OPERATIONAL GUIDE

CRYPTOCURRENCIES

ASSET RECOVERY

FEDERAL PROSECUTION SERVICE

OPERATIONAL GUIDE
CRYPTOCURRENCIES
ASSET RECOVERY
FEDERAL PROSECUTION SERVICE

FEDERAL PROSECUTION SERVICE

2nd CHAMBER OF COORDINATION AND REVIEW

OPERATIONAL GUIDE
CRYPTOCURRENCIES
ASSET RECOVERY

Brasília - MPF 2023

Available at:
<http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes>

Criminal Chamber
Permanent Members
Carlos Frederico Santos
Coordinator
Associate Federal Prosecutor General

Luiza Cristina Fonseca Frischeisen
Associate Federal Prosecutor General

Francisco de Assis Vieira Sanseverino
Associate Federal Prosecutor General

Deputy Members
Paulo de Souza Queiroz
Associate Federal Prosecutor General

Adriana de Farias Pereira
Federal Circuit Prosecutor of the Republic

José Robalinho Cavalcanti
Federal Circuit Prosecutor of the Republic

Coordination and Organization
Cryptocurrency Working Group
2nd CHAMBER OF COORPERATION AND REVIEW

Alexandre Senra
Federal Prosecutor in Espírito Santo

Anamara Osório Silva
Federal Circuit Prosecutor of the Republic
Deputy Secretary for International Cooperation/PGR

Eduardo El Hage
Federal Prosecutor in Rio de Janeiro

Marisa Varotto Ferrari
Federal Prosecutor in Rio de Janeiro

Thiago Augusto Bueno
Federal Prosecutor in Amazonas

Tiago Misael de Jesus Martins
Federal Prosecutor in Minas Gerais

Office of the Prosecutor General 2nd
Chamber of Coordination and Review
SAF Sul, Quadra 4, Conjunto C
Telephone +55 (61) 3105-5100
70050-900 - Brasília - DF
www.mpf.mp.br

INDEX

INTRODUCTION

This is the first version of the guide for the Federal Prosecution Service's action on cryptocurrencies. The main objective is to make the member understand the discussions, qualifying them to adopt the proposed actions or not.

The guide is organized into three parts. The first brings together information necessary to understand the discussions and functional guidelines proposed. The second brings the discussions and guidelines themselves. The last one features templates that can be used by members of the MPF in case studies.

Understanding this guide does not require prior knowledge on cryptocurrencies, making it, in this sense, a guide from scratch. However, this is still an operational guide; it is not a course on cryptocurrencies or Blockchain. It represents, therefore, a snapshot of what matters to the MPF's actions in this matter. The sea of knowledge one foot deep would be of no use herein. Instead, the guide delves into strategic locations, to the necessary depth.

Throughout the text, notably in the first part, the guide makes use of operational definitions useful for the proposed discussions, without pretense of scientific rigor. We have not found a more objective way to fulfill the purpose of this guide.

An example: cryptocurrencies have been defined as digital assets that cannot be copied. This is not to disregard the importance of elements such as cryptography and Blockchain technology, but rather to demonstrate that they are not necessary to understand the term “cryptocurrency” in the context used in this guide.

The guide is not exhaustive nor does it aim to be. Even within the first section (which matters to the MPF’s actions), the topic is potentially inexhaustible. Two other subsequent snapshots were then made: this first version was limited to the subtopic of asset recovery, which seemed to us to be the most urgent; and the focus is Bitcoin, although much of what is said herein is applicable to many other cryptocurrencies.

CRYPTOCURRENCIES

Cryptocurrencies are digital assets that cannot be copied. They also serve as the designation of a genre.

Next, each of these propositions is examined.

CRYPTOCURRENCIES ARE DIGITAL ASSETS THAT CANNOT BE COPIED

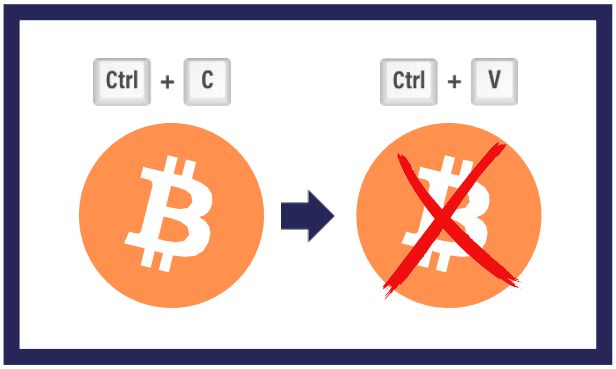
May 25, 2022, from my computer, in Vitória/ES, I submitted the pdf of this guide, still in preparation, to a colleague at the MPF. From this simple conduct, at least three more copies of the PDF emerge. The document, which previously only existed on my computer, now also exists in the “sent items” box of my e-mail, in the “received items” box of this colleague’s e-mail and on his computer, as soon as he downloads the file.

On the same day and place, I submitted 0.1 bitcoin from my wallet to another wallet. Shortly afterwards, my wallet now has 0.1 less bitcoin and the destination wallet now has 0.1 more bitcoin.

Despite having used the verb “submit” in both situations, the consequences of “submitting” were completely different.

The first situation involved a copiable digital object, while the second involved a digital object that cannot be copied.
– A digital object, in this sense, scarce.

What if, instead of a document in .pdf format, I submitted a photograph or a film? We would be facing the same problem, consistent with the lack of scarcity of these media, which, as digital assets, can be copied at a cost very close to zero.



It is, therefore, the attribute of scarcity that particularizes cryptocurrencies and not the fact that they are digital assets. Games and computer programs, for example, are also digital assets, but they can be technically copied, as piracy clearly highlights.

CRYPTOCURRENCIES AS THE DESIGNATOR OF A GENRE

Cryptocurrency is synonymous with token in the broadest sense and designates a genus, made up of species that can be classified using various criteria.

Let us take a look at some of them.

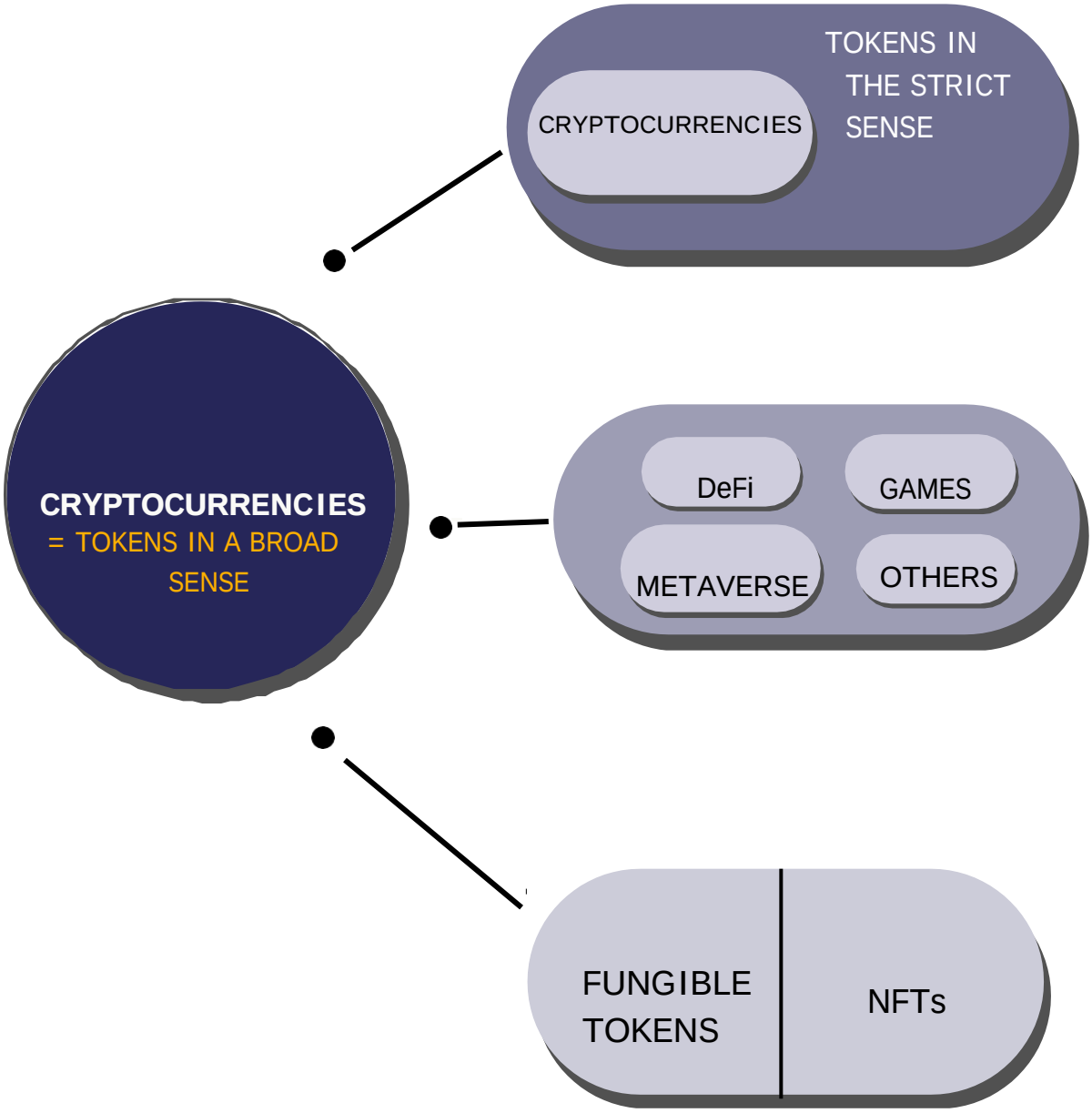
(a) Depending on whether or not they serve to pay fees for using a Blockchain: cryptocurrencies and other tokens.

(b) Depending on the purpose of the application to which they are linked: DeFi tokens, gaming tokens, metaverse tokens, etc.

(c) According to fungibility: fungible tokens and NFTs.

Evidently, some correlations can be drawn between these classifications. For example: all cryptocurrencies are fungible tokens; Metaverses are usually structured around fungible tokens and NFTs. But doing so at this time would cause unnecessary confusion.

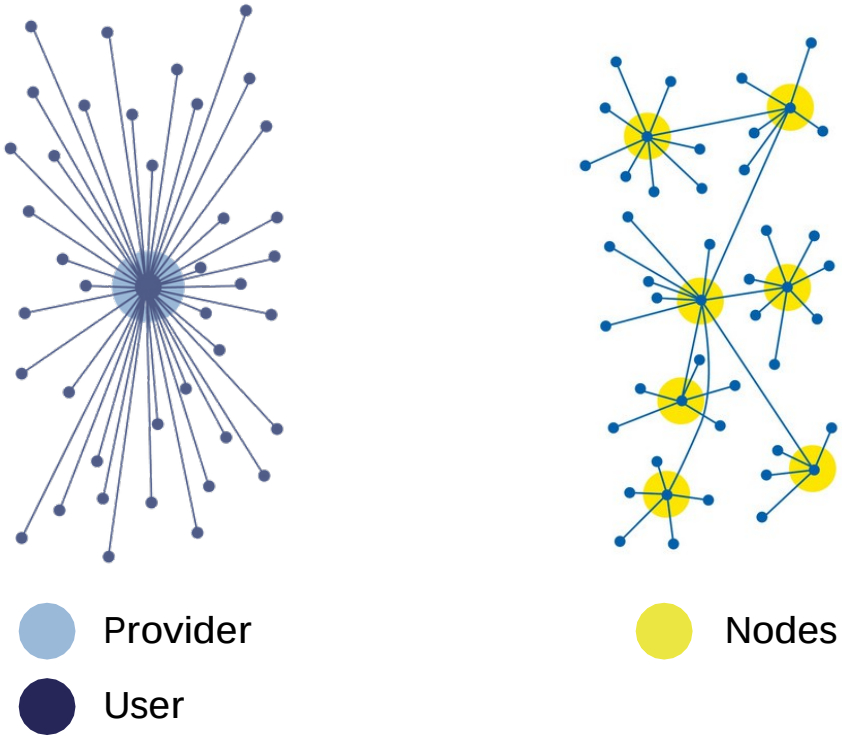
The species that are of interest to this guide will be adequately addressed later.



