LUISS

Department
of Business and Management

Course of Blockchain and Cryptocurrencies

Blockchain and Metaverse:
The Present of the Future

Prof. Massimo Bernaschi
SUPERVISOR

246441 Daniele Amantini
CANDIDATE

Academic Year 2021/2022

Table of Contents

INTRODUCTION

Over the last decade, anyone going to a bar or pizzeria with friends will have said the classic phrase, "If I could go back, I would buy Bitcoin." More recently, everyone will have seen a picture of a stylized monkey being sold for millions and thought, "How crazy." Many others will surely have heard or read about Mark Zuckerberg renaming his colossus as "Meta" to give a very early hint of the amazing concept of the metaverse, where time and space are two concepts that take on a different form. Fewer will have heard of, read about, or looked up the blockchain, which is the backbone of cryptocurrencies and NFTs, and to put it mildly, the coal of the "metaverse" locomotive.

The purpose of the present work is to provide some basics on the concepts of Metaverse, Blockchain, NFT, and cryptocurrency, citing practical examples and attempting to shed more light on the positives and negatives sides of each.

THE METAVERSE

In July 2021, Mark Zuckerberg put Facebook's future on the metaverse. After renaming the company "Meta," he promised to invest billions of dollars in building the Metaverse platform. Other companies like Nike are also working on their plans for the Metaverse. The Metaverse is difficult to define. It is usually described as a persistent online 3D universe where people socialize, work, and play in the form of avatars, which are digital representations of their identities. This is possible because multiple virtual spaces are directly connected. Unlike a Zoom chat, these rooms do not disappear when you are done. They are still there and can be used by someone else. Meta and other companies are calling the Metaverse the future iteration of the Internet. A virtual world that parallels our lives in the real world. However, this is not a completely new idea since it has been discussed for decades. Dr. Genevieve Bell, director of the ANU School of Cybernetics in Australia, says that another way to think about the metaverse is that it has always existed in different parts of the world. If we look at different types of online communities, we can say that tastes of metaverse already exist. They just have been called in different ways. Even if the metaverse does not fully exist yet, some platforms contain metaverse-oriented elements. Roblox and Minecraft are two well-known platforms that, for years, have been building virtual worlds with which avatars could interact. Another example is Fortnite, which integrates aspects of virtual, augmented, or mixed reality to provide users with an immersive gaming experience. A distinction needs to be made here. Virtual reality refers to fully digital spaces accessed through hardware such as the VR headset and motion-controlled controllers, in which objects can appear real even if they are not. Augmented reality (AR), on the other hand, is a related but different technology. It brings digital objects into the real world, often without the need for a headset, although it is sometimes used. Some experts see augmented reality as a gateway to broader adoption of the metaverse. Advances in software have given users more realistic experiences, as digitally reproduced reality has a higher degree of fidelity to reality. However, critics say that the technology needs further development to achieve the realism required for the metaverse. The concept of the metaverse generally introduces many other concepts that together can be fundamental to improving its quality, supporting various operations, and enhancing user experiences. Some of the most important concepts that can be defined as building blocks of the metaverse are cryptocurrencies, blockchain, and NFTs.

TRAVIS SCOTT CONCERT

On April 24 at 1 PM Rome time, during the quarantine related to the spreading Covid 19 pandemic, the well-known American rapper Travis Scott gave a live concert. How many people participated? If we do not count all those who followed the concert on Twitch or other streaming platforms, there were about 12 million people. This was possible because the concert did not take place in the classic live mode, which means you stand in line to buy a ticket, you buy a ticket, you spend money on transportation, you get to the concert venue, you wait at the entrance, and finally you find your seat. For the first time in the history of music, Travis Scott performed on a popular gaming platform, Fortnite, giving everyone the opportunity to participate in the event. Connected players were able to wander the map and watch Travis Scott's giant avatar performing with one of his unreleased tracks. The collaboration between the rapper and the Fortnite platform managed to create an unprecedented event that made up for the rapper's physical absence with a very immersive experience. Travis did not sing his songs live. The whole thing was recorded, but the lyrics were so perfectly synchronized with the images that it was almost impossible to tell it was just a recording.

The show was breath taking, not so much because of the concert itself, which lasted just about ten minutes, but because of what it meant. It gave us a taste of the unique potential of the metaverse, where physical locations and temporal spaces become completely distorted, and a new reality is created. Travis Scott's concert could be a true revolution in live concerts and the prelude to a long series of similar events. In the future, events could literally be live, with the artist performing remotely directly on the platform and interacting with fans. There are several artists planning something like this. Ariana Grande, for example, is already planning to perform in a way similar to Travis Scott. This new way of performing will, on the one hand, give artists the opportunity to be followed by more fans at the same time and, on the other hand, give fans the chance to feel closer to their idols and, why not, save a lot of money to participate to an event.

To be fair, there was also an initiative by the well-known DJ Marshmello to recreate a concert experience in Fortnite before Travis Scott. However, this was only a weird avatar of the DJ placed in a context that was not impressive. It was almost a flop. To be clear, Travis' concert did not lay the groundwork for a total replacement of the material and social experience of a concert but rather opened the gates for alternatives to the modes we have all become accustomed to.

THE BLOCKCHAIN

A blockchain is a public and distributed ledger shared among users of a digital network. The main goal of a blockchain is to store information digitally, especially about transactions and legal contracts. Blockchains play a crucial role in the cryptocurrency ecosystem. Without blockchain, there would be no cryptocurrencies. It can be compared to a standard database, but there are actually a few differences that allow blockchain systems to be more effective and instrumental in certain circumstances, such as in a low-trust environment.

