PRIVACY PRESERVING BLOCKCHAINS AND QUANTUM SAFETY

Universitat Oberta de Catalunya

Zuzanna Elzbieta Szalaty Szalaty

Privacy

TF Tutor Name

Katarzyna Kowalska

Professor responsible for the department

Andreu Pere Isern Deyà

Date

13/07/2023

Universitat Oberta de Catalunya

uoc.edu

FINAL WORKSHEET

Work title:	*Privacy preserving blockchains and quantum safety*
Author's name:	*Zuzanna Elzbieta Szalaty Szalaty*
Consultant name:	*Katarzyna Kowalska*
PRA name:	*Andreu Pere Isern Deyà*
Delivery date (mm/yyyy):	*06/2023*
Degree or program:	*Informatics Engineering*
Final Work Area:	*Privacy*
Language of work:	*English*
Keywords	*Blockchain, Monero, cryptography.*

Resumen del Trabajo

La privacidad se ha convertido en un factor importante para cualquier usuario. Hoy en día se ofrecen formas de preservar la privacidad, en cualquier entorno, sobre todo en el mundo del Blockchain que es algo que avanza día a día. Sin embargo, esas soluciones se ven en peligro ante la inminente aparición de los ordenadores cuánticos. Soluciones como el cambio del tipo de criptografía podrían ofrecer respuestas ante la aparición de adversarios cuánticos.

Abstract

The protection of one's privacy has become a necessity for every user. Currently, it is possible to maintain privacy in any application, but especially in the ever-evolving world of Blockchain technology. However, these solutions are

in jeopardy because quantum computers are imminent. The emergence of quantum adversaries could be countered with measures such as modifying the type of cryptography.

Index

List of figures

1. Introduction

1.1 Context and needs

Nowadays the preservation of privacy is one of the biggest concerns when using technology. Blockchain offers a wide range of possibilities and functionalities in different fields, not only in cryptocurrency but also revolutionizes and provides innovation with concepts such as eHealth, Iot, supply chains or smart cities [1].

However, the majority of Blockchains do not offer complete privacy, despite innovating and streamlining numerous processes. Whenever a transaction involving bitcoins occurs, all relevant information is stored and available to all users. Additionally, the aforementioned information cannot be changed or deleted, which is in violation of the GDPR's right to be forgotten [1].

Due to this problem, different methods have been emerging over time to urge the anonymity of the user and allow users to have control over their data. However, despite the fact that some of these methods are efficient, another problem arises: these proposed methods are threatened by quantum computers [1,2].

Many of the methods mentioned above to protect privacy are based on problems or algorithms that are difficult to solve or that require a long time to solve by classical computers. However,since quantum computers are faster and stronger,they can solve problems such as keys and hashes faster,so encryption and data protection are threatened. Therefore,privacy faces not only the challenge of protecting it from human and computer threats,but also a new threat,quantum computers. This problem opens the way for the creation of a program called the Post-Quantum Cryptography Standardization Program, launched by the National Institute of Standards and Technology,which seeks to find a new algorithm that can resist attacks generated by these quantum computers [2].

In this work, an analysis and investigation of the threats to privacy, the reliability of the proposed methods, and their effectiveness against quantum computers will be carried out. Finally, a specific blockchain case that is certainly not quantum safe will be investigated, and an attempt will be made to propose a solution to solve the problem.

1.2 Objectives

The following work is carried out to fulfill two main objectives. The first objective is the review of the privacy preserving blockchains and their methods in order to determine whether the mentioned methods are quantum safe or not. After providing an overview of the aspects related to privacy, the next objective is the study of a specific blockchain that is not quantum safe and after analyzing its operation, it will be intended to provide some solution or method to make it quantum safe.

In order to achieve the main objectives the following actions should be taken:

- To study and to comprehend the concept of privacy and quantum safe in Blockchain.
- To study the existing methods to preserve privacy on Blockchain.
- To investigate a specific blockchain (such as Monero).
- To provide some fix in order to preserve privacy which is quantum safe, based on what was discovered about the chosen Blockchain.
- To present the conclusions of the conducted study.

1.3 Impact on sustainability, ethical-social and diversity

Regarding ethical competencies and gender perspective, the Sustainable Development Goals with which the TFM is aligned are listed below:

The SDG (Sustainable Development Goal) “Build resilient infrastructure, promote sustainable industrialization and foster innovation”. In this paper, the methods that favor privacy preserving for the Blockchain are studied, since the Blockchain is known for its role in supply chains, which is an important part of sustainable development [3].

Blockchain is a technology that also favors the inclusion of any country in the process, such as Blockchain transactions, since it lacks intermediaries and allows its use by anyone from anywhere in the world, in addition to providing a tool with total transparency [4].

By analyzing privacy preservation and the methods to achieve it in Blockchain, in addition to trying to propose a quantum safe solution, it is intended to offer tools to users so that the use of Blockchain does not imply a violation of privacy.

1.4 Methodology

The methodology used in this work is quantitative. This is a theoretical work in which the different existing methods to preserve privacy in blockchain will be analyzed, in addition to evaluating whether they are methods that are quantum safe. In addition, a technology that is not quantum safe will be analyzed, and from the data and information collected during the investigation on privacy-preserving methods, a solution to quantum safety will be offered.

This work has been divided into different phases and in each one of them the process is similar. The first step is the searching and collection of information, next the analysis of the information collected and finally conclusions. In order to fulfill the second objective of this work, one more step is added, which is the proposal of a solution after the investigation of existing privacy preserving methods.

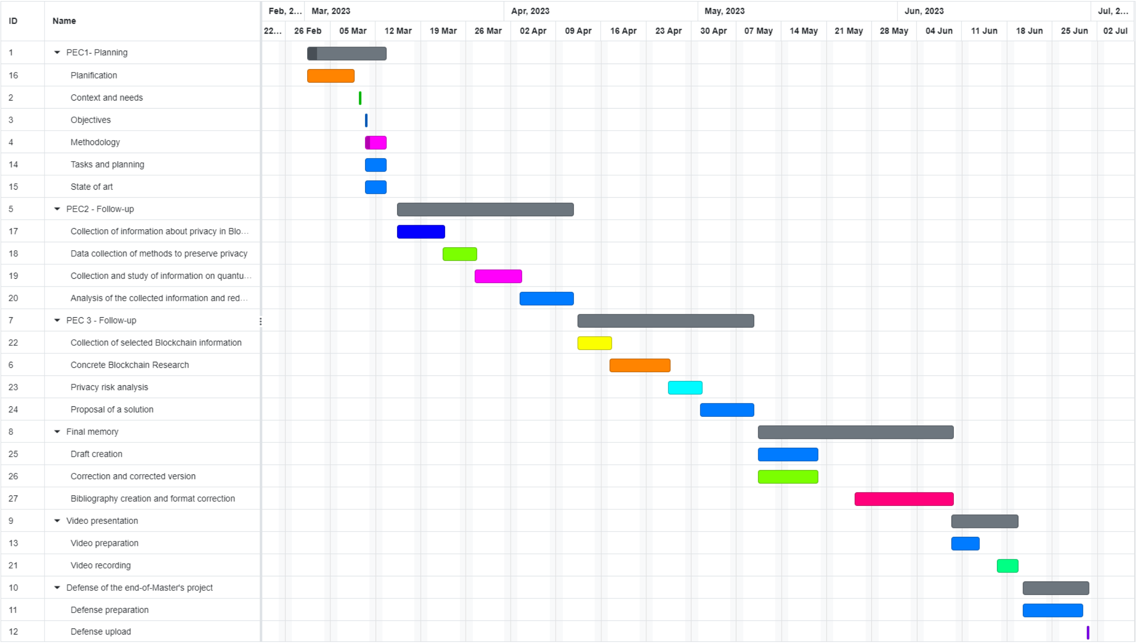
1.5 Tasks and planning

The following table shows the planning carried out for the TFM. It has been divided into six phases that coincide with the campus tasks.

Name	Start Date	End Date
PEC1- Planning	**Mar 01, 2023**	**Mar 13, 2023**
Planification	Mar 01, 2023	Mar 08, 2023
Context and needs	Mar 09, 2023	Mar 09, 2023
Objectives	Mar 10, 2023	Mar 10, 2023
Methodology	Mar 10, 2023	Mar 13, 2023
Tasks and planning	Mar 10, 2023	Mar 13, 2023
State of art	Mar 10, 2023	Mar 13, 2023
PEC2 - Follow-up	**Mar 15, 2023**	**Apr 11, 2023**
Collection of information about privacy in Blockchain	Mar 15, 2023	Mar 22, 2023
Data collection of methods to preserve privacy	Mar 22, 2023	Mar 27, 2023
Collection and study of information on quantum safety in Blockchain	Mar 27, 2023	Apr 03, 2023
Analysis of the collected information and redaction	Apr 03, 2023	Apr 11, 2023
PEC 3 - Follow-up	**Apr 12, 2023**	**May 09, 2023**
Collection of selected Blockchain information	Apr 12, 2023	Apr 17, 2023

Concrete Blockchain Research	Apr 17, 2023	Apr 26, 2023
Privacy risk analysis	Apr 26, 2023	May 01, 2023
Proposal of a solution	May 01, 2023	May 09, 2023
Final memory	**May 10, 2023**	**Jun 09, 2023**
Draft creation	May 10, 2023	May 19, 2023
Correction and corrected version	May 10, 2023	May 19, 2023
Bibliography creation and format correction	May 25, 2023	Jun 09, 2023
Video presentation	**Jun 09, 2023**	**Jun 19, 2023**
Video preparation	Jun 09, 2023	Jun 13, 2023
Video recording	Jun 16, 2023	Jun 19, 2023
Defense of the end-of-Master's project	**Jun 20, 2023**	**Jun 30, 2023**
Defense preparation	Jun 20, 2023	Jun 29, 2023
Defense upload	Jun 30, 2023	Jun 30, 2023

Figure 1 shows an initial Gantt chart showing tasks with their corresponding time frames.



