Blockchain: In-Depth Analysis

Authors: **Catarina Oliveira, 98298**
Daniela Dias, 98039
Hugo Gonçalves, 98497
Rodrigo Lima, 98475

Date: **10/05/2022**

Index

1. Introduction

Blockchain, at its core, is a system that records information in a way that makes it difficult or impossible to change or cheat the system. It is a ledger of transactions, in other words, a collection of recorded transactions that are duplicated, distributed, and shared across an entire network of nodes that include computer systems. As a database, a blockchain stores information in digital format.

Blockchains have been attracting lots of attention for the last decade, especially in response to their role in cryptocurrency systems, such as Bitcoin. It has shown to be a great tool for maintaining a secure and decentralized record of transactions, facilitating the process of tracking assets in a business network. It is worth noting that blockchain can track both tangible (physical properties) and intangible assets (intellectual properties).

Cryptocurrencies have been considered highly valuable due to multiple key attributes found in any currency: scarcity, divisibility, acceptability, portability, durability, and resistance to counterfeiting (uniformity). However, its main source of value lies in its restricted supply and increasing demand. As the supply diminishes, demand for cryptocurrency increases, inevitably raising its value. At the same time, blockchain has made it impossible to copy or counterfeit these kinds of cryptocurrencies, by keeping track of every transaction made.

No matter the area this technology is used, blockchain promises to guarantee the fidelity and security of an immutable record of data and generate trust (especially in transactions) without the need for third parties.

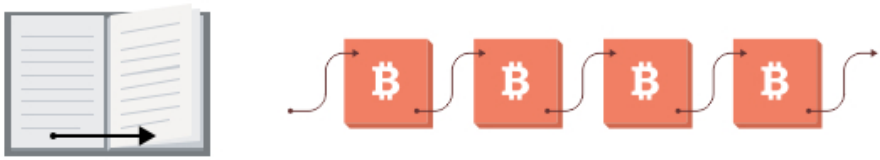
2. Blockchain analysis

Blockchain, to put it simply, is just a data structure stored in a file - the way this structure is built and organized is what makes it special.

The structure of blockchain can be put in abstractedly as a book. A book is composed of pages, text, and information about itself, in the same way, the blockchain is also composed of blocks, the contents and the headers.

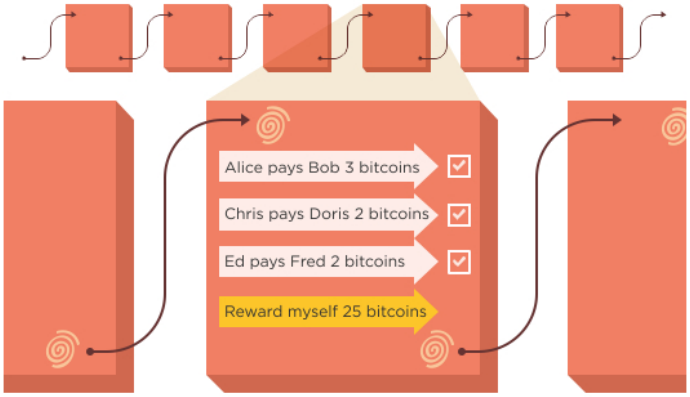
Each block of the blockchain has its content, this being, for example, the amount of a transaction or the source/destination of it. This content enables a logging system like a ledger in banking services. In the same way that a ledger in a bank has a list of transactions made by or to that bank, a blockchain is a list of blocks where each block stands for a transaction made on that blockchain.

A block is composed also of another key attribute that gives blockchain the integrity needed to be a reliable source of truth used for monetary transactions, this one being the **header**. The header is composed of technical information about the block, a reference to the earlier block, and a fingerprint (hash) of the data held.



Like a book with pagination present on each page, a blockchain has blocks with references made to the earlier block, enabling strict ordering of the blocks.

The use of a fingerprint, instead of a timestamp or a numerical sequence, enables easy validation of the blocks. Each fingerprint is generated by a known algorithm. By knowing the algorithm and the block that the fingerprint stands for, any user can verify if any data has been tampered with. If a fingerprint is consistent with the data and the fingerprints relate to a chain, then the blockchain is internally consistent. If a user tampered with any data inside a block of the blockchain, the fingerprints from that point forwards would be different which would indicate that the blockchain is no longer consistent.



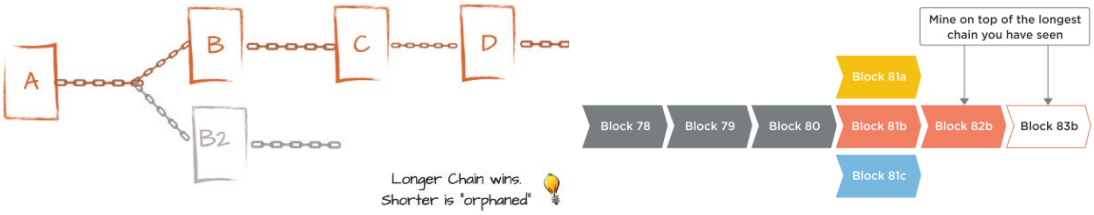
3. Blockchain security

Although a blockchain can be represented as just a file, data structure wise, the file itself is a file distributed by several nodes. These nodes are a peer-to-peer network and, while distributing the file, a transaction can be verified by checking the consensus of the majority. The consensus of the majority is earned by querying all the nodes and checking if a transaction made by another node can be trusted.

