Security in the Seizure and Storage of Cryptocurrencies

João Maurício Barros Ascensão, *Student, Instituto Superior Técnico (IST)*

***Abstract*—With the increase in the popularity of cryptocurrencies and the consequent increase in the number of crimes and cyber-attacks, it became important to use mechanisms that protect and keep cryptocurrencies safely stored in wallets.**

After a criminal investigation involving cryptocurrencies, the Judiciary Police seizes these cryptocurrencies and stores them in wallets. In this work, a threat analysis method was applied to five possible types of wallets that the PJ can implement: Paper Wallet, Mobile Wallet, Web Wallet, Desktop Wallet, and Hardware Wallet. This analysis method aims to identify the one that is subject to the least number of threats and consequently to the least number of internal and external attacks. After the analysis, the type of wallet that showed the best reliability in terms of security was the Hardware Wallet, because, in addition to being subject to fewer threats and attacks, it has good characteristics for storing large amounts of cryptocurrencies for long periods of time.

The fact that the private key is under the control of a person can lead to the total loss of the value of cryptocurrencies, in case of destruction of the key, death of the person, or no backups of the data.

Hence, the idea to create a hierarchical model based on Secret Sharing concepts: divide the key that gives access to cryptocurrencies by several shares and by many participants (Secret Sharing concept) so as not to leave this key under the control of one person only. This means that it becomes more difficult for someone with illegal activities in mind to access cryptocurrencies. Thus contributing to a significant improvement in the security levels of the cryptocurrencies seized by the PJ.

***Key Words*—Threat Analysis, Attack Trees, Cryptocurrencies, Secret Sharing, Wallets**

I. Introduction

Cryptocurrencies over the years have increased in popularity around the world. In 2008, Satoshi Nakamoto [1] created Bitcoin, the most famous cryptocurrency. It is a payment system that works based on open-source software algorithms that use a global peer-to-peer network to create new currencies, register and validate transactions. Private keys are essential for carrying out transactions, as they are the ones that allow identifying the owner of the bitcoins. They are mainly used to sign cryptocurrency transactions and consequently spend them taking into account the corresponding public key. Since these private keys are the most important asset to be protected by people who have these cryptocurrencies, it is necessary to use mechanisms that store them safely, these mechanisms are called wallets - used to transfer cryptocurrencies and to store secure private keys [2].

Bitcoin has brought many advantages to people or organizations that make any type of payment online, for example, users have total control of their money, there is no type of payment of additional fees in transactions, there is no financial entity responsible for transactions and storage of money (decentralized system), transactions are irreversible and it is not necessary to use the user's personal data, thus guaranteeing total anonymity. [1] [2].

On the other hand, the characteristics presented above caught the attention of criminals. The fact that Bitcoin is a decentralized payment system, that is, without any regulatory body and that it is possible to carry out transactions in anonymity, has made authorities of authority worldwide, namely those in Portugal, concerned about illegal transfers of products and services and other types of online crime such as money laundering [3].

A. Problem

In the event of illegal cyber activities involving cryptocurrencies, the Judiciary Police (PJ – Portuguese acronym) is the entity responsible for the investigation and respective seizure of all technological equipment, especially the wallets, which are where the cryptocurrencies involved in the criminal activity are kept. After the investigation is completed, it is necessary to safely store the amount of cryptocurrencies apprehended. Moreover, to store these amounts of cryptocurrencies, PJ has some solutions, several types of wallets (Paper Wallet, Mobile Wallet, Web Wallet, Desktop Wallet, Hardware Wallets and among others). Each type of wallet has its own characteristics, but the focus of this work will be on the security component, that is, the objective is to choose a type of wallet that meets more security requirements for the PJ to be able to store the seized cryptocurrencies. with the minimum risk of losing or being stolen and preferably not having too high costs. Later on, the most secure wallet type for the PJ will be presented with a proposal to improve security in the storage of cryptocurrencies in the wallet.

B. Methodology

The types of wallets under analysis are Paper Wallet, Mobile Wallet, Web Wallet, Desktop Wallet, and Hardware Wallet.

To choose the best and safest type of wallet to be implemented by the PJ, a threat analysis process will be used, that is, a method will be chosen to determine the types and quantities of threats to be addressed that each type of wallet is subject. For this, a threat identification methodology, known as STRIDE [5], will be used, where an analysis will be made between the threats of this methodology and the threats identified in each type of wallet.

Once these threats are identified for each wallet, attack trees will be used as a method to identify what type and how many attacks each wallet is subject to. Once these attack trees are created, parameters will be chosen to evaluate and analyze each attack in the attack tree and to understand those that are most likely to happen to each type of wallet.

Taking into account the type of wallet, the identification of threats, and the assessment of the parameters of the attack trees, the safest wallet will be chosen as a proposal for implementation by the PJ.

