POLITECNICO DI TORINO

Master's Degree in Engineering & Management

Bitcoin, cryptocurrencies & central banks

Supervisor:

Riccardo Calcagno

Candidate

Matteo La Rosa

December 2021

SUMMARY

Introduction

In recent years the world economy, especially thanks to technological and IT evolution, has seen ever greater changes, but above all numerous tools that have joined the already very complex financial world.

An important novelty that can be taken into consideration regarding a revolution in general payment systems: the use of "cryptocurrencies".

With Bitcoin as the progenitor, 2021 was the year of cryptocurrencies, the year in which they reached their all-time highs.

More than 13 years after the creation of bitcoin, with the consequence of the new releases of new altcoins, several nations around the world have agreed that they can no longer ignore this now rampant phenomenon.

There are many questions that economists, politicians and scholars ask themselves, but despite the fact that several years have passed, the scarcity of official documentation prevents them from providing correct answers.

There are many currents of thought: those who consider bitcoin as the exchange tool of the future, those who see it as an unsafe medium as it is not controlled, those who see it as a basis for the creation of official digital currencies.

The following document aims to analyze the world of cryptocurrencies as a medium of exchange.

In the first chapter the concept of money is taken up again.

The second shows a historical analysis of Bitcoin and the concept of blockchain. The main Altcoins are also briefly analyzed.

The third chapter analyzes the concept of CBDC, the advantages and disadvantages of their possible release.

In the fourth, a study is made of those states that have begun to take a stance towards cryptocurrencies and CBDCs.

Finally, before drawing conclusions in the last chapter, the fifth analyzes Bitcoin as a financial asset, with possible future developments, argued for and against.

CHAPTER 1

Money concept

Since XIX century, before with classical and neoclassical economists, and then with J.M Keynes, the functions of money have been debated.

According to **Quantitative theory of money**, developed by classical and Neoclassical, money had two different functions:

- Trading instrument
- Instrument to evaluate

First function was related to the thought that money has substituted **barter**, the oldest technique used between people to make exchanges, influencing the prices level, but without affecting real phenomenon of economic system. Barter had very high transaction costs, so money had the role to overcome all the inconveniences of it.

Second function instead was related to the possibility to find something acting as standard of values, as unit of account, to become "numeraire good". According to this theory it is important to understand that money itself has not an essential use because whatever good could be used as standard of value.

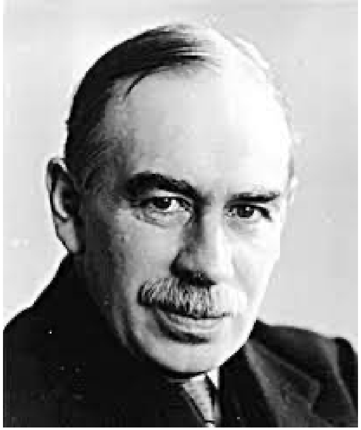


Figure 1- John M. Keynes

On the other hand, Keynes accepted the two roles proposed by Classical and Neoclassical, but added a new function related to **precautional** and **speculative** capacities of money. Money is held for reasons precautionary as the receipts and payments can vary randomly, while it is held for speculative reasons, since it is considered as a stock of alternative value to the possession of bonds whose price is uncertain. As a result, capital gains and losses may occur. In general, in the choice between currency and "Bonds", individuals seek to **maximize expected final wealth**.

It is possible to affirm that Keynesian theory is characterized by considering that money performs the function of **store of value** in addition to the functions of **means of payment** and **measurement of value**, already highlighted by quantitative theory. In this sense, the currency represents one among many financial assets which, together with the various real assets, constitute instruments of allocation of availabilities available to agents. Hence, the currency belongs to the same way with all these other activities, from which it is distinguished, however, by the possession of some properties in a "characterizing" way.

Money is the **most "liquid" asset** in what is immediately expendable to make transitions of all kinds. For **liquidity** in fact, we mean the ability of a financial asset to **convert quickly to low cost in circulating currency and to be immediately expendable**.
To a different extent it is in fact, also owned by many other businesses, so much so that it is possible to order all financial assets according to their degree of liquidity, on a scale with the circulating currency.
Economic agents consider the liquidity feature to be valuable of the currency so as to be willing to hold the latter even if in the absence of a return, or in any case in the face of lower rates of return compared to assets competitors: the yield differential represents a cost that economic agents are willing to pay to hold cash in the form of cash balances and therefore, enjoy the benefits in terms of liquidity services offered by the currency itself.

When economic agents must decide whether to allocate their availabilities in the form monetary or alternatively, consider several elements relevant. In particular, the coin can turn out to be more attractive since it is easily and quickly transferable, at no cost, and guarantees the face value of the sums invested.

Keynes thought that the liquidity-preference is determined by **rate of interest**: a lowering of the interest rate makes liquidity preferable for two reasons: firstly, it is preferred to hold money to take

advantage of a possible **increase in the rate in the future**; secondly, it is preferred to hold money to **avoid capital losses** resulting from the fact that when the interest rate increases, the value of the securities decreases. He called the low level of interest as "**liquidity trap**", a situation in which people hold all they wealth in a liquidity form.
The belief in a future negative event is key, because as consumers accumulate cash and sell bonds, this will drive bond prices down and yields up. Despite rising yields, consumers are not interested in buying bonds as bond prices are falling. They prefer instead to hold cash at a lower yield.

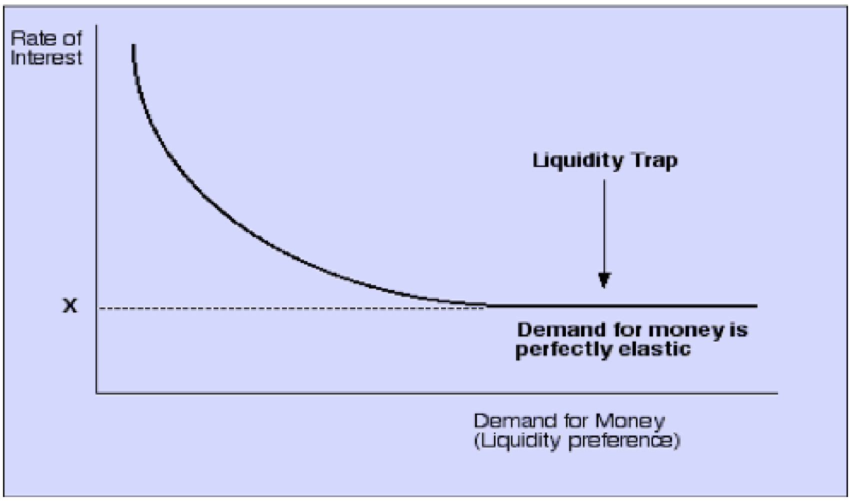


Figure 2- Liquidity trap

A notable issue of a liquidity trap involves financial institutions having problems finding qualified borrowers. This is compounded by the fact that, with interest rates approaching zero, there is little room for additional incentive to attract well-qualified candidates. This lack of borrowers often shows up in other areas as well, where consumers typically borrow money, such as for the purchase of cars or homes.

There are a number of ways to help the economy come out of a liquidity trap. None of these may work on their own, but may help induce confidence in consumers to start spending/investing again instead of saving.

1. The **Federal Reserve can raise interest rates**, which may lead people to invest more of their money, rather than hoard it. This may not work, but it is one possible solution.
2. **A (big) drop in prices**. When this happens, people just can't help themselves from spending money. The lure of lower prices becomes too attractive, and savings are used to take advantage of those low prices.
3. **Increasing government spending**. When the government does so, it implies that the government is committed and confident in the national economy. This tactic also fuels job growth.

Governments sometimes buy or sell bonds to help control interest rates, but buying bonds in such a negative environment does little, as consumers are eager to sell what they have when they are able to. Therefore, it becomes difficult to push yields up or down, and harder yet to induce consumers to take advantage of the new rate.

In general, when consumers are fearful because of past events or future events, it is hard to induce them to spend and not save. Government actions become less effective than when consumers are more risk- and yield-seeking as they are when the economy is healthy.

CHAPTER 2
Cryptocurrencies

There are many definitions of cryptocurrencies, but they can be resumed in:

“They are a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a national currency, but is designed to be accepted by some parties as a means of payment and can be transferred, stored or traded electronically. Cryptocurrencies use computer software running across a network and rely on various established cryptographic techniques (hashing, digital signatures or one-way cryptographic functions) to control access and verify transactions. They use some form of ‘consensus mechanism’ to validate transactions; that is, a mechanism to achieve agreement across the network on whether a transaction is valid or not.”
*(*Reserve Bank of Australia, 2019*)*

“*A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology—a distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.*”
(Investopedia, 2021)

They are a very simple definition given by one of the most famous websites about finance and investment. But nowadays, to define what cryptocurrencies are, is still not easy.

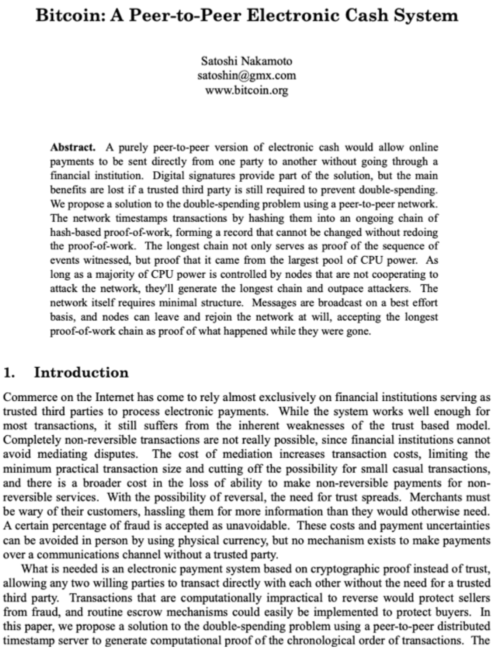
Origins

A first debut of the concept of cryptocurrency has its roots in the distant 1982, with the publication of an article by David Chaum[1], entitled "Blind Signature for Untraceable Payments", in which a new concept was introduced: the concept of "blind signatures", a sort of digital signature that is placed on the message before it is opened and read.

The same author stressed the practical implications of this project in the payments sector, which can be expressed without the need for control by the authorities and with the adoption of anonymous forms using pseudonyms.

In 1988, Chaum published a paper entitled "The Dining cryptographers’ problem: unconditional sender and recipient untraceability", in which for the first time the concepts of "public key" and "private key" were discussed. Although Chaum's project did not have a real practical realization, it nevertheless captured the interests of the Cyberpunk movement, a group of activists who saw in information technologies and cybernetics useful tools for radical change in society, which in 1994 included it in the manifesto of the Crypto - Anarchists.

In essence, the anarchists of the manifesto identified in the cryptography and



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. 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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The

Figure 3- Original version of Bitcoin: A Peer-to-Peer Electronic Cash System, Nakamoto 2008

[1] American computer scientist and cryptographer, known as a pioneer in cryptography and privacy-preserving technologies

ciphering system devised by Chaum, a tool that could potentially prove useful in their struggle for sovereign power.

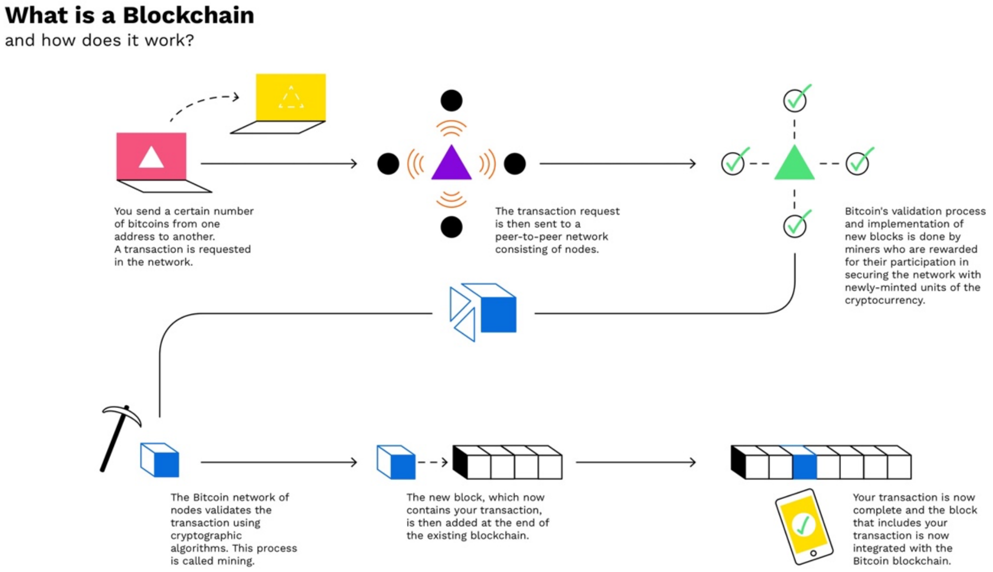
Based on the ideas of Chaum, Wei Dai, a Chinese computer engineer and exponent of the cyberpunk group, came to a concrete idea of cryptocurrency in 1998, and proposed a system of exchange of value and stipulation of contracts, which were based on the use of a digital currency that guaranteed the anonymity: "b-money".
After some tests his theories were impossible to be implemented because they were not able to avoid **double spending**, a process which permitted to duplicate coin and spend it more than one time.
So, to see the birth of Cryptocurrencies, it is necessary to wait for 2008, turning point year for all theses theorized during all previous years.

In fact, the 18 august 2008 the *bitcoin.org* domain was registered for the first time on *anonymousspeech.com* by a person with the pseudonym of **Satoshi Nakamoto**, and, in October of the same year, there was the online publication of a white paper dealing with the subject, also considering the aforementioned cryptography; this document, called "*Bitcoin A peer-to-peer electronic cash system*", contained all the technical details of the cryptocurrency which, to date, is considered the most important (and not only by capitalization), but, above all, proposed for the first turns the idea of not tracking money, but **transactions**.

In this way, with the **traceability of transactions**, a brake is placed on the phenomenon of "double spending", guaranteeing greater trust in the system since, by preventing "double spending", or rather that the same Bitcoins were used for different transactions, it is not possible to create money out of thin air.
On January 3, 2009 the official launch of Bitcoin in the market took place; in fact, the first block of 50 BTC was put in place, the **Genesis block**, also called **block zero**, containing a sentence that read the title of an article on the front page of the “Financial Times”: “Chancellor on brink of second bailout for banks”.
But after more than 12 years the mystery remains about the identity of the creator of Bitcoin, about who the person behind the pseudonym of Satoshi Nakamoto is.

Blockchain

The cryptocurrencies system, seen by many as revolutionary, has its foundations in a technology called **Blockchain**. Blockchain is structured on a very complex organization based on a series of blocks that store a series of transactions validated and correlated by a **Timestamp**. The Timestamp guarantees security to the model, as it prevents the operations, once performed, from being canceled or modified.