BLOCKCHAIN

Blockchain is the primary species within the genus of ‘distributed ledger technologies’

Information can be ledged in a centralized manner, at a single point in the network, also known as a provider, in contrast to the other points in that network, referred to as users. Alternatively, information can be ledged in a decentralized manner among various points in the network, which are herein referred to as nodes.



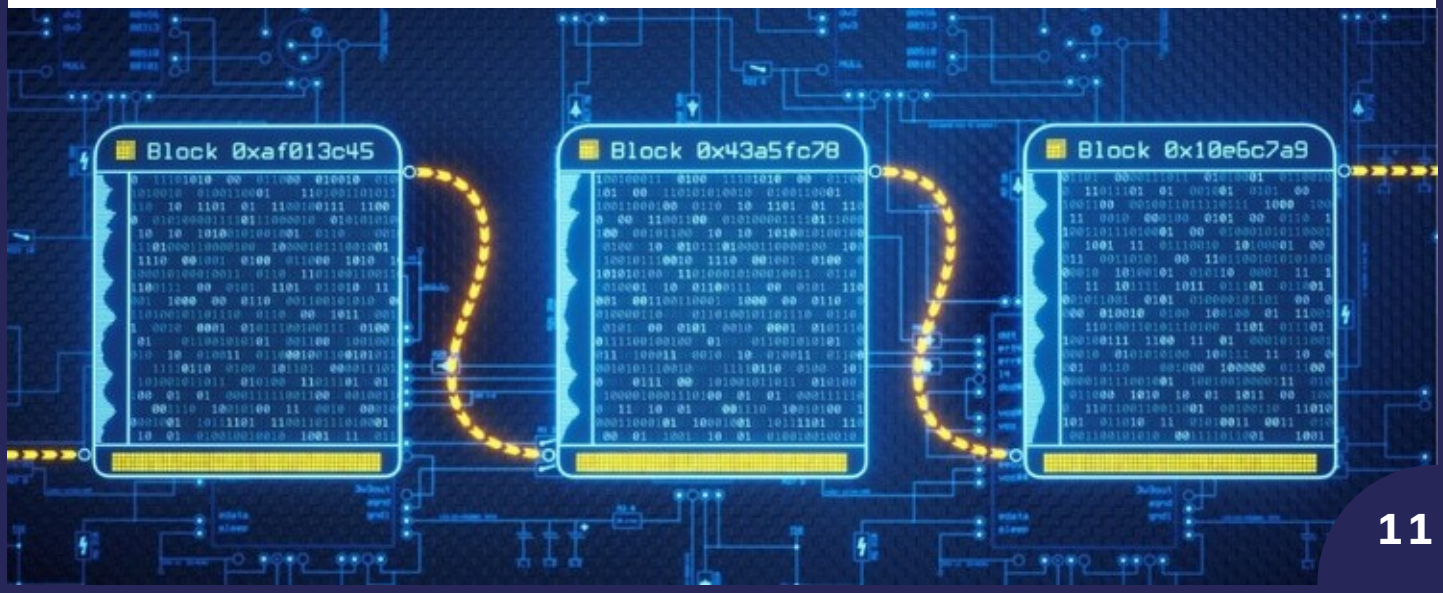
Each way of doing it has its advantages and disadvantages.

Centralized ledgers are extremely cheap and fast, but they depend on trust in the authority responsible for this ledger. Decentralized or distributed ledgers, in turn, are comparatively more expensive and slower to create, but do not require trust in any authority.

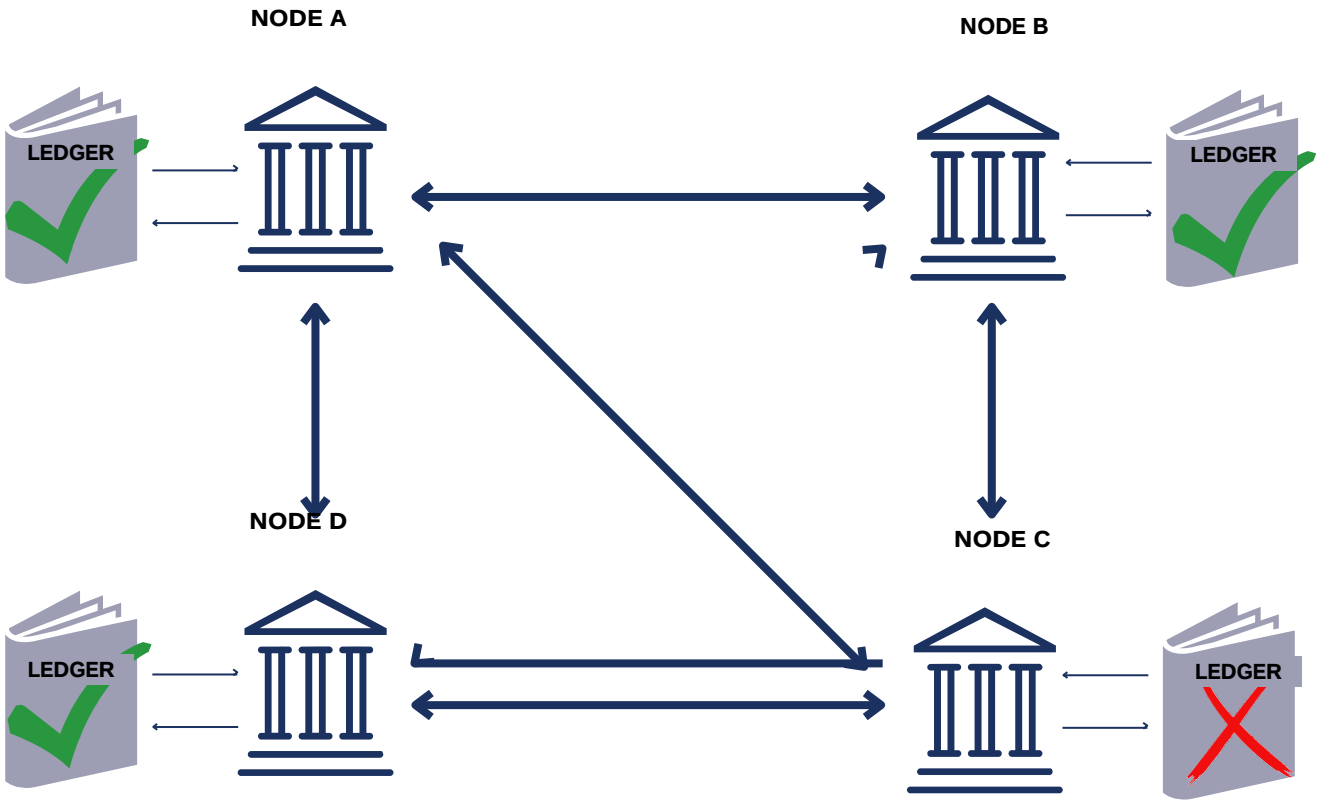
One example. Transactions between accounts on the same cryptocurrency exchange are fast and cheap, but their veracity requires us to trust that exchange, responsible for the centralized ledger of information. Transactions made between bitcoin addresses are more expensive and slower, but do not require trust in any authority, because there is no authority responsible for the ledger, which is maintained in a distributed manner among the various nodes of the network.

Just one of the practical repercussions of this difference: a centralized ledger can be tampered with by the authority responsible for it; a distributed ledger cannot be tampered with by anyone.

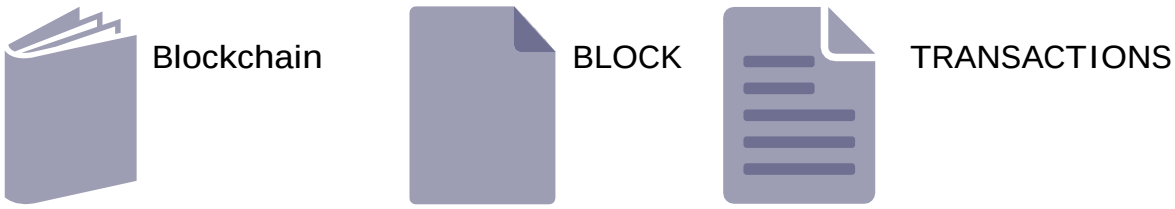
Blockchain is a type of distributed ledger, composed of chronologically ordered data blocks, where each block immediately links to the previous one and confirms, through mathematical proofs, the transactions contained in all previous blocks.



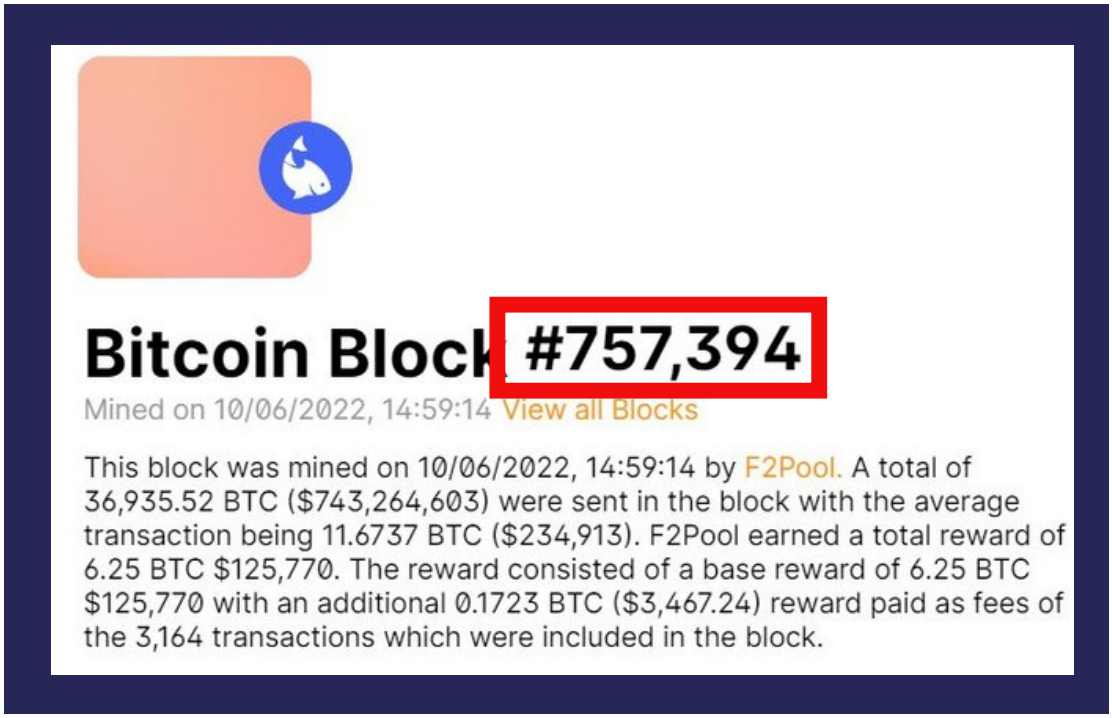
Think of Blockchain as being a ledger present in several ways around the world. They are not copies made from the same original, but rather copies, of equal importance and originality, synchronized with each other, where any undue change made in one of these copies is easily perceived and quickly repelled by the others.