ID	Name
1	▾ PEC1- Planning
16	Planification
2	Context and needs
3	Objectives
4	Methodology
14	Tasks and planning
15	State of art
5	▾ PEC2 - Follow-up
17	Collection of information about privacy in Blo...
18	Data collection of methods to preserve privacy
19	Collection and study of information on quantu...
20	Analysis of the collected information and red...
7	▾ PEC 3 - Follow-up
22	Collection of selected Blockchain information
6	Concrete Blockchain Research
23	Privacy risk analysis
24	Proposal of a solution
8	▾ Final memory
25	Draft creation
26	Correction and corrected version
27	Bibliography creation and format correction
9	▾ Video presentation
13	Video preparation
21	Video recording
10	▾ Defense of the end-of-Master's project
11	Defense preparation
12	Defense upload

Figure 1: Gantt Diagram

1.6 State of art

To carry out this work, different resources are used, such as scientific articles obtained from databases such as the IEEE Xplore library, as well as journal surveys. Basic concepts are investigated about what a Blockchain is, its privacy threats, requirements of blockchain privacy preservation and methods to preserve it.

Methods to preserve privacy are found in numerous articles, including ring signature, non-interactive zero-knowledge proof and mixing services [5, 6]. A large amount of information is found on the mentioned methods, however, in these articles their effectiveness against quantum computers is not mentioned. Regarding the second objective of this work, Monero, a Blockchain which is not quantum safe, is a privacy-centric cryptocurrency that attracts more users due to the improvements in their privacy with respect to Bitcoin. However, these improvements are not enough since it continues to have weaknesses related to its mixin sampling strategy [7].

In light of this, numerous scientific articles have led to the discovery of a potential quantum-safe solution for the Monera cryptocurrency. Lattice-based cryptography is a solution, but it is imperfect because it is currently inefficient; therefore, additional research and development must be conducted to completely replace elliptic curve cryptography and ensure that Monero is resistant to quantum computer attacks.

2. Blockchain

2.1 Introduction

Blockchain technology is based on transactions that are sent between users, it can be cryptocurrencies like Bitcoin in whose transactions Bitcoins are sent. It is called a blockchain because it is a chain of blocks. Each block has a unique identifier that corresponds to the hash value of its head, i.e. it comes from the block value (content) and also contains the hash value of the previous block, which points to that block [8].

This is a structure that ensures that the information contained in the block or the header itself is complex to manipulate. If a block is modified, the hash of the next block and the next block must be modified because they are grouped with the above-mentioned hash. Another reason why it is almost impossible to change the block transaction is due to the mechanism on which the blockchain is based called “proof of work”, making such changes very computationally expensive [8].

In order to ensure the effectiveness and security of the Blockchain, the above-mentioned Proof of Work protocol is used. The name of this protocol stems from the fact that the client must do the work and that work must be verified by the network. As explained, this is done by obtaining the nonce value through complex computation operations. This is an asymmetric process because the part that is performed by the client is quite difficult while the network verification is relatively simple [7].

Proof of work is the method to confirm and obtain new blocks for the network. Miners are responsible for confirming transactions and ordering blocks. This procedure involves the use of special processing units and electronic circuitry to solve complex mathematical puzzles, resulting in considerable power consumption. The miners compete with each other to solve these puzzles. The winner can update the Blockchain, verifying the latest transactions and is rewarded with a predetermined amount of cryptocurrency [9].

Bitcoin was the first Blockchain to use this type of consensus mechanism and was followed by other Blockchains such as Ethereum. However, many Blockchains are currently migrating to a Proof of Stake consensus mechanism.

Proof of Work is used to prevent users from over-generating or counterfeiting cryptocurrency. At the same time, it has the function of preventing double spending (someone spending the same cryptocurrency more than once). There is no entity that controls cryptocurrencies, so Proof of Work is needed to prevent theft or counterfeiting [9].

Like the Proof of Work protocol, the Proof of Stake protocol is based on consensus among network participants. The nodes working in this protocol are called validator nodes, which are randomly chosen to decide whether to validate a block and whose task is to validate transactions or create new blocks. To validate operations, the validator nodes do not need to solve complex puzzles in Proof of Work [10].

This system has many advantages. It keeps a decentralized Blockchain secure. To create illegitimate transactions it would be necessary for the attacker to corrupt 51% of the nodes on the network. As the value of cryptocurrency increases, more and more miners are motivated to join the network, which makes the Blockchain more secure and gives it more power. It is impossible for transactions to be intercepted by an attacker because of the processing power used and implicitly the number of nodes in the network [9].

If someone wishes to alter the balance, a new transaction must be generated. Another reason why changing the content of this blockchain is almost impossible is because there are copies of it. Therefore, in the remote case of having modified it, the other participants in the network will discard it when they notice the difference between the original and the copy. This and the previous reasons make the Blockchain a technology in which it is almost impossible to modify and in which everything is recorded publicly, mimicking accounting books [8]. Blockchain Technology is known as Distributed Ledger Technology (DLT).

2.2 Blockchain features

The characteristics that define the technology of the blockchain are immutability, transparency and decentralization. It is immutable because nothing that has happened in the system can be deleted or modified.

Since every transaction is completely transparent and requires the approval of 51% of participants, the information can be verified at any time by any participant.

Finally, decentralization is due to the fact that the information is distributed (replicated) to several nodes, so it is not concentrated in one place, avoiding single failure points and offering large information availability to the participants [11].

In the network of nodes, two types of nodes can be distinguished: users carrying out transactions with cryptocurrencies and the nodes managing the network. Mining nodes are responsible for sharing and storing all the information on the blockchain (complete copies), but ordinary users only need the necessary parts to complete their transactions successfully because the data will be sent to the mining nodes [11].

In the case of transactions in Blockchain, this consists of a user (identified and authenticated) having to sign the transactions carried out with the digital signature cryptography mechanism; for example, in the case of Bitcoin, the ECDSA (Elliptic Curve Digital) system is used. To conduct this transaction, the information that the user must send is the number of assets to be transferred, its public key, the recipient's public key, and they must sign the data with their private key [11].

After initiating a transaction, the miners are responsible for checking the validity of this transaction (they examine not only one transaction, but several transactions because they collect groups of transactions to examine them) and the mining process would begin. It should be noted that the mining of the block is attempted by several miners and whoever succeeds in doing it is the one who sends the same mined block to the other nodes of the blockchain. Figure 2 shows the operation scheme of the blockchain transaction, where the owner of the transaction is identified as having two public and private keys that sign the transaction by generating a digital signature.

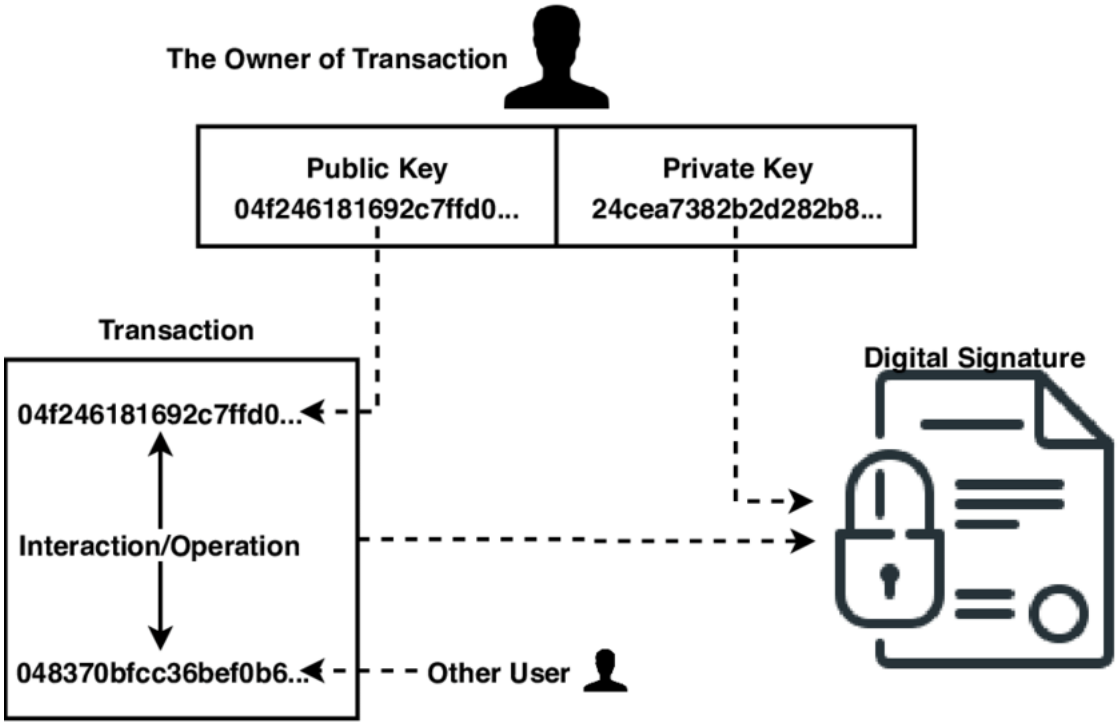


Figure 2: Blockchain transaction [12].

To understand the mining process, it is worth pointing out the elements that make it: the block name, which is the hash of the block name and is the block identifier and generated twice using the SHA256 hash function; the hash of the previous block; nonce, which is the value that must be obtained during the mining process and must be a very small value that results in the calculation of the double hash of the name; the time stamp, which is when the block has been created and the root of the The nonce value is difficult to find and computationally expensive since the miners have ten minutes to find it and a conventional computer could take hundreds of years to find it [11].

Due to the fact that it is so complex to obtain, proof-of-work technology is used to verify transactions and mining, making blockchain transactions safe. However, there are also challenges that this technology faces, an example of which is the 51% problem. As previously mentioned, 51% of the mining nodes must approve all transactions, which could be problematic if someone controlled 51% of the network and was able to carry out fraudulent transactions that he or she would personally approve and reach a fraudulent consensus [11].

3. Privacy in Blockchain

Today, we are more connected than ever and, at the sametime, more exposed than ever before. Blockchain is now applied in many areas such as health care, Big Data, ad-hoc networks, and industry 4.0, IoT, storage, business and cryptography.