You send a certain number of bitcoins from one address to another. A transaction is requested in the network.

The transaction request is then sent to a peer-to-peer network consisting of nodes.

Bitcoin's validation process and implementation of new blocks is done by miners who are rewarded for their participation in securing the network with newly-minted units of the cryptocurrency.

The Bitcoin network of nodes validates the transaction using cryptographic algorithms. This process is called mining.

The new block, which now contains your transaction, is then added at the end of the existing blockchain.

Your transaction is now complete and the block that includes your transaction is now integrated with the Bitcoin blockchain.

Figure 4- Blockchain structure

It also allows to associate a certain and legally valid date and time to an IT document, attributing a timestamp that can be opposed to third parties. Each block includes the **hash** (a non-invertible computer algorithmic function that maps a string of arbitrary length into a string of predefined length) which uniquely identifies the block and allows the connection with the previous block by identifying it.

The technology also allows the creation of **shared archives**, obtaining an articulated computer network in which the numerous and different transactions are kept through a decentralized database which will also include the amounts of the same and the pseudonyms of those who carry them out; this meticulous structure therefore becomes difficult to violate, being able to make changes, at a later stage to the transaction, only with the consent of the counterparty.

A single **digital register** is therefore created which will base its operations on the numerous nodes of this organization and will be available for consultation by all, thus guaranteeing significant transparency and traceability.

The blockchain can therefore be considered a technology that belongs to the category of **Distributed Ledger technologies**, **DLT**, which can be defined as a set of systems conceptually characterized by the fact of referring to a distributed ledger, governed in such a way as to allow access and ability to make changes by multiple nodes of a network. Any transaction, or the data that represents it, is subjected to an asymmetric **double key signature mechanism** which, although not equipped with certificates issued by accredited certifiers (the blockchain precisely provides for the overcoming of centralized certifying bodies), works with a similar mechanism to that of the digital signature. DLTs provide for the use of **cryptographic algorithms** that enable the user to use the system, providing him with a public and a private key that is used to sign transactions or to activate smart contracts or other services connected to the blockchain.

Smart contracts have the task of verifying the fulfillment of certain conditions and automatically carrying out actions (or providing instructions so that certain actions can be performed) when the conditions determined between the parties are reached and verified. In a nutshell, the Smart Contract automatically executes itself when the data which refer to real situations are the same to data which refer to the agreed conditions and clauses, which are already present in the contract.

The DLTs therefore envisage a validation mechanism, which in turn is distributed, based on the concept of consensus, that is, on mechanisms that also govern this type of participation of the nodes.

The methods of managing consent, together with the logics for setting the register, represent two of the main qualifying points of the identity card of Distributed ledger technologies.
Very important is the concept of **Proof of work** (Pow), which already existed before Bitcoin and is perhaps among the greatest ideas behind Nakamoto's white paper, because it achieves trustless and distributed consensus.

A reliable and distributed consent system means that if you want to send and / or receive money from someone you do not need to rely on third party services, unlike when using traditional payment methods, where you need to use a third party to set up the transaction. This will then maintain its own private ledger which stores the transaction history and balances of each account.
With Bitcoin and a few other digital currencies, everyone has a copy of the ledger, so no one has to rely on third parties, because anyone can directly verify the written information. Proof-of-Work, is the original consensus algorithm in a Blockchain network.
In Blockchain, this algorithm is used to confirm transactions and produce new blocks to the chain.
With Pow, miners are pushed to compete each other to complete all the transactions, extracting bitcoin and earning the reward.
A decentralized ledger collects all transactions in blocks; however, great care must be taken to confirm transactions and organize blocks.

Proof of stake is a different way to validate transactions and obtain distributed consensus. It is still an algorithm, and the purpose is the same as Pow, but the process of achieving the goal is quite different. Unlike Pow, where the algorithm rewards miners who solve mathematical problems with the aim of validating transactions and creating new blocks, with **proof of stake (PoS)**, the creator of a new block is chosen deterministically, to depending on its wealth, also referred to as "stake".
Also, all digital currencies were created earlier in the day and their number never changes.
This means that there is no block reward in the PoS system, so the miners accept the transaction fees.
(BitcoinNews, 2018)

Another determining factor is that which, by means of a complex technique that allows the creation of encrypted blocks linked together by means of unchangeable encrypted keys guarantees the non-duplicability of information.
As a demonstration of the security and inviolability of this technological organization, it must be said that since 2009, countless attempts have been made to violate the blockchain, but no one has ever succeeded; the blockchain is public and therefore anyone can have access to it, but it is inviolable precisely due to the fact that it is distributed in a huge amount of computers and therefore there would not be a single server to modify, but a very high figure.

Blockchain is based on a network **P2P**.
Its 5 fundamental characteristics are:

1) **Transparency**
2) **Security**
3) **Immutability**
4) **Decentralization**
5) **Consent**

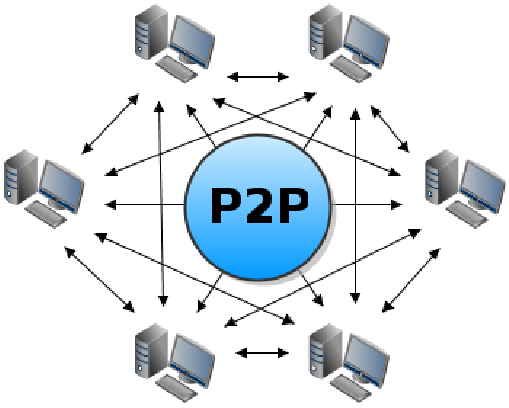


Figure 5-P2P

Starting from these principles, the blockchain has become the digital declination of a new concept of **Trust**.
For these reasons, some believe that the blockchain can also take on a value for certain aspects of a "political" type, as a platform that allows the development and realization of a new form of **democracy**, truly distributed and able to guarantee everyone the possibility to verify, to "control", to have total transparency on the acts and decisions, which are recorded in unchangeable and shared archives which have the characteristic of being unalterable, unchangeable and therefore immune from corruption.

The blockchain is also often associated with the concept of **virtual currency and digital payment**. It has great value both in the extraordinary Bitcoin experience, and as a platform for the management of transactions and exchanges of information and data even in completely different sectors far from finance and payment.

(BitcoinNews, 2018)

Main type of cryptocurrencies

With the years come by, the number of cryptocurrencies has increased exponentially and in June 2020, the platform *coinmarketcapt.com* said that there were more than 2600 on the market.

In September 2021, the same platform affirmed that according to capitalization the 5 most important cryptocurrencies on the market were:

CRYPTO	MARKET CAPITALIZATION
Bitcoin	$788,548,858,269
Ethereum	$338,345,537,692
Tether	$68,748,869,171
Cardano	$65,288,720,392
Binance Coin	$60,003,605,851

It is easy to understand from the different capitalizations that, although there are thousands of different cryptocurrencies, Bitcoin occupies most of the market.

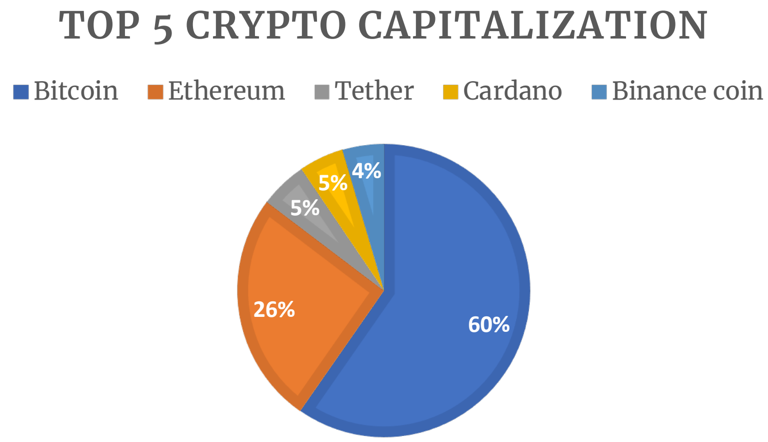


Figure 6- Market capitalization

Ethereum

If the Bitcoin blockchain aims to decentralize online banking and redesign the transaction system, the Ethereum blockchain aims to use a blockchain to replace the Internet's third parties: those that store data.

Ethereum was born in 2013 by Vitalik Burerin, a developer of Russian origin who grew up in Canada; he collected the main features of the platform in a white paper from November 2013 and subsequently published further specifications in a yellow paper in early 2014. July 30, 2015 is the release date of the first version of the platform.

Ethereum can be defined as a planetary scale computer. With Ethereum we move from the concept of Distributed Ledger to that of Distributed Computing or World Computing: a "world-virtual computer" that tries to decentralize the existing client-server model and is composed of all the computers connected to the Ethereum network but, in parallel, it is autonomous from them. Therefore, those who are part of the network will have access to an immutable and shared archive of all the operations that have been carried out: "Any possibility of downtime, fraud, censorship and third-party interference". Ethereum is reliable, safe, transparent, everywhere (wherever there is an Internet network). It is also a programmable blockchain: it does not limit itself to making predefined and standardized operations available, but allows users to create their own and to develop different types of decentralized blockchain applications, not necessarily limited to cryptocurrencies alone.

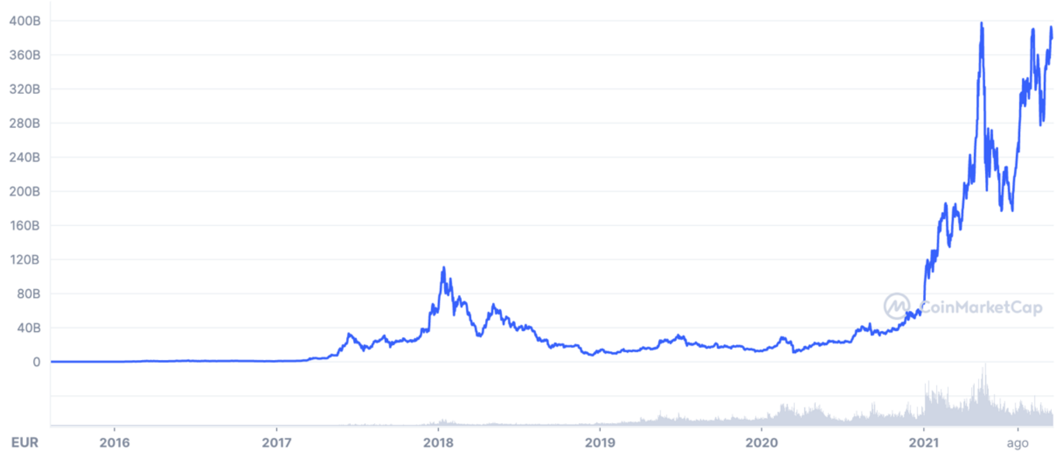


Figure 7- Ethereum market capitalization

How does the Ethereum blockchain work?
Those who participate in Ethereum work on a P2P (or peet-to-peer) network and can develop smart contracts using the computational resources of the network; the use of these resources is remunerated with a cryptocurrency, ether. Ether or ETC is, like bitcoin, an equal and decentralized cryptocurrency that uses cryptography to control its creation and transactions; it has a binary functionality, since it is both the computational power needed to produce the contracts and the compensation to the users for their realization.

(Ethereum.org, 2021)

Tether, 2021

Tether

Tether is a stablecoin, that is, a digital currency that aims to be a stable replacement for a legal tender (fiat currency). On the official website, the definition assigned to cryptocurrency is as follows: "*Tether converts money into digital currency, to anchor or tie the value to the price of currencies such as the US dollar, the euro and the yen*". (Tether, 2021).

Tether (USDT) is the world's first stablecoin (a cryptocurrency that simulates the value of a fiat currency). It was originally launched in 2014 under the name Realcoin by Bitcoin investor Brock Pierce, entrepreneur Reeve Collins, and software developer Craig Sellers.

USDT was initially issued on the Bitcoin protocol through the Omni Layer, but has since migrated to other blockchains as well. In fact, as the graph below shows, most of its offering is on Ethereum as an ERC-20 token. Additionally, it is issued on several other blockchains, including TRON, EOS, Algorand, Solana, and OMG Network.

As the original Tether white paper explains:

"Each outstanding unit of Tether issued is backed at a 1: 1 ratio (i.e., one USDT Tether is one US dollar) by the corresponding unit of fiat currency in the reserves of Hong Kong based company Tether Limited".

Tether is very important because it is able to fill the gap between crypto and fiat currencies. It offers investors an easy way to get a 1: 1 trade for the USD, without the inherent volatility of other cryptocurrencies.

Thanks to this stability, investors can hold a digital asset similar to a fiat currency but with the ability to exchange it for other currencies in the crypto markets. The main features make Tether a popular currency - albeit not immune to risk.

Tether can be used for:

Quick access to market stability

If the price of Bitcoin or other crypto assets is falling fast, you can quickly trade it for USDT instead of trying to withdraw.

Easy transfer of funds between exchanges

With Tether, you can move your funds between exchanges very quickly. This can also be useful for arbitrage with other currencies.

Trading on crypto-only exchanges

Some exchanges do not offer fiat deposits and withdrawals, but allow USDT trading. By getting Tether first, you can trade on these exchanges without worrying about market volatility or allocating your main trading funds to BTC (or other crypto).

Forex style trading

Since USDT is pegged to USD, you can engage in Forex-style trading by trading local (non-US) currencies for USDT when their value is high against the USD. After that, you can withdraw in local currencies when their price drops or exchange it for other assets.

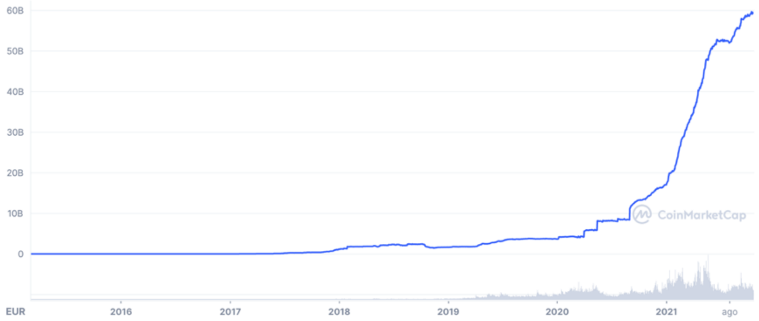


Figure 8-Tether market capitalization
(Thether.to, 2021)

Cardano

Cardano is the platform on which ADA was developed, a cryptocurrency that can be used to send and receive funds.
It is a smart contract platform created in 2014, with some features similar to Ethereum that offers new levels of security and scalability thanks to a multilayer architecture.
It is considered a “unicum” in the cryptocurrency universe because it was born with an extremely rigorous scientific and philosophical approach.
Cardano stands out for a, almost philosophical approach.

