LAB University of Applied Sciences

The viability of blockchains

LAB University of Applied Sciences
Bachelor of information technology (Double Degree Programme)
2022
Joan Sebastià Palop Gisbert

Abstract

Author(s)	Publication type	Published
Palop Gisbert, Joan S.	Thesis, UAS	2022
	Number of pages	
	79	

Title of Publication

The viability blockchains

Degree and field of study

Bachelor of Information Technology (Double Degree Programme)

Name, title, and organization of the client (if the thesis work is commissioned by another party)

Abstract

Blockchains are a new technology that has risen to a worldwide knowledge level in the past few years, and they have been anything but polarizing. A large group is defending them, praising their capabilities, and talking about the huge potential they can reach. At the same time, the rest insists that blockchains are unnecessary and that the problems they bring are more detrimental than the supposed benefits could attain.

This thesis aims to determine whether blockchains are a viable option in the future of technology or if they are a bust by tackling them from their core and inner workings up to the top, going through their history and current applications and situation to their security capabilities.

The analysis of the premise concludes that blockchains are a technology that can be used in many areas where it would not bring any meaningful improvements, instead of becoming more detrimental to it as the array of issues is not insignificant. They create many problems that they attempt to solve with little success and try to fix others that do not need fixing.

Keywords

Blockchains, Smart Contract, Cybersecurity, Cryptocurrency, Ethereum, DApps, Solidity, Environment

Contents

1 Introduction

Blockchain technology has made a very fast rise in terms of popularity these past few years, mainly propped up by its relation to cryptocurrencies as they are the technology they are built upon. With all the hype that has come it's way, a lot of misinformation and misconceptions about it have.

Still, blockchain technology has not seen great advances in the last few years that its popularity has risen. It has been at the same point of almost being completely mainstream but still lacking that last piece to make the final jump. There are many reasons why this is and has been the situation for blockchains. They bring many advantages to the table, but many are intertwined with other issues. Finding the balance between these two sides of the coin has been something that researchers working in the field have not been able to accomplish to this day.

This situation has brought the public to the point it is now, raising the question of if blockchains are really needed and if the advantages they provide outweigh the detrimental issues they bring with them. In order to make a statement on this matter, understanding blockchains is really important.

Understanding blockchain technology from its core to its applications is the focus of this thesis. It will go through blockchains history and present-day status and its main concepts and components to achieve this. Then, it will go through its most notable applications today: Smart Contracts and DApps to its security qualities and capabilities to, finally, its future perspective and viability.

2 Blockchains

2.1 Blockchains and their history

Blockchain is a technology that is usually associated with cryptocurrencies. The term blockchain originated in the way they work, where multiple blocks of information are linked, forming the chain, hence the name Blockchain. Specifically speaking, a Blockchain is a decentralized and distributed global ledger, like a database with its data distributed among many computers instead of storing it in one like it is usually done. (Elrom 2019,8; Shekhar Sarmah 2018,23*.)

Because a Blockchain is decentralized, there is supposedly no overarching institution or governing body that has control over or is involved in any way in managing the blockchain. Much of the appeal for the technology and its use in new fields came mainly because of this characteristic. There is no way to alter the contents of a blockchain once a transaction has been recorded and verified. No further changes like adding more blocks with information can be made unless the entire network agrees. (Elrom 2019,8-9; Benton & Radziwill 2017,4.)

As no commanding entity is involved in the blockchain, the network is operated by abiding by a specific rule set or policy agreed upon to create that blockchain. Each of the members involved in the blockchain is called a peer or node. (Elrom 2019,9.)

The history of blockchains can be traced back to some different points in time and is mainly tied with its most common usage until today: cryptocurrencies.

Beginning as early as 1975, reports were already indicating that the arrival of a paperless office was nearing. Then, in 1976 a paper on “New Directions in Cryptography” was released with a discussion on the distributed ledger. This is one of the core concepts behind blockchains, and how it works will be explained in the next section, but it is a record of transactions. (Benton & Radziwill 2017,3; Shekhar Sarmah, 2018, 23*.)

Following that, with the growth in the Cryptography field, the concept of Time-Stamping documents was presented by two researchers from Bellcore: Stuart Haber and Scott Stornetta. This is considered the origin of the core concept behind blockchains: every new movement and block added to the blockchain is pinpointed to an exact time. It is then impossible for the user to lie or try to trick the system into changing the date to a previous or later one than the one it is. This is incredibly important and is one of the main attractions that the technology of blockchains provides. They quickly made significant improvements to the technique because of its potential and made the breakthrough of being able to store

multiple documents onto a single block. (Benton & Radziwill 2017,3; Shekhar Sarmah, 2018, 23*.)

Another important concept that contributed to the creation of blockchain technology is Digital Currency, which came into the frame based on a model proposed by David Chaum. This then caused the appearance of Protocols like e-cash schemes that brought up double spending detection. (Shekhar Sarmah, 2018, 23*.)

Even if all these previous points contributed in some way or another toward the creation of blockchain technology, either providing a core concept or technique used by it, researchers like to award the invention of blockchain technology to Satoshi Nakamoto.

With the publishing of his paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System,” the concept of blockchain went from a primarily unknown one to being worldwide known. The article's focus was directly tied to the idea of conducting a direct online payment from one party to another without needing the oversight of a third one. It described an electronic payment that would be based on the concept of cryptography, one of the previously mentioned concepts. The paper also included a solution to the problem of double-spending, which was presented earlier. The proposed fix was a digital currency that would not be duplicated or spent more than once. The concept of the distributed public ledger where every transaction made could be traced back to a specific date and be confirmed if that coin was not spent before that time, which would also help solve the trouble that double spending could cause. (Shekhar Sarmah, 2018, 24*.)

Since the first Bitcoin network was released in early 2009, the rise of blockchain technology and other technologies based on it has been very prominent. As stated, their use in cryptocurrencies is the most known worldwide, but the possibilities and multiple proposals of new ways to use it or incorporate it into other products or services have been rising in the past years as well, as can be seen in Image 1. (Benton & Radziwill 2017; Shekhar Sarmah, 2018, 24*.)

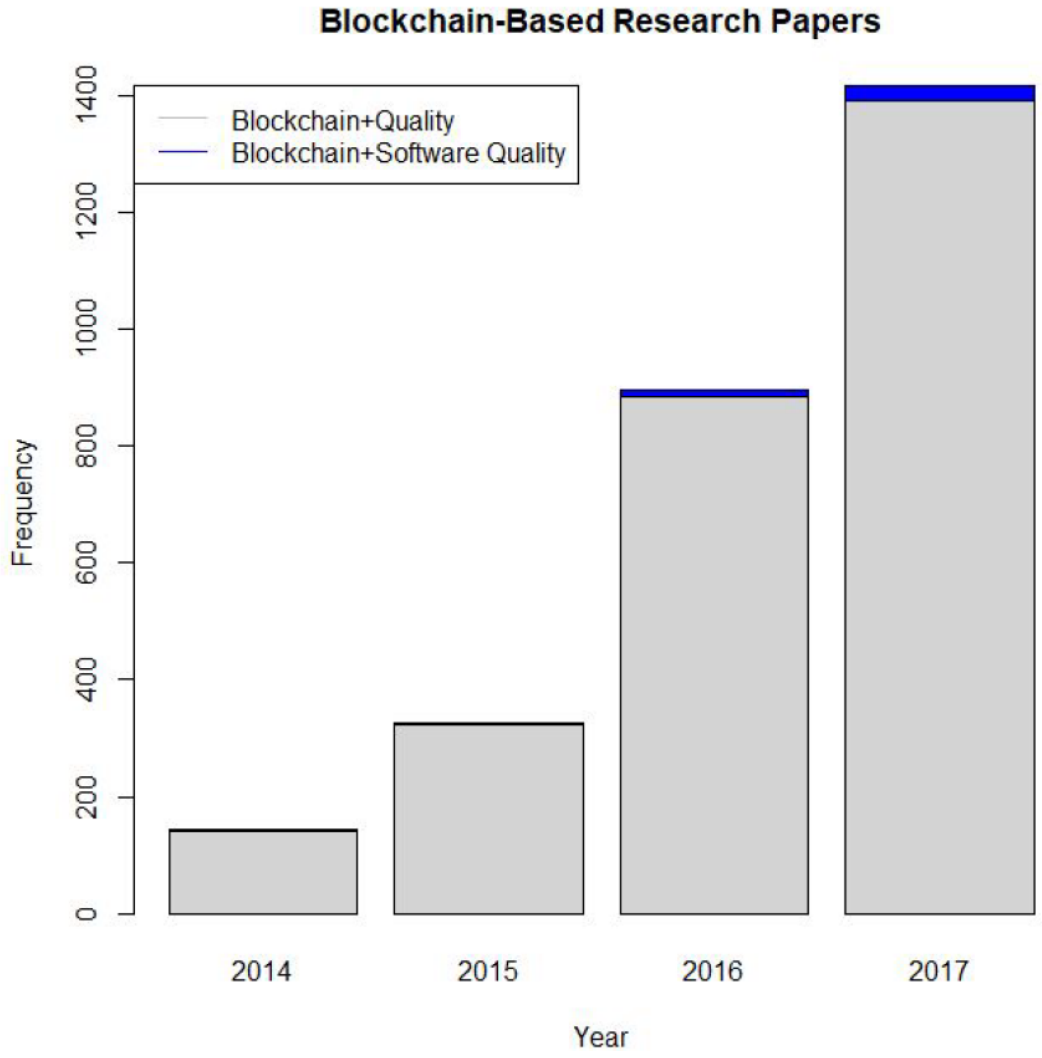

Image 1. The rise in popularity of blockchains from 2014 to 2017. (Benton & Radziwill 2017.)

The essential virtue of blockchain is the ability to automate mechanisms of trust without a central authority (like a central bank, government, or military), which mitigates risk, and enables all manner of efficiencies in human interaction whether in business or government contexts, whether formal or informal. (Benton & Radziwill 2017,3.)

In 2015 one of the most significant breakthroughs for blockchain technology happened: the launch of the Ethereum platform. This platform, loosely interpreted in Image 2 below, made the blockchains able to work with loans and contacts. Thus, the “Smart Contracts” were born, which will be explored more in-depth later. Because of the platform’s ability to provide a faster, safer, and more efficient environment, the technology became incredibly popular and accessible to more of the public that had been in the dark until then. (Benton & Radziwill 2017,3; Shekhar Sarmah, 2018, 24*.)

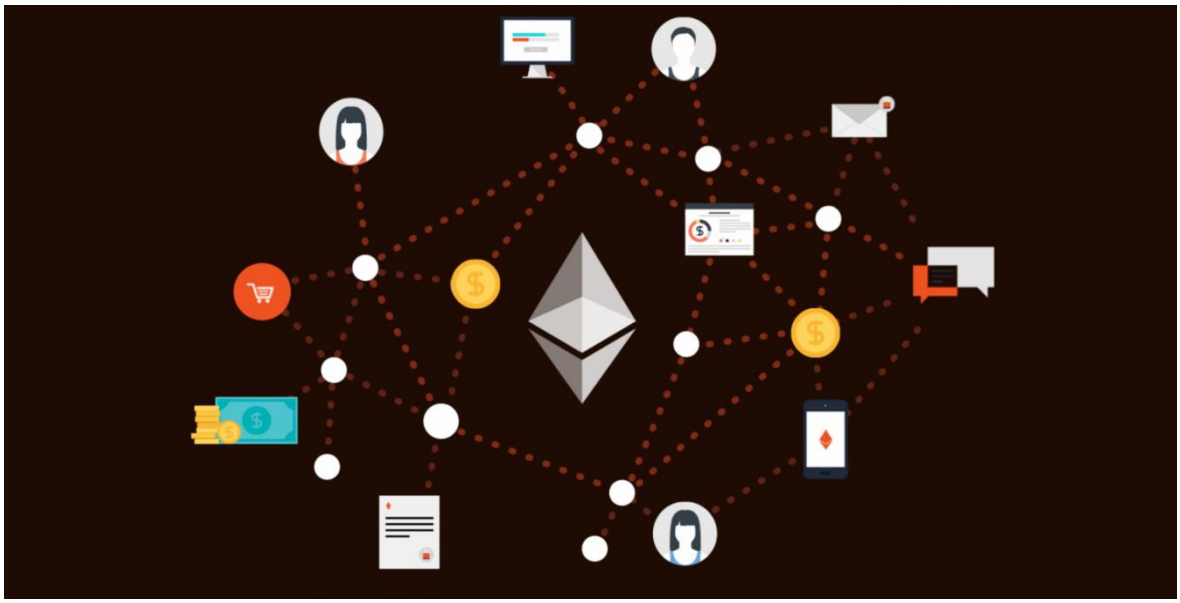

Image 2. A representation of the Ethereum network (Naydenova 2017.)

These are some of the many reasons why the concept of blockchains is incredibly tied to cryptocurrencies nowadays. It went into the spotlight with it, and it seems complicated to separate one from the other, but make no mistake, it is its most common use nowadays. The cryptocurrency market is incredibly huge and is growing more every day, with more corporations and the general public getting into it and trying to learn or take part in it. Still, the possibilities that blockchain technology promises to provide seem very promising and incredibly fascinating, from modifying the way current proceedings are done to enabling new and exciting ones that were not possible before this technology appeared.

2.2 Inner workings of blockchains

Understanding how blockchains work is essential to extracting the maximum potential out of the technology and forming an opinion about it. Seeing as new developers and researchers are looking into it every day, having a basic understanding of it will come in handy, as there might be a chance that the technology will find its way into your industry or field in one way or another. (Benton & Radziwill 2017,4.)

2.2.1 Transactions

A blockchain is a compilation of data, usually referred to as blocks linked to the previous one in the chain, hence the term blockchain. They are linked between them by referencing

the preceding block. Once a new block is added to the blockchain, a reference is made to that previous data and is kept that way forever, as can be seen in Image 3 below. (Elrom 2019,9.)

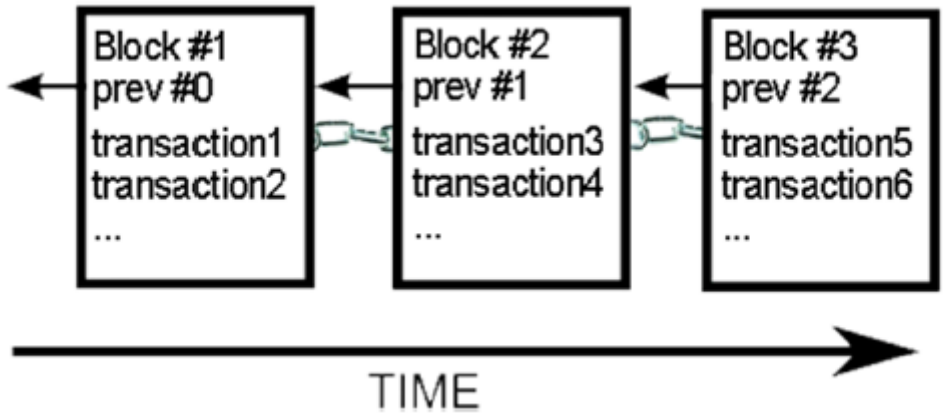

Image 3. A representation of blockchain. (Elrom 2019,10.)

A transaction inside a blockchain is the interaction between two nodes in the network. This interaction can be a cryptocurrency transfer or a recording of some type of file inside a block. Each block can contain none or many transactions. In many blockchains, the constant addition of blocks is a usual practice so that the malicious users are never able to catch up and create a blockchain with their altered blocks. These additions are made of blocks that can be empty of transactions as well. (Yaga et al. 2018,9.)

Even if the data for every transaction is largely different depending on the purpose of the blockchain or the users, the methods for materializing that transaction stay mostly the same throughout various kinds of blockchains: The user sends the information through to the blockchain network. This information may contain several fields depending on what is being sent, like the sender's address or other ways to identify itself, their public key, a digital signature, and transaction input and outputs. (Yaga et al. 2018,9.)

As can be seen in Image 4 below, these inputs are usually a list of the digital assets that are going to be transferred to the other party. The transaction must reference the source of the digital asset and prove that they have access to the private key, verifying that they effectively have access to that asset. This is where the digital signature comes in. As the sender signs the transaction, they prove their access to the private key. (Yaga et al. 2018,9.)

The outputs are usually the address of the recipient of the digital assets along with how much of that asset they are to receive. (Yaga et al. 2018,10.)

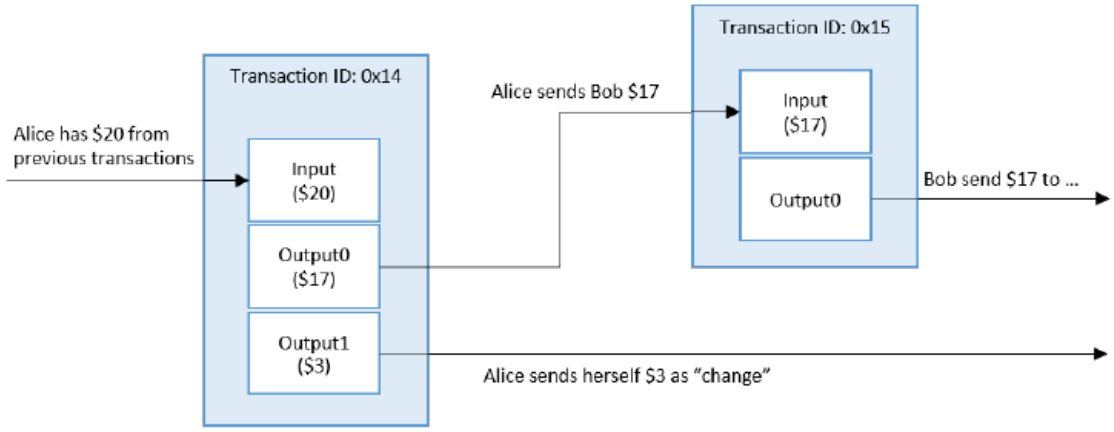

Image 4. Example cryptocurrency transaction between two parties. (Yaga et al. 2018,10.)

Transactions are mainly associated with cryptocurrencies, as is the case in many concepts of blockchains. Still, they can be used to store data publicly and have it stored there forever, for example, using the transaction to transfer data. Other ways in which transactions are used are through the concept of smart contracts, where transactions can be used to send data, process it, and store that result on the block. Therefore, smart contracts are among the most powerful tools that can be utilized on blockchains and will be looked at later. (Yaga et al. 2018,10.)

Of course, one of the critical matters that arise is checking the credibility and verifying each transaction that is done, ensuring that the terms of the blockchain network are met. Checking if the transaction is authentic is one of the most important concepts of how the blockchain works and will be explained later.

A ledger is merely a record of transactions, and it is a concept that has been around for a very long time. They used to be written with pen and paper until modern times, and now they are stored in a database owned by the owner of that ledger on behalf of the clients. The possibility that blockchains offer is the decentralized ownership of these ledgers, which is a concept that is being looked up these times, as many concerns come up in the use of the traditional centrally owned ledgers like the lack of trust, security, and reliability of those ledgers. (Yaga et al. 2018,13.)

Most of these concerns can be fixed by using distributed ledgers via the blockchain technology: Ledgers that are centrally owned may be damaged or completely lost if there is an attack and the responsible party for the ledger does not have a backup, while blockchains are distributed by design and have many backup copies synced. Every user can keep their copy of the ledger so that it can be restored in case one peer loses the data, and it is imperative that a user must always have the complete blockchain stored because of how

the protocol works when new peers enter the network. All this makes the loss of the ledger very hard, if not almost impossible. (Yaga et al. 2018,14.)

Other concerns on the security side of centrally owned ledgers are that an attack on one part of the ledger will take down the whole system if it ends up being successful, as there is a high chance they are stored on a homogenous network. Blockchains prevent this because they are a heterogeneous system, where each node is different from the other, effectively reducing the chances that an attack succeeds by a considerable amount. This concept applies to the potential of having a problem in the system where the centralized ledger is stored. If there is a power outage or technical issue of some sort, the whole network could become unavailable. The chances of that same event happening to all the blockchain network nodes are meager. (Yaga et al. 2018,14.)

Lastly, one of the more common concerns is the transactions happening on the ledger. When doing a transaction on a centrally owned ledger, the user has to trust that the overseeing party is checking and verifying every transaction. In a blockchain network, all transactions must be verified by all the other nodes, as is shown in Image 5 below. If a transaction is not valid, the other nodes will detect it and reject that transaction. Another concern of this kind is related to the transaction list, which, once again, the user must trust the owner to keep up to date with all the valid transactions and not alter their contents. In a blockchain, every valid transaction is recorded and stored on the blocks, which can be checked after the fact and kept with the timestamp present for as long as the blockchain is standing. If a node would not reference all the previous transactions and the previous block, or it changed the data, the rest of the network would reject it once again. (Yaga et al. 2018,14.)