3.1 Introduction

Blockchain is not controlled by anyone (third party), which is simultaneously a disadvantage and a benefit. Blockchain security is based on elliptic curve encryption, which consists of public key encryption (asymmetric encryption) based on elliptic curves. Elliptic Curves are flat curves represented by the following equation:

$$y^2 = x^3 + ax + b$$

Users who wish to interact with the Blockchain generate their keys using this equation [13].

The use of Blockchain also involves certain risks, such as hijacking consensus mechanisms through user coalitions (51 per cent attacks), mining sidechain or parallel chains, distributed service denial attacks through the injection of many spam transactions and attacks focused on permissioned blockchain capabilities. As far as privacy is concerned, blockchain technology does not comply with GDPR (General Data Protection Regulation), and in smart contracts personal data leakage may occur [14].

The types of information exposed in transactions utilizing this technology must be considered: on the one hand, there is direct information about senders and recipients, and on the other hand, there is information about third parties involved in transactions [14].

The blockchain technology is still in development, and it faces certain privacy challenges, such as the challenge of correcting things (as once the transaction is made, you cannot make any corrections) or the right to be forgotten. It provides transparency, as everyone can see transactions. It uses a cryptographic mechanism to access, sign, and encrypt transactions. Private keys can be connected directly to users or to things such as wallets. It is safe because of its decentralization and irreversible characteristics [14].

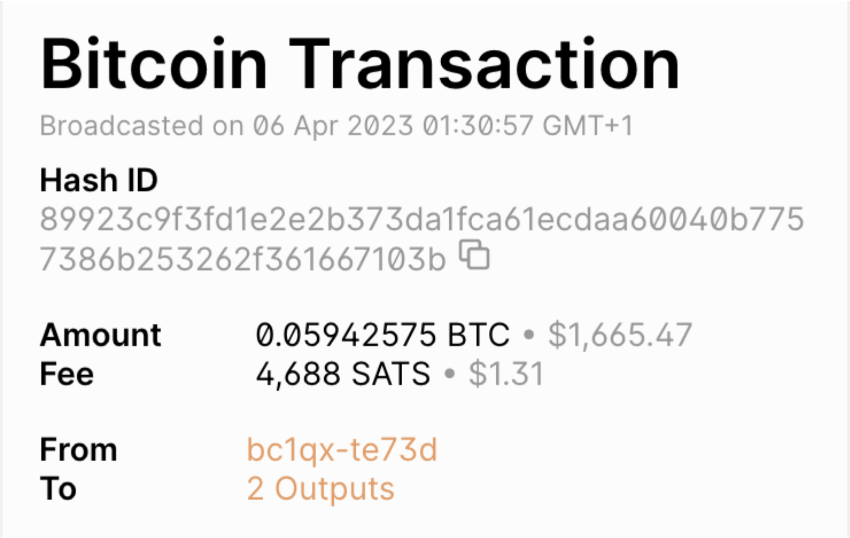
Blockchain has two main security features, availability and integrity. There are also methods for preventing double-spending and anonymization. However, some methods must be implemented that guarantee unlinkability and confidentiality [15].

3.2 Methods to preserve privacy

In blockchain transactions, four key elements can be located. There is the sender (who makes the transaction), the recipient (who receives the transaction), the amount sent, and the date and time at which the transaction is completed. The privacy of these elements is endangered.

Firstly, despite the lack of direct connections to personal data, it can be obtained by the user's connection through the transaction. On the other hand ,amounts, dates, and times are public data that anyone can consult. Participants' personal information can be obtained from their wallets, addresses or transactions. All this is because the transactions are open to the public [10].

In Figure 3 a real Bitcoin transaction is shown, this data is obtained from a public website because the transactions are open to everyone, in the transaction details there are the transaction hash ID, the amount of transactions, the fees paid and the issuer.



Bitcoin Transaction

Broadcasted on 06 Apr 2023 01:30:57 GMT+1

Hash ID
89923c9f3fd1e2e2b373da1fca61ecdaa60040b775
7386b253262f361667103b

Amount	0.05942575 BTC • $1,665.47
Fee	4,688 SATS • $1.31
From	bc1qx-te73d
To	2 Outputs

Figure 3: Example of a Bitcoin transaction [16].

The main privacy risks associated with the use of Blockchain technologies are listed below:

- **De-anonymization**: It is not enough to use pseudonyms in transactions. Therefore, a list of attacks that can jeopardize the anonymity of those involved in transactions has been drawn up. First of all, network analysis: blockchain uses a P2P network because nodes share their IPs during transactions, so attackers can discover the issuer's real name by connecting them. Address clustering is also a problem, as all addresses of the same user can be obtained. Finally, from transaction fingerprints, you can obtain input/output balance (IOB), time of day (TOD), time of hour (TOH), random time interval (RTI), and hour of day (HOD). The attributes mentioned could promote the loss of anonymity [17].

- **Transaction Pattern Exposure:** By using techniques such as transaction graph analysis,transaction characteristics are analyzed over a period of time to find patterns, as well as an anonymization method that can reveal the user's financial history. The AS-level deployment analysis is based on recursive connections to client networks of blockchain networks and obtains IP so that attackers can discover the structure of their network [17].

The following sub-chapters describe methods for protecting the privacy of the receiver and sender.

3.2.1 Mixing Services

A mixer is used to obscure the transactions. In other words, transactions' information is public and everyone can access the link between the sender and the receiver. The relationship mentioned is lost by the use of a mixer (also called laundry or tumbler) [12].

One example is the mixing coins, in this method the addresses and coins sent are mixed in the transaction (CoinShuffle) [13].

There are two types of mixing services: centralized and decentralized. Onionbc, Bitcoin fog, Bitmixer, Helix per gram and many other pages offer this centralized service, which is responsible for mixing transactions in exchange for fees. In this way,they eliminate the direct relationship between the sender and the receiver.

The use of this service also has its disadvantages, as attackers can steal the assets they send for transactions by not sending them to the recipients. Furthermore,these sites record transactions with logs, so that the user entrusts personal data to these sites, so that personal data may be threatened or exposed. Since these pages are centralized service, the servers are vulnerable to denial of service attacks [17].

In this instance, decentralized services are based on a large number of untrusted peers who mix messages, reducing the harm that denial of service attacks on decentralized services can cause. There are two methods of executing this process, CoinJoin, i.e., a protocol aimed at combining transactions performed by different users in order to maintain their anonymity, so that if someone observes the transactions performed,they cannot identify the issuer or the assets sent.

Another method is MPC, which is a cryptographic security concept that requires multiple parties to participate in accessing resources, i.e., one user cannot unlock the resources because it needs other participants. This concept is used in blockchain technology to design MPC wallets to store tokens and cryptocurrencies, and its security is based on the fact that private keys are divided among multiple devices [14].

3.2.2 Zero-Knowledge Proof and Confidential Transactions

This method is based on the cryptography of elliptic curves. Statements can be proved to be true without knowing the value or additional information. It is possible to confirm that a+b=c without knowing the values of a,b and c [10].

The use of this method in blockchain transactions makes them confidential, because their data are encrypted by encryption and only the proof that they are correctly calculated must be published. This method also offers the possibility to hide certain blocks and restrict access to them. The advantages of this method are that they enable privacy, transaction security, and scalability,providing a higher performance for blockchain. However, this method has limitations due to the mathematical equations it uses for operation and the fact that it is necessary to encrypt transactions and provide proof that the transactions are accurate for the verifier [13].

3.2.3 Ring signatures

Ring signatures are also known as anonymous signatures. Users are grouped into groups, and each user has his signature. In order to hide the signature of the transaction and thus ensure anonymity, the signatures that will be signed can be any signature of any group member. The origin of the signature is therefore unknown. The Security is based on the fact that it is computationally unlikely that the original signatory of the transaction will be found. [10, 15]

Because users must wait for the process to find participants, this technique aims to eliminate the delay that mixing services cause. In this case,users can sign with the ring signature, so it is not possible to know who signed and it remains completely anonymous [17].

3.3 Quantum safety in Blockchain

Quantum computers are more likely to break code because they have more power, quantum superposition states, and solve polynomial time problems [13].

3.3.1 Quantum safety

The adaptation of the methods mentioned in the previous section and their quantum safety are not as simple as making some small changes; in most cases, they require in-depth analysis and new technologies. Finding effective methods against quantum opponents is difficult [18].

In the Blockchain, a public and private key is used. If the private key is intended to be obtained from the public key, a conventional computer may take thousands of years of calculation, while a quantum computer may do so in seconds or minutes [18].

Monero's cryptocurrency uses the ring signature and the ring confidential transactions (RTC) allowing the sender to disclose only the information necessary to confirm its transaction without the need to disclose the money spent. Blind computation is the operation of transactions between users and servers without supplying any data of the user(e.g. input, output,algorithm used). However, this technique was neither valid nor safe before the emergence of quantum computers [19].

3.3.2 Quantum computers

It all began 1985 when an Israeli physicist at the University of Oxford, England, described the first quantum computer, i.e. a quantum computer that could simulate any other quantum computer. After this event, in 1994 Peter Shor proposed an algorithm for quantum computers that efficiently discovered the main factors of an integer. This represents a dangerous advance for cryptographic systems, especially those with the public key on which the blockchain is based, because it is based on the difficulty of finding total number factors that have been compromised since then. Later, researchers at Yale University created the first 2-Qubit computer (the basic measurement unit of quantum computation), and in 2016 IMB Research Succeeded in making a 5-Qubit Quantum computer available to the public in the cloud for anyone who wanted to try it [21].

The basic measurement unit of these computers is the qubit, or quantum bit. The speciality of this measurement unit is that a bit can represent a 1 or 0 at the same time, almost opposite to the conventional unit that can take the value of 1 or 0 [21].

It is worth pointing out the latest advances in quantum computers. It's the first 433-qubit processor developed by IBM, a well-known multinational technology company, and the new processor with the largest number of qubits to date. This processor is far superior to any classic computer. The company is also working to improve quantum software, such as by offering mitigation options through APIs offering error correction and mitigation options, so that users can modify speeds with lower errors, facilitate the use of quantum computers, and accelerate application development. In this sector, there is a very promising future with the goal of reaching quantum computers with more than 4000 qubits in 2025, which will go beyond the current capabilities of existing physical electronics [21].