One key difference between blockchain and standard databases is that blockchain collects information in blocks. When a block is created, validated, and added to the blockchain, it is linked to the previous block header through its hash value and forms a chain. Each block is also timestamped, giving thus the possibility to see the exact time it has been created and added to the blockchain. Another important difference is immutability. Information in the blockchain can be accessed and read by users, but it cannot be deleted or modified, whereas in a standard database the CRUD capability allows users to edit and possibly delete data. Another important aspect of blockchain is decentralization. Decentralization is essential to avoid the so-called single point of failure, where the collapse of a single part of a system would bring down the entire system. Centralization increases the likelihood that data will be put at risk due to Internet disruptions, power problems, etc. With blockchain, these concerns are eliminated because the data is distributed among multiple users on a network. Each user has a copy of the entire blockchain, making it impossible to lose or corrupt data. This is also essential in avoiding a malicious user from successfully altering a record in the blockchain. Since the other nodes would not be altered, the only solution is to alter the data of all copies of the blockchain distributed across all nodes. This is practically impossible and should prevent malicious users from performing such malicious actions.

Transparency is another feature provided by the blockchain. Due to the decentralized nature of the blockchain, all information about transactions can be accessed and read by all users of a network. How is it possible? Because, as mentioned earlier, users have their own copy of the chain, which is updated as blocks are confirmed and added. This not only provides transparency but also traceability. Let us look at the most widely used and well-known cryptocurrency, Bitcoin.

One of the ways to obtain a fraction of bitcoin is to purchase it through a cryptocurrency exchange. Most of these platforms are centralized, which makes it easier for malicious users to hack them and potentially steal other users' bitcoin. Unfortunately, there have already been cases of hacked accounts where owners of bitcoins on the exchange have lost everything but, while the identity of the hacker can somehow be kept completely anonymous, the stolen Bitcoins are easily traceable. If the stolen Bitcoins are taken somewhere else or spent, users can trace them. This nice feature is the result of a combination of blockchain and bitcoin features. A very tricky question we should ask ourselves is: besides these pretty interesting features, is blockchain technology really secure? The immediate answer is yes, it is. As mentioned earlier, blockchain guarantees a high level of decentralization, trust, and robustness, but what really provides a high level of security is the consensus algorithm that is at the heart of blockchain technology. Consensus is the mechanism used to reach the necessary agreement on the validity of a single data value or a single state of the network and create a valid block to add to the chain.

The best-known mechanism is proof-of-work (PoW), which is used by several blockchains, such as Bitcoin. The unimaginable computing power required to solve complex mathematical puzzles provides an extremely high level of security, but on the other hand, transaction rates are inefficient, and the energy consumption is excessive. Another well-known consensus algorithm that attempts to overcome those issues is Proof-of-Stake (PoS), which will be adopted by Ethereum 2.0. We will not go into too much detail in this section, but it is at least worth mentioning that the main difference is that the first algorithm allows all users to actively participate in the transaction verification and validation process, and potentially receive a reward, whereas the second algorithm only allows a small subset to be randomly selected for each transaction. Thus, due to the consensus algorithm, the application of blockchain technology can reduce trust costs. By using proof-of-work or proof-of-stake, users can also make transactions with people they do not know or trust. For this reason, blockchain can be a valid solution, especially in low-trust environments.

In summary, the main benefits of Blockchain are the overall improvement in accuracy by eliminating human involvement in the verification process, the reduction of costs for intermediaries, the security of transactions, transparency, and making tampering more difficult.

The main disadvantages are inefficiencies in terms of time spent verifying transactions, facilitation of illegal activities, the uncertainty of the legal framework, and limitations in data storage. The facilitation of illegal activities is not directly due to the Blockchain itself, but because it supports cryptocurrencies that, in combination with the anonymity provided by the blockchain are used by malicious users to hide the source and pathways of their criminal actions. One of the most common illegal activities in question is money laundering.

BLOCKCHAIN IN THE METAVERSE

In this section, we might try to answer the question: do we actually need a blockchain to build the Metaverse?

With the advent of Blockchain technology, many concepts that previously existed only as theories are now starting to become reality. One of them is the metaverse.

The blockchain is the backbone of environments where cryptocurrencies and NFTs are the protagonists since it enables their existence and their correct functioning. Cryptocurrencies and NFTs are used to build perfectly functioning economies in the virtual world, where you can buy, own, and sell any virtual asset you want. For example, you can buy real estate from a friend or sell digital art objects to a perfect stranger. As mentioned earlier, these are just two of the most important key concepts of the metaverse, and the only way to make them work is to use the blockchain. Many blockchain-based platforms already use NFTs and cryptocurrencies to provide an ecosystem for owning, creating, and monetizing decentralized digital assets. Blockchain enables decentralized data storage, a fundamental characteristic that differentiates the Metaverse from the traditional Internet, which relies heavily on centralized applications. Instead, the Blockchain provides access to any digital space without the need for intermediaries and centralized applications. It is important to mention that the Metaverse has two main components: Hardware and Software. The hardware includes physical tools that allow users to conveniently interact with augmented reality, like VR headsets. So, it has nothing to do with the Blockchain. When we talk about software, we refer to a digital environment with available content for users. Such an environment should be based on different technologies that guarantee many important features like security, decentralization, smart contracts, trust, and monetary relationships. One of the technologies that will be used to create and support the metaverse is the Blockchain, which is a secure decentralized database where users can interact in a dynamically updated network. Nowadays, the blockchain alone is not able to fully support the metaverse. We are talking about a relatively new technology that needs time to be improved and correctly used. Nevertheless, it is a good candidate to play a significant role in the metaverse.