Moving on with the metaphor of the distributed ledger, imagine that said book receives new pages over time and that on each sheet there may be many or few lines written. The sheets correspond to Blockchain blocks. The phrases correspond to the transactions of each block.



In the case of Bitcoin, provided that its first block has been mined (Block Zero), at 4:15 pm (UTC-3) on JAN/03/2009, a new sheet is added approximately every ten minutes. At this exact moment, at 3pm on OCT/06/2022, said book already has 757,395 pages. [1]



1- Block number 757,394 corresponds to the 757,395th sheet of our book because Block Zero corresponds to the first sheet.

BITCOIN

Bitcoin was designed to be a payment system without intermediaries.[2] However, to continue understanding the subject, more relevant than knowing this is knowing that “Bitcoin” is an ambiguous word.

Three of its meanings, despite being closely related, need to be discerned: Bitcoin-hardware, Bitcoin-software and Bitcoin-cryptocurrency.

Bitcoin-hardware is the name given to the set of physical devices around the world, responsible for the security of the Blockchain against any fraud attempt. That is the Bitcoin network.

Bitcoin-software is the term used to refer to the program that runs on these physical devices, of which they are part, in a simplified manner: the Blockchain, a random generator of key pairs and a set of rules.

In an analogy, bitcoin hardware is for your notebook, just as bitcoin software is for the Windows or Linux you run thereon. In the same way that notebooks and Windows are not confused, bitcoin-hardware and bitcoin-software should not be confused.

2- http://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf

We have already discussed Blockchain. We will discuss the key pair generator later. We will now talk about some of the rules of the Bitcoin protocol, starting with the definition of what bitcoin is - cryptocurrency.

Bitcoin-cryptocurrency (BTC) is a scarce digital asset whose first purpose is to serve as payment that the software makes to the hardware to function and whose second purpose is to serve as currency for the payment of fees by those who want to make use of the bitcoin network.

Let us briefly examine each of these purposes.

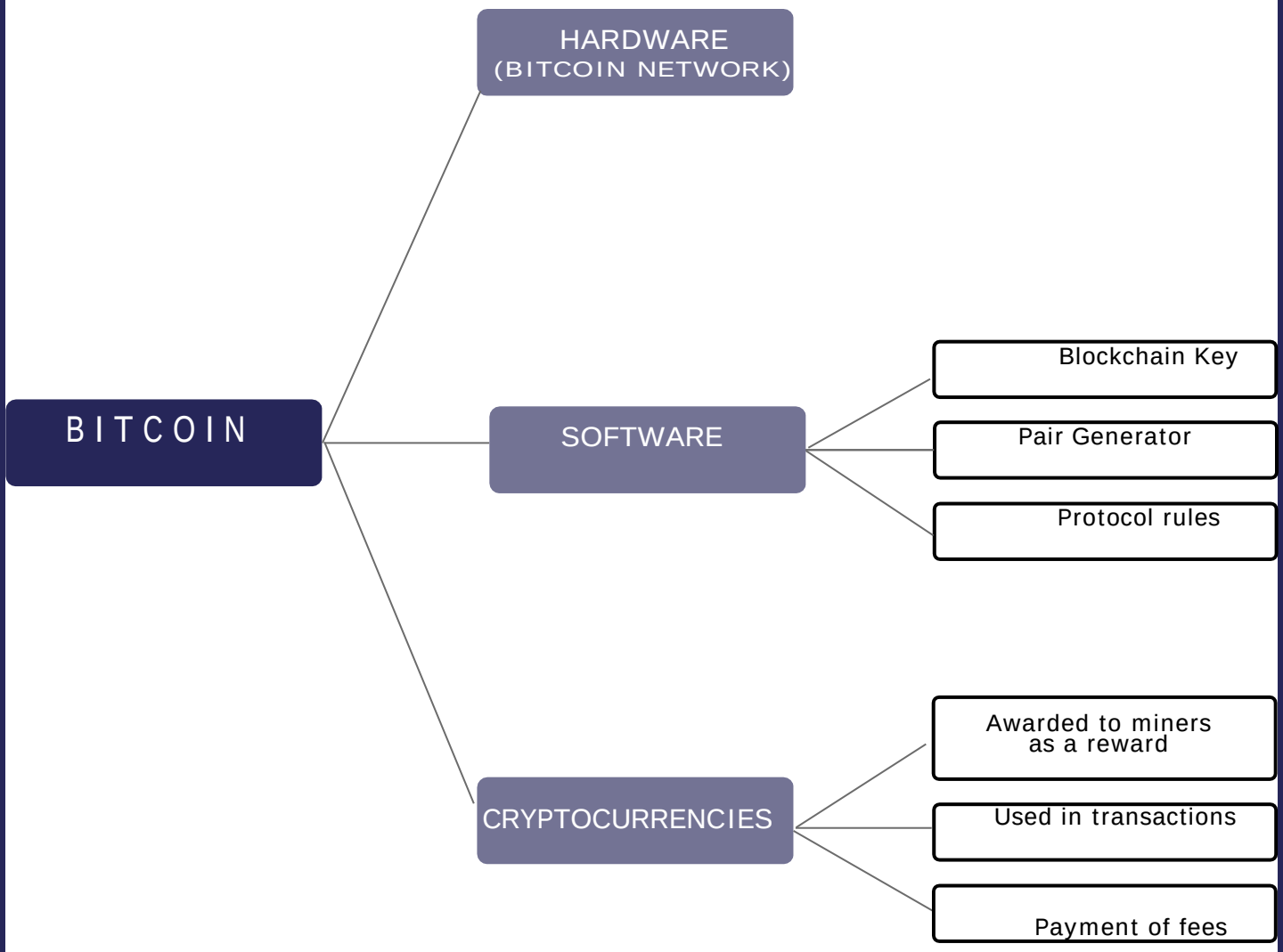
First purpose: New blocks are added to the Blockchain through a process commonly called “mining”, which involves a high expenditure of electrical energy and computational power. This is a dispute, fought between miners, aiming for a reward, consisting of new BTC issued and assigned, for each new block, to a winning miner.

Second purpose: In order to submit BTC through the Bitcoin network you do not need to be a miner nor do you need to have a Blockchain copy with you. However, a small transaction fee must be paid, necessarily in BTC.[3] For this reason the BTC is a cryptocurrency, because it plays the role, in this context, of a currency.

Its issuance follows some protocol rules:

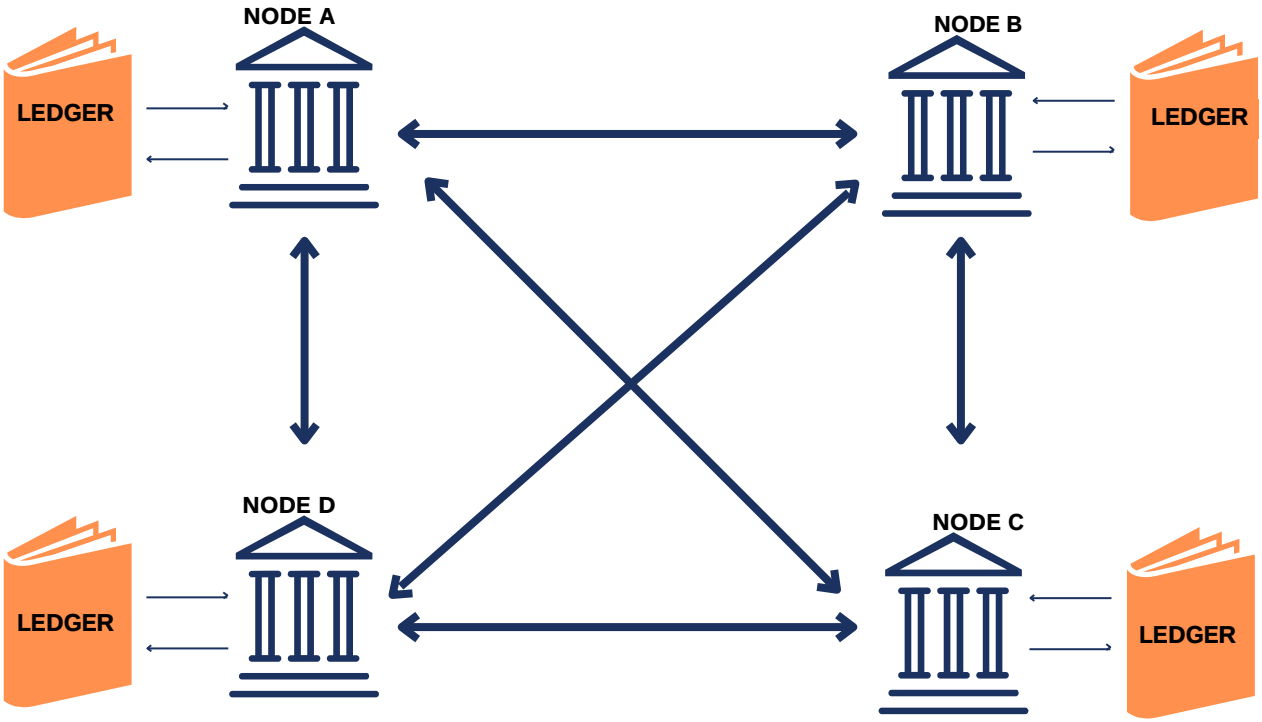
- it is limited to 21 million;
- it takes place with each new block mined;
- initially it was 50 BTC per block and currently it is 6.25 BTC per block,
- considering that it is halved every 210,000 new blocks, in a process referred to as halving.

3- The amount of the transaction fee does not depend on the amount transacted but on two other factors: the space that the transaction occupies on the Blockchain and the demand for using the Bitcoin network. The larger the space occupied by the transaction and the greater the demand for using the network, the higher the fee to be paid.


BITCOIN
HARDWARE
(BITCOIN NETWORK)
SOFTWARE
Blockchain Key
Pair Generator
Protocol rules
CRYPTOCURRENCIES
Awarded to miners
as a reward
Used in transactions
Payment of fees

WHERE ARE THE CRYPTOCURRENCIES LOCATED

As digital assets that they are, cryptocurrencies are not in the physical world. From the user's perspective, cryptocurrencies can be with them or with third parties. From a technical perspective, cryptocurrencies are with no one. They are entries into a public, distributed ledger called the Blockchain. Either they are in this book or they simply do not exist.



