance, it began at 50 bitcoins and has experienced multiple halving events, resulting in a reduced reward of 6.25 bitcoins as of August 2023 and the next halving will be approximately in 2024 and it will drop the reward to 3.125 BTC. Until now it is announced the number of bitcoin releases will be stopped at 21 million<sup>xiv</sup>.

```
CAmount GetBlockSubsidy(int nHeight, const Consensus::Params&
consensusParams)
{
    int halvings = nHeight /
consensusParams.nSubsidyHalvingInterval;
    // Force block reward to zero when right shift is undefined.
    if (halvings >= 64)
        return 0;

    CAmount nSubsidy = 50 * COIN;
    // Subsidy is cut in half every 210,000 blocks which will
occur approximately every 4 years.
    nSubsidy >>= halvings;
    return nSubsidy;
}
```

`int halvings` give us the integer number (approximated by default) of halving done until that block and to avoid loop situation if the number is too high the function returns zero and so there is not block reward.

For example, `int halvings = 740,805 / 210,000` or `int halvings = 3.52764286` (rounds to 3).

The most crucial part of the “`nSubsidy`” is the “`>>`” or “*bitwise right shift*” operator. In the C++ programming language, this operator is commonly used for bitwise shifting (easily a shift of the bit right or left). In this context, it represents an “arithmetic shift to the right by one bit”, which is equivalent to dividing by two. This operator is significant because it demonstrates how the supply schedule determines the stopping point for division.

Ex. A `>>3` shifts our initial binary number by three spaces to the right, which drops the three furthest digits and creates another new number.

Before (in 2009): 10010101000000101111100100000000 (or 50 BTC)

After 3 halvings: 100101010000001011111001000000 (or 6.25 BTC)

Block rewards in a blockchain ecosystem have several important purposes:

1. *Incentive*: because they motivate miners to invest computational power and resources in mining, fostering competition and ensuring network security.

2. *Coin Distribution*: Block rewards enable a fair and decentralized distribution of newly created cryptocurrency coins, providing a mechanism for equitable participation in the network.

3. *Transaction Confirmation*: Miners' validation and confirmation of transactions are vital to blockchain functionality. Block rewards serve as compensation for their efforts and the resources expended in this process.

Overall, block rewards play a vital role in motivating miners, distributing coins, and compensating validators within the blockchain ecosystem.

1 BTC = 100,000,000 SAT

H	Binary Number	Units of <i>COIN/SAT</i>	Bitcoin
–	10010101000000100000000000000000	5,000,000,000	50 BTC
1	10010101000000100000000000000000	2,500,000,000	25 BTC
2	10010101000000100000000000000000	1,250,000,000	12.5 BTC
3	10010101000000100000000000000000	625,000,000	6.25 BTC
4	10010101000000100000000000000000	312,500,000	3.125 BTC
5	10010101000000100000000000000000	156,250,000	1.5625 BTC
6	10010101000000100000000000000000	78,125,000	78,125,000 SAT
7	10010101000000100000000000000000	39,062,500	39,062,500 SAT

8	10010101000000100000000000	19,531,250	19,531,250 SAT
9	1001010100000010000000000	9,765,625	9,765,625 SAT
10	100101010000001000000000	4,882,812	4,882,812 SAT
11	10010101000000100000000	2,441,406	2,441,406 SAT
12	1001010100000010000000	1,220,703	1,220,703 SAT
13	100101010000001000000	610,351	610,351 SAT
14	10010101000000100000	305,175	305,175 SAT
15	100101010000001000	152,587	152,587 SAT
16	10010101000000100	76,293	76,293 SAT
17	1001010100000010	38,146	38,146 SAT
18	100101010000001	19,073	19,073 SAT
19	10010101000000	9,536	9,536 SAT
20	1001010100000	4,768	4,768 SAT
21	100101010000	2,384	2,384 SAT
22	10010101000	1,192	1,192 SAT
23	1001010100	596	596 SAT
24	100101010	298	298 SAT
25	10010101	149	149 SAT

26	1001010	74	74 SAT
27	100101	37	37 SAT
28	10010	18	18 SAT
29	1001	9	9 SAT
30	100	4	4 SAT
31	10	2	2 SAT
32	1	1	1 SAT

*Figure 15 these are all the bitwise right shifts that occurs every 210,000 block*

The concept behind this is to initially utilize block rewards as a catalyst for the system and subsequently reduce their significance over time, moving to transaction fees as the primary source of incentives, since after the 21 million reached no more bitcoin will be issued. This is also the reasons why Bitcoin is considered a deflationary currency.

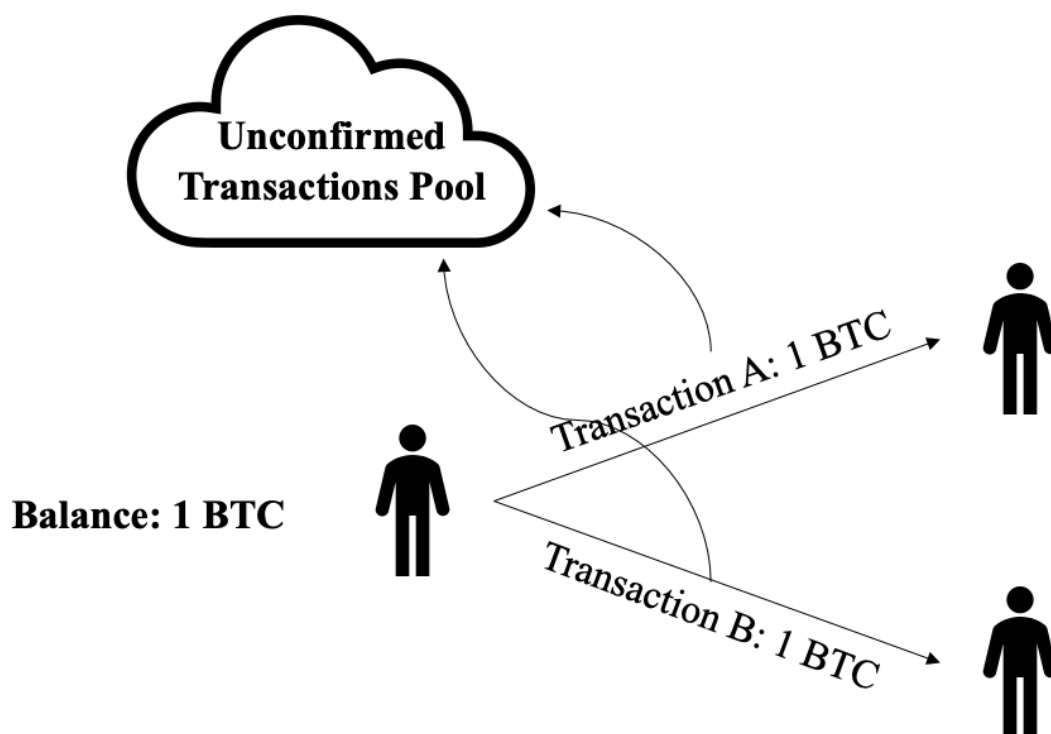
### **Longest chain rule**

What happens if a bookkeeper receives two valid blocks from two different block-creators and they both reference the hash of the same previous block? The solution is granted by the ‘‘Longest chain rule’’. It states that the valid Blockchain is determined by the chain with the highest total proof-of-work or computational work accumulated. Proof-of-work refers to the computational effort miners put in to solve the required mathematical problems and add new blocks.

According to this rule, the chain with the greatest cumulative proof-of-work is considered valid, and thus all other competing chains are deemed invalid. Miners always aim to extend the longest chain by adding new blocks, ensuring consensus and network security.

The longest chain rule is crucial for securing the Bitcoin network. It prevents potential attacks and ensures that most participants are needed to alter the established transaction history. Manipulating the blockchain would require an attacker to possess more computational power than all other honest miners combined, making it highly challenging and expensive.

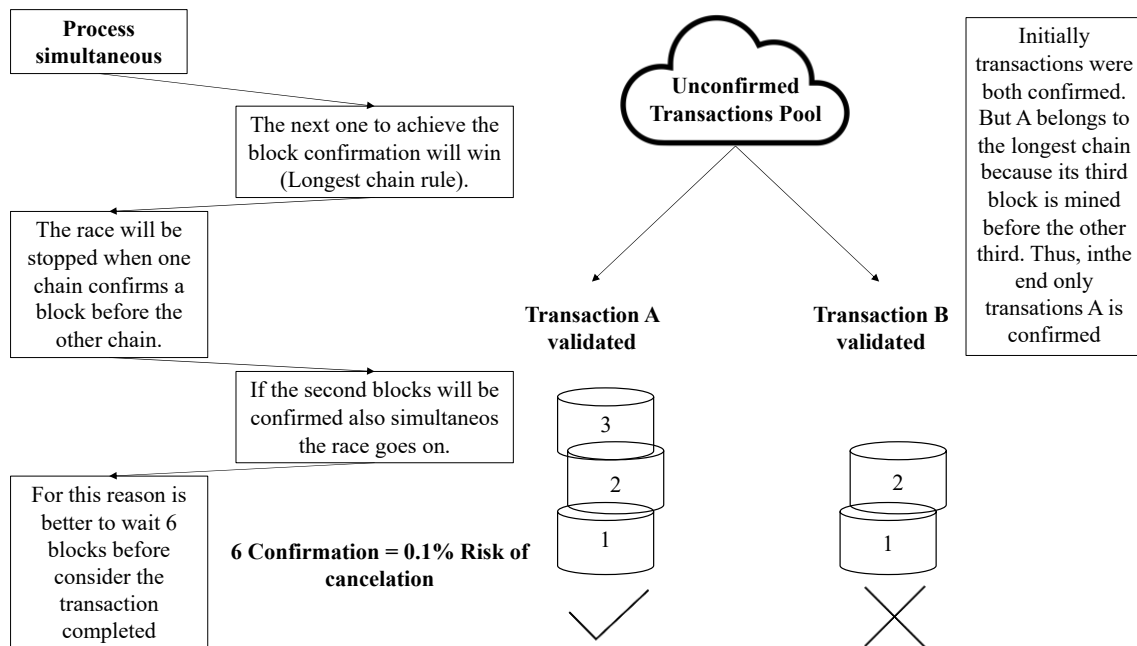
### Double Spending Problem



What happens instead if someone create two transactions using the same bitcoins? One payment to for example to an online retailer and the other to him/herself? With the longest chain rule maybe, it is possible that the first valid transaction will be orphaned (it means that belongs to a block in the shortest chain) so the payment will be never recorded on the chain instead the other yes.

Thus, if the process happens simultaneously a race will be opened, and the one which will achieve first the block confirmation will win. This can continue for a high number of block and for this is advised to wait 6 blocks before considering a transaction confirmed and so valid with a low percentage risk, around the 0.1%.





## Transactions

The core aspect of the Bitcoin system revolves around transactions, as they hold utmost significance. All other components within Bitcoin are specifically designed to facilitate the creation, distribution, verification, and eventual inclusion of transactions into the universal record in the blockchain. Despite that we must step back because it is important to introduce the *wallet*. BTCs are recorded in the Bitcoin's Blockchain which contains all the transactions and no accounts' balances as many people thought. The wallet, instead, contains "only" the user's keys (one or more).

Once we understand this we can go into more detail regarding the transactions. They represent distinct portions of bitcoin currency that are *indivisible*, recorded on the blockchain, and universally acknowledged as legitimate by the entire network. Bitcoin full nodes meticulously monitor all available and usable outputs, referred to as "*Unspent Transaction Outputs*" (UTXO), discrete and indivisible units of value, denominated "Satoshi" (SAT).

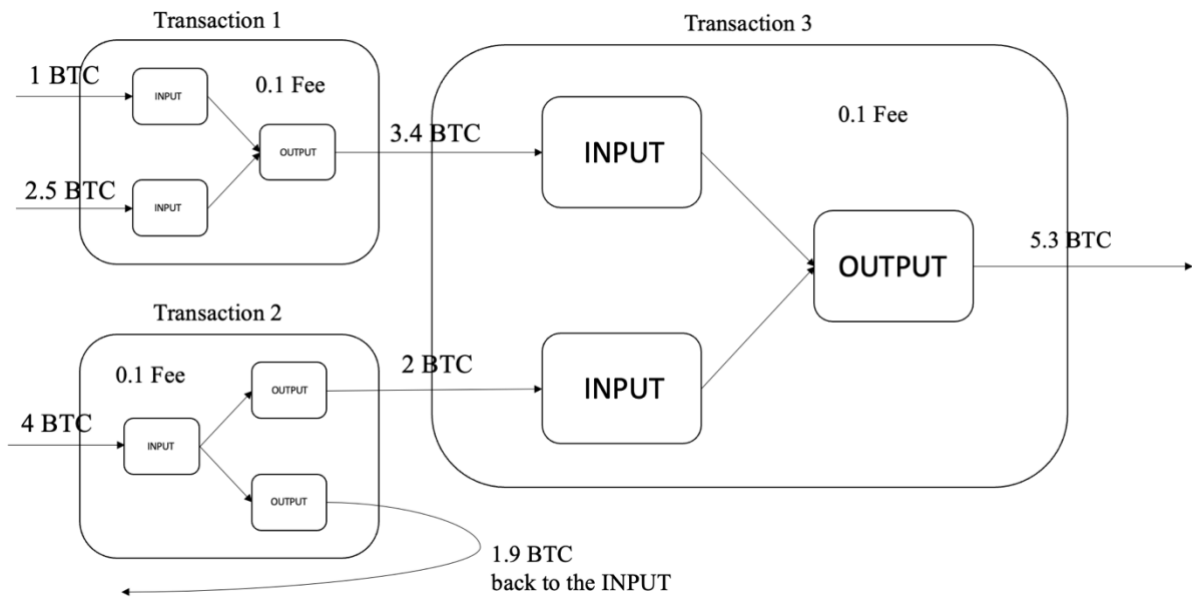


Figure 16. Bitcoin transactions and UTXOs.

In transaction 2 the buyer has a UTXO equal to 4 BTC and the payment require only 2 BTC so, the output is divided in two: one to the seller and the other as new UTXO to the buyer.