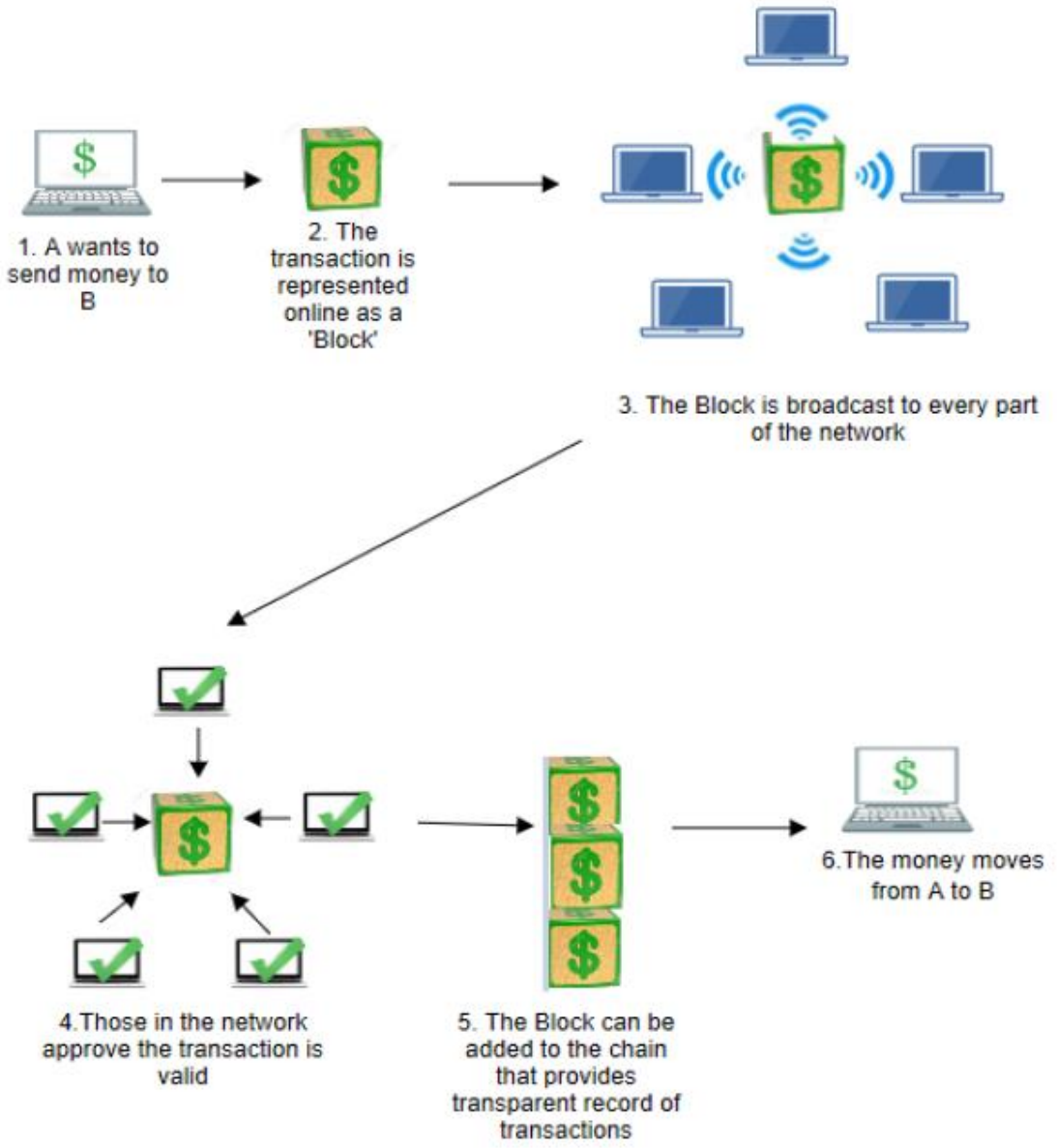

Image 5. How a blockchain works when conducting a transaction. (Shekhar Sarmah, 2018, 25*.)

The last concern arising from having a centrally owned ledger is privacy. If there is a breach in the system, the attacker could steal personal and other sensitive data from the users and the organization. This means that the user once again has to trust the governing party to keep the system updated and have the right security measures to avoid these attacks. Blockchains bypass this problem simply because of their nature and how they are designed. As they are distributed, the point of attack that exists in the case of a centralized owned ledger is nonexistent. Even though information on a blockchain is usually public and has nothing of value to steal, there could be a case where the network is privately owned by an

organization, or the attacker could be looking to attack the users. Attacking the blockchain itself would be useless as the rest of the nodes would resist the inclusion of a fraudulent node, and if a single node is found to be out of date, only that node would be affected, not the whole system. (Yaga et al. 2018,15.)

2.2.2 The block

A usual representation of a blockchain is done by providing an image of a vertical stack, showing all the blocks pertaining to the blockchain stacked on top of each other. This representation is very clever in showing the “height” of the blockchain, which is the distance between the base block or the origin, and the last block added up until that point to the blockchain. Another way to represent a blockchain is as in Image 6, where blocks are laid out horizontally and linked with each other. (Antonopoulos 2017,195.)

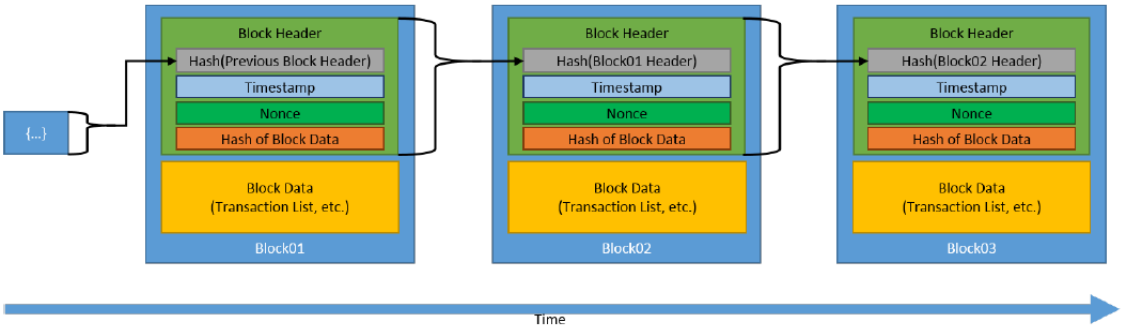

Image 6. A generic chain of blocks with their fields exposed. (Yaga et al. 2018,17.)

Each block pertaining to a blockchain has an identifier, a hash number generated when the block is created by the SHA256 cryptographic hash algorithm. This number is then stored on the header of the block. This is the way each block is linked to the previous one that came from the chain via the “previous block hash” field present in the block's header. This field contains the hash of that previous block or parent block inside its header. The sequence of hashes creates the link between all the blocks that compose the chain up until that first block, usually denominated genesis block. (Antonopoulos 2017,195.)

Each block has just one of the “previous block hash” fields, as seen on Image 6, as it can only ever have a single parent, but there are some cases where a block will have multiple children. This case only happens when multiple blocks are getting created and discovered simultaneously; this event is called a fork. The conflict is resolved eventually when only one of the children's blocks becomes part of the blockchain. (Antonopoulos 2017,195.)

One of the key features of blockchains and their security comes from the concept of having links between these blocks. As they are a field inside each block’s header, it also affects

that block's hash code. This means that the block's hash is calculated using the parent's one, and so when the parent's hash changes, the children's does as well, as well as the children of the children, and so on. This cascading effect through all the blocks ensures that once a block has a lot of generations beneath it, all the hashes pertaining to those blocks would need to be recalculated. The cost of doing so in a huge blockchain is humongous, so it ensures that once a blockchain is very long, its deep history is immutable, which provides security. (Antonopoulos 2017,196.)

A block has a structure composed of 4 parts, some of which are of fixed size and others depending on the block. First is the Block Size, a 4-byte field that contains the block's size in bytes from the end of the field onwards. The second is an 80-byte field and is the Block Header, which consists of three sets of metadata: (Antonopoulos 2017,196.)

The first is where the reference to the parent block is stored, a 32-byte hash of the previous block on the blockchain. (Antonopoulos 2017,197.)

The second set consists of three 4-byte fields that are: The Timestamp, which keeps the approximate creation time of the block, the Difficulty Target, which is the Proof-Of-Work algorithm difficulty target for this block and the Nonce, which is a number that is used only once in combination with the hash and data to produce a digest hash number that will change every time with the change on the nonce number, this is specifically used in conjunction with the Proof-of-Work algorithm to keep changing the digest values but keeping the same data. The Proof-of-Work algorithm is an algorithm used in many blockchains as part of the consensus model of the same name, which aims to add a new block to the blockchain every 10 minutes. To achieve this goal, the algorithm changes the difficulty of mining the new block depending on how fast it is being done by the miners. If they add new blocks too fast, the hash computations will get harder and harder. If the contrary happens, they get easier every time. (Antonopoulos 2017,197; Yaga et al. 2018,9; Daly,2022)

Lastly, the third set consists of the Merkle tree root, a 32-byte field essential for verifying the block's data. "*It is the hash of all the hashes of all the transactions that are part of a block in a blockchain network"* (Jake Frankenfield,2021).

They are used to make sure the data blocks sent between all the nodes of a blockchain network are not modified and undamaged. This works because the Merkle Tree enables the quick verification of data and the fast and secure mobilization of a significant amount of data from one of the nodes to the other. This is because every transaction in a block has a hash code associated with it. Each new hash for every new transaction stored onto that block is stored in a tree-like structure, specifically a binary tree structure. This way, each hash is stored and linked to its parent. Since transactions are stacked on the same block,

these are also hashed, resulting in a Merkle Root. Thanks to the tree structure, the Merkle Root, which contains each of the hashes stored on that block, provides a hash value that can validate everything present on that block. This way, only that transaction hash, and the sibling node, if it is existent on the tree, are needed to be verified in order to proceed upwards, repeating this step until reaching the top of the tree, speeding up the verification and transactions by reducing the amount of hashing needed to be done. (Jake Frankenfield,2021.)

This is what happens in image 7, as in order to verify the node “Hk,” only the hashes of the nodes shaded in blue will be needed. For any node to prove that “Hk” is indeed part of the Merkle root, with those four hashes as a path, it will do so by computing four additional pairwise hashes, which would be “Hkl,” Hijkl,” “Hijklmnop,” and the Merkle tree root, all rounded in dashed lines.

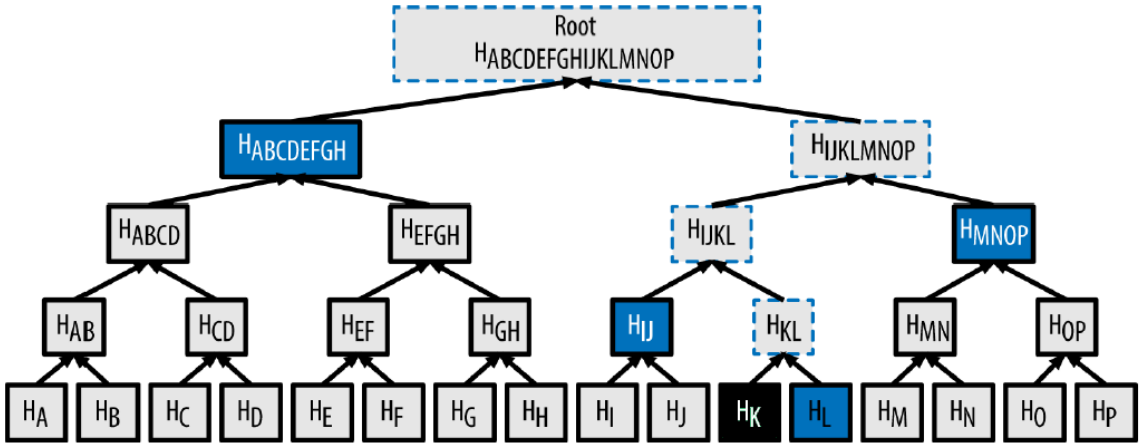

Image 7. A Merkle tree showing the necessary hashes to verify an element. (Antonopoulos 2017,202.)

The last field that compromises the Block Header is a 4-byte field that contains the version number used to indicate software or protocol updates. (Antonopoulos 2017,197.)

After the Block header, there is a field that ranges from 1 to 9 bytes that counts how many transactions follow inside the block. (Antonopoulos 2017,197.)

Lastly, the transactions are stored on the body of the block. The size of this field is highly variable depending on the number of transactions stored on each block. (Antonopoulos 2017,197.)

As has been referenced many times, the hash of each block is one of the essential pieces that keep the blockchain together and give it its characteristic structure. The block identifier is created by hashing the block header twice through the SHA256 algorithm. This returns

the block header hash, a 32-byte hash that receives its name as it is computed using just the block header. (Antonopoulos 2017,197.)

The block hash identifies a block uniquely and unambiguously and can be independently derived by any node by simply hashing the block header. (Antonopoulos 2017,197.)

This hash is not included in the data structure, neither once it is created nor when it is being transmitted through the network. It is calculated by each node and transmitted as it is being received from the network. The block hash is only stored in case it is needed for faster lookup and extracting from the disk. (Antonopoulos 2017,198.)

There is a second way of identifying a block inside a blockchain, its height. The height of a block is determined by its position inside the blockchain, considering that the origin or genesis block is at height 0. Each block stacked upon each other adds another step in height. (Antonopoulos 2017,198.)

Identifying a block with height might not always be the best though, as it is not a unique and ambiguous identifier like the block hash is. Even though every block will have a fixed height on the blockchain, and it will never change, it might not be unique to that one block. Multiple blocks could be competing for the same height competing for the same position, which is what happens when forking occurs. Apart from this, the block height is also not a part of the block's data structure. Even though it might be stored in another database for faster search and retrieval purposes, the height of a block is calculated dynamically when the block is received from the network onto a new node. (Antonopoulos 2017,198.)

2.2.3 Mining

All the blocks of a blockchain are encrypted using public-key cryptography, which is a method that has existed since the 1970s and is used in a large amount of security matters on the internet today. A pair of keys will be created for any blockchain user, one public and one private. Both keys will be needed to decrypt the information received. Still, the public key is the one that will be shared with the other members of the blockchain and will be used in order to encrypt any information that is directed toward the owner of that same public key. The users' keys are also used to sign a contract or transaction. This is done because the signature is not only based on their keys but on the signature that corresponds to the top block of the blockchain, so once that contract has been signed, it is verified by the rest of the users, and the content is able to be added to the new block. (Benton & Radziwill 2017,6.)

Once a new block is added to the blockchain, all the previous transactions that were before the creation of that one are organized and packed on a new block, and the rest of the users should be able to verify the contents stored, as well as determine which signatures were used on that new transaction. (Benton & Radziwill 2017,6.)

All this process makes it so that if anyone tried to access earlier entries on the blockchain to modify them, the whole network would notice and try to stop the attempt. This is one of the security traits that blockchain technology possesses. And, as the blockchain grows, there is more and more need for storage space and more computational cost to add new blocks and store the blockchain itself, as mentioned before. This all leads to the point of discussion, which is where blockchains are today, which will be expanded later. Overall, the environmental concerns and lack of scalability for the technology are hot talking points focused on and researched to make the technology sustainable for the future. (Benton & Radziwill 2017,6.)

Because creating new blocks and contributing to the blockchain is so costly, some mechanisms help give incentives to those miners who want to contribute. The mechanism in case is a reward system that rewards the miners who respect the rules set by the creator of the blockchain. Trying to cheat the system proves to be more detrimental to yourself than being a good user and following the rules, as it will provide you with more profit. In the case of Bitcoin, there has always been a reward for any user that provides computing power in order to create a new block. The reward is some Bitcoin in return, the amount has been lowered throughout the years, but it is still a significant amount. This is where the Proof-of-Work consensus model comes in once again, as the evidence of having mined that new block is part of how it works: Since checking if the new block has been created requires an extra of computing and processing power, the way PoW works is that the user that publishes the next block does so by being the first that can completely solve a very computationally intensive and expensive puzzle. This puzzle is explicitly designed to be very hard and intensive to solve but checking if the answer is correct is relatively easy. This way, the rest of the nodes pertaining to the network can quickly validate that proposed block. (Benton & Radziwill 2017,7; Yaga et al. 2018,19.)

Consequently, any block that did not pass the test and was not verified by the rest would be discarded. By doing this, the miners are rewarded for contributing resources, and they keep on collaborating in creating new blocks for the blockchain. As discussed previously with the Proof-of-Work algorithm, the difficulty is adjusted dynamically so that a new block is added with at least ten minutes in between. (Benton & Radziwill 2017,7; Yaga et al. 2018,19.)

This process is perfect in keeping the miners participating and ensuring that the blockchain continues to grow, but as mentioned, it is very environmentally unsustainable. Using proof-of-work as a means of evidence to demonstrate that you mined a block means that the cost of mining that block is directly tied to the electricity and power that is needed to keep the servers that were used to mine that block running, which in turn means that the fossil fuel power used to do that is included in the equation as well. If blockchains are to move forward, the research located towards finding new ways to verify the mining, like Proof-of-stake, is vital and will play a significant role in the sustainability of the technology. (Benton & Radziwill 2017,7.)

As specified, blockchains exist with and make use of computer networks. It would be impossible for the nodes to be connected otherwise and for the distributed ledger to be maintained and distributed. The internet is the most used network, but the possibility of using alternate options, such as private networks inside of a company, or using other methods such as VPNs, is not out of the cards. This comes with other disadvantages, as some corporation or other entity could field a large amount of computational and processing power to mine endlessly and make it impossible for other entities to mine on that blockchain. (Benton & Radziwill 2017,7-8.)

2.2.4 Categorization and types of Blockchains

Blockchain networks can be differentiated depending on the way their permissions work. If a blockchain is permissionless, anybody can create a new block and add it to the chain, and everybody can participate and collaborate. On the contrary, if a blockchain is permissioned, only a particular set of users can enter and add new blocks to that blockchain. It is a more private and controlled environment that might be seen more inside corporations or other organizations that need their blockchain to be confidential. Knowing the difference between these types and which type of blockchain you are working on is essential as it greatly affects other aspects of blockchains. (Yaga et al. 2018,5.)

Permissionless blockchains are open to anyone who wants to publish new blocks, record transactions, or read the history of that blockchain. They are often open-source software that is open to download to anyone. This opens the door to users who might want to take advantage of this fact by negatively affecting the system. In order to prevent this kind of behavior from users and promote the creation of new blocks correctly, consensus models like the previously mentioned Proof-of-work and Proof-of-stake are implemented in order to prevent these malicious users from publishing new blocks, as it would take more resources to do so. (Yaga et al. 2018,5.)

On the other hand, permissioned blockchains are the ones where the access is limited and controlled by some authority, be it centralized or decentralized, and they can control which users of the network can do any action. There might be a case where the oversight only allows a specific set of users to read the blockchain, other instances in which everyone can read but not write, etc. The only constant is that the party that oversees the blockchain controls who can access the blockchain in any way be it reading the history or adding a new block. (Yaga et al. 2018,5.)

Permissioned blockchains retain a lot of the properties of the permissionless kind while taking advantage and getting rid of many of the mechanisms used to preserve the other type. They use consensus models for the publishing of new blocks but are able to bypass the need to expend resources when doing so. This is because to be a user inside this network, your identity has to be verified beforehand, and every user present can supposedly trust the others, as the privilege of being part of the blockchain could be revoked if there is misconduct or they are found to be trying to either cheat the system, insert new blocks with malicious intent, amassing resources and so on. This leads to these consensus models being generally faster and lighter on the computational cost side of things for permissioned blockchains. (Yaga et al. 2018,5-6.)

Permissioned blockchains offer other possibilities as well. They offer organizations the possibility of having their private blockchain and implementing tighter measures to protect their data, as well as enabling collaborations with other organizations that might not be entirely trustworthy. Once an agreement is reached between the parties on the consensus model to be used, they can invite other business partners that can then use their distributed ledger to record transactions or any other use they might find suitable. If a single organization is controlling the blockchain, the trust between that organization and the users of the blockchain is necessary for it to work. (Yaga et al. 2018,6.)

Another characteristic that permissioned blockchains have is that they enable the possibility of choosing which transaction details can be revealed depending on which user or credentials that user has. This can allow a certain level of private transactions inside that chain, meaning that the transaction is visible to every member of the network, but the details of the said transaction are only visible to the involved parties. (Yaga et al. 2018,6-7.)

Another kind of blockchain is the sidechains or pegged sidechains which are blockchains where the digital assets can be moved from one to another. Inside this, there are two types: one-way and two-way, depending on if the movement is allowed just from one blockchain to the other or if the movement goes both ways, respectively. (Shekhar Sarmah, 2018, 26*.)

Lastly, these two kinds of blockchains are opposite each other: Tokenized and Tokenless blockchains. Tokenized blockchains are the standard, while tokenless blockchains lack the ability to transfer data and assets. Even though they can not transfer data they can still prove useful when it is not needed to do so, for example, when there is only a need to transfer data between trusted parties. (Shekhar Sarmah, 2018, 26*.)

2.2.5 Common myths and limitations around blockchains

The incredible amount of interest and hype of being a rising technology has not escaped the blockchains at all. It happens with many technologies that see this kind of meteoric rise to worldwide status. Many organizations will launch projects and new initiatives that have a focus or make use of the blockchain technology even if it is not needed for that case precisely just because it is the new thing, and they do not want to miss out on it or be behind the competition. This has led to many misconceptions and myths surrounding blockchains.

The first misconception that has formed around blockchains is the immutability that they have been assumed to have. The fact that they are entirely immutable is not wholly accurate. There can be cases where the blockchain can be modified. These cases present themselves in the event of adding new blocks to the blockchain. In some blockchains, the last blocks added to the blockchain or tail blocks are subject to being replaced, and, in most cases, the blockchain implementation will choose the longest chain as the correct one when multiple chains are competing for the spot. This can cause the transactions pertaining to the discarded blocks to be put back onto the pending transactions pool or to be included in a different block. This is why most blockchain users prefer to wait for a few blocks before determining a transaction is verified. (Yaga et al. 2018,34.)

This weakness can be exploited in permissionless networks by using the attack commonly known as the 51% attack. This attack will be expanded upon later, but it is an attack where the offender gathers many resources dedicated to creating new blocks, specifically 51% of those resources, to garner the majority of those and make a change inside the blockchain. This attack is not very hard to carry out, but it is costly, and it scales the more profound the attacker wants to get into the blockchain. (Yaga et al. 2018,34.)

This attack can be easily stopped in permissioned networks, though, as the owner's control over the users is tight. They can force the users to publish nodes in a fair manner by reinforcing that their publisher status will be removed if they disobey or cause trouble so that a situation where there are many competing chains does not arise. This control is handy to

prevent malicious behavior, but it can also allow the owner to replace any number of blocks using legitimate methods. (Yaga et al. 2018,34.)

One of the other misconceptions that have arisen is the usual catchphrase that many people use to sell the blockchain technology to those who don't know much about it or are trying to get into it, which is that no one is controlling the blockchain, no leadership or governing body. This is simply untrue, as has already been explained: Permissioned blockchain networks have a governing party that sets the rules and controls the blockchain network and its users. Even permissionless networks are governed by their users and the developers that created them in the first place. In both cases, a group has a certain amount of control over the network.

Software developers always keep some control over the blockchain network as their software is the one used to compile and create these blockchains. Even if some users might try to enter the code and create a different variation, most of them will not be able to do so and will be stuck with the version the developers put out, leaving them with some power for however long the blockchain lasts. Because of this, they are also held accountable when something goes wrong with a new update. These new updates are usually consulted with the network users before being sent online, and users can opt out of having them if they desire to do so. This can result in forks created by having the old and new versions separated in two chains that stay like that until all the users have adopted the latest version, which is what happens in Image 8. Therefore, there is a long discussion period before doing these updates. This dynamic changes significantly in permissionless networks as the nodes can adopt the changes done by the publishing nodes but are not required to do so. This, in turn, puts the power on to the publishing nodes, which can choose to marginalize a part of the user base which might not agree with the changes by forcing them to get them if they want to stay on the main fork and not be in their own. (Yaga et al. 2018,35.)