We have already seen how the Blockchain provides security, decentralization, and trust. Smart contracts are self-executing contracts, where the terms of the agreement between the buyer and seller are written directly into lines of code that can be executed on a blockchain. It is directly clear from the definition of smart contracts that they can govern economic, legal, and social relationships between members of the metaverse. In addition, they can be used to establish and implement the basic rules to be followed when performing all types of operations in the metaverse itself. As far as monetary relationships are concerned, it is quite intuitive that cryptocurrency, being an integral part of the blockchain and not relying on intermediaries, can replace fiat currency and be an effective way to conduct financial transactions in a decentralized ecosystem.

By solving all these requirements of the metaverse, blockchain technology enables the construction of a stable, robust, and reliable virtual ecosystem. So, the answer to the question posed at the beginning is clear: Yes, on one hand, Blockchain technology is necessary for building the metaverse, on the other hand, it is not the only one needed. As said before, blockchain should be used in combination with other technologies that will represent the building blocks of the metaverse. Many experts agree that it is impossible to realize a "perfect" virtual ecosystem without blockchain technology. This is mainly because users should be able to securely own, buy, and sell digital properties by moving assets in a market from different platforms without centralized authorities, and blockchain would ensure the transparency and efficiency of such a digital asset market.

AVALANCHE vs SOLANA

Many people are already familiar with the two main blockchains, namely Bitcoin and Ethereum. In this section, we would like to analyze two of the most interesting blockchains on the market, namely Avalanche and Solana. Both are developing decentralized applications that are increasingly moving to the forefront in various fields such as play-to-earn games, NFTs and DeFi. These two projects are very similar in many characteristics and different in others like they have different roots and offer different services. Let us try to compare their main weaknesses and strengths from a technical point of view. The first one, Avalanche, is described as an incredibly fast, cost-effective, and eco-friendly blockchain. Avalanche is supported by a huge community of more than 680,000 people and by Ava Laps Group, a group of people who run the Fortune 500, which is an annual list of the 500 major American companies like Walmart, Google, Apple, and so on. The Avalanche project was born in 2020 and aims at providing all the functionalities of the DeFi world in a single project. The second project is Solana. Born in 2017 it is supported by an even bigger community of over 1.7 million users and by the Solana Labs, which is the team behind the project that is in charge to support it from a technical perspective. Solana's blockchain is one of the fastest-growing with a very interesting average cost per transaction of $0.00025.

After this brief introduction of the two blockchains, let us take a closer look at the two projects and try to understand the technical features that best differentiate them. As said before, they both allow the development of dAPPs, but Solana counts a higher number of projects, around 1,500. Both ecosystems have a wide range of technologies, like centralized and decentralized cryptocurrency exchanges, stable coins, play-to-earn, smart contracts, and so on. Regarding smart contracts, there is a first important difference that is, while Avalanche relies on a subchain strategy to facilitate transaction management, Solana uses the main chain.

Now, when it comes to blockchain, the concept of speed is of crucial importance. To compare Avalanche and Solana, under this point of view, we can use two basic parameters, namely TPS and finality. The former stands for Transactions Per Second, the latter refers to the time it takes to get native tokens on the blockchain, that in our case are respectively Avax and Sol. Avalanche has finality of 2 seconds and a TPS of 4500 but the developers have stated that in the future it could reach a TPS of 20000.

Solana, instead, presents a finality of 20 seconds and a theoretical TPS of 65,000 TPS, because as a matter of fact there were several service interruptions due to network congestion.

Another characteristic that is fundamental to consider, is the consensus mechanism, which, as we recall, is the method of validating transactions within the blockchain. Avalanche uses a proof-of-stake while Solana a Proof-of-History (PoH), which consists of a sequence of computations to cryptographically verify the time elapsed between two events.

The other feature we are going to compare is decentralization. Decentralization is possibly the core of blockchain and it helps in countering the centralization of power in many fields like finance. The Nakamoto coefficient is a possible indicator to assess how decentralized a blockchain is. It corresponds to the smallest number of validators whose combined stakes account for 33% of all Avax or Sol deployed. The higher the Nakamoto coefficient, the more decentralized the network. Avalanche has a coefficient value of 26, while Solana of 19. To be fair, one should not look only and exclusively at that value, but also take into account the number of validators within a given blockchain. For Avalanche, 1200 validators are counted, while for Solana there are 1249. From this, one can conclude that Avalanche is a little more decentralized.

THE CRYPTOCURRENCY

The idea of revolutionizing the current financial situation is not entirely new. In fact, the crypto movement emerged in the 1970s in the U.S. from libertarian critiques of the state. They consider central banks illegitimate and government taxes a huge scam. Cryptocurrencies are the practical implementation of that criticism.