Summary			
This transaction was first broadcasted on the Bitcoin network on December 28, 2013 at 12:12 PM GMT+1. The transaction currently has 521,102 confirmations on the network. The current value of this transaction is now \$765,149.			
Advanced Details			
Hash	d5ad-ba2f ☒	Block ID	277,316
Time	28 Dec 2013 12:11:54	Age	9y 6m 15d 17h 30m 54s
Inputs	1	Input Value	—
Outputs	1	Output Value	\$0.00
Output Value	25.09094928 BTC \$765,149	Fee	0 BTC \$0.00
Fee/B	-	Fee/VB	-
Size	110 Bytes	Weight	440
Weight Unit	-	Coinbase	Yes
Witness	No	RBF	No
Locktime	0	Version	1
BTC Price	\$30,495.02		

When we receive bitcoin in our wallet it means it has been detected a UTXO that can be spent with one of the keys controlled by our wallet. Thus, a user’s bitcoin “balance” is the sum of all

UTXO that user's wallet can spend and which may be scattered among hundreds of transactions and hundreds of blocks.

In general, transactions are made of an output (new UTXO) and an input (old UTXO), except for the one called the "coinbase" transaction, the first which appears in a new block which contains the miner's reward for the mining effort. The reward consists in new-coin base reward and the transaction fees.

```
{
  "txid":
"d5ada064c6417ca25c4308bd158c34b77e1c0eca2a73cda16c737e7424afb
a2f",
  "size": 110,
  "version": 1,
  "locktime": 0,
  "fee": 0,
  "inputs": [
    {
      "coinbase": true,
      "txid":
"0000000000000000000000000000000000000000000000000000000000000000
000",
      "output": 4294967295,
      "sigscript": "03443b0403858402062f503253482f",
      "sequence": 4294967295,
      "pkscript": null,
      "value": null,
      "address": null,
      "witness": []
    }
  ],
  "outputs": [
    {
      "address": "1MxTkeEP2PmHSMze5tUZ1hAV3YTKu2Gh1N",
      "pkscript":
"2102aa970c592640d19de03ff6f329d6fd2eecb023263b9ba5d1b81c29b52
3da8b21ac",
      //value in Satoshi
      "value": 2509094928,
      "spent": true,
      "spender": {
        "txid":
"6856b45c47423ef184a54a206a10c2e5c365cb147e608a899a3a08eb051df
72c",
        "input": 0
      }
    }
  ],
}
```

```

"block": {
  "height": 277316,
  "position": 0
},
"deleted": false,
"time": 1388185914,
"rbf": false,
"weight": 440
}

```

Once explained all the elements to understand a Bitcoin transaction we can summary and follow step by step each phase:

1. The wallet creates the transaction and assign it to output owner (UTXO);
2. The transaction is sent to the neighboring nodes and at the same time they check and validate. This guarantee only valid transactions are propagated across the network;
3. The transaction is added to a memory pool where transactions await until they can be included into a *candidate* block;
4. Once built the miner start to resolve the Proof-of-Work algorithm to win the game and receive the reward.

Here an example, the first image is a block refers to the coinbase transaction before, mined in 2013, instead the second is a block mined this year.

Details			
Hash	00000-7bdc4 6	Depth	521,108
Capacity	20.85%	Size	218,629
Distance	9y 6m 15d 18h 13m 39s	Version	0x2
BTC	10,296.9863	Merkle Root	c9-2e 6
Value	\$7,382,939	Difficulty	1,180,923,195.26
Value Today	\$313,369,213	Nonce	924,591,752
Average Value	24.5751462436 BTC	Bits	419,668,748
Median Value	0.45180000 BTC	Weight	874,516 WU
Input Value	10,297.08 BTC	Minted	25.00 BTC
Output Value	10,322.08 BTC	Reward	25.09094928 BTC
Transactions	419	Mined on	28 Dec 2013 at 00:11:54
Witness Tx's	0	Height	277,316
Inputs	1,009	Confirmations	521,108
Outputs	1,472	Fee Range	0-444 sat/vByte
Fees	0.09094928 BTC	Average Fee	0.00021706
Fees Kb	0.0004160 BTC	Median Fee	0.00010073
Fees kWU	0.0001040 BTC	Miner	Unknown

Details			
Hash	00000-61328 ☹	Depth	4
Capacity	157.98%	Size	1,656,513
Distance	9y 6m 15d 18h 23m 30s	Version	0×20004000
BTC	2,419.5398	Merkle Root	48-08 ☹
Value	\$73,691,779	Difficulty	53,911,173,001,054.59
Value Today	\$73,646,365	Nonce	3,819,327,135
Average Value	0.9396271252 BTC	Bits	386,218,132
Median Value	0.00259820 BTC	Weight	3,992,682 WU
Input Value	2,419.68 BTC	Minted	6.25 BTC
Output Value	2,425.93 BTC	Reward	6.39030090 BTC
Transactions	2,575	Mined on	12 Jul 2023 at 19:16:08
Witness Tx's	2,376	Height	798,421
Inputs	7,932	Confirmations	4
Outputs	6,392	Fee Range	0-136 sat/vByte
Fees	0.14030090 BTC	Average Fee	0.00005449
Fees Kb	0.0000847 BTC	Median Fee	0.00002280
Fees kWU	0.0000351 BTC	Miner	Unknown

As we can see the difficulty and the transaction's number increased and the reward to the miners decreased due to Bitcoin's value (from around 700\$ in 2013 to 30,500\$ in 2023).

## Governance

One of the greatest enigmas of the 21st century stems from the realm of cryptocurrency, specifically the identity of Satoshi Nakamoto. The question of "Who is Satoshi Nakamoto?" has captivated the world, as this figure remains shrouded in mystery and speculation.

In February 2009, Satoshi Nakamoto created the first-ever online message board post exclusively dedicated to cryptocurrency on the P2P Foundation forum. In this seminal post, Nakamoto introduced Bitcoin, and since that moment thousands of people have joined the community. In 2023, the number of Bitcoin miners had surpassed one million, working to verify the data that constitute the Bitcoin blockchain. Nevertheless, it is important to note that these miners represent only a fraction of the total Bitcoin holders, which is estimated to exceed 100 million people and this demonstrates the widespread adoption and interest in Bitcoin among individuals across the globe.

Coming back to Satoshi Nakamoto character, he possesses a substantial number of bitcoins, estimated to be around 1 million as of 2013. If Satoshi were to ever transfer this considerable quantity, the community would quickly become aware of it. This is because the addresses linked to Satoshi are closely monitored. Such a movement would undoubtedly have a significant impact on the price of Bitcoin.

Over the years a lot of identities have been attributed to Satoshi Nakamoto: from Dorian Nakamoto, a sixty-four-year-old Japanese who lives in California, Dr. Craig Wright, an Australian computer scientist and others. All these theories have never been confirmed.

The real-world identity of Satoshi Nakamoto holds significance due to the potential implications it could have on the future of Bitcoin. If the true person behind the pseudonym were to be revealed, their influence and decisions could hold considerable weight in shaping the direction of Bitcoin. This raises concerns as it could potentially centralize a system that is fundamentally designed to be decentralized.

Despite that most likely theory about this character is that Satoshi Nakamoto is not an individual but a group of cyberpunks who wish to remain anonymous and maybe for the reasons above the truth is better left hidden.

## Ethereum

*“The intent of Ethereum is to merge together and improve upon the concepts of scripting, altcoins and on-chain meta-protocols, and allow developers to create arbitrary consensus-based applications that have the scalability, standardization, feature-completeness, ease of development and interoperability offered by these different paradigms all at the same time. Ethereum does this by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions. A bare-bones version of Namecoin can be written in two lines of code, and other protocols like currencies and reputation systems can be built in under twenty. Smart contracts, cryptographic "boxes" that contain value and only unlock it if certain conditions are met, can also be built on top of our platform, with vastly more power than that offered by Bitcoin scripting because of the added powers of Turing-completeness, value-awareness, blockchain-awareness and state”<sup>xv</sup>*

This is an extract of the Vitalik Buterin whitepaper of 2014 in which the founder started to introduce his new project. Shortly, we can say that the differently from Nakamoto who issued a new coin, totally decentralized that maintains a value without any backing value, or central issuer, the Buterin’s purpose was to create a new way of considering the cryptocurrency with the introduction of the “Smart Contract” and “DApps” two great innovation which would be taken from the new cryptocurrencies introduced in the following years.

### What is Ethereum?

In the previous chapter we saw how the Bitcoin’s purpose was to replace national currencies after the vulnerabilities shown by the financial system during the 2008 crisis. On the other hand, Ethereum started to be developed in 2013 during an “economic boom”, time in which resources are higher and credit rationing for innovative ideas is reduced. For this reason, Buterin decided to create Ethereum, a decentralized global software platform powered by blockchain technology, which has revolutionized the blockchain model through the possibility to execute data and logic with the “Smart Contracts”, small bits of general-purpose logic that

are stored on Ethereum's Blockchain and once invoked (by sending ether) update the nodes' ledger with the result.

As Bitcoin, invulnerability and data integrity is guaranteed by the Ethereum's Blockchain.

Despite some features which are in common between Bitcoin and Ethereum like the digital assets skeleton on which they both are founded or the public and permissioned Blockchain there are a lot of differences between these two protocols.

## Accounts

In the Blockchain the account type depends on the action you can take. In Bitcoin the list included different kind of users but each one with the saving money feature instead in Ethereum with the smart contract introduction exists another account type:

1. *Accounts that only store ETH*: very similar to the Bitcoin's addresses and are sometimes known as Externally Owned Accounts (EOA), you make payments by signing transactions with the appropriate private key.
2. *Accounts that contain "Smart Contracts"* have a special code which a simple EAO cannot have. They do not have a private key. Instead, it is owned (and controlled) by the logic of its smart contract code: the software program recorded on the Ethereum blockchain at the contract account's creation and executed by the EVM. Briefly when a transaction destination is a contract address, it causes that contract to *run* in the EVM, using the transaction data, as its input. Transactions can also contain *data* indicating which specific function in the contract to run and what parameters to pass to that function.

## Gas

In Bitcoin you can add a small amount of BTC as a transaction fee, to have your transaction processed first, that goes to the miner who successfully mines the block. Likewise, in Ethereum you can add a small amount of ETH as a mining fee which goes to the one who successfully runs the process. Ethereum has a concept of gas which is a sort of price list, based on the



computational complexity of different types of operation you are instructing the miners, to make your transaction.

For example, a simple transfer of ETH from one account to another uses an average of 21,000 gas instead uploading and running a smart contract uses more, also depending on their complexity.

When an Ethereum transaction is submitted: the gas price (the amount of ETH you are prepared to pay per unit of gas, higher in busier period) and the gas limit (a ceiling for how much gas you are prepared for a transaction to consume) must be specified.

$$\text{Mining fee(eth)} = \text{gas price(eth/gas)} \times \text{gas consumed(gas)}$$

If the gas limit is exceeded by the gas consumed during computation :

- The state of the contract prior to execution is restored;
- All ETH used to pay for the gas is taken as a mining fee and it is *not* refunded.

### **Ethereum blocks and mining time**

Currently, Bitcoin's blocks are a little under 1MB in size whereas the Ethereum ones are measured by complexity of data contained. Right now, an Ethereum block has a target size of 15 million gas and a maximum limit of 30 million gas, thus for example it can contain more or less  $15 \text{ million} / 21,000 = 730$  transactions in a block. In Bitcoin, you currently get around 1,500 – 2,000 basic transactions in a 1MB block.

The mining time is also different maybe due to the sizes, in Ethereum the time between blocks is around 14 seconds compared with Bitcoin's 10 minutes. So, in 1 hour are generated 250 blocks in Ethereum and 6 in Bitcoin, with a daily average of 1 million transactions handled.

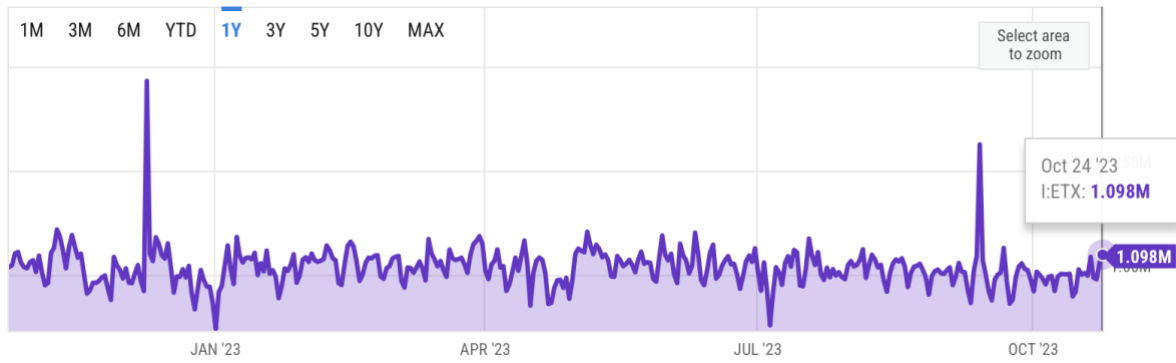


Figure 17. Ethereum transaction handled per day

As the rate increases the “block clashes” frequency (called “uncle” blocks) arise too, but differently from Nakamoto’s protocol the miners get rewarded, because the block can be recalled by a later one. In this situation the originally miner gets the “uncle reward” and the one who recall this block receives the “uncle referencing reward” which is a smaller amount compared with the previous one. This innovation achieves two important things:

1. it incentives miners to mine even though there is an high chance of creating a non-mainchain block;
2. it increases the security of the blockchain by acknowledging the energy spent creating the uncle blocks.

## ETH issuance

The number of ETH in existence are:

$$\text{Pre-mine} + \text{Block rewards} + \text{Uncle reward}$$

The pre-mine was created during the crown sale in 2014 and are equal 72 million ETH distributed to initial supporters and to the project team itself. It was decided that every year the cap for the ether’s generation is 25% of the pre-mine total, so no more than 18 million per year. Block reward is equal to 3 ether after the Byzantium upgrade in October 2017 and in the end the uncle rewards as discussed before is the amount due to the miners of clashed blocks (more or less 7/8 of the full reward) and the amount gained by the miners which recall these blocks which are valid but not in the mainchain due to the high rate of generation.