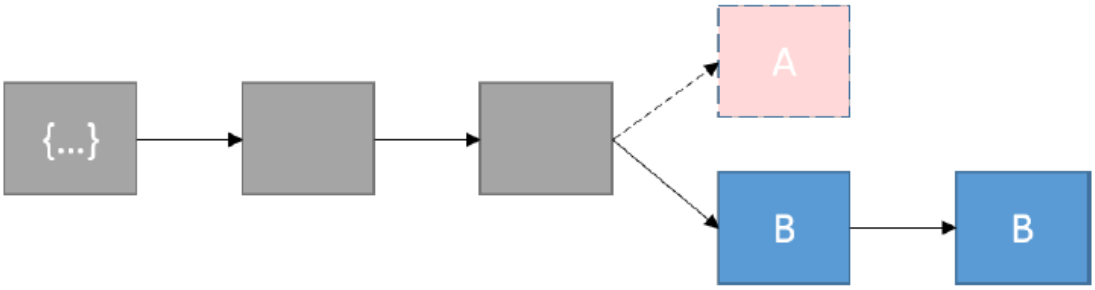

Image 8. A fork happening and getting resolved on a ledger. (Yaga et al. 2018,28.)

Another problem that has arisen as blockchains have evolved is the 'Oracle Problem' which refers to the fact that there are no reliable ways to transmit data beyond digital and store it

on a blockchain. This is not a problem specific to blockchains, general real-world data is tough to get in an accurate and verified way, and some blockchains might require the acquisition of that kind of data which is not possible as of now. Many projects have tried to tackle this problem by providing data in a blockchain in readable byte/opcode so that it is reliable, but it is still a work in progress. (Yaga et al. 2018,36.)

The death of a blockchain is one of the limitations it might have, even if it is something that may never happen, as the chance that some of the nodes that used to be part of one are still running is very high. In that case, the defunct blockchain would not be suitable to be used for any kind of historical record as any attacker would have an easy time replacing any blocks he desired as the few publishing nodes left would not be enough to stop it. (Yaga et al. 2018,36.)

One of the most significant limitations blockchains suffer is controlling their users. It has already been stated how blockchains try to incentivize users to keep building and maintain exemplary conduct while using the network, such as rewards and punishments for not following the rules, but, especially in the case of permissionless blockchains, the threat of malicious users trying to cheat the system and take advantage of those rewards, for example, cannot be ignored. Still, it is tough to get an attack to work as the resources to gain enough power to do it are enormous. Apart from having malicious users inside the blockchain, the overseeing organization or party responsible for managing the network might also have malicious intent, which in this case is much harder to contain. (Yaga et al. 2018,38.)

Following the list of significant concerns is one of the bigger and most talked about ones present: the energy the technology requires to function. In most cases, the resources needed to keep a blockchain running, doing all the operations usually done on them, and adding new blocks and transactions are not negligible. The figures are reaching record highs every year as more and more blockchains appear and those already present continue to grow. Most of the energy waste comes from the operations done to solve the necessary puzzles the nodes are presented with because of the proof-of-work system currently used in most blockchains. Therefore, it is a big talking point and one of the main concerns moving forward.

The last misconception that is usually talked about is identity verification on blockchains. Signing a transaction done on a blockchain links that same transaction to the corresponding owner of the private keys but is in no way associated with the real-world identities of the users. As of now, there are no facilities whatsoever that can link identities to the private keys used to operate on the blockchains. But there are many other ways of connecting or

linking your identity to a blockchain. For example, having your wallet address on your webpage can be considered a way of doing so as your address would then be directly linked to your real-world identity, but blockchain implementations are not designed with the goal of identity management in mind. (Yaga et al. 2018,40.)

3 Current situation of blockchains

3.1 Blockchains now

The current situation of blockchains is at an interesting point. It feels like it has been at a tipping point from being a widely used technology for a few years now. It has been stuck on that same spot of almost making the jump for these past years. The unprecedented rise of cryptocurrencies brought it into the spotlight and separating both terms has been hard. Still, it is apparent that, at least in these last few years, it has started to drift away from being exclusively tied to them and has started to find its footing.

Blockchain's most popular current application is in cryptocurrencies. It is the technology supporting the groundwork for them, providing an infrastructure where the trading and mining of the coins is possible. Since its launch in 2009, it has been the most popular use by far and the one most people know it for. So, as cryptocurrencies already have more than a decade of study and experience, blockchains are not the same. Even if they have been the supporting technology for them, they are still in a phase where there is a lot to learn about them and the possibilities they offer, which is where most of the hype surrounding the technology comes from. It promises to provide a lot of options in many fields, create a lot more jobs and even improve the global economy. So, seeing the potential, questions arise as to why more organizations have not tried to tackle it and use it for their purpose. (Ismail,2021.)

Many organizations have indeed tried to see what it is about this technology and have put resources into researching how they could use it. Huge companies like IBM, American Express, and UNICEF have all been exploring blockchain applications in their fields. Some estimate that the use of blockchains as a service will be an industry more than double what it is today. (Malkov,2021.)

The key to the enterprises that try to get into the technology is finding the feature that helps their case. Blockchains, as of now, are not able to provide a solution or improvement for general use. They are more suited to doing so for more specific areas inside a business or field, so organizations that want to use them should thoroughly research their operations and find which benefits of using blockchains could provide them with the best improvement. (Baker,2021.)

This is very apparent in this survey done in November 2019 conducted by Forrester Research which was commissioned by EY. After delivering the results, shown in Image 9, the EY U.S. blockchain practice leader released a statement analyzing the results: (Baker,2021.)

"Preservation of data integrity was the number one driver and most common use case for blockchain adoption. About half of all the respondents said they prioritize use cases that would improve efficiencies and enable new revenue models like supply chain track and trace, payment support processes and digitization of document flows." (Zur, 2019.)

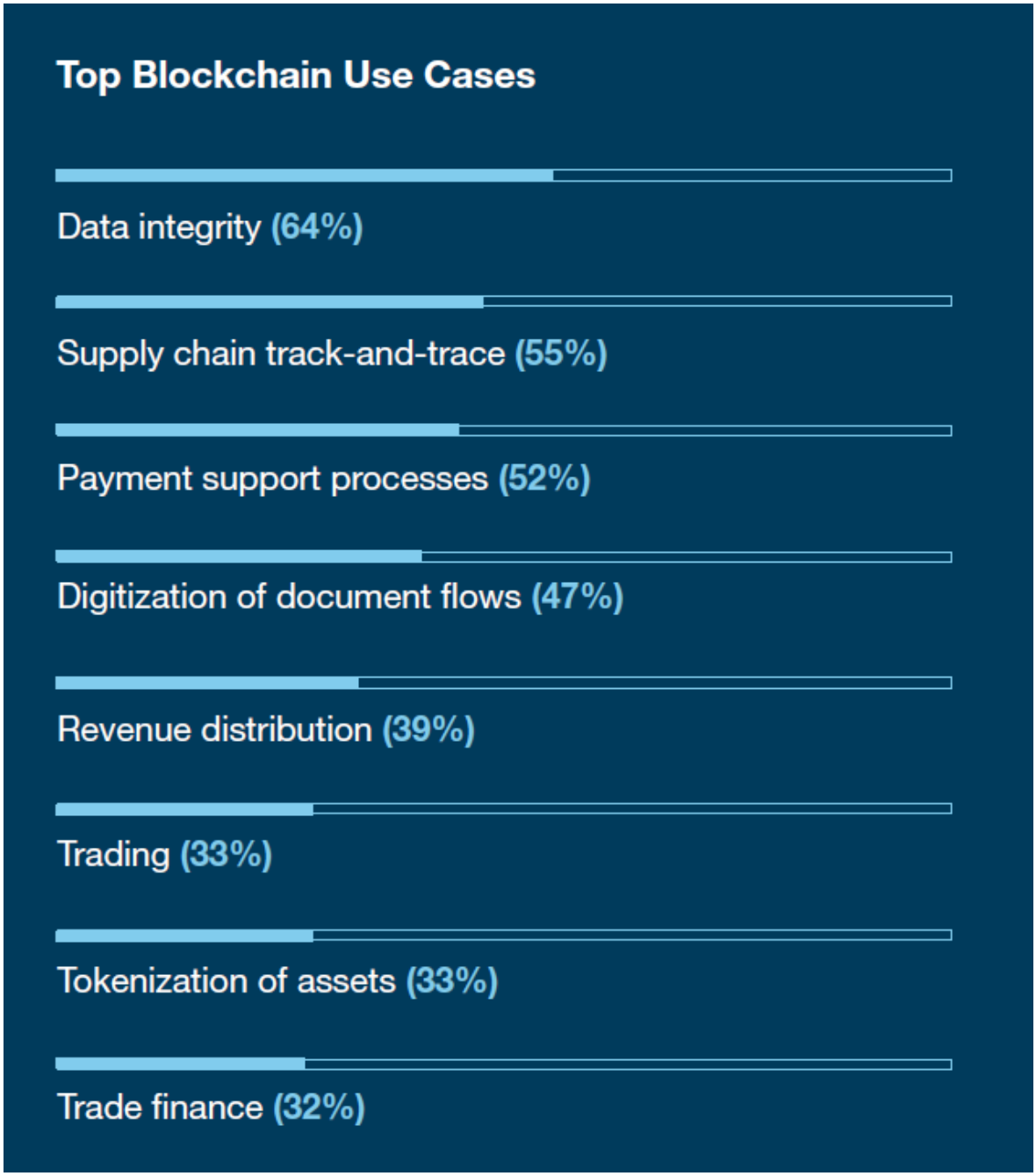

Image 9. Results of the commissioned study conducted by Forrester Consulting on behalf of EY. (Forrester 2019.)

So, many organizations can recognize which of the advantages blockchain can provide aids their case and operations, but why is the impact not noticeable in the industry? This is mainly caused because for most of the blockchain's existence, its insertion into the picture with cryptocurrencies until not much time ago has been plagued with organizations and enterprises not committing fully to researching these matters and trying to make blockchain work with their model. This is not the case anymore as more corporations are investing many resources in blockchains. (Malkov,2021.)

As more big corporations start to look into blockchains, others will undoubtedly feel the pressure to follow, as seeing others trying to make it will derive the perception that blockchain projects are a huge risk that might not return an equal amount of reward and start looking more like promising projects that could improve their organization. (Malkov,2021.)

Apart from this, upgrading about 90% of the blockchain infrastructure of current implementations will consequently mean that a lot more companies will get exposed to the technology. They will garner a lot more knowledge and understanding of the technology and the potential it has, which will help its growth. (Malkov,2021.)

For these many reasons, according to Statista, about 33% of global organizations say that their companies are working on creating a digital currency using the means provided by technology. (Statista,2021)

So, what is stopping blockchain from reaching that tipping point and finally starting to make the huge jump it has been projected to make for so many years is the question that is heard a lot when talking about the subject. Many of the reasons have already been specified, but one of the main reasons that seem to be standing in its way is the governments' reluctance to adopt the technology ultimately. Still, small steps are being taken by several countries all around the world, mainly in response to the rise of cryptocurrencies as many central banks around the world like the Central Bank of England, Bank of Canada, and banks in Singapore and Thailand have started experimenting on the possibility of implementing a Central Bank Digital Currency (CBDC). (Ismail,2021.)

Another reason for the hold out of the technology is the lack of development in its application layer. The development of applications and other improvements are being made in the name of functionality and power over being usable or simple to understand to make the user experience better. This is a massive problem because even if it is essential to accomplish these feats, the technology is reaching a point where the lack of balance between both sides is starting to make the reality of the technology reaching the point it has been projected to make for years more challenging. New users are not willing to learn to use this new product if the experience is not friendly or the interface is not done well enough so they can

understand from the start. Therefore, a lot of work is being put into improving these matters because even if you build a product that can change the world, the application layer is what will enable that product to make that a reality. (Malkov,2021.)

There are many reasons why blockchains have not completely tipped over that point they have been in these past few years, and they certainly could remain at that exact point for more time if the issues they present are not entirely fixed. Loudon Owen, who is a CEO at Toronto, Ontario-based enterprise blockchain development company DLT Labs, has an interesting take on the matter: He specifies that the impact predicted to happen for blockchains has not been manifested yet because it created a “pause” effect on corporations, as they got the initial appeal of the technology but were not sure about the following steps to take which left many enterprises looking at the industry waiting to advance leaving it stale until now. Therefore, he thinks that the future of the technology in the enterprise is at the hands of a few selected key people and corporations. (Ismail,2021.)

3.2 Current applications of blockchains

As stated, many organizations and corporations have started investing their time and resources in looking for new ways of using blockchain technology. Taking apart the ones trying to investigate the future uses of blockchain and what they can provide, many have already made strides in many fields and are starting to see the fruits of their labor and investments paying off.

Some of the prominent organizations already making use of the technology are, for example, IBM, which has created a blockchain that is already being used to provide transparency and data integrity to healthcare systems. Apart from that, they are also looking into providing a network that makes the management and exchange of skill-based credentials easier, which could improve the general working industry as a whole. (Ismail,2021.)

Another global company making progress with blockchain technology is Shell, which is using blockchain technology in collaboration with finance partners to create a platform to accommodate the trade and settlement of crude oil. (Ismail,2021.)

Another one of these companies is the Canadian division of Walmart, which uses blockchain technology to deploy a food traceability system. Another one of the uses usually appointed to blockchains is that it can improve the traceability of the products and set timestamps of transportation and arrival to different establishments correctly. This system

focuses on eliminating the disputes that could arise between shippers and carriers of invoices, which would spark when something did not coincide or one side would not agree. Using the technology provides a way to avoid these conflicts through matching. It now has all the information synchronized on a single ledger and will stay that way forever, leaving no room for misunderstandings or mistakes. (Ismail,2021.)

As seen with these examples, there are already many ways in which the technology can be profited from and used to improve already present systems within these organizations. There were not many massive changes in how these companies operate, and they did not need to shift their whole focus to integrate the technology, which is how it has been done until now. Still, the best way of doing it is to implement it to improve existing procedures inside your organization and not need to do a huge shift of resources, market direction, or business practices. This way, the transition is a lot more manageable and leaves a lot of space for both the people involved and the company's management, avoiding the disruption that the contrary would incite.

A big part of the use in blockchain technology right now comes from the Decentralized Applications, generally referred to as DApps. These applications are built on a blockchain or a distributed ledger technology, hence the name, and it is where a lot of the future of blockchains is placed. Their potential is very high, and a lot can be done with them already nowadays.

It is very far-fetched to think about this matter as a single DApp will be able to revolutionize the market like another mobile app or new service that comes out and instantly proves it's worth shooting itself to the top, but if a specific DApp gains enough recognition and proves that the purpose to which it was designed is indeed working out this, in turn, means that the potential staying power for the blockchain technology in that industry could be for real. (Malkov,2021.)

3.3 Cryptocurrencies

When speaking of current applications of blockchains or where they stand right now, it is entirely unavoidable to run into cryptocurrencies. It is the most commonly known use of blockchain technology, which brought it into the mainstream and made it worldwide known.

This is the case because they are the first use of the technology as it is, back in 2009 when the first Bitcoin network was released. Since then, both concepts have been thrown around a lot, and when cryptocurrencies started growing exponentially in popularity, the concept of blockchains ended up being tied to them.

There are many different cryptocurrencies, each one of them working differently from the other under different sets of rules and different ways to make everything work. Because of this, generalizing cryptocurrencies as a whole can be a little bit dangerous. Just because one cryptocurrency works or is labeled a certain way does not mean that every single one is like that, as can be seen in Image 10, where all the different types of cryptocurrencies are displayed. (Lewis 2018,149.)

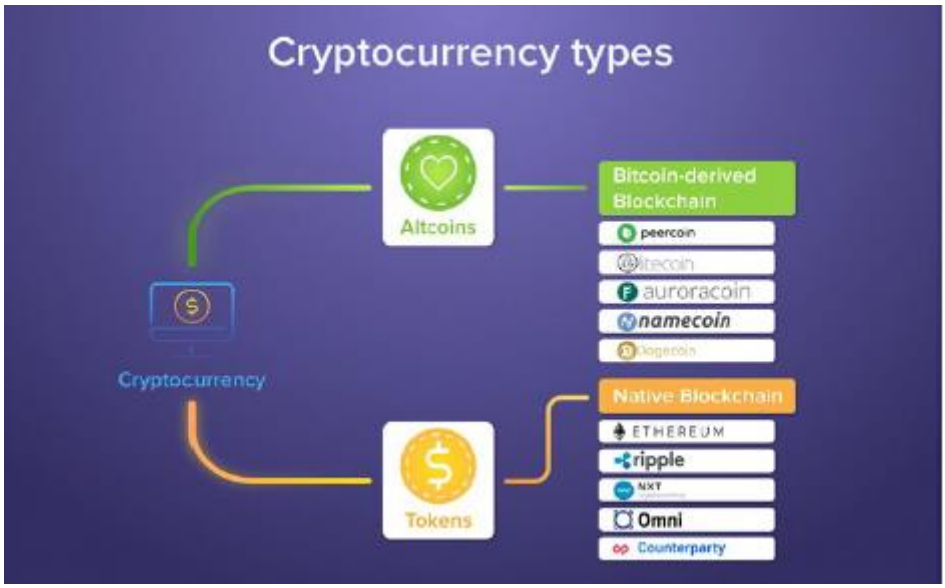

Image 10. The different types of cryptocurrencies. (Elrom 2019,14.)

So, as stated, the first Bitcoin network was launched in 2009, and the first reference to them in 2008 via the white paper published by Satoshi Nakamoto. This came out on these dates because of the downfall of the Global Economy during the 2008 Global Financial Crisis. Around the time when the crisis was already in full force, Satoshi released the white paper alluding to his creation (or their as it has not been found until this day whether Satoshi is a single person or a group of people, as many people have pointed out) which would be a system for electronic transactions that would not have to rely on putting your trust on an organization. And so began the first of many blockchain implementations, which would also serve as the starting point for every new one that has come after it. (Burniske & Tatar 2018,66.)

Satoshi did not come up with the concept in the short while the crisis had been going on as he had the whole system coded once the paper was released to prove to everyone that the concepts and ideas he was putting out could indeed work. The general consensus is that he started formalizing the concept around late 2006 and coding it in mid-2007, when speculations about the state of the U.S. housing market, which would be the determining factor of the start of the crisis, started to arise. (Burniske & Tatar 2018 ,66-67.)

From that point on, everything is history. Satoshi released the technology's source code as he started amassing more followers and more interest and then finally released the first public Bitcoin network at the start of 2009, as the crisis kept getting worse.

The cryptocurrencies that have spawned on Satoshi's base can be defined as digital mediums of exchange that have no central authority managing it. The tasks usually done by this missing overseeing authority are done by the users of said cryptocurrency. By using blockchain technology, each of the transactions done with a cryptocurrency is stored in blocks pertaining to a blockchain that serve as cryptographic proof of the transactions, as explained previously. (Ashford & Schmidt, 2022.)

Cryptocurrencies are not an easy field to get into, specifically investing. A lot of knowledge must be acquired to properly start investing and not be scammed or lured into making a grave mistake that could cost you money. Even then, there is a saying that must be taken into account, which is “Only invest money you can afford to lose,” as even if you are very knowledgeable of the subject or know your way around the whole field is a highly speculative investment, where massive price swings are the norm. A safe investment is a simply non-existent concept. There are many financial advisors that strongly advise against investing at all. (Ashford & Schmidt, 2022.)

3.4 Ethereum

Ethereum is often referred to as the “world computer,” built on the concepts laid out by Bitcoin. In the same way, Bitcoin is a trustless validation and distributed data storage, and Ethereum is a trustless validation and distributed storage and processing of data and logic. (Antonopoulos & Wood 2018,42; Lewis 2018,241.)

The term “world computer” comes from the vision that Ethereum showcased when they launched their service. They wanted to create a platform that would be unstoppable, resistant to censorship of any kind, self-sustaining, and decentralized. They attributed all these characteristics to the concept of a world computer. To understand a bit better what Ethereum is, this definition provided by Andreas M. Antonopoulos and Dr. Gavin Wood gives two explanations from two different perspectives:

From a computer science perspective, Ethereum is a deterministic but practically unbounded state machine, consisting of a globally accessible singleton state and a virtual machine that applies changes to that state.

From a more practical perspective, Ethereum is an open-source, globally decentralized computing infrastructure that executes programs called smart contracts. It uses a blockchain to synchronize and store the system's state changes, along with a cryptocurrency called ether to meter and constrain execution resource costs. (Antonopoulos & Wood 2018,42.)

Ethereum has a public blockchain that, as of 2018, was running on about 15000 computers and has a cryptocurrency that holds the number two spot in the popularity list worldwide, only behind Bitcoins. This cryptocurrency is called Ether which is the token of the Ethereum blockchain. (Lewis 2018,241.)

Ethereum and its blockchain set themselves apart from others like Bitcoins by being able to pack more than just payment data in their transactions. In the same way Bitcoin works, many protocols written as code are run as Ethereum Software, creating Ethereum transactions containing data about Ether Coins that are then recorded on the blockchain. But apart from storing that payment data, transactions can also create smart contracts, which will be explained later. Simply put, they are small bits of general-purpose logic stored on the blockchain and all its pertaining nodes. This is represented by Image 11, which many outlets started to use to explain what Smart Contracts could be capable of changing, for example, the process of buying a house. (Lewis 2018,241.)

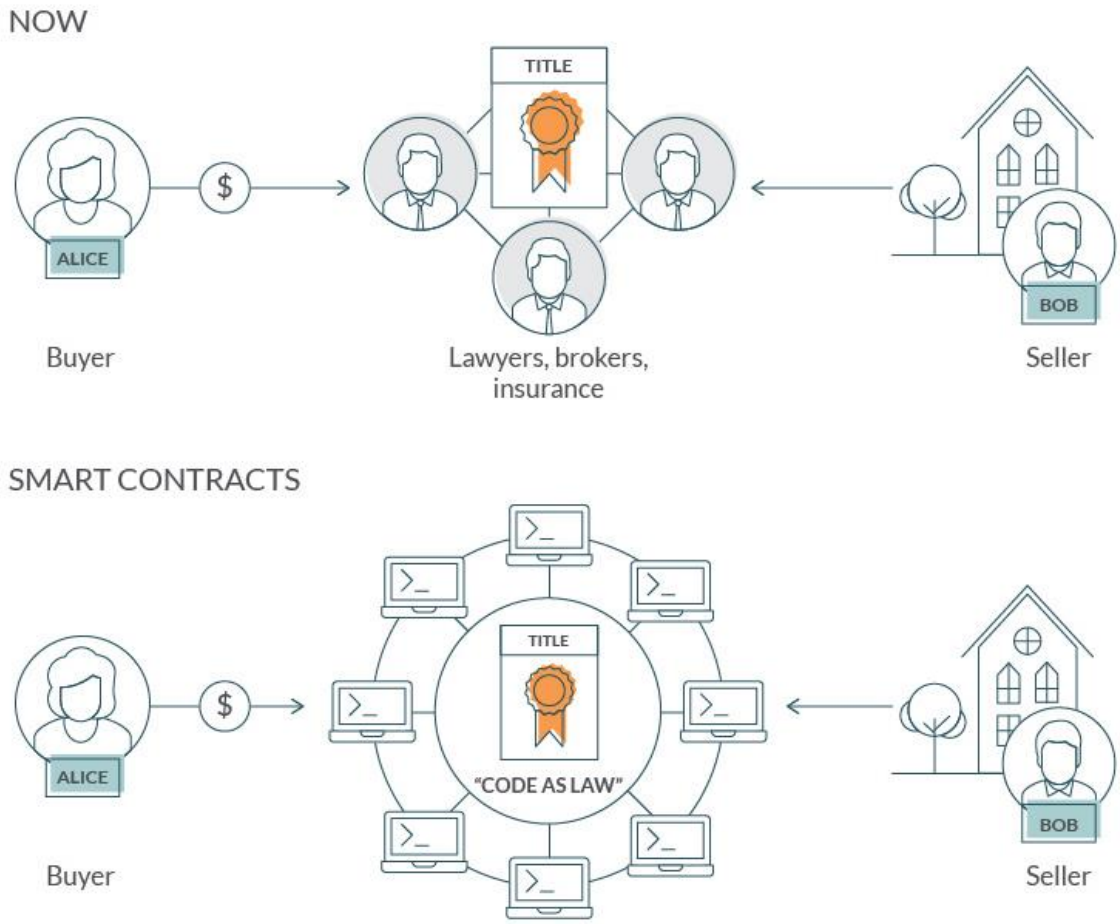

Image 11. Comparison of how smart contracts could tackle the process of buying a house. (Boichenko, 2018.)