The development team did not start from a roadmap, but first of all wanted to identify the principles, best practices and development lines to which it includes, identifying about fifteen key points, which we report as presented on the official website:

- *Separation of accounting and calculation on different levels*
- *Implementation of core components in modular code*
- *Small groups of academics and developers competing with peer-reviewed research*
- *Use of interdisciplinary teams, including InfoSec experts*
- *Rapid iteration of white papers, implementation and new research needed to correct detected problems*
- *Ability to upgrade systems in post-deployment without destroying the network*
- *Development of a decentralized funding mechanism for future works*
- *Long-term vision on improving the design of cryptocurrencies, so that it can use on mobile devices with a reasonable and safe user experience*
- *Bringing stakeholders closer to the management and maintenance of their cryptocurrencies*
- *Recognition of the need to post multiple assets in the same ledger*

- *Inclusion of optional metadata in transactions to better conform to the needs of legacy systems*
- *Consider the best features of all alternative currencies out there*
- *Adopt a standards-based process*
- *Explore the social elements of commerce*
- *Find a middle ground to enable interaction with regulators without compromising the core principles inherited from Bitcoin.*

The Cardano protocol works on two distinct layers: on the first, the so-called Cardano Settlement Layer (CSL), you can find all the information on transactions, a bit like with Bitcoin (how much, emissary, receiver, time of transfer), and it is always on this level that the tokens of the platform, ADA, are transferred; the second level, the Cardano Control Layer (CCL) manages the account data, therefore the information of smart contracts, such as digital identities.

The separation of the two layers has the dual advantage of allowing updates to be made separately and in a targeted manner and increasing security, since the compromise of one layer does not affect the second as well.

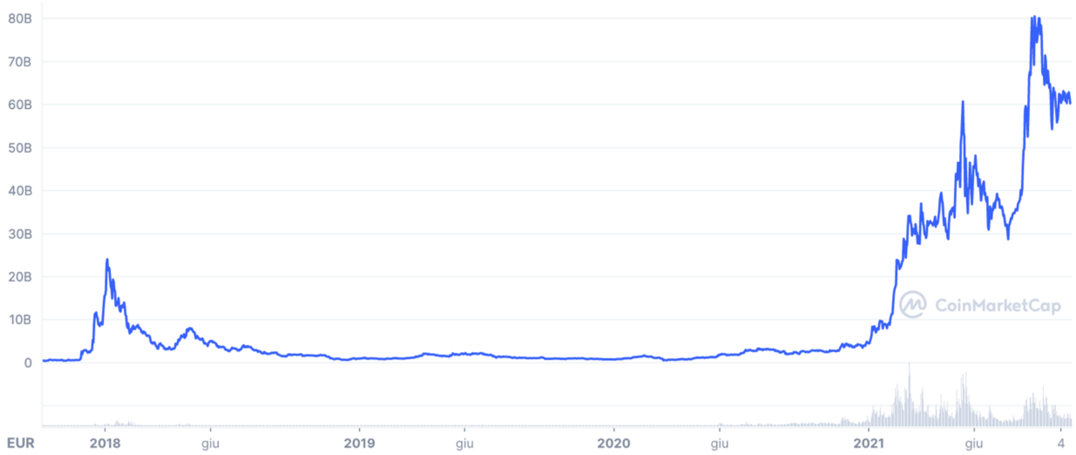


Figure 9-Cardano market capitalization

(Why Cardano, 2020)

Binance Coin

Binance Coin (BNB) is one of the most talked about cryptocurrencies since it began to exist (2017), and is the official cryptocurrency of Binance, from which it takes its name.

Binance is one of the world most important exchange born in China in 2017 and it has an average daily trading volume of 2 billion, with one goal: to become a pivot in the provision of infrastructure services in the blockchain system.

Binance Coin was born within a very integrated ecosystem, and its purpose is simply to access all Binance services at a reduced price. In particular, by buying tokens you have the opportunity to reduce the commissions to be paid to the exchange when exchanging cryptocurrencies and money.

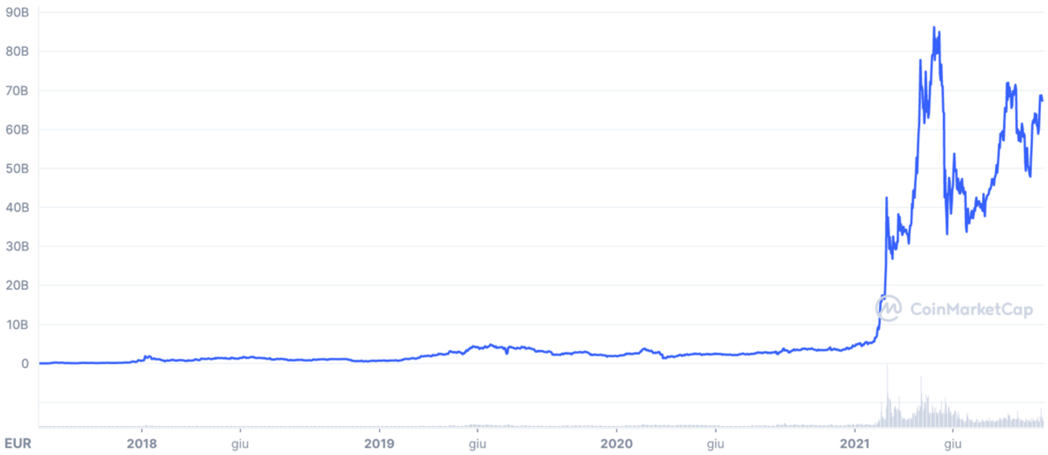


Figure 10-Binance Coin market capitalization

(Binance.com, 2021)

CHAPTER 3
Cryptocurrencies and central banks

Now, it is important to understand what the impact of cryptocurrencies on the market is and what would be consequences for the future. To do that it is necessary to go to remember that Bitcoin was created in 2008, a disastrous year for the world economic system, which has come to question the banking operating system and monetary policies, a period in which some people began suspicious also about Central Banks.
Nakamoto wanted to create a new form of coin, impossible to be influenced, an exogenous entity, detached from countries, banks and so on.

As the years go by, banks has started to understand the potential of blockchain and its derivatives, and they have tried to find new ways to apply distributed ledger technology (DLT) to their business.
Venture capitalists and financial institutions are investing heavily in DLT projects trying to find new financial services to provide, but also to improve the delivery of old ones.
(Bech Morten, Garratt Rodney, *Central Bank Cryptocurrencies*, 2017)

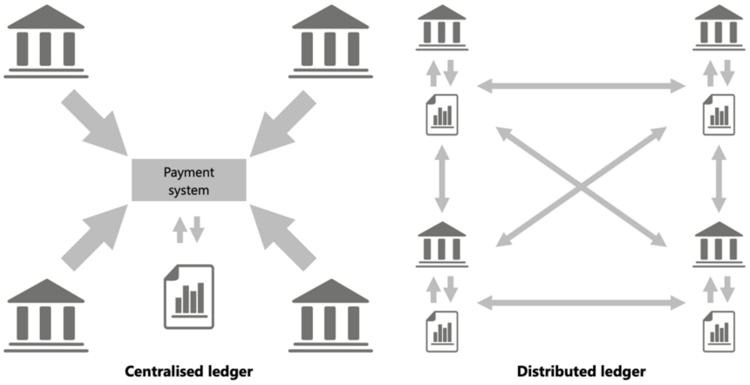


Figure 11-Centralized ledger vs. Distributed ledger

In the last period central banks has started to make announcements about their opening to DLT, and the possibility of new central bank cryptocurrencies has started to become a concrete possibility. On the

other hand, the lack of laws that regulate this sector it is not helping this important news.
Two are the possible liabilities issued by a central bank:

- Physical bank notes.
- Electronic central bank deposits.

Cash is the main payment method, but it doesn't pay interest. One of the main characteristics of notes is that they permit people to remain **anonymous** because it is not necessary to a third entity which record the transfer of cash. These kinds of transactions are **final and irrevocable**.

In contrast to bank notes, to access to central bank reserves is not as easy. This is typically limited to qualifying financial institutions that operate in the large-value payments system.
In different countries, only people who satisfy specific requirements can have an account at the central bank of the country itself.
This specific type of current accounts are transcribed within the books of the central bank, and allow you to settle credits between all participants. It is possible to say that these transfers correspond to approximately all digital transactions in the economy. Finally, since these transactions are present in the liabilities of the central bank, and being recorded in the ledger of the central bank, they are almost completely risk-free, final and irrevocable.

These important news about digital values have lead central banks to think about a new way to offer a new kind of value to clients by centralized accounts on their books. Therefore, there would be the opening to public of a service which, nowadays, is opened just to some financial institutions.

(Enger Walter, Fung Ben S.C, *Central Bank Digital Currency: Motivations and implications*, 2017)

Central Bank Digital Currency

“A Central Bank Digital Currency (CBDC) would be an electronic form of central bank money that could be used by households and businesses to make payments and store value. This wider access to central bank money could create new opportunities for payments and the way the Bank maintains monetary and financial stability”.
*(*Bank of England, 2020*)*

“Central bank digital currency (CBDC) is a generic term for a third version of currency that could use an electronic record or digital token to represent the digital form of a nation's currency. CBDC is issued and managed directly by the central bank and could be used for a variety of purposes by individuals, businesses, and financial institutions”
*(*Fed, *2021)*

Briefly resuming, a central bank would be able to distribute a decentralized digital value in the same way the physical value is distributed. This digital value wold be called Central Bank Digital Currency (CBDC). It would be a normal monetary value stored in a electronical token which would represent liabilities of central bank and it would be possible to use it to make payments.

(*Shobhit Seth, Central Bank Digital Currency (CBDC), 2021*)

Main advantages of CBDC

At first, the first advantage is that CBDC can **ameliorate retail payments** by making available efficient, secure, and modern central bank money to everyone in those, and strengthening the resilience, availability and contestability of retail payments. According to that there would be a switch from electronic payments made by money of commercial banks to electronic payments made by money of central banks.

"From a studio of Sveriges Riskbank's of 2018, they have found that collapsing demand for cash in the absence of CBDC, citizens would no longer have access to the central bank balance sheet. In that country of the world, trust in the currency would entirely depend on trust in financial intermediaries issuing and managing commercial money." The Riksbank concludes on the basis of its report that the "*proposed focus of this programme should be on developing an e-krona that constitutes a prepaid value (electronic money) without interest and with traceable transactions*".

(The Block Research, A *Global Look at CBDC*, 2020)

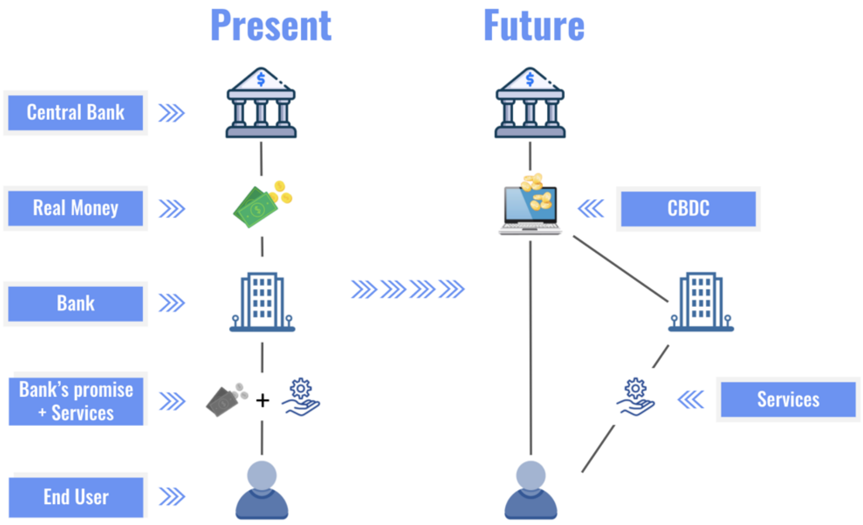


Figure 12-CBDC

Preserve central bank seigniorage revenue and guarantee central bank money for the public

A lot of studies shows that the use of bank notes in different countries has declined for the past 20 years. The idea now is to create a "**cashless society**".
This would cause an important problem for central banks, which they would risk to lose one of their primary sources of revenue: **seigniorage**. Seigniorage is a function of the value of bank notes outstanding.
Better explained, seigniorage is the sum of revenues that derive from issue of money. For central banks, seigniorage income can be defined as the flow of interest generated in return for banknotes in circulation (monetary base). Simpler, to print coins and put them into circulation, central banks ask for a price, a counterpart, for each banknote issued.
States ask central banks (which issue it) for money and pay a fee. A tot per banknote, a tot per coin.
So, the monetary seigniorage means that: for each printing or issue of money, commercial banks must pay as it does not issue the currency directly if it has it issued by the central bank and pays it a tax.

Seigniorage would decrease proportionally to a decrease in the number of banknotes on the market, above all if the reduction is about higher denomination notes.
The main consequences of that would be that a central bank might need to rely on government funding, and this could ultimately undermine its autonomy.

Issuance of CBDC would not be the only one response for the significant reduction of demand for bank notes, reduction which would threat seigniorage, because there are other ways for banks to sustain its revenues.
Indeed, a central bank could decide to charge other fees for various services it provides to financial industry participants, also imposing non-interest-bearing reserve requirements on bank deposits or other types of stored-value payment schemes.

Finally, a central bank could expand its balance sheet by buying government bills and bonds with reserves (similar to quantitative easing), to the extent that monetary policy objectives were not compromised and financial markets were not distorted.

Support unconventional monetary policy and reduce the lower bound on interest rates

A common idea is that after the 2008 financial crisis, major economies found themselves in a liquidity trap, where a lack of demand required very low real interest rates to shift aggregate demand towards potential output. And practically speaking, several countries have set moderately negative official interest rates.

For example, "Swiss National Bank (SNB) reduced its interest rate on sight deposits to −0.75 per cent in January 2015, in Sweden, the Riksbank lowered its repo rate to −0.1 per cent in February 2015, and currently its benchmark interest rate is −0.5 per cent, the Bank of Japan has maintained its policy interest rate at −0.1 per cent since January 2016, the European Central Bank (ECB) benchmark refinancing rate has been zero since March 2016, and the rate on its deposit facility, which banks use to make overnight deposits with the Eurosystem, was set at −0.1 per cent in June 2014, and declined to −0.4 per cent by March 2016".

What if a central bank wanted to reduce the effective lower bound (ELB) on interest rates?

Banknotes can bel held as an alternative to interest-bearing financial instruments, so depositors and investors who hold cash have instruments alternatives with a negative interest rate.
But, to hold large amount of cash generate risks and and high costs of storage.
The negative return on cash generates negative interest rates.