That done, a proposal to improve security in the cryptocurrency storage process will be presented based on the application of Shamir's Secret Sharing concepts [7]. The goal is to present a proposal for a model in which the private keys that give access to cryptocurrencies are not under the control of a single person, but rather by a certain number defined by those responsible for the investigations. The focus once again is on the security of private keys, which consequently give access to the amounts of cryptocurrencies.

Although in the thesis the PJ is mentioned numerous times, the content of the thesis is solely the responsibility of its author. The thesis was not valid by the PJ nor does it in any way constitute a proposal by that entity.

II. Analysis of Threats to the Storage of Cryptocurrencies

The process of apprehending cryptocurrencies resulting from criminal acts is done as follows: when any illegal activity is detected by the PJ, it quickly tries to reach the place where the offense is being carried out. After arriving at the scene and capturing the criminal, the process of seizing cryptocurrencies begins. In an initial phase, responsible inspectors confiscate all material at the scene of the crime, identify and screen all electronic devices that may be involved in a certain way with the crime. After this sorting, the next step is to analyze all the transactions carried out by the criminal and investigate where the cryptocurrencies are kept. For example, if the computer or smartphone is turned on, it is possible to verify the existence of wallets (web wallets, desktop wallets, mobile wallets) and carry out an investigation of the number of cryptocurrencies involved in the criminal activity. In order to carry out this type of investigation, appropriate analysis software is used.

It should be noted that when the responsible entities seize cryptocurrencies, the criminal no longer has access to them. When wallets with the respective amount of cryptocurrencies are found, they are confiscated and it is up to the responsible entities to store them in the safest way.

This work focuses on this last stage of storage, as this is where the seized cryptocurrencies are stored, in wallets.

A. Identification and Characterization

The wallets are stored inside the headquarters of the Judicial Police, on hardware devices with or without an internet connection, on servers, or in safes. This storage mode depends on the type of Wallet. As such, Paper Wallets will be stored in safes, Mobile Wallets and Desktop Wallets will be stored on hardware devices with an Internet connection (eg computers and smartphones), Web Wallets on corporate servers, and Hardware Wallets on hardware devices without internet connection (eg pen drives, external drives, among others).

Figure 1 presents the model of the system under analysis in this chapter, with all the intervening components and their relationships.

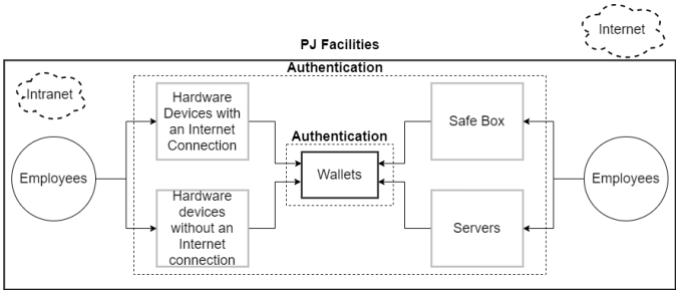

Figure 1: System Model

Right in the center of the model you can find the entity “Wallets”. These are where the amounts of cryptocurrencies seized in the PJ investigations are stored. This entity is the most important of the entire system and it is also the entity that does not want any attack to have access to your information. The purpose of this system is for cryptocurrencies to be stored in Wallets at the headquarters of the PJ with the highest possible levels of security, that is, to protect unauthorized and unauthorized access to Wallets' information. These Wallets are protected by an authentication factor, an access password. Only someone with this Wallet password can access the private keys and consequently the cryptocurrency value stored there.

The four entities around are the different places or devices where the Wallets can be stored. Each of these entities is protected with an authentication factor and only authorized employees have access credentials. Basically, if any other person (internal or external) or unauthorized employees tries to gain access to the information present on the Wallets, it is considered a security breach to the system. Internal people are interpreted as people who visit the PJ facilities and external people are interpreted as attackers.

The limit of this system represented by the larger rectangle is the physical facilities of the PJ. Within this limit, there is the Intranet, which is a private network that can only be accessed by users or internal employees with access credentials. All entities within this limit follow PJ rules and guidelines. Outside this limit, there is the Internet to which the PJ has no legislation, but defends itself against its dangers using firewalls and antivirus.

In this model, all forms of storing cryptocurrencies are represented and arrows are used to identify the only people who can access them. In order to have access, you will need to have access credentials for the various levels of authentication installed on the system.

B. Asset Identification and Access Points

The most critical assets of this system are:

- Wallets: where the amounts of cryptocurrencies are stored.
- Safe: physical space where paper Wallets can be stored.
- Servers: technology where web Wallets can be stored.
- Hardware devices with an Internet connection: devices where mobile and desktop Wallets can be stored.
- Hardware devices without an Internet connection: devices where the hardware wallets can be stored.

Wallets are the most critical asset of the entire system, as the goal is that no one accesses your content without being duly authorized. The remaining four assets are also very critical to the system because once your security is compromised, it becomes easier to access Wallets.