These smart contracts are executed by invoking them, which is done by sending Ether to them. Once a smart contract is invoked, all the nodes run the code and update their ledgers according to the results. These smart contracts are run by all the participants using an operating system known as the Ethereum Virtual Machine (EVM). (Lewis 2018,241.)

To run or create these contracts and be a part of the Ethereum network, the download of the Ethereum client is very recommended. It is not strictly necessary as the possibility of creating the code yourself exists, but using the Ethereum client with the software it provides accelerates and facilitates the process a great deal. The Ethereum client will connect your computer over the internet with the other computers running the software and start downloading the Ethereum blockchain, so they are caught up with the latest state of the blockchain. (Lewis 2018,242.)

Once this process has been completed, your computer will essentially become a node on the network, equal to the rest of the nodes and running the Ethereum Virtual Machine. This will enable you to connect to the Ethereum network, where you will be able to mine for new

blocks, validate all transactions and blocks, create new transactions and smart contracts, and run those smart contracts. (Lewis 2018,242.)

These are the reasons why Ethereum's blockchain is different from the other open ones that came before it, as its primary purpose is not to be a digital currency payment network. Of course, that is a part that is still present in the blockchain as it is essential for the blockchain to function, but its use is as a utility currency to pay for the use of the Ethereum platform. And not only that but also the fact that the blockchain was designed as a general-purpose programmable blockchain that can run a virtual machine (EVM) that can run code of any complexity, enabling Ethereum to function as a standard computer would. (Antonopoulos & Wood 2018,43.)

4 Inside Blockchains

4.1 Smart contracts

The origin of the term ‘smart contract’ dates back to around 1994, when Nick Szabo defined it as follows:

“A computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.” (Yaga et al. 2018,32.)

They are a collection of code and data that is deployed using verified transactions that the users of the blockchain can perform. The smart contract is executed by nodes in the blockchain network it was deployed on, and each of those nodes has to return the same results after its execution. These results will then be stored on the blockchain. (Yaga et al. 2018,32.)

Smart contracts provide a lot of different possibilities to programmers and the users of the blockchain. One of the ways they can be used is by receiving data coming from transactions done by the users and using said data as parameters to be used on the functions existing on the smart contract. Once the data has been received, the program executes the function with the parameters specified in the data sent through the transaction to provide the service needed, as evidenced in Image 12 below. (Yaga et al. 2018,32.)

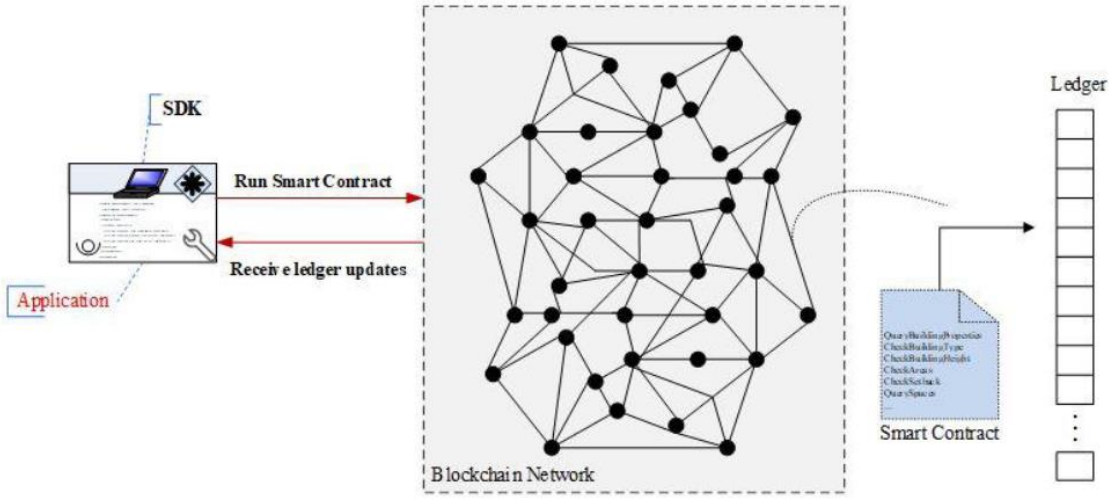

Image 12. Blockchain infrastructure with smart contracts. (Nawari & Ravindran 2019.)

The purposes they can fulfill do not necessarily have to be financial. They can perform calculations, store information, expose properties that are used to reflect a publicly disclosed state, and if needed or appropriate, they can automatically proceed to send funds to other accounts in the network. (Yaga et al. 2018,32.)

Above all the purposes, one of the most significant traits of smart contracts is that because they are stored on the blockchain, they can be used as a trustworthy third party when needed, as their content is tamper evident and resistant. (Yaga et al. 2018,32.)

One characteristic that all smart contracts must have is that they have to be deterministic, which means that they will always provide the same results given the same input. Also, every node executing the smart contract must agree to the new state obtained as output after the execution is completed. In order to achieve this goal, smart contracts are not able to operate outside of the window provided by the data that is directly provided via the transaction. Everything intended to be used has to be sent as a parameter. If a smart contract overrides this and uses any data from outside its own system, then it is said to be using an 'Oracle.' (Yaga et al. 2018,32.)

In many of the existing blockchain implementations, the publishing nodes execute the smart contracts at the same time as when publishing new blocks onto the blockchain. Still, in some other ones, some publishing nodes do not execute the code and only verify the result once the ones that are executing it are done. (Yaga et al. 2018,32.)

One aspect that is differentiated usually between the different types of blockchains regarding smart contracts is how the process is carried out and paid for. In permissionless blockchains that can execute them, the user who is proceeding with the transaction invoking the smart contract will have to pay for the cost of the corresponding execution. Apart from this, in permissionless blockchains, there is a time limit established that states how much execution power can be consumed by the call made to a smart contract which is based on the complexity of the code that has to be run. If this limit is surpassed, the execution is immediately stopped and the transaction is consequently discarded. This mechanism is in place to appropriately reward the publishers for executing the code while simultaneously preventing malicious users from performing attacks such as deploying smart contracts that would perform DoS consuming all the resources for publishing nodes. (Yaga et al. 2018,32-33.)

On the other hand, in permissioned blockchain networks, the payment of the resources used on the transactions that invoke the smart contract is not strictly necessary because of the nature of these networks as they are designed with having verified participants and alternative methods of punishing incorrect behavior are in place as has been stated previously. (Yaga et al. 2018,33.)

4.1.1 The functioning of smart contracts

Smart contracts work in a very specific way on every blockchain that has their use enabled or can use them. The content of the smart contracts defines the possibilities the users have when they want to make use of them, but some things never change between smart contracts. One of these characteristics has been mentioned previously, which is that the code of the smart contract is immutable. Once it is deployed to the blockchain, it cannot be changed, there is no way to enter and change the code, and it can only be called throughout the transactions and the code that is present. The only way to modify the code or change the characteristics they offer is by deploying an entirely new instance of the contract. (Antonopoulos & Wood 2018,246.)

Another characteristic they all share is their deterministic nature, which has also been mentioned. It is a critical aspect of how they work. For every different user that runs it, the execution result must be the same, given the same parameters and inputs and the same timestamp or state of the blockchain when it was executed. (Antonopoulos & Wood 2018,246.)

One thing that is necessary to clear out is that the word Contract has no legal meaning whatsoever in the context of Smart Contracts. They are computer programs written in a high-level language, just as many other programs.

They also need to be compiled to the low-level bytecode that runs in the EVM, which architecture can be seen below in Image 13. Once they have been compiled, they are deployed to the Ethereum Platform in a special transaction known as the contract creation transaction. This transaction is sent to the address reserved for this purpose, the contract creation address 0x0 or zero address. This address is special because it does not represent an EOA, which is an externally owned account, or a contract, which are the two types of accounts and addresses in Ethereum networks, as can be seen below in Image 14. It does not represent an EOA because of the lack of a corresponding private-public key pair for the transaction, so it can never spend the ether it is sent or initiate another transaction. Hence, the only purpose is to serve as a destination which indicates that the user wants to create and publish that contract. (Antonopoulos & Wood 2018,220-246-248.)

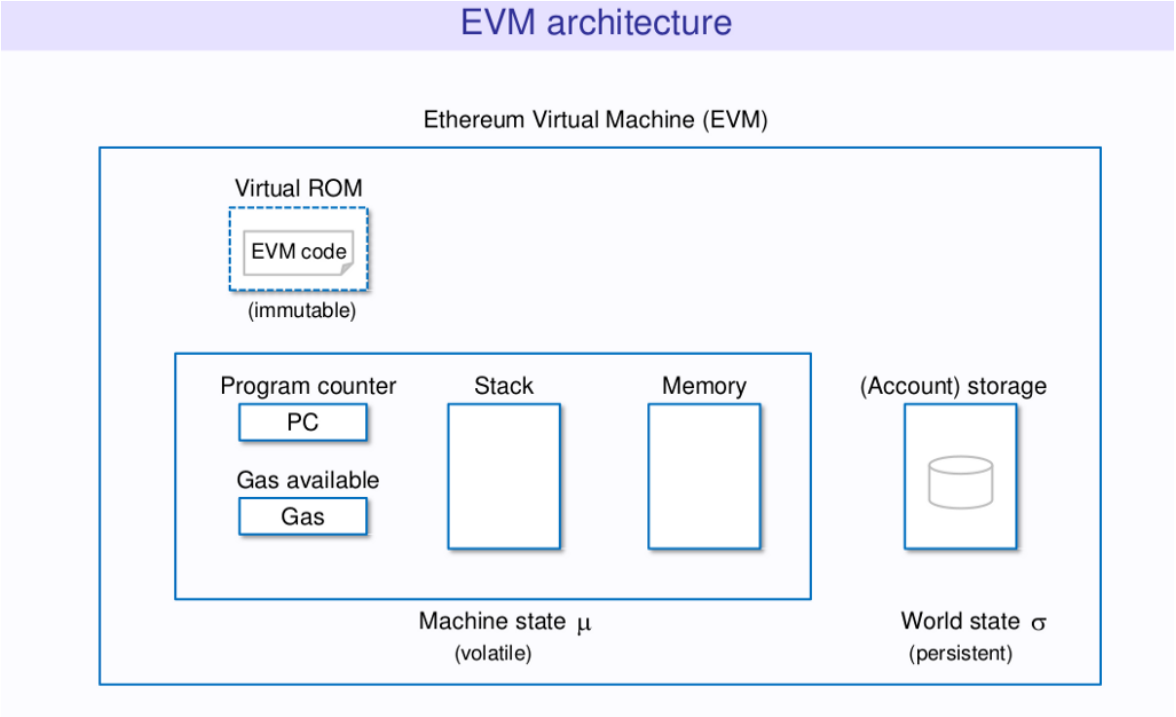

Image 13. EVM architecture. (Fabrisde 2019.)

The transaction only needs the data containing the compiled code, which will be used to create the contract, but some ether can be included if the user desires to do so. If the value field is set to the amount of ether the creator states, the new contract will start with an already existing balance. But if the ether is sent to the address without a contract in hand, the ether will be lost as once it reaches the address it will become unspendable and lost forever as it has no contract to credit. (Antonopoulos & Wood 2018,220.)

Each contract deployed is identified by its Ethereum Address which is derived from the transaction to create the contract as a function that uses the account responsible and the nonce. The Ethereum Address can effectively be used as a recipient in a transaction to send the ether to the contract or to call one of the functions inside it. (Antonopoulos & Wood 2018,248.)

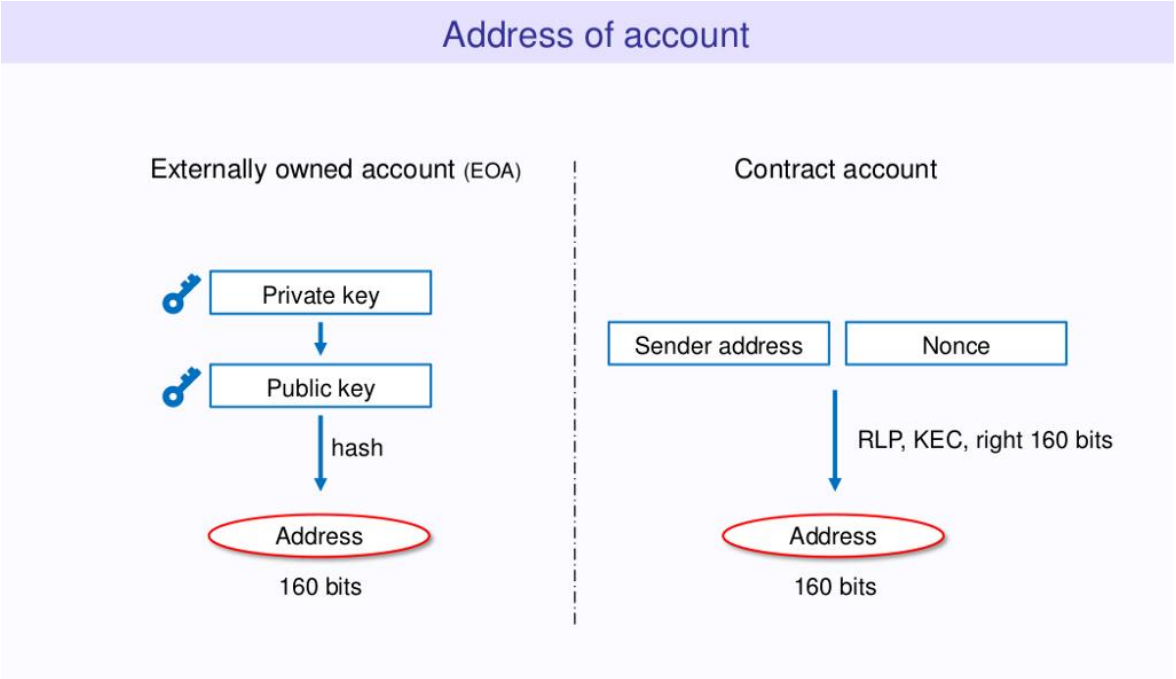

Image 14. The two types of Ethereum accounts. (Fabrisde 2019.)

The smart contract creator has no special privileges once it is deployed on the platform as the contract accounts created are private, meaning that smart contracts are effectively owned by themselves. The smart contract creator could code in some protocol privileges onto the contract before deploying it. Still, theoretically, they do not receive any private key or another way to control it once it is deployed. (Antonopoulos & Wood 2018,248.)

Another characteristic common to all smart contracts is that they are only run when called by a transaction. The rest of the time, they are dormant. The only way they are executed ultimately is if a transaction originating from an EOA has invoked them or if they are a part of a chain of contract calls which is a common occurrence when a contract has a call to another one. Also, the Ethereum computer can be considered a single-threaded machine, which means that contracts never run concurrently with one another as the system has no parallelism in place. (Antonopoulos & Wood 2018,248.)

Transactions are atomic, which means that the operation will always be done without changing context or any disruption from other operations. This will be the case no matter how many contracts they call or what the contracts they are calling do. The changes in the global state are recorded if the execution of the transaction has been completed successfully, which means that the program reached the end of the code without an error in execution. In case the transaction fails because of an error while running, the state is rolled back to the point where the transaction began as if it never ran in the first place. The only remains of the failed transaction are the record saying it was attempted but failed and the ether

deducted from the account that started the transaction. (Antonopoulos & Wood 2018,248-249.)

As mentioned previously, the only way to change or modify a smart contract is by deleting it and deploying a new one, as there is no way to directly change the code of a contract once it has been deployed. A contract can be deleted, effectively removing its code and internal state from the address it was stored on, leaving the account empty. Sending any transaction to that account will return nothing as there will be no code to execute. In order to delete a contract, the opcode “Selfdestruct” can be called, and the EVM will execute it. This operation costs negative gas, which is essentially a gas refund. It is important to note that the transaction history will not be deleted, as it is stored on the blockchain and is immutable. The opcode “Selfdestruct” will only be available if the original creator of the smart contract deemed it necessary. If it is not programmed with that functionality and does not appear on the code, then the smart contract cannot be deleted. (Antonopoulos & Wood 2018,249.)

4.1.2 Before developing a smart contract

Before developing a smart contract, a crucial step must be taken, which is choosing the language in which it will be written. As mentioned before, the EVM is a virtual machine, and like any other computer, it runs a special form of code called the EVM bytecode, analogous with your computer’s CPU. Even if it is possible to code a contract directly in this bytecode, the use of a high-level language that will be compiled afterward makes the process a lot easier. Coding this way is easier because the EVM bytecode is awkward, heavy, and very tough for programmers to read and understand. (Antonopoulos & Wood 2018,250.)

In theory, every high-level programming language could be adapted to write smart contracts. Still, it would be a very cumbersome experience as many requirements must be met to be compatible with the EVM bytecode. These requirements stem from the fact that the EVM is a very constrained and minimalistic execution environment. It also needs a very specific set of EVM instructions, functions, and variables to function correctly. Considering all these factors, it is easier to create a smart contract language from scratch than adapt a currently existing one. Therefore, many languages with the special purpose of being used to program smart contracts have emerged. (Antonopoulos & Wood 2018,250.)

When programming any kind of software, the programmer has to choose the language that best suits its case or the one that will provide better results once it is done. Programming a

smart contract is no different, and while every type of programming language has its advantages, declarative programming languages have proven to be the better choice. (Antonopoulos & Wood 2018,250.)

The reason behind this choice is that other types of programming languages broadly classified under the Imperative tag are languages that produce software that introduces a great chance of finding bugs. This is because imperative programming puts a high degree of difficulty on producing programs that execute exactly as the programmer expected to, as the ability of any single part of the program to change the state of another makes it hard to reason about that program's execution and the opportunities for bugs arise. (Antonopoulos & Wood 2018,250.)

On the other hand, declarative programming languages provide a much better understanding of how the program will behave. Every part of the program can be understood in isolation, and there will be no influence from one to another and no side effects during the execution. (Antonopoulos & Wood 2018,251.)

Because of all these reasons, as bugs are costly in an environment like this, the importance of coding smart contracts without any side effects is very high so seeing the program execute in its expected behavior is as well. Even if declarative languages are widely accepted choice and occupy most of the spectrum when it comes to smart contract programming languages, it does not really mean that Imperative languages are completely out of the picture. The most popular choice for writing smart contracts in Solidity is indeed an imperative language. (Antonopoulos & Wood 2018,251.)

This is a list of some of the currently supported programming languages for smart contracts:

- Solidity: The most popular choice when selecting a high-level programming language for writing Ethereum smart contracts. It is an imperative, object-oriented language that has a similar syntax to JavaScript, C++, or Java. As it is the most popular language, the community behind it is huge, and the possibility of asking or finding answers to your problem is very high. It is also statically typed, which means that the type of a variable is known when the compilation is being done. It also supports Inheritance which means that you can extend other contracts and makes use of complex user-defined types. (Antonopoulos & Wood 2018,251; Ethereum 2021.)
- Yul: It is an intermediate language for Ethereum. It is compiled to accommodate the needs of different backends. It supports the EVM and Ewasm, the Ethereum flavored WebAssembly, and is designed to be a usable common denominator of both

platforms. It is a great target for high-level optimization stages that can equally benefit both EVM and Ewasm platforms. It is a simplistic and functional low-level language that allows one to get much closer to raw EVM bytecode. (Ethereum 2021.)

- Serpent: An imperative programming language with similar syntax to Python. This language can also be used to write declarative code, but it is not completely free of running into the problems of an imperative language like side effects and state changes. (Antonopoulos & Wood 2018,251; Ethereum 2021.)
- Vyper: This language has a lot of similarities to Serpent, with the syntax being similar to Python again. It has strong typing as well as small and understandable compiler code. It was purposely designed with fewer features than other programs like Solidity in order to make contracts more secure and easier to audit. It is a great way to get started for programmers already proficient with Python who want to write smart contracts because of their similarities. Its smaller number of features makes it great for the quick prototyping of ideas. Vyper also aims to be easy to audit and maximally human-readable. (Ethereum 2021.)
- LLL: This language is declarative. It was the first high-level language developed for Ethereum smart contracts, but its use has decayed to being rarely used today. (Antonopoulos & Wood 2018,251.)

There are a lot of choices for this part of development, depending on what suits your needs, your previous knowledge, or the project you have in mind. As it has been stated, Solidity is very much the most popular choice of the bunch. It is the default language used not only in the Ethereum blockchain but in other EVM-like blockchains, so it is the most natural choice when starting out on writing Smart Contracts.

4.1.3 Developing and deploying a smart contract

Solidity was conceived by Dr. Garvin Wood to provide a language explicitly created to write smart contracts with features to support execution in the Ethereum world computer directly. After other developing contributions, the attributes that resulted from the creation are quite general, which is why it has ended up being used in many other blockchain implementations and platforms. (Antonopoulos & Wood 2018,253.)

The main pull of the Solidity Project, which is now developed and maintained as a separate independent project on GitHub, is its compiler. The Solidity compiler, solc, converts pro-

grams written in the Solidity language to EVM bytecode. The other aspect the project manages is the very important application binary interface, also known as ABI, standard for Ethereum smart contracts, which will be explained later. (Antonopoulos & Wood 2018,253.)