So, the reduction of ELB requires the increase of cost of claims, or the reduction of cash utility as a way to avoid negative interest rates.

This means banknotes or at least banknotes in denomination so as to avoid the frictions related to the conservation and storage of large amounts of cash.
In general, the larger the elimination of cash, the lower the ELB, with other conditions equal.
In the same way central bank could increase liquidity frictions stopping the notes convertibility or discounting/taxing their value in exchange for other liabilities of central bank.

But to eliminate larger denomination notes to reduce ELB doesn't require the introduction of CBDC: in fact, to introduce CBDC and to eliminate 500 euros note are two independent decisions.
So, it is possible to see that reduction of ELB isn't a sufficient motivation for CBDC emission.

In last years, given ELB on interest rates, some central banks have opted for a quantitative easing, buying financial assets like bonds directly from market participants.
In this way CBDC would support quantitative easing by easily transferring central banks funds to individuals and firms and so, helping the aggregate demand. This is called "helicopted money".
However, this kind of transfer would be also possible without CBDC but for sure, it would have higher costs.
In a nutshell, CBDC would be able to help transfers, but there are also other ways to do that. And this kind of operations are extremely rare.

Reduce aggregate risk and improve financial stability

Financial systems are characterized by highly levered firms which operates in the payment system, and they conduct liquidity and transformation of deadlines.
Banks issue liabilities which can be used in two ways: as store of value and as means of payment.
This is "inside money" and it comprehends private credit and money claims.
Obviously, there are conditions in which there would be problems and in the worst case the internal stock of money can reduce itself causing dramatic consequences for economy.

In this way, if people and firms would start to use CBDC in both ways, as means of payment and as store of value, they would use a method potentially risk-free.

On the other hand, the conversion from bank deposits to CBDC would have negative impacts on bank funding and credit provision, and consequently, on financial instability.

So, resuming, the type of impact of CBDC on the market would depend on different causes.

Increase contestability in payments

Generally, central banks are interested in make payments system as efficient as possible and CBDC would be useful for these reasons.

- "CBDC could provide an alternative to bank notes, cheques, debit and credit cards, on-line transfers, etc. So, CBDC could provide for more contestability in retail payments".
- "CBDC could also be used for large-value payments among banks and firms, and so could provide for more contestability in large-value payments as well".
- "CBDC could also facilitate access to the central bank's balance sheet for a wider range of financial institutions or even non-banks, thus making it easier for these firms to enter the payments industry, promoting contestability".

Promote financial inclusion

Some people suggested that CBDC could be useful to ameliorate financial inclusion, which in the most of modern countries is not a problem, but not all over the world.

In emerging economies, CBDC would become a means of payment easily accessible for all.

At the same time is true that it wouldn't be the only one solution because in countries like Kenya or Perù have found alternatives to CBDC like M-Pesa or Modelo.

Inhibit criminal activity

Sometimes operations made by large amount of cash are related to criminal activity. So, the elimination of cash with the introduction of CBDC, would be able to inhibit criminal activity. But in this way CBDC is not the only alternative. And at the same time, to have a digital and anonymous form of cash would also help criminal activities.

Second advantage would be to overcome the usage of banknotes for illicit payments and store of value. So, the reduction of banknotes would limit money laundering, terrorism financing and financing of illegal associations. On the other hand there would still be a problem related to the anonymity of CBDC.

(Stephen Cecchetti, Kim Schoenholtz, *Central bank digital currency: The battle for the soul of the financial system*, 2021)

(Cameron, Emery, Ma, Noone, *Cryptocurrencies: Ten years on*, 2019)

Main disadvantages of CBDC

There are 4 different problems related to CBDC emission:

- **Disintermediation**: in this case the inertia would help to maintain funds in the bank system for a while, on the long-term financial tensions would lead uninsured deposits to flee private banks to central banks. A
- **Currency substitution**
- **Lack of privacy**: CBDC would make traceable each transaction.
- **Inability to ensure compliance**: there would be the necessity to find people who work will be ensure that users of CBDC will be law abiding. And this is extremely costly. Nowadays this is outsourced from banks.

“One way to manage the privacy and compliance challenges is through the creation of *intermediated* CBDC. In this framework, brokers (or banks) provide individual account services, guarding privacy, monitoring compliance and aggregating balances into accounts at the central bank (which would presumably bear interest). However, this approach does *not* eliminate the risks of domestic disintermediation or currency substitution. Funds would still flow into the central bank, just indirectly through what are narrow banks in all but name”.

(Stephen Cecchetti, Kim Schoenholtz, *Central bank digital currency: The battle for the soul of the financial system*, 2021)

Other people think that CBDC would lead to misalignment because Ritengono che la CBDC porterebbe a varie distorsioni proprio a causa della disintermediazione bancaria: on the one hand, the central bank would take advantage of an unfair competitive advantage in collecting deposits and accumulate undue power and market share, on the other hand, the other would have disadvantages in credit emission, that would lead to financial lost which would fall on the taxpayer.

Generally, CBDC is like banknotes, but it would be more comfortable for some specific functions because it would be safer in for transactions in physical places and online payments.
It would also be extremely cheaper with respect to banknotes. All these factors are pros for CBDC usage.
It is expected that some merchants would decide to accept the usage for CBDC because without commissions on each transaction, would become a valid alternative to banknotes (on which bank would charge lower fees because CBDC is cheaper than banknotes), bancomat and credit card (on which are already charge fees from banks).
So, it seems that merchants would easily accept CBDC as payment method as long as the costs are lower, and people decide to accept it as a payment method.

Briefly speaking, to estimate how many CBDC would circulate is extremely difficult, but it is expected that they would be adopted as retail means of payment.
At the same time, it would be considered as store of value. And this is possible in situation in which interest rates are low and to detain a digital currency with low risks would be safer and cheaper (because detain the same amount in banknotes would have problems that have been mentioned before).

(Stephen Cecchetti, Kim Schoenholtz, *Central bank digital currency: The battle for the soul of the financial system*, 2021)

CHAPTER 4
Cryptocurrencies of central banks

Due to the success of cryptocurrencies like Bitcoin, governments throughout the world have gained interest in developing their own cryptocurrencies. Russia, China, Iceland, the UK, Canada, and the Philippines have all made efforts or signaled plans to build national cryptocurrencies. In part, these efforts represent the desire of policymakers to leverage the potential efficiency gains of cryptocurrencies over the existing forms of money transfer. Additionally, these currencies are an attempt to reassert government control over monetary policy when faced with the threat of an essentially untraceable, distributed cryptocurrency like Bitcoin.
It is no coincidence that authoritarian governments like Russia and China make the shortlist.
In the following pages an analysis of the situation of the main active states in the world of cryptocurrencies is reported.

United States

In 2016, **Federal Reserve Bank** (central bank of the United States) with Massachussets Institute of Technology, have started to develop a new platform for a digital dollar: **Fedcoin** a blockchain-based peer-to-peer payment system for Federated learning (an emerging collaborative machine learning method to train models on distributed datasets with privacy concerns) to enable a feasible Shapley value (solution concept based on the idea of reimbursement for a player who participate in a coalition) based profit distribution. Opposite from Bitcoin network where miners “mine” new blocks of currencies by solving meaningless puzzles, in FedCoin, blockchain consensus entities calculate Shapley value and a new block is created based on the proof of Shapley (PoSap) protocol.

The main idea behind this project would be to substitute cash and, as a consequence, it seems that some companies have tried to slow down its development frightened by the idea to be cut out from the market, or to lose profits.

In other words, the goal is to create a stable (tying the value of Fedcoin to value of dollar) and dependable cryptocurrency that delivers the practical advantages of bitcoin even if this means involving the central government and abandoning the Libertarian principles that many believe underlay Bitcoin's creation.

This new possible form of coin would not be a competitor of cryptocurrencies, but of fiat: Fedcoins would only be created if an equivalent amount of cash or reserves were destroyed at the same time.

An important issue is that, since the Fed acts as the gateway in and out of Fedcoin, it will have to know the public address of a Fedcoin recipient. Cash conversions could be done anonymously, but conversions of bank deposits would imply the Fed would know the owner of the public address. This identity-link could be broken via a third party funds distributor which accepts Fedcoin on a recipient's behalf and distributes them to the recipient anonymously. Of course, this would have to be trusted thirdparty and the Fed would have to agree to this.

At the moment Fedcoin has not yet been launched on the market.

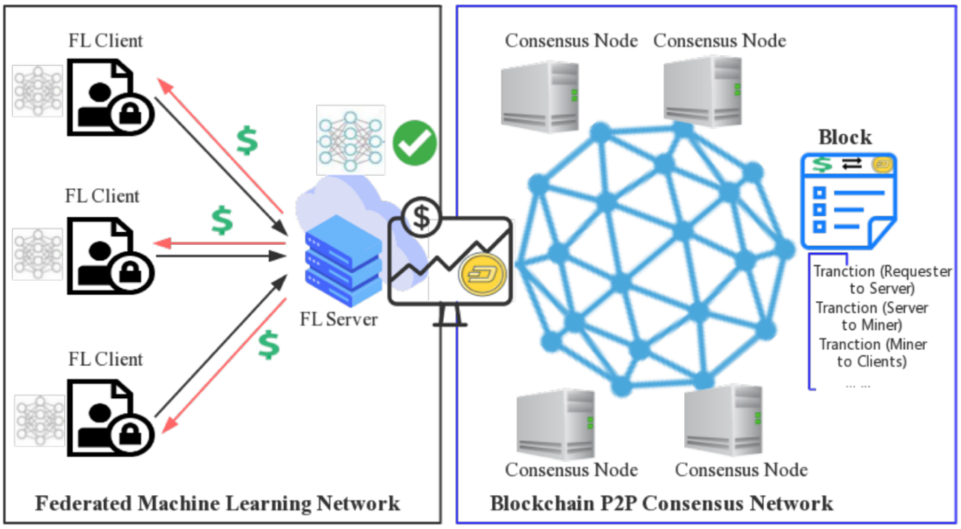

FL Client
FL Client
FL Client
$
$
$
FL Server
$
Federated Machine Learning Network
Consensus Node
Consensus Node
Block
Tranction (Requester to Server)
Tranction (Server to Miner)
Tranction (Miner to Clients)
... ...
Consensus Node
Consensus Node
Blockchain P2P Consensus Network

Figure 13- Fedcoin structure

(Yuan Liu, Shuai Sun, Zhengpeng Ai, Shuangfeng Zhang, Zelei Liu, Han Yu, *FedCoin: A Peer-to-Peer Payment System for Federated Learning*, 2020)

Russia

On 2017 the Russian president Vladimir Putin announced to be interested in the issuing of a state-sponsored cryptocurrency and on July 2021 has decided to form a first pilot group for the testing of CryptoRuble, a digital currency with the aim not to be an alternative to Bitcoin but to Ruble.
Twelve banks have been chosen for a small test while, following the plan, in 2022 they will permit citizens to test these digital tokens. The idea which lead the project is that CryptoRuble will give an important hand to decrease costs within the financial system, and at the same time, it will boost competition among banks.

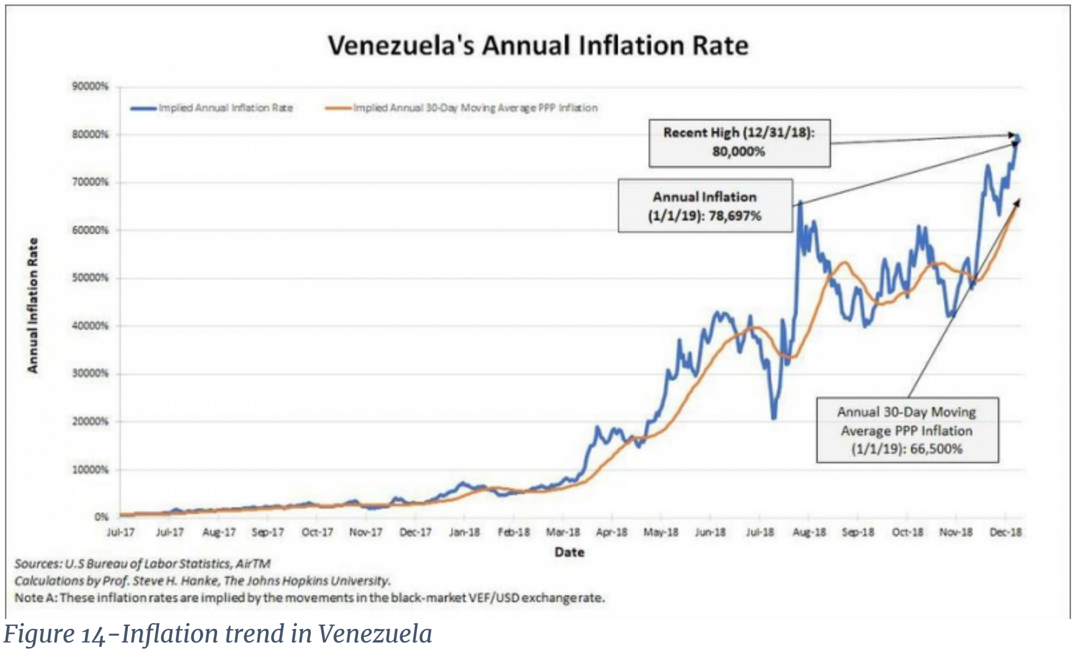
The CryptoRuble is expected to operate like the Russian ruble, just in digital and encrypted form. The CryptoRuble will have the same price the ruble has and will be able to be exchanged with traditional rubles.

Differently from decentralized cryptocurrencies in this case mining is not planned, and all transactions are recorded via blockchain and verified by a centralized government authority.
One of the main reasons for CryptoRuble is that Putin is interested in blockchain because transactions are encrypted, so it would be easier to send money anonymously and without worrying about sanctions placed on the country by the international community which won't have proof about his traffics. CryptoRuble will create a buffer layer that only the Russian government will have control over with pertinent information inaccessible to the U.S., the E.U., etc. Russian elite can launder their money using CryptoRuble, become impervious to (or less affected by) economic sanctions, make their assets currently tied up because of the U.S./E.U. controls (more) liquid, and so on.
Another is that it could help to stomp out other crypto like Bitcoin and Ethereum which are not under the control of government.
(Frankenfield Jake, *CryptoRuble*, 2021)

Venezuela

“The petro is a new sovereign cryptocurrency issued, developed and sponsored by the Bolivarian Republic of Venezuela, which is backed by one or more commodities (such as oil, gold, diamonds, coltan and gas) and which uses an electronic public ledger (or list of entries) of transactions conducted in that cryptocurrency maintained by various participants in a network of computers (commonly known as a blockchain) as a mechanism to ensure the transparency, validation and integrity of all such transactions.” (Norton Rose Fulbright)

On December 2017 Venezuela, one of the countries with the highest inflation in the world (2.665 % in 2021), decided to launch Petro, a new cryptocurrency purportedly backed by the country’s oil, natural gas, and mineral reserves. The Petro was launched in 2018 but has so far failed to gain traction or help solve the country's economic problems.