It is necessary not to confuse cryptocurrencies with a balance in cryptocurrencies. Cryptocurrencies are ledged on the Blockchain; cryptocurrency balances are ledged in a private and centralized database, belonging, for example, to an exchange.

A designation commonly used in this differentiation is that of on-chain transactions and off-chain transactions. In the first case, you do not need to trust anyone, just the Blockchain security process. In the second case, it is necessary to trust the person responsible for the centralized ledger.

This is because, when a customer opens an account on an exchange, the private keys to that account are held by the exchange, which is responsible for carrying out operations on the customer's behalf – and not by the customer himself/herself.

To receive deposits in cryptocurrencies, the exchange assigns each customer an address on the Blockchain. After the cryptocurrency is received at the customer's individual deposit address, the exchange transfers it to its own safer addresses (cold wallets).

When it comes to withdrawing cryptocurrencies, exchanges typically group withdrawal requests from various customers into one single transaction, originating from the exchange's addresses, which are similar to bank checking accounts, and having the addresses provided by each customer in their request as destinations.

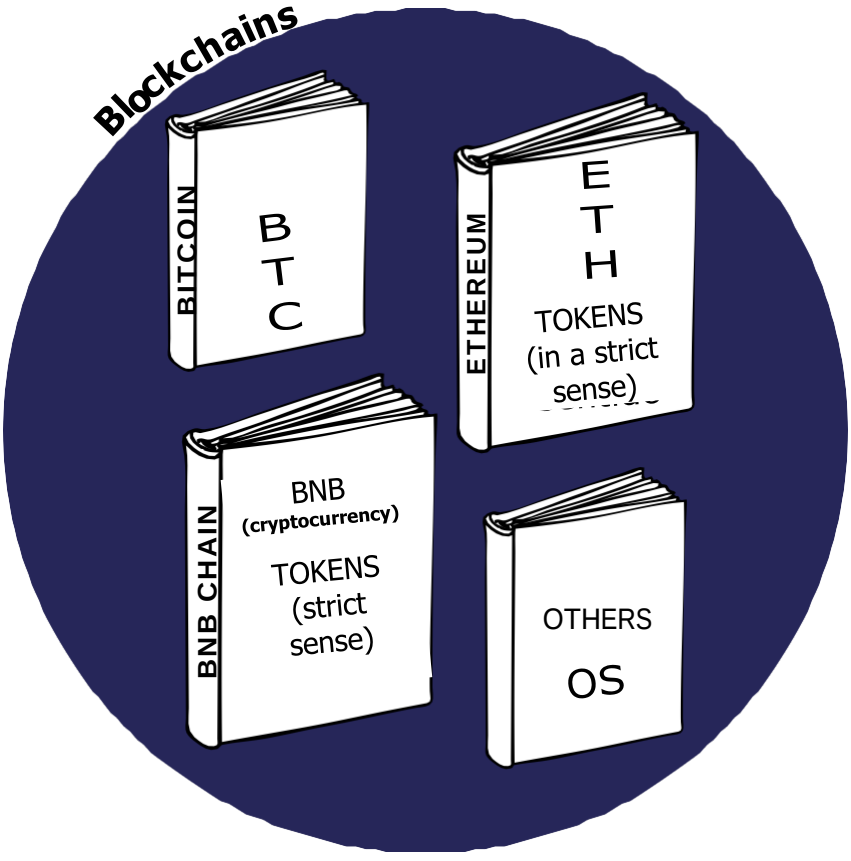
The exchange's withdrawal addresses must have enough cryptocurrencies to enable withdrawals requested by customers and must not be confused with deposit addresses. Deposit addresses are individual to each customer. Withdrawal addresses, in turn, are common.

Hence, the reason why, in order to identify which transactions were carried out by the exchange on behalf of a given customer, it is not sufficient to just look at the Blockchain. It is also necessary to access the exchange's internal transaction data and documents, a type of "ledger" for the company. For this access, the template for lifting the secrecy of specific transactions contained in the annex to this Guide (Draft for the Lifting of Telematics Secrecy of Operations with Cryptocurrencies in SIMBA) is recommended.

BEYOND BITCOIN:
PUBLIC BLOCKCHAINS AND PSEUDONYMS

In the beginning, there was only Bitcoin. A Blockchain with one single type of cryptocurrency, BTC, transactable and used as a means of payment for the use of the network. Today there are several Blockchains, maintained by different networks.

There are Blockchains that have many transactable cryptocurrencies, i.e., they can be sent and received. However, in each of them, it is possible to identify your cryptocurrency, i.e., the cryptocurrency whereby the network fees must be paid.



Blockchain	Cryptocurrency	Other cryptocurrencies	Block Explorer
Bitcoin	Bitcoin (BTC)	-	Link
Ethereum	Ether (ETH)	USDT, UNI, ICP, CRV etc	Link
BNB Chain	BNB	BUDS, CAKE, USDT[4] etc	Link

An exception worth of ledging is the Monero Blockchain, whose content is not publicly accessible. Monero (XMR) is the cryptocurrency of this Blockchain and the primary example of the so-called privacy coins".[5]

Let us return to examining Blockchains in general. Despite being public, they are pseudonyms. This means that, typically, from a simple viewing, it is not possible, as a rule, to know therein whom the individuals involved in the cryptocurrency transactions recorded are.

The identification contained in the book is not by name but by public address (something like an account number). In other words, we can easily consult all the transactions made by certain accounts, but we will not know, by simply reading the book, who the people behind them are. Verify:

4 - Homonymous cryptocurrencies can exist on more than one Blockchain. For example, USDT exists on the Ethereum Blockchain and USDT on the BNB Chain.

5- Privacy coins will not be discussed in detail in this first version of the guide.

Address

USD BTC

This address has transacted 2 times on the Bitcoin blockchain. It has received a total of 3.02625922 BTC ($58,013.78) and has sent a total of 3.02625922 BTC ($58,013.78). The current value of this address is 0.00000000 BTC ($0.00).

Address	bc1q84m06cqjj8xm77a9j72pz6245r6zzp35nu9dya
Format	BECH32 (P2WPKH)
Transactions	2
Total Received	3.02625922 BTC
Total Sent	3.02625922 BTC
Final Balance	0.00000000 BTC

Transactions

Fee 0.00037180 BTC
(165.982 sat/B - 65.343 sat/WU - 224 bytes)
(260.000 sat/vByte - 143 virtual bytes)

-3.02625922 BTC

1 Confirmations

Hash ec6fc328520989802fa264bba0f30cced23ca03ac3faf0...

2022-10-11 13:43

bc1q84m06cqjj8xm77a9j72pz6245r... 3.02625922 BTC

3KeDmvaCJeV64QCC3ynfXkzCMpS... .00201913 BTC
358JVUtKdhaTdfKRY8RaHXm4saA... .02386829 BTC

Fee 0.00036660 BTC
(165.135 sat/B - 65.348 sat/WU - 222 bytes)
(260.000 sat/vByte - 141 virtual bytes)

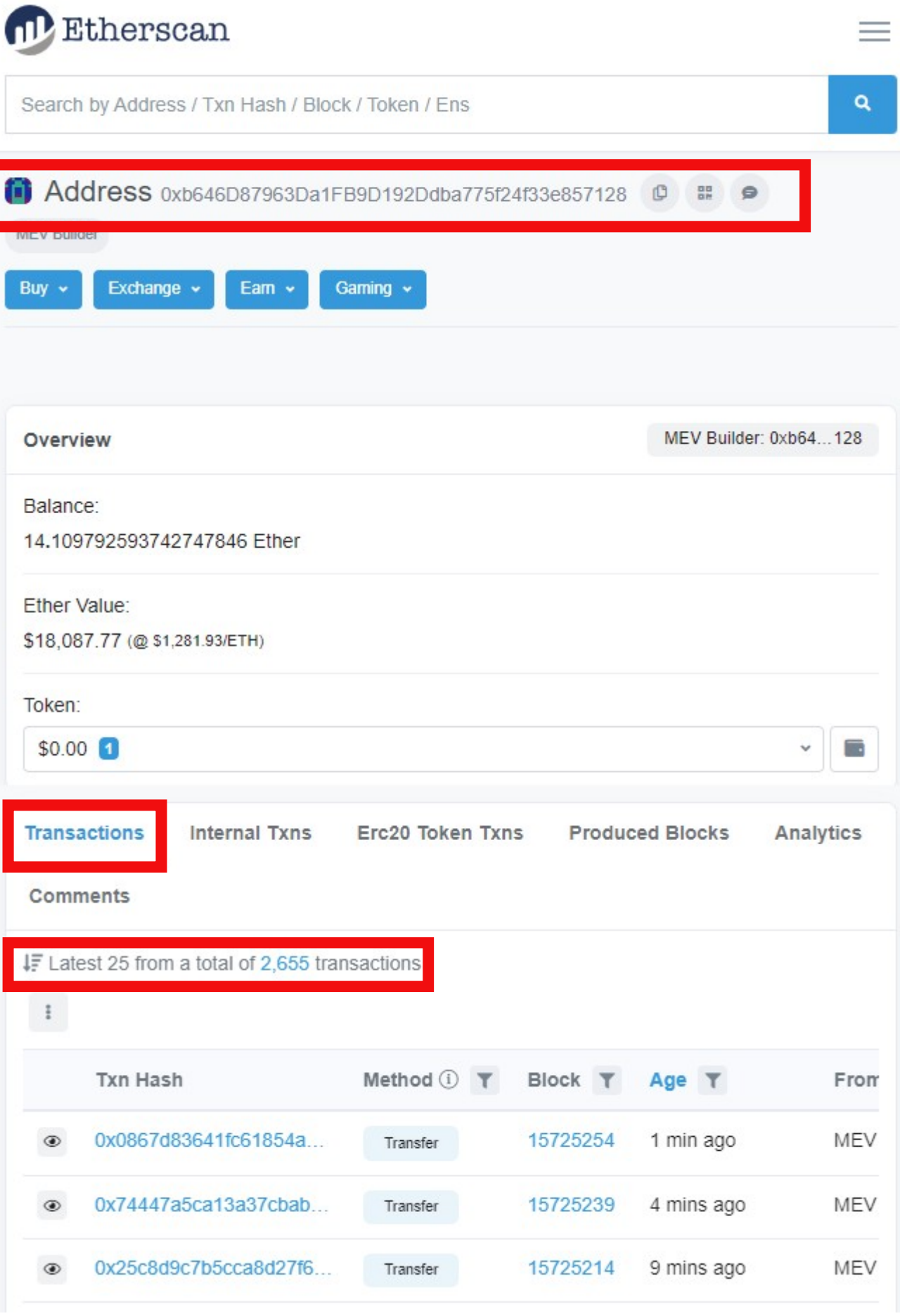
+3.02625922 BTC

Hash a045730dbc010368444ebb4df2aef11d063ee9035ffa3...