The biggest difference between Ethereum and Bitcoin generation is that BTC halves approximately every four years and has a planned finite cap, whereas ETH generation continues to be generated at a constant number every year indefinitely.

## **Governance**

As Nick Tomaino argues in a blog post that the governance: *‘may prove to be as important as the science and economics of blockchains’*.

A sharp contrast between Bitcoin and Ethereum is in the Governance policy which leads many people to prefer the former. The first protocol does not have an active, identified leader, whereas the second with its creator make the chain vulnerable because all the powers are in the hand of one person. Doubts are justified from actions taken in the past, he supported a *hard fork* to recover the lost funds in a hack attack but this will be discussed in the next pages.

## **PoW vs PoS**

From the 6<sup>th</sup> of September 2022 Ethereum started to change the consensus protocol from the Proof of Work in which, as I mentioned in the previous chapter with Bitcoin, every ten minutes starts a competition to be the first node to verify a new transaction to receives a reward in coin, to Proof of Stake. This new rule requires traders to “stake” some of their digital assets as collateral, which is then locked up in a deposit. If a trader adds a transaction to the blockchain that other validators deem to be invalid, they can lose a portion of what they staked. There is usually a lower limit to how much validators can stake. After the limit is surpassed, validators can stake as much as they want and the more a trader stakes, the more likely they are to be chosen by the algorithm to try to validate the transaction and so get the reward.

## **Smart Contracts**

Let’s introduce the main Ethereum feature: the Smart Contracts. They are short computer programs, and so are executed in a determinist way, stored on Ethereum to guarantee the security of the code. The steps involved in the in the creation of the smart contract are:

1. *Uploading* the smart contract to Ethereum's Blockchain, by sending the code to miners in a special transaction, and then if it is successfully processed an address is assigned to the contract. It is calculated using a combination of the creator's address and how many transactions that creator has ever sent.
2. To *run* the smart contract is necessary to create a transaction pointing to the contract's address and supply whatever information the expected by the code and the gas required for the execution.

The objective of this innovation is to remove the human factor from decision-making because everything is needed for the compile is written in the code, nothing has to be interpreted and for this reason in many fields they are replacing the traditional contract. The benefits of using this kind of contract compared with the traditional one are:

1. No trusting intermediaries;
2. Rely on reputational insurance;
3. Speed in the execution;
4. Cheap, you have to write only once and so the payment is done only one time;
5. Reusability, in the real world you have to sign different contract instead with the smart contract is it possible to point the transaction to the same address differently;
6. Fraudless, token can be verified on the Blockchain and the digital signature is eligible for spending their contracts.

The innovative technology is being started to use in several fields from the payment or insurance field to the most innovative which is the Decentralized Finance (DeFi) which is a movement that aims at making a new financial system that is open to everyone and does not require trusting intermediaries like banks to achieve that design relies heavily on cryptography blockchain and smart contracts.

DeFi platforms allow people to lend or borrow funds from others, speculate on price movements on various assets using derivatives, trade cryptocurrency, insure against risks, and earn interest in a savings account. DeFi applications are subject to high risk, so high interest rates and currently this economy is valued around 195 mln€.

## DApps

Decentralized Applications are applications built on open-source and decentralized network of Ethereum blockchain technology which uses smart contracts and front-end users' interfaces to create platforms.

We have already studied smart contracts and we know that once deployed on the network you cannot modify and alter (unless you use the command *SUICIDE* which deletes the code and its address). So DApps are decentralized because they are controlled by the logic written into the contract and not by individuals.

The main features are:

1. *Decentralization*: as said before they cannot be managed by a centralized authority;
2. *Turing complete*: because it can be used to calculate each kind of resolvable problem, with the only constraint given by the amount of gas which is equal to the transaction's need;
3. *Deterministic*: DApps performs the same function everywhere;
4. *Isolated*: DApps are executed in the EVM, so that if there is any bug in the smart contract, it will not hamper the networks normal functioning

Ethereum was chosen to develop DApps thanks to its community of developers which has been continuously growing since the launch of the project in 2014 and then for its ability to monetize through for example crowdsale or the simple issuance of NFTs which have become very popular in the recent years.

Pros:

1. *Privacy*, anonymity guaranteed;
2. *Complete data integrity*, data stored on the Ethereum blockchain is cryptographically immutable;
3. *Verifiable behavior* because there is not a central authority;

4. *Zero downtime*, because once the application is deployed, the network is always able to serve its clients;
5. *Never go offline* as all the blockchain technologies.

Cons:

1. *Maintaining* because one published cannot be modified;
2. *Node work*: performance overhead of the nodes because of the large amount of data to manage.

	<b>DAPP</b>	<b>WEBAPP</b>
<b>FRONTEND</b>	HTML, CSS and Javascript	HTML, CSS and Javascript
<b>BACKEND</b>	Smart Contract	Django, Node or Rail
<b>DATA</b>	Block	Company server

### **Ethereum Virtual Machine**

The Ethereum Virtual Machine, or shortly EVM, is the core around the Ethereum protocol runs. It handles the execution of the Smart Contracts (simple transactions between EAO do not need the EVM involvement). Although it has the characteristics of a physical "machine", the EVM is not a real device. This "virtual" machine is in fact kept alive by the thousands of nodes that simultaneously run the Ethereum blockchain. Anyone managing a node on Ethereum immediately participates in the EVM.

It is a quasi-Turing-Complete machine, *quasi* because as seen all execution processes are limited to a finite number of computational steps by the amount of gas available for any given smart contract execution.

The Ethereum Virtual Machine is responsible for the storage, processing and transmission of smart contracts based on Ethereum, analyzes newly generated transaction data and updates its documentation accordingly whenever smart contracts on the Ethereum blockchain are changed.

## **Oracles**

Oracles represent mechanisms enabling Ethereum smart contracts to access external data sources. The term "oracle" comes from Greek mythology, denoting an individual connected to divine beings, capable of foreseeing the future.

Oracle can be thought of as a mechanism for bridging the gap between the off-chain world and smart contracts, allowing the latter to enforce contractual relationships based on real-world events and data broadens their scope dramatically.

In the context of a decentralized public blockchain like Ethereum, which involves numerous nodes processing transactions, maintaining determinism is of utmost importance. In the absence of a central authoritative figure dictating the truth, it is imperative that nodes reach a uniform state subsequent to applying identical transactions. Any situation where node A executes the code of a smart contract and obtains a result of "3", while node B acquires "7" after executing the same transaction, would jeopardize consensus and erode the decentralized nature of Ethereum's value as a computational platform. The previously said scenario also underscores the issue associated with integrating external information into blockchain design.

However, oracles present a solution to this problem by extracting data from off-chain sources and recording it on the Blockchain for consumption by smart contracts. As data stored on Ethereum is immutable and publicly accessible, its nodes can securely utilize the off-chain data imported by the oracle to compute alterations in state without compromising consensus.

To accomplish this, an oracle generally consists of an on-chain smart contract alongside off-chain components. The on-chain contract receives data requests from other smart contracts, which it then forwards to the off-chain component (referred to as an oracle node). This oracle node can interact with data sources - using methods such as application programming interfaces (APIs) - and initiate transactions to store the requested data within the storage of the corresponding smart contract.

## **AAVE**

AAVE is the most developed decentralized crypto lending platform which uses smart contracts to automate the process and it is a good example of DeFi platform which grows from \$0 to \$3B in less than a year.

Aave specializes in overcollateralized loans, meaning that users will need to deposit crypto worth more than the amount that they wish to borrow, 80% of the current value of the pledged collateral, to protect lenders from loan default or collateral drops too much in value.

The most famous AAVE's feature is the *Flash Loan*, created to take advantage from arbitrage opportunities within the crypto market, which must be paid back within the same block on the blockchain with an interest rate equal to 0.09%.

AAVE also provides an annual percentage yield (APY) for who deposits assets on the platform, that is paid out in the same asset in which is deposited.

This is a good example of an innovative app created on Ethereum that since the launch captured some attentions from the curious and smart community of the crypto.

As AAVE, I am sure also other kind of ingenious and inventive application takes place on the blockchain world because smart contracts are features not still exploited at 100% in the financial field.

## **DAO hack**

Dao was launched in 2016, the aim was to be a decentralised autonomous organisation acting as a direct venture capital company. It gave the opportunity, by owning DAO tokens, to profit from the organisation's investments. In the first year, a sum of \$150 million was raised in ETH.

During the sale of the tokens, many computer scientists expressed concern about a vulnerability in the code that could have caused them to lose the entire sum raised. During the correction actions, however, a user exploited this issue and appropriated part of the funds, which at the time were 14% of all ETH in circulation.



In this moment of great stress for the entire community, Vitalik took matters into his own hands, proposing a soft fork, whereby the code was updated to prevent future attacks and the hacker was blacklisted, effectively blocking all activity within the blockchain.

Despite some debate the soft fork was implemented, however, during the implementation another code-related issue was discovered that prompted the founder to change tactics and impose a hard fork, bringing Ethereum's history back to before the attack, precisely to block 192,000, thus returning the funds to the users of the DAO organisation.

These moves have created many problems and have highlighted the great difference between the governance of Ethereum and Bitcoin, with the figure of Vitalik being very cumbersome and always ready to intervene to resolve any problems, which in certain cases effectively cancel out the power of the community, a fundamental feature of every Blockchain.

After this return to the past, Ethereum was divided between those who went against the founder and those who supported the choice, giving rise to two different coins Ethereum Classic and Ethereum.



Figure 18. Ethereum classic price.

	<b>Bitcoin</b>	<b>Ethereum</b>
<b>Definition</b>	Decentralized Digital Currency	Decentralized software platform and digital currency
<b>Creation</b>	2008	2013
<b>Purpose</b>	Replace national currency	Maintainig a decentralized payment network and storing computer code
<b>Smart Contracts</b>	×	✓
<b>Hash Algoritm</b>	SHA-256	Keccak-256
<b>Consensus Mechanism</b>	PoW	PoS
<b>Block time</b>	10 minutes	14 to 15 seconds
<b>Block limit</b>	1 MB	Gas quantity
<b>Energy consumption</b>	Very High	Low
<b>Structure</b>	Simple	Complex and feature rich
<b>Rewards</b>	Depends on the halving	3 ETH
<b>Popularity</b>	1st most popular	2nd most popular
<b>Average transaction handled per day</b>	400 thousands	1 million

## International Payments

The digital payments sector has been evolving rapidly for several years now, as we have seen in this chapter and alongside the most widespread and used international digital payment management model today, called SWIFT, an innovative peer-to-peer approach based on blockchain technology is gaining more and more traction, trying to shake a decade-old monopoly.

The SWIFT code is not a money transfer system but rather an international communication protocol between credit institutions which serves banks all over the world to have a unique system recognized everywhere despite being created with characteristics of neutrality, also for its vast use (it is the most used system in the world) is increasingly used as an instrument of geopolitical and financial pressure, as in the recent Russia case in 2022.

Despite all this technicism I think to better understand the complex international movement of money, it is important to know the *Bank Pyramid Hierarchy* which involves the main actors.

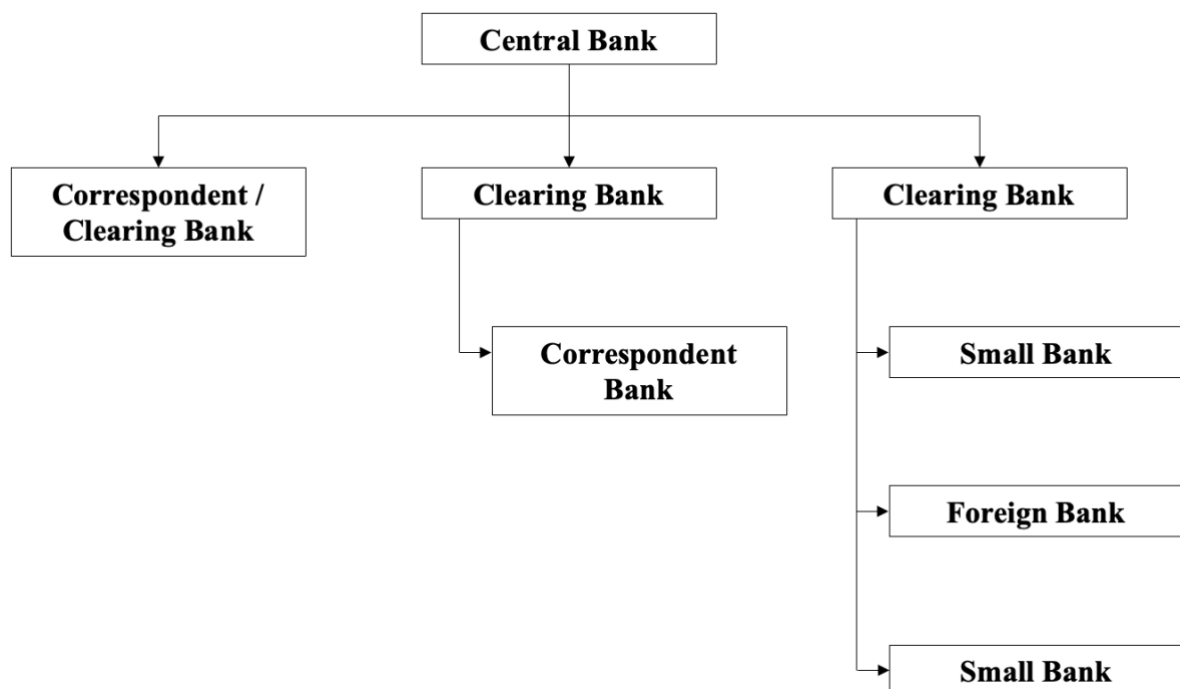


Figure 19. Bank pyramid hierarchy.

At the top we can see *Central Banks (CB)* which enables banks, in its jurisdictions, to pay each other electronically, it acts as a *bank for the banks in its currency zone*.

One layer below there are *Clearing (intermediary) Banks* called in this way because they can clear payments (netting of the transaction) by the direct contact with CB. The *Correspondent Bank* are a subcategory of Clearing one, they are used by the domestic to execute and complete international payments without having to open branches abroad. In the end, we find *Small Banks* which do not have an account on the Central Bank and need to pass through a Clearing one to conclude the payment.