Sources: U.S Bureau of Labor Statistics, AirTM
Calculations by Prof. Steve H. Hanke, The Johns Hopkins University.
Note A: These inflation rates are implied by the movements in the black-market VEF/USD exchange rate.

Figure 14-Inflation trend in Venezuela

So, in early 2018, the government decided to propose Petro Gold, a new crypto with its value linked to the value of gold and other precious metals, but it was unclear if they were talking about gold produced in Venezuela, or gold that may remain in country's reserve.

The Petro Gold cryptocurrency announcement represents new other efforts by the Venezuelan government to aovid economic sanctions placed on it by the U.S. and other developed countries. In fact, the U.S. Treasury Department declared that Venezuela's cryptocurrency potentially violates international sanctions.

At the end of 2019 Maduro said "*The Petro is a marvel and a miracle that reaches our workers and retired workers of the country in order to make their purchases. It is a unique and extraordinary new experience of our economy. We are an example to the world!*"

In that month the government started to pay workers partly in Petros and partly in bolivar.

(Frankenfield Jake, *Petro Gold*, 2021)

In 2020 the government signed a new tax agreement that allows to start collecting taxes and fees in Petro.

(Norton Rose Fulbright, *Venezuela issues general legal framework on cryptoassets and the "petro" cryptocurrency*, 2018)

El Salvador

El Salvador is one of the last countries to show interest in cryptocurrencies (2021). Without having its own currency, in El Salvador people use dollars as medium of exchange. Studies said that each month expatriates Salvadoran send home nearly 700.000$ incurring in a lot of fees.
In fact, El Salvador's economy relies heavily on remittances, or money sent home from abroad, which make up around 20% of the country's gross domestic product (GDP).
More than two million Salvadoreans live outside the country, but they continue to keep close ties to their place of birth, sending back more than $4bn (£2.8bn) each year.
Government has decided to opt for Bitcoin in order to reduce all this expenses and it has started to partnered with several wallet and ATM providers to install the infrastructure to permit this migration.

However, many experts are of the opposite opinion: according to the International Monetary Fund (IMF), the adoption of bitcoin by El Salvador would be a risky and potentially dangerous move.

Above all, among the population the adoption of bitcoin is viewed with considerable distrust: many Salvadorans fear that the volatility of cryptocurrency could affect their savings, and according to surveys, two thirds of the population would like to abolish the law that sanctioned the adoption of bitcoin.
The 7th of September 2021, El Salvador has entered history becoming the first country in the world where Bitcoin has acquired legal tender alongside the national currency.
(Scozzari Carlotta, *La Stampa*, 2021)

China

From September 2021, Cina has declared that all transactions made by digital coin are illegal. This is a direct consequence of the decision of this spring when the government has decided to ban all financial institutions in the nation from providing cryptocurrency-related services to their customers.
Thus China intends to “stop speculation, criminal activities, illegal fundraising, money laundering”.

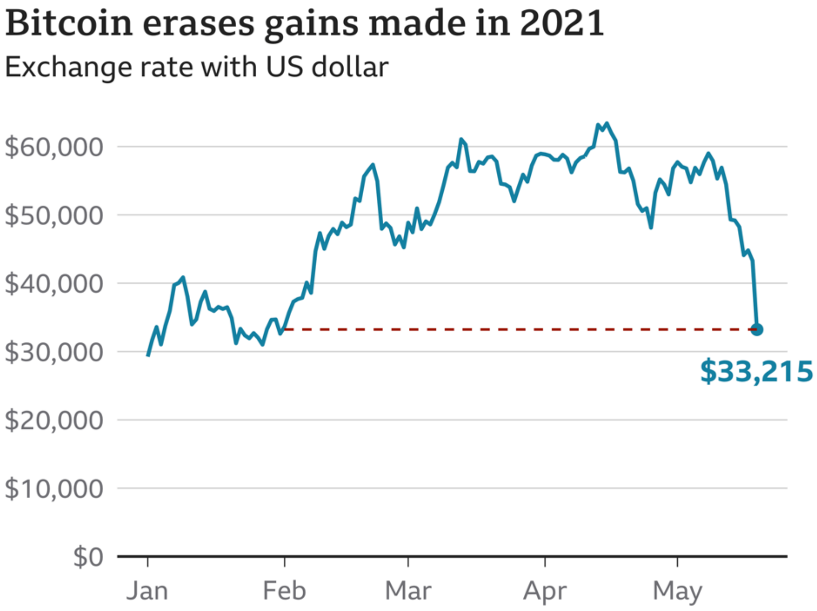


Figure 15- Bitcoin consequences after China's decision (May 2021)

Two important reasons would be at the basis of this choice:

1. **E-Yuan**
2. **Carbon emissions**.

According to the first reason, after some experiments, it seems there are already several Chinese regions that directly provide salaries in digital currency and there is an increasing spread of virtual wallets on the main online payment apps (Alipay and WeChat). Of course, the Beijing government could never have allowed the parallel development of the Chinese e-yuan virtual currency with cryptocurrencies, for obvious reasons. First of all, the fact that cryptocurrencies are conceived with characteristics (anonymous, encrypted) absolutely free from any control and, therefore, decidedly distant from Chinese ideologies. Unlike cryptocurrencies, in fact, the e-yuan is completely centralized and managed by the Chinese central bank. The latter could, if necessary, access the related data without hindrance, unlike what happens with cryptocurrencies. These characteristics, combined with increasingly frequent market fluctuations, have probably led the Beijing government to effectively halt the development of cryptocurrencies in China.

As for carbon emissions, however, the issue is of an environmental nature, also in line with the long-term development plans of the Chinese government.

It was noted, in particular, that the production of bitcoin consumes enormous amounts of energy. Just think, for a quick comparison, that the annual production of bitcoin for China alone emits the same amount of CO2 as the whole of Portugal.

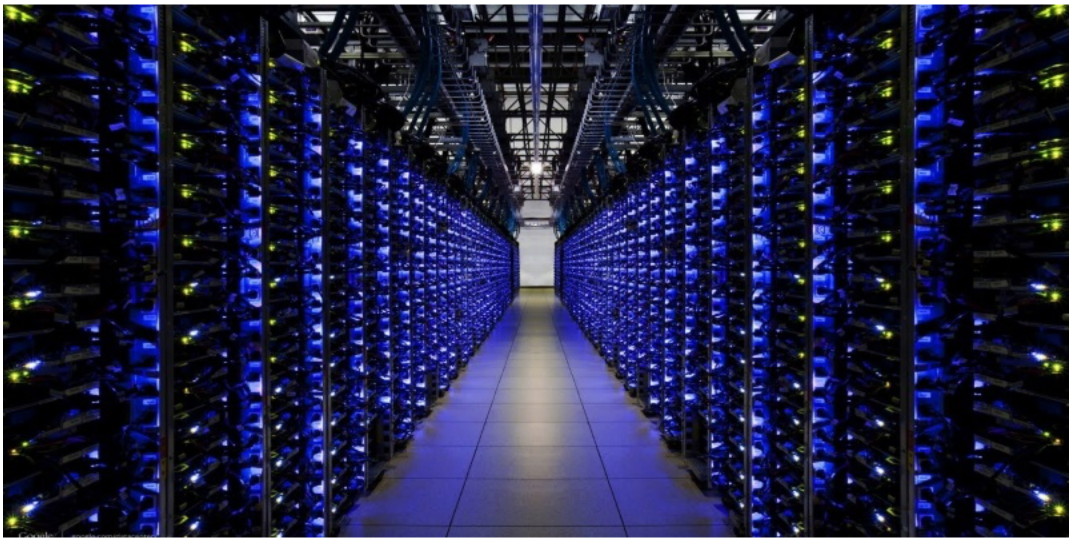


Figure 16-Mining center

The reason behind so much pollution is, essentially, the processing capacity of the data necessary for the creation of bitcoin. In fact, for mining, very powerful computers are needed that consume a lot of energy. According to the Cambridge Bitcoin Electricity Consumption

Index, mining activities over a calendar year consume 121.36 terawatt hours (TWh) of electricity. A truly impressive amount.

To obtain these levels of electricity, various sources are required, including coal-fired power. Specifically, the latter played a primary role. In fact, consider that the impact of the various sources on the production of electricity was respectively 17% for hydroelectric power plants, 20% for a mix consisting of wind, nuclear, gas and solar, and the remaining part for the coal (we are talking about over 60%). Here, then, is that the impact of coal on the issue of bitcoin production is very significant and the two issues are deeply interconnected.

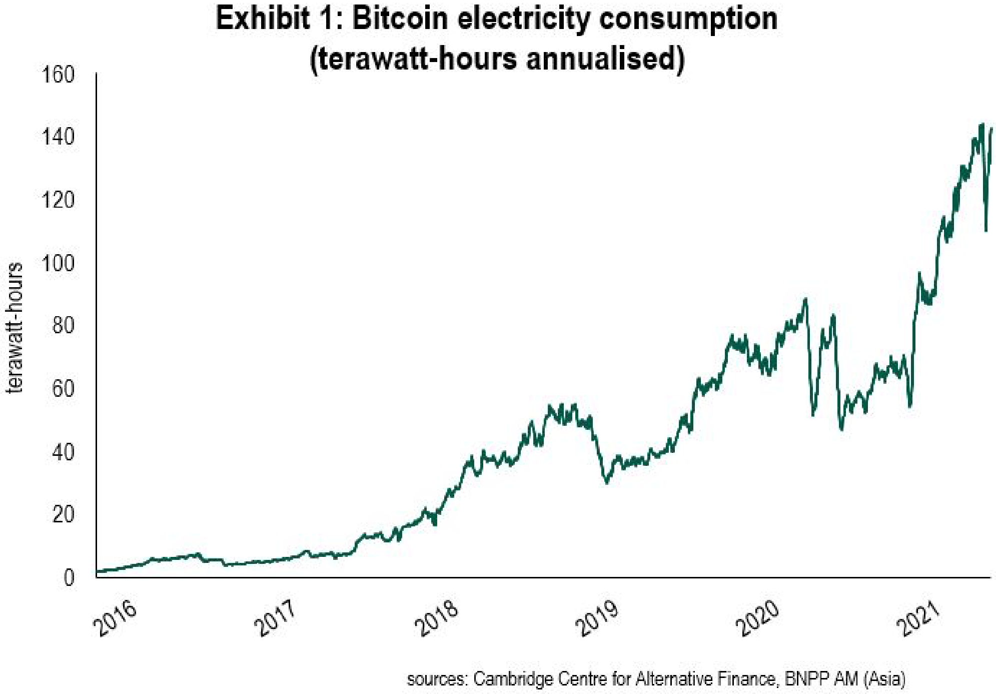


Figure 17- Bitcoin electricity consumption

Consequences of this decision were in some cases disastrous, causing a great confusion and the flight from the country to other Asian countries or USA.

(Bedini Davide, *La Cina dal blocco del bitcoin al lancio dell'eYuan: cosa c'è dietro e gli sviluppi futuri*, 2021)

France

In 2021 France started to test crypto assets in a series of government bond deals.

They have made one of the biggest and most important tests with cryptocurrencies in an established leading market making bond transactions thanks to digital assets and blockchain technology.

The biggest player of French financial markets has used a national digital currency issued by Banque de France for 10 months to experiment how it works in the country's debt market.

This experiment was led by the securities depository Euroclear and included many of France's largest banks, as well as the French public debt office and the central bank, and used a system developed by US-based IBM.

In March 2020, Banque de France started to study how digital currencies issued by the central bank would be exchanged settled if they had been converted to tokens, with agreements recorded in a digital ledger. Typically, transactions are reconciled between the parties, recorded, and assets transferred to a single authority, such as a central bank or securities depository.

Lawmakers are concerned of how private sector could react with cryptocurrencies, and how these could lead central banks to lose their control of monetary policy.

The consortium included BNP Paribas, Crédit Agricole CIB, HSBC and Société Générale. The groups traded the government bonds as security "tokens" and settled them with cryptocurrencies supplied by the central bank.

They started to study how a central bank's currency could be used in day-to-day activities such as issuing new bonds, using them in repurchase agreements, as well as paying coupons and redeeming agreements, if it can be useful or not.

Isabelle Delorme, deputy chief executive of Euroclear France, said

“*We have together successfully been able to measure the inherent benefits of this technology, concluding that the central bank digital currencies can settle central bank money safely and securely*”.
More or less, during the experiment were run successfully circa 500 instructions in both primary and secondary markets.

(Stringer Olivia, *Bitcoin price: Crypto-fund assets explode to all-time high as first-ever ETF launched*, 2021)

At the end of October 2021, the CEO of Binance, one of the largest crypto exchanges in the world, announced that he wanted to start building a blockchain and crypto ecosystem in Europe from France. The "Objective Moon" project, worth over 100 million euros, sees the collaboration with the local financial technology association France FinTech, which will help Binance communicate and work with the local fintech sector.

The goal of this project will be to create a Binance hub in France, seeking to bring new jobs to positions not yet present in Europe.

This initiative is yet another demonstration of the opening of the French state to the world of cryptocurrencies.

(Erhan Kahraman, *Cointelegraph*, 2021)

Japan

Japan has been the first country which tried to regulate cryptocurrency in March 2016 defining virtual coins and their exchanges. According to it, if an individual wishes to engage in a virtual currency exchange service, he must obtain a registration with the prime minister, by applying containing the details concerning the digital currencies he owns and all the information regarding the exchange services he wishes to carry out.

In April 2017, Japan's Financial Service Agency decided to give authorization to use digital currencies as a method of payment. **Consequently, crypto gains the same value of physical money.**

Despite all these laws in favor of cryptocurrency exchange services, physical money still has dominance in Japan; indeed, in January 2018, Yuko Kawai[2], said in an interview that Japan is not yet at the stage at which the BOJ could consider issuing a central bank digital currency, since there is no demand. Furthermore, Yuko Kawai declared in Japan "*do we really need a digital currency in the nation where cashless living isn't making much progress*?", which clarifies why BOJ is not planning to mint its own virtual currency. In addition, a cyber-attack to one of the cryptocurrency exchanges in Japan, Coincheck Inc., brought the FSA to changes its strategy towards virtual monies from enhancing their growth to monitoring them, with the aim of preventing similar attacks in the future. Indeed, on January 26, $500 million were stolen from the Tokyo-based exchange Coincheck, event that undermined Japan's reputation as a "blockchain-friendly" nation. As a result of this heist, the BOJ published a Q&A, which gives an overview of virtual currencies, highlighting the risks the public should be aware of when investing in virtual monies, including the risk of theft, explaining the differences between them and national currency and warning the public, who should do not assume it is a necessarily profitable investment.