Regarding the most critical access points in the system, we have:

- Internet
- Intranet: corporate network limited to users or employees with access permissions.
- Employees: Employees are considered to be an access point, as these can be a means used by an attacker to gain access to Wallets.

These three access points are the only means that can be used to compromise the security of critical system assets.

C. Threat Determination

To determine the threats in the system under analysis, the STRIDE threat table [4] was used and related to the system's critical assets and access points [6]. Each asset or access point that is marked with an "x" in the types of STRIDE threats represents that it is subject to that type of threat.

TABLE I
STRIDE THREATS FOR ASSETS AND ACCESS POINTS

Assets / Access Points	**STRIDE Threats**					
	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Wallets	x	x		x		
Safe Box	x	x		x		
Servers	x	x		x	x	
Hardware devices with an Internet connection	x	x		x	x	
Hardware devices without an Internet connection	x	x		x		
Internet					x	
Intranet					x	
Employees	x		x	x		x

This threat table was used in order to facilitate the identification of some threats that the system is subject to. The remaining threats and vulnerabilities will be identified in the attack trees.

For each type of wallet, attack trees will be designed with the objective of discovering new threats, vulnerabilities, and drawing an attacker profile. Each attack tree will be related to these threats already identified. First, a description of this type of wallet will be made, as well as the active one it is related to, then the attack tree will be drawn with its respective relations and description of possible attacks to the system and finally, the parameters of the tree will be evaluated and attack chosen for this system.

As for the evaluation of the attack tree parameters, tables will be built after the design of the attack trees in which each attack will be evaluated according to the chosen parameters. The evaluation parameters chosen to analyze this system are:

- Technical difficulty of the attack: it has to do with the level and technical knowledge for the execution of the attack.
- Probability of success of the attack: the probability that this attack will materialize and compromise the system.
- Cost of the attack: monetary value necessary for the execution of the attack.

The scale of values for each parameter has the following attributions:

- Low
- Medium
- High

All values assigned to the analysis parameters are evaluated for each type of Wallet and at the end, the values are compared and the type of Wallet with fewer threats and vulnerabilities is chosen. The goal is to choose a type of Wallet for the Judicial Police to implement when seizing cryptocurrencies resulting from crimes.

D. Paper Wallet

In this type of Wallet, the private key is encrypted in the form of QR-Codes in paper format. As the name implies, these types of Wallets are practically impossible to suffer any type of external attack (eg. hackers).

For attackers, the main objective is to have access to the cryptocurrencies that are within the Paper Wallet. This type of wallet is normally kept in physical spaces under the protection of a responsible person. For this Wallet, a safe will be used as a physical storage space.

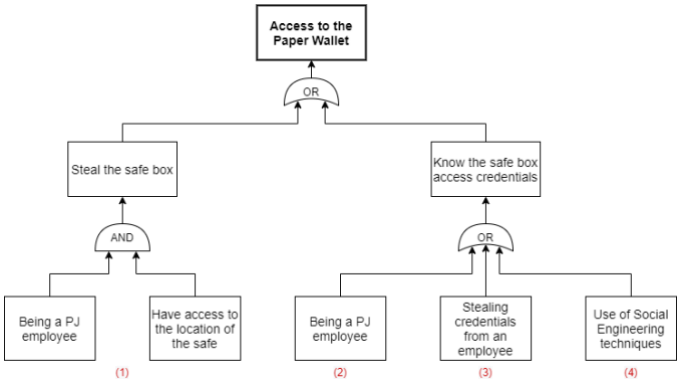

Figure 2: Paper Wallet Access Attack Tree

Note: the numbers in parentheses in the attack tree identify possible attacks on the security of the Paper Wallet.

It should be noted that in this type of wallet, the threats are internal, that is, the only possibility to access the Paper Wallet is if the attacker is an employee of the PJ. Sometimes dissatisfaction with work or earnings, emotional pressures, family uneasiness leads employees to behave incorrectly and try to harm the organization.

In this type of Wallet, there are two different ways for an attacker to try to access the Paper Wallet and steal the cryptocurrencies stored there. One is to steal the safe where this Wallet is and the other is to obtain credentials to access the safe. Taking into account these two ways of accessing the Paper Wallet, it was possible to remove four possible attacks through the attack tree.

Table II shows the analysis of the attacks through the evaluation parameters of the attack trees selected for this wallet.

TABLE II
ASSESSMENT OF ATTACKS ON PAPER WALLET

Attack	The technical difficulty of the attack	Attack probability of success	Attack cost
1	Low	Low	Low
2	Low	High	Low
3	Low	Low	Low
4	High	Low	Low

Table II identifies the attacks that can compromise the paper wallet (four attacks) and the classification of the three parameters chosen *a priori* to analyze each type of attack. In table II, the attack number (2) is selected in gray, as it is the attack with low technical difficulty and with a high probability of success, so it is with this type of attack that the PJ has to worry about implementing the paper wallet cryptocurrency storage mechanism.