After this we can start with the explanation, in a practical way, of how international payment works nowadays and for that SWIFT (Society for Worldwide Interbank Financial Telecommunication) a global financing messaging network is the example because more than 45 million transactions are carried out every single day making the most common way to send the money abroad.

Let's understand how it works with an example.

Alice, an Australian girl, wants to send 1,000\$ to Matteo, an Italian boy. Thus, with the SWIFT Alice tells to her local Australia bank to send the money to Matteo Italy bank, the system guarantees that each passage is done correctly and after 3-5 days Matteo can check on his home banking account the quantity received. But behind the scenes happens that there are many intermediaries involved during the transmission:

1. Local Australia bank;
2. Clearing and correspondent intermediary bank, established in USA. It needs to be established in USA because only banks with the US banking license can hold US Dollars in their account and since the SWIFT works with US Dollars need to be like that;
3. Matteo's bank;
4. FED which net off the payments.

Here below the entire process explained with SWIFT, which is responsible for the communication between the characters:

**BEFORE**

<b>FED</b>			
<b>Asset</b>		<b>Liabilities</b>	
		Matteo's US Bank	100,000\$
		Alice's US Bank	100,000\$

<b>Matteo's US Bank</b>			
<b>Asset</b>		<b>Liabilities</b>	
Reserves	100,000\$	Italy Bank	15,000\$

<b>Alice's US Bank</b>			
<b>Asset</b>		<b>Liabilities</b>	
Reserves	100,000\$	Australia Bank	20,000\$


<b>Matteo Italy Bank</b>			
<b>Asset</b>		<b>Liabilities</b>	
US Bank Account	15,000\$	Matteo Account	5,000\$


<b>Alice Australia Bank</b>			
<b>Asset</b>		<b>Liabilities</b>	
US Bank Account	20,000\$	Alice Account	10,000\$


Matteo's Bank has an open account with a correspondent US Bank, which also plays a role of clearer (the same for the Alice's one).


The FED, in which all the clearing banks have opened an account, once the transaction takes place, will move the money from one account to another, keeping the total liabilities amount the same as before.


**AFTER**

<b>FED</b> 			
Asset		Liabilities	
		Matteo's US Bank	101,000\$
		Alice's US Bank	99,000\$

<b>Matteo's US Bank</b> 			
Asset		Liabilities	
Reserves	101,000\$	Italy Bank	16,000\$

<b>Alice's US Bank</b> 			
Asset		Liabilities	
Reserves	99,000\$	Australia Bank	19,000\$

<b>Matteo Italy Bank</b> 			
Asset		Liabilities	
US Bank Account	16,000\$	Matteo Account	6,000\$

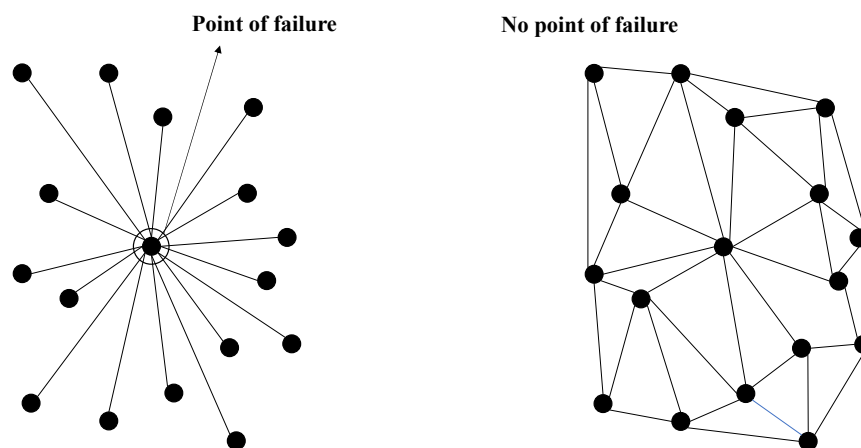
<b>Alice Australia Bank</b> 			
Asset		Liabilities	
US Bank Account	19,000\$	Alice Account	9,000\$

Matteo, 3-5 days after the transaction, receives the money on his balance, thanks to the SWIFT and the many intermediaries involved in this mechanism.

### **SWIFT and Cryptocurrencies issues**

The recent cases of cyber incidents involving banks connected to the SWIFT network have reignited the debate around the security and cyber resilience of the system as the risks associated with it are multiple:

1. It is *not designed for real time transaction*, because 3-5 days are needed and the involvement of intermediaries makes the process longer;
2. *Not all banks have this connection*, most of the time due to political reasons and the exit from SWIFT, in a highly globalized and interconnected world like the current one, entails various critical issues;
3. The system gets much more complicated when *time zones* go into play, critical for a system of international payment which make the transactions longer;
4. A lot of error occurs in many different places, and according to the London School of Economics and Political Science the percentage is around six per cent<sup>xvi</sup>;
5. It is expensive due to the high number of intermediaries involved which is never under 4 or 5;
6. The last but not least, SWIFT is a centralized system, by one single organization and as we have understood from the blockchain, a single point of failure can lead to potential systemic risk.



All these points have in common a possible resolution in the blockchain, on which transactions are theoretically transparent. Since there is no central entity in a superordinate position compared to the others, they do not have a single point of failure and cannot be altered by attacking a single node of the network. Alteration of data and operations would require control

of at least 51% of the nodes of a certain blockchain and would require coordinated and simultaneous manipulation.

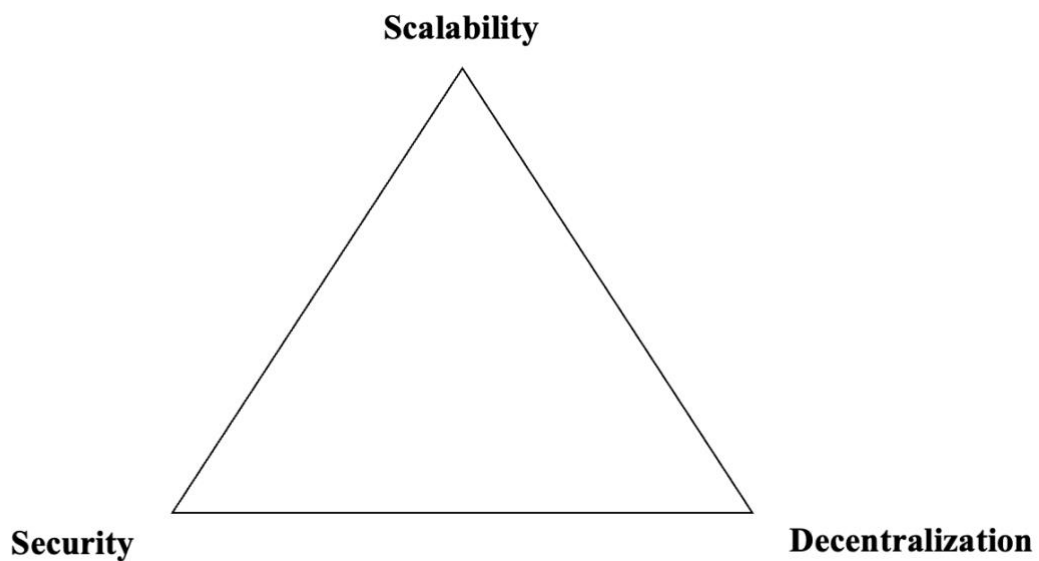
When an institution or company controls a database, it is theoretically easier for malicious actors to access the data contained therein and modify it compared to when the database is managed in a widespread manner. Each block of the blockchain is also connected to all the blocks preceding and following it. This makes it difficult to tamper with a single record because a hacker would have to modify not only the block containing that record but also all those linked to it to avoid detection of the manipulation. Records on a blockchain are ultimately protected via cryptography: network participants have their own private keys that are uniquely assigned to transactions made and act as a personal digital signature. If a record is modified, the signature becomes invalid, and the peer network is immediately put in a position to identify the anomaly.

Despite the advantages deriving from the widespread management of the digital register on multiple nodes, the blockchain is subject to some vulnerability profiles typical of decentralized models. Below we present the most common approaches used by attackers to manipulate systems distributed across multiple nodes<sup>xvii</sup>:

1. *51% Attack*, this is a situation in which a single entity manages to find itself able to control the majority of the nodes in the network, but the probability of its occurrence is inversely proportional to the costs that the implementation of such a scheme entails for the attacker, which are extremely high;
2. *Sybil Attack*, really close to the previous one, in which a person tries to take control of the network by creating different accounts, nodes or computers. In the world of distributed ledgers, this translates into the management of multiple network nodes by a single user. In this way, attackers can manage to outnumber honest nodes in a network, by creating sufficient fake identities;
3. *Replay Attack*, in which the executor intercepts and then repeats a valid data transmission within a network. They can be used to trick financial institutions into duplicating transactions, allowing the perpetrator to withdraw money directly from victims' accounts;



4. *Human error*, which is translated into faults, defects, and operating anomalies. Therefore, bugs can exist in blockchain code resulting from human error, and such bugs can be exploited by malicious actors for their own benefit, as happened in the DAO Hack;
5. “*Cryptocurrency Trilemma*”, as seen the number of transactions handled by the SWIFT protocol is extremely high and not guaranteed by the blockchain technology. Instead the trilemma talks about the impossibility of satisfying the three principles of blockchains: *Decentralization, Throughput Scalability and Security at the same time but only two.*



The world of blockchain is constantly developing and with the passage of time it is becoming more and more perfect but, despite this, it is not without weaknesses and in some cases even debilitating ones as seen in the DAO Hack or the trilemma which until now has been unresolvable, with only one layer architecture.

This chapter was a general study of how the two main cryptocurrencies work, with some practical applications that are already present or that perhaps will be implemented but which nevertheless make us understand their power.

Are these blockchains bubbles? I don't think so, but nothing is certain. As seen, they have many applications in different fields, not only the financial one, and its technology would make it possible to reduce the physical time of transactions, from banking transactions that require the bank as an intermediary, to those perhaps concerning the purchase of physical goods with some doubts concerning the possible solution to the trilemma. Through smart contracts we have then

seen that in the future, if technology advances further, we will be able to avoid going through very expensive intermediaries, such as notaries in real estate purchases, and rely only on the secure lines of code.

Numbers are on our side and only time will tell if this tool will be adopted, but we can say that the premises are good enough.

## Central Bank Digital Currency (CBDC)

The Central Bank Digital Currency introduction is one of the most recent advances in this field and across the world financial institutions and governments are interested in this innovation.

For these reasons, I decided to investigate examining their development, traits and prospective in the financial system in particular the consequences for commercial banks.

During the last years many countries started to develop its own digital currency:

1. since 2014 the People's Bank of China (PBOC) has been developing a digital Yuan and testing it out in a number of cities;
2. the Central Bank of Sweden (Sveriges Riksbank) launched an e-krona pilot program in late 2020;
3. the Bank of England (BoE) is studying a digital Pound and it will decide in the coming months whether to move towards or not.

In this chapter will be discussed how CBDC is designed by governments, its advantages and disadvantages and the reason why it is gaining so many attentions from the public institutions around the world.

### Overview

*“CBDC is central bank-issued digital money denominated in the national unit of account, and it represents a liability of the central bank.”<sup>xviii</sup>*

It is a legal tender issued by Central Bank and as the other currency it will represent in a digital form a medium of exchange, a store of value and a unit of account (the three function of money). It is a digital version of the fiat currency with also the same value.

Aspect	CBDCs	Cash	Digital Assets
<b>Issuing Authority</b>	Issued and backed by a central and Monetary Authority	Issued and backed by a central and Monetary Authority	Managed by algorithms
<b>Form</b>	Digital	Physical	Digital
<b>Guarantee</b>	Central Bank Liability	Central Bank Liability	Privately issued
<b>Payment acceptance</b>	Legal Tender	Legal Tender	Limited Acceptance
<b>Anonimity</b>	Depends on the structure	Yes	Yes
<b>Structure</b>	Centralized	Centralized	Decentralized

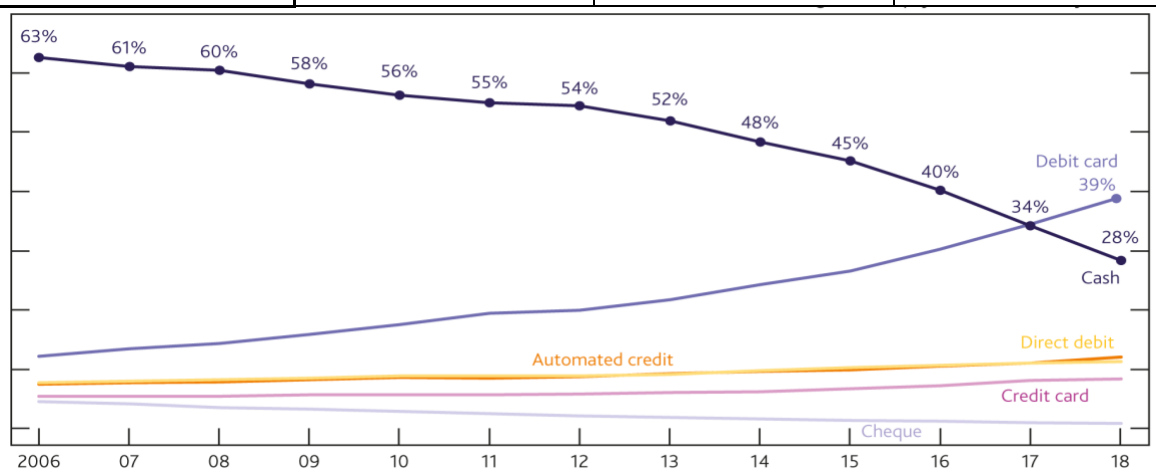


Figure 20. Payments in UK.

CBDC are interesting because payment method is changed during the years and from 2017 cash started to be less used rather than privately money which continues to increase its use and innovativeness.