The search for the network consensus, plus the integrity validation natively supported by the data structure, enables good security on the blockchain if done correctly. Although there are some security checks made on a blockchain, there are also flaws in it.

A node that generates blocks, also called a "***miner***," that is dishonest can attempt to create blocks that include or exclude specific transactions of his choosing. This is mitigated by other nodes implementing honest transactions that were ignored by the dishonest node. However, on a network scale, if a group of miners that represent a majority (>50%) are the source of truth of that network and they have dishonest goals, those goals will translate into the real transactions because the consensus of the network is determined by them. Although this represents a strong security mechanism in big networks such as Bitcoin, on smaller public networks this may be a huge problem and attackers may use this to attack the network – see an example of an attack.

Depending on the block generation implementation used by a blockchain, there might be also flaws in the overall security of that network in this aspect. In bitcoin's blockchain, for example, the addition of a block to the blockchain needs to comply with the rule of the "***longest chain".*** The rule of the longest chain describes that a block should be added to the network if and only if that block has a speculated hash value or lower in its fingerprint. The longest chain rule also dictates that if a node has more blocks chained together than other nodes, then that block has the legitimate chain to be used and the other blocks made by other nodes will be unused. This means that, if a dishonest miner creates a longer chain of blocks than the rest of the network, it can unwind a transaction making it an orphan (an unused block in a blockchain).

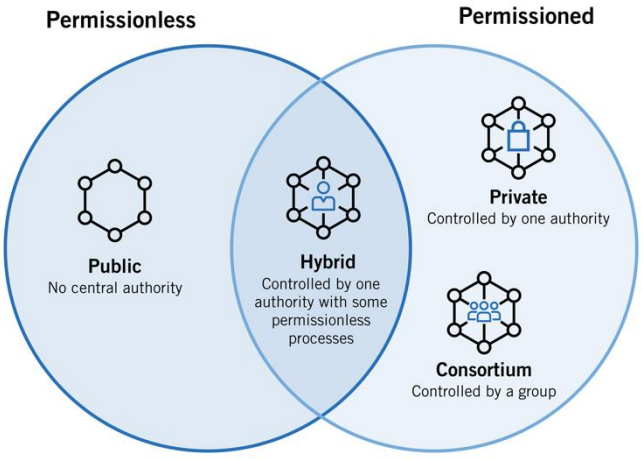


4. Blockchain currencies and networks

4.1. Types of blockchain networks

There are several ways to build a blockchain network and to set the visibility of the blockchain. The Blockchain network's visibility can be public, private, or administered by a consortium. Meanwhile, all types of blockchains can be characterized as permissionless, permissioned, or both.

Permissionless blockchains allow any user to join the blockchain network pseudo-anonymously and do not restrict the rights of the nodes on the blockchain network. On the other hand, permissioned blockchains restrict access to the network to certain nodes and may also restrict the rights of those nodes on that network. The identities of the users of a permissioned blockchain are known to the other users of that permissioned blockchain, not to mention participants need to obtain an invitation or permission to join.



4.1.1 Public blockchain networks

A public blockchain is available for anyone to join and participate in (seen in Bitcoin and Ethereum, for example). This type of blockchain network includes some problems and some advantages that will be analyzed in more detail below.

4.1.1.1 Problems with public networks

Among the problems, we have the sometimes-substantial computational power required to be part of the blockchain and the little or no privacy for transactions.

Most public networks have Proof-of-Work algorithms which determine that each node needs to perform a computational challenge to process a transaction. However, these challenges need a lot of power and take a long time to be completed. Bitcoin network, for example, can only process around 7 transactions per second, while the Visa network (one of the biggest traditional networks for payments) can process up to 24 000 transactions per second. This high consumption of energy has social, economic, and Ambiental drawbacks, as we are going to see ahead.

On top of that, everyone, using a blockchain explorer such as Blockchain.com can check all the transactions made in a public network to a wallet and even check the current existent balance in that wallet. While it is true that everyone can inspect the transactions in a certain wallet, in ecosystems like the Bitcoin network, there is no way to associate the wallet address to the identity of its holder as the addresses are 34 characters long and usually look like this:

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Example of bitcoin address

Besides that, all the transactions made are spread through the entire network. Once the network is formed by a peer-to-peer group of nodes, it is impossible to trace a transaction back to its source.

4.1.1.2 Advantages of public networks

Some of the advantages are ***security*** and ***decentralization***. Once no company or entity owns the entire or majority of the network, if the network is big enough, there is no way to roll back the network and undo transactions/operations once it would require a consensus of 51% of the nodes in the network, which is practically impossible to reach in public and extensive network such as Bitcoin.