E. Mobile Wallet

This wallet works as a smartphone application where private keys are stored there and it is possible to move cryptocurrencies using only the mobile phone. The Mobile Wallet is very practical, but it presents some threats considering that it is in a hardware device with an Internet connection and consequently makes it susceptible to external attacks (eg hackers).

For this type of wallet, the main objective of attackers is to access the value of cryptocurrencies stored in this wallet. For this wallet, will be using a smartphone (hardware device with an Internet connection) as a storage medium.

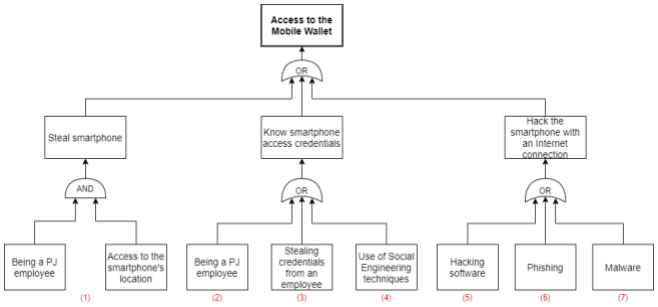

Figure 3: Mobile Wallet Access Attack Tree

In this type of wallet, the threats are both internal and external, that is, the attackers may be PJ employees or external people with malicious objectives.

In this type of wallet, there are three different ways for an attacker to access the mobile wallet and steal the cryptocurrencies stored there. The first is to steal the smartphone where the wallet is, the second is to somehow obtain the credentials for accessing the smartphone and the last is to hack the smartphone. It should be noted that in the latter the smartphone must be connected to the Internet, otherwise, it does not pose any type of threat to the wallet. Taking into account these three ways of accessing the mobile wallet, it was possible to remove seven possible attacks through the attack tree.

Table III shows the analysis of the attacks through the evaluation parameters of the attack trees selected for this wallet.

TABLE III
ASSESSMENT OF ATTACKS ON MOBILE WALLET

Attack	The technical difficulty of the attack	Attack probability of success	Attack cost
1	Low	High	Low
2	Low	High	Low
3	Low	Low	Low
4	High	Low	Low
5	High	Low	High
6	High	Low	High
7	High	Low	High

Table III shows the seven possible attacks on the mobile wallet as well as the classification of each parameter chosen for the analysis. The purpose of these tables is to select those attacks that are more likely to happen, with less technical difficulty, and with a lower cost, as these are the most likely to happen. An attack that involves a lot of technical knowledge will not occur as often as an attack that involves more basic concepts.

In this table, we can see that there are two attacks identified with another color, this means that they are the most likely to happen in relation to the mobile wallet. These are the attacks that the PJ has to worry about if it decides to implement the mobile wallet as a storage mechanism for cryptocurrencies.

F. Web Wallet

In this type of wallet, private keys are stored on the organization's servers. All company employees have access to the organization's Intranet, that is, an employee with privileged access, knowledge of the organization's systems, and other hacking knowledge can access the web wallet. The same applies to an attacker from outside the organization, the fact that private keys are stored on servers makes them more susceptible to external attacks.

For this type of wallet, the main objective of attackers is to access the Corporate Servers where the private keys are stored and consequently have access to the web wallet.

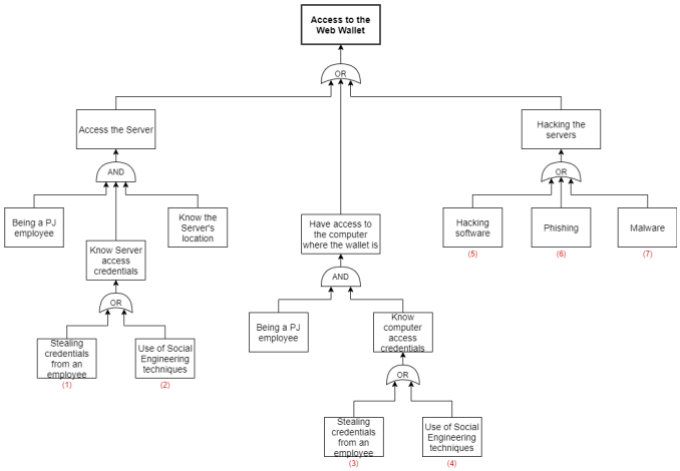

Figure 4: Web Wallet Access Attack Tree

Note: web wallets are stored on computers, but their private keys are on the organization's corporate servers.

In the web wallet, threats can be either internal (fraudulent employees) or external (external people who have malicious intentions in mind to harm the organization).

In this type of wallet, there are three different ways for an attacker to access the web wallet and steal the cryptocurrencies stored there. The first way is to have access to the server that stores the wallet's private key, the second way is to have access to the computer where the wallet is and the third way is to hack the server where the private key is stored.

Taking into account these three ways of accessing the web wallet, it was possible to remove seven possible attacks through the attack tree.

Table IV shows the analysis of the attacks through the evaluation parameters of the attack trees selected for this wallet.