So, one of the main reasons for the development of cryptocurrencies is to replace fiat currencies and solve some of the problems associated with them. However, current cryptocurrencies do not conform, or at least not completely, to established and accepted definitions of money. For example, cryptocurrencies cannot be considered true units of exchange because they are not globally recognized. Today, since not obliged by the law, there are a few companies, entrepreneurs, and individuals who accept them as a final means of payment compared to those accepting fiat currency. However, they are increasing. There is no legislation regulating cryptocurrencies and giving them the status of legal tender. Moreover, since cryptocurrencies pose a major problem with the volatility of their value, they cannot be considered a store of value (a necessary condition to be considered money). Therefore, in the absence of some basic requirements, cryptocurrencies are often classified as financial assets and referred to as "crypto-assets." Today the most established, well-known, and globally used cryptocurrency is Bitcoin (BTC). 1 Bitcoin is worth about €30,000 at the time of this writing and there are about 18.8 million coins in circulation, representing a market capitalization of about €564 billion. The volatility of cryptocurrencies is underlined by the fact that 1 Bitcoin was worth about €50,000 until a few months ago, and if we look at the charts of many other cryptocurrencies, we can see how quickly and abruptly their value changes. There are several ways to obtain bitcoins. One can exchange it for fiat currency through the so-called centralized cryptocurrency exchanges (Coinbase, Binance), or exchange it for another cryptocurrency through decentralized cryptocurrency exchanges (Bisq), or alternatively through the mining process directly on the platform from which the cryptocurrency in question originates. Mining is a fundamental process of cryptocurrencies that keeps the entire ecosystem alive in some way and can vary from cryptocurrency to cryptocurrency. In the case of Bitcoin, for example, it consists of solving computational puzzles. The more complex the puzzles are, the more computational power is required. Through mining, users verify and validate transactions and add them to the blockchain. Users who participate in transaction validation are rewarded with either a predetermined amount of cryptocurrency or a transaction fee. As mentioned earlier, if there were no longer incentives for its users to participate in this process, a platform's ecosystem would collapse, and so would the value of cryptocurrencies.

At this point, a question might arise: If Bitcoin, like other cryptocurrencies, is highly volatile and limited in its use, why do people buy it? The answer lies in its functional system, which operates outside the financial system and offers a high level of anonymity. Bitcoin is very useful, sometimes even indispensable, for illegal transactions (buying weapons and drugs on the black market), laundering the proceeds of crime, and other actions that could be detected by authorities without an adequate anonymity system. There are very many reasons why malicious users buy and use cryptocurrencies.

Fewer, on the other hand, are the motivations for buying cryptocurrencies for non-criminal purposes. According to many analysts and investors, the main reason for buying cryptocurrencies is to make profits. In the financial market, people usually buy a stock for short-term speculation purposes or to hold it in order to profit from it in the long run. The same is true for cryptocurrencies and given their volatility, it can be practical to speculate about them in the short term.

MOST INTERESTING CIRCULATING CRYPTOCURRENCIES

Bitcoin (BTC) is certainly the best known and most widely used blockchain, and thus cryptocurrency. In second place is Ethereum (ETH). Currently, there exist thousands of other cryptocurrencies, many of which are meaningless because either worthless, created just for fun, or simply not promising at all. However, there are some that are very interesting in what they offer to the users of their blockchain. In this section, we want to analyze some of the most interesting ones like Cardano (ADA), Tether (USDT), Monero (XMR), Litecoin (LTC), and Polkadot (DOT) platforms.

Cardano was founded by a team of academics and engineers and is based on a scientific approach that has been peer-reviewed. The primary goal is to present an alternative to Ethereum by being the third generation blockchain, but also providing solutions for interoperability, voter fraud, and legal contract tracking. For this reason, it is sometimes referred to as the "Ethereum killer". Voter fraud is a quite new feature, which has been introduced by the founder of Cardano, Charles Hoskinson. His words: *"We've been building the infrastructure for that"*, let us understand a possible implication of his blockchain in future important elections. The consensus algorithm Cardano uses is a PoS called "Ouroboros" and is based on the idea of dividing time into "epochs" that last 5 days and "slots" that last one second. For each slot, there is a lottery based on the available stake, as in a normal PoS, to select the slot leader who will be responsible for validating transactions, creating blocks, and adding these blocks to the Cardano blockchain. Ouroboros allows users to organize themselves into pools, encouraging even those users who do not have enough computing resources to actively participate in the validation process.

Tether's native coin, the USDT, is one of the first "stable coins" that aim at binding its value to a fiat currency to reduce volatility, in this case to the U.S. dollar. Tether offers the ability to facilitate the use of fiat currencies in a digital way by allowing users to make simple transfers from other cryptocurrencies back to fiat money and vice versa. Tether's Omni protocol supports transactions in US dollars, euros, and Japanese yen. Its current market capitalization is over 80 billion.

Monero is an open-source cryptocurrency that offers extremely high levels of security, privacy, and non-traceability. The development of this cryptocurrency is entirely donation-based and community-driven. Its blockchain is configured to hide all transaction details. Due to the concepts of "stealth address" and "ring signature", it is not possible to trace the transaction history. The stealth address refers to the fact that users' addresses are randomly generated for each transaction, while in the ring signature technique, a group of cryptographic signatures appears but the actual one cannot be isolated as they all appear valid.

Litecoin (LTC) was introduced a few years after BTC and tries to keep all the positive features of BTC and avoid the negative ones. LTC and BTC differ in the maximum number of possible circulating currencies (84 and 21 million, respectively), total market capitalization (8 and 800 billion, respectively), and transaction confirmation time (2.5 and 10 minutes for a transaction, respectively). One of LTC's main strengths is that it uses PoW, but with an algorithm called Script, which is simpler than BTC's SHA -256 and is designed to reduce the computational power required for mining and reduce the likelihood that mining pools will be formed.