2022-10-11 13:06

bc1q5xutv5gr72t7f9cpjwea8rspx45... 3.10129645 BTC

bc1qxy08jgn8lm3kdpe2lh4zj9qgjs2... .07467063 BTC
bc1q84m06cqjj8xm77a9j72pz6245r... .02625922 BTC

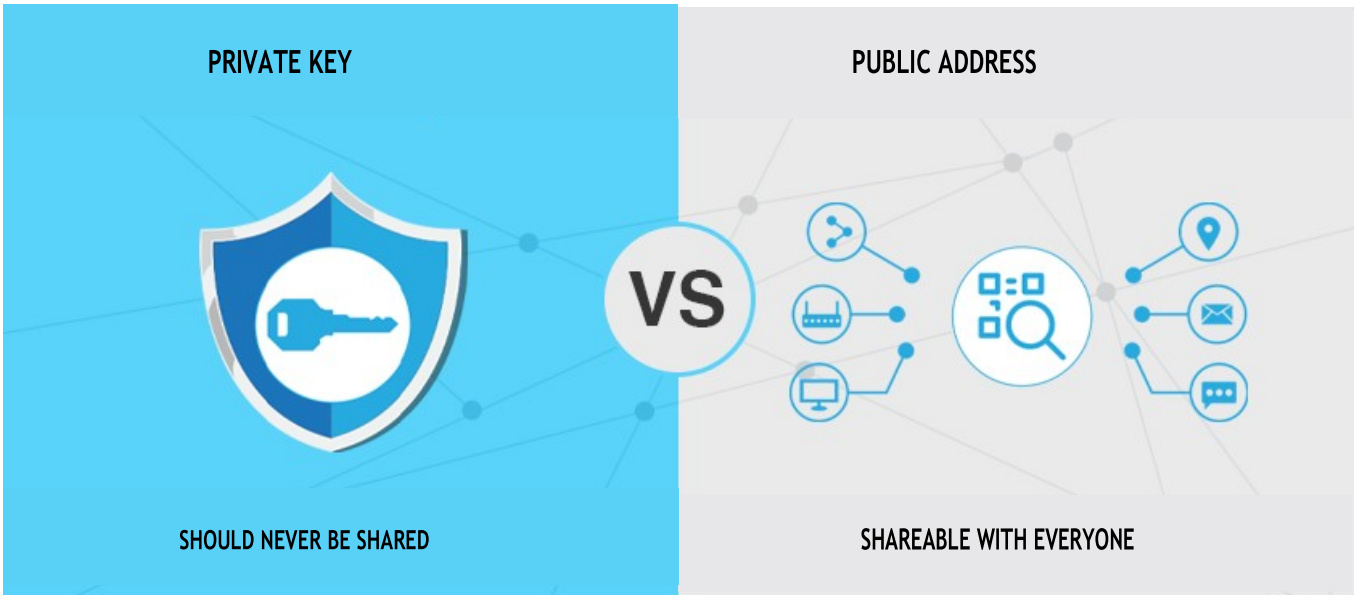

Etherscan
Search by Address / Txn Hash / Block / Token / Ens
Address 0xb646D87963Da1FB9D192Ddba775f24f33e857128
Buy
Exchange
Earn
Gaming
Overview
MEV Builder: 0xb64...128
Balance:
14.109792593742747846 Ether
Ether Value:
$18,087.77 (@ $1,281.93/ETH)
Token:
$0.00 1
Transactions
Internal Txns
Erc20 Token Txns
Produced Blocks
Analytics
Comments
Latest 25 from a total of 2,655 transactions
Txn Hash
Method
Block
Age
From
0x0867d83641fc61854a...
Transfer
15725254
1 min ago
MEV
0x74447a5ca13a37cbab...
Transfer
15725239
4 mins ago
MEV
0x25c8d9c7b5cca8d27f6...
Transfer
15725214
9 mins ago
MEV

STORAGE OF CRYPTOCURRENCIES

Storing cryptocurrencies means to possess the private key that allows you to transact them.

In order to proceed, there are two terms that must be understood: private key and public address, which form a pair, also referred to as an account. A cryptocurrency account is nothing more than this pair.

The private key and the public address maintain a one-to-one correspondence relationship. In other words: for each private key, there is a unique public address and for each public address, there is a unique private key.



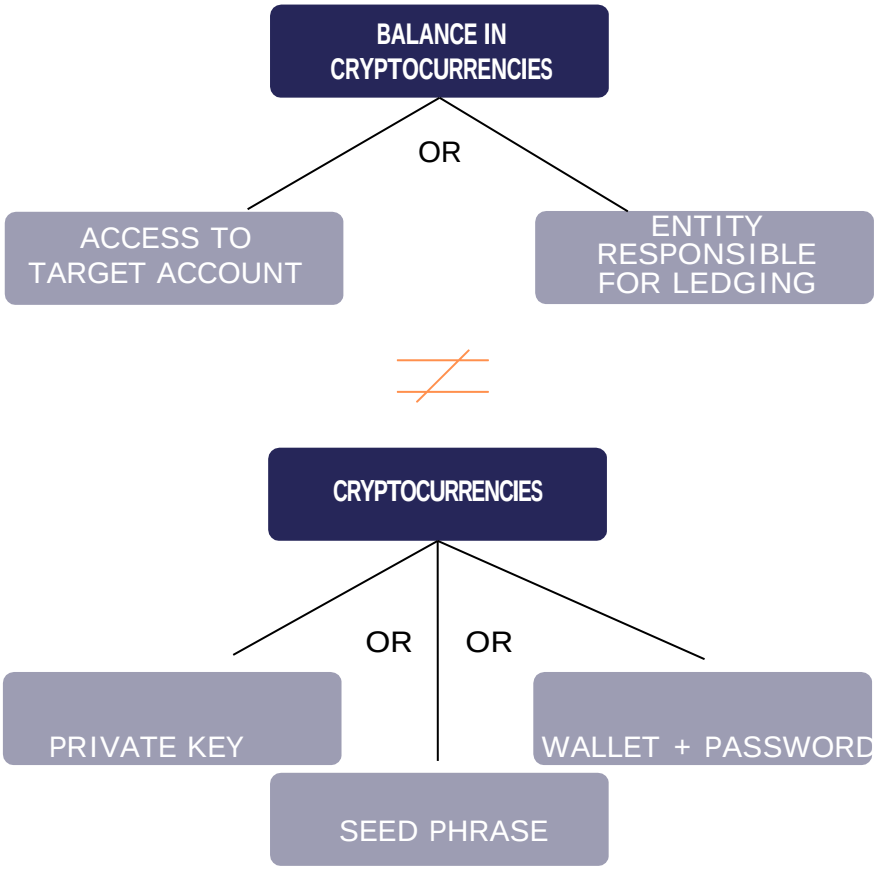
Think of the private key as the key to your house and the public address as your home address. Consider, also, that this private key has two particularities: it – and only it – opens a door that cannot be broken into and it is a key that comes with your address written on it.

This results in some consequences. Let us highlight two of them. Disclosing your public address does not pose any risk of losing your cryptocurrencies, because the door cannot be broken into (first). Nevertheless, disclosing your private key allows anyone to enter your home and steal everything of value there, because with the key you have access to the address (second).

CRYPTOCURRENCY TRANSACTION

Balances in cryptocurrencies, as they are released in centralized private ledgers, can be transacted and blocked by anyone who has access to the target's account (login + password + contingent multiple authentication factors) or, more easily, by the very exchange or company responsible for ledging.

Cryptocurrencies, on the other hand, can be transacted by anyone who has access to the private key of the respective account, the seed phrase of a wallet or the wallet itself plus the password to access it.



We have already discussed the private key in the previous topic. Now we will move on to the concepts of wallet, access password and seed phrase.

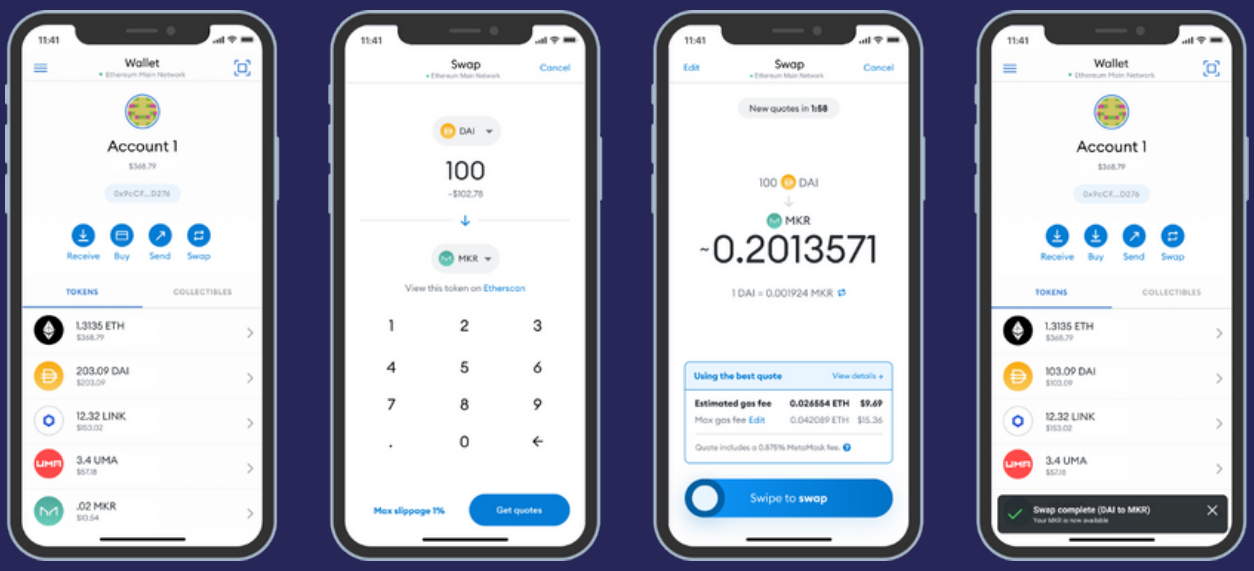
WALLETS

Cryptocurrency wallets are not like cash wallets. Money wallets store money. Cryptocurrency wallets do not store cryptocurrencies, but rather the private keys that allow them to be transacted.