However, if the network is small or in its beginning, then the attackers may try to launch as many nodes as needed to get 51% of the network. Once they have control over 51% of the network, they can prevent new transactions from being processed and generated.

Therefore, we can say that the security of a blockchain network depends on its size and on the number of nodes it contains. While a vast network such as Bitcoin may be immune to 51% attacks, some small networks have suffered this “51% attack” before. An example of this is the attack on the Ethereum Classic network in 2018.

4.1.2. Private blockchain networks

A private blockchain network, as the name indicates, is private and usually owned by an entity or company. This entity controls who can be a node and which permissions that node will have. These networks are, therefore, ***permissioned*** networks. Examples of these networks are Ripple and Hyperledger. This type of blockchain network also includes some disadvantages and advantages.

4.1.2.1 Advantages of private networks

The main advantages of private blockchain networks are their ***speed*** and ***scalability***. Once they are controlled and owned by a private entity and have a limited number of clients, they are a centralized network that, therefore, can process thousands of transactions per second. Besides that, they are easy to scale, as the owner of the blockchain only needs to deploy more nodes to scale the network.

4.1.2.2 Disadvantages of private networks

On the other hand, the main disadvantages of private blockchain networks are their ***security*** and ***privacy***. Once a private entity owns these networks, then there is no anonymity in the network, as the administrator can know exactly who made some transactions in the network.

Once these blockchain networks are typically smaller, another problem is their security, making them more vulnerable to malicious attacks as already explained before. This problem can be mitigated by the validation of the transactions by certified and trusted nodes.

To try to address these issues, **consortium** blockchain networks were created.

4.1.3. Consortium blockchain networks

Consortium blockchain networks are networks that are controlled by a group of entities or organizations (rather than only one organization as is in private networks). One famous example of these networks is the GSBN (Global Shipping Business Network Consortium).

4.1.3.1 Advantages of consortium networks

Once these networks are owned by a group of entities, they can achieve a higher level of ***decentralization*** than private networks as the nodes are controlled by a group of organizations, instead of one, and can be ***fastest*** than public blockchains as they have a limited number of clients.

4.1.3.1 Disadvantages of consortium networks

Sometimes, setting up a consortium can be an arduous process as it requires cooperation between the several entities that are part of the consortium. Besides that, some of the members may not have the resources or needed infrastructure to implement and maintain the technology, making the ones that have second thoughts about if the price and needed resources are worth it.

4.2. Main currencies and networks

Currently, there are more than 2000 blockchains distributed within the diverse types of blockchains already discussed in topic 4.1. Types of blockchain networks. However, some blockchains stand out either by their popularity or by the unique way they work and different problems they try to solve. Some examples of these blockchains are:

- **Bitcoin:** The most popular blockchain technology.
- **Ethereum:** The most popular smart contract and decentralized apps blockchain technology. Also, the second most popular blockchain in market capitalization.

4.2.1. Bitcoin

The Bitcoin network was created in 2008 by Satoshi Nakamoto to implement a quite simple concept – a virtual coin that allows secure and private transactions using a peer-to-peer network. However, in opposition to the regular digital payment methods like PayPal that rely on the traditional banking system and accounts to move the money from/to the already existent bank accounts, the bitcoin is completely decentralized, i.e., it does not depend on any governmental or private institution to transfer the funds.

All the transactions involving Bitcoin are stored in the bitcoin blockchain which is like a bank's ledger – a log of the funds going out and in accounts. The traditional accounts are ***wallets*** in Bitcoin's network, and each one of these wallets is identified by a unique 34 bits length identifier.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh
Example of bitcoin address

The transactions sent through the bitcoin network are processed by powerful machines usually called "miners." These miners perform the necessary equations to verify and record every transaction in the network. Once these transactions are finished and appended to the blockchain, we are the holders of the value transferred to us and we can trade it for traditional currencies, using an exchange, or trade it for goods in some store that accepts Bitcoin as payment.

4.2.1.1 How does Bitcoin have value?

Something that may be confusing sometimes is how Bitcoin, which is a 100% virtual resource can have real value in the real world. The simple answer is that its value has the same

source as the traditional currency does, i.e., it is valuable because it has proven itself to be a viable and convenient way to store and trade value.

This means that it can easily be traded for services, goods, or other virtual and physical assets. It is scarce (the bitcoin limit was set up to be 21 million units), secure, portable, and easily divisible, allowing transactions of all sizes. It is comparable to the dollar or euro, with the exception that it is not controlled or emitted by any governmental organization; instead, it is emitted by the miners that should deliver value - solve complex problems to store and validate new information in the network - to be rewarded with Bitcoin.

In 2020, up to 15 000 entities accepted Bitcoin as payment worldwide, proving that it has real value and can be a secure, decentralized and valid method of payment for goods worldwide.