TABLE IV
ASSESSMENT OF ATTACKS ON WEB WALLET

Attack	The technical difficulty of the attack	Attack probability of success	Attack cost
1	Low	Low	Low
2	High	Low	Low
3	Low	High	Low
4	High	High	Low
5	High	Low	High
6	High	Low	High
7	High	Low	High

Table IV shows the seven possible attacks on the web wallet and the respective classification of each parameter chosen for analysis. Of the seven attacks, only (3) and (4) have high probabilities of success, so these are the ones that in the case of implementation of the web wallet, the PJ has to worry about and protect. It should be noted that these two types of attacks only happen if there are fraudulent employees inside the premises of the PJ, otherwise, the probability of these attacks ever materializing is low.

G. Desktop Wallet

This type of wallet is downloaded and installed on a computer and keeps private keys on the hard drive. The desktop wallet does not need third parties to use your data, as is the case with the Web Wallet that needs corporate servers to store your private keys, thus making it a slightly more secure solution. Although at first glance this type of wallet seems more secure, computers can be connected to the Internet, thus making it impossible to fully trust cryptocurrency storage.

Note: a type of wallet that is on a device with an Internet connection is always more susceptible to a greater number of threats than a wallet that is on a device without an Internet connection.

For this type of wallet, the main objective of attackers is to access the computer on which the desktop wallet is installed.

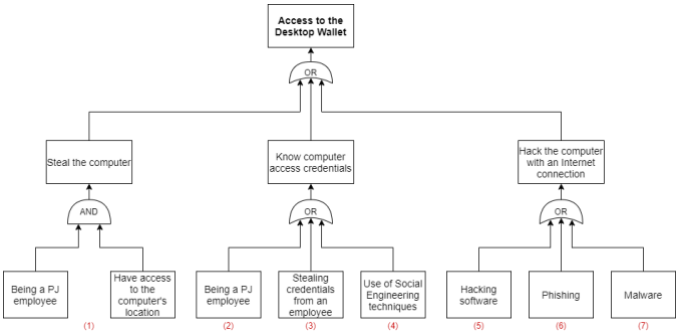

Figure 5: Desktop Wallet Access Attack Tree

On the desktop wallet, there are both internal and external threats to your security. The three main ways that it can lead to improper access to the desktop wallet are for example theft of the computer where the wallet is installed, an employee

knowing the credentials of accessing the computer, and hacking the computer.

Taking into account these three ways of accessing the web wallet, it was possible to remove seven possible attacks through the attack tree.

Table V shows the analysis of the attacks through the evaluation parameters of the attack trees selected for this wallet.

TABLE V
ASSESSMENT OF ATTACKS ON DESKTOP WALLET

Attack	The technical difficulty of the attack	Attack probability of success	Attack cost
1	Low	High	Low
2	Low	High	Low
3	Low	Low	Low
4	High	Low	Low
5	High	Low	High
6	High	Low	High
7	High	Low	High

Table V shows the seven possible attacks on the desktop wallet and the respective classification of each parameter chosen for analysis.

This table shows that there are two attacks identified with gray color, this means that they are the most likely to happen and those that will be more successful. These are the attacks that the PJ has to worry about if it decides to implement the desktop wallet as a storage mechanism for the confiscated cryptocurrencies.

H. Hardware Wallet

This type of wallet is one of the safest options for storing any type of cryptocurrency, as it stores private keys on hardware devices without any direct connection to the Internet, that is, it does not lack any external attack attempt via the Internet.

For attackers, the main objective is to have access to the cryptocurrencies that are inside the hardware wallet. This type of wallet is usually stored on flash drives or external disks.

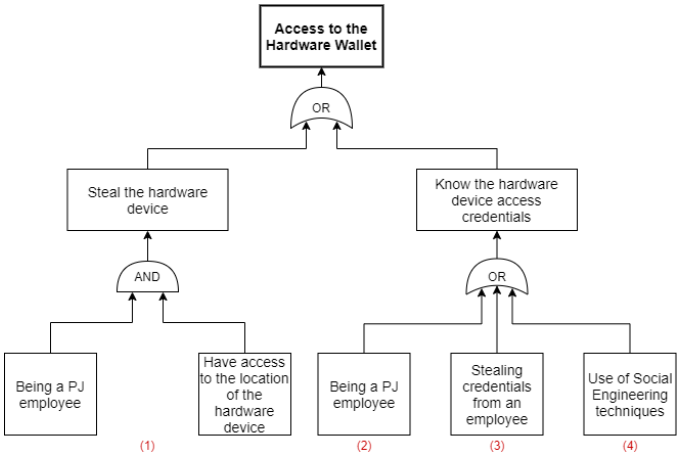

Figure 6: Hardware Wallet Access Attack Tree

In this type of wallet, the threats are only internal, that is, the only possibility to access the hardware wallet is if the attacker is an employee of the PJ. Dissatisfaction with work or earnings, emotional pressures, family uneasiness is all characteristics that can lead employees to perform functions incorrectly and try to harm the organization.