Wallet, in this context, is also an ambiguous term and three meanings will matter to us:

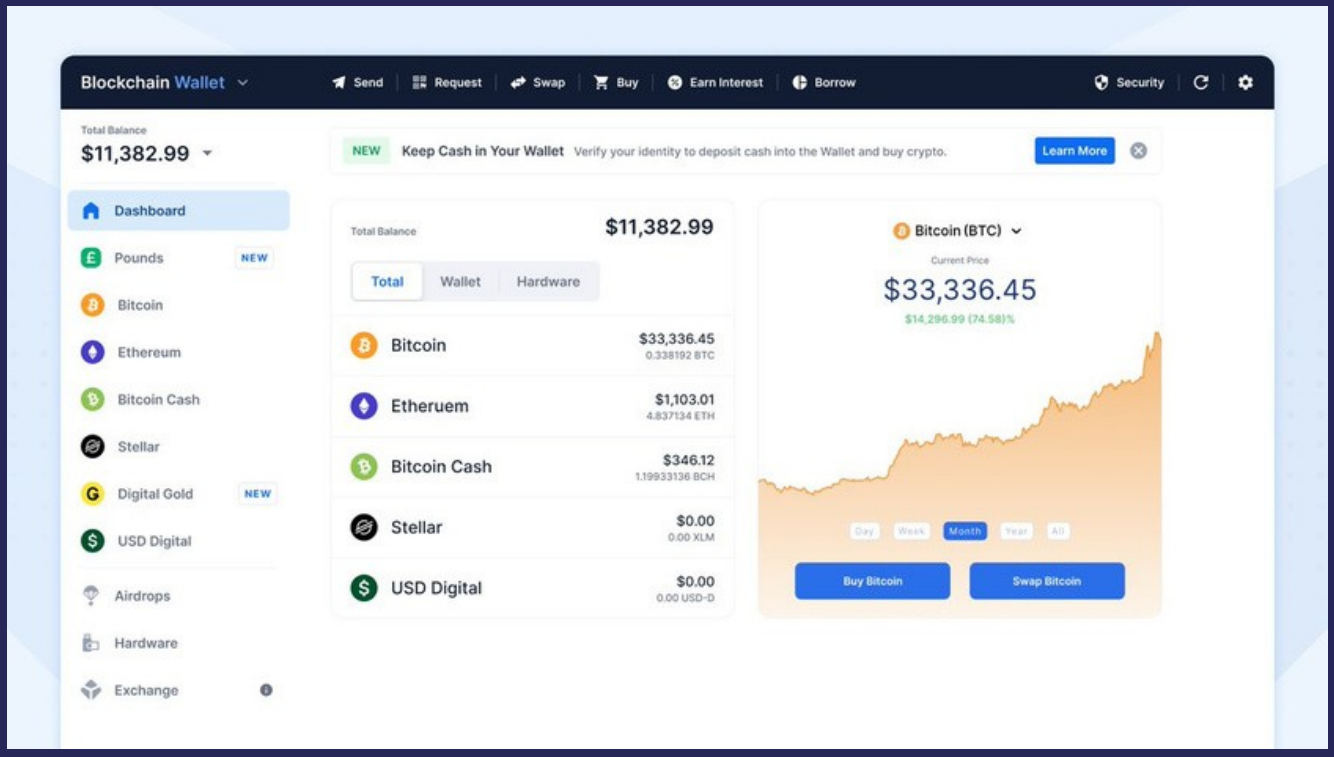
- wallet as the name given to a piece of paper (paper wallet), where the details of an account (private key and public address) are written down;
- wallet as the designation of a physical device specifically created for the custody of private keys (hardware wallet); and
- wallet as the name given to a piece of software that helps users to keep their private keys and that can be run online (webwallet), installed on the computer (desktop wallet) or on the cell phone (mobile wallet).

HARDWARE WALLET (TREZOR AND LEDGER)

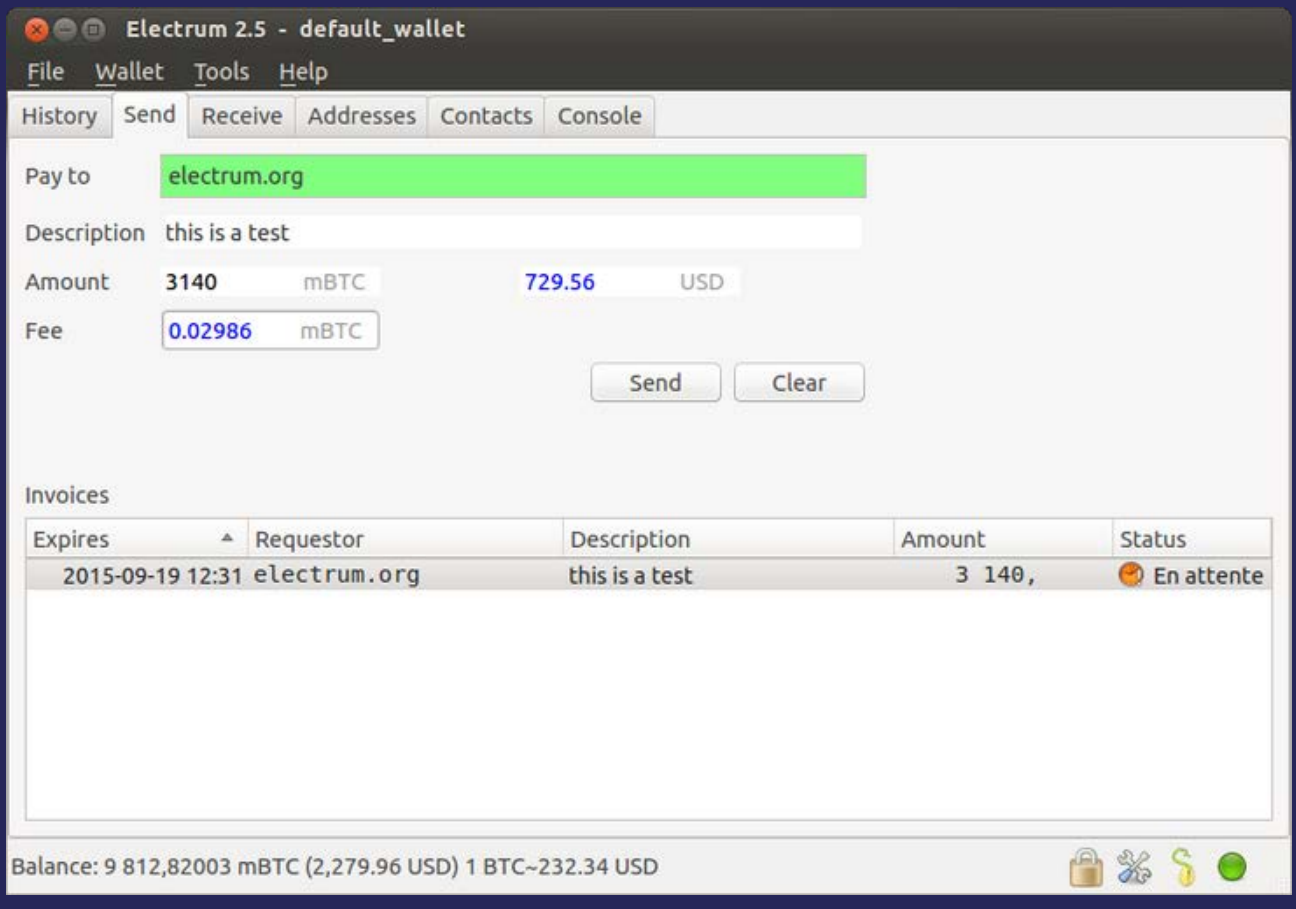


MOBILE WALLET

PAPER WALLET



WEB WALLET



DESKTOP WALLET

Paper wallets and webwallets have important contraindications. The first because they will only be safe if created and managed by someone with in-depth technical knowledge on the subject. The second because they store private keys in the cloud, increasing the risk of unauthorized access to them.

The other wallets are basically differentiated by the place where the private keys are stored. In the hardware wallet, the private keys are on a specific physical device[6]. In the desktop wallet, on the computer. And in the mobile wallet, on the cell phone.

Access password (PIN)

If your wallet were stolen, you would certainly lose the money stored there. However, if your cryptocurrency wallet or the device on which it is installed were stolen, you would not lose your cryptocurrencies unless the criminal knew your password or managed to crack it.

This is because, in order to prevent unauthorized access, cryptocurrency wallets store private keys in encrypted form. What allows them to be decrypted is the password created by the user, also known as PIN (personal identification number).

In practical terms, for the transaction of cryptocurrencies in an account:

- whoever has the decrypted private key does not need the password;

6- In proper use and operation, hardware wallets are the safest type of wallet for two reasons. Firstly, because they do not allow the keys stored there to touch any online environment. Secondly, because they require the physical pressing of a button every time the user intends to carry out a transaction.

- whoever has the encrypted private key needs the password;

- whoever has only the password has nothing.

Seed phrase

A single wallet typically comprises multiple accounts (three, eight, twenty…)[7] and with each new account used by the user, it would become more complex to make a backup of their respective private keys.

To overcome this difficulty, wallets make use of the “seed phrase”, which is presented as a random sequence of 12, 18 or 24 words, out of two thousand and forty-eight words in the English language.

If the private key is like the key to your house, think of the seed phrase as a keychain with all your keys (house key, car key, office key, etc.). In other words, the seed phrase is equivalent to all your keys, allowing whoever has it to enter all those environments and remove everything of value they find there. Technically, the seed phrase represents a master private key/ extended private key from which all others derive.

7- The possibility of new accounts being created in one single wallet is practically inexhaustible.

CRYPTOCURRENCY TRADING

The two main ways of trading cryptocurrencies are as follows:

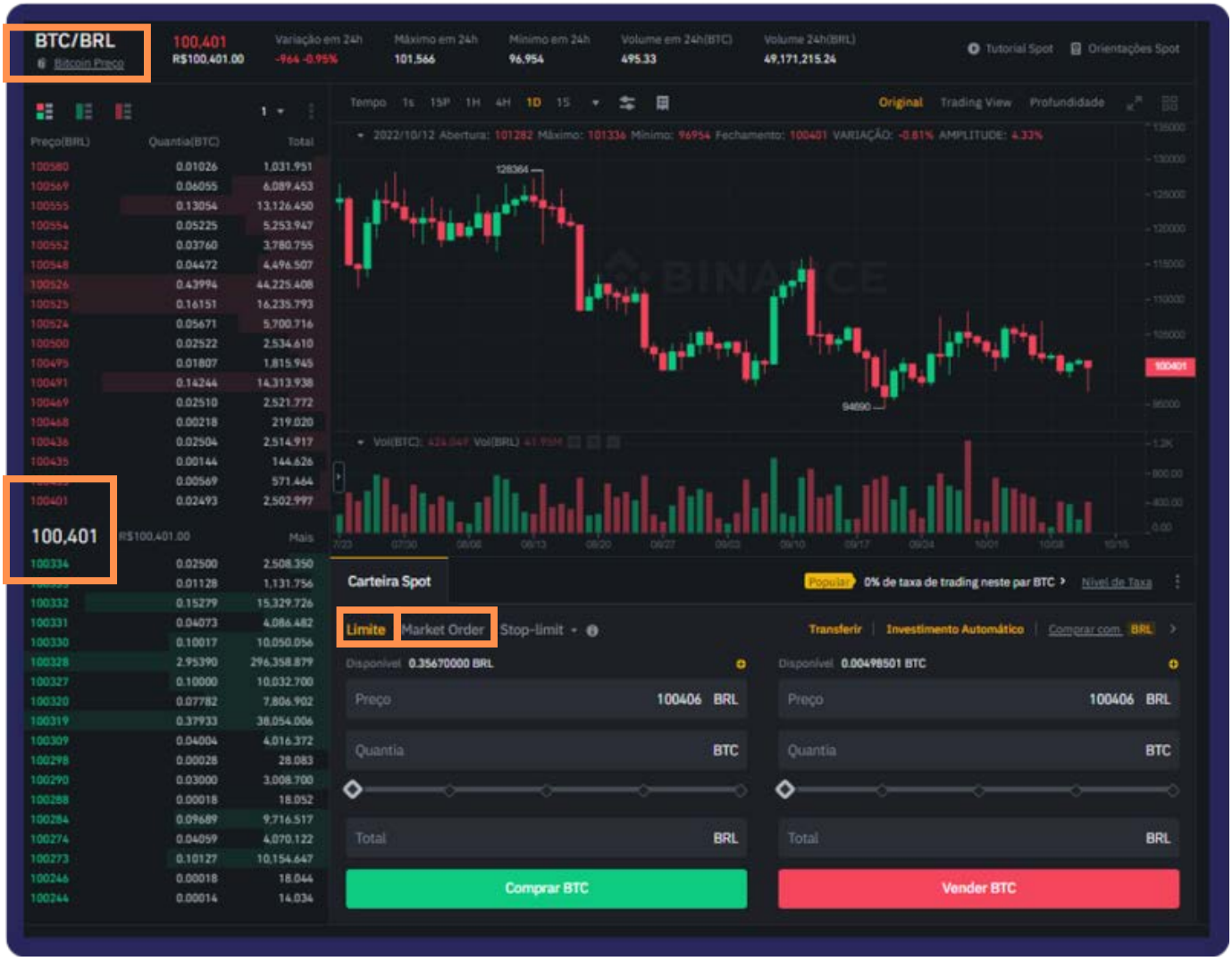
- peer to peer (P2P): non-intermediated negotiations, made directly between two wallets;

- on exchanges: intermediated negotiations, made through order books available on a centralized platform.