Finally, Polkadot (DOT) is a unique PoS cryptocurrency whose main goal is to provide interoperability between other blockchains. Its protocol is designed to connect both permissioned and permissionless blockchains.

Probably the most interesting feature of Polkadot is the ability to create dApps on its blockchain. This is not a brand new concept, as it is also possible with Ethereum, but the way Polkadot does it is different. While Polkadot allows developers to create their own blockchain using the security Polkadot's chain already has, Ethereum requires developers to take their own security measures. This can discourage small projects from proceeding, as their small blockchains make them more vulnerable to cyber-attacks. This polkadot concept is called shared security.

Other very interesting cryptocurrencies that we will not analyze but are worth mentioning are Stellar (XLM), Zcash (ZEC), Bitcoin Cash (BCH), Dogecoin (DOGE), Tonne (TRX), Chainlink (LINK), and Polygon (MATIC).

THE NFT

In a fully digital world like the Metaverse, where there are no financial intermediaries, the keyword is and must be "security." To date, there are no legal rules that govern and control the metaverse. It lacks some inalienable human rights and duties that we are used to owing and respecting. One basic right is the right to property and the rights associated with it. How can we enforce our property right to a particular item or copyright to a particular work of art in a lawless world?

Smart contracts are used to establish policies that must be followed, and non-fungible tokens, or NFTs, are used to uniquely and securely identify digital assets created on the Internet. As their name implies, non-fungible tokens are neither reproducible nor exchangeable. An Ethereum crypto coin, for instance, is fungible in the sense that you can change it with another one without losing its value, utility, or purpose. NFTs are therefore unique. There is not a specific category of object that can be classified as an NFT. Indeed, an NFT can be a video, an image, an audio, and so on. An NFT is a sort of certificate of authorship that identifies the object as a copyrighted object.

NFTs highly depend on the blockchain and cannot exist without it. It is precise because of this linkage to the Blockchain that NFTs represent something unique, an exceptionally powerful tool that guarantees the uniqueness of a product and protects its owner/creator. In the real world, it is often easy to check whether a work of art is counterfeit or a copy but in the digital world, the story changes. For example, given two identical images, how do you establish which is the original and which is the copy? Well, it is very difficult, if not impossible. NFTs do just that, they guarantee the uniqueness of an object and make it possible to immediately know whether it is original or not. NFTs are contained in the blockchain, and, due to its structure, the information contained in it cannot be changed. This ensures that the product is unique and cannot be reproduced.

For obvious reasons, NFTs are considered a revolution, especially, in digital art. As for the practical aspect, the person who purchases a work linked to an NFT does not buy the work as in the real world, where once you buy a product, you physically own it. Indeed, through an NFT one buys in a certain sense, the ability to assert a right to that work through a smart contract that automatically verifies the execution of a contract.

In producing a particular work, the artist stores a specific object, such as a photograph or film, in a digital format that is linked to a sequence of numbers. Such a sequence of numbers is then associated with another independent sequence through a hash function, which is a cryptographic function that maps data of arbitrary size, called a "message," to a fixed size, the "hash." It is a one-way function, which means that it is virtually impossible to invert or reverse the calculation. The hash thus represents an important tool that serves as a guarantee to the owner. Once the hash is calculated, it is then inserted into a blockchain, using an associated timestamp to verify the history of transactions of that specific NFT. It is important to clarify that only the hash of work or digital content is contained in the blockchain, while, in general, the digital content is stored somewhere on the internet

BORED APE NFT

Bored Ape Yacht Club, or simply Bored Ape, is an NFT collection built on the Ethereum blockchain. The collection consists of procedurally generated cartoonishly rendered profile images of humanoid apes. The parent company of Bored Ape Yacht Club is Yuga Labs, which launched the project with a pre-sale of tokens on April 23, 2021. Owning a Bored Ape NFT grants exclusive access to a virtual private club with exclusive events. In the year following its launch, Bored Ape's revenue was around $1 billion. Several celebrities, including Justin Bieber, Snoop Dogg, Neymar, and Steve Aoki, have not hesitated to spend huge sums on a Bored Ape. The Bored Ape collection was born almost by accident. Four friends wanted to create something for fun, not suspecting that these tokens would later be the subject of much attention and criticism. The criticism stems from the idea that dirty money is flowing around these NFTs and their exaggerated prices. The Bored Ape, as well as all other NFTs, aim at providing their owners with the original piece of art and grant them property rights. Indeed, the owners of Bored Ape NFTs are considered to own a unique data entity stored on a blockchain that definitively and immutably records its provenance. Anyone accessing the blockchain where the NFTs are stored can verify both the affiliation with a single user and the sales history of a particular NFT and, thus, its previous owners.

Bored Ape's collections consist of 10,000 unique NFTs that serve as membership cards for the before mentioned Yacht Club. At launch, the NFTs were sold at 0.08 Ether each, equivalent to $190 at the time. Bored Ape Yacht Club stated that "NFT owners have full marketing rights to their ape."

After the unexpected and resounding success of Bored Ape, Yuga Labs began hiring experts in various fields such as art, social media management, and other types of managers, as it aspires to become a Web3 lifestyle company. The company also released secondary resources, namely Bored Ape Kennel Club, Mutant Serum, and Mutant Ape Yacht Club, which increased the value of Bored Ape Yacht Club, expanded the user network, and rewarded the first investors and buyers of a Bored Ape NFT.