The first step of building a smart contract with Solidity is choosing the version you will be using. Solidity follows a semantic versioning philosophy when displaying its version, which follows this pattern: MAJOR. MINOR. PATCH. (Antonopoulos & Wood 2018,254.)

The “Major” number is incremented each time any major and backward-incompatible changes happen. The “minor” number is incremented as backward-compatible features are added between major releases. The “patch” number is incremented for any backward-compatible bug fixes released. (Antonopoulos & Wood 2018,254.)

The common way versions are denominated is by using the “minor” number as the major version and the “patch” number as the minor version. So, if the solidity version were 0.3.30, the major version would be three and the 30 the minor version. (Antonopoulos & Wood 2018,254.)

Solidity programs include a pragma directive that indicates to the compiler what version of the compiler the program is expecting. This pragma is read by the compiler and will warn about an error if the compiler version is incompatible with the specified pragma. These pragma directives are not compiled into EVM bytecode and are only used as a means for the compiler to check if the version pragma specified by the programmer is compatible with the version needed to compile successfully. Adding this version pragma is almost essential as it avoids problems with mismatched compiler and language versions. (Antonopoulos & Wood 2018,254-261.)

One of the core aspects of Solidity mentioned earlier was the managing of the Ethereum Contract ABI standard. The application binary interface is the interface between the two program modules, normally the OS and the user programs. The ABI specifies how data structures and functions are accessed in low-level code. It is the main way of encoding and decoding data into and from machine code. (Antonopoulos & Wood 2018,259.)

In Ethereum, the ABI is used to encode contract calls for the EVM and to read data out of transactions. The purpose of an ABI is to define the functions in the contract that can be invoked and describe how each function will accept arguments and return its result. (Antonopoulos & Wood 2018,259.)

The ABI of a contract is specified as a JSON array of function descriptions and events. A function description kind of JSON object contains many fields such as type, name, inputs,

outputs, constant, and payable. On the other hand, an event description object has these other fields type, name, inputs, and anonymous. (Antonopoulos & Wood 2018,259.)

The ABI is created when the contract is compiled with solc. So, once the programming of the Smart Contract is completed and the compilation is done, an example of the return of said command would be:

```
$ solc --abi Faucet.sol
======= Faucet.sol:Faucet =======
Contract JSON ABI
[{"constant":false,"inputs":[{"name":"withdraw_amount","type":"uint256"}], \
"name":"withdraw","outputs":[],"payable":false,"stateMutability":"nonpayable", \
"type":"function"},{"payable":true,"stateMutability":"payable", \
"type":"fallback"}]
```

Image 15. Example of execution of solc command. (Antonopoulos & Wood 2018,259.)

As you can see in Image 15, the JSON array describing two functions was created after compiling. These two functions were present in a small contract created for testing. Once this JSON file is present, any application that wants to access the contract it corresponds to can use it once it is deployed. Once this ABI is present, the only other thing an application needs to interact with a contract is the direction to which it has been deployed. (Antonopoulos & Wood 2018,259.)

4.2 DApps

Explaining what a Decentralized Application or DApp is in broad terms is relatively simple. It can be summarized by saying they are Applications that, contrary to the normal kind, run on a single computer, run on a different number of computers. Hence the name decentralized. According to the official definition provided by the official Ethereum documentation:

A decentralized application (dapp) is an application built on a decentralized network that combines a smart contract and a frontend user interface. On Ethereum, smart contracts are accessible and transparent – like open APIs – so your dapp can even include a smart contract that someone else has written. (Svantes,2022.)

Dapps are digital applications or programs that run on a blockchain instead of one computer. Like the blockchains they are run on, they lack control by an overseeing party, and they can be used for many different purposes. (Frankenfield,2022.)

Smart contracts come into the frame by acting as the application's backend per se. As DApps have their backend running on decentralized networks, the smart contracts deployed on blockchains play their part in this process. (Svantes,2022.)

The application's frontend is written in any programming language like any other app. It is used to make the necessary calls to its backend again, just like any other normal application.

The main characteristics of DApps are that they are Decentralized. One of the main appeals of the technology is having no ruling authority over the application, and not having a central point of failure are great advantages. DApps are impossible to shut down theoretically, as the data is distributed to all its nodes, and the failure of one node will mean the others will keep the network running, never shutting completely down. They are deterministic, just as smart contracts are, which means that they will accomplish the same function regardless of the environment they are used in. Dapps can also perform any action if given the right and required resources to operate. They are isolated, as they are executed in the EVM in case the smart contract has a bug. If it wasn't like this, the bug could affect the functioning of the blockchain network it was deployed in. These characteristics differentiate the architecture structure heavily from the traditional Centralized Client-Server that most services use nowadays, as illustrated in Image 16. (Svantes,2022.)

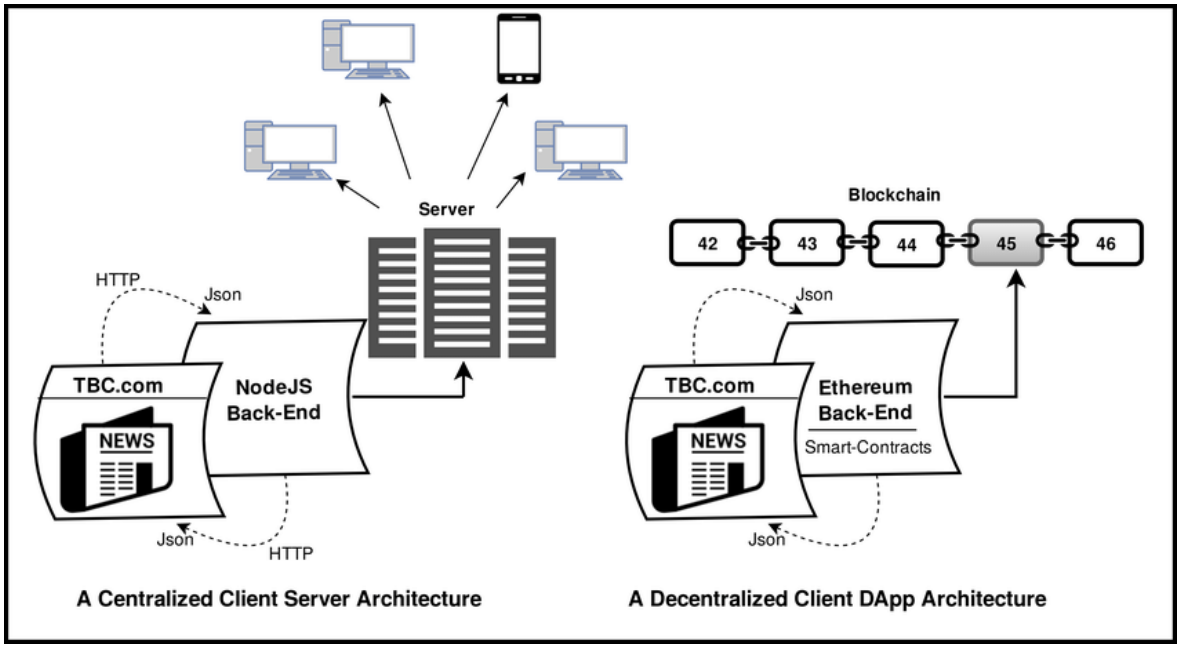

Image 16. A comparison between traditional client-server architecture and the alternative that DApps present. (Sayeed et al. 2020.)

These are some examples of decentralized apps:

- PopcornTime: This Decentralized Application does not use a blockchain but is still one by definition as by using the BitTorrent protocol, it streams videos between users in real-time. It has been labeled as a decentralized version of Netflix. (Raval 2016,9.)

- OpenBazaar: This one aims to be a decentralized version of eBay. No authority can determine what the sellers can and can not sell or establish some fees for using the service. It is also built on the BitTorrent protocol but has the problem that each seller has to have their store hosted, which means they need to have a server running to have their store be seen by the users browsing the app. The infrastructure of this app requires a system of incentivized storage miners. The application uses BitTorrent's protocol for data transfer purposes and Bitcoin for the transactions between the different sellers. (Raval 2016,9.)

- Lighthouse: Is a Bitcoin wallet embedded with a series of smart contracts which help pledge money directed towards certain projects. Once the project goal has been reached, the accumulated funds can be retrieved from the project backer's Lighthouse wallet. The pledgers that helped can undo their pledges if they wish without any involvement from the creator. This decentralized application is the perfect example of how to use the already existing infrastructure, the Bitcoin infrastructure, to create a useful application. It is just the combination of a simple UI with some Bitcoin smart contracts built together as a wallet. (Raval 2016,10.)

- Gems: Gems is a social-messaging app trying to create a business model fairer than the one WhatsApp is using. Instead of acting as a middleman who profits from its data, it is issuing its currency and letting its advertisers pay its users. The users can also earn by referring others to the network, incentivizing the growth of the platform and making everybody involved profit even more. The currency they use is Gems, a meta-coin based on Bitcoin. The developers also receive a profit by developing and maintaining the software running. As the userbase grows, the value of the currency rises. It is a profitable model, but it has not opened its source code, so checking the complete capabilities is still something that has not been done. (Raval 2016,10.)

Like any other technology, DApps have their fair share of both benefits and drawbacks, and it has been hard for developers to balance both sides.

Starting with the benefits, one of the biggest ones is that DApps that have been deployed effectively have zero downtime. Once the smart contract has been deployed on the blockchain, every user will have access whenever they desire to interact with that contract, which means interacting via the DApp. This characteristic also solves the problem that malicious attacks provoke on applications. Usually, the common DoS attack would not work on an individual Dapp. (Svantes,2022.)

Another benefit of developing DApps is the privacy that comes from using them, which originates from the fact that there is no need to provide a real-life identity to use them, just as is the case in blockchains. They also share many other advantages that are associated with blockchains: the resistance to censorship because of the lack of an overseeing party that controls the content, no one can control and block specific users from deploying DApps, submitting transactions, or reading data from the blockchain; and they provide complete data integrity which means that the data stored is completely immutable and reliable forever. (Svantes,2022.)

The last big benefit that DApps provide is the trustless nature they have. There is no need to trust an authority to check the behavior of the contracts, as they can be analyzed and are guaranteed to execute always in predictable ways, which is impossible in normal systems where an overseeing authority can manipulate results or behavior to their advantage. (Svantes,2022.)

As it can be seen, most of the benefits that come from DApps are inherited from the ones blockchains benefit as well, mainly qualities of the program's abilities to safeguard user privacy and the freedom that comes from being a decentralized infrastructure without a central authority ruling everything that goes on in the network.

And as the benefits, the drawbacks that stem from DApps also come hand in hand with some of the problems that blockchains have. One of the problems that are encountered when developing DApps is their maintenance. DApps can prove to be a bit problematic to maintain as the data and the code that has been already published to the blockchain are much harder to modify or correct than normal software. Even if a bug or security vulnerability is found in the DApp, correcting the mistake and updating it with a new version can prove to be a very hard task. (Svantes,2022.)

Another issue they share with blockchains is the lack of scalability. The huge performance overhead that exists right now is huge. As Ethereum tries to reach the level of security, integrity, transparency, and reliability they have set as a goal, every Dapp run keeps running and storing every transaction, adding on to that the PoF work that goes into each one of them, the processing power and time they use. It all ends up adding to a huge amount. A back-of-envelope calculation puts the overhead at about 1 million times the cost of standard computation currently. (Svantes,2022.)

The next issue can occur on certain occasions when a DApp takes too many computational resources from the network, resulting in that network getting backed up. If more transactions than possible for the network to handle are being sent, the pool of pending unconfirmed transactions grows uncontrollably. (Svantes,2022.)

One of the biggest issues is one of the ones that has been mentioned previously as well as referring to blockchains as a whole, which is the lack of a proper user-friendly experience. Until now, good UIs and other aspects that could collaborate to create a better user experience have been lacking, and with the difficulty that setting up a tool stack necessary to interact with the blockchain with very good security can prove to be the path toward having that good user experience can be a bit far away. This, in turn, means that the initiative of users to try to get into using these applications diminishes greatly. (Svantes,2022.)

The last problem that DApps could eventually run into is a little weird as it contradicts one of the most popular established benefits of the technology: decentralization. With enough user-friendly and developer-friendly Dapps created and deployed onto the base layer of Ethereum and it might end up looking like a centralized service. If this were to happen, their benefits would cancel themselves. (Svantes,2022.)

In conclusion, the development of DApps has a very good list of advantages and benefits, not only during the development process but as well once they are deployed onto the blockchain, but this list could be compromised in the event a certain set of circumstances goes in a specific way so weighing both sides to be equal and balanced is proving to be a hard task for developers.

5 Blockchain and cybersecurity

5.1 Security of a blockchain

Addressing the security of a blockchain is a very interesting matter as there are many qualities that they inherently acquire because of how they work and how they are designed. The design based on the principles of cryptography and all the work that goes on to assure that the transactions are legit and the consistency of the whole blockchain is maintained go a long way to making it a very reliable system by itself.

Still, the use of the technology does not effectively eliminate the need to use proper cybersecurity and have proactive risk-managing strategies in case an attack happens. Most of the usual risks involve human action interfering, as with all the other typical cybersecurity problems encountered. Having a very strong cybersecurity program is still a very important matter, even more so as hackers acquire more knowledge about blockchains and how to attack their vulnerabilities. (Yaga et al. 2018,47.)

Current cybersecurity standards are relevant in blockchains or protecting systems that use the blockchains in the background or are based upon/relying on them. These standards will need a certain set of adjustments to adapt to the characteristics and features that blockchains have separating them from other technologies. However, they still provide a good base for a strong cybersecurity system. (Yaga et al. 2018,47-48.)

Many current cybersecurity standards have a lot of relevance with blockchain technology used by many businesses and corporations. One example is the NIST Cybersecurity Framework, which was not designed explicitly with the idea of being used on blockchains. Still, because of its broad approach of covering many areas of cybersecurity, the businesses that make use of it can develop new policies and processes that identify and control risks specifically affecting blockchain technology. (Yaga et al. 2018,48.)

One important aspect of blockchain security that must be known before getting to learn more about the subject is the importance of differentiating both types of blockchains from each other. Public and private blockchains have different needs and requirements on their security front regarding the privileges needed for participating in the blockchain and to access the data inside the blockchain. Therefore, knowing the type of blockchain that is being worked on and applying the correct measures is essential in obtaining and configuring a good security plan.

The main security trait it acquires from its design is decentralization. Being a decentralized system makes it extremely hard to hack. When an organization is hacked, they usually have

a centralized server that can be easily targeted by the group of hackers trying to get in. With blockchains, this is not a concern because of the decentralization. The amount of computing power required to hack into each one of the nodes that composes a network would be an enormous effort on the hacker's part. (Antonopoulos 2017,269.)

Bitcoin's blockchain is the most popular and the one with the biggest prize to acquire in case of completing the task and has been targeted a lot of times by hackers, groups of cybercriminals, and other entities trying to get that money. So far, no one has been able to succeed, which is a testament to how well the structure was set up since the start. (Antonopoulos 2017,270.)

Its security resides in the ability to have decentralized control over the private keys given to each user and the independent transactions validated by miners. These two are the pillars of the security. Suppose all the keys are put into a single place, as with many of the early bitcoin exchanges. In that case, the control is taken from the people and more into a central system which could then be hacked, leading to detrimental consequences. The second is keeping the transactions on the blockchain, which is usually done to try and reduce the fees associated with transactions or accelerate the process of doing them. Doing that means that transactions are stored in a server off of the blockchain, which is only synchronized occasionally to the current state of the network. This practice once again defers from the decentralized nature of the technology. It leads to centralized ledgers that are not secure, which can be easily falsified, leading to diverted funds and depleted reserves without other users noticing. Resisting the temptation of moving to a more known system with centralized tendencies is very important to avoid subverting the advantages that blockchain security inherently provides. (Antonopoulos 2017,270.)

The security architecture of blockchains is different from other traditional systems. The consensus system creates a public ledger that is completely decentralized. This system makes it so that the root of trust of the blockchain is the genesis block, which builds the chain of trust up until the last verified block. In applications where blockchains are used, the only thing that should be explicitly trusted is a fully verified blockchain. If the application puts its trust in anything other than the blockchain, it is effectively exposing itself to vulnerabilities and should be a cause for concern. (Antonopoulos 2017,271.)

A way in which blockchains can be vulnerable is because their code is usually open-source, and it has many characteristics that attract hackers. One of those characteristics is the fact that it is open source to show transparency and promote other people to contribute to the code. Another characteristic is that much of the code that is released cannot be considered mature enough to be release grade, and it presents a great vulnerability that knowledgeable

attackers can exploit. And finally, especially in cryptocurrency-related blockchains, losing data can mean a lot more than a simple privacy breach. Once the funds have been transferred, it is hard to track them down, and the transfer is irreversible. (Elrom 2019,419.)

As blockchains' popularity has risen a lot in the last few years, these concerns have grown a lot as well. Every day, a new attack is made on a blockchain, and many losses are reported when these succeed. Because new attacks are invented daily, regulatory laws are always advised and revised often as understanding common attacks, security, privacy, compliance, and regulations can prove to be a very hard task to overcome. (Elrom 2019,420.)

5.2 Potential attacks on blockchains

Attackers looking to exploit blockchains for their gain know very well of all the blockchain’s problems and vulnerabilities, so it is very important to know about them as well and create efficient preventive security systems that can tackle the issues that the many attacks that could be aimed toward the blockchains could cause. As the myth around them has grown that they are an inherently secure technology, businesses can overlook the security side in order to adopt the technology faster. Please make no mistake, as specified previously, blockchains are not fully secure and require the proper knowledge and measures to keep them as safe as possible. (Geroni 2021a.)

Getting ready for any attack that might come the way of the blockchains that need protection is practically impossible. It was specified that new attacks are created every day, as malicious users try to take advantage of the vulnerabilities and gain as much as possible. Understanding the vulnerabilities that are present as well as the way they were exploited could be crucial knowledge when setting up the system that will try to prevent the new attack that could come the next day.

Blockchains can receive multiple kinds of attacks differentiated by the area of the technology that is being targeted in each specific one. The attacks can be divided into three different types: the ones aimed at the Blockchain PeerToPeer network itself, wallet cyberattacks directed toward wallets inside blockchains, and finally, platform attacks directed toward the platforms that support the blockchain. These include exchanges, websites, and lending platforms, for example. (Elrom 2019, 431.)

5.2.1 Attacks on to the P2P network

First, let us look at the attacks that are infringed on the Blockchain PeerToPeer network:

- 51% attacks: The 51% or double-spending attack happens when a blockchain node manages to amass more than 50 percent of a blockchain's hash rate, which means that the node can then alter and manipulate blocks. This attack is incredibly high cost and very hard to pull off on large blockchains because of the number of nodes already existing on the blockchain and the miner competition present in them. Blockchains like Ethereum's or Bitcoin's demand too high of a level of resources to pull an attack like this successfully. Small blockchains suffer from this kind of attack more commonly. It is much easier to spend the resources necessary to amount the control in a blockchain with fewer nodes and less processing power needed. (Elrom 2019, 439; Geroni 2021a.)

  Still, huge blockchains are not exempt from this problem. In 2018, three renowned cryptocurrency platforms suffered from this attack amounting to a huge amount of money being lost. These three platforms were Ethereum Classic, ZenCash, and Verge. Losses in general recently amount to around $20 million annually because of these attacks. (Geroni 2021a.)

  The main problem of the attack is that it takes a lot of resources in order to pull off. According to crypto51.app, the cost of a 51% attack on the Bitcoin blockchain would cost about $1,534,103 per hour as seen in Image 17 below.

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$789.19 B	SHA-256	201,611 PH/s	*$1,534,103*	0%
Ethereum	ETH	$369.38 B	Ethash	1 PH/s	*$1,670,487*	6%

Image 17. Cost of a 51% attack on Bitcoin and Ethereum's network. (Image: crypto51.app.)

To prevent this kind of attack as an investor, the necessary steps to take would be to check the cost that it would take to attack the blockchain you are investing in and check if there is an existing mechanism in case the attack happens. (Elrom 2019, 441.)

A good example of a mechanism to help in case the attack happens is creating a hash that holds a snapshot of the transactions and balances of each one of the blocks of the blockchain and then storing it into a larger blockchain, leaving it protected from the attack as a backup. (Elrom 2019, 441.)

Other good practices to avoid running into trouble because of a 51% attack are improving the monitorization of the mining pools and ensuring a higher hash rate as

well as refraining from using the Proof-of-Work consensus mechanism in favor of other ones like Proof-of-Stake. (Geroni 2021a.)

- Routing attacks: As blockchains depend on the massive volume of data transfer done in real-time, these attacks are a great concern. A hacker could intercept the data being transferred to an Internet Service Provider (ISP). The most dangerous aspect of this attack is that they are anonymous. These attacks are usually carried out to leak confidential data or to extract some monetary benefit without the blockchain network users even realizing it is going on. Detection of these attacks is hard, which is why they can be so dangerous as deciphering the attack before it has already done a lot of damage could be very hard. (Geroni 2021a.)

  These attacks include BGP hijacks which is a maliciously rerouted Internet Traffic attack. They are made by falsely announcing the ownership of groups of IP prefixes. (Elrom 2019, 443.)

  Large mining farms are an ideal target for these attacks as they are centralized in a few geographical locations, making them the best target for an ISP-targeted attack. Attackers can carry out the attack by making a Partition Attack, which is when an ISP can hijack a few IP prefixes, effectively partitioning the PeerToPeer network. Or they can cause a Delay Attack, which is done by making the ISP delay the traffic coming and going toward a specific node in the network, which will result in a delay in block propagation and slowing transactions greatly. (Elrom 2019, 444.)

  The effect of an attack of this kind could escalate to reduce the revenue of the node that received the attack and turn into a 51 percent attack because fewer nodes are influencing the node at that time. Apart from these consequences, the attack could also prevent a transaction from being sent by large entities such as exchanges. (Elrom 2019, 444.)

  In order to prevent these kinds of attacks, the creation of a custom script or the installation of hardware to monitor the network could go a long way in helping. Many ISPs themselves provide a paid solution to do these tasks and monitor the network to prevent an attack. (Elrom 2019, 444.)

- Sybil Attacks: These attacks obtain their name because of their nature of attempting to influence the PeerToPeer network by creating multiple identities and taking control of multiple nodes. It creates various fake accounts to take control of a network. When it succeeds, the entity that has control over those fake accounts has additional voting power inside the network and can influence it as they will. (Elrom 2019, 438.)

If the attack is successful, the attackers can use their nodes to attempt and out-vote the rest of the honest nodes present in the network. If they get the majority vote, the attackers could then refuse to receive blocks or transfer fake blocks, making the network unreliable and dangerous. (Elrom 2019, 438.)