4.2.1.2 Bitcoin's mining algorithm

In the above sections, we always referred to Bitcoin's mining process as the process of solving complex mathematical puzzles. In reality, the process behind Bitcoin mining is way simpler than it looks.

In simple words, the Bitcoin miners must come up with a 64-digit hexadecimal number (***hash***) that is less than or equal to a target SHA256 hash. The miners will use brute force to generate different hashes and check if those are less or equal to the target hash; if the generated hash by them is not less or equal, then they'll generate another hash. The miner to get the first and closest hash to the target hash will be the one who may generate the next block of the blockchain.

In python, the algorithm to mine Bitcoins, i.e., to try to guess a lower hash than the target hash would be something like this:

```
MAX_NONCE=10000000        # Or While True to run forever
def mine(block_number,transaction,previous_hash,prefix_zeros):
  prefix_str='0'*prefix_zeros
  for nonce in range(MAX_NONCE):
    text= str(block_number) + transaction + previous_hash + str(nonce)
    hash = SHA256(text)
    # print(hash)
    if hash.startswith(prefix_str):
      print("Bitcoin mined with nonce value :",nonce)
      return hash
  print("Could not find a hash in the given range of upto", MAX_NONCE)
```

4.2.2. Ethereum

The Ethereum network was released initially in 2015. In opposition to Bitcoin, Ethereum was not conceived to act as a digital currency. Instead, the Ethereum network was created to be a decentralized network of computing that would provide the decentralization and security of the blockchain to decentralized apps (Dapps). These Dapps can be everything from financing tools to games and complex databases that will run in the Ethereum network.

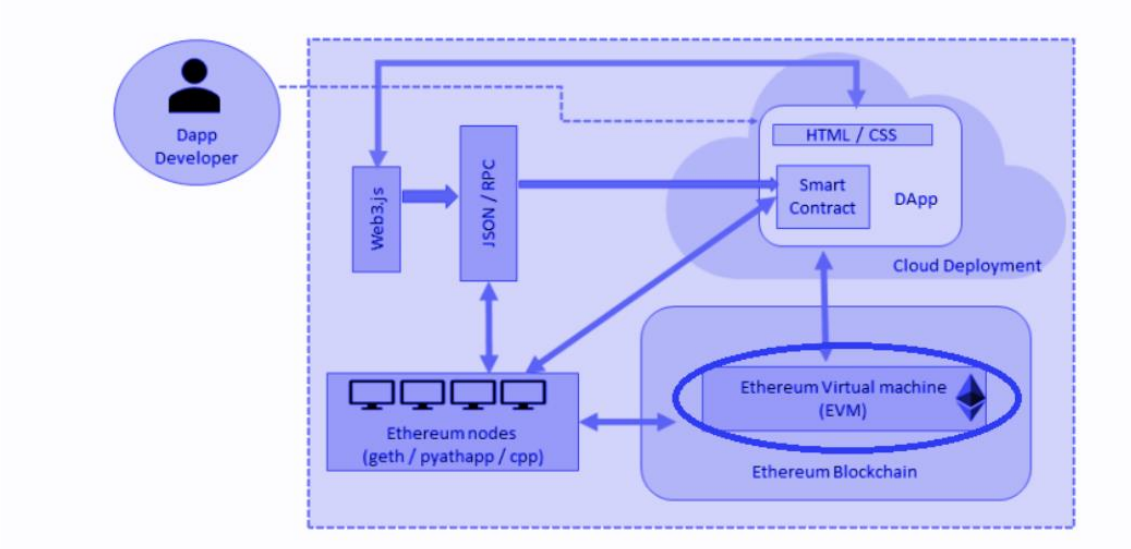
While Ethereum can also be used to send money across the world and process transactions, this is not its main purpose. The main purpose of the Ethereum network is to process

data in a decentralized way. That's the reason why the way Ethereum works is somehow different from the way Bitcoin works.

4.2.2.1 How does Ethereum work?

While Bitcoin can be compared to a huge bank ledger, the Ethereum blockchain network is more like a giant virtual computer. This "giant virtual computer" is composed of a lot of other "small" computers (***nodes***). The giant computer will receive tasks to process (***smart contracts***) and distribute them across its nodes. Each one of these nodes will then process that information and return it to the main "virtual computer" that will return the results.

Anyone can be part of the Ethereum network by running the Ethereum software and "renting" their hardware to process the tasks attributed. This participation is rewarded using the ETH token (Ethereum cryptocurrency), which can then be traded by traditional currencies or goods.



4.3. Types of proofs

The blockchain applications, whether they are cryptocurrencies or another kind of blockchain-based application, will only work if the integrity and trustworthiness of the network can be ensured. Therefore, all the new data that is generated must be verified by the nodes that are part of the network before that data can be put in a block and appended to the blockchain where it should remain stored forever.

To verify the data, there must be any sort of consensus algorithm implemented in the network so the nodes can agree on if some data is valid or not. That is where the proof mechanisms take place. The proof algorithms are used by the blockchain to reach a consensus between all the nodes and decide whether some piece of information is valid or not and should be appended or not to the blockchain.