[2] Head of the Bank of Japan (BOJ) division

Furthermore, on April 018, the FSA suggested to abandon virtual currencies such as Monero, Dash and Zcash, since, according to the agency, they are the virtual monies favored by criminals and hackers, being them more difficult to track than other digital currencies. Nevertheless, Japan remains one of the less hostile Asian country for what concerns virtual coins.

(Ramirez Elain, Forbes, 2021)

(Adelstein Jack, Forbes, 2021)

India

On august 2021, some American state sources, revealed that Governor of the Reserve Bank of India, is interested in launch a pilot for a new digital rupee.

According to Governor, the main initial decision is about the technology to be used.
The possibilities are:

- **Centralized ledger**: in this case there would be a proprietary database for central bank.
- **Distributed ledger**: in this case there would be a database accessible for multiple entities.

In parallel to the possibility to create a new CBDC, in India government is trying to regulate legislation about cryptocurrencies.

It is not easy to understand the real position of government because they have changed their idea different times.

In March 2021 leaked some information about a possible stop for exchange of bitcoin.
It seems that the reason was precisely the desire to release a proprietary CBFC.

A government commission in 2019 had suggested up to 10 years in prison for people who mine, generate, hold, sell, transfer, dispose of, issue or trade in cryptocurrencies.

Instead, a few months later, the possible turnaround would seem to be functional precisely to the release of the new state cryptocurrency. Updates will surely follow in the coming months. In any case, now, India remains one of the nations with the highest level and investments in bitcoin.

(Kay Chris, *Paytm May Consider Bitcoin Offerings if India Legalizes Crypto,* 2021)

International Monetary Found

In 2014, Christine Lagarde, the managing director of IMF defined Bitcoin as suspicious and stated that they were used for primarily for money laundering.

In 2016, the International Monetary Fund issued a paper, in which the authority deeply analized the argument, trying to make comparisons with other fiat currencies and investigating all the technologies behind cryptocurrencies.

After this first part, they have analyzed all the risks related to virtual currencies, to understand all the possible consequences that a virtual coin could cause on financial and monetary stability.

In the end, given the fact that virtual currencies were at their early stage, they did not pose relevant risks to neither monetary nor financial stability.

Finally, the authority concluded analyzed benefits about a possible regulation of digital coins.

To reduce fraud, tax evasions and other illicit activities associated with the use of such monies, what’s more, Lagarde asserted authorities should hurry up and enact some procedures to handle cryptocurrencies, pointing out that “*Not so long ago, some experts argued that personal computers would never be adopted, and that tablets would only be used as expensive coffee trays. So I think it may not be wise to dismiss virtual currencies*”.

Christine Lagarde also called for an implementation of more severe measures in order to reduce illicit activities using the same technology enabling such actions; indeed, she proposed to use the same distributed ledger technology to increase the speed of information sharing between market participants and regulation institutions, to create “*registries of standard, verified, customer information along with digital signatures.*", also with the help of other technologies, to enhance the soundness of digital market for customers.

In June 2018, in the IMF f&d magazine, Dong He[3] pursued a further analysis of cryptocurrencies, highlighting the lack of three principal functions that a reliable monetary system must be able to achieve:

- the ability to function as a lender of last resort
- the protection against the risk of deflation
- the capability to respond to a shock in a flexible manner.

At the same time, he also pointed out that if in the future virtual coins’ framework got stronger, central bank monetary policy would not be able anymore to successfully affect the monetary system; to this end, he suggested Central Banks should struggle to improve national currencies stability, for what concern its unit of account function, together with maintaining public trust in fiat monies and actively monitoring the development of cryptocurrencies, taking into consideration the possibility to issue their own digital currency, to “*stay in the game in a digital sharing, and decentralized service economy*”.

(Tucker Jeffrey A., *IMF Head Foresees the End of Banking and the Triumph of Cryptocurrency*, 2017)

[3] Deputy director of the International Monetary Fund’s Monetary and Capital Markets Department

European Union

Over the past year, the EU has tried to propose a framework for regulating cryptocurrencies.

In the second half of September 2021, the European Council declared that the Parliament Council could start negotiations to ensure that the new framework proposed is adopted into law.

Named as MiCA, this framework broadly captures cryptocurrencies such as bitcoin and promises to permit cryptocurrency businesses to easily expand across the EU by facilitating a passport license.

The MiCA's goal is to create a regulatory framework for the crypto-asset market that supports innovation and harnesses the potential of crypto-assets in a way that preserves financial stability and protects investors.

The package that has been discussed contains a digital finance strategy, proposals on crypto-asset markets (MiCA) and digital operational resilience (DORA) as well as a proposal on distributed ledger technology (DLT). This package is important to fill a gap in existing EU legislation by ensuring that the current legal framework does not hinder the use of new digital financial instruments while at the same time ensuring that such new technologies and products fall within the scope of the application of financial regulations and agreements on the management of operational risks of companies operating in the EU. In doing so, the package aims to support innovation and the take-up of new financial technologies, while providing an adequate level of consumer and investor protection.

The Council and the European Parliament will now start negotiations on the proposals that, once met with an interim political agreement between their respective negotiators, both institutions will formally adopt the agreements.

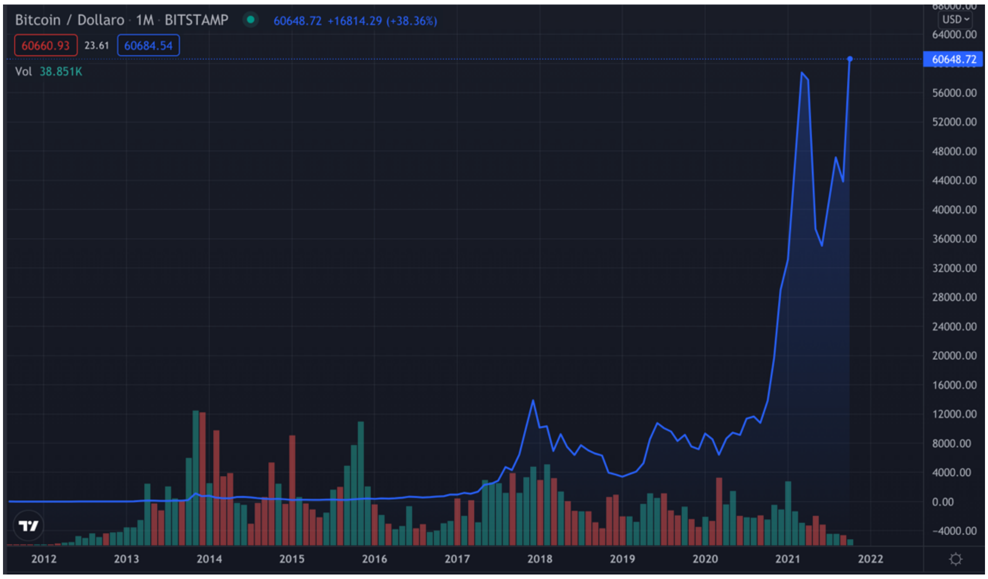
(Handagama Sandali, *CoinDesk*, Nov 2021)

CHAPTER 5
Bitcoin: a financial asset

One of the big questions in finance is whether to buy a certain asset, be it a stock a bond or another financial instrument, and add the asset to an investment portfolio. Optimally an investment portfolio would generate high returns for a low as possible risk, in good but also in bad times.

One of the best solutions to reduce risk is to diversify.

During bad times, a special kind of assets which perform well are hedges and safe heavens, necessary to save the situation. The asset that is considered a safe haven par excellence is gold, capable of providing security both in times of crisis and uncertainty. After 2008 the growth of bitcoin has been incredibly important arriving in these days (October 2021) at a value of 60.584,00 $.



In 2014, Angela Rogojanu[4] and Liana Badea[5] said "*Bitcoin is like gold, but in a virtual environment*"and one year later, Dyhrberg[6] compared

[4] Professor at ASE Bucharest
[5] PHD Economic doctrines and communication, Bucarest
[6] Researcher at University College of Dublin

it to US Dollar in her work "*Bitcoin, gold and the dollar – A GARCH volatility analysis*".
So, is Bitcoin a profitable investment? Does it offer diversification advantages for a global market portfolio? Is it a safe heaven? These are the fundamental questions to understand if Bitcoin is a profitable investment or just a speculative asset.
Defining **hedge** as an asset that is negatively correlated (uncorrelated) with another asset or portfolio on average, **safe haven** as an asset that is negatively correlated (uncorrelated) with another asset or portfolio in certain periods only and a **diversifier** is an asset that has a weak positive correlation with another asset on average, this analysis starts to compare Bitcoin with gold.

(Rogojanu, Badea, *The issue of competing currencies. Case study – Bitcoin*, 2014)

Bitcoin VS Gold VS Dollar

In 2016, Dyhrberg (from *Bitcoin, gold and the dollar – A GARCH volatility analysis, Dyhrberg 2016)* said that both bitcoin and gold derive most of their value from the fact that they are scarce and costly to extract. Neither of them has a nationality or is controlled by a government. "Both assets are 'mined' by several independent operators and companies. Gold was used as a medium of exchange during the gold standard but was abandoned due to liquidity problems. Similar problems might occur for bitcoin if the user base expands further. However, on certain points gold and bitcoin are different. **Gold** is primarily used for its store of value abilities and for its negative correlation with the American dollar which makes it useful for hedging. Such abilities are not certain for bitcoin but will be investigated".
At the same time, Whelan[7] compared bitcoin with dollar because of their limited intrinsic value and by the fact they are used as medium of exchange, but considering an important difference: dollar is managed by government, bitcoin doesn't.
The analysis made in order to answer to the previous questions involve GARCH framework, useful to identify elements by which

[7] Managing director at Digital assets

bitcoin in sensitive and analyzing the correlation between dollar, gold, and bitcoin involving variance.

According to figure 18, it is represented that bitcoin has a trend similar to other financial assets because its price change because of certain shocks, passing by positive and negative time trend.

(Dyhrberg Anne Haubo, *Bitcoin, gold and the dollar – A GARCH volatility analysis*, 2015)

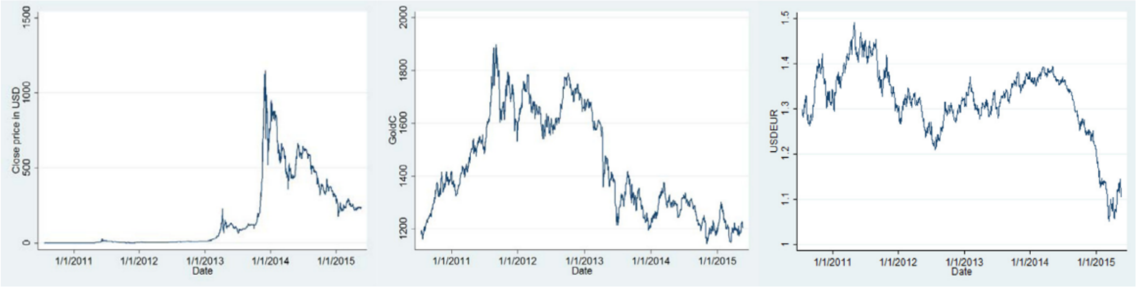


Figure 18- The levels of the bitcoin price, the gold bullion rate and the dollar-euro exchange rate from July 19th 2010 to May 22nd 2015

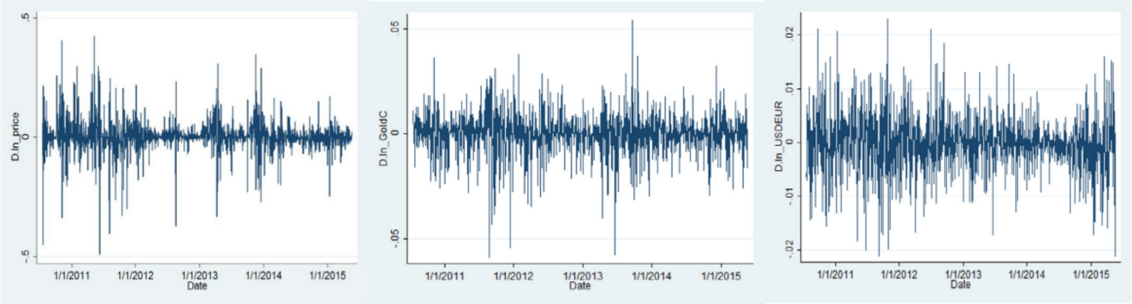


Figure 19-The first differences of the logged bitcoin price, gold bullion rate and dollar-euro exchange rate from July 19th 2010 to May 22nd 2015

GARCH framework

GARCH framework, acronym of **Generalized Autoregressive Conditional Heteroskedasticity** was developed by Robert F.Engle in 2003 and describes an approach to estimate volatility in financial markets. This model led him to win Nobel Memorial Prize for Economics.
The general process for a GARCH model involves three steps. The first is to estimate a best-fitting autoregressive model. The second is to compute autocorrelations of the error term. The third step is to test for significance.
The analysis involve two different types of GARCH model:

- GARCH model with explanatory variables
- GARCH model which investigates if the return of bitcoin is asymmetrically affected by leverage effect (exponential).