3.3.3 Quantum resistant cryptography

To address the threats from quantum computers that threaten the security provided by the cryptographic digital signature systems of the blockchain, such as the case of the digital signature ECDSA of the bitcoin cryptocurrency, some blockchains that have already implemented signatures are listed below [20].

This is the Quantum Resistant Ledger (QRL), which is a Blockchain that uses an XMSS signature (the abbreviation means Extended Merkle Signature Scheme) and whose security is based only on the existence of safe hashing functions and not on the digital signatures that it was based on the existence of the difficulty factoring integers [20,22].

On the other hand, attacks-resistant signatures are called Blockchain Post-Quantum Signature (BPQS). It is a variant of the XMSS protocol that allows multiple transactions with the same signature. This is an advantage because a transaction may go wrong,so the possibility of resigning with the same node is useful. The difference between XMSS and BPQS is that XMSS is based on the existence of a single Merkle Tree, where as XMSS is based on a small Merkle Tree with two leaves. While XMSSi increases in width and height, BPQS only increases in height [20,23].

4. Monero

The personal data of the users is increasingly compromised, the amount of data collected by websites, applications and services offered online makes it necessary to apply measures and use systems that protect the privacy of its users. In the world of Blockchain, privacy is just as compromised as in any of the aforementioned cases. In this way Monero arises and it is a Blockchain focused on privacy [15].

Founded in 2014 as a fork (the deviation of the original code that used it as the basis for development) of another cryptocurrency, Bytecoin [16].

Most cryptocurrencies are not private, in the case of Bitcoin all transactions are public. To make such private transactions the user has to use transaction mixers and VPNs. Bitcoin is not anonymous, the information of the remittent and destinatary accounts and the amount sent are shown. Despite the use of pseudonyms, if more information is collected, the real address from which the transfer was made can be obtained, discovering the author of the transfer [24].

Unlike the popular Bitcoin Blockchain, where spent coins are identified and assigned to users, Monero makes use of mixins, obfuscating transactions and thus offering privacy and anonymity to users. Monero has become popular due to the fact that it offers greater privacy than Bitcoin [15].

In Monero in theory it is not possible to track and link transactions. With data obtained from transactions which are not obfuscated, companies can make behavior patterns. If, for example, an attacker took over the balance of a user's account, they could attack to obtain the income that is in their account. Additionally, because this cryptocurrency is decentralized and not under the control of a central authority, users are protected from authoritarian regimes [24].

Fungibility is a feature of Monero, if something illegal has been done in the past, users may not want to use those coins and they sell for lower prices than new coins. In Monero all transactions are private, unlike other platforms that allow you to choose to make a private transaction or not [24].

After analyzing the aim of granting privacy to this cryptocurrency, it could be assumed that this fact occurs so that illegal actions such as money laundering can occur, however the main objective is to respect the right to privacy of users [24].

However, Monero Blockchain cryptocurrency was even used on an online market, AlphaBay as a form of payment, but this page was closed due to its illegal use. In Monero transactions, 25 percent of accounts are illegal, because by providing greater privacy and allowing the user to be anonymous, it favors the appearance of users who seek to hide their identity in order to carry out illegal actions [15].

Despite the fact that this Blockchain has a major advantage, privacy, it also has vulnerabilities, one of which is the deduction mixin. The Monero software allows the users to configure the number of mixins used by default. This means that most mining inputs (64.04%) are called 0-mixin transactions, equivalent to traditional transactions with Bitcoins. Despite the advantage of using mixins if this system is not used correctly, the user will not be protected as much as in traditional Blockchain [15].

4.1 How Does Monero Work

Monero was launched in 2014 and its name means currency in Esperanto. It is a protocol that does not make public the sending or receiving account or the amount sent. To camouflage such data, Monero uses Ring Signature, the issuer's address is mixed with that of many other users, forming a group of addresses [25].

The only thing that is known is that someone from the group sent the information, however it is not known who. The sent amount is hidden due to the so-called ring confidential transaction, only a small part of the information is transmitted which is enough to verify the legitimacy of the sentamount [24]. The cryptographer Nick Szabo proposed the ring confidential transactions in 2001, and Monero implemented them in 2017. To carry out this type of transaction, the user must select the set of signatures (ring) that he wants to use. Then, using his signature and the selected signatures, he generates the so-called ring signature [25].

One of the vulnerabilities of Monero is Cryptojacking. Due to fungibility and the fact that mining is not as expensive as, for example, Bitcoin, this allows these attacks. This is because the mining of Monero is not so expensive, a web page can implement a script that would mining cryptocurrencies with the resources of the visitor to that page. This attack can be prevented and solved by checking the Blockchain in order to find these transactions towards the owner's account, but due to Monero fungibility, it is not possible to determine whether the cryptocurrencies were transferred to the owner of the page that facilitates this type of attack [16].

In order to hide the recipient's identity, a secret address is used. A sender creates a random, unique address; by using a hidden address, only the sender and the recipient can know where the payment was sent,and this address is used only once. This creates a separation between the address to which it is sent and the funds that are transmitted, thus hiding the balance of the sender. Only the recipient's key knows that the funds can be linked to the available address. The Monero protocol has its own currency called XMR. XMR is mined by computers that must decode cryptographic problems, called Proof of Work [24].

Monero uses a different algorithm than Bitcoin. Bitcoin works with the SHA256 algorithm and Monero works with the CryptoNight algorithm. CryptoNight is designed to be ASIC resistant which means that very powerful computers are not needed to mine XMR, almost any computer can mine XMR. Some of the disadvantages of Monero are: Inflationary policy, Bitcoin is limited to 21 million Bitcoins, there is no limit to the amount of XMR that can be mined. Another disadvantage is the mining speed, 1 block is mined every 2 minutes and the reward per block varies over time. Despite these disadvantages XMR is among the top 20 cryptocurrencies [24].

4.2 Monero Specifications

Bitcoin uses a pair of public and private keys to encrypt transactions. In Monero, two are used: a viewing pair of keys and a spending pair of keys ,which provides more anonymity and versatility. The system of two pairs of keys allows users to make their private viewing keys public to provide maximum transparency to their own movements. But thanks to the existence of a pair of spending keys, even if someone has a private view key, they cannot steal the resources available from the user account, as with this key only the view is possible and to get the resources, they would have to use the other pair of keys whose role is the use of funds [16].

In Bitcoin, a transaction consists of one or more inputs that refer to the outputs. Each transaction consists of an input and output set. The output consists of a number of bits and a recipient address. The input is an output from a previous transaction, so it is formed by the digital signature of the output's recipient. The Total output cannot be greater than the total input, and the output can only be used once [7].

Figure 4 shows the relationship between the input number of BTC and the output BTC number. It can be observed that the number of input BTC that enters is equal to the number of outputs that come out. The amount of BTC output can never exceed the amount of BTC input.

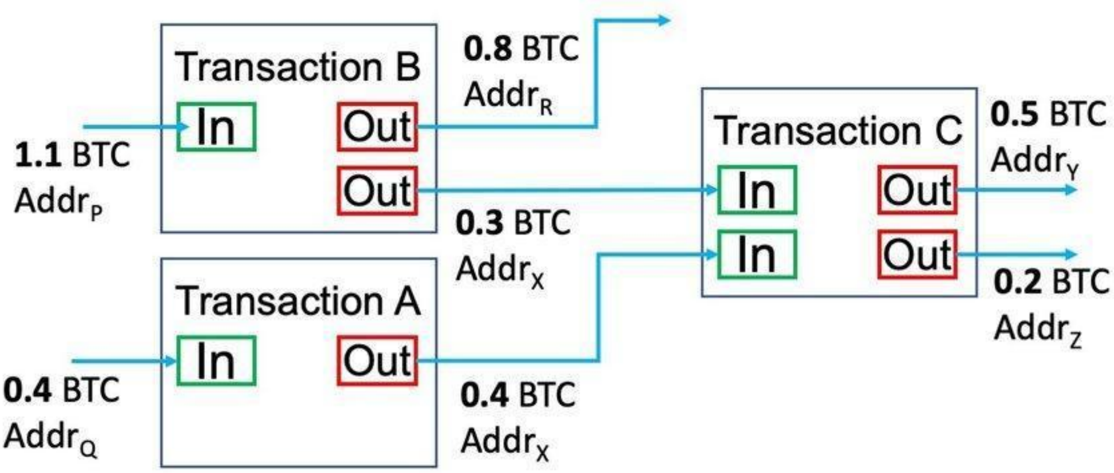


Figure 4: Input and output Bitcoin schema [26].

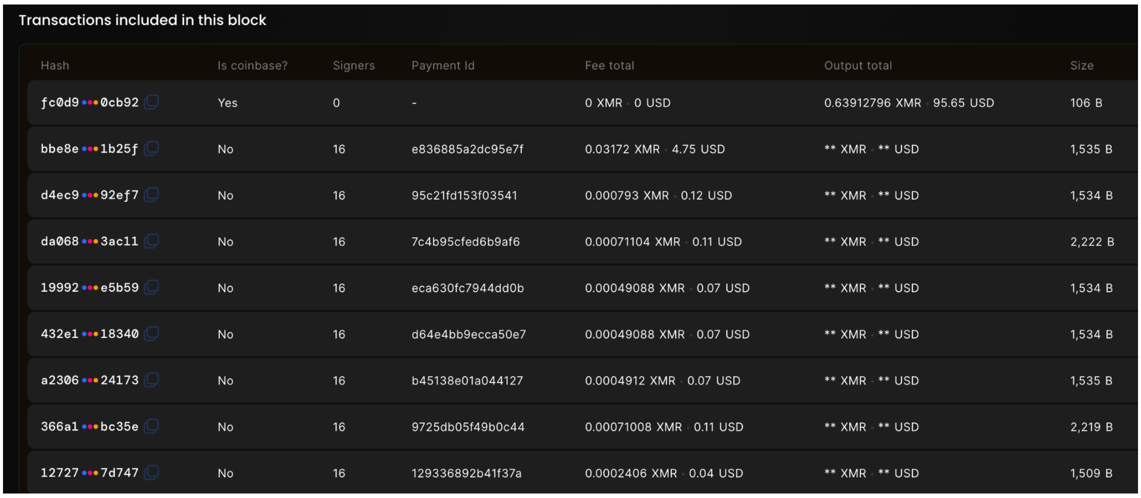
In Monero, transactions do not have this direct reference to inputs and outputs, the inputs are in the form of a ring in which the output is found, and the inputs of other components of the ring may not even be the same address as the user's wallet. In other words, it is other inputs of the user or other addresses that make up the ring. These inputs are called decoys.