These algorithms are the core of the high security granted by the blockchain applications and should work perfectly to maintain the network secure and intact.

Once there is a huge amount of blockchains implemented, with an also a huge number of different purposes, then a lot of different types of consensus algorithms were created. Each one of these algorithms has their particularities and use-cases as we are going to see in more detail in the section below.

4.3.1. Proof of Work

The ***Proof of Work*** (POW) is a process that involves a set of different nodes, usually called ***miners.*** These ***miners*** will participate in the process by solving complex and, therefore, expensive (in energy consumption terms) puzzles using CPUs, GPUs, ASICs, etc. Once a miner solves one of these puzzles, it will receive a block as a reward if they were the first to find to solution to that puzzle.

Since only the first miner who finds the solution to a puzzle is rewarded, and these puzzles can only be solved by trial and error, it requires a high amount of computational power to find the solutions quickly enough (before anybody else does). All this “high power” leads to high annual power consumption. The annual power consumption of Bitcoin is estimated at 51.13 TWh – equivalent to 5 million houses annual consumption – which leads to a high Ambiental, and economic impact as will be discussed below.

4.3.2. Proof of Stake

The ***Proof of Stake*** (POS) randomly selects one of the ***validators*** to produce the next block. For a node to become a ***validator*** it should lock up their tokens (cryptocurrency) for a selected amount of time or own a determined number of tokens. The way validators are rewarded depends on the blockchain technology but usually, they are rewarded by the fees of the transactions stored on the block they just produced. This proof process is way more efficient than the Proof-Of-Work once it doesn’t require any kind of expensive problem solving by the validators.

4.3.3. Proof of Capacity

In the ***Proof of Capacity*** (POC) process each one of the nodes contains a set of solutions to complex puzzles and mathematical challenges stored in devices such as hard drives. These stored solutions can then be used to solve the puzzles and therefore, produce blocks. The users who have a higher number of stored solutions (higher storage capacity) and can find those solutions quickly enough will have more chances of producing the block. Usually, the nodes are rewarded by the fees of the transactions that were stored/processed by the blocks they just created.

4.3.4. Proof of Elapsed Time

The ***Proof of Elapsed Time*** is a proof process in which a node is selected to create a block by a process that chooses the node randomly considering the time that node spent waiting. The way this process is implemented is different from blockchain to blockchain but, usually, the network provides a random wait time to each one of the nodes that are part of that network. The node that is ready first, i.e., the node that had the smallest wait time will produce the next block.

For this proof to work efficiently, the network needs to assure that the wait time given to each one of the nodes is indeed random and that no users can run multiple nodes by themselves.

4.3.5. Proof of Identity

In the ***Proof of Identity*** process, the network will compare the private key of a user, that it already owns, and check if the identity of the user matches the identity attached to a specific transaction. Any user that can be identified by the network can create a block of data and present/send that block of data to any other user in the network. This type of consensus mechanism is used in prototypes of blockchains for smart cities, where the proof-of-stake mechanism can be used to verify the identity of the citizens.

4.3.6. Proof of Authority

The ***Proof of Authority*** consensus process is a variation of the Proof-Of-Stake process that aims to solve some of the later problems. While the Proof-Of-Stake algorithms assume that people who have more tokens locked up will be more motivated to act in the network's interest - because at the end of the day, they are the ones that have more to lose with the failure of the network -, it doesn't take into account that someone who locked up 50 tokens (and therefore is the one who invested more) is only investing 1% of their money, while someone who invested 40 tokens may be investing 100% of their money, and therefore has more to lose than the higher investor.

The ***Proof of Authority*** determines that to be a ***validator,*** instead of stake tokens, the users will stake their identity. That way, all the validators may put their reputation on the line to have the right to create new blocks in the blockchain. This model removes the potential monetary discrepancies between the validators and makes sure that everyone should be equally motivated to work for the network's success.

4.3.1. Proof of Activity

The ***Proof of Activity*** process is a mix between the Proof of Work and the Proof of Stake processes that try to combine the advantages of the two mechanisms and tries to avoid their weaknesses.

The first part of this algorithm works like in Proof of Work, i.e., the miners will compete against each other to generate a new block to the blockchain. The ones that can find the solution to the puzzle quickly enough will be able to generate the block.

The second part of the algorithm is similar to Proof of Stake. The participants are randomly selected considering the number of tokens they have locked up. The chosen participants (validators) will have the responsibility of confirming the validity of the generated block.

Once all the selected validators validated the block, the process is completed, and the new block can then be attached to the blockchain.

4.4. Protocols

A protocol is a set of basic rules that allow some process to work as expected under the conditions it was conceived to work in. Protocols are not exclusive to cryptocurrency or blockchain; a lot of protocols are used on the internet, for example, to make sure it will perform a certain task as expected or make sure it will comply with certain security requirements, etc. HTTP, for example, is a protocol used on our daily basis that stands for “Hypertext Transfer Protocol” and allows us to access websites and data available on the web.