The attack can also be large enough to amount to the majority of the nodes on a network, which would then turn to the previously mentioned 51 percent or double-spending attack, as they would be able to control the majority of the network's hash rate and change blocks at their will. (Elrom 2019, 438.)

The way to prevent these attacks or discourage them is by rendering them impractical for the attackers. This can be done by putting a cost on every part that involves the Sybil attack, such as creating an account, running the servers, having electricity, etc. (Elrom 2019, 438.)

The bigger blockchains have been taking into account these attacks for some time now and have come up with some ways to combat them. For example, the bitcoin Proof-of-Work consensus algorithm requires a lot of processing power as creating a block is proportional to the total processing power. This discourages attackers from targeting the network because miners would rather mine by the rules established rather than risk losing on a failed attack. If the network uses the Proof-of-Stake consensus mechanism, which requires the stacking of coins, the attacker would also be risking the loss of their assets if they wanted to go ahead with the attack. (Elrom 2019, 438.)

Another way to discourage this attack is by establishing a chain of trust, which would require trust before allowing any entity entrance onto the network. One way to go about this is to enable a user to create a new account but not give it the full amount of privileges for a certain amount of time before it can be verified. (Elrom 2019, 439.)

Other ways have been presented by huge blockchains, such as charging a transaction fee that discourages attackers or establishing a meritocracy. A meritocracy would mean that a certain set of users would have more power over the rest. These users would be the older accounts, for example, which could have gained trust because of their reputation and being in the network for a long time. (Elrom 2019, 439.)

- Miner ransomware: Ransomware attacks are common in the plane of cybersecurity, and hackers found a way to affect blockchains by attacking network miners with this kind of software. Ransomware is malicious software with the purpose of blocking

the computer it strikes until the money (ransom) is paid to the attacker. (Elrom 2019, 441.)

The way it is used is very similar to the common use in personal computers. It locks up mining rigs when it is installed by the users unknowingly and locks the miner until the desired amount is paid.

One of the most famous cases is the hAnt ransomware, shown in Image 18, which has been speculated to be included with a version of the mining rig firmware. Once it is installed, it has access to the firmware of the miner and can effectively control it. (Elrom 2019, 442.)

The attacker then displays a message when the miner logs in that threatens to overheat and destroy the computer. This can be done by turning off the fans if the victim does not comply with the requests being made by the attacker, which are infecting other devices or paying a specific bitcoin ransom. (Elrom 2019, 442.)

Image 18. Screenshot from miner ransomware hAnt. (Elrom 2019, 442.)

As with any ransomware, getting rid of it is an extremely hard task. Attackers craft the software very carefully and can include a script that detects when it is disconnected from the internet which could then damage the computer. The best way to go about it is to remove the ransomware from the miner's storage surgically. (Elrom 2019, 443.)

Of course, the best way to avoid the problem altogether is by not downloading any firmware upgrade that is not originated from the official site of the provider.

- Eclipse Attack: An eclipse attack can be performed on a PeerToPeer network on its own or by pairing it with another one, such as the 51 percent attack. The point of the

attack is to gain control of a peer's access to information inside the network by manipulating it so that the nodes communicate exclusively with malicious nodes. Once that has succeeded, the attacker can manipulate the mining and the consensus mechanism. (Elrom 2019, 443.)

The best way to prevent this attack is by regularly running analyses, simulations, and experiments to find the necessary countermeasures to avoid them.

5.2.2 Attacks on Wallets

The next kind of attack is Wallet Cyberattacks, these attacks come in many shapes and forms, but their end goal is always to rid the wallet owner of their private keys. They usually follow a process of phishing the victim to get their confidential information, and then once they get it, they transfer the funds from that wallet to their own. (Elrom 2019, 431.)

The best way to prevent these attacks from happening to blockchains and affecting the wallets is to remove cryptocurrencies from exchanges completely when they are not being used and then store them on a cold wallet centralized storage. This practice is one of the best ways to tackle the problem, and there are multiple hardware wallets available in the market to achieve the purpose. It is one of the best ways because it allows having the highest level of protection possible and avoids the loss of assets in exchanges completely. Here are the most common wallet attacks:

- Online Wallet Phishing-Malware attacks: These can be done in multiple ways. Some are very common as it is one of the easier techniques that a malicious party could employ to get sensitive information. Hackers perform these attacks by phishing to bait users into giving them their credentials by posing as an authentic, authoritative source to scam them into giving their information. (Geroni 2021a.)

  These attacks are performed by sending emails that request information about the users' credentials via fake hyperlinks. Once the user is compromised, the blockchain itself has a great vulnerability that can be exploited further by the hacker. This attack is becoming more common every day, and it keeps raising its concern for every blockchain network. For example, an attack like this that was carried out against Electrum's wallet caused more than 1 million in total losses. (Elrom 2019, 433 ; Geroni 2021a.)

  A more complex way of performing this attack is by setting up malicious servers. This was the case for the attack on Electrum's wallet. When the server was accessed by the user to perform a transaction, the server replied with a legit-looking

message telling the user that they needed to update their wallet, along with a link that redirected him to a fake version of the wallet with malware. Once the user put his credentials on the fake version, they were sent to the attacker, which he used to transfer the private keys pertaining to the user to their wallet. (Elrom 2019, 433.)

As a user, apart from completely avoiding online wallets and using cold storage, the risk of running into this problem can be avoided by performing a series of steps: The first is not to download any software that is not coming from an official source, never download online wallets or upgrade from any other source that is not the wallet's official site, always check the URL for little misspellings and other tricks that attackers use to confuse users. Always take care of the private information you have. Your credentials and other sensitive data must always come or go to a verified party and not be shared lightly. You should always check the GPG signature of all the software you download not to give away any assets to unintended parties. Lastly, recognizing a false support number is very important. Checking official sources and not falling for a wrong number that was posted by a hacker on any search engine is important. (Elrom 2019, 434.)

As a developer, it is very important to educate the network users not to make the mistakes that have been mentioned previously. Setting up help pages, tutorials, and other posts can help avoid these kinds of problems. Apart from that, being assured that the GPG signature is verified is also very important. (Elrom 2019, 434.)

- Keylogger Malware: One of the methods hackers can use to get a user's sensitive information from the network is using Keylogger software. It is a popular choice all around, and it is no different in the blockchain. Attackers can use a keylogger or screen scraper to record everything the user types and capture passwords or other personal information. These attacks are a lot more common when the computer is in a public space, as the perpetrator needs to attach an actual USB to the computer in order to record the key log. (Elrom 2019, 435.)

  Apart from completely abstaining from logging in using your private credentials on a public computer, checking if there is a USB key attached to your computer and avoiding accessing important accounts accordingly can greatly decrease the risk of this attack. Doing a thorough search through the processes running on your computer can also help identify if there is anything weird going on. (Elrom 2019, 435.)

- Dust attack: Dust attacks are carried out by sending a small transaction that attackers then use to spam the blockchain network and take up a block space or to mark the targeted addresses so that the user is confused by it and transacts the assets,

which would then help the attacker identify a user's personal information by tracing their transaction history. (Elrom 2019, 436.)

As a user, it is important to avoid spending unrecognized transactions. As a developer, implement a coin control feature so that unrecognized transactions can be tagged as "Do Not Spend" and not be included with the rest of your transactions. (Elrom 2019, 436.)

- Hot wallet attack: When a hot wallet attack happens, the attacker has successfully retrieved a wallet's private keys from a hot wallet where those private keys were stored online. This can be done by phishing, password cracking, or any other method, but once it is done, the keys are pulled from the network and then transferred to the attackers' wallets. (Elrom 2019, 436.)

  This can happen when the private keys are stored in a "hot wallet." These hot wallets exist because exchanges keep the user's private keys online, so real-time withdrawals are allowed from wallets. Hot wallets have been the target of attacks in the past as they present a huge vulnerability in the system's security. (Elrom 2019, 436.)

  In order to avoid this attack, the best a user can do is to make use of one of the cold wallet software and keep their assets under their control in one of them, not on centralized exchanges like hot wallets. (Elrom 2019, 437.)

  As a developer, keeping a cold wallet to store users' keys instead of using hot wallets is a great practice. A good example of this is Coinbase.com, which has claimed that it holds about 98 percent of its users' funds on paper backups geographically distributed to safe deposit boxes. (Elrom 2019, 437.)

  Another good practice as a developer is to encrypt the private keys if they are to be stored on an online network. If there is no possibility to store them otherwise, encrypting them with a strong encryption key can help protect them. Watching for unusual activity in the network can also help keep the keys safe. For example, many exchanges approve of large withdrawals manually instead of trusting an automated system. (Elrom 2019, 437.)

5.2.3 Attacks on the platform

The last type of usually perpetuated attacks are directed toward the platform. As mentioned previously, the reason why blockchains are secure naturally is because of the decentralized nature of the platform. All the data is distributed between nodes. The fact that mining is very energy expensive makes the cost of an attack skyrocket, and the risk of losing a huge

amount of money disincentivize attackers from trying. Another factor that helps keep blockchains safe is that their code is open source. Even if it can be a gateway to be exploded for vulnerabilities, it also allows developers to quickly implement changes based on research and recommendations by security experts. (Elrom 2019, 444.)

Despite that, these conditions do not apply to every blockchain in existence. The platforms that provide services built on safe blockchains, like exchanges, lending platforms, wallet-based services, or dapps that private store keys are not completely secure or exempt from attacks. Following are the largest attacks that have happened to the different platforms existing:

- DoS and DDoS Attacks: Denial-of-Service and Distributed-Denial-of-Service are the most common kinds of attacks performed on any platform. They are executed to cut the user off from the targeted service. The difference between both terms is that when an attacker is performing a DDoS, they are using multiple machines attacking at once instead of just one, increasing their success ratio and making it harder to find their exact location. (Elrom 2019, 452-453.)

  Some of the biggest blockchain networks have simple built-in systems to combat and prevent DoS attacks. Still, so many smaller ones have no protection against them and can be very vulnerable. (Elrom 2019, 453.)

  The most common attacks of this kind are the following: Buffer overflow, where an attacker sends more traffic to the target than it is effectively able to handle, this then crashes the service, and the attacker can control the service; ICMP flood, which is an attack where the network is overloaded by forcing one of the nodes of it to distribute bogus packets to the rest of the nodes which in turn overloads the network completely shutting it down; Next there is the SYN flood, where an attacker sends a request to connect to a service but is never fully resolved and authenticated, the hacker can then attack all the ports that have been left open because of the request until it crashes the service; Finally, an NTP/DNS amplification, an attack that is targeted on to NTP server, an attacker sends a huge number of UDP packets and spoofs the source IP. Once they have that information, they can then make the NTP server believe that their overloading traffic is legit from the intended target, which causes the server to crash. (Elrom 2019, 453.)

  Taking a firm stance against these attacks is very important as they are one of the most common and can easily result in big losses if a good system to prevent or take care of them is not in place. Filtering bad traffic using a script to check for these

attacks or using a good firewall, like shown in Image 19, can be very efficient. (Elrom 2019, 454.)

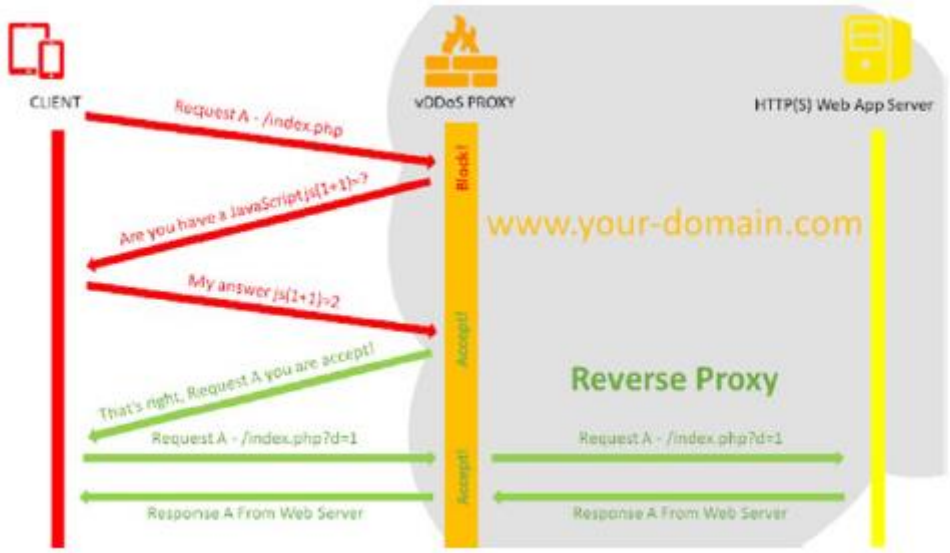

Image 19. Explanation of DDoS protection reverse proxy. (Elrom 2019, from vddos.voduy.com, 454.)

Making use of dedicated hardware to handle these attacks in order to keep them on the servers to detect and filter the attacker's traffic is a good option. Taking advantage of the services already provided by ISPs and cloud services can also go a long way in helping take care of these attacks, as they commonly have some systems in place to take care of possible attacks. (Elrom 2019, 455.)

- Credential attacks: Attacks aimed at authentication and credentials such as password cracking have caused huge losses to multiple platforms. One of the most famous attacks was infringed on an exchange, specifically Mt.Gox's. This attack was possible because hackers gained access to an auditor's credentials and then transferred their bitcoins to their wallets. (Elrom 2019, 446.)

  Another attack of this kind could be made directly on a user instead of an exchange by taking over the user's account. The hackers took advantage of a phone company that enabled the takeover of phone numbers by providing very simple billing information. They ported a number to a new service provider and approved a reset of the accounts' credentials by using SMS verifications. (Elrom 2019, 446.)

  Once again, the best way to avoid running into this problem is by avoiding storing your assets on a hot wallet or centralized exchange, keeping them instead in your cold wallet. Not registering on sites that don't have an SSL certificate and using

strong and unique passwords can also help in being protected from these attacks. (Elrom 2019, 446-447.)

Setting up multiple layers of authentication security is also really helpful in preventing getting your credentials stolen, as having one layer compromised does not mean an irrecoverable breach. Installing an antivirus to keep your computer safe from malware, ransomware, and phishing sites can help prevent the installation of software that may be used to gain your credentials. Finally, using a VPN, especially on a public network, is highly recommended to have an extra layer of protection. (Elrom 2019, 447.)

As a developer, there are a lot of possibilities to go through in order to keep your platform safe. Setting up a security tester that ensures that users create and use strong and encrypted passwords is very important. Setting up the tester, implementing multiple layers of authentication, and providing a reliable confirmation service for important operations like transfers is very important. Once the assurance of a good encrypted credential method is achieved, the next step is to ensure that all of the users' private information is safely stored and encrypted in a server disconnected from the internet. (Elrom 2019, 448.)

Using SSL on all pages and AES-256 encryption and hashing all passwords with a cost factor of 12 is also a good practice. Add to that the locking of the account in case multiple failed logins occur, and the possibility of suffering the consequences of being attacked will have been greatly reduced. (Elrom 2019, 448.)

Another good practice that can be done from a developer's point of view is using a remote connection on the development computer you are using. Encrypting data on your hard drive and setting up an automatic computer lock for inactivity can also help. If your computer is left unattended, it will lock itself and require your password to be restarted, effectively protecting it from attacks if the event were to happen. (Elrom 2019, 448.)

Apart from those, setting up a strong firewall and using a VPN is also very important, especially on public networks that are not secured. Finally, using software from reliable sources and avoiding the use of libraries that have root access can also prevent falling victim to one of these attacks. (Elrom 2019, 448-449.)

- Faulty Code: Faulty code is the other side of the coin when it comes to the fact that the code is open-source. It is also one of the biggest reasons for losses for platforms,

so much so that some corporations even started setting bounties for white-hat hackers to go and find bugs in their code. (Elrom 2019, 449.)

As a developer, avoiding the use of SQL Injections, an attack where a hacker sends illegal SQL statements through a text entry input box in order to gain access to private content, which is then used to add, change or delete data from that database. Implementing SQL injection filters can reduce the chance of falling victim to this vulnerability. (Elrom 2019, 450.)

Another attack that explodes vulnerabilities in code is a CRSF attack, where the attacker exploits service requests to modify and retrieve data and verify the authenticity of POST, PUT and DELETE requests. This attack can be avoided by restricting the set of IPs to which the service responds, filtering out unwanted or unknown IPs that might want to take advantage and use an attack of this kind. There are also many tools available to avoid CRSF attacks. (Elrom 2019, 450.)

The last kind of attack is known as an XSS attack. A cross-site scripting attack is performed by injecting malicious code into a trusted website. There are many tools and libraries to take care of this kind of attack online. (Elrom 2019, 450.)

- Dependency Backdoor Attack: These attacks start as social engineering attacks and then include the injection of malicious software. The social engineering attack is executed by the attacker confining his real identity and motive to gain access to data, similar to phishing. For example, getting an email from someone posing as your boss trying to get some specific information. (Elrom 2019, 450-451.)

  In order to avoid suffering from these kinds of attacks, the best practice as a user is once again to use a cold wallet and keep your confidential information away from a place where it could be stolen when compromised by a vulnerability of this kind. As a developer, it is extremely important to take care when handling open-source libraries. They rely on many packages and libraries from which many are not even supported by their developers, exposing them to an attacker that could inject malicious content into them. (Elrom 2019, 452.)

There are many more attacks that could happen to the blockchain network and more happen every day as attackers learn new techniques and ways to explode the different vulnerabilities they present. As it has been seen through this chapter, there needs to be an effort from both developers and the users of the network put in in order to face the different attacks and issues they might encounter along the way. This amount of effort is not guaranteed at all, as developers tend to half do important steps of the process, and customers do not care

enough to take notice of the issues present and still prevail the same practices they have been doing since forever.

5.3 Blockchains and their applications in cybersecurity

After grasping a good understanding of the vulnerabilities present in the technology, it is time to look at the other side of the coin, the help that blockchain can provide in the cybersecurity field moving forward.

To better understand how blockchains could help cybersecurity, let us see the landscape in this field for these last few years. The Cybersecurity field is growing exponentially every year. As we produce more data, we create new ways to protect it, and so hackers do the same from their side to try and attack them. (Singh 2022.)

The statistics from these past years regarding cybersecurity show some pretty clear points of concern as well as other interesting data that can help in tackling the problem: about 95% of data breaches are the cause of human error, which reinforces the fact that the weakest link in cybersecurity is always the human behind the computer. Data breaches are some of the most common cybersecurity problems and one of the most detrimental when they succeed. In just the first half of 2020, data breaches accumulated the exposure of over 35 billion records. Apart from that, they can come in many forms, which is one of the factors that make them such a huge issue. Of recorded ones, about 45% come from hacking, 22% caused by phishing, and about 17% from malware. (Singh 2022.)

The malware itself is one of the most common causes of cybersecurity concerns. It is very widespread and relatively easy to implement into anything that goes over the internet. For example, over 90% of malware is implanted and delivered by email, an astounding number for such a common use service. Over 200 000 malware samples are produced every single day, with that number expected to also rise exponentially with time. Malware is also hard to recover from once it has hit. About 34% of businesses hit by it took more than a week to regain access to their data. (Singh 2022.)

All in all, cybercrime-related damage was projected to cost about $6 trillion in 2021, with that cost also rising more every year. Ransomware costs have also skyrocketed to about $75 billion every year. (Singh 2022.)

Like many aspects of technology, cybersecurity will also continue to evolve with time, and with cybersecurity, the counterpart of cybercrime will as well. With the rollout of 5G networks, for example, faster download speeds will create more avenues for hackers to expose vulnerabilities and encourage larger attacks. (Singh 2022.)

Another aspect that could be exploited in the future is the Internet of Things (IoT). As of last year, the number of projected devices to be online amounted to about 13.8 billion. With the huge interest the technology has garnered, corporations keep finding new applications for it, and with that, more potential security vulnerabilities that could be exploited by attackers. (Singh 2022.)

This is where blockchains can come in and put their grain of help onto the field. Here are some examples where blockchain could help current cybersecurity problems present:

- Social media platforms are a part of everyday life for a large number of people nowadays. With the number of platforms present rising every year, the same problem keeps being repeated, which is that they are protected by very weak and unreliable passwords. This can cause issues, as large amounts of metadata are collected when interacting in social media applications. If hackers get their hands on this data, the consequences could be very detrimental. Blockchain technology can help by being the backbone of a standard security protocol where it could serve as a better alternative to common end-to-end encryption. (Singh 2022.)

- By using edge devices, which are devices that provide an entry point directly onto the enterprise or service provider's core network, many hackers have been able to gain access to complete systems in the past. With the growth in devices controlling smart homes, a security breach could have dire consequences for the family habituating it. Blockchains can be used to secure those systems or specific devices by decentralizing their administration. (Singh 2022.)

- With the problem mentioned above of the growing amount of data produced every day, storing that data in a centralized way can effectively leave it exposed to attacks performed by hackers. With blockchains, storing that data in a decentralized manner can go a long way to secure it much more, making it almost impossible for attackers to access those storages. (Singh 2022.)

- Blockchains can also verify activities like patches, installers, or firmware updates. They can also be used to protect data from attackers while it is being transferred by using strong encryption. Finally, they can be used to avoid DDoS attacks by decentralizing the Domain Name System (DNS) entries. (Singh 2022.)

The decentralized nature, combined with other characteristics a blockchain has, presents potential uses that could be taken advantage of in the field of cybersecurity. Attributes like the data transparency and integrity it provides could help enterprises trying to find solutions or improvements to their cybersecurity systems.

6 The future of blockchains

6.1 Blockchains moving forward

After getting acquainted with blockchains, one of the most prominent questions that arise is how or in what ways can more be extracted from this technology, which of its redeeming characteristics can be taken advantage of and be used in other fields to improve them, and in what ways can the detrimental aspects of it be improved upon or reduced moving forward.

These themes have already been explored throughout this document, as many concerns about the technology have punctually appeared and many other good qualities have. This question is one that a lot of people in the industry are looking at, and as of now, there are already a lot of views on how this technology can persist and improve in the future.

6.1.1 Scalability

One of the biggest problems for blockchains moving forward is the platform's scalability. The problem originates mainly from the fact that the number of nodes is growing every day, but four main factors affect the scalability of the technology:

- The limitations in processing a transaction are the most important issue, as when it happens, every node must add information regarding that transaction in the ledger. This, in turn, means that the full amount of information of every transaction up until that point could overthrow the system. There is also the fact that every network must contain all the data from its inception up until now to maintain the data accuracy and keep its trust. Finally, the biggest problem stems from hardware limitations which only grow as the networks grow bigger. It becomes increasingly difficult to set up and maintain the hardware that is required to operate nodes. (Geroni 2021b.)
- The second factor affecting scalability is transaction fees. The great growth that has been happening to all blockchain networks these past few years has led to an increase in the complexity of the processes executed to validate transactions which has led to a rise in demand for more computation power to mine. As the number of transactions that want to be passed grows with this, the amount that stays in a queue waiting to be verified grows as well, creating a huge problem. (Geroni 2021b.)
- Block size is another big factor that causes issues for the scalability of blockchains. It is also related to the growing number of transactions that are being done every day as the time it takes to process each one is increased, the queue piles up, and this has led to the block size not being enough to contain the growing number of

transactions, which affects scalability greatly as storing every new blocks becomes increasingly more costly and difficult. (Geroni 2021b.)