Recently, on April 25, 2022, because of a hacking attack originating from Yuga Labs' Instagram account, four NFTs from the Bored Ape collection and ten from other collections were stolen. The estimated value is around $3 million. This exaggerated value of Bored Ape is clearly not the actual value of a Bored Ape NFT, but a sort of status symbol for some millionaire users. There are many Bored Ape NFT owners who have admitted to buying their apes, even at crazy prices, for potential marketing and branding projects associated with a Bored Ape NFT.

SOME PROMISING METAVERSE PROJECTS

Today, there are some developers who are trying to apply the idea of the metaverse to their blockchain projects. Some of the most interesting projects are The Sandbox, Dcentraland, Axie Infinity.

The Sandbox was originally developed as a normal mobile app and then turned into an interesting metaverse built on the Ethereum blockchain network. Within the game, users can create and sell digital assets using Sandbox's own coin, Sand. The idea is that users create and personalize their avatar, which is connected to a special electronic wallet used to manage NFTs, Sand, and assets. The game offers a play-to-earn model to encourage users to play more and more to boost the domestic economy.

Decentraland is another Ethereum-based 3D metaverse where users can create avatars as usual and buy virtual lands to develop them for various purposes, such as organizing various events or creating digital content and selling it. Such purchases can be made with Decentraland's native currency, Land, and ownership of real estate is guaranteed through NFTs. Of course, virtual real estate is the core of the project. An interesting aspect is that this metaverse is controlled by a decentralized, autonomous application, namely Decentraland DAO, which treats landowners like shareholders. Namely, they can actively participate in DAO and potentially cast their vote for new initiatives and developments.

Axie Infinity is another Ethereum blockchain-based metaverse that, like The Sandbox, offers a play-to-earn model. In this metaverse, users can train fantasy creatures called Axies, similar to Pokémon sneakers. By training these creatures, the trainer earns the native currency, Axs, which can be spent on buying, training, or equipping new Axies, which are traded as NFTs. Like everywhere else, there is plenty of speculation and madness. Suffice it to say that the most expensive purchase of one of these Axies was for about $800,000.

THE NEGATIVE SIDE OF BLOCKCHAIN

Not all that glitters is gold. While we have seen the most interesting and innovative aspects of blockchain, it is good to understand what the critical issues are that could have serious consequences not only for the individual user but for the entire ecosystem of a blockchain. Let us face it, this technology, as promising as it may be, has serious gaps that are very difficult to close.

Vitalik Buterin has tried to summarize the problems of blockchain in his "Trilemma." He claims that three of the fundamental features of blockchain cannot exist simultaneously due to the structure of the blockchain itself. We are talking about decentralization, security, and scalability. Unfortunately, the blockchain problems do not end there. It is not only the impossibility of achieving these three features at the same time.

Let us start right away by analyzing two of the biggest difficulties blockchain developers and users face, namely scalability and inefficiency. Inefficiency in terms of time needed to verify transactions and energy consumption. Let us take a practical case, Bitcoin. Due to the way PoW works, the more computing power and electrical energy invested, the greater the chances of solving the puzzle and receiving the prize. This, of course, creates problems in terms of energy consumption. Moreover, PoW is very slow in terms of the rate at which transactions are verified. Transactions are validated in blocks and each block contains around 2500 transactions. PoW dynamically adjusts how much computing power it needs to find a valid block, limiting the creation of a block to about one every 10 minutes, meaning around 2500 transactions per minute and only 4-5 per second. From these two points of view, the Bitcoin network and many other blockchains that rely on PoW are very inefficient. If we compare Bitcoin with VISA technology, the latter performs around 24,000 transactions per second. Obviously, there are no chances that a cryptocurrency based on a blockchain can replace or at least compete with fiat currency and all already established technologies in terms of efficiency.

As if that were not enough, there are also issues related to scalability, which is the growth of the network itself. Let us imagine a hypothetical situation in which the number of users using Bitcoin for transactions instantly doubles. In such a scenario, the transaction verification process does not change, and this has two consequences. First, security increases as the number of users involved in transaction verification increases, and second, each transaction is preceded by twice as many transactions as before. This means that each user has to wait twice as long before their transaction is approved. What if the network were to increase 10, 50, or 100 times? The waiting times would become so exhausting and frustrating that no one would want to use such a blockchain.

Another crucial issue is interoperability. Each blockchain is designed to provide services to anyone using its own cryptocurrency. This means that a user who owns Bitcoin will not be able to access the services of another blockchain like Ethereum, as the latter requires the use of its own cryptocurrency. You might think that this is no big deal since the same thing happens with fiat currency when you want to buy a sandwich with euros in England, for example. It's true. But while switching fiat currencies is extremely easy, switching from one cryptocurrency to another is not. It is extremely complicated. Since cryptocurrencies are purely digital currencies, this is not acceptable. Moreover, we should consider that today there are thousands of blockchain-based platforms and applications, each with its own cryptocurrency.

How can we get around all the obstacles that fiat currencies face when the blockchain does not even allow for a hundred transactions per second? How is it possible to overcome space and time with such a technology that brings these major problems? Obviously, it sounds impossible. However, many solutions have been proposed, and some of them are quite interesting.