With cryptocurrencies, it is no different, the protocols will establish the structure of the blockchain: how will the decentralized “database” work, which algorithms will be used to attest to the validity of the data, etc.

Since the creation of Bitcoin, a lot of different blockchains and cryptocurrencies were created. Each one of them has its own purpose and implements their own protocol, however, there are some “categories” of protocols. These categories were created taking into account similar points between all the different blockchains.

4.4.1. DeFi

DeFi is short for *Decentralized Finance* and, as the name indicates, this protocol defines a peer-to-peer set of financial services on public blockchains (mainly on Ethereum). With blockchains that implement DeFi protocols, their users can have access to a lot of operations that are supported by the traditional banks – earn interest, borrow currencies, trade currencies, buy insurance, etc. without having to deal with all the paperwork and without the costs that are usually associated with the traditional banking system.

4.4.1.1. Advantages of DeFi

The main advantage of DeFi blockchains is their ***speed*** as, unlike the traditional banks, it doesn’t require paperwork or a third party (bank manager, etc.) to handle the operations for us.

Another advantage of DeFi blockchains is its ***flexibility.*** The assets under DeFi blockchains can be moved anywhere at any time without asking for permission, waiting for a long time, or paying expensive fees.

4.4.1.2. Disadvantages of DeFi

Some of the main disadvantages of DeFi protocol is the ***fluctuation*** of transaction rates in Ethereum network. Once most of the DeFi blockchains are implemented on top of Ethereum network, those networks are bound to the transaction fees on Ethereum network.

When using DeFi blockchains, all the records for ***tax purposes*** must also be kept by the users of the blockchain, once there isn’t a professional doing that for us.

4.4.2. CeFi

CeFi stands for "centralized finance." The idea behind CeFi is to create crypto investment opportunities that offer some of the yield benefits of DeFi with some of the convenience and security of traditional financial-services products (also known as **TradFi**). **CeFi** allows you to earn yield via crypto-based accounts that are functional like a traditional bank's savings accounts but may offer higher returns. This account acts just like a normal bank account, where you can borrow money, buy, and sell crypto, spend and earn rewards with a crypto debit card, and more.

4.4.2.1. CeFi borrowing and CeFi lending/saving

As previously mentioned **CeFi** allows the users to borrow money against their crypto holdings, the same way nowadays we use traditional assets as collateral to apply for a bank loan. The users pay interest for borrowing money and this is how the yield is generated, furthermore **CeFi** loans typically require little or no paperwork. But be aware that **CeFi** lacks government-backed insurance.

4.4.2.2. Advantages of CeFi

- Boosted transaction processing
- Increased buying and selling processes (fiat-crypto trading)
- Support cross-chain exchanges of multiple cryptocurrencies
- Customer support available
- Easy to use

4.4.2.2. Disadvantages of CeFi

- Higher transaction fees due to third-party compliance
- Lack of control over funds
- Personal information necessary
- Lack of transparency

4.4.2.2. Risks of CeFi

Most of the risks associated to **CeFi** depend on the product and provider because each **CeFi** product is unique, and your holdings may be used in various ways, so it's important to do research before the use of **CeFi**.

Crypto deposits are not eligible for any government-backed insurance that protects savings held by banks.

CeFi providers could lock up your principal for some time.

4.4.3. Stablecoins

Stablecoins are a digital currency that is pegged to a “stable” reserve asset like the U.S. dollar or gold. **Stablecoins** are designed to reduce volatility relative to unpegged cryptocurrencies like Bitcoin, being more suited to everything from day-to-day commerce to making transfers between exchanges. They’re one of the most popular ways to store and trade value in the crypto ecosystem (example of a Stablecoin: USD Coin (USDC)). Operating on the Ethereum blockchain, Stablecoins inherit the following properties:

- Stablecoins are global, open, and accessible to anyone on the internet, at any time.
- They’re digitally native to the Internet and programmable.
- They’re cheap, fast and secure to transmit.

4.4.3.1. Advantages of Stablecoins

Stablecoins come with a digital, programmable, and blockchain-based nature. They are **safe** because of their **stability**.

One of the advantages of **Stablecoins** are the **borderless payments** since they can be sent via the internet with no regard for countries, banks, or any intermediaries, and these transactions are direct and immutable. They can’t be blocked or censored because they are carried out on the blockchain.

The lack of intermediaries and the peer-to-peer nature of Stablecoins make transactions a lot cheaper than traditional transactions of funds. Unlike regular bank transfers or credit card payments, which immediately charge you a certain fee and commissions, transactions carried out with Stablecoins incur a **minimal cost**.

Blockchain-based transactions are **faster** compared to traditional ones. The reasons for this are for verifications and anti-money laundering (AML) processes. As soon as the transaction is initiated, it usually takes minutes for the funds to hit the receiver’s account.

Stablecoins transactions are carried out on public blockchains. Users can monitor each transaction, regardless of whether they initiated it or not. This provides another level of **transparency**.