The first transactions are ledged on the Blockchain and are therefore called onchain. The second ones are released in the private ledger of the entity responsible for the platform, and can be called offchain.

Book is an instrument for facilitating the meeting of people with opposing interests, in other words, those who want to buy and sell a given asset. Or, more technically, of those who want to exchange A for B with those who want to exchange B or A, in any quantities.

We have reproduced below the image of a book in order to subsequently highlight certain elements within this book).



1) **Traded pair:** a book always concerns two assets. In this case, BTC and BRL, intended, therefore, to facilitate the meeting of those who want to exchange bitcoins for reais, sell, with those who want to buy bitcoins.

2) **Order:** it is the formalization of an intention.

Order types:

- purchase order or sales order;

- market order and limit order.

One example: If I want to buy bitcoin, I must formalize this intention through a purchase order. If I'm willing to pay whatever the best seller is asking for it, regardless of the price, my order will be at market;

whereas if I establish a maximum price, above which I do not wish to buy, my order will have a cap.

Market orders are executed immediately, regardless of the market price. Limit orders, on the other hand, go to the order book (sell orders in red and buy orders in green), where they wait for a market price that satisfies the established cap to be reached.

3) **Spread:** is the difference between the best sell order and the best buy order (100,401 – 100,334 = 67.00).

4) **Operation:** is the name given to the meeting of two opposing orders.

5) **Market price of an asset:** is the price corresponding to the last operation (BRL 100,401.00).

BRAZILIAN LAW ON CRYPTOCURRENCIES

Virtual Assets

At the end of 2022, the first law on the cryptocurrency market was enacted in Brazil. Law No. 14.478/22 provides guidelines to be observed in the provision of virtual asset services – the name adopted by the legislation for cryptocurrencies – and in the regulation of providers of such services.

The new Brazilian law considers a virtual asset: "the digital representation of a value that can be negotiated or transferred by electronic means and used to make payments or for the purpose of investment" (art. 3). [8]

8- The definition of virtual assets given by art. 3 of Law No. 14.478/22 is not the same as that adopted by the CVM in Guidance Opinion No. 40/22. Therein, the CVM adopted the following concept of cryptocurrencies: digitally represented assets, protected by cryptography, which can be the subject of transactions executed and stored through distributed ledger technologies (DLTs). Usually, cryptocurrencies (or their property) are represented by tokens, which are intangible digital securities. Cryptocurrencies are often referred to as tokens and can perform several functions. The CVM adopts a functional approach to classifying tokens into a taxonomy that will serve to indicate their legal treatment: Payment Token (cryptocurrency or payment token): seeks to replicate the functions of currency, notably that of a unit of account, medium of exchange and store of value; Utility Token: used to purchase or access certain products or services; and Asset-backed token: represents one or more assets, tangible or intangible. Examples include security tokens, stablecoins, non-fungible tokens (NFTs) and other assets subject to tokenization operations. Out of this classification adopted by the CVM, only items i and iii can perform "the digital representation of an amount that can be negotiated or transferred by electronic means and used to make payments or for investment purposes" (art. 3, Law No. 14.478/22). These are those tokens that can, under the new law, be considered virtual assets.

The same device determines that they are not virtual assets:

- **The national currency** (the Real, art. 1, Law No. 9.069/95[9]) and other foreign currencies, such as the euro, dollar, etc.;

- **Electronic currency**, defined in Law No. 12.865/13 as resources stored in a device or electronic system that allow the end user to carry out a payment transaction (art. 6, item VI), such as operations with credit and debit cards, prepaid cards and cell phone transactions, etc. Such transactions are intermediated by payment institutions, members of the Brazilian Payment System and the credit market of the National Financial System, supervised by BACEN and regulated by the National Monetary Council;

- Instruments that provide their holder with access to specified products or services or benefits arising from these products or services, such as **points and rewards from loyalty programs**; and

- Representations of assets whose issuance, bookkeeping, negotiation or settlement are provided for by law or regulation, such as **securities and financial assets**[10]. Said norm is complemented by the sole paragraph of art. 1 of Law No. 14.478/22, which excludes assets from the new cryptocurrency law representing securities (Law No. 6.385/76), without amending the CVM's jurisdiction.

9- It is interesting to note the shape that the Central Bank of Brazil (BACEN) has given to the **Digital Real**, a type of Central Bank Digital Currency, CBDC) which has the same backing as fiat currency, would also distance it from the concept of virtual assets discussed herein. Find out more at https://www.bcb.gov.br/estabilidadefinanceira/real_digital.

10- Financial assets constitute goods or rights that a company or person owns and that can generate income, such as shares, money, public bonds, investment funds, bank deposit certificates, etc.

Virtual Asset Service Providers

Virtual Asset Service Providers – PSAVs are legal entities that perform, on behalf of third parties, at least one of the virtual asset services (art. 5). These are companies currently called **brokers** or **exchanges**.

The following are **virtual asset services** defined in the new legislation:

- The exchange between virtual assets and national currency or foreign currency
- The exchange between one or more virtual assets;
- The transfer of virtual assets;
- The custody or administration of virtual assets or instruments that enable control over virtual assets – such as account holders' private keys; or
- Engaging in financial services and providing services related to an issuer's offering or sale of virtual assets.

Entity of the Federal Public Administration, indicated in a subsequent act of the Executive Branch, may authorize the performance of **other services** that are, directly or indirectly, related to the activity of the virtual asset service provider.

Law No. 14.478/22 subjects PSAVs to important national laws by establishing that their activity must comply with the following guidelines, specified in an act of the federal body (art. 4):

- Free enterprise and free competition;
- Good governance practices, transparency in operations and a risk-based approach. The latter opens up space for the international regulatory trend defended by the FATF/GAFI;

- Information security and protection of personal data, referring to the rules of the General Data Protection Law (Law No. 13.709/2018);

- Protection and defense of consumers and users. The norm is complemented by art. 13 of the new law, by expressly establishing that operations conducted in the virtual assets market will be subject, as applicable, to the Consumer Protection Code (Law No. 8.078/90);

- Protection of popular savings;

- Solidity and efficiency of operations; and

- Prevention of money laundering (Law No. 9.613/98) and financing of terrorism (Law No. 13.260/16) and the proliferation of weapons of mass destruction, in alignment with international standards.

Federal Regulation

It will be the responsibility of the body or entity of the Federal Public Administration, defined in a future act of the Executive Branch, to establish which financial assets will be regulated, for the purposes of Law No. 14.478/22. This same body will have the power to previously authorize PSAVs to operate in Brazil, in addition to establishing the events in which authorization may be granted in a simplified procedure. Art. 6 provides that an act of the Executive Branch will assign to one or more bodies or entities of the Federal Public Administration the discipline of the operation and supervision of the PSAVs.

Art. 8 provides that institutions authorized to operate by BACEN may exclusively provide the service of virtual assets or combine it with other activities, pursuant to the regulations to be issued by a body or entity of the federal Public Administration indicated in an act of the federal Executive Branch.

Furthermore, it is the responsibility of the regulatory body or entity indicated in an act of the Federal Executive Branch (Art. 7), to:

- Authorize operation, transfer of control, merger, spin-off and incorporation of PSAVs;

- Establish conditions for holding positions in statutory and contractual bodies in PSAVs and authorize the installation and exercise of people in management positions;

- Supervise the PSAVs and apply the provisions of Law No. 13.506/2017 (which deals with the administrative sanctioning process of BACEN and CVM), in case of non-compliance with Law No. 14.478/22 or its regulations;

- Cancel, ex officio or upon request, the authorizations of PSAVs; and
- Provide for the events whereby the virtual asset services of art. 5, will be included in the foreign exchange market or whereby they must submit to the regulation of Brazilian capital abroad and foreign capital in the country.

After its entry into force, Law No. 14.478/22 also provides for a subsequent deadline for PSAVs to adapt to the regulations. This period will be defined by the federal body to be designated, but will not be less than six months (art. 9).

Criminal Provisions and Complementary Norms

Art. 10 of Law No. 14.478/22 introduces a new form of fraud in art. 171-A into the Criminal Code: **“Fraud with the use of virtual assets, securities or financial assets”.**

Art. 171-A. Organize, manage, offer or distribute wallets or intermediate operations involving ***virtual assets, securities or any financial assets*** *in order to obtain an illicit advantage, to the detriment of others, inducing or keeping someone in error, through deceit, ruse or any other fraudulent means.*

Penalty – imprisonment, from four (4) to *eight* (8) years, and fine.

Law No. 14.478/22 also amends the sole paragraph of art. 1 of Law No. 7.492/86 to include the following:

Art. 1 For the purposes of this law, a financial institution is considered to be a legal entity governed by public or private law, whose main or accessory activity, cumulatively or not, is the raising, intermediation or application of financial resources (Vetoed) from third parties, in national or foreign currency, or the custody, issuance, distribution, negotiation, intermediation or administration of securities.

Sole Paragraph. The following is equivalent to a financial institution:

I - the legal entity that raises or manages insurance, exchange, consortium, capitalization or any type of savings, or third-party resources;

I-A – a legal entity that offers services relating to operations with virtual assets, including intermediation, negotiation or custody;

II - the natural person who carries out any of the activities referred to in this article, even if occasionally.

As a result, the PSAVs become financial institutions by equivalence and are subject to all crimes against the National Financial System - SFN of Law No. 7.492/86.

The anti-money laundering standards introduced by the new legislation will be analyzed in the following topic.

Finally, Law No. 14.478/22 amended the Anti-Money Laundering Law to include Article 12-A, which sets forth the creation of the National Register of Politically Exposed Persons (CNPEP), made available through the Transparency Portal.

As of its validity, the bodies and entities of any Powers of the Federal Government, the States, the Federal District and the Municipalities must submit to the CNPEP manager, in the form and frequency defined in regulation, updated information regarding their members or former members classified as politically exposed persons (PEPs) in current legislation and regulations. The CNPEP management body will indicate in active transparency, via the internet, bodies and entities that fail to comply with the obligation.

The aforementioned persons bound by the Anti-Laundering System will include consultation with the CNPEP among their procedures to comply with the obligations provided for in arts. 10 and 11 of the Anti-Laundering Law, without prejudice to other steps required by law. § 3

FINANCIAL INVESTIGATION OF CRIMES INVOLVING CRYPTOCURRENCIES

The use of the financial system by criminals to transfer, store or conceal the proceeds of crime challenges State investigative bodies to collect, analyze and present evidence of the financial transactions used for this purpose, as a way of strengthening and enabling criminal prosecution before the Judiciary and the recovery of the assets involved.