To protect Monero from the aforementioned problem faced by the Blockchain called double spending, Monero uses a cryptographic key called KI, Key Image. This Key is generated from the output and the private key of the issuer. As a result, double spending attacks are impossible because outputs and keys always produce the same KI values. As a result, checking to see if the ring used the KI on Blockchain would be effective in thwarting this kind of attack [16].

Another feature of this protocol is that it allows the use of subaddresses. Sub addresses are addresses derived from the primary address and obtained cryptographically making it impossible to derive the primary address from the secondary. In this way, a user can maintain his anonymity using that secondary address so that the transactions carried out from them are not linked to him.

RingCT, Ring Confidential Transactions is a method whose objective is to hide the amounts of outputs. This method, introduced in January 2017,made its use mandatory for all Monero transactions, except for coinbase transactions. Coinbase transactions are reward transactions sent to miners who have solved the block. The coins transferred to these miners are coins that have never been issued via blockchain,they are completely new coins. These transactions are always the first transaction of a mining block [27].

As shown in Figure 5, the Coinbase transaction is the first block transaction, and it is the only transaction that shows the output total to all users. The other transaction's output is not shown in order to maintain the user's privacy. Another important characteristic of these transactions are the signers. As explained before, this type of transaction is signed by a group of users,so in Figure 5, the number of signers for each transaction is shown.



Transactions included in this block

Hash	Is coinbase?	Signers	Payment Id	Fee total	Output total	Size
fc0d9•••0cb92	Yes	0	-	0 XMR · 0 USD	0.63912796 XMR · 95.65 USD	106 B
bbe8e•••1b25f	No	16	e836885a2dc95e7f	0.03172 XMR · 4.75 USD	** XMR · ** USD	1,535 B
d4ec9•••92ef7	No	16	95c21fd153f03541	0.000793 XMR · 0.12 USD	** XMR · ** USD	1,534 B
da068•••3ac11	No	16	7c4b95cfed6b9af6	0.00071104 XMR · 0.11 USD	** XMR · ** USD	2,222 B
19992•••e5b59	No	16	eca630fc7944dd0b	0.00049088 XMR · 0.07 USD	** XMR · ** USD	1,534 B
432e1•••18340	No	16	d64e4bb9ecca50e7	0.00049088 XMR · 0.07 USD	** XMR · ** USD	1,534 B
a2306•••24173	No	16	b45138e01a044127	0.0004912 XMR · 0.07 USD	** XMR · ** USD	1,535 B
366a1•••bc35e	No	16	9725db05f49b0c44	0.00071008 XMR · 0.11 USD	** XMR · ** USD	2,219 B
12727•••7d747	No	16	129336892b41f37a	0.0002406 XMR · 0.04 USD	** XMR · ** USD	1,509 B

Figure 5: Monero transactions [28]

4.3 Monero and Quantum Computers

The risk of attacks by quantum computers is lower than the risk of Bitcoin Monero, but is still a medium risk. This is due to the signature scheme used in this EdDSA protocol. EdDSA is vulnerable because its security is based on discrete logarithm problems. Because Monero uses a protocol to provide privacy and anonymity, the amount of transactions is hidden, so the attacker will have to rely on luck to choose high-value transactions. Monero offers anonymity to users through Pedersen Commitments and Range Tests [17].

The Pedersen Commitments are cryptographic algorithms that allow users to enter certain values without revealing them, but users cannot change them at any time. In fact, this can be demonstrated to prove the validity of blockchain transactions. With these algorithms, you can find the total number of inputs without revealing each value, and verify that the transaction is valid without revealing unnecessary information. Range Proof is a zero-knowledge system that allows you to know whether a value is negative or positive without revealing the value [29].

Cryptonote is a protocol that creates cryptocurrencies and uses ring signatures and different keys to transfer them [14]. This is a very fast hashing algorithm that is part of the CryptoNote consensus protocol. Nicolas van Saberhagen, a developer whose identity is unknown, created this algorithm on December 12, 2012, and it has excellent scalability. It is an algorithm that uses native AES encryption and uses functions such as Keccak and Blake-256, which are safe hash functions. Using cache will optimize this algorithm and use the maximum CPU power in the process. This algorithm has many advantages; however, due to the adaptation of the ASIC devices to this algorithm, they have taken over the mining, and therefore it is necessary to find an alternative to this algorithm [32].

ASIC are devices aimed at offering the maximum performance used in the mining of cryptocurrency. Its acronym means application-specific integrated circuit. This type of equipment was used especially for Bitcoin mining,so that only possible to mine cryptocurrencies using this type of system. This is a major disadvantage because the purpose of Blockchains is to become a decentralized system. The existence of such equipment, which is the main objective of cryptocurrency mining, leads to the centralization of mining and makes it impossible for small users to mine [30].

Monero changed the PoW scheme from Cryptonight to RandomX,which is not vulnerable to quantum attacks [17].

RandomX is a Proof of Work type of algorithm whose aim is to replace the one previously used called CryptoNight, as it provides more privacy protecting the network from ASIC mining and only allowing CPU mining. It is a necessity to resist theAISC's progress. The development of this algorithm began on 31 October 2018 and the first version was published on 5th May 2019. It was developed by tevador, hyc, vielmetti, antanst, and SChernykh and began being used on the Monero network on 20 November 2019 [31].

Its most important features that it is based on randomness, which is why the name has been given to it, is designed that a completely random work area is created that consumes a lot of memory and uses very advanced virtualization technologies for virtualization, which is what makes it resistant to ASICs [30].

This algorithm not only withstands ASCI, but also withstand GPUs because these chips do not have the appropriate instructions to execute the very complex operations proposed in this algorithm. This Algorithm can only be used by the CPU and thus resists other types of mining. With regard to the cryptographic aspects of this algorithm, itunes Blake2b hash functions, AES symmetric cryptography and generates its passwords using Argon2d.

RandomX PoW consists of a series of steps. The first is the generation of a key that will be used as a Blockchain hash,called a "keyblock". To provide greater security, this key must be changed every 2048 blocks. Thekeys aregenerated using the data contained in the blockchain and a secure key generation system [31].

62 percent of transaction inputs are vulnerable to chain reactions, which means that the actual input can be deducted by deletion. In 62% attacks, real inputs can be obtained by checking transactions on the blockchain to see if they have already been spent, so the insufficient inputs in the past will be real. Monero

mixtures are screened so that it is possible to distinguish real coins according to their age. The actual input is usually the “newest”.

Mixing is a fake, non-real input that is grouped with the real input and hidden. The mix count is the total number of other signatures, except the sender's in the ring signature authorizing the transaction. The Bitcoin mixture is different from the one used in Monero. In Monero, new transactions are mixed with old transactions on the blockchain. However, in Bitcoin, the sender's coins are mixed with the coins of other users to create a transaction with many inputs and outputs [32].

Changes have already been made to Monero to address the attacks. Sampling distributions have been updated to match the actual description more closely. Regarding the problem of including inputs that have already been publicly deanonymized as mixins, if an output A has been extracted from a transaction and that output appears in a future transaction, it is obviously a decoy. The solution will be to exclude the outputs from the pools that have already been mined, but it is quite difficult due to the number of pools [32]

There are quantum-resistant signature schemes, but nowadays they need large keys and generate signatures of an equivalent size [32].

The existence of a potential attacker with a quantum computer exposes Monero's security, but this is not exclusive to Monero but to all cryptocurrencies. Although there are no free quantum computers, thanks to IBM's quantum experience, you can now test code for quantum computers using open-source quantum hardware. However, IBM is not the only company that allows this type of experience [33].

4.3.1 Monero vs Bitcoin

The Random X-Work Proof used by Monero is much more secure than that used by Bitcoin (more secure for quantum opponents). How the keys are generated in Monero is unsafe. Today, public keys are published, but this is an unsafe practice and puts the user's private key at risk [33].

In Monero, the address is composed of a public key, so the user doesn't even have to share a public key, and it's enough to publish a wallet address so that the quantum assistant can obtain his public key from the address and his private key. The solution could be the use of one-time addresses, or at least those that users publish and know. This is because, even if these wallets are empty because they have only been used for a specific transaction, you can obtain all the transaction history [33].

In Monero ring signatures, key images can be broken, and then members of the ring used to construct ring signatures can be easily identified. The mitigation would be to move to a post-quantum ring signature system, which would also address the key problem. But the actual post-quantum schemes are now not efficient due to the large keys that are needed, and it takes so long to verify that even the most practical ones will make it difficult to convince members of the Monero community that they are sufficiently effective for use and practice. The following table compares the length of the keys required by quantum algorithms and classical algorithms. It can be seen that there is a significant difference in length, indicating that these post-quantum schemes are not yet ready for use.

Algorithm	Private key (bytes)	Public key (bytes)	Type
Kyber-512 **Kyber-768** **Kyber-1024**	1632 2400 3168	800 1184 1568	Quantum
Lightsaber **Saber** **FireSaber**	1568 2304 3040	672 992 1312	Quantum
RSA-3072 **RSA-7680**	384 960	384 960	Classical

RSA-15360	1920	1920	
Curve25519	251	256	Classical

Table of key lengths for various algorithms [42].

The Petersen commitments utilized by Monero provide flawless anonymity. Monero amounts are safe. However, if you possess a quantum computer, you can generate income. This could be detrimental to the money supply because it would be impossible to detect if it occurred.

To mitigate this issue, you must decide whether it is more important to conceal the quantity or whether it cannot be manipulated. If one of the options must be chosen, what must be done is to ensure the supply of money by changing commitments. In Monero, a non-quantum secure algorithm is used to generate transaction hashes, ids, and block hashes; post-quantum hash should be used. The change would not be so sudden since post-quantum hashes can be added to the current hashes so that security is not compromised [33].