## **Key drivers**

Faster payments, mitigation for clearing and settlement risk and a rapid digitalization could be reasons that induced Central Bank pushing in the CBDC's development but according to Deloitte there 4 key drivers which have a greater weight in its evaluation and development:<sup>xix</sup>:

1. Need to bring Central Bank back to the center of currency creation and trust.

New form of currency has been developed and Central Banks are increasingly aware that they may individually need to play a central role in the system rather than remain an observer. Thus, a new digital currency, that carry the benefits of the new moneys, is needed to maintain the politic position held by CBs during the years;

2. CBDCs have immense potential to bring efficiencies in the financial system.

The adoption of this innovation can enable real-time and cost-effective globalization of payments system, which is a real issue nowadays as seen in the previous chapter, and the time zone differences are not more a problem. Also, the ESG cost (predominantly borne by banks and households) of printing money would become zero and improve the efficiency of money in the clearing, settlement, and post markets activities.

3. Improve financial access and financial inclusion.

A ADB (Asian Development Bank) recent study suggests that CBDCs may offer a highly efficacious solution to the problem of financial inclusion by granting underbanked community access to digital currency.

4. Enhancing monetary and fiscal policy.

The Central Bank issues and manages CBDCs, using it as a tool for monetary policy, modifying the amount of money available to the economy directly from its ledger.

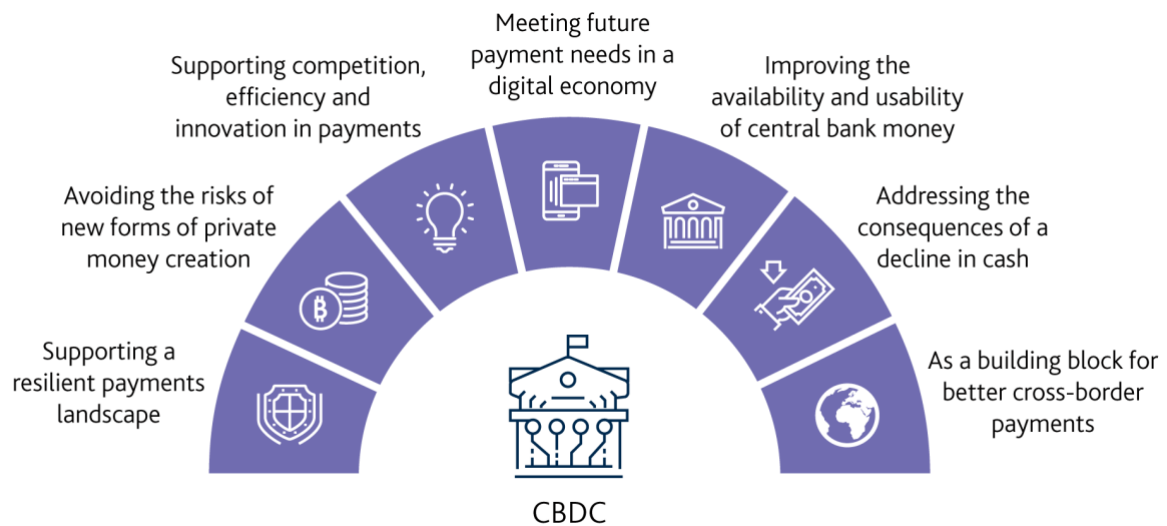


Figure 21. Opportunities for CBDCs to support Monetary and Financial Policies<sup>xx</sup>.

### Regulator’s consideration

There are a set of decisions that need to be evaluated, during the design and implementation of CBDCs, about privacy, distribution model, technology, and access. On the other hand exists also more technical considerations about the infrastructure, database or ledger on which transactions are recorder or the device through which initiate payments.

### Technologies and access points

CBDCs design is an extreme challenge, it is an innovative feature that enter in a world too bound and stuck with the past. Distributed Ledger Technology (DLT) is often associated with this currency, as the other new innovative form of currency, but finance has always worked with centralized ledgers as common storage where the control is in the hands of a trusted administrator authorized to make changes to the database. Thus, transaction will be cleared by Central Banks but token or account-based approach has to be decided<sup>xix</sup>:

- *Token based* approach: in which transactions involve wallets the transfer is executed changing the balance of this two by CB. This method increases the financial inclusion and the privacy because no person is linked and appear in the ledger but at the same time adds more difficulty in tracing money laundering and fraudulent transactions.

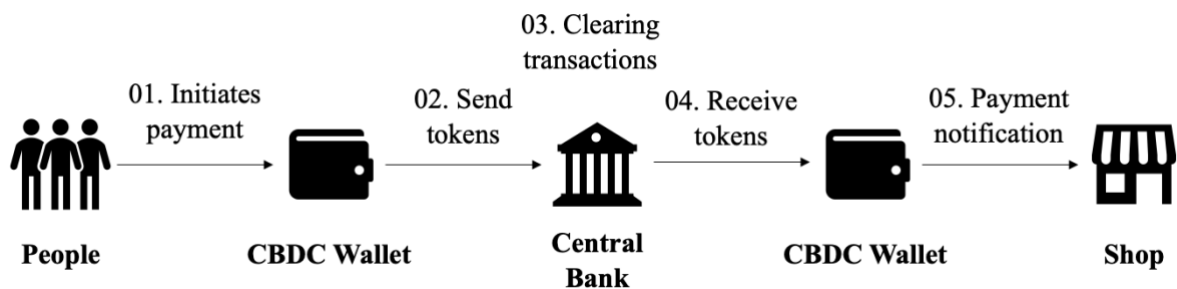


Figure 22. Token-based CBDCs transactions

- *Account based* approach: in which the distribution and transaction involve transfer from one account to another. It means that identity verification is needed linked with a digital account and thus low level of privacy.

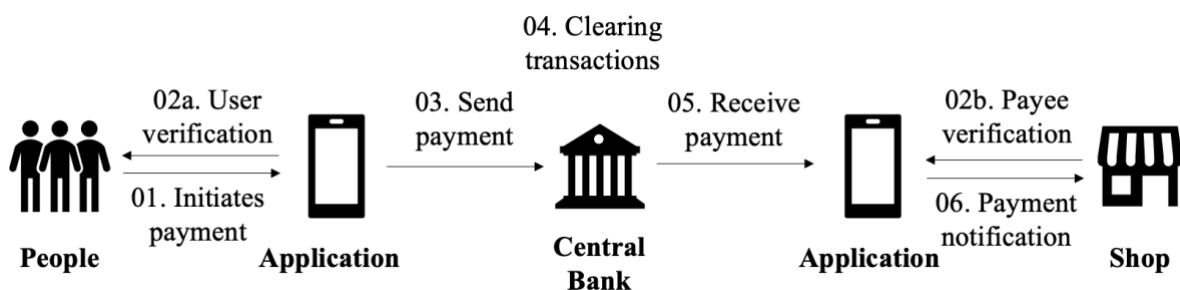


Figure 23. Account-based CBDCs transactions

Regulators for cross-borders payments prefers the first one due to the high degree of anonymity and high financial inclusion because is required only an internet connection. On the other hand, the account-based approach allows regulators to monitor transactions and a high degree of involvements in the process.

### Retail vs Wholesale CBDCs

The choice in this match is about which actors must be involved in the process, for this exists two possible solutions:

1. *Retail based CBDC*: in this case the actors involved go from the Central Bank until individual, this promotes financial inclusion and a cashless economy (so the reduction of the cost associated with the printing of physical money). This retail model proposed include two different scenarios:

- *Indirect*: in which the issuance and the management of digital currency is done by intermediaries, in this case financial institutions.

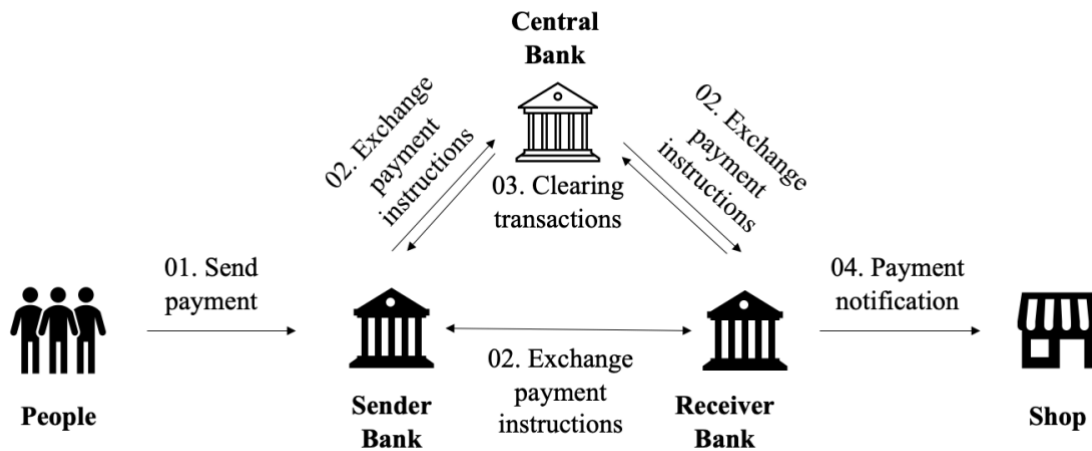


Figure 24. Indirect retail model

- *Direct*: in which the intermediation is avoided, and the currency is distributed by Central Bank. In this case the roles and responsibilities of CB increase dizzy and might affect the structure of the current financial system.

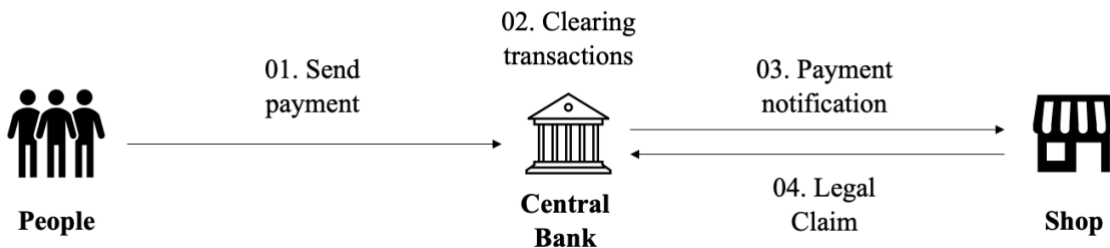


Figure 25. Direct retail model

2. *Wholesale based CBDC*: in this case the currency is used to clear large-value payments between financial institution, for instance in cross-border settlements. It improves security, credit, and settlement risk. Thus, in this case people are not involved.



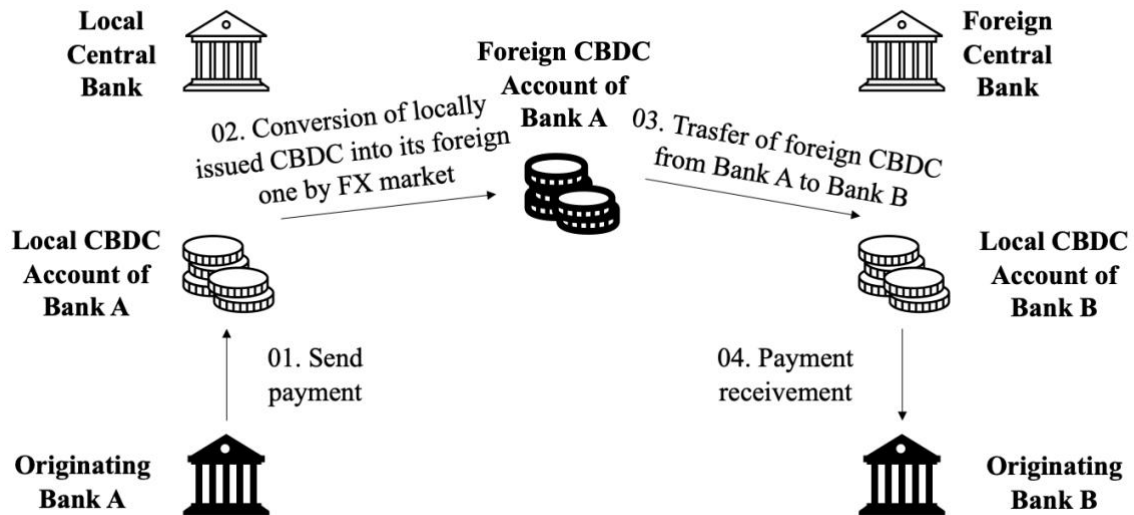


Figure 26. Wholesale model

Which of these schemes is better is not known because to decide is important to evaluate the macroeconomic situation: if the reason to adopt the CBDCs is to increase the financial inclusion maybe the retail approach suits better, instead if the settlement risk is the cause the wholesale can be the answer.

### CBDCs distribution model

The distribution model can be classified in two categories depending on how the currency is circulated within the economy, with always the token and account based provided.

1. *One-tier approach*: this case foresees that the Central Banks is the solely responsible for the issuance of the CBDCs and despite from one side it can have a higher overview of the transactions taken place on the other side it could have serious implications on financial services balances, since their deposits will seriously decrease.

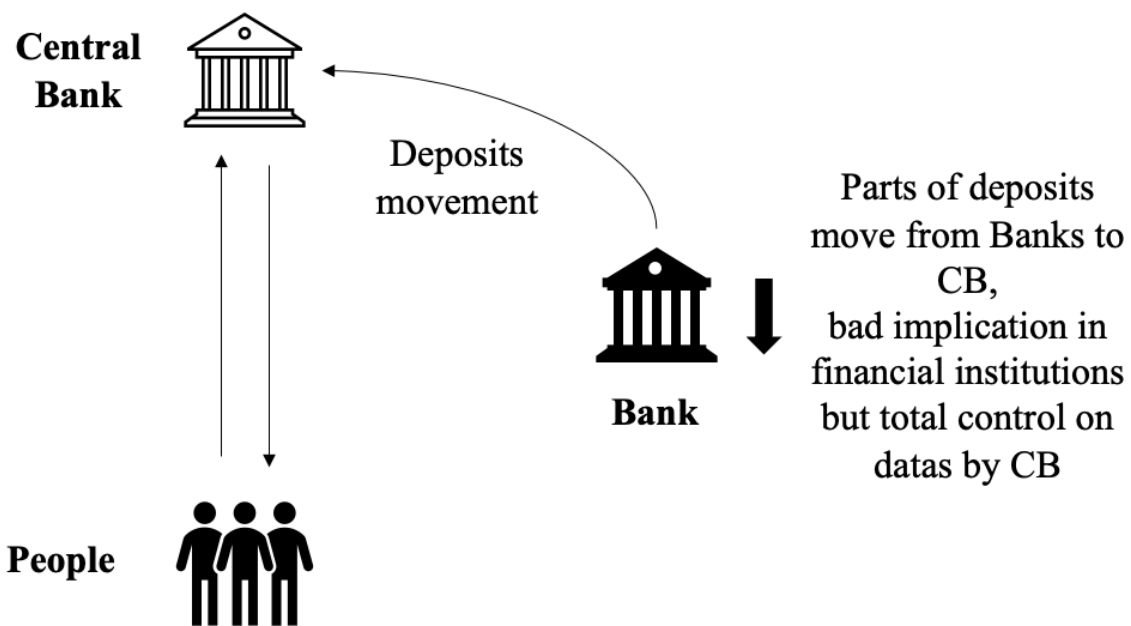


Figure 27. One-tier approach

2. *Two-tier approach*: this is like how the distribution happens nowadays and is done by banks to costumer.