POSSIBLE SOLUTIONS

To save the Blockchain, there is the concept of the new. The Blockchain is indeed an absolutely new technology, and all new inventions, findings, and creations are not perfect at the beginning. While it is true that blockchain has serious problems on one side, on the other side it has already shown some of its potential, and they are enormous. The possibilities for a practical application of blockchain are many, as are the benefits that can be derived from it, and this is precisely why entire communities of users, specialized platforms, and experts are investing huge sums of money and devoting their hearts and souls to discovering ideas that can solve these problems.

With regard to the problems of the inefficiency of the transaction verification process and the enormous amount of energy required, it has been concluded that the solution lies in improving the consensus protocol. The proof-of-stake adapted from Ethereum 2.0 is a practical example of this. The basic idea of PoS is that for each transaction verification, a subset of nodes on the network is randomly selected based on the amount of stake each user owes. The higher the amount, the more likely it is to be selected as a validator. With this strategy, the PoS mechanism tries to solve the problem of energy consumption. Since miners no longer need to rely on vast farms of special-purpose hardware to gain an advantage, it also means that PoS provides greater immunity to centralization. The exact details of such a consensus protocol vary by project, but in general, we can distinguish three common phases. In the first phase, the network selects validators based on the number of cryptocurrencies they have deposited into their wallets. The chance of being selected for validation is roughly related to the total percentage of coins deposited. So, in a sense, PoS literally rewards the most invested participants. Once the winners of the selection have validated the last transaction block, other validators are called to confirm that the block is correct. When a certain number of confirmations is reached, the block is validated and added to the blockchain. Finally, the third phase consists of a reward in native cryptocurrency allocated to all validators, which is generally distributed by the network in proportion to each validator's effort.

However, PoS does not seem to be the ultimate solution. While it is true that it solves some important problems, at least in part, it is equally true that it raises others. The most important of these problems is certainly the reduction in the level of security compared to PoW, where each node is involved in validating transactions. It almost seems like fighting one problem by introducing others. The problem could discourage many and provide no incentive to improve blockchain technology. However, some of the proposed solutions to combat the problems are promising. One of them aims at solving the inefficiency of the transaction verification process and scalability issues. One of the most promising is "sharding." Sharding is not a new idea. In fact, it is used for common database partitioning, although it is called horizontal partitioning. It simply consists in dividing a large database into smaller databases so that it is easier to work with them and identify any problems. When we apply the sharding technique to the blockchain, the blockchain itself is divided into individual shards. Each shard contains a unique set of smart contracts and account balances. These shards are processed in parallel by the network so that a large number of transactions can be processed simultaneously. Instead of each network node holding a copy of each block from its creation block to the last block, this information can be split and held by different nodes. Ethereum 2.0 is a well-known blockchain protocol that is testing the use of shards. It is clear that sharding cannot be applied if the blockchain uses PoW, where all users focus on each transaction. In a blockchain that relies on PoS, such as Ethereum 2.0, the situation is different. Each group of validators, chosen at random, can be assigned a specific shard. However, while sharding ensures better efficiency in terms of transaction verification timing, a fragmented blockchain leads to communication problems among the different shards. Again, the idea solves one problem by creating others that in turn need solving. Ethereum 2.0 has found its solution in the beacon chain, which is used for communication and coordination between shards.

Another promising solution proposed by Bitcoin for the problem of scalability and inefficiency is the Lightning Network. The Lightning Network is nothing more than a second-tier network that transmits signed transactions between peers and relies on the blockchain only for the final settlement of funds. The idea is that two users open a channel, following some predefined rules, and within the channel perform the required number of transactions in real-time. These transactions are "invisible" to the other users, and only the final commitment is registered in the blockchain and is therefore public. With this solution, we enable transactions not to be limited to block size, confirmation times become irrelevant, and the blockchain does not need to store every single transaction. Here is how it works: Let us say two users, say A and B, want to do some transactions with each other. Now, they can either use the standard method, where it takes a lot of time to complete all transactions, or they can open a lightning channel, where all transactions, except the final commitment, are completed in real-time. To open it, both parties must fund the channel equally, and each transaction requires multiple signatures. The moment they built the channel, a commitment transaction is created and adjusted after each transaction to ensure that the correct amount of bitcoin is allocated to both users A and B.

Once the two users have completed their transactions, the channel must be closed before the correct amount of cryptocurrency can be transferred back to the respective owners. Such closure can take place in three ways. The first, called collaborative, is for one of the parties to initiate the closure of the channel with the agreement of the other party. The second possibility is called unilateral and consists of one party initiating the closure without the consent of the other party. In such a situation, a time block is used to guarantee the honest party that it can challenge the closure with a remedial transaction. The third case is called "breach" and occurs when a party tries to close the channel with an old transaction where it had more money. During the blocking period, the honest party can not only get their money back but also the entire capacity of the channel. When the honest party is offline, the task can be delegated to other nodes, called watchtowers, which receive a fee for monitoring.

PERSONAL OPINIONS AND CRITICISM

The purpose of this section is to report on some of the criticisms and personal opinions about all the concepts exposed in the article.

Let us start with the Blockchain, the core around which everything revolves. Blockchain is a very interesting concept, considering the high level of transparency, decentralization, and privacy it provides. In my opinion, transparency and privacy are important concepts, but they cannot always go in the same direction, and sometimes they even contradict each other. Transparency should not only mean that anyone can access blockchain records, but also those malicious users and fraudulent transactions are detected and intercepted since all details of transactions are transparent. However, it is not like this. The high level of privacy makes it very complicated to track down crooks, malicious individuals, and their schemes. Sometimes it makes it even impossible. A threshold on the level of privacy should be found so that, on the one hand, it satisfies some users to enjoy certain anonymity, and on the other hand, does not hide fraudulent activities and criminals.