- The last factor is also related to transactions. Specifically the aforementioned time it takes for them to be verified. This validation process takes a lot of time, pending transactions start to pile up on the queue, as shown in Image 20, and the time spent in this queue has to be taken into account as well, as it is not trivial. The response time problem is related to the high transaction fees that have to be paid, resulting in a bad scalability problem. (Geroni 2021b.)

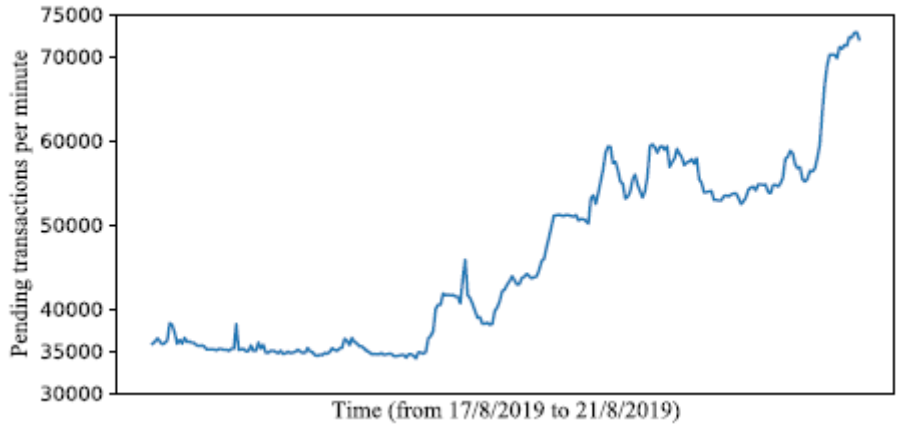

Image 20. The number of Ethereum pending transactions in a certain period. (Zhou et al., according to Etherscan.io, 2020)

All these problems expose the trouble that growth in users and, in turn, transactions can mean for blockchains. If networks cannot be expanded in capacity to adopt new users, then the future can look very bad for the technology and its adoption. Therefore, solutions to these problems have been a huge point for the researchers and programmers working on the subject.

When researching potential solutions for blockchain's scalability problem, one of the main themes is the Blockchain Scaling Trilemma. This trilemma is a loose concept, but it specifies that if you want to improve scalability by using a permissioned network, you are essentially giving up on the decentralization quality of the technology. It states that in blockchains, the only possibility is to have two of the three main qualities: decentralization, scalability, and security. (Geroni 2021b.)

To circumvent this issue, trade-offs and compromises must be made to obtain a decent level of scalability. Some solutions to this are:

- Implement blockchains that use better consensus mechanisms like Proof-of-Stake instead of the common Proof-of-Work. A lot more networks are looking into some new consensus mechanisms that are faster and can solve some scalability problems. The aforementioned PoS does not require the solution of huge cryptographic algorithms as it ensures consensus via the selection of validators according to their stakes on the network. Adoption of this algorithm could boost the capacity of networks along with improving their security and decentralization. (Geroni 2021b.)

- The second solution involves a method based on distributed databases, sharding. As illustrated in Image 21 below, it consists in breaking down transactions into smaller pieces of data called shards, which are then processed simultaneously in parallel, enabling sequential work on multiple transactions. By using sharding, the information could be divided between nodes while still ensuring the consistency of the data. Shards serve as proof for the mainchain while ensuring interaction with each other for sharing addresses, general state, and balances by leveraging cross-shard communication protocols. (Geroni 2021b.)

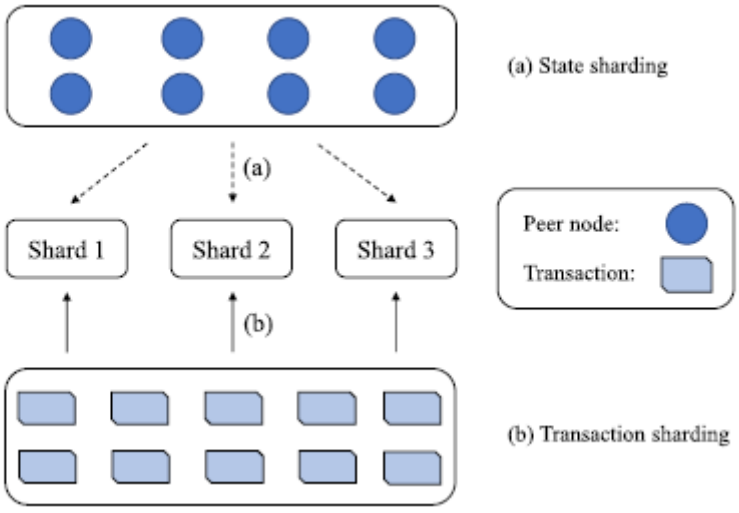

Image 21. A representation of sharding. (Zhou et al., 2020)

- The final solution that provides promising results for solving scalability issues is a nested blockchain. It is a decentralized network infrastructure that leverages the main blockchain for establishing parameters for the larger blockchain network. It ensures the execution of transactions over an interconnected network of secondary chains. This is one of the most promising solutions to the scalability problem blockchains have. (Geroni 2021b.)

All these proposed solutions are still in their experimental stages. Still, they show the potential to proceed to investigate them as the scalability problem is one of the main factors detaining blockchains from growing further and being a staple in technology moving forward. Developers are looking at the problem from many perspectives that have proposed different solutions, such as augmenting block size. Still, not many concepts have been picked up as no answers have been proven to be the best to solve the problem, so the search for a more feasible solution continues. (Geroni 2021b.)

6.1.2 Environmental concerns

The other great concern for blockchains is their growing negative impact on the environment. As the world moves toward becoming more environmentally friendly and away from fossil fuel usage in favor of renewable energy sources to preserve the planet's resources, blockchains stand out by going the opposite way to this trend.

The base of the problem comes from the fact that every time computing power has been mentioned in this document, that power must be produced or obtained from some source, and it comes from these non-environmentally friendly ones. Mining, which is the most popular method to validate transactions, is very energy-consuming. Sometimes, some networks can effectively consume more than an entire country by themselves, as seen in Image 22. (Reiff 2021.)

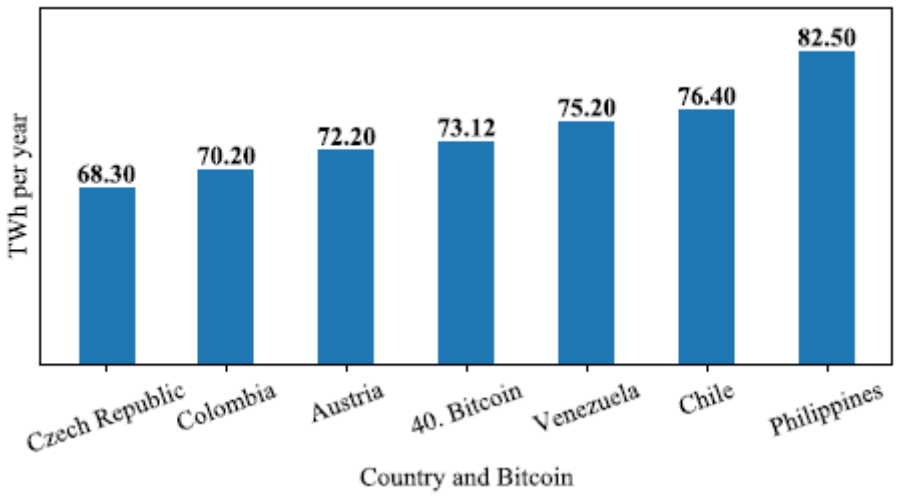

Image 22. Energy consumption by country and Bitcoin. (Zhou et al., according to https://digiconomist.net/bitcoin-energy-consumption, 2020)

The energy required for each blockchain varies, but the most popular is estimated to be using about 2100 kilowatt-hours(kWh), which is about what an average US household con-

sumes in 75 days. As this energy is generated from non-renewable energy sources, blockchains like Bitcoin have an annual carbon footprint comparable to the release of 97.2 megatonnes of carbon dioxide, which roughly equals the number of yearly emissions from Argentina. (Bandera 2022.)

There is still a portion of the energy supply provided by renewable energies such as hydropower which amounts to about 39% of the energy. Still, it is greatly overshadowed by other facts, such as the 30 kilotons of electronic waste mining on Bitcoin's network produces. (Reiff 2021.)

The numbers show a huge problem, as Bitcoin's blockchain uses 91 TWh of electricity each year for mining, which equals about 0.5% of the world's electricity consumption, more than all of Finland annually and nearly seven times more than what Google consumes each year. Mining for Ethereum produces more than 47 million tons of carbon dioxide emissions every year. (Reiff 2021; Bandera 2022.)

Mining also generates a huge amount of electronic waste, as the hardware used to mine becomes obsolete very quickly. (Reiff 2021.)

All this begs the question, can mining require less energy? This is where the use of different consensus mechanisms comes in once again, as the use of Proof-of-Work inevitably brings in high energy usage. The need to have both expensive hardware and huge amounts of electricity to power it is the main characteristic that keeps the security and the competition of the blockchain rolling, but the impact it has on the environment is hugely negative. (Reiff 2021.)

Therefore, dropping this mechanism in favor of others like Proof-of-Stake, Proof-of-History, Proof-of-Elapsed, Proof-of-Burn, Proof-of-Capacity, or other ones that are currently being developed can prove to be the right way to proceed once again as they are methods that do not rely on extensive computing power opting instead for other forms of achieving the same goal. (Reiff 2021.)

6.2 Considerations and experiments for potential applications

Before going over the potential applications for blockchain technology moving forward, it is important to consider some considerations. Since the technology is fairly new, compared to many other areas, many corporations are looking for any possible way to fast track and incorporate it into their plans as the fear of being one of the ones that missed out on it grows. The question most corporations ask themselves is how they can incorporate this technology instead of asking themselves if they need to make use of it. This leads to frustration and

waste of resources when they realize that it can not just simply be used generally in any area. (Yaga et al. 2018,41.)

6.2.1 Considerations

The following list contains some of the features or needs that an organization could encounter that would suit a solution or improvement by using blockchain technology:

- Need of many participants.
- Distributing participants.
- Want or need for lack of trusted third party.
- Workflow is characterized by transactions of digital assets or information between multiple parties.
- There is a need for a globally scarcer digital identifier like it would happen with digital art, digital land, or digital property.
- There is a need for a decentralized naming service or ordered registry.
- A cryptographically secure system of ownership is needed.
- There is a need to reduce or eliminate manual efforts regarding reconciliation and dispute resolutions.
- There is a need to enable real-time monitoring of activity happening between regulators and regulated entities.
- Full provenance of digital assets and full transactional history to be shared between all network participants is needed. (Yaga et al. 2018,41.)

If any of these needs suits the problem the corporation is trying to solve or tackle by using blockchain technology, then the possibility of doing so is there, and they have a good chance of extracting a lot from it. Many agencies and organizations have developed guides to help others determine if blockchains suit their problem or specific system or activity. They help choose the kind of blockchain technology that would benefit them most. (Yaga et al. 2018,41.)

An example of this is what the United States Department of Homeland Security (DHS) Science & Technology Directorate has developed for the case, a flowchart that helps determine whether a blockchain is what is needed for a new project or initiative. This flowchart can be seen below in Image 23:

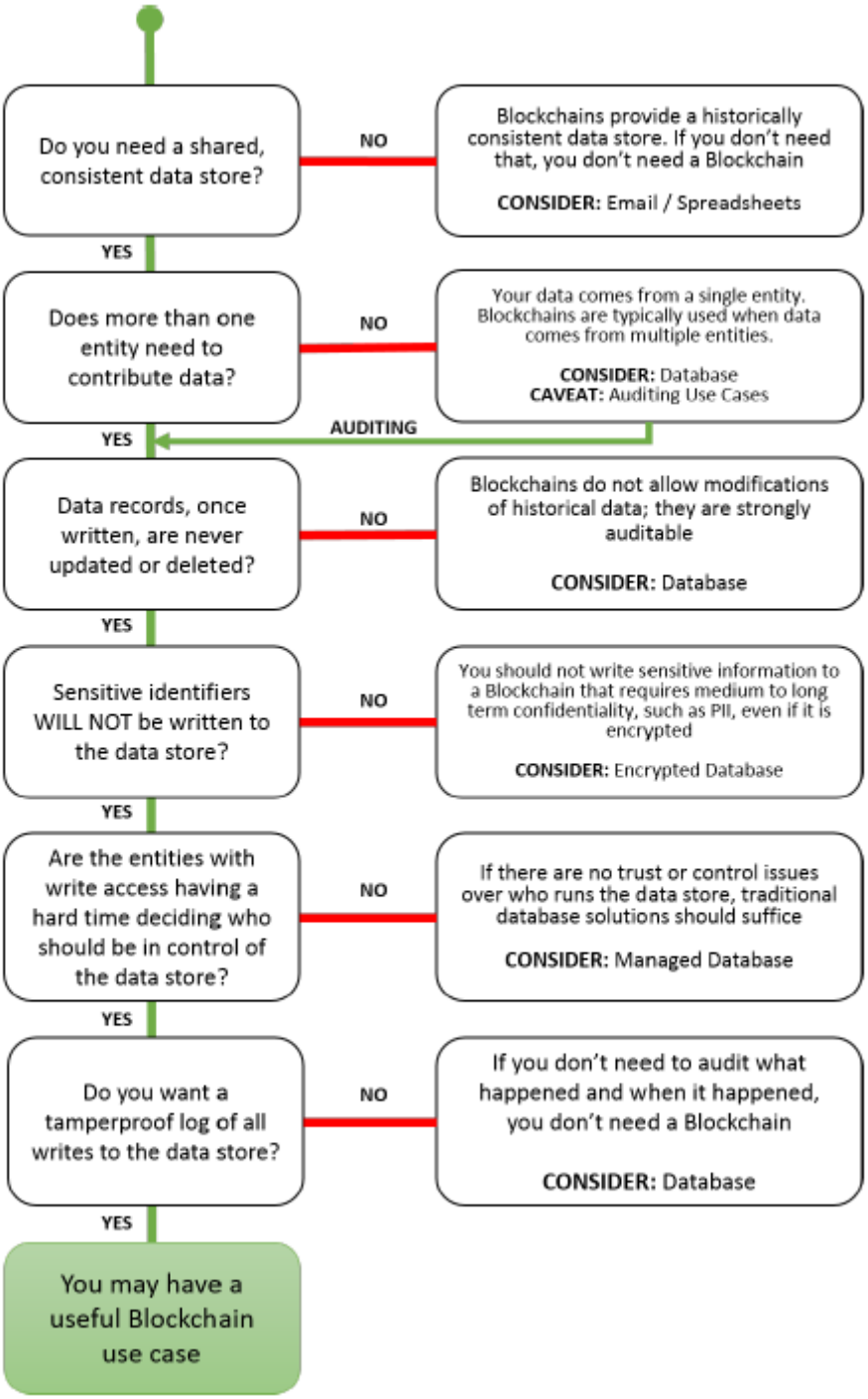

Image 23. DHS Science & Technology Directorate Flowchart. (Yaga et al. 2018,42.)

Like this, many other organizations have taken the same approach of creating guidelines that essentially ask: Do you really need blockchain? As many corporations emphasize the fact that moving away from traditional systems could cause more harm than good. Some articles resort to driving the point home of its good aspects, such as the decentralization, censorship, and others bring up the problem it would cause to use them. Therefore, some

other considerations have to be taken into account before finally deciding to use it: (Yaga et al. 2018,43.)

- Data Visibility is one of the bigger topics, as in the case of using permissioned blockchains, they may or may not reveal the data inside publicly. It may be the case that the data is only visible to those inside the network. Suppose the data stored inside is governed by a set of regulations such as Personally Identifiable Information (PII) or General Data Protection Regulation (GDPR). In that case, the data could not be suited to be stored even with a permissioned blockchain network. (Yaga et al. 2018,44.)

  On the other hand, in permissionless blockchains, which allow everyone to view the data, this data is generally public. However, it still raises questions about whether everyone should have access to this data and if there is any harm in having it that way. (Yaga et al. 2018,44.)

- The full transaction history could be beneficial to some institutions but detrimental to others. (Yaga et al. 2018,44.)

- Avoiding the reception of fake data from the users contributing to the blockchain, such as the case could be for networks that receive data from sensors for IoT purposes. This can be a very difficult task to command. Even if smart contracts could help the cause, they could still cause huge problems. (Yaga et al. 2018,44.)

- The fact that data on a blockchain is tamper-resistant can also create a problem in certain situations. If a set of data must be updated because the old has become obsolete, there are ways to deprecate that data and add the new one to the blockchain. However, that old data would still be contained inside the network even if it is not shown within an application processing the data. (Yaga et al. 2018,44.)

- Transaction processing speed is another one of the considerations to be considered before diving into the technology. As of now, the transactions in the vast majority of permissionless blockchains are still much slower than in other systems because of the slow publication time for blocks. Corporations must ask themselves if their service could sustain the slow processing time. (Yaga et al. 2018,44.)

- Another consideration for organizations is compliance with the rules established by the governments and other entities. Of course, blockchain technology is not excluded from following any applicable laws and regulations. Many regulations affect the information that can be placed on a blockchain or that may limit the type of data that can be transferred across the geographic boundary of the country it is based

on. In other instances, legislations may dictate that the first write of a transaction must be written to a node that is present within their borders. And finally, another example could be the storage of data like federal records, which in the case of the U.S., are subject to many different guidelines, laws, and regulations when storing them and subsequently when using blockchain for this purpose. In any of these cases, the use of a permissionless blockchain is heavily advised against. The use of a sort of hybrid approach that can satisfy all the requirements is recommended. (Yaga et al. 2018,45.)

- In permissioned blockchain networks, the permissions must be considered as well. Granularity for specific user roles inside the blockchain must be determined as in permissioned blockchains the presence of more traditional roles like administrator, user, or validator is a possibility. Deciding who can administer and revoke permissions as well as how easy that task can be is another decision that must be taken. (Yaga et al. 2018,45.)
- Avoiding all the nodes having similar characteristics, such as hardware, location, and messaging schema, is very important to prevent the risk of having these factors be identical to each other. This risk must be mitigated using the decentralization capabilities of the technology and the use of heterogeneous devices. (Yaga et al. 2018,45.)

6.2.2 Blockchain Experiments

This small chapter will be directed toward the several Blockchain experiments that have been going on since the technology entered the spotlight. With the increase in corporations taking an interest in it, a series of them have been doing these so-called experiments to try and obtain new use cases that would suit it. These experiments are often described as use-cases. A good example is the following list presented in Image 24 by Peter Bergstrom: (Lewis 2018,327.)

Image 24. Blockchain potential use cases by industry. (Lewis 2018, according to Peter Bergstrom,327.)

Another example of this is this very detailed infographic from Matteo Gianpietro Zago in the following Image 25, which shows a huge array of different areas in which blockchain could be used in the real world, even going through the length of putting in different companies that have been specializing, experimenting or even already showing example of that exact use case:

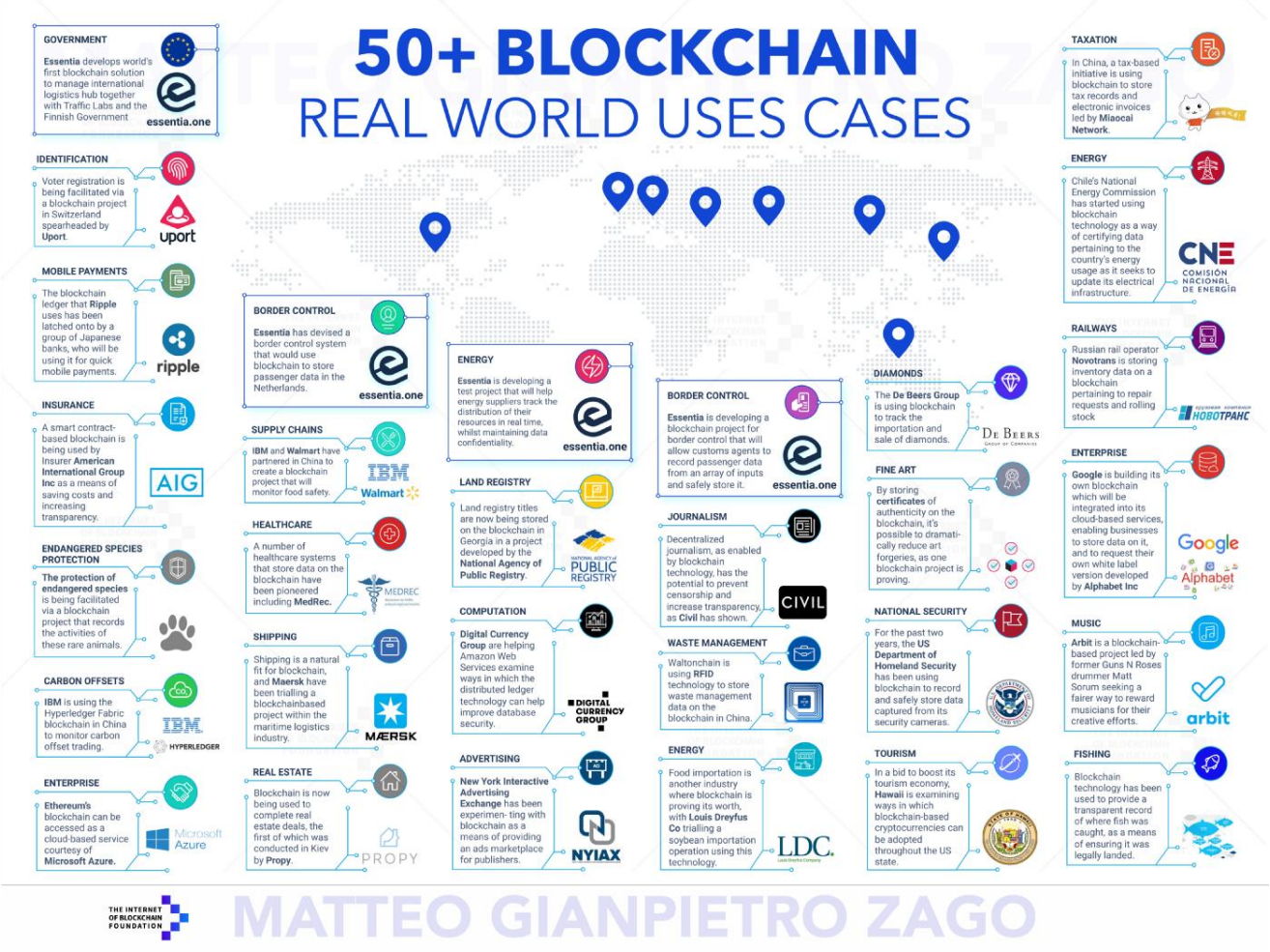

Image 25. Potential blockchain use cases in the real world. (Lewis 2018, according to Zago, 328.)