In this type of wallet, there are two ways for an attacker to access the wallet hardware and steal the cryptocurrencies that are stored there. One is to steal the hardware device where this wallet is and the other is to obtain the credentials to access that device. Taking into account these two ways of accessing the hardware wallet, it was possible to remove four possible attacks through the attack tree.

Table VI shows the analysis of the attacks through the evaluation parameters of the attack trees selected for this wallet.

TABLE VI
ASSESSMENT OF ATTACKS ON HARDWARE WALLET

Attack	The technical difficulty of the attack	Attack probability of success	Attack cost
1	Low	High	Low
2	Low	High	Low
3	Low	Low	Low
4	High	Low	Low

Table VI identifies the four attacks that can compromise the hardware wallet and the respective classification of the three parameters chosen to analyze each type of attack. In the table, the attacks (1) and (2) are selected with another color, because they are attacks with low technical difficulty and with a high probability of success, so it is these types of attacks that the PC has to worry about if implementing hardware wallet as a storage mechanism for cryptocurrencies.

It should be emphasized once again that this type of attack takes place only if there are fraudulent employees inside the facilities of the PJ.

III. SECRET SHARING IN THE SECURITY OF CRYPTOCURRENCIES STORAGE

The main objective of this section of the work is to make sure that the keys that give access to cryptocurrencies are not under the control of a single person because unlike other seizures of money, gold, silver, jewelry, drugs, etc., the value it is not in the seized object, but in the data. The problem that arises here is that this data is trivial to copy and consequently susceptible to stealing. If a fraudulent person gets his hands on this data, he can steal the total value of seized cryptocurrencies.

The fact that the private key is under the control of a person can lead to the total loss of the value of cryptocurrencies, in case of destruction of the key or death of the person and no backups of the data.

Then we had the following idea: divide the key that gives access to cryptocurrencies by several shares and by some participants (the concept of Secret Sharing) so as not to leave this key under the control of just one person. This means that it

becomes more difficult for someone with illegal activities in mind to access cryptocurrencies. Thus contributing to a significant improvement in the security levels of the seized cryptocurrencies.

Bearing in mind and taking into account this challenge in this section of the work, a procedural and operational model for the process of storing cryptocurrencies in wallets by the PJ will be elaborated, applying concepts from Shamir's Secret Sharing model with a hierarchical structure of PJ positions. The purpose of this model is to improve the levels of confidentiality, integrity, and availability of data in the cryptocurrency storage process.

A. Model

In this model, the dealer will distribute parts of a private key of a wallet that stores cryptocurrencies. In the present model, the dealer is the inspector responsible for criminal investigations related to cryptocurrencies. The main task of these inspectors, in addition to completing the investigation and securely storing the cryptocurrencies, is not to let any PJ employee have unauthorized access to the wallet where the cryptocurrencies are located. In this model, they distribute parts of a private key to only those people who really need access to the information inside the wallets.

The distribution and reconstruction of this private key are done through a hierarchical structure. The secret will be distributed using a k number of shares and a number of participants defined by those responsible for capturing the cryptocurrencies. These values of k and n can vary according to the criticality of the information present in the wallets, that is, the secret.

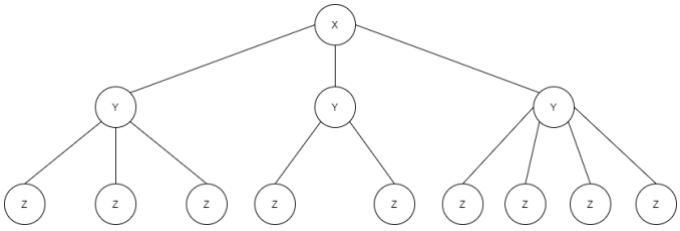

Figure 7: Model Proposal with a Possible Hierarchical Structure for the PJ

In this model proposal, three hierarchical levels can be included (X, Y, Z), with X being the highest level in the hierarchy, which includes all PJ management bodies, Y the intermediate level in the hierarchy, where they are all units of PJ and Z at the lowest level are included, where all subunits or teams of PJ are included. In this model proposal, only three hierarchical levels are visible, but new levels and new participants can be added, depending on the organization for the organization. In this case, three levels were proposed taking into account the organization chart of the PJ.

The inspectors responsible for the investigation and capture of cryptocurrencies distribute the secret by a certain number k of shares corresponding to a number n of participants. The shares in this model may be electronic devices such as computers, flash drives, external disks, among others, they may also be in paper format, kept safely by each participant, or even memorized in the head. The purpose of the shares is that the participants have kept each piece of the secret safe and that the share of each participant cannot be corrupted by any external factor. When it is necessary to carry out a reconstruction of the secret to have access to the information, the participant must be present and in possession of his share for this process to be possible.