4.4.3.2. Disadvantages of Stablecoins

The principal disadvantage of **Stablecoins** is the **Centralization**, with the majority of the Stablecoins pertaining to an individual organization. This creates another form of authority, like what banks currently have, since a single entity controls its issuance and minted supply. Not all the Stablecoins are centralized (DAI), but most of them are.

Stablecoins are usually pegged to FIAT currencies, making their value depends on the current condition of the global economy and subject to inflation.

There is also a big lack of regulation for **Stablecoins**.

5. Social and economic impact of blockchain

5.1. Benefits

Blockchain promises a secure, peer-to-peer mechanism for verifying information. It provides the support necessary for the decentralized, anonymized tracking and transaction of digital currencies around the world.

However, block chaining has other applications beyond cryptocurrency. From insurance, real estate to crowdfunding and data management, it will continue to be adapted in many ways to the mainstream business world. Some of the world's emerging economies are benefiting from the integration of blockchain technology in several ways, such as banking and financial services, supply chains, agriculture, and managing land ownership records.

Supporters of blockchain believe that it could enhance the distribution of government services in many nations, help to provide identity services, and even help to enhance freedom of speech and anti-corruption activities as well.

5.1.1. Economic Benefits

Blockchain technology claims to speed up and reduce the cost of transactions and boost financial inclusion by providing more opportunities for those without easy access to financial services. Blockchain payments can also improve the efficiency of payment procedures for many businesses, such by getting rid of the payment delays and the time-consuming procedures of other outdated payment systems. With blockchain, instant, secure transactions can be an affordable alternative for many businesses.

On the other hand, blockchain can be used as a secure technology to make financial transactions without any unknown or undesired intermediaries. After all, conventional financial transactions are impossible without intermediaries (like banks) that are responsible for making sure that the money gets transferred to the chosen recipient. Like this, the process stays transparent to us, and we lose a great amount of control over the transaction. Blockchain proposes a great alternative to banks: one can send their digital payments from their virtual wallet to a recipient’s virtual wallet with the help of a set of digital keys.

5.1.2. Social Benefits

The adoption of blockchain technology can help to facilitate the delivery of public and government services, while dealing with elections, identity management, and taxes. Currently, the standards of identity management are different across the world, making the identification process long, inconvenient, and vulnerable. A combination of biometric technology and blockchain can replace the outdated identity management system.

Meanwhile, a growing problem in today’s digital age revolves around intellectual property. Many owners of digital work all over the world find it hard to protect their rights, as any work of art can be stolen, copied, and distributed by pirates. However, with blockchain technology, we can

find means to prove one's ownership and, at the same time, the authenticity and integrity of any given work found on the Internet.

Another social issue that can be solved with blockchain is the faulty or even fraudulent voting systems found in many countries (e.g., voting machine hacks, voting miscounts, and forced voting). A blockchain-based voting system has the potential to eliminate all these issues: when a vote is saved in the blockchain, it can be tracked in real time, and it can never be changed. This technology can eliminate the possibility of tampering in any election. By enabling blockchain-based voting solutions, the government could also protect the anonymity of the voter with transparent crypto algorithms.

5.2. Problems

For many years, the focus has been on the benefits of blockchain in various areas; however, now everyone's attention is turned to the various challenges and bottlenecks that are preventing the widespread adoption of blockchain.

These challenges can range from technical problems – such as immaturity (slow and cumbersome), lack of scalability, difficult integration with legacy system and complexity -, to social and environmental problems – such as security and privacy difficulties, high environmental costs and lack of regulatory clarity and good governance.

5.2.1. Economic Problems

The adoption process of blockchain technology comprises several phases, including design, development, implementation, migration, and maintenance. Despite the long-term benefits of blockchain, investment costs and development costs necessary to manage a blockchain system can quite high. This can outweigh the mentioned benefits, and, for many, it prevents the adoption of blockchain technology.

5.2.1. Social Problems

Blockchain has some fundamental privacy problems by virtue of its design, as it was designed to be publicly distributed: each node that processes transactions and builds the blockchain necessarily has access to the blockchain transaction data itself. Although the information is anonymized using blockchain wallet addresses as identifiers, the other details of a transaction are plain to see. A term we can use here is pseudonymity, which means that blockchain has "data points which are not directly associated with a specific individual, but where multiple appearances of a person can be linked together."

For example, many blockchain applications require smart transactions and contracts to be indisputably linked to known identities, and thus raise important questions about privacy and of the security of the data stored and accessible on the shared ledger (i.e., collection in which account transactions are recorded).

On the other hand, the decentralization of authority and the lack of regulations found in blockchain (even within blockchain transactions) mean there are no entities, regularity bodies or moderators to enforce law and order in the network.

5.3.1. Ambiental Problems

One of the major problems currently found in blockchain comes from the environmental costs the high energy consumption it engages in. As mentioned previously, blockchain is a system that sometimes uses a proof-of-work model to determine which node wins the right to confirm the next block in the chain (where nodes compete to solve a complex equation fastest), which has proven to be an extremely energy-intensive process.