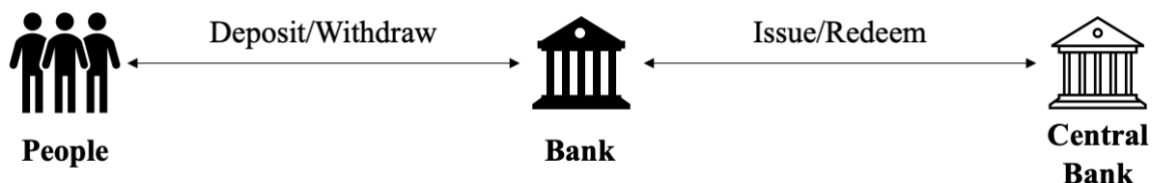


Figure 28. Two-tier approach

The choice between these two approaches is so complex since it has implications on financial markets. The one-tier grants a higher control over dates but at the same time can revolutionize the actual system since costumers may prefer to open accounts directly with Central Banks and thus a large portion of deposits may move away from banks to Central Bank accounts. This scenario can be managed by design specific wallet with different kind of transaction, balance and time limits or differentiating the holder: corporate or the personal.

Central Banks need to ensures that CBDCs issuance goes in parallel with a rulebook in which are analyzed the risk associated with the framework chosen and provide the possible solution to these issues.

## Interest bearing CBDC and non-interest bearing CBDC

CBDC could be proposed to be interest-bearing, and in this case compete directly with deposits instead the version which does not provide gain would be a digital version of cash. This is an important decision because it determines the impact on the banking system's liquidity, the former with an high effect instead the latter a lower one.

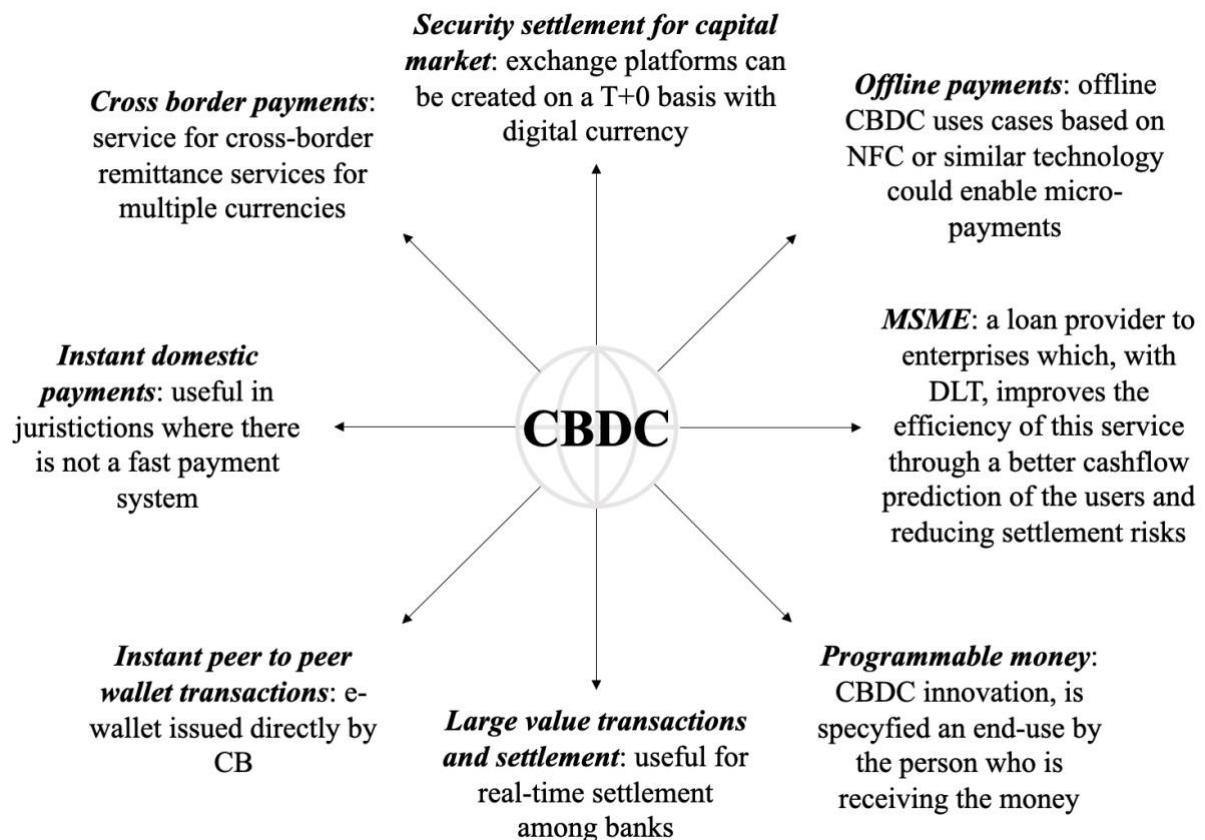


Figure 29. CBDC use cases

## CBDCs around the world

According to the International Monetary Fund (IMF), almost 80% of Central Banks are considering creating their own CBDCs, the reasons are different but principally because they have the potential to boost financial inclusion, create new innovative payment systems which improve the efficiency and open up new monetary policy opportunities.

Different stages go along the born of CBDC:

1. *Research*: in this phase is studied the effects of the project in the other countries, use cases and implications;
2. *Pilot*: the CBDC is evaluated on a small scale in the real-world settings;
3. *Development*: technologies are developed on a small scale and tested;
4. *Inactive*: in which the works are stopped;
5. *Cancelled*: moving forward are rejected and the project is abandoned;
6. *Launched*: CBDC is entered into the market.

In the diagram below some of the ongoing projects around the world:

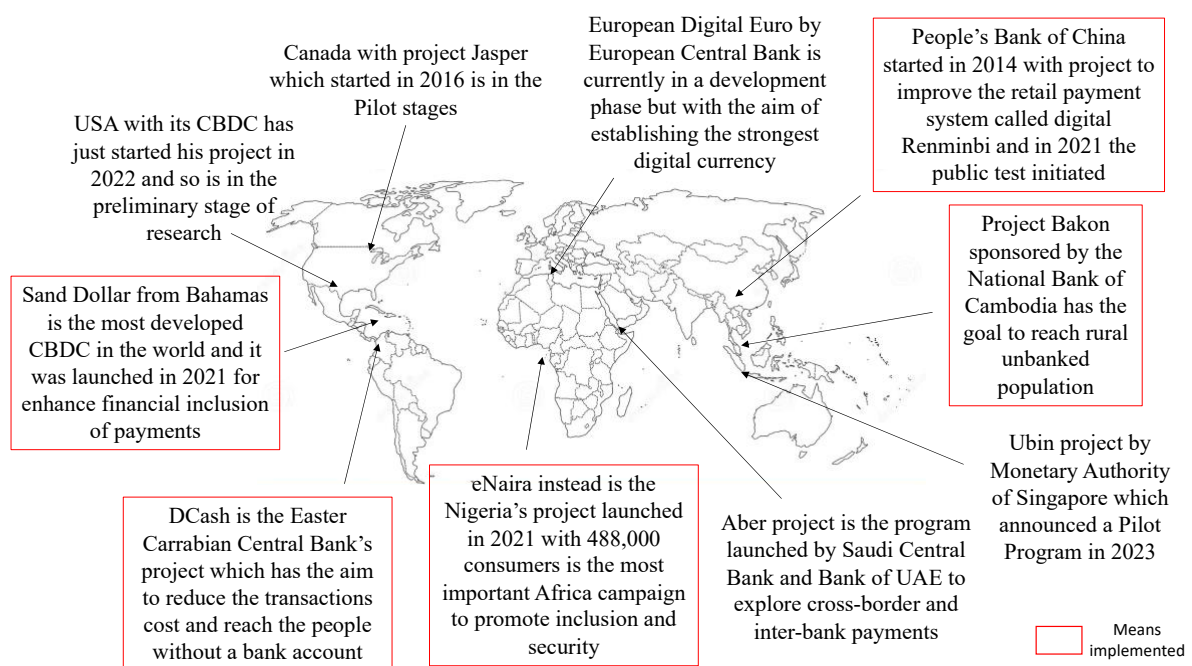


Figure 30. CBDC projects around the world

The ideas about this project are many but, in this moment, only five countries have implemented the CBDCs and are in the last stages.

### **Sand Dollar: the Bahamas Digital Currency**

Since only the 48% of Bahamians have access to credit card facilities from the traditional banking sector, the Central Bank of Bahamas introduced the Sand Dollar, a digital version of the Bahamian dollar. Its main objective, as it is imaginable, is to enhance the financial inclusion and then increase the competitiveness of the domestic payment system. It is a retail version because it studied to individuals and is based on Distributed Ledger Technology (DLT). The approach is a two-tier, so the currency is issued by CB but distributed by financial institutions. The Customer use a wallet to make transfers and so it is token based. Payments are possible offline but exists a maximum limit equal to \$1,500 monthly.

### **DCash: the Eastern Caribbean Digital Currency**

The reason for this project is born from the objective to offer a secure and quick method to make payments, extended the financial service to individuals without a bank account, and thus it is a retail currency. The technology behind the structure is the blockchain, in particular the Corda platform but this time it works as account-based. The currency is issued by the Central Bank and distributed by financial institutions. Offline payments are not allowed, and its use case is for domestic and cross border transactions. In the future its aim is to replace the cash with the CBDC for all the kind payments.

### **eNaira: the CBDC from Nigeria**

Central Bank of Nigeria launched its own digital currency to enhance the security of the payment system, through an innovative traceability protocol, and to promote financial inclusion. It is a retail currency and with specific daily limit. The approach is the two tier one in which local banks are used to overcome the adoption problem of digital wallet. It uses the structure of the token and exists three types of account: individual, business and government.

<b>Aspect</b>	<b>Individuals</b>	<b>Business</b>	<b>Government</b>
<b>eNaira app to open account</b>	Yes	No	No
<b>Financial Institution verification</b>	Yes	Yes	No
<b>Central Bank verification</b>	No	No	Yes
<b>Daily limit</b>	1,000,000	1,000,000	Unlimited
<b>Daily balance</b>	5,000,000	Unlimited	Unlimited

### **China Digital Renminbi or Digital Yuan**

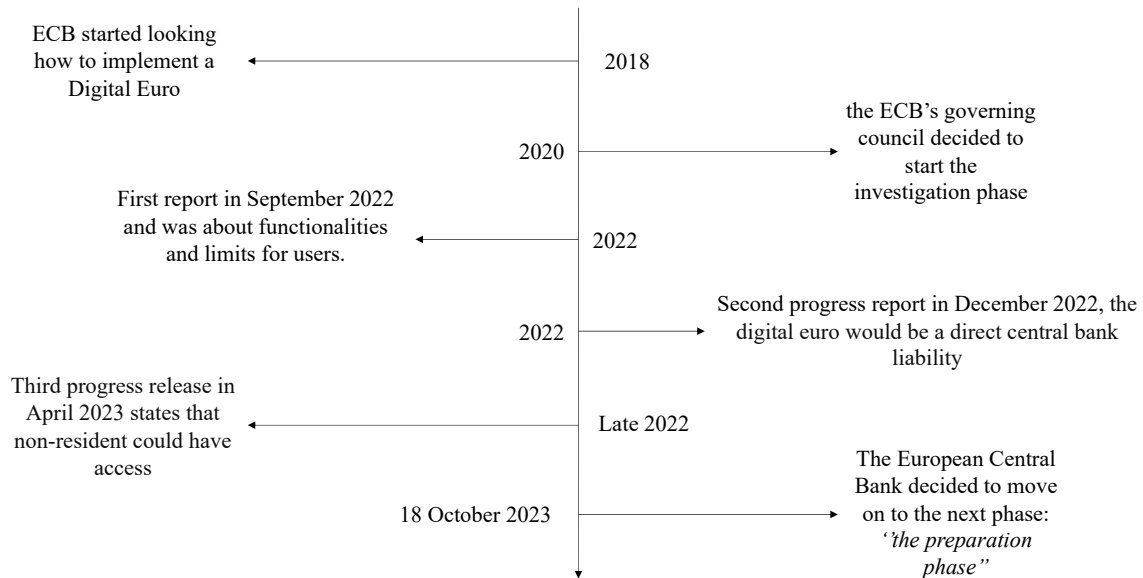
The project initiated in 2014 to improve the efficiency of everyday transactions reducing the linked costs and to replace cash. It is account-based with a two-tier approach; it allows offline payments and there are not transaction limits. However, its structure differs from the previous because it does not utilize the Distributed Ledger Technology (DLT) to record the transactions but a state-owned database and this allows the Central Bank to exert complete control over the currency and transactions. Digital Yuan is expected to handle 300,000 transactions per second.

### **Bakong project: the Cambodia National Currency**

The last currency under our magnifying glass is the Cambodian one which has the aim to reach rural unbanked populations. It uses a DLT and seen the purpose it is a retail coin which uses token technology. In 2023, more than 10,000 users adopt it and has a throughput of 2,000 transactions per second. In the future Central Bank of Cambodia is looking for ATM withdrawals and deposits.