4.3.2 Elliptic Curve Cryptography

To explain why Monero is not quantum-resistant, we must first introduce the cryptography on which it is based, Elliptic Curve Cryptography, as well as the associated terminology.

4.3.2.1 Public Key Cryptography

Public Key Cryptography was proposed in 1976 by Diffie and Hellman. The scheme is based on each user having a pair of keys, a public key that is public to everyone and a private key that the user must keep in a safe place. This type of encryption is based on trapdoor functions. This concept refers to the fact that the function in output B in input A can easily be transformed, but it is almost impossible to get output B from input A [34].

4.3.2.2 Asymmetric cryptography

Asymmetric cryptography refers to two keys: a private key used to decrypt data and sign it; a public key used to encrypt data and validate signatures. Asymmetric cryptography and symmetric cryptography are distinct from one another because symmetric cryptography relies on the existence of a single shared key between users who are involved in the communication [34].

Previously, the security of asymmetric cryptography was based on the factorization problem of large integers. As a computationally large number, it was impossible to obtain the first numbers from which these numbers derive. However, today, asymmetric cryptography is based on elliptic curves, giving rise to the elliptic curve cryptography used in Monero. In Monero, in particular, the Edwards25519 curve is used [34].

4.3.2.3 Monero private and public keys

A pseudorandom generator (PRNG) on the Keccak hashing function generates Monero root private keys, and the outcome of the previous hashing round essentially determines the outcome of the following one [34].

<u>The Keccak algorithm</u>

A sponge construction is a type of finite internal state algorithm that accepts a variable-length bit string as input and returns a variable-length bit string as output. The function is made up of the following components [37, 41]:

1) A function that acts on a fixed number of bits (f).
2) A padding rule (pad).
3) A rate (r).

A sponge function also accepts a string of bits (N) as a parameter, and its length (d) must be specified because its size is variable. It is known as a sponge construction because the bits of the variable-length string are "absorbed" by the defined function, and then the output string of bits is "squeezed" out of its state, as shown in the following formula [41]:

$$z = \text{SPONGE}\ [f,pad,r](N,d)$$

The function operates on strings of a fixed number of bits, denoted by b. The rate must be an integer greater than zero and less than b. Alternatively, the capacity c is a positive number obtained by subtracting b from r. The padding rule is a function that provides padding and is necessary since the function used accepts fixed-length bit strings, but the sponge function applies to variable-length bit strings [41].

Having described the components of the function, the steps of the sponge construction are described below [41]:

1) The pad function on N is used to create a block of size P:

$$P = pad(r, len(N))$$

2) The value of n, which is an integer, is obtained; therefore, the length of P must be divisible by r:

$$n = len(P) \,/\, r$$

3) The capacity value is calculated:

$$c = b - r$$

4) Divide P into length r blocks:

$$P = P_0 || \dots || P_{n-1}$$

5) The state S is initialized to a string of b zero bits:

$$S = 0^{b}$$

6) The following steps are applied to each block of P from 0 to n-1, each of those blocks being P_i:
    - P_i is extended by a string of length 0 bits c.
    - The previous result is XORed with S.
    - The function is applied giving rise to a new value of S:

$$S = f(S \oplus (P_i \,||\, O^{c}))$$

7) Z is initialized to an empty string.
8) As long as the length of Z is less than d,
    - 1st r bits are appended from S to Z.
    - If z < d f is applied to S.
9) The last step is to truncate Z to the length of d bits.

Public keys

As for public keys, they are derived from private keys using the Edwards25519 curve with some Monero-specific modifications. The purpose of the public key is to be shared, unlike the private key. Although it is relatively easy to get the public key from the private key, it is not the same in the other direction. The public key is a point (x,y) on an elliptic curve [34].

4.3.2.3 Elliptic Curve Cryptography

Elliptic Curve Cryptography is a form of cryptography based on elliptic curves over finite fields. Victor Miller and Neal Koblitz proposed this type of cryptography in 1985. It is a type of cryptography based on the elliptic curve definite logarithm problem, defined by the equation $y^{2} + xy = x^{3} + ax + b \bmod p$ [35].

Mathematical concepts

The first concepts to define are finite fields. Sets form algebraic structures called fields, which have two basic operations—multiplication and addition—and satisfy association, distribution, and conversion properties. The p set of integer modules refers to all integers from 0 to p-1 using the previous operations of addition and multiplication. The finite points (x,y) of the elliptic curve belong to a set, and any operation between these two points will lead to another point in the curve. As can be seen in the diagram, the elliptic curve is symmetrical on the x-axis (a mirror image), there is no peak, and it never crosses itself. Figure 6 illustrates an elliptic curve as an example [35].

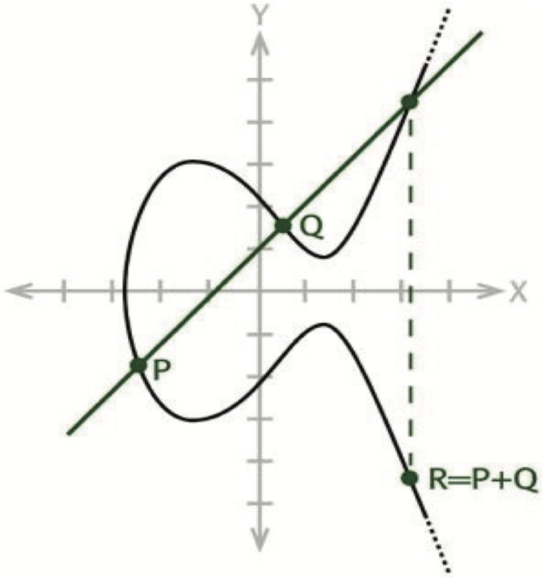


Figure 6: Elliptic Curve

4.3.2.4 The use of elliptic curves in cryptography

Because of rounding errors caused by the use of real numbers, elliptic curves are used in the finite field equation $y^2 = x^3 + ax + b$. It is based on the existence of a finite number of points, and the coordinates are integers. To get another point in the curve, add one point (x,y) to the curve several times. The second point is represented as follows: Q = P +... + P = nP. Because it is difficult to obtain n after a point is generated, smaller keys are safer than other cryptographic systems such as RSA. In this cryptography, there are two types of finite fields: prime fields (F_p) with a prime number of elements, and binary fields (F_{2^m}) with a prime number of elements. In RSA, security is based on the difficulty of solving the problem of determining a large integer. In ECC, security is based on the discrete logarithm problem (ECDLP) of elliptic curves. This problem is based on obtaining n, and the values Q and P are known based on the points Q obtained Q = n x P [35,36].

4.3.2.5 Edwards25519 Elliptic Curve

The curve equation is as follows:

$$- x^2 + y^2 = 1 - \left(\frac{121665}{121666}\right) \times x^2 \times y^2$$

The basic point G is specific to each curve; in this case, the point G is G = (x,⅘), and for each point in the EC, P = nG. The finite field of this curve is $F_{2^{255}-19}$ obtained from the following function [35,36]:

$$- x^2 + y^2 = 1 - \frac{121665}{121666} x^2 y^2$$

A 256-bit integer that requires 32 bytes to represent it is the element of this finite field [35].

As mentioned above, the curve values are finite, so a modulo value must be set as a value limit. The value must be a prime value, and in this curve, l = 2^{252} + 27742317777372353535851937790883648493 [35].

For the total coordinates of the curve, this set value is also the first number, q = $2^{255} - 19$. The equation used for this curve is $ax^2 + y^2 = 1 + dx^2y^2$, and a, d, and x are finite fields (forming a set of 0 to p-1) [35].

4.3.2.6 Elliptic curves for key generation

As explained in the previous paragraph, the Keccak algorithm obtains a private key (k) that meets 1 < k < N. From this private key, the public key K = kG is obtained [35].

For example, in a key exchange such as Diffie-Hellman, two users (A and B) want to communicate and generate a private key k_A, k_B, from which they get a public key $K_A\ and\ K_B$. In this way, they use private keys to encrypt the message and share the public ones so that other users can decrypt it [35,36].

4.3.2.7 EdDSA Signature Algorithm

The pseudorandom number for private keys is not generated in Monero every time, but uses a hash value derived from the signer's private signature and the sent message. The signature is generated by following the following steps:

1) The hash function h applies to the signature's private signature (hk) hash function, and the signature's message (m) is m.
2) In the next step, R = rG y s = (r + H(R, K, m) x k)) is calculated.
3) As a result of this process, the signature pairs are (R, s).

Due to the uncertainty compared to quantum computers for elliptic curves, another type of encryption is proposed, namely, lattice-based encryption [33,36].

4.3.3 Lattice-based cryptography

To first comprehend this type of encryption, the following concepts must be defined:

- **Lattice**: A lattice is a set of points that lie in a space of dimension n and that has a periodic structure. Those points are generated from n-linearly independent vectors [40]:

$$b_1,\dots b_n \in \mathbb{R}^n$$

- These vectors are known as a **basis of the lattice**. The lattice generated from these vectors is a set of vectors represented by the following definition [40]:

$$\iota(b_1 \dots b_n) \;=\; \{\, \sum_{i=1}^{n} x_i b_i : x_i \in Z \,\}$$

- **Vector**: It is a straight line segment built from points that are oriented in a two-dimensional or three-dimensional plane.

The points represented in the grid follow a pattern known only to the participants in the communication; they are the basis vectors. The lattice is built using these points, and through operations done with them, the rest of the lattice coordinates are built. In Figure 7, a lattice is shown, which, as can be observed, has a lot of points defined on a finite space [38].