B. Model Instantiation and Best Practices

The purpose of these rules is to make the model versatile for all organizations that make this type of apprehension and to ensure that data is safeguarded in the event of any internal or external malicious act.

1. In this first rule, no employee can reconstruct the secret alone. The creation of this rule meets the main objective of this chapter of the work, which is the fact of not leaving the key to access cryptocurrencies under the control of a person or employee. Not letting an employee alone reconstruct the secret means that cases, where an employee has illicit activities and breaches of the security of the employee's devices or work area, are minimized. In case of a security breach, cryptocurrencies are safeguarded with the use of this rule. This rule is valid for all hierarchical levels.

2. In the second rule, at least two employees from different hierarchical levels are needed to reconstruct the secret and consequently have access to the wallet information. This rule comes again to fulfill the main objective of this section of the work (not to allow the key to access cryptocurrencies to be under the control of one person or employee). It was defined that the secret can only be reconstructed when employees from different hierarchical levels are involved so that there is mandatory communication between the levels and the secret is not reconstructed by a single direction, unit, or team. This need for communication with at least another hierarchical level leads an employee x to know why employee y needs to want to access cryptocurrencies. With this rule, a kind of natural control is created to access cryptocurrencies, that is, if an employee x perceives that there is no need for the employee y to access the cryptocurrencies, he can report the situation to the boss or give another alternative or advice y employee to continue with his activities. Thus increasing the security levels of the cryptocurrencies seized by the PJ.

3. In this third and final rule, at least one employee of the subunit or team responsible for capturing and storing the cryptocurrencies is required to reconstruct the secret. This rule exists for the team that made the apprehension to know why other teams, units, or directions want to access cryptocurrencies. If the responsible team knows the reason why other employees want to access cryptocurrencies, it makes this process much safer and proof against malicious internal acts. It should be noted that not even employees of high hierarchical levels can access cryptocurrencies without the presence of a member of the apprehension team in the process of reconstructing the secret.

This hierarchical model uses some concepts of Shamir's Secret Sharing, namely, regarding the definition of the number of participants n, a number of shares k, and the relationship between n, k, and the process of reconstructing the secret. With the rules described above, the model is able to offer continuous-time availability of data, that is, any of the employees to whom part of the key data has been distributed needs and has reasons to access the cryptocurrencies, this access is designed at any time (with the participation of one of the employees of the team that carried out the seizure of cryptocurrencies). It also offers greater confidentiality and data integrity in the process of storing cryptocurrencies.

In case of any fraudulent employee, destruction, or corruption of a participant's share, there is a backup of all the information that each employee has. This backup is in the possession of the team responsible for capturing the cryptocurrencies and can only be used in these specific cases. This backup creates the necessary redundancy for this model to increase security levels against this type of situation.

Using this model, the PJ is able to increase the levels of information security against possible attacks, malware, malicious acts, human errors, and improper access to its systems and reduce the side effects of a possible breach of internal or external security.

IV. Analysis of Results and Conclusions

The analysis of the Paper Wallet shows four possible attacks on the breach of its security and the consequent theft of cryptocurrencies. Of these four attacks, the one that is most likely to happen is attack number two (being an employee of the PJ, having credentials to access the safe and access the paper wallet), if and only if there are fraudulent employees inside the PJ premises. But, now bringing the reality of things, the four possible attacks identified for this type of wallet are all internal in character, that is, the PJ can control all the factors around it so that these types of attacks never happen if it gets to implement a paper wallet for storing the seized cryptocurrencies. For the PJ this type of wallet is a good solution because, in addition to not being connected to any device with a direct connection to the Internet, it presents fewer threats and attacks than the other types of wallet. The only one with the same number of threats and attacks is just the hardware wallet that will be analyzed later.

Mobile Wallet can verify the existence of seven possible attacks to the breach of its security. Of these seven, only two have a more credible chance of success compared to the remaining attacks. These two attacks have low levels of technical difficulty and costs, so they can be more recurrent attacks than those involving more technical knowledge and high monetary values. This type of wallet is one of the most practical, but it has some security vulnerabilities since it is on a device with a direct connection to the Internet. Being on such a device, the number of threats goes up as can be seen in the STRIDE threat table and consequently the number of attacks goes up, making this type of wallet less safe for storing the seized cryptocurrencies.

Regarding the Web Wallet, there are seven possible attacks to access the wallet and consequently steal the cryptocurrencies stored there. Of the seven possible types of attacks, the most likely to be successful are number three (stealing credentials from an employee to gain access to the computer where the wallet is) and number four (using social engineering techniques to know credentials access to the computer where the wallet is located). The fact that in this type of wallet the private keys are stored on servers and the software of the wallet is on a computer or smartphone (both connected to the Internet) leads to a higher number of threats and attacks, as can be seen in the table of STRIDE threats and the attack tree of the web wallet. This type of wallet is very similar to mobile wallets and desktop wallets, the only difference being that private keys are stored on the organization's servers. If the server is compromised, all cryptocurrencies stored in the wallets may be in danger. This wallet is very practical daily, but at the security level, it is not very secure, since it is on devices with a direct connection to the Internet and the private keys are stored on servers under the control of people other than users. Looking at these results and features, the web wallet is not a good solution for the PJ to store the cryptocurrencies seized in its investigations.