(Investopedia, *Generalized AutoRegressive Conditional Heteroskedasticity (GARCH)*, 2021)

The first is identified by these two equations:

$$\begin{aligned}\Delta lnprice_t = {} & \beta_0 + \beta_1 lnprice_{t-1} + \beta_2 lnprice_{t-2} + \beta_3 Fed_{t-1} \\ & + \beta_4 USDEUR_{t-1} + \beta_5 USDGBP_{t-1} + \beta_6 FTSE_{t-1} \\ & + \beta_7 Gold\ Future_{t-1} + \beta_8 GoldCash_{t-1} + \varepsilon_t\end{aligned}$$

$$\begin{aligned}\sigma_t^2 = {} & \exp(\lambda_0 + \lambda_1 Fed_{t-1} + \lambda_2 USDEUR_{t-1} + \lambda_3 USDGBP_{t-1} + \lambda_4 FTSE_{t-1} \\ & + \lambda_5 Gold\ Future_{t-1} + \lambda_6 GoldCash_{t-1}) + \alpha\varepsilon_{t-1}^2 + \beta_{\sigma_{t-1}^2}\end{aligned}$$

The second is identified by:

$$\begin{aligned}\Delta lnprice_t = {} & \beta_0 + \beta_1 lnprice_{t-1} + \beta_2 Fed_{t-1} + \beta_3 USDEUR_{t-1} \\ & + \beta_4 USDGBP_{t-1} + \beta_5 FTSE_{t-1} + \beta_6 Gold\ Future_{t-1} \\ & + \beta_7 GoldCash_{t-1} + \varepsilon_t\end{aligned}$$

$$\begin{aligned}\ln(\sigma_t^2) = {} & (\lambda_0 + \lambda_1 Fed_{t-1} + \lambda_2 USDEUR_{t-1} + \lambda_3 USDGBP_{t-1} + \lambda_4 FTSE_{t-1} \\ & + \lambda_5 Gold\ Future_{t-1} + \lambda_6 GoldCash_{t-1}) + \alpha\left(\frac{\varepsilon_{t-1}}{\sigma_{t-1}}\right) \\ & + \gamma(\left|\frac{\varepsilon_{t-1}}{\sigma_{t-1}}\right| - \sqrt{\frac{2}{\pi}} + \delta \ln(\sigma_{t-1}^2))\end{aligned}$$

In the following table are reported results for GARCH (1,1):

Table 1-Volatility persistence of the return on bitcoin with explanatory variables with dependent variable return on bitcoin

VARIABLES	MEAN EQ.	VARIANCE EQ.
Federal funds rate (t-1)	0.0982***	-6.801***
	(0.0359)	(1.127)
USD-EUR exch. Rate (t-1)	0.0502***	9.828***
	(0.0190)	(0.954)
USD-GBP exch. Rate (t-1)	-0.0790***	-10.04***
	(0.0307)	(1.584)
FTSE index (t-1)	9.25e-06**	-0.000832
	(3.74e-06)	(0.000158)
Golds futures rate (t-1)	0.000176	-0.0191*
	(0.000177)	(0.0106)
Gold cash rate (t-1)	-0.000161	0.0163
	(0.000178)	(0.0107)
L.ar	0.0827***	
	(0.0307)	
L2.ar	-0.0222	
	(0.0269)	
L.arch α		0.327***
		(0.0214)
L.garch β		0.636***
		(0.0159)
Constant	-0.0291	4.920***
	(0.0488)	(1.620)
Observations	1768	1768

Data in parentheses are standard errors; ***=p<0.01; **=p<0.05; *=p<0.1.

The variance equation shows that, like gold, bitcoin has low convergence to the long-run equilibrium, volatility clustering and high volatility.

From the analysis is evidenced that the return on bitcoin is more affected by the demand for bitcoin as a medium of exchange and less by temporary shocks to the price which indicate similarities to a currency. In 2008, Hammoudeh and Yuan[8] found that gold was much more affected by the demand for jewelry and recycling as it is a precious metal and not an industrial metal and is less influenced by short term shocks.

“With the same yield volatility and the most influential type of shock, it seems that bitcoin and gold have important similarities. This is also confirmed by the observation of the explanatory variables. The coefficient on the federal funds rate suggests that when it rises, and the US dollar appreciates, there will be an increase in imports, with a probable increase in online purchases.

Since bitcoin is a particularly suitable currency for international online purchases, this will lead to an increase in demand, and a consequent increase in interest rates. The advantage of this cryptocurrency as a medium of exchange is therefore evident.
Another factor is highlighted by the FTSEI coefficient: the stock market would make investors more risk-prone and therefore more likely to invest in assets such as bitcoin, in the event of a positive shock.
This is also evident from the variance equation: here an abrupt positive change in volatility would lead to a reduction in the yields of bitcoin, demonstrating its safety in situations of this type. It would seem the umpteenth confirmation of the excellent risk management capacity of bitcoin.

Ultimately, the results obtained from this analysis would demonstrate that bitcoin's yields behave like an exchange rate in that it is extremely sensitive to the federal funds rate and the characteristics of the medium of exchange.
At the same time, it has also been shown that there are important similarities with gold. In conclusion, bitcoin could be somewhere between a currency and a commodity.
Exponential GARCH model instead, studies effects related to how bitcoin reacts to bad or good news.

[8] Professors of Drexel University

The main results are reported in this table:

Table 2- Results from second method of GARCH

VARIABLES	MEAN EQ.	VARIANCE EQ.
Federal funds rate (t-1)	0.0988***	-0.978***
	(0.0338)	(0.230)
USD-EUR exch. Rate (t-1)	0.0505***	1.813***
	(0.0181)	(0.191)
USD-GBP exch. Rate (t-1)	-0.0844***	-1.914***
	(0.0300)	(0.287)
FTSE index (t-1)	9.21e-06**	-0.000120***
	(3.66e-06)	(2.88e-05)
Golds futures rate (t-1)	0.000160	-0.00727***
	(0.000162)	(0.00209)
Gold cash rate (t-1)	-0.000143	0.00685***
	(0.000163)	(0.00211)
L.ar	0.100***	
	(0.0297)	
L.earch α		0.00776
		(0.0154)
L.earch_a γ		0.545***
		(0.0252)
L.egarch		0.834***
		(0.00982)
Constant	-0.0233	1.203***
	(0.0442)	(0.310)
Observations	1768	1768

Data in parentheses are standard errors; ***=p<0.01; **=p<0.05; *=p<0.1.

From the predominance of the gamma coefficient of the proposed equation, it is evident that, like gold, good and bad news also have a symmetrical impact on its volatility in bitcoin.
Consequently, bitcoin and gold could both be hedging market risks, because both have a symmetrical reaction to outside news, while other assets don't. Furthermore, since there is no leverage effect, bitcoin is the best solution for a particularly risk-averse investor.

Summarizing the results of the two analyzes, bitcoin proves to be like the dollar and gold. In fact, this acts as a currency because it reacts as a medium of exchange without being regulated, therefore in any case different from a currency evaluated. Compared to gold, bitcoin has a similar behavior in the event of good and bad news

As stated by Dyhrberg, "*The overall result suggests that bitcoin is somewhere between a currency and a commodity due to its decentralized nature and limited market size. However, this does not mean that bitcoin is less useful than current assets on the market. Conversely, this classification suggests that individuals in portfolio management and market analysis can gain a more detailed view of the market by including bitcoin which allows them to make more informed decisions and get another hedging instrument. Additionally, bitcoin can be used as a tool for risk-averse investors in anticipation of bad news. Therefore, the position of bitcoin in the market would be between gold and the dollar on a scale with one extreme that is pure store of value advantage and the other extreme is a pure means of exchange advantage.*
This result suggests that bitcoin can provide some advantages of both commodities and currencies in financial markets and thus be a useful tool for portfolio management, risk analysis and market sentiment analysis. "

(Dyhrberg Anne Haubo, *Bitcoin, gold and the dollar – A GARCH volatility analysis*, 2015)

Fundamental analysis

Different variables, economic or financial, are fundamental to evaluate the value of a security

Usually, analyzing the crypto, the main aspects is the technology on which bitcoin are based, trying to understand how its scaling challenges might affect the digital currency's value.
In fact, one of the causes for a reduction of demand, and so of price, is that digital currency's transactions grow costly and time-consuming on account of block size limitations.

Fundamental analysis is usually used to evaluate different asset classes like equities, fiat currencies and so on, but, as it is easy to understand, to evaluate bitcoin is complicated.
However, even though bitcoin has been described as a new asset class, the same rules that apply to fiat currencies also apply to cryptocurrencies, said Tim Enneking, chairman of Crypto Asset Management. "*All the laws of economics apply – in full – to cryptocurrencies*," he said.
As a result, he emphasized that the starting point for all fundamental analysis should be the supply and demand that drives prices.

Demand has a key role because it is affected by several variables affect bitcoin demand, like user adoption, transaction activity and trading. The importance of user adoption is crucial to a cryptocurrency's long-term viability. As for what drives user adoption, the analysts said money can have many uses. At its most basic level, money is a store of value, a medium of exchange and a unit of account.
Outside of small circles, bitcoin has never really been used as a unit of account, said Enneking.

But bitcoin in the last years has gained significant traction as a medium of exchange, also considering that hundreds of companies, including eBay and PayPal, have agreed to accept the digital currency since its inception in 2009.

In addition, the number of confirmed transactions per day has generally followed an upward trend, according to data from Blockchain. Transactions started surging in early 2012, rising from more than 7,000 per day at the start of April 2012 to more than 300,000 per day now.
Arthur Hayes, co-founder and CEO of leveraged bitcoin trading platform BitMEX, said that the extent to which bitcoin is perceived as a store of value is a major driver of the digital currency's price.

At the same time, also supply has a key role.
The maximum number of bitcoin which can be on the market has been set by Nakamoto to 21 million and nowadays there are more than 19 million. As it is easily to say, this aspect is completely in contrast with the fiat world, where banks can potentially print an infinite number of cash

The last aspect that has to be considered: major events.
There have been a large quantity of events which have caused important changes in bitcoin price.

(Bitscoins, 2017)
(Gurguc Zeynep, Knottenbelt William, *Cryptocurrencies: Overcoming barriers to trust and adoption*, n.d)

Bitcoin price

In the last years, the bitcoin's price trend has been very swinging also due to continuous problems and attempts at fraud fomented by the lack of regulation.

There have been periods in which price variations has overcome even their usually volatile swings, resulting in massive price bubbles.

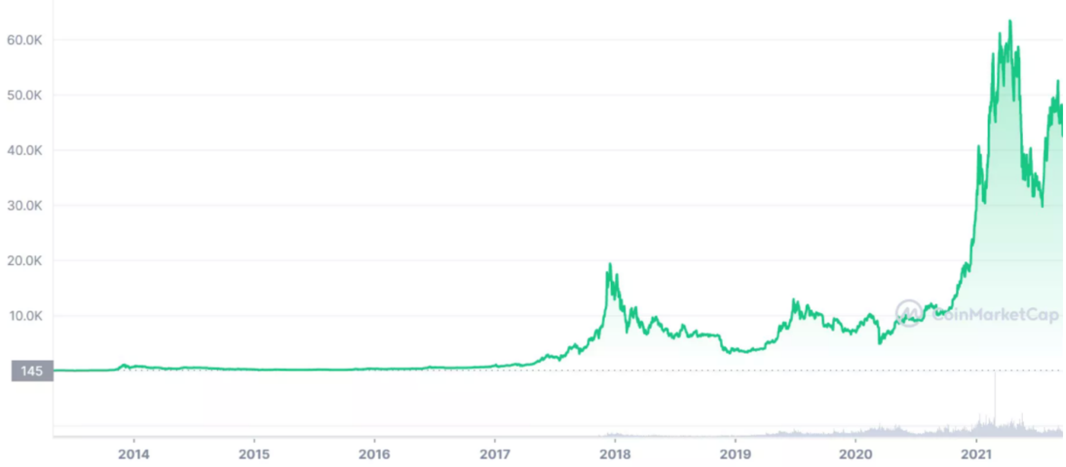


Figure 20- Bitcoin price from 2013 to 2021

- On April 2011 bitcoin price was circa around 1$. After less than 3 months it went to 32$ (+3200%) and lowering again in November 2011 (arriving at a value of 2$).
- In 2013 there were two bubbles. The first was in April 2013 when the price passed from 13.4$ to 220$; the second was at the end of the year, passing from 123.2$ to 1.156,1$ and lowering again to 760$ three days later. In 2015 price touched again $315.
- In 2017 the price was around $1000 but after a brief decline, from March to December it passed from 975$ to $20.089. This was a turning point for Governments who started to think about a way to compete with bitcoin (CBDC).
- In 2020, due to pandemic, bitcoin passed from $7.200 to $18.353, arriving to $60.000 on March 2021 and to $66.974 on October 2021.

In general, it is possible to understand that bitcoin price is following the Gartner Hype Cycle, due to hype about its potential and troughs of disillusionment that resulted in crashes.
This cycle is characterized by 5 phases useful to describe all the life of a new technology:

1. Technology trigger: start of a new technology which is still immature.
2. Peak of inflated expectations: marketing is useful to launch the new technology. Here a lot of company reach important goal but at the same time there are a lot of failed.
3. Trough of disillusionment: lowering of interest because of lack of reaching of expected results.
4. Slope of enlightenment: technologies which resist during phase 3 spread and people starts to become conscious about the potential of new technology.
5. Plateau of productivity: new technology achieves a solid position on the market.

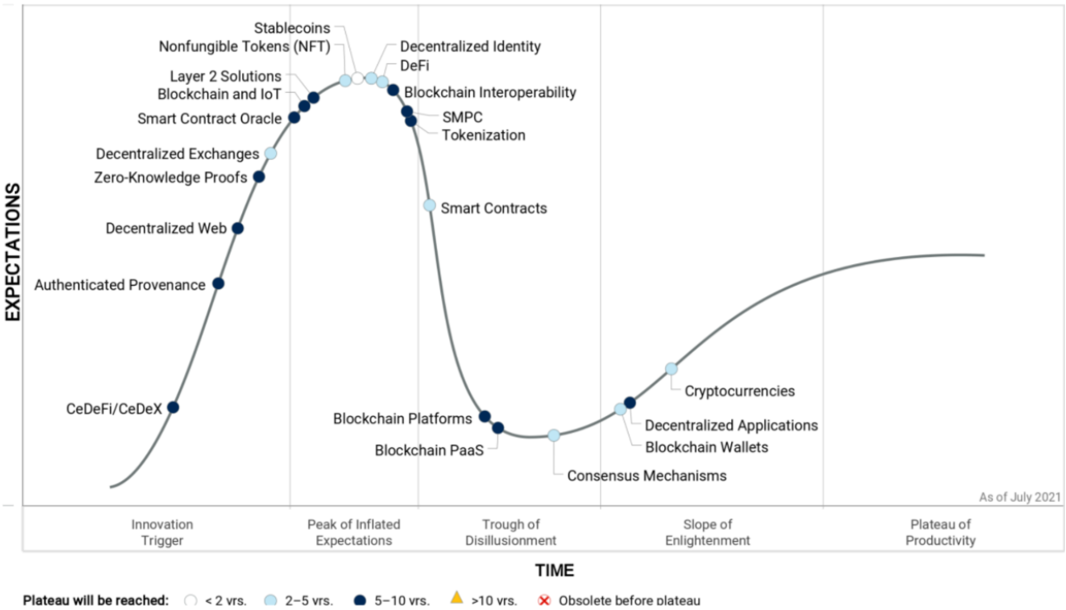


Figure 21- Gartner Hype Cycle

In this cycle speculative bubbles are fundamental to provide funding and drive a new technology’s evolution. And so, each swell and ebb in Bitcoin's price has shone a spotlight on the shortcomings of its ecosystem and provided a fresh infusion of investor funds to develop its infrastructure.

Previously the analysis of Bitcoin's price showed that its price was a function of its speed or its use as a currency for daily transactions and trading. But cryptocurrency trading volumes are a fraction of their traditional counterparts, and Bitcoin has never taken off as a daily medium of transaction.