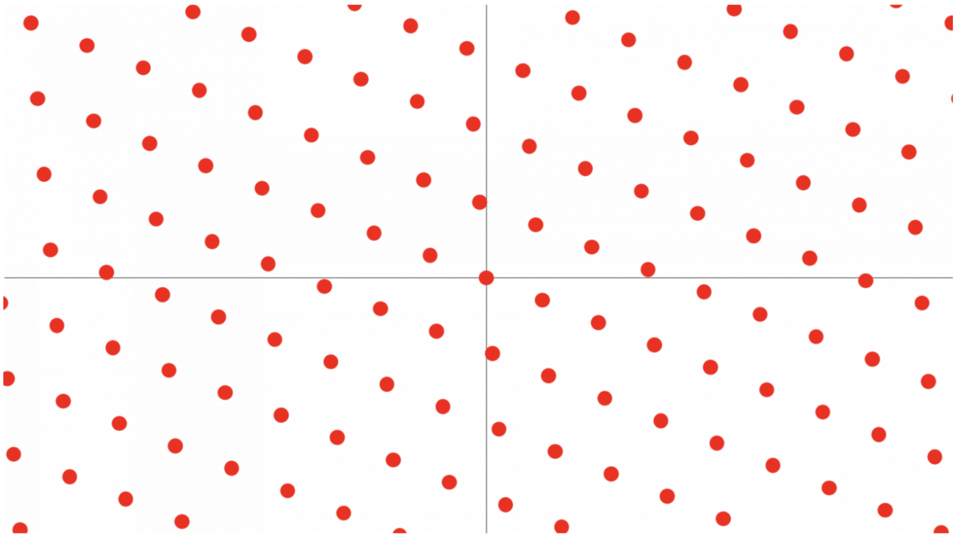


Figure 7: Lattice Example

For example, when a calculation is made with these points, if the base vectors are (7, 3) and (2, 1), the other points of the grid will be obtained. Different base vectors can generate the same lattice. If the base vectors (76, 38) and (29, 13) generate the lattice points, these points can be added to give us points (105, 51), deduced and obtained (-47, -25), or multiplied. The problem based on this type of encryption is known as the shortest vector problem, which consists of finding the shortest non-zero vector given the basis of this lattice. Figure 8 shows how to create a lattice using points produced by operations using basis vectors [38].

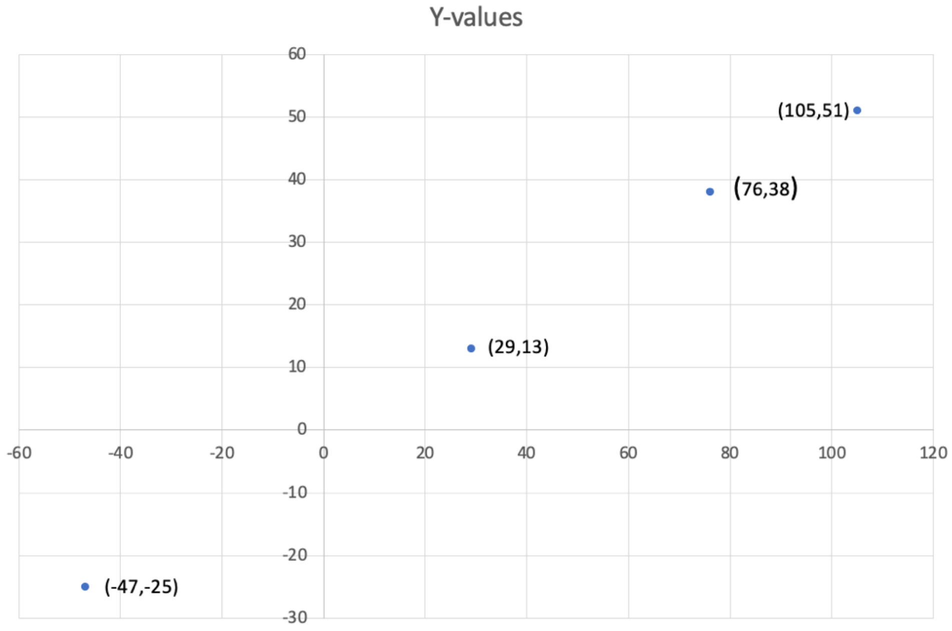


Figure 8: Example of a lattice with base vectors.

The above example is based on two basic vectors in two dimensions. However, in the actual case, the grid can be composed of multiple vectors and multiple dimensions. If a point on the grid is used to encrypt a message, this leads to a point close to the grid but not to the grid. The recipient of the message can decrypt the message because it has the value of the base vector that generated this grid. However, the attacker only has the nearest point on the network and must find the closest point between the encrypted message and the public key of the message sender [39].

To explain this concept, it is important to note that there are two types of foundations: good basis and bad basis. An example of a bad basis is the vector that is formed by the following points (6,14) and (3,8). This is because if you want to get the closest point to this base using the point (11.6, 4.2), you will solve the following formula with Gaussian elimination [39]:

$$a(6,\ 14) +\ b(3, 8) \approx (11.6,\ 4.2)$$

$$a\ =\ 13.4 \quad\ b\ = -\ 22.9$$

$$13(6, 14) -\ 23(3,\ 8) =\ (9, -\ 2)$$

Figure 9 shows the points that the previous equations calculated. This result and the point closest to it will differ significantly from those generated with a good basis, which will be depicted on the following pages.

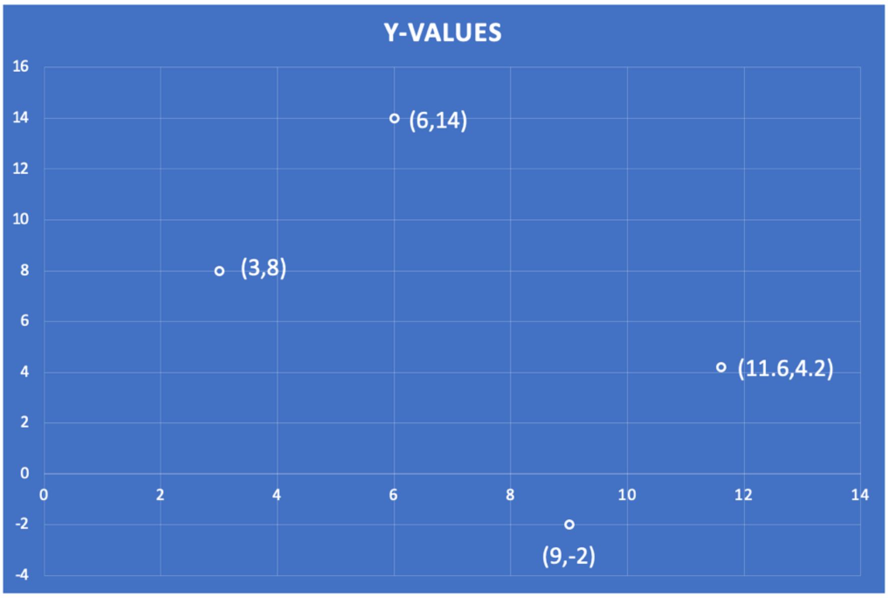


Figure 9: Lattice created using a bad basis

Since the lattice numbers must be integers, these numbers must be rounded, which can lead to multiple possibilities and false results, generating points that are not close to the base vectors. For example, if the good base is (3,0) and (0,2), it is like the following [39]:

$$a(3, 0) +\ \ b(0, 2) \approx (11.6,\ 4.2)$$

$$a\ =\ \ 3.86 \quad\ b\ =\ 2.1$$

$$4(3, 0) +\ 2(0, 2) =\ (12, 4)$$

It is difficult to obtain the closest vector problem if the bad base is used. And as it is shown in Figure 10, the obtained nearest point to basis is very different from the obtained using a bad basis [39].

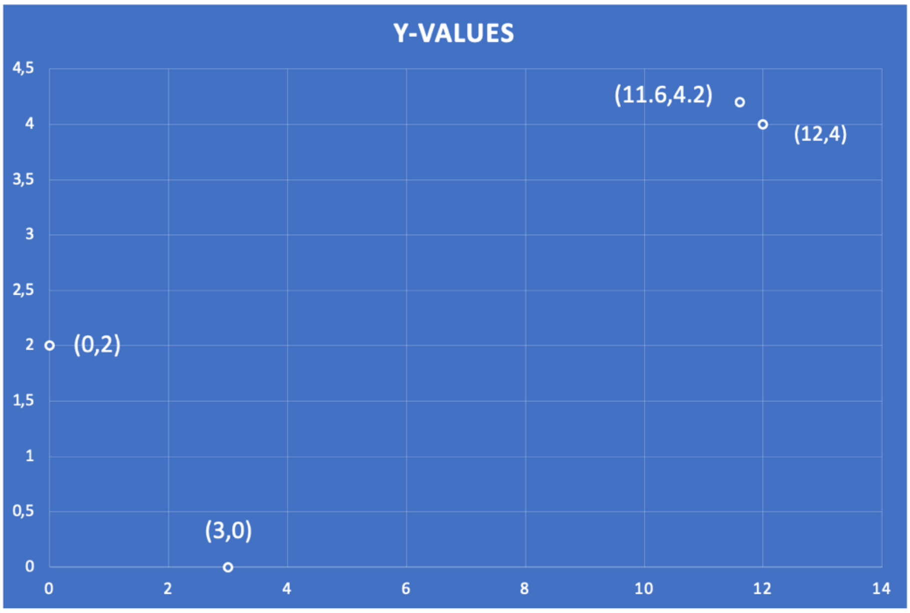


Figure 10: Lattice created using a good basis.

4.3.3.1 Use of lattice in cryptography

If a bad base is used as a public key as shown in the previous chapter and a good base as a private key previously as a message (if the message is represented as a point) as (14, -24), the procedure will be as follows [39]:

1) A calculation using the public key is done:

$$14(6, 14) - 24(3, 8) = (12, 4)$$

2) A random vector called an error vector is chosen to generate a point close to the grid but not inside it. For example:

$$e \ = (-\ 0.4,\ 0.2)$$

3) When adding an error vector to a point generated by a encrypted message, the next point remains:

$$(12, 4) + e \ = \ (11.6, 4.2)$$

For the decryption process, Gaussian elimination is used to obtain the a and b values. Multiply these values by the private keys as follows:

$$4(3, 0) + \ 2(0, 2) = (12, 4)$$

The next step is to get the closest point to the base vector, from the following formulas $a(6, 14) + \ b(3, 8) = (12, 4)$

The result is a = 14 and b = 24 as encrypted messages.

This type of cryptography has advantages, but even if the keys used are shorter than those used in other types of cryptography, the keys used in this type of cryptography are larger than those of the RSA protocol. This means a difficult proving time, so in practice it would be slower, but it would be quantum safe [38].