The Desktop Wallet works basically like the mobile wallet, only instead of the wallet being on a smartphone, it is on a computer. Checking in the attack tree that the wallet is susceptible to seven possible attacks, of these only two have a good chance of success which is in the case that the computer with the wallet installed there is stolen and in the case that an employee with access credentials to the computer access the wallet and withdraw all your funds. It should be noted that these two attacks are more likely to happen when there are fraudulent employees inside the facilities of the PJ. This type of wallet is practical, but again it has security vulnerabilities. The fact that it is installed on a computer with an Internet connection means that it has more threats and, consequently, a greater number of possible attacks on your security (verified in the STRIDE threat table and in the corresponding attack tree). Taking into account the previous information, the desktop wallet is not a good solution for the PJ to keep the seized cryptocurrencies, as a result of illegal acts.

Finally, in Hardware Wallet, there are four possible attacks to the wallet's security. Of these four attacks, only two are more likely to materialize, such as attack number one (being a PJ employee, knowing the location of the hardware device and stealing the device) and attack number two (being a PJ employee, know the credentials to access the hardware device and access the hardware wallet). These two attacks are more frequent if and only if there are fraudulent employees inside the PJ facilities. The number of threats and attacks is lower than wallets with Internet connections, as can be seen in the STRIDE threat table and in the respective attack tree. Fewer threats and fewer possible attacks reveal that this wallet in terms of security is a good solution for the PJ. This type of wallet, within the category of cold wallets, is a good solution for storing large monetary values for long periods of time. That is exactly what the PJ needs, a secure mechanism that does not have any type of connection to the Internet and that allows storing the

cryptocurrencies seized for a long time or even define some use for them.

In short, of the five types of wallets analyzed in this work, the Hardware Wallet in terms of cryptocurrency security is the best option for the PJ to store the seized cryptocurrencies after the investigations.

Regarding the model based on Secret Sharing concepts, often assets of high importance for an organization, such as cryptocurrencies, are under the responsibility of only one person. This is not a good strategy to preserve information security within an organization. If this model is implemented, it means that the data is distributed only by the people who need to know or need it to work and that in the absence of one of these people it is possible to have access to that information. Thus preventing possible fraudulent employees from corrupting the information or having access to unauthorized information.

This model is given in case the PJ wants to increase their levels of information security concerning the process of storing the seized cryptocurrencies.

If this model is applied, together with the use of a hardware wallet to store private keys, cryptocurrencies will be more secure against possible attacks or malicious acts within the PJ.

Imagining that the PJ chooses to use hardware wallets for the storage of private keys that consequently give access to the seized cryptocurrencies. In addition to cryptocurrencies being protected against attacks via the Internet, with the application of this model they are also safer against attacks by employees from within the PJ, making the process of storing cryptocurrencies safer.

With the application of Secret Sharing in this model, the shares (pieces of private key data) of employees, distributed by inspectors responsible for criminal investigations involving cryptocurrencies, are more protected and there is only some kind of access to information when all conditions are met, that is, the number of shares required, respecting the hierarchical rules imposed by the model. This is a possibility of implementing Secret Sharing on a hardware wallet to improve security in the process of storing cryptocurrencies by the PJ.

The future work of this dissertation involves communicating to the PJ the analysis regarding the security of the different types of wallets used to store cryptocurrencies and the proposal of a model based on Secret Sharing to improve the process of storing cryptocurrencies seized by the PJ. In addition to presenting the analysis and the model, the team responsible for criminal investigations involving cryptocurrencies may be asked what types of wallets they use most and what methods or good practices they use to keep them safe. To make those responsible for this area of the PJ see that the implementation of hardware wallets is an asset in terms of the security of cryptocurrencies for the organization.

V. References

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. ResearchGate.

[2] Gentilal, M., Martins, P. & Sousa, L. (2017). TrustZone-backed Bitcoin Wallet. Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems pages 25-28.

[3] *Cointelegraph*. What is Cryptocurrency. Guide for Beginners. Available in: https: //cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies.

[4] Kohnfelder, L., Garg, P. (1999). The threats to our products. In Microsoft Interface. Microsoft Corporation.

[5] Simonjan, J., Taurer S., & Dieber, B. (2020). A Generalized Threat Model for Visual Sensor Networks. Sensors, Vol. 20.

[6] Shostack, A. (2008). Experiences Threat Modeling at Microsoft. Microsoft. Available in: http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-413/paper12.pdf

[7] Shamir A. (1979). How to Share a Secret. Communications of the ACM, Vol.22, pages 612-613. Available in: https:// dl.acm.org/doi/abs/10.1145/359168.359176