As the network grows, the number of competitors increases, and there is a fight for more computer power, which consumes energy. The energy consumption is extremely inefficient because, in the end, just one node will win the right to confirm the next block. Although some solutions to this energy consumption have been studied (such as proof-of-stake protocols), there are still many challenges to face to minimize this problem.

6. Conclusions

Technological advancements take a long time to mature and reach a stable form that can be introduced into the market. Like any technological innovation, blockchain will follow the same, slow trajectory of adoption over the coming years.

While blockchain technology has its own set of problems, there is a lot of effort and dedication coming from many people who want to find the best solutions for these problems. Despite the challenges it currently faces, blockchain promises to improve the speed and security of many processes involving the transfer and storage of data – things highly valuable as the world and our lives keep getting increasingly digital.

As industries and technologies keep evolving rapidly, developers will find increased applications for blockchain technology, becoming a more prominent part of our daily lives.

7. References

Abderahman Rejeb, K. R. (2022). Barriers to Blockchain Adoption in the Circular Economy: A Fuzzy Delphi and Best-Worst Approach. *Sustainability*, 23.

Coinbase. (2022). *What is a blockchain?* Retrieved from Coinbase: https://www.coinbase.com/learn/crypto-basics/what-is-a-blockchain

Coinbase. (2022). *What is cryptocurrency?* Retrieved from Coinbase: https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency

Coinbase. (n.d.). *Coinbase*. Retrieved from What is CeFi?: https://www.coinbase.com/learn/crypto-basics/what-is-cefi

Coinbase. (n.d.). *What is a protocol?* Retrieved from Coinbase: https://www.coinbase.com/learn/crypto-basics/what-is-a-protocol

Coinbase. (n.d.). *What is a Smart Contract?* Retrieved from Coinbase: https://www.coinbase.com/learn/crypto-basics/what-is-a-smart-contract

Coinbase. (n.d.). *What is a stablecoin?* Retrieved from Coinbase: https://www.coinbase.com/learn/crypto-basics/what-is-a-stablecoin

Coinbase. (n.d.). *What is Bitcoin?* Retrieved from Coinbase: https://www.coinbase.com/learn/crypto-basics/what-is-bitcoin

Coinbase. (n.d.). *What is DeFi?* Retrieved from Coinbase: https://www.coinbase.com/learn/crypto-basics/what-is-defi

Coinbase. (n.d.). *What is Ethereum?* Retrieved from Coinbase: https://www.coinbase.com/learn/crypto-basics/what-is-ethereum

Daly, L. (2022, January 21). *What Is Proof of Work (PoW) in Crypto?* Retrieved from The Motley Fool: https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/proof-of-work/

GoodFirms. (n.d.). *Top 10 Problems that Blockchain Solves*. Retrieved from GoodFirms: https://www.goodfirms.co/blog/problems-blockchain-solves

IBM. (n.d.). *What is blockchain technology?* . Retrieved from IBM: https://www.ibm.com/topics/what-is-blockchain#:~:text=Blockchain%20defined%3A%20Blockchain%20is%20a,patents%2C%20copyrights%2C%20branding

Joshi, N. (2019, April 23). *8 blockchain consensus mechanisms you should know about*. Retrieved from Allerin: https://www.allerin.com/blog/8-blockchain-consensus-mechanisms-you-should-know-about

Kelleher, J. P. (2022, March 15). *Why Do Bitcoins Have Value?* Retrieved from Investopedia: https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp

Law360. (2019, January 14). *The Privacy Questions Raised by Blockchain*. Retrieved from Bradley: https://www.bradley.com/insights/publications/2019/01/the-privacy-questions-raised-by-blockchain

Levy, A. (2022, February 28). *5 Problems With Blockchain Technology*. Retrieved from The Motley Fool: https://www.fool.com/investing/stock-market/market-sectors/financials/blockchain-stocks/problems-with-blockchain/#:~:text=In%20big%20public%20blockchains%20such,their%20investment%20into%20computing%20resources

Meijer, C. R. (2020, February 29). *Remaining challenges of blockchain adoption and possible solutions*. Retrieved from Finextra: https://www.finextra.com/blogposting/18496/remaining-challenges-of-blockchain-adoption-and-possible-solutions

Naga. (2019, December 13). *Where Do Cryptocurrencies Get Their Value?* Retrieved from Naga: https://naga-global.com/blog/where-do-cryptocurrencies-get-their-value-10996744

Reiff, N. (2021, October 26). *How Blockchain Can Help Emerging Economies*. Retrieved from Investopedia: https://www.investopedia.com/tech/how-blockchain-can-help-failing-economies/#:~:text=Among%20its%20many%20advantages%20(first,easy%20access%20to%20financial%20services

Wang, K. E. (2021, August 19). *Types of Blockchain: Public, Private, or Something in Between*. Retrieved from Foley: https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between