At the beginning of its life, when the liquidity in market was very low and there were very few investors, there were wide price swings when investors booked profits or when an adverse industry development was reported. Rise and fall of cryptocurrency exchanges also influenced bitcoin’s price trajectory.
The other important factor affecting Bitcoin's price in its early days was traction with mainstream online retailers: Its price crossed the $1,000 threshold in January 2014 after online retailer Overstock announced that it would begin accepting Bitcoin for purchases.

When mining operations began to take hold, the price of Bitcoin began to follow its marginal cost of production, largely due to the cost of electricity needed to run mining equipment. As the Bitcoin network grew, so too did its mining difficulty, requiring ever-larger amounts of energy.

Starting from 2017, reaching a wide number of people interested, its price has started to change frequently due to each regulatory pronouncement, whatever it was positive or negative.

Another important factor is the growing interest not only for retail investors, but also for institutional and, as a consequence, this has led to a large inflation of liquidity in the system and to a reduction of volatility.
During pandemic of 2020, there was an important rally after important economists has talked about the possibility to transform bitcoin in a store of value to hedge against inflation from increased government spending during the pandemic itself.

Another important catalyzer for bitcoin's price increase are halving events, particular moment in which there is a reduction of bitcoin available in the market due to a change in the algorithm which generally lead to a reduction of miners.

Ultimately, economic instability is another indicator of price changes for Bitcoin. Since the beginning, the cryptocurrency has positioned itself as a supranational hedge against local economic instability and government-controlled fiat currency. According to reports, there is a period of increased economic activity on the Bitcoin blockchain after an economy encounters roadblocks due to government policy. Countries like Venezuela, which have experienced an incredibly high inflation, have seen the enormity of the use of Bitcoin as a means of transaction and storage of wealth. This has led analysts to believe that cryptocurrency price hikes and global economic turmoil are linked.

(Edwards John, *Bitcoin's Price History*, 2021)

Future predictions

Predictions for the future value of Bitcoin vary based on who makes the estimate. According to Jeremy Liew, a partner at Lightspeed Venture Partners, Bitcoin could reach $500,000 per coin by 2030. According to the June 2020 Crypto Research Report, the cryptocurrency could go over $397,000 by 2030. Yet others predict that Bitcoin is just a bubble and they are worthless, predicting a very low value in a decade.

Thesis against Bitcoin

Nouriel Roubini, professor at NYU is one of the most famous economists against bitcoin.
In one of his interviews he said: "*Gold is used in industry, in the jewelry market, and historically has been recognized as a stable store of value against various risks, which include inflation, devaluation of currencies, financial crises, and political and geopolitical risks*", underlying the idea that defining Bitcoin as digital gold, is a serious mistake.

Instead, "*Bitcoin and other cryptocurrencies do not generate income or have a utility, which means that there is no way to understand their fundamental value*".

Nowadays it is particularly difficult to define how overvalued this is because "*we can determine the fundamental value of these cryptocurrencies*". According to him, the correct definition is "bubble" and the dizzying growth of Bitcoin cannot be explained by the expectation of higher inflation in the future.
"*While the price of gold and other inflation hedges have reflected these changes in a limited way, the price of Bitcoin has risen more than tenfold, from a low of $ 5,000 to over $ 60,000 in a year. You cannot explain such a thing with the fear of a devaluation of currencies, because if there was such a strong concern, gold and other assets such as TIPS (US inflation-indexed government bonds) would have reported a stronger rally than actually observed*".

For Roubini, the inflation risk cannot explain the boom in cryptocurrencies: "*There is something else that must be considered*".

"*The supply of Bitcoin remains controlled, but scarcity is not enough to make a particular product valuable*", Roubini later argued. which has even come to question the decentralized nature of Bitcoin itself.

This coin was born with the declared purpose of guaranteeing safe transactions without intermediaries between the parties. "*99% of crypto transactions take place on centralized platforms*," said the economist, "*the reality is that the crypto ecosystem is not decentralized. An oligopoly of miners essentially controls 70-80% of Bitcoin and Ether mining. These miners are in places like China, Russia, and Belarus, which are strategic rivals of the United States and have a different legal system. Therefore, the US National Security Council is starting to worry about the risks this could pose to the US*".

At the beginning of April 2021, in USA, the largest part of professional investors of Bank of America thought that bitcoin was a bubble.
On the other hand, a small part (15% circa) saw bitcoin as speculative asset.
After the exponential increase in price of February 2021, bitcoin has become the most crowded assets for volume of trades.

Another important exponent of thesis against Bitcoin is Alan Greenspan, the former chairman of Federal reserve. During an interview for Bloomberg Television, he explained that currencies need to be backed by something in order to work properly, bringing as example the gold standard period, during which monies had a precise and widely known intrinsic value. He also added that even paper currencies are backed by the trust of the issuer, claiming he does not understand if Bitcoin has some kind of backing and that "*You have to really stretch your imagination to infer what the intrinsic value of bitcoin is. I haven't been able to do it. Maybe somebody else can. [...] you asked me is this a bubble in bitcoin. Yeah, it's a bubble*".
Following the statement of Adam Smith "money can serve no purpose other than purchasing goods", Paul Krugman, an economist and professor at Princeton university, as well as Nobel-

prize winner in 2008, tried to assess Bitcoin's role as store of value and medium of exchange and asserted that Bitcoin

CNBC has tried to propose a solution to help people understand the value of Bitcoin: originally conceived by Tom Lee, co-founder of Fundstrat Global Advisors and former chief equity strategist at J.P. Morgan, the method consists in treating it as a digital business (i.e. Netflix, Google or Amazon), since almost everyone is able to perceive the value of such companies. Tom Lee tried to propose to system to understand Bitcoin: the first is based on the theory that Bitcoin will partially replace gold at some point in the future and according to his calculations, the cryptocurrency would replace 5% of gold demand after five years, which would make one Bitcoin worth more than $20.000; the second hypothesis relied on Metcalfe's law, which states the value of a network depends on the number of people using the network itself . CNBC also include Fundstat's observation on the application of the law to the Bitcoin system, which reached the conclusion that roughly 90% of the digital money price fluctuations are explained by the number of users of the network.

(Ossinger, Roubini says bitcoin is the biggest bubble in human history, 2018)
(Cox Jeff, Bitcoin is a bubble, 2021)

Chapter 6

Conclusions

In the current historical period, characterized by a strong economic crisis and discontent with the banking system, cryptocurrencies are proposing themselves as an alternative monetary system that intends to upset the economic, political, and even social balances.

We have seen how Bitcoin, born in 2008 from the mind of one or more unknown people, was not a creation for its own sake, but rather a way to shed light on the problems and discontent related to the management of money by central banks. And to all the central control bodies, guilty of having poisoned the global economy through the manipulation of the monetary supply.

Through a peer-to-peer transaction system, regulated by an IT protocol, Bitcoin presents itself, simultaneously, as a currency-unit of account and a payment system independent of any centralized control, placing the entire community of users.

The fact that states have begun to move in the field of crypto allows us to understand that the fear that these cryptocurrencies could gain a greater footing in society is well founded.
However, the scenario opened by Bitcoin and other virtual currencies generates opportunities and risks at the same time. The documentation regarding cryptocurrencies is still very sparse.

Nowadays, investing in this field still involves many risks as the market is particularly volatile and for many, an investment of this type has nothing different from gambling.

To date, it is still early to define the future for Bitcoin, for altcoins and for CBDCs. It is clear that if the former were to take hold as a medium of exchange, there would be a huge change for the entire economic system, where banks would assume a small role. On the contrary, in the event of a CBDC issue, the change would certainly be important and revolutionary, but the control of the banks would still remain constant.

As for the Blockchain, given that large companies have decided to test its applications in contexts separate from that of cryptocurrencies, it could survive the class of assets that have fostered its notoriety. Of course, the competitive nature of pre-existing markets would influence their diffusion, as the blockchain is more likely to justify its adoption in contexts where the cost of verification is currently high due to regulation or the infrastructure. Government choices in different jurisdictions will be another key factor defining where we might first see a state-sponsored cryptocurrency, a less expensive payment system running on a distributed ledger or experimenting with more complex forms of resolution and reconciliation.

It is therefore still too early to decide whether Satoshi Nakamoto's legacy will change the payment system as social networks have changed the way people connect, or if it will end in a stalemate, stifled by regulation and loss, of trust or, finally, if it will survive as a niche reality, too small to represent a serious turning point for society but too fascinating to disappear entirely.

SOURCES

Cameron Dark, David Emery, June Ma and Clare Noone *Cryptocurrency: Ten Years On*, 2018
https://www.rba.gov.au/publications/bulletin/2019/jun/cryptocurrency-ten-years-on.html?utm_source=rbanews&utm_medium=email&utm_content=cryptocurrency-ten-years-on&utm_campaign=bulletin-2019-jun

Luke Conway, *Blockchain explained*, 2021
https://www.investopedia.com/terms/b/blockchain.asp

BitcoinNews, 2018
https://thebitcoinnews.com/proof-of-work-explained/

Tether, 2021
https://tether.to

Why Cardano, 2020
https://why.cardano.org/en/introduction/motivation/

Bech Morten, Garratt Rodney, *Central Bank Cryptocurrencies*, 2017
https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf

Enger Walter, Fung Ben S.C, *Central Bank Digital Currency: Motivations and implications*, 2017
https://www.bankofcanada.ca/wp
content/uploads/2017/11/sdp2017-16.pdf

Bank of England, 2020
https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=encriptovahash=A71920A2FFB6511E43F787019C549262049CC7A8#page=49

Shobhit Seth, *Central Bank Digital Currency (CBDC)*, 2021 https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp#:~:text=A%20CBDC%20is%20issued%20and%20regulated%20by%20a,currency,%20they%20may%20erode%20the%20privacy%20of%20citizens.

Stephen Cecchetti, Kim Schoenholtz, *Central bank digital currency: The battle for the soul of the financial system*, 2021 https://voxeu.org/article/central-bank-digital-currency-battle-soul-financial-system

Yuan Liu, Shuai Sun, Zhengpeng Ai, Shuangfeng Zhang, Zelei Liu, Han Yu, *FedCoin: A Peer-to-Peer Payment System for Federated Learning*, 2020 https://arxiv.org/pdf/2002.11711.pdf

Norton Rose Fulbright, *Venezuela issues general legal framework on cryptoassets and the "petro" cryptocurrency*, 2018 https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/la---venezuela-issues-general-legal-framework-on-cryptoassets-and-the-petro-cryptocurrency.pdf?la=en&revision=49bc066c-090d-46ce-b9a9-2b502b0c1755

Frankenfield Jake, *Petro Gold*, 2021 https://www.investopedia.com/terms/p/petro-gold.asp

Stringer Olivia, *Bitcoin price: Crypto-fund assets explode to all-time high as first-ever ETF launched*, 2021 https://www.express.co.uk/finance/city/1508002/bitcoin-price-live-cryptocurrency-news-etf-launched-assets-invest-latest

Tucker Jeffrey A., *IMF Head Foresees the End of Banking and the Triumph of Cryptocurrency*, 2017 https://fee.org/articles/imf-head-predicts-the-end-of-banking-and-the-triumph-of-cryptocurrency/

Dyhrberg Anne Haubo, *Bitcoin, gold and the dollar – A GARCH volatility analysis*, 2015
http://www.stat.ucla.edu/~frederic/415/F18/bitcoin.pdf

Investopedia, *Generalized AutoRegressive Conditional Heteroskedasticity (GARCH)*, 2021
https://www.investopedia.com/terms/g/garch.asp

Bitscoins, 2017
https://www.bitscoins.net/what-bitcoin-traders-should-know-about-fundamental-analysis/

Gurguc Zeynep, Knottenbelt William, *Cryptocurrencies: Overcoming barriers to trust and adoption*, n.d
https://www.imperial.ac.uk/media/imperial-college/research-centres-and-groups/ic3re/CRYPTOCURRENCIES--OVERCOMING-BARRIERS-TO-TRUST-AND-ADOPTION.pdf

Edwards John, *Bitcoin's Price History*, 2021
https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp#citation-13

Bedini Davide, *La Cina dal blocco del bitcoin al lancio dell'eYuan: cosa c'è dietro e gli sviluppi futuri*, 2021
https://www.agendadigitale.eu/cittadinanza-digitale/la-cina-dal-blocco-del-bitcoin-al-lancio-delleyuan-cosa-ce-dietro-e-gli-sviluppi-futuri/

Scozzari Carlotta, *La Stampa*, 2021

https://www.lastampa.it/economia/2021/09/07/news/el-salvador-e-il-primo-paese-dove-il-bitcoin-e-moneta-legale-il-presidente-bukele-ne-ha-comprati-per-21-milioni-di-dollari-1.40677014

Handagama Sandali, *CoinDesk*, Nov 2021
https://www.coindesk.com/policy/2021/11/24/european-council-takes-one-step-closer-to-ratifying-landmark-crypto-regulation/

Binance
https://www.binance.com/it/buy-BNB

Erhan Kahraman, *Cointelegraph*, 2021
https://it.cointelegraph.com/news/binance-to-spend-115m-in-france-to-develop-european-crypto-ecosystem

Ethereum
https://ethereum.org/en/

Ramirez Elain, Forbes, 2021

https://www.forbes.com/sites/elaineramirez/2018/05/10/is-japan-still-asias-crypto-haven-after-coincheck-heist-probably-not/?sh=3ce7c4f3258e

Adelstein Jack, Forbes, 2021
https://www.forbes.com/sites/adelsteinjake/2018/04/30/japans-financial-regulator-is-pushing-crypto-exchanges-to-drop-altcoins-favored-by-criminals/?sh=6948ff2b1b8a

Kay Chris, *Paytm May Consider Bitcoin Offerings if India Legalizes Crypto*, 2021
https://www.bloomberg.com/news/articles/2021-11-04/paytm-may-consider-bitcoin-offerings-if-india-legalizes-crypto

The issue of competing currencies. Case study – Bitcoin, Rogojanu, Badea (2014)
https://econpapers.repec.org/article/agrjournl/v_3axxi_3ay_3a2014_3ai_3a1(590)_3ap_3a103-114.htm

Metal volatility in presence of oil and interest rate shocks- Hammoudeh, Yuan (2008)
Cameron, Emery, Ma, Noone, *Cryptocurrencies: Ten years on*, 2019

https://www.rba.gov.au/publications/bulletin/2019/jun/cryptocurrency-ten-years-on.html?utm_source=rbanews&utm_medium=email&utm_content=cryptocurrency-ten-years-on&utm_campaign=bulletin-2019-jun

Ossinger, Roubini says bitcoin is the biggest bubble in human history, 2018
https://www.bloomberg.com/news/articles/2018-02-02/roubini-says-bitcoin-is-the-biggest-bubble-in-human-history

Cox Jeff, Bitcoin is a bubble, 2021
https://www.cnbc.com/2021/04/13/bitcoin-is-a-bubble-say-74percent-of-bank-of-america-survey-respondents.html