	<b>Bahamas</b>	<b>Eastern Caribbean</b>	<b>Nigeria</b>	<b>China</b>	<b>Cambodia</b>
<b>Distributed Ledger Technology (DLT)</b>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	No	<i>Yes</i>
<b>Token-Based</b>	<i>Yes</i>	No	<i>Yes</i>	No	<i>Yes</i>
<b>Account-Based</b>	No	<i>Yes</i>	No	<i>Yes</i>	No
<b>Offline Usability</b>	<i>Yes</i>	No	No	<i>Yes</i>	No
<b>Transaction Limit</b>	Yes, \$1,500 monthly	No	Yes, depends on the specific wallet	No	Yes, depends on the specific wallet
<b>Distribution Approach</b>	Two-tier	Two-tier	Two-tier	Two-tier	Two-tier
<b>Domestic Payments</b>	Yes	Yes	Yes	Yes	Yes
<b>Cross Border Transactions</b>	No	Yes	No	No	Yes

## Digital Euro



In response to the decline use of cash and to mitigate the risk of the euro being overtaken by other foreign digital currency the European Union (EU) and the European Central Bank (ECB) announced in October 2020 the investigation phase of the project, which in the next years will fulfill a digital form of the Euro.

Digital Euro will improve financial inclusion and the international payments, with faster transactions and a more resilient system, but it has also other politic implications.

The European CBDC will be akin to the cash payment system but at the same time it could be its concurrent and thus, the design is an extremely hard and important subject.

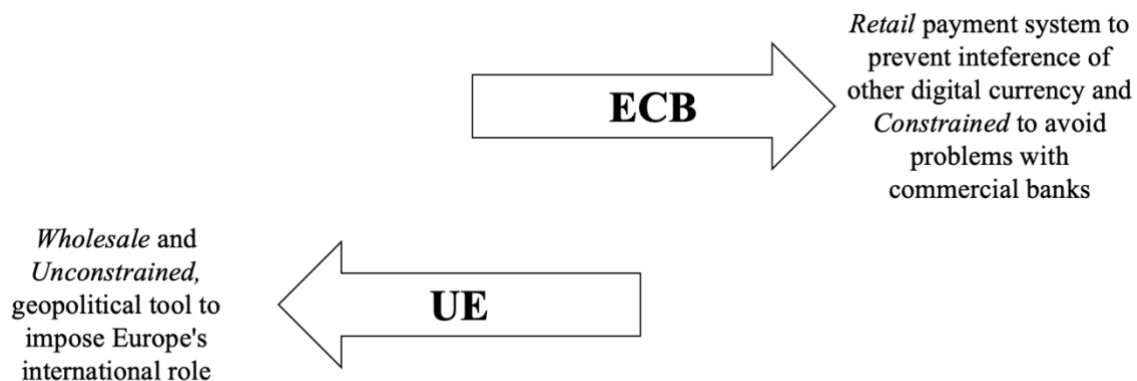
### Different visions between the founders

Digital Euro has received great attention only in recent years and this has led to a study by the European Central Bank and the European Union. However, different stakeholders have different views.

European Central Bank wants a protocol which substitutes the cash payments system which is going in disuse, and which does not create problem with commercial banks. On the other hand,



from a more politic point of view there is the European Union which asks a system to increase the international position of Europe and avoid the possible consequences of the USA penalties. The former purpose could be achieved by creating a parallel system to SWIFT methods, but at the same time it could have seriously repercussion in the banking sector which is what the European Central Bank wants to avoid.



Different views make the design extremely hard and has kept the European Commission busy for many years, so much so that it has not offered answers on the topic until now.

### **European CBDC approaches**

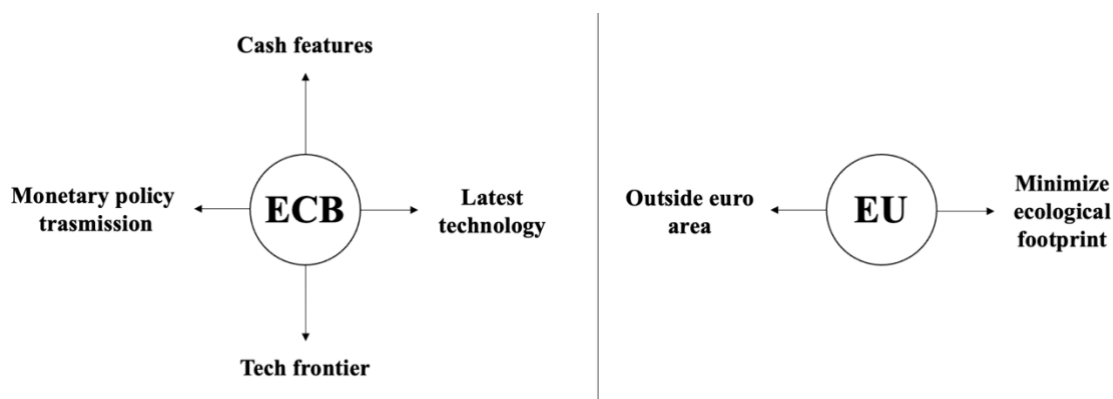
Nothing was announced yet but during this period of silence different and controversial theories were born to satisfy the different views from the two parties involved.

From the BCE's standpoint the requirements to meet in to ensure that the digital euro will be a viable replacement for the fiat currency in the future:

- *Cash features*: the CBDC will have to replicate the features of cash to counter the emergence of private digital currencies and give the EU a new form of money;
- *Tech frontier*: in order to be more attractive than other foreign currencies;
- *Monetary policy transmission*: it needs to be remunerated at the interest rate to enable the Central Bank to directly influence the consumption and investment choices of the non-financial sector;
- *Latest technology*: to be more attractive for the FinTech industry.

Instead on the other hand the European Union (EU) has more political needs compared to the previous which instead are more technical and from a financial perspective. The EU wants to increase the European position around the world, creating a global digital currency which must meet these two requirements:

- *Outside euro area*: it must be accessible from all over the world, used everywhere;
- *Minimize ecological footprint*: it needs to be designed to reduce the overall cost and with a design that should be energy and resource efficient.



## Design

Certain considerations must be taken into account when a new currency is designed, and the divergence of views is also another constrain that must carefully thought.

Before trying to give a shape to the design of this new currency it is important to understand which topics are discussed and the reasons why.

This new currency must be available all the time, everywhere and at the same time give the privacy and anonymity features of cash.

The technology behind could be both centralized and decentralized but the former is the one with the highest probability of success. Most of the effective finance systems have an hub which controls and complete transactions, managing a very high number of that and remembering the “*Cryptocurrency Trilemma*”, the most effective method is the centralized despite some privacy issues.

The transmission mechanism is not an important matter, since both account and token-based systems are efficient enough to handle transactions, with the second better from the point of view of privacy, which however is not guaranteed in any case by centralized technology.

Offline usability is an important stuff, since this technology wants to replace the cash, it has to allow payments where internet connection is vacant and so a platform with a system of automatic update when connectivity returns available is needed.

The remuneration instead is an issue extremely difficult to address a solution. A zero interest rate protocol does not offer the opportunity to the ECB to influence the consumption and investment choices, instead a remuneration protocol gives consumers an alternative to bank deposits, with the possibility of fast movement of deposits from commercial bank to central bank accounts which creates banking crises.

Once we have given a general vision of the boundaries of this digital euro, we now try to establish a design.

### **ECB constrained scenario**

In October 2020 was released a report in which the ECB's governing council decided to start the investigation phase about the European CBDC and since that date three reports about different issues have been issued.

The first report was published in September 2022 and was about functionalities and limits for users. It states that should be used only for payments and not as investment tool to maintain a financial stability and not cause a mass movement of deposits from commercial banks to the central one.

For these reasons in a speech in June 2022, Fabio Panatta (Member of the ECB's Executive Board) disclosed that the holdings limit will be around 3,000 - 4,000€ which is equal the average amount of cash used by European citizens annually. With a banked population around 300 million, this implies a deposit movement around 1,050 billions euro (6.5% of the total, equal to 16,137 billions euro) from commercial banks to the central one.

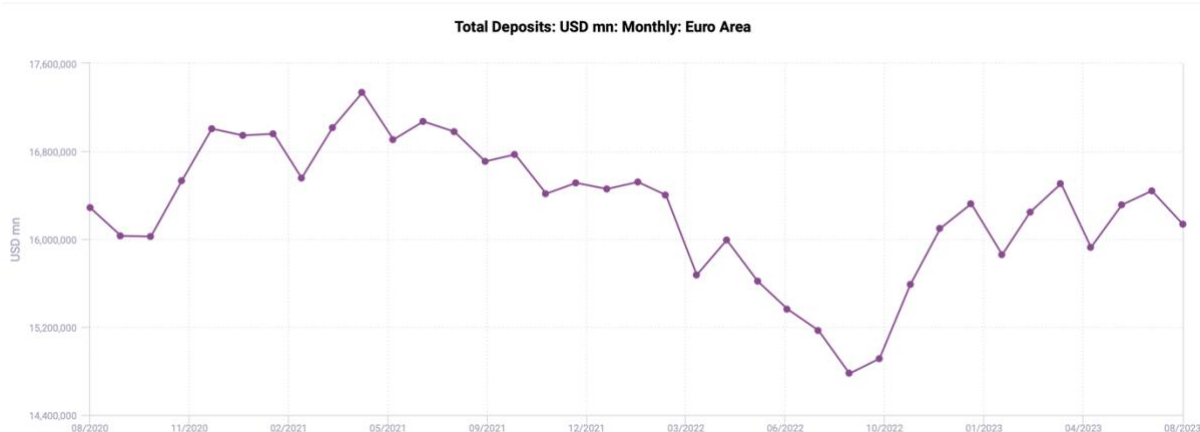


Figure 31. European Union total deposits, “<https://www.ceicdata.com/en/indicator/european-union/total-deposits>”.

Since the actual excess liquidity is around 3,600 billions is not expected a great disruption in the financial system because the losses can be recovered from the excess also doing a favor to the commercial banks in period of negative interest rates.

The digital euro should replicate cash features as much as possible, anonymity is not fully ensured but the ECB will apply the highest standards of privacy. This is due to worries about money laundering and the difficulty in controlling the amount in circulation, which is necessary to limit its use for investment purposes .

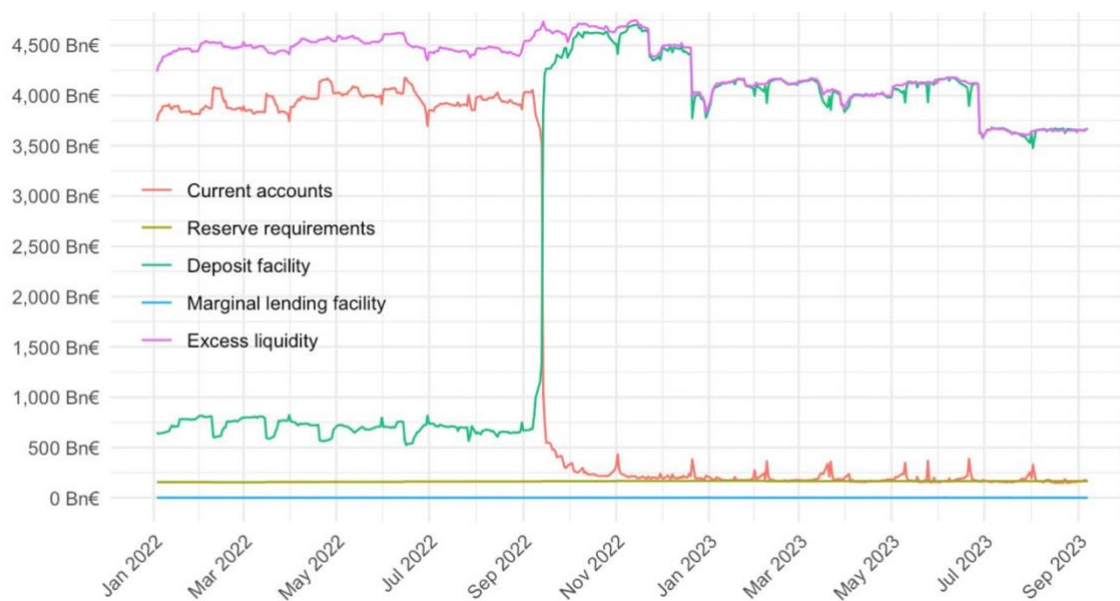


Figure 32. Excess liquidity graph, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747868/IPOL\\_ATA\(2023\)747868\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747868/IPOL_ATA(2023)747868_EN.pdf).

$$\text{Excess liquidity} = (\text{Current accounts}) - (\text{Reserve requirements}) + (\text{Deposit facility} - \text{Marginal lending facility})$$

According to the second progress report in December 2022, the digital euro would be a direct central bank liability, in other words, account holders will have a direct claim on the central bank that is convertible one-to-one with the euro, without a remuneration but at the same free. This differs from the euros that we use digitally today since deposits in a commercial bank in the euro area are only partially guaranteed by the state, to the amount of €100,000<sup>xxi</sup> and are remunerated by interest rate.

The third progress release in April 2023 states that non-resident could have access on the condition that they have an account with a euro area payment provider and that the Digital Euro will not be a programmable money. This means that the ECB would not determine with where, when and for which purpose the currency is used.

This is the scenario provided by ECB with the purpose of digitalize the financial sector and the cash overtaken by digital euro, despite that with the holding limit to 3,000 - 4,000€ the investment needed to implement is not sure it is worth it, but at the end of this year probably we will have more answer from the commission.

### **EU unconstrained scenario.**

Once viewed the scenario in which the CBDC issuance has a holding limit, let's try to imagine a hybrid in which corporate and governments can join this new way of payments with no strings attached to anyone.

In this case the holding limit does not exist and thus, the issuance has no constraint.

Considering the extreme scenario in which families and corporates in Europe move all their saving in the Central Bank there could create disruption in the financial system with magnitude consequences for the commercial banks.

Indeed, an increase in the amount of CBDC issued is associated with a change in equilibrium, with shifts in deposits. This affects both ECB and commercial bank accounts.