As for the transaction verification process, it not only consumes excessive energy but also leads to exhausting waiting times. Personally, I prefer to pay a little more to get speed and efficiency in return. However, what I find most critical is the almost complete lack of regulation. This absence leaves users with few legal options to get their money back if something unforeseen happens during one or more transactions. There are of course some possible remedies but, in my opinion, not enough to allow the average user to blindly trust the blockchain.

Moving to cryptocurrencies, the first problem that stands out is certainly the volatility of most of them. The value of a cryptocurrency can skyrocket in a very short period, but it can also plummet. Recently, one of the most famous cryptocurrencies with one of the highest market capitalizations lost 99.99%. I am talking about Luna, the cryptocurrency of Terra. For an instrument that is supposed to replace the fiat currency, or at least represent a revolution, such extreme volatility is certainly not helpful. Cryptocurrencies are indeed used as an instrument for speculation. This is undoubtedly one of the main drawbacks of cryptocurrencies.

Another aspect that I am very critical of is the difficulty of fully understanding what a cryptocurrency is and, more importantly, how it works. Setting up an account on a blockchain is often convoluted and complicated, and the steps to obtain cryptocurrencies are very difficult to follow. In this sense, I could argue that the lack of intermediaries means that people with little background knowledge are much more vulnerable to hacking. The idea that a single digital currency could replace fiat currency is certainly interesting but impossible at the same time. There are too many cryptocurrencies, now thousands, and each of them has different problems related to scalability, volatility, and so on.

Instead, when I talk about NFTs, my confusion and doubts increase. I am not questioning the usefulness of an instrument that can protect some of the fundamental rights, such as the right to property and all the rights derived from it, especially in a reality where there are no laws and legal norms. What I question is the value that is given to them. There have been cases, like that of Bored Ape, where NFTs were bought for millions of dollars. This astronomical value is certainly due in part to the fashion of the time, a status symbol of sorts, and so on, but the greater concern should be the unprecedented ease with which money can be laundered.

Finally, as for the metaverse, I believe it can revolutionize some or all sectors, especially gaming. However, the enormous enthusiasm surrounding the metaverse itself stems largely from the fact that it is little more than a grand experiment. It is human nature to travel with the mind, creating myths and sometimes false illusions in the hope of a better future. A practical example is the Covid 19 pandemic, where every time a possible vaccine became known, people began to fantasize about the uncertain future, sometimes assuming that the vaccine would be the solution to all the problems associated with the virus and the lifestyle it caused. Returning to the metaverse, I personally believe that investments and projects should continue even in the face of seemingly insurmountable obstacles. In fact, each of the essential elements of the metaverse has advantages, but also disadvantages that can sometimes jeopardize the security and financial well-being of the individual. The metaverse is an ambitious, revolutionary, and unique project that, if pursued with perseverance, dedication, and cooperation, can overcome some of the problems that could slow its growth or spell epochal failure.

REFERENCES

1. **Massimo Bernaschi.** *Blockchain and Cryptocurrencies*. Teaching materials, academic year: 2021/2022 **(**https://www.luiss.it/)
2. **Adam Hayes.** *Blockchain explained*. March 05, 2022 (https://www.investopedia.com/terms/b/blockchain.asp)
3. **PixelPlex Team.** *Decentralized Economy — the Role of Blockchain in the Metaverse*. February, 2022 (https://pixelplex.io/blog/importance-of-blockchain-in-metaverse/)
4. **Thippa Reddy Gadekallu, Thien Huynh-The, Weizheng Wang, Gokul Yenduri, Pasika Ranaweera, Quoc-Viet Pham, Daniel Benevides da Costa, and Madhusanka Liyanage.** *Blockchain for the Metaverse: A Review*. March 21, 2022 (https://arxiv.org/pdf/2203.09738.pdf)
5. **Be Curious Finance.** *Solana vs Avalanche – Chi vince?* May 22, 2022 (https://www.youtube.com/watch?v=VYmAimIVdGw)
6. **Wikipedia.** *Bored Ape*. Updated June 2, 2022 (https://en.wikipedia.org/wiki/Bored_Ape)
7. **Robyn Conti, John Schmidt.** *What Is An NFT? Non-Fungible Tokens Explained*. April 08, 2022 (https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/)
8. **Mitchell Clark.** *NFTs, explained*. Updated June 6, 2022 (https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq)
9. **ProssimaFase.it.** *17 Vantaggi e svantaggi della Blockchain*. (https://prossimafase.it/17-vantaggi-e-svantaggi-della-blockchain/)
10. **Katya.** *Cardano elections: how blockchain can be the future of voting*. January 29, 2021

(https://swyftx.com/au/blog/cardano-elections-how-blockchain-can-be-the-future-of-voting/)

11. **Emanuele Atturo.** *Il concerto di Travis Scott nel mondo parallelo di Fortnite cambierà tutto*. April 27, 2020 (https://www.esquire.com/it/lifestyle/tecnologia/a32277024/travis-scott-fortnite/)
12. **Paul Tassi.** *Fortnite's Travis Scott Concert Was A Stunning Spectacle And A Glimpse At The Metaverse*. April 23, 2020 (https://www.forbes.com/sites/paultassi/2020/04/23/fortnites-travis-scott-concert-was-a-stunning-spectacle-and-a-glimpse-at-the-metaverse/?sh=74aa9b282e1f)