Lattice-based cryptography is secure against post-quantum computer attack and classical computer attacks. The question might arise as to why this type of cryptography is not used today, rather than just considering its use to prevent quantum computer attacks.

It is a rather inefficient cryptosystem. If the security of the algorithm were based on lattices of dimension n, the size of the public key would be O(n4) which would transform each encrypted bit into O(n2) bits. There are works that propose changes to reduce the size of the keys such as [43] and [44] in which keys of size O(n2)are presented, the length of the encryptions being only O(n). However, despite having the advantage of decreasing the length of the keys, the security offered by this type of cryptography decreases since they do not base their security on the shortest vector problem (SVP) but on the problem by Dirichlet and worst-case quantum hardness of the SVP. The first one is not directly related to any standard lattice problem while the second one is based on the existence of a quantum algorithm that is somewhat uncertain because to this day the existence of a quantum algorithm that surpasses classical algorithms is unknown for lattice based cryptography [40].

Conclusions and future work

The privacy implications of Blockchain and cryptocurrencies have been analyzed. Although there are methods for maintaining privacy in cryptocurrency transactions, such as mixin services, zero-knowledge proof, and ring signatures, the advent of quantum computers has rendered these ineffective.

Lattice-based cryptography, which is resistant to attacks carried out by quantum computers, could be implemented as an alternative to Elliptic Curve Cryptography in the case of Monero. However, this type of cryptography still has drawbacks that must be addressed, such as slow verification, which must be improved in the future before the solution can be implemented.

In addition to the proposed solution for Monero, there are additional solutions that should be studied, such as replacing bulletproof range proofs with quantum resistant range proofs. However, this field is still to be studied and is constantly being studied, so you must stay up-to-date. Day by day, incremental progress is made in this field. Change from Pedersen commitments to switch commitments would be another change to examine; however, due to a lack of documentation in this regard, it is still challenging to propose a solution based on this type of commitment.

Despite the fact that commercial quantum computers are not yet a reality, and are still unknown, it is important to begin implementing solutions because privacy will be compromised the moment these types of computers become accessible to everyone.

5. Bibliography

[1] J. Bernal Bernabe, J. Luis Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, A. Skarmeta, “Privacy-Preserving Solutions for Blockchain: Review and Challenges”, 31th of October 2019 [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8888155 [Accessed: 1-Mar-2023].

[2] T. M. Fernández-Caramés, P. Fraga-Lamas, “Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks”, 23th of January 2020 [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8967098 [Accessed: 2-Mar-2023].

[3] “Goal 9: Build resilient infrastructure, promote sustainable industrialization, and foster innovation”, 2023 [Online]. Available: https://www.un.org/sustainabledevelopment/infrastructure-industrialization/ [Accessed: 3-Mar-2023].

[4] “Goal 16: Promote just, peaceful and inclusive societies ”, 2023 [Online]. Available: https://www.un.org/sustainabledevelopment/peace-justice/ [Accessed: 4-Mar-2023].

[5] Q. Feng, D. He, S. Zeadally, M. Khurram Khan, N. Kumar, “A survey on privacy protection in blockchain system”, *Journal of Network and Computer Applications*, 2018.

[6] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, S. Shimizu, “Privacy preservation in permissionless blockchain: A survey”, *Digital Communications and Networks*,Volume 7, Issue 3, 2021.

[7] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin, “An Empirical Analysis of Traceability in the Monero Blockchain”, *Proceedings on Privacy Enhancing Technologies,* 2018.

[8] C. Zozaya, J. Incera y A. Lidia Franzoni, “Blockchain: Un Tutorial”, *Money as a Social Phenomenon of Trust,* Memorias de la Reunión Anual University of Dallas, Ciudad de México, September 29-30, 2017.

[9] “Proof of Work: ¿Qué es y cómo funciona? | Explicación fácil en español”, Youtube, 21th October 2021 [Online]. Available: https://www.youtube.com/watch?v=v8Xyu699bOA [Accessed: 1-May-2023].

[10] J. Segura, “¿Qué es Prueba de participación / Proof of Stake (PoS)?”, 6th July 2018 [Online]. Available: https://academy.bit2me.com/que-es-proof-of-stake-pos/

[Accessed: 1-May-2023].

[11] “Conceptos básicos de *blockchain* y Bitcoin”, apuntes de M1.875 - aula 1, Universitat Oberta de Catalunya, 2022.

[12] M. Aydar, “Simplified scheme of a blockchain transaction”, July 2019 [Online]. Available: https://www.researchgate.net/figure/Simplified-scheme-of-a-blockchain-transaction_fig2_334361184 [Accessed: 15-March-2023].

[13] K. Ikeda, “Security and Privacy of Blockchain and Quantum Computation”, 2018.

[14] J. Alonso Lecuit, “La seguridad y privacidad del blockchain, más allá de la tecnología y las criptomonedas”, 12 de noviembre de 2019.

[15] R. Zhang, R. Xue and L. Liu, “Security and Privacy on Blockchain”, *ACM Comput. Surv.,* 52, 3, Article 51, July 2019.

[16] “Bitcoin Transaction”, 2023 [Online]. Available: https://www.blockchain.com/en/explorer/transactions/btc/89923c9f3fd1e2e2b373da1fca61ecdaa60040b7757386b253262f361667103b [Accessed: 15-March-2023].

[17] Q. Feng, D. He, S. Zeadally, M. Khurram Khan and N. Kumar, “A survey on privacy protection in blockchain system”, *Journal of Network and Computer Applications,* 2018.

[18] R. Chatterjee, K. Chung, X. Liang and G. Malavolta, “A Note on the Post-Quantum Security of (Ring) Signatures”, *the 25th International Conference on Practice and Theory of Public-Key Cryptography,* 2022.

[19] G. Maynés i Moreno, “Blockchain: pasado, presente y futuro”, mayo 2018.

[20] T. Van Trinh, “Quantum-safe Bitcoin”, 2020.

[21] “IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two”, 9th November 2022 [Online]. Available: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two [Accessed: 5th-May-2023].

[22] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I.Nitto and T. Schroeter, “Blockchained Post-Quantum Signatures”.

[23] A. Dames, “What Is Quantum-Safe Cryptography, and Why Do We Need It?”, 10th March 2022 [Online]. Available: https://www.ibm.com/cloud/blog/what-is-quantum-safe-cryptography-and-why-do-we-need-it [Accessed: 15-March-2023].

[24] “Criptomoneda MONERO (XMR) : TODO lo que necesitas saber | Explicación sencilla en Español”, Youtube, 5th March 2021 [Online]. Available: https://www.youtube.com/watch?v=9pAi3aFb7Zo [Accessed:

15-March-2023].

[25] "What is Ring Confidential Transactions (CT)?", 2023 [Online]. Available: https://crypto.news/glossary/ring-confidential-transactions-ct [Accessed: 15-March-2023].

[26] M. Javad Amiri, "Transactions input and output in blockchain", March 2021 [Online]. Available: https://www.researchgate.net/figure/Transactions-input-and-output-in-blockchain_fig6_333337548 [Accessed: 15-March-2023].

[27] G. Ayala, "¿Qué es una transacción coinbase?", 24th May 2019 [Online]. Available: https://academy.bit2me.com/que-es-coinbase-transaccion/ / [Accessed: 1-May-2023].

[28] Blockchair, "Monero block", 2023 [Online]. Available: https://blockchair.com/monero/block/2881538 [Accessed: 1-May-2023].

[29] "Moneropedia", 2023 [Online]. Available: https://web.getmonero.org/resources/moneropedia/pedersen-commitment.html [Accessed: 1-May-2023].

[30] G. Ayala, "¿Qué son mineros ASIC?", 1st August 2018 [Online]. Available: https://academy.bit2me.com/que-son-mineros-asic/ [Accessed: 1-May-2023].

[31] G. Ayala, "¿Qué es algoritmo de minería RandomX en Monero?", 17th August 2020 [Online]. Available: https://academy.bit2me.com/que-algoritmo-mineria-randomx-monero/ [Accessed: 1-May-2023].

[32] C. Benziane, "Monero Transaction Traceability", 22nd March 2018 [Online]. Available: https://bitcointechweekly.com/front/monero-transaction-traceability/ [Accessed: 15-May-2023].

[33] A. Corbo, M. Krawiec-Thayer, B. G. Goodell and Monero Research Lab, "Evaluating cryptocurrency security and privacy in a post-quantum world", September 2020 [Online]. Available: https://github.com/insight-decentralized-consensus-lab/post-quantum-monero/blob/master/writeups/technical_note.pdf [Accessed: 16-May-2023].

[34] "Monero Documentation", 2023 [Online]. Available: https://monerodocs.org/ [Accessed: 17-May-2023].

[35] V. Kapoor and V. Sonny Abraham, "Elliptic Curve Cryptography", 20th May 2008, *ACM Ubiquity,* Volume 9, Issue 20 [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/1386853.1378356. [Accessed: 17-May-2023].

[36] K. M. Alonso, "Monero privacy in the Blockchain", 2023 [Online]. Available: https://openaccess.uoc.edu/bitstream/10609/75205/6/alonsokTFM0118memoria.pdf / [Accessed: 18-May-2023].

[37] “Keccak”, 2023 [Online]. Available: https://keccak.team/keccak.html [Accessed: 18-May-2023].

[38] D. Micciancio and O. Regev, “Lattice-based Cryptography”.

[39] N. Körtge, “The Idea behind Lattice-Based Cryprography”, 26th May 2021 [Online]. Available: https://medium.com/nerd-for-tech/the-idea-behind-lattice-based-cryptography-5e623fa2532b / [Accessed: 18-May-2023].

[40] O. Regev, “Lattice-Based Cryptography”, *Tel Aviv University, Israel.*

[41] “SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions”, August 2015 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf [Accessed: 20-May-2023].

[42] J. Hekkala, K. Halumen and V. Vallivaara, “Implementing Post-quantum Cryptography for Developers”, January 2022.

[43] M. Ajtai, “Representing hard lattices with O(n log n) bits”, *Proc. 37th Annual ACM Symp. on Theory of Computing (STOC)*, 2005.

[44] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography”, *Proc. 37th ACM Symp. on Theory of Computing (STOC*), 84–93, 2005.