But these graphics ultimately lead to nothing concrete. These kinds of lists and graphics are done with the purpose of creating more hype for the technology, as they are sharable but ultimately misleading because they are not real use cases but experiments that have been conducted to apply blockchains to multiple kinds of industries and business workflows whether that was done appropriately or not. (Lewis 2018,328.)

These experiments might lead to something that could catch some attention and get picked up to evolve on it. Still, ultimately most of the possibilities raised will be eventually discarded because more appropriate tools already exist for many of the cases presented. This ultimately leads to the same point that it is not clear cut what processes can be improved directly using the technology and if the payoff for doing so is worthwhile. Many of these corporations are starting projects containing blockchain just for the sake of it. They either include the keyword to get more funding or more buzz around the project or to get more enthusiasm from management for using this new technology instead of thinking if the use of it is indeed necessary. (Lewis 2018,329.)

As was the case in the previous point, many questions can be very useful to ask to try and understand the use and value of blockchain technology when conducting one of these experiments.

In the case of public blockchains, it can be very useful to understand:

- Will all parties involved run the nodes, or will one have to trust another?
- If the blockchain is backlogged, what impact will this have on its users?
- In what ways will the project deal with forks and chain splits?
- How is data privacy going to be achieved?
- How will operators keep up with the evolving regulations they will have to comply with?

On the other hand, for private blockchains understanding these points is very useful:

- Who will have the authority to run the nodes, and why will it be that party?
- Who is going to be able to write blocks?
- Who is going to validate blocks and why?
- If the project's purpose is data sharing, why can't a web server be used?
- Is there a natural central authority whom everyone trusts, and if this is the case, why are they not hosting a portal?

Finally, for any blockchain:

- What data is going to be represented on the blockchain, and what data is instead going to be 'offchain'?
- What are the tokens of the blockchain going to represent?
- When a token is passed from one party to another, what does this ultimately mean in real life?
- What is the protocol if a private key is lost or copied? Is this acceptable?
- Are all parties complying with the data that is being passed around the network?
- How will upgrading inside the network be managed?
- What's the content stored inside the blocks?

(Lewis 2018,331.)

Some of these questions are fairly similar to the ones proposed in the last part, and they might take different degrees of relevance depending on the kind of project the corporation is taking on. There will certainly be a lot more to be asked in order to complete the project successfully. (Lewis 2018,331.)

The point of this chapter is not to take the information coming from the media at face value, as most of it is just buzzwords wanting to create more hype and clicks for their articles, opting instead to take a more investigative approach to understand the value of the technology and any of these experiments is the right move. At the stage the technology is standing right now, understanding its trade-offs is better than instantly jumping in and going straight for new projects. (Lewis 2018,331.)

6.3 Potential applications for blockchains

Once the research process is done, and the proper experiments have been conducted, there are a series of industries where the decentralization and application of blockchains could prove to be beneficial in case they were implemented accordingly.

One of the biggest cases gaining traction nowadays is the Internet of Things. On its own, the topic is garnering a lot of interest from the whole world, and more organizations are starting to realize the immense potential it has, so the investments have been going strong these past years. Blockchains can be a technology that can be applied to it and create a great duo.

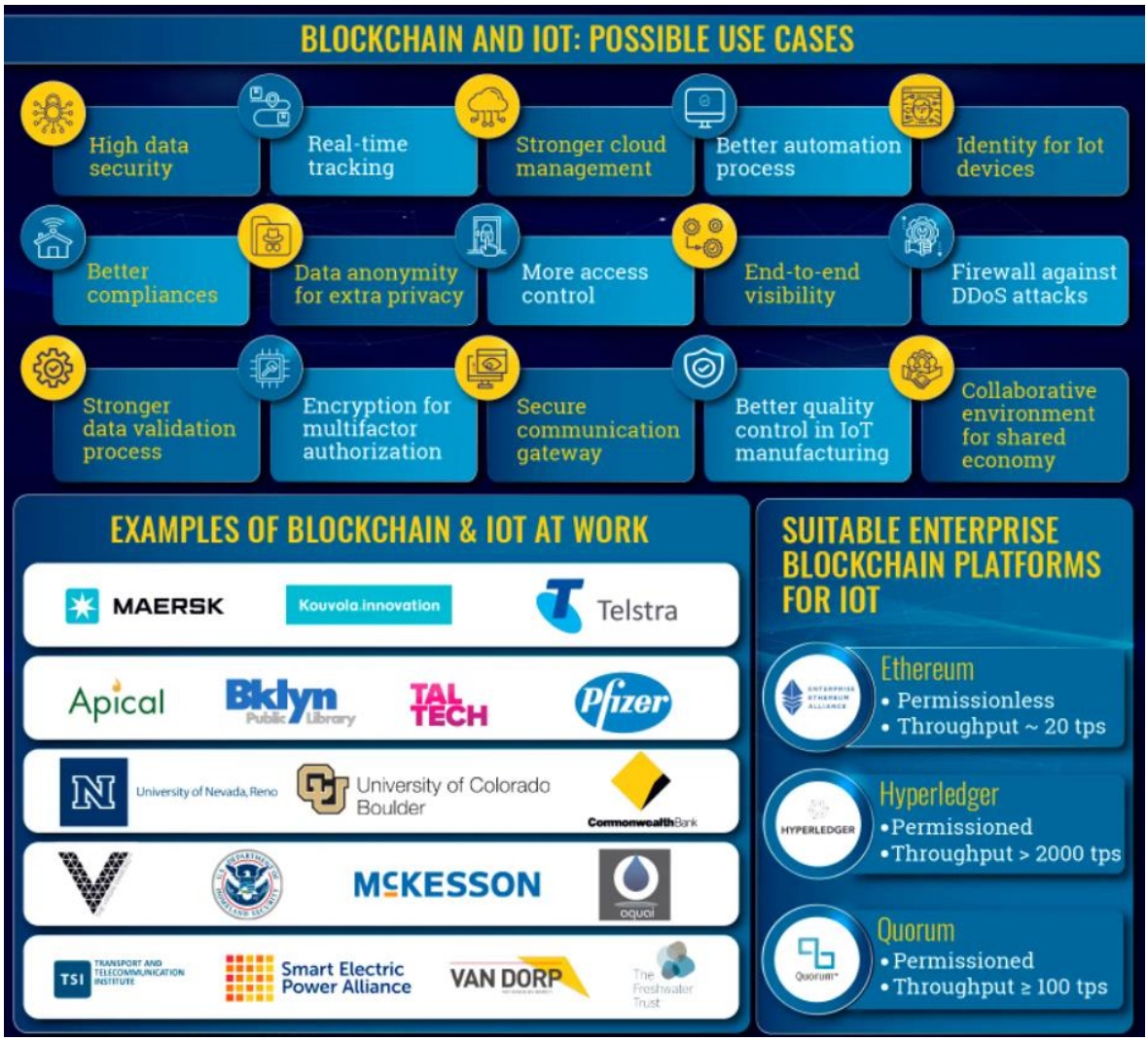

Image 26. Possible use cases of Blockchains and IoT. (Anwar 2019.)

As Image 26 shows, there are many ways in which blockchain could be used inside IoT. One of these cases is the high data security, as it is one of the aspects that raises the most concern with the developers working on it. By using blockchains to aid security, the enterprise would get a full proof secured network that could offer facilities that no third-party provider could, as well as a robust verification process based upon consensus algorithms that would make data entry fairer. (Anwar 2019.)

Other benefits of using blockchain to improve security would include the immutability of the whole system, which would serve when an attacker attempts to manipulate the network as the system would detect and take care of the issue instantly. Having a system that could reliably validate and store the data in its decentralized ledger would also help the IoT scene. (Anwar 2019.)

This last use can be translated to another industry gaining a lot of traction in these last few years, which is Big Data. By next year it is predicted to become a $100 billion industry as

the importance and need for information grows. Applying the characteristics that blockchain brings to the table could improve security. (Anwar 2019.)

These last two points make the storage, transparency, and verification of information stand out as one of the main attractions and containers of the biggest potential inside blockchains. The usage of the technology for this purpose can provide greater security and integrity since the data can be stored in a decentralized way. It will be much harder to hack the system and access or delete the data. It can also mean better access to data since there is no company in the middle overseeing operations and so it can be accessed faster and cheaper as well. (Levy 2022.)

One of the uses related to this is how smart contracts inside blockchains can provide greater transparency to insurance providers by storing all claims or speeding up the process for claimants to receive payments. By storing all the claims in a blockchain, clients would be unable to claim the same event twice, or clients themselves could prove that a certain claim exists and must be complied with. (Levy 2022.)

Another use related to data privacy and protection is the storage of personal data of interest, like social security numbers, date of birth, or others. Storing this data on a blockchain's public ledger would keep it safer than what the current systems offer and make the process of accessing and identifying that information better for industries such as travel, healthcare, finance, and education. (Levy 2022.)

If this private information of citizens is stored inside a blockchain, it could be taken advantage of in the event of voting, as blockchains would ensure that nobody would vote twice and that no votes could be tampered with. Apart from these features, it could also simplify the process of voting since it could be done by making a few swipes on a smartphone. (Levy 2022.)

Another use of citizens' personal information stored inside blockchains would be for the government to use it for their benefits, such as welfare programs, social security, and medical care. It would effectively reduce the chance of fraud and the total cost of running the operations. It could also aid the beneficiaries in receiving the funds faster through digital disbursement via the blockchain. (Levy 2022.)

The storage of data on blockchains could also benefit medical institutions. Keeping medical records stored on a blockchain would allow doctors and other medical professionals in the field to obtain accurate and up-to-date information regarding their patients with a lot more efficiency and speed, allowing for more timely treatment in some cases. This system would

ensure that patients attending different doctors could receive the best care possible. (Levy 2022.)

Other properties that come with blockchains, such as smart contracts, can be used in other areas like real estate, where transactions require a ton of paperwork to verify the financial information and ownership to transfer deeds and titles to the new owners. Making use of blockchains to record real estate transactions could provide the means for a more secure and accessible form of verifying and transferring ownership, which would ultimately speed up transactions, reduce paperwork and save money. (Levy 2022.)

Using blockchain technology in logistics and supply tracking is one of the applications that is already a reality in some corporations. Using it to track items as they move through logistics or a whole supply chain network can provide advantages as it eases communication between the different parties involved because data is available and secured in a public ledger. It cannot be altered either, so it strengthens trust. This all turns into everyone involved working together easily and with great trust. (Levy 2022.)

The last set of potential applications has been gaining lots of attention, especially this year. Using blockchain to track music and film files distributed around the internet can be made to make sure that artists are rightly paid for their work. It can also be used to reduce the amount of piracy in the industry since files will not be able to be reproduced. The technology can also be used to track playbacks on streaming services such as Spotify and provide a smart contract that could provide greater transparency and assurance that the artists would be receiving the correct amount of money they are owed. (Levy 2022.)

This kind of use could lead to the controversial non-fungible tokens, also known as NFTs. These are commonly described as a means to digitally own the rights to digital assets, including any digital art. Since it prevents that asset from being duplicated, it can make the experience like investing in physical art but instead just owning a receipt that specifies that you own that asset. NFTs are controversial for many reasons, but they have been a hot topic in social media for some time now as they have started to gain more traction and attention, mainly because of exposure brought by celebrities and other people of influence. (Coggan 2022.)

Excluding the concerns that already carry over from using blockchain technology, like the immense amount of computational power required and electricity consumed to make the NFTs, there are also a lot of artists that have raised their voices concerning the use of these tokens in their ecosystem. They are angry that NFTs are changing hands for astronomical amounts of money and that money is more often than not leading to other parties that are not the artist. Given that the original purpose of these tokens was to give control by asserting

digital ownership of your assets, the idea that they are becoming elitist is causing a lot of tension. The buy-in barrier is already pretty big to overcome for the common foe, and the actual cost to buy one of these NFTs means the marketplace is becoming a playground for the super-rich. (Coggan 2022.)

Apart from this, many people are using NFTs with direct malicious intent by creating illegal scams and auctions where tokens created using other famous brands without consent are being sold for huge amounts of money. This once again shows the obscure side of the whole technology, which has taken a lot of traction and interest from many people worldwide for the wrong reasons. (Coggan 2022.)

7 Summary

All that blockchains have proven to be is a big talking point for all the wrong reasons. Blockchains could potentially improve some areas where they can be exploited completely. These areas are very scarce and not very common. Even in those specific areas, the already implanted policy or way of doing things would work much smoother than a blockchain until it could be fully adapted. Blockchains falter when going up against the tasks pit against them in all the other areas. Some concepts, like storing personal data from citizens or medical records in a shared public ledger, are flawed per se and should never be considered as it would be nightmarish if they were realized. Others like using blockchains to “revolutionize” the global shipping industry and reduce fraud inside it. They can only track things already being tracked by manufacturers and shippers, so it would not be a revolution but a standardization. This claim also relies heavily on the fact that every manufacturer would pick the same chain, which is a bold assumption. Many firms want all their information centralized and concealed to protect themselves from corporate espionage. The reason why no decentralized, shared ledger has been used to put all the information is not that it’s been impossible, but because it’s highly undesirable.

The bigger problem, in that case, is heavily related to the fraud part. Man-in-the-middle attacks, which are the ones blockchains try to protect themselves from most heavily, are rare. Global shipping needs to deal with it in certain capacities. Still, most fraud doesn’t come from altering information as it is being passed between parties, but rather from colluding parties that entered bad information at the start of the process. Most fraud comes from people who technically have permission to be doing what they’re doing. Blockchains have made them absurdly easy rather than preventing these common types of fraud. The main reason they need to be so resistant to these man-in-the-middle attacks is that the decentralized nature of the network makes them acutely vulnerable to those attacks. This all means that blockchains fall short at doing most of the things they’re trying to do, and a lot of the innovations in blockchains are attempts at solving problems that blockchains introduced.

The other side of blockchains is the completely negative future perspective they currently have: No scalability at all for years since their creation, no advances on that front, and only empty claims backed up by the word of the developers. And, of course, the incredibly negative environmental impact still has not seen any improvement either, as the more efficient consensus mechanisms are still the less common. And, even if they are more efficient, they are still highly redundant and high energy-consuming. Both these problems are still not seeing the light at the end of the tunnel, and it does not seem like that front will improve in

the coming years. All that leaves blockchains as just simply a giant log of transactions with loads of inherent problems that don’t seem to have a plausible solution.

References

Adam Levy. Published in 2022. 15 Applications for Blockchain Technology. Retrieved on the 11th of March 2022. Available at https://www.fool.com/investing/stock-market/market-sectors/financials/blockchain-stocks/blockchain-applications/

Andreas M. Antonopoulos, Dr. Gavin Wood, 2018.Ebook. Mastering Ethereum, Building smart contracts and DApps. Sebastopol, California, United States: O'Reilly Media, Inc. https://github.com/ethereumbook/ethereumbook

Andreas M. Antonopoulos. Mastering Bitcoin, Programming the open blockchain. Ebook. Sebastopol, California, United States: 2nd edition O'Reilly Media, Inc. https://github.com/bitcoinbook/bitcoinbook

Antony Lewis, 2018. The basics of bitcoins and blockchains.Ebook. Miami, Florida, United States: Mango Publishing Group. Amazon

Art Malkov. Published in 2021. Where Is Blockchain Now? Current Trends Affecting the Industry's Enterprises. Forbes. Retrieved on the 8th of February 2022. Available at https://www.forbes.com/sites/forbesbusinesscouncil/2021/03/03/where-is-blockchain-now-current-trends-affecting-the-industrys-enterprises/?sh=5a230f5033ce

Chris Burniske, Jack Tatar,2018. Cryptoassets, The innovative Investor's Guide to Bitcoin and Beyond. Ebook. New York, New York, United States: McGraw-Hill Education. Amazon

Diego Geroni. Published in 2021. Blockchain Scalability Problem – Why Is It Difficult To Scale Blockchain. Retrieved on the 8th of March 2022. Available at https://101block-chains.com/blockchain-scalability-challenges/

Diego Geroni. Published in 2021. Top 5 Blockchain Security Issues In 2021. Retrieved on the 1st of March 2022. Available at https://101blockchains.com/blockchain-security-issues/

Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. Blockchain Technology Overview. Retrieved on the 2nd of February 2022. Available at https://doi.org/10.6028/NIST.IR.8202

Elad Elrom, 2019. The Blockchain Developer.Ebook. New York, USA: Apress. Amazon

Ethereum. Published in 2021. SMART CONTRACT LANGUAGES. Retrieved on the 17th of February 2022. Available at https://ethereum.org/en/developers/docs/smart-con-tracts/languages/

Fredrik Svantes. Published in 2022. INTRODUCTION TO DAPPS. Retrieved on the 18th of February 2022. Available at https://ethereum.org/en/developers/docs/dapps/

Georgia Coggan. Published in 2022. What are NFTs? non-fungible tokens explained. Retrieved on the 12th of March 2022. Available at https://www.creativebloq.com/features/what-are-nfts#:~:text=Why%20are%20NFTs%20controversial%3F&text=There's%20a%20lot%20of%20money,a%20huge%20amount%20of%20energy.

Gerardo Bandera. Published in 2022. Is Cryptocurrency bad for the environment? Retrieved on the 9th of March 2022. Available at https://www.fairplanet.org/story/is-cryptocurrency-bad-for-the-environ-ment/#:~:text=It%20is%20estimated%20that%20each,generate%20exorbitant%20greenhouse%20gas%20emissions.

Hasib Anwar. Published in 2019. Blockchain and IoT: The dynamic duo. Retrieved on the 11th of March 2022. Available at https://101blockchains.com/blockchain-and-iot/#4

Jake Frankenfield. Published in 2021. Decentralized Applications (dApps). Retrieved on the 18th of February 2022. Available at https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp

Jake Frankenfield. Published in 2021. Merkle Root (Cryptocurrency). Investopedia. Retrieved on the 3rd of February 2022. Available at https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp#:~:text=A%20Merkle%20root%20is%20the,block%20in%20a%20blockchain%20network.

Kate Ashford, John Schmidt. Published in 2022. What Is Cryptocurrency? Retrieved on the 11th of February 2022. Available at https://www.forbes.com/advisor/investing/what-is-cryptocurrency/

Kaya Ismail. Published in 2021. A Look at the Current State of Blockchain. CMS Wire. Retrieved on the 8th of February 2022. Available at https://www.cmswire.com/information-management/a-look-at-the-current-state-of-blockchain/

Lyle Daly. Published in 2022. What Is Proof of Work (PoW) in Crypto? The Motley Fool. Retrieved on the 3rd of February 2022. Available at https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/proof-of-work/#:~:text=The%20proof%2Dof%2Dwork%20algorithm,too%20slowly%2C%20they%20get%20easier.

Mariela Naydenova. Published in 2017. Stability in the Ethereum network. Retrieved on the 15th of March 2022. Available at https://www.leaprate.com/cryptocurrency/ethereum/stability-ethereum-network/

Morgan C. Benton and Nicole M. Radziwill. Quality and Innovation with Blockchain Technology. Retrieved on the 31st of January 2022. Available at https://arxiv.org/abs/1710.04130

Nathan Reiff. Published in 2021. What's the Environmental Impact of Cryptocurrency? Retrieved on the 8th of March 2022. Available at https://www.investopedia.com/tech/whats-environmental-impact-cryptocurrency/

Nawari O. Nawari, Shriraam Ravindran. Published in 2019 .Blockchain technology and BIM process: Review and potential applications. Retrieved on the 10th of March 2022. Available at https://www.academia.edu/40578593/Blockchain_technology_and_BIM_process_Review_and_potential_applications?from=cover_page

Pam Baker. Published in 2021. Today's blockchain use cases and industry applications. TechTarget. Retrieved on the 8th of February 2022. Available at https://www.techtarget.com/searchcio/feature/Todays-blockchain-use-cases-and-industry-applications

Published by Forrester in 2019. Seize The Day: Public Blockchain Is on The Horizon. Retrieved on the 8th of February 2022. Available at https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/blockchain/ey-public-blockchain-opportunity-snapshot.pdf

Qiheng Zhou,Huawei Huang, Zibin Zheng & Jing Bian .Published in 2020. Solutions to Scalability of Blockchain: A Survey. Retrieved on the 8th of March 2022. Available at https://ieeexplore.ieee.org/abstract/document/8962150

Sarwar Sayeed,Hector Marco-Gisbert,Tom Caira. Published in 2020.Smart Contract: Attacks and Protections. Retrieved on the 11th of April 2022. Available at https://www.researchgate.net/publication/338926064_Smart_Contract_Attacks_and_Protections

Simanta Shekhar Sarmah. Understanding Blockchain Technology. Retrieved on the 15th of January 2022. Pages 23-29. Available at https://www.researchgate.net/profile/S-Sarmah/publication/336130918_Understanding_Blockchain_Technology/links/5d913eb9a6fdcc2554a69c7c/Understanding-Blockchain-Technology.pdf

Siraj Raval, 2016.Ebook. Decentralized Applications, Harnessing Bitcoin’s Blockchain Technology. Sebastopol, California, United States: First edition O’Reilly Media, Inc.

Statista. Blockchain technology use cases in organizations worldwide as of 2021. Retrieved on the 8th of February 2022. Available at https://www.statista.com/statistics/878732/worldwide-use-cases-blockchain-technology/

Surajdeep Singh. Published in 2021. Potential Use Cases of Blockchain Technology for Cybersecurity. Retrieved on the 28th of February 2022. Available at https://www.itbusinessedge.com/security/potential-use-cases-of-blockchain-technology-for-cybersecurity/

Tetiana Boichenko. Published in 2018.Nuts and bolts of Ethereum smart contract development for businesses. Retrieved on the 11th of April 2022. Available at https://www.n-ix.com/nuts-and-bolts-ethereum-smart-contract-development-businesses/

User Fabrisde. Published in 2019.Getting Deep Into EVM: How Ethereum Works Backstage. Retrieved on the 3rd of April 2022. Available at https://medium.com/@fabrisde167/getting-deep-into-evm-how-ethereum-works-backstage-ea70203e3124