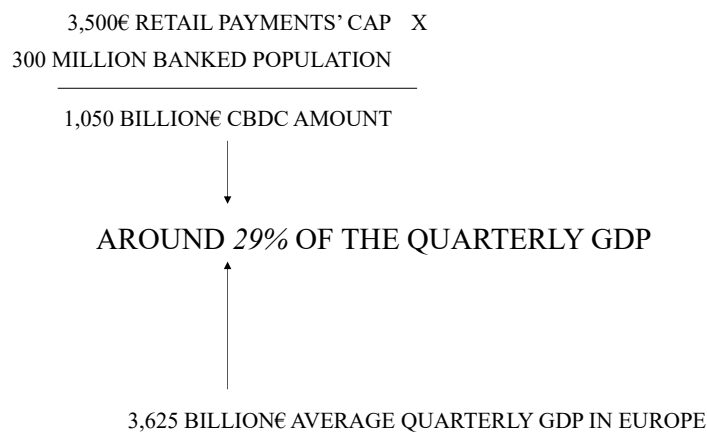
- In the balance sheet of the Central Bank, there is an increase in assets, because the decrease in reserves and cash does not fully compensate for the issuance of CBDCs; furthermore, profit also increases because by making CBDCs deposits less profitable than normal deposits in commercial banks, the interest rate at equilibrium is lower, and this combined with an increase in assets causes profits to increase compared to the current situation.
- On the commercial bank' balance sheet on the liability side there is a shift from deposits of customers to funding from the ECB and assets from loans to private sector towards government bonds, required as collateral by Central Bank.

The consequence of this shift can bring the financial system to its knees with a compression in the margin from loans, which tends to affect bank lending supplies and GDP (called as “bank disintermediation effect”<sup>xxii</sup>).

These two scenarios described satisfy the different views by ECB, which wants an innovative way of payments which replicate the euro and the EU which wants Europe leader in the international payments.

Which is the better implementation being extremely hard to say but according to Smetz<sup>xxii</sup> and Burlon, which have performed six different CBDC policy rules (3 quantity one under 3 different regimes) the optimal issuance between 15% and 45% of quarterly GDP.

Thus, with this criterion if we analyze the first scenario, with an average quarterly GDP around 3,625 billion euro, the percentage is 29%, thus is the optimal choice (the second scenario goes over the 65 % per design so it is not considered).



## **Geopolitical reason behind the Digital Euro**

Since World War II, the US has understood the power that currency can have in the world economy. From the Bretton Woods agreements, that came into force in 1944 in which fixed exchange rates were instituted with the dollar playing a central role, to today where the American currency is accepted as a means of payment for all raw materials and heads the SWIFT payments system. From these, one can see how the dollar is not just an instrument of exchange, as we have always understood currencies today, but has become a political medium through which the US has imposed its authority. The case of Russia, which has been cut off from international payments, is only the latest example of a practice that has been used extensively since the post-war period.

On the other hand, relations between Europe and the United States have deteriorated slightly over the past fifteen years, both economically and politically, becoming no longer as solid as they were in the last century and placing the old continent in the middle between the US and China (in particular, the latter has become Germany's main trading partner).

These two situations have caused the EU to question the introduction of a CBDC that would allow for a much faster, more efficient, and strategically independent global international payments system for Europe, avoiding possible sanctions and allowing the exchange of raw materials through its currency.

In an increasingly globalized world, the Digital Euro would provide Europe with greater unification, with Europeans' savings being shared in the Central Bank, and it would make it possible to intercept the new demand for digital payments otherwise destined for China with its Digital Yuan.

## **Future Perspective**

As analyzed in the chapter, there are many implementation proposals in this sector, and what until a few years ago seemed like a distant hypothesis will now probably become reality.

At the conclusion of the preliminary phase on 18 October 2023, the European Central Bank decided to move on to the next phase: ‘*the preparation phase*’, which has been started on 1<sup>st</sup> November and will last two years.

The digital euro *"would be configured as a digital form of cash that could be used to make any digital payment throughout the euro area and would be widely accessible, free of charge for basic functionality and available both online and offline. It would ensure the highest level of privacy and allow users to settle payments in central bank money instantly"* and also *"could be used for person-to-person payments, at points of sale, in e-commerce and in transactions with public administrations"*.

The preparation phase for the digital euro *"will involve the development of the standards manual and the selection of suppliers who could develop the necessary platform and infrastructure"* and after two years it will be decided whether to move on to the next phase of preparations, creating the conditions for a possible issuance and introduction of a digital euro in the future.

Panetta added that citizens' preference for digital payments made Europe adapt and be ready for a new currency alongside cash that could keep up with the times. This, he adds, would increase the efficiency of European payments.

President Christine Lagarde added that the digital euro would stand alongside cash, which would always be available, so that no one would be left behind<sup>xxiii</sup>.

In the Eurosystem's vision, *"a digital euro would be offered free of charge to individuals for basic functionality. A cost-sharing scheme between intermediaries and merchants would incentivise the former to distribute a digital euro, as is the case for other electronic payment instruments, and would provide adequate safeguards against merchants being charged excessive fees"*<sup>xxiv</sup>.

As for the ceiling that each user will be able to hold in digital euros (which is a different matter from the amount of the payment), the preliminary stage has not defined a maximum threshold. This decision will be taken by the EU legislator on the eve of the launch of the digital euro. But from what has been analysed, the threshold tested so far is probably around €3,000, but nothing is yet certain.

As with many innovations, the challenge is to find the right balance between fostering innovation and maintaining stability and protection for customers. But despite this, the will to innovate is there and probably in the next 5 years we Europeans will have to interface with this new payment method which will be a turning point for the European financial system.



## **Cryptocurrencies, CBDCs and concluding remarks**

In this analysis I have tried to explain the basics of Bitcoin and Ethereum, while also introducing the topic of Blockchain technology, then I have provided some general background on the topic of CBDCs, and I hope I have been as clear as possible in dealing with a very complex topic for neophytes.

In spite of this, I hope you have understood that the digital currency industry is still at an early stage, but the most important thing you can begin to glimpse is: the willingness to reduce the traceability of payments, with privacy protection methods guaranteed for example by the Blockchain system.

### **Cryptocurrency vs Central Bank Digital Currency**

Once Bitcoin, Ethereum and CBDCs have been analyzed very specifically, it is possible to understand how different these realities are, from the purposes for which they were created, to the structure that underpins them, and finally the effects on the economy. Understanding the differences between the various types of virtual currencies is necessary to fully understand them, which is why here is a list of the main differences.

- *Issuing entities and reasons:* CBDCs are issued by Central Banks to increase the effectiveness of the payment system which in the last years, is turning to digital payments. Instead, Cryptocurrencies are put into circulation by private entity as means of payment and with investment purposes;
- *Anonymity:* in the CBDCs case this topic is under discussion but probably it will not be granted, on the other side the transactions are visible to everyone but is not possible to know the people behind that;
- *Scalability and speed:* the scalability is not a problem for the two systems but with implications in the transactions speed; indeed Cryptocurrencies due to the mining process a low speed since they can handle only 6 blocks per hour instead CBDCs with a centralized authority are faster;
- *Recording process:* As previously mentioned the recording process is the centralized for the CBDCs to grant a higher transaction handling;

- *Regulation:* Central Banks around the world are starting to study the CBDCs with their policies instead cryptocurrencies, except for a few exceptional states, have not yet had adequate regulation;
- *Economy consequences:* CBDCs can induce Banking System run instead the Crypto one for their purposes are without risks;
- *Auditability:* The higher transparency granted by the CBDCs design allows financial institutions and regulators to audit instead the Blockchain technology with its distributed ledger makes that more difficult;
- *Environment:* the CBDCs ecosystem comprises central banks, commercial banks, and end consumers instead of most common digital assets, which are backed by a peer-to-peer network.

	<b>Central Bank Digital Currency</b>	<b>Cryptocurrency</b>
<b>Entity</b>	Central Bank	Private entity
<b>Reasons</b>	Increase the effectiveness of current payment system	Means of exchange, a store of value, and a form of speculation
<b>Anonymity</b>	No	Yes, but not always
<b>Speed</b>	High	Low, 10 minutes per block, remember the "Crypto trilemma"
<b>Scalability</b>	High	High
<b>Recording process</b>	Centralized ledger	Decentralized ledger
<b>Regulation</b>	High	Low
<b>Auditability</b>	Yes, by financial institutions	Independent issuer
<b>Economy effects</b>	Important to understand	Not relevant

## **Concluding analysis**

Currency over the centuries has evolved steadily from concrete forms, such as barter, to the FIAT we use today that is not backed by any physical asset but only declared legal claim by the issuing states.

I have tried to analyze the new forms of money that are taking shape in recent years, from digital assets to digital currencies issued by Central Banks, analyzing their design and possible scenarios.

Bitcoin and Ethereum have a very complex structure derived from the use of the Blockchain, but which guarantees a high level of security and privacy but does not allow them to handle a high throughput, with its only layer of development.

The Digital Euro, on the other hand, has a more centralized structure, since it will probably be issued and managed by the Central Bank, which will allow it to manage high throughput but without all the privacy policies of decentralized structures. We have analyzed the two main designs with the main consequences in the banking sector, which in Europe is fundamental as a '*bank-centric economy*', because it is the issuer of 80% of financing, unlike the United States where the percentage is much lower, around 30%.

We have seen that even the concept of currency has increasingly evolved from a simple medium of exchange to a real geopolitical tool, as in the most recent case of Russian sanctions, which may lead states to gain greater strategic independence from US hegemony.

In the coming years we will be faced with a change that will probably impact the European economy and the way we handle payments.

I believe that, the future of digital payments is towards CBDCs as they are issued by authorities that are able to transmit trust to users who are still very sceptical and uneducated on this issue, and at the same time guarantee a higher throughput that could perhaps replace even SWIFT, which is too expensive and slow for today's world.

On the other hand, cryptocurrencies will, in my opinion, have their place, they will always function as a financial instrument (a subject not of my interest and which I preferred not to deal with), and at the same time the increased privacy will drive many away from this world. A small number of users, relieved by the use of CBDCs as well, will lead to a better management of transactions, without exaggerated increases in queues and consequently the associated fees to have payments validated as soon as possible, which we talked about in the Bitcoin chapter.

In the coming years we will be faced with a change in the way we handle payments that will probably impact the European but also the global economy. Many states around the world are making efforts to try to anticipate others' moves in this field, as they are aware of the economic opportunity that would be granted to the pioneers of this technology.

In the meantime, on 14th October 2023, Ferrari announced that it would accept bitcoin payments to buy its cars, and who knows, maybe in the not too distant future other giants will also move in this direction.

Schumpeter, Austria Finance Minister in 1919, used to say that to “*innovate is to do old things in a new way*”, a definition that gives an idea of how important it is to adapt payment methods to an increasingly dynamic and globalized world, reducing costs and time associated with transactions and hegemonies of States over others.

## References

---

- <sup>i</sup> “*The basics of Bitcoins and Blockchains, an introduction to Cryptocurrencies and the technology that power them*”, Antony Lewis.
- <sup>ii</sup> “*Purchasing power of the Consumer Dollar in U.S. City Average*”,  
<https://fred.stlouisfed.org/series/CUUR0000SA0R>.
- <sup>iii</sup> “*Consumer price Index*”, <https://fred.stlouisfed.org/series/CUUR0000SA0R>
- <sup>iv</sup> “*A history of money from ancient time to the present day. Cardiff: University of Cardiff*”, Glyn Davies 1996.
- <sup>v</sup> “*Fiat Money*”, [https://en.wikipedia.org/wiki/Fiat\\_money](https://en.wikipedia.org/wiki/Fiat_money)
- <sup>vi</sup> “*The history of money*”, <https://www.pbs.org/wgbh/nova/article/history-money/>
- <sup>vii</sup> “*Digital Euro*”, [https://www.ecb.europa.eu/paym/digital\\_euro/html/index.en.html](https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html)
- <sup>viii</sup> “*What is money?*”, [https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/what\\_is\\_money.en.html](https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/what_is_money.en.html)
- <sup>ix</sup> “*Cryptocurrency*”, <https://en.wikipedia.org/wiki/Cryptocurrency>.
- <sup>x</sup> “*Bitcoin: A Peer-to-Peer Electronic Cash System*”, Satoshi Nakamoto.
- <sup>xi</sup> “*Mastering Bitcoin: programming the open blockchain*”, Andreas M. Antonopoulos
- <sup>xii</sup> “*Bitcoin source code*”, <https://github.com/bitcoin/bitcoin>.
- <sup>xiii</sup> “*Fee variation*”, [https://ycharts.com/indicators/bitcoin\\_average\\_transaction\\_fee](https://ycharts.com/indicators/bitcoin_average_transaction_fee).
- <sup>xiv</sup> “*How does Bitcoin source code define its 21 million cap?*”,  
<https://unchained.com/blog/bitcoin-source-code-21-million/>.
- <sup>xv</sup> “*Ethereum whitepaper*”, in 2014 by Vitalik Buterin.
- <sup>xvi</sup> “*London School of Economics and Political Science*”,  
<https://blogs.lse.ac.uk/businessreview/2019/11/04/do-six-per-cent-of-financial-transactions-sent-via-the-swift-system-really-fail/#:~:text=SWIFT%27s%20published%20error%20rate%20is%20six%20per%20cent>.
- <sup>xvii</sup> “*Sicurezza dei sistemi di pagamento, Blockchain e Swift a confronto*”,  
<https://www.agendadigitale.eu/sicurezza/sicurezza-dei-pagamenti-swift-e-blockchain-a-confronto/>
- <sup>xviii</sup> “*Ready, steady, go?*”, BIS paper, <https://www.bis.org/publ/bppdf/bispap114.pdf>
- <sup>xix</sup> “*Central Bank Digital Currency*”,  
<https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf>.

---

<sup>xx</sup> “*Opportunities for Bank’s objectives*”,

<https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper>

<sup>xxi</sup> “Progress with the Digital Euro”, By Maria Demertzis, Catarina Martins

<sup>xxii</sup> “*The optimal amount of central bank digital currency in circulation*”, Frank Smetz and Lorenzo Burlon

<sup>xxiii</sup> “*Eurosystem proceeds to next phase of digital euro project*”,

<https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231018~111a014ae7.en.html>.

<sup>xxiv</sup> “*What does the Europe say about CBDC?*”, <https://www.startmag.it/economia/euro-digitale-bce/>