As an investigative method, the Financial Investigation focuses on financial matters related to illicit conduct, attempting to identify and to document, for evidentiary purposes, the transaction of money during the course of criminal activity[11]. In other words, Financial Investigation is a method that seeks to connect people to other people, places and events through financial facts[12]. This type of investigation revolves around the concept of financial data, which represents information linked to money, assets, expenses and finances, present in almost all aspects of a person's life.

This financial data has been dematerialized since the early 2010s, in the wake of the 2008 global financial crisis, following the migration of traditional financial relationships to digital means and the advent of a **cryptomarket** parallel to the national financial systems.

11-FATF, Operational Issues Financial Investigations Guidance, 2012, p. 03.

12- SLOT, Brigitte; SWART, Linette de; DELEANU, Ioana; MERKUS, Erik; LEVI, Michael; KLEEMANS, Edward. Needs assessment on tools and methods of financial investigation in the European Union: Final report. Rotterdam: ECORYS, 2015, p. 09-17.

Cryptocurrencies represent the most important facet of this immaterial money, constituted, after all, by bits in someone's computer system, bringing financial investigation closer to computer investigation and requiring important intercessions between financial secrecy and the secrecy that covers some digital traces.

As assets, the financial investigation of crimes involving cryptocurrencies is carried out through the **same asset investigation methodology** used by the Federal Prosecution Service to track other assets, as set out in the Asset Recovery and Asset Administration Guide prepared by a working group established by the 2nd and 5th Chambers of Coordination and Review.[13]

If the investigation methodology is the same, the technological tools used for asset tracing (remote search and in-person search) and the particularities involved in the seizure and administration of this type of asset required the development of a guide focused solely on cryptocurrencies.

ASSET TRACING METHODOLOGY

The term Financial Investigation is used for the complex of activities involving the collection, analysis and use of financial information by law enforcement agencies. Although this document presents a methodological suggestion for carrying out financial investigation, it seems certain that the appropriate measures for each case must be determined by the case itself. Only the latter demands the necessary measures for its own success – and this, perhaps, represents the golden rule of any investigative effort.[14]

13- BRASIL. Federal Prosecution Service. 2nd Chamber of Coordination and Review. Operational Guide – *Persecução Patrimonial e Administração de Bens*, 2017. (Asset Recovery and Asset Management, 2017) Available at: https://portal.mpf.mp.br/novaintra/areas-tematicas/camaras/criminal/publicacoes/roteiros-de-atuacao-restrito/roteiro_atuacao_persecucao_patrimonial.

14- MARTINS. Tiago Misael de Jesus. *Persecução Patrimonial por Meio de Investigação Financeira, em BRASIL*. (Asset Recovery through Financial Investigation, in BRAZIL). Federal Prosecution Service. 2nd Chamber of Coordination and Review. *Temas Processuais, Prova e Persecução Patrimonial*, 2019. (Procedural Issues, Evidence, and Asset Recovery, 2019) Available at: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea-de-artigos-temas-processuais-prova-e-persecucao-patrimonial.

In any case, financial investigators need to keep in mind that they must patiently “follow the money”; In the crimes discussed herein, if the money is not followed, the crime pays.[15]

Despite the difficulties arising from the globalized and instantaneous flow of assets in contemporary times, it must always be borne in mind that assets are the objective of the crime committed. Thus, criminals like to maintain some degree of control over their assets and, as a result, there is usually a “paper trail” that can lead the investigation back to the offender. This paper trail can also be followed to identify additional offenders and the location of evidence and instruments used to commit the crimes.[16]

Financial investigators develop hypotheses based on available information. The imagined hypothesis determines the extent and type of information required to prove its merit. Identifying the type of information needed allows the investigator to determine where this information is stored (whether in open or closed sources, for example). Once the investigator has determined what information is needed and where it is stored, he or she can anticipate the methods and challenges in obtaining the information (e.g., direct access to public databases, access upon direct request, lifting of judicial confidentiality, etc.). Thus, he or she implements a data collection plan that leads to the successful attainment of information necessary to prove the hypothesis.[17]

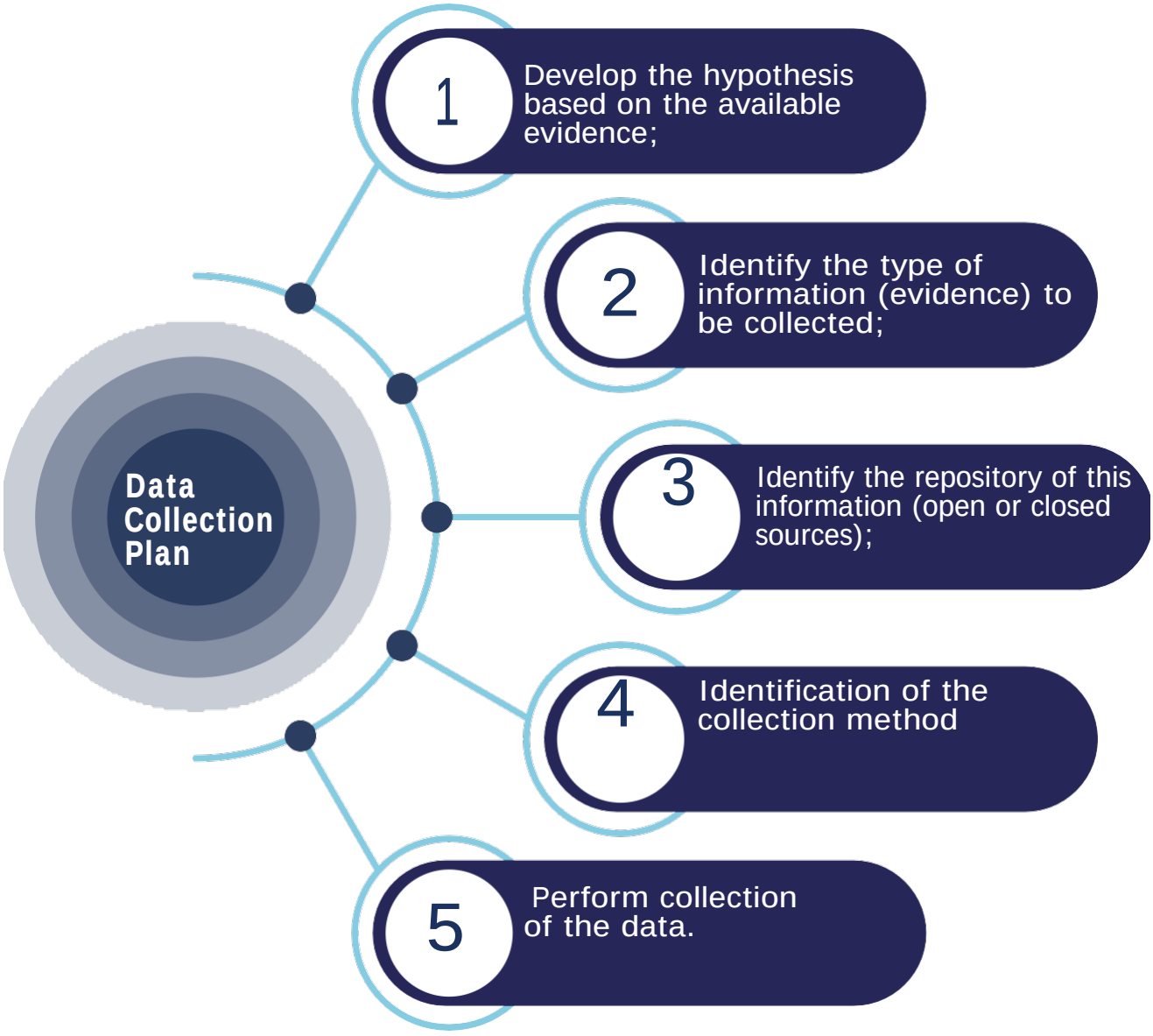
This reasoning can be showcased by the following graph:[18]

15- UNODC. Criminal Intelligence: Manual for Analysts. Vienna: UNODC, 2011, - p. 35-36.

16- FATF, idem, p. 07.

17- FATF, idem, p. 17.

18- MARTINS, idem.


Data Collection Plan
1
Develop the hypothesis based on the available evidence;
2
Identify the type of information (evidence) to be collected;
3
Identify the repository of this information (open or closed sources);
4
Identification of the collection method
5
Perform collection of the data.

The methodology for collecting financial information is based on a confidential phase, initiated to allow the adoption of information collection measures without the target's knowledge, particularly due to the real possibility of rapid dissipation of assets and destruction of evidence by modern technological means; and in an overt phase, in which this precaution is no longer necessary, v.g., because no assets were located in the confidential phase or because the assets to be discovered by measures adopted in the overt phase are expected to make up for the discarding of the surprise of the precautionary attachment measures.

At the beginning of the confidential phase, much of the data is found in open sources of information. Every investigation starts slowly and gains momentum as information and data are accumulated[19]. In order to gather this information, the researcher first makes use of the so-called open sources, consisting of all information publicly available through the internet, social media, printed and electronic media, as well as records maintained by public bodies or private bodies, but with public access[20].

It is not the intention of this work on cryptocurrencies, which only recalls methodological concepts on asset investigation, to describe open research sources, but only to present their existence and usefulness in the context of Financial Investigation. To consult open sources in Brazil and abroad, it is recommended to consult the Asset Recovery and Asset Administration Guide, chapter III, items 4 and 5.

By gathering information contained in an open source, it is possible to seek access to closed sources, understood as those to which the investigator does not have access, via direct search or request, without the need for judicial intervention. Closed sources are commonly identified as subject to legal secrecy, such as banking, tax, telephone, telematics data, etc.

19- UNODC, idem, p. 41.
20- FATF, idem, p. 18.

In the MPF, the templates adopted for access to financial and tax data are found in the drafts of the Banking Transactions Investigation System – **SIMBA**[21] and of the Tax Investigation System – **SIFISCO**[22], while the receipt of telephone data, if of interest to the investigation, can be received in the Telephone Records Investigation System – **SITTEL**[23]. In turn, the templates for requests to lift the confidentiality of telematics data are compiled on the e-Evidence portal, maintained by the Cybercrime Support Group.[24]

The presented sequence of collecting data from open sources for then to move on to closed sources was adopted for teaching purposes only. What happens in practice, in fact, is a feedback from the sources. This is because information is collected again in the open environment, as new information is brought by closed sources and vice versa.

With the collection of these sources of evidence, it may be appropriate for the case to carry out an overt phase with interrogations of the targets, their family members, formal or informal associates, search and seizure at their residence (art. 240, § 1, b and h, CPP), in their companies, offices, seizure of computers for forensic examination, seizure of accounting books for auditing, etc.

TOOLS FOR ASSET TRACING OF CRYPTOCURRENCIES

Subject to the methodology presented in the MPF's Asset Recovery Guide, the tracing of cryptocurrencies typically begins with consultation of open sources for the ledging of transactions, which are of great importance in the context of cryptocurrencies that adopt a public ledger.

21- Available at https://portal.mpf.mp.br/simba/php/Simba.php.

22- Available at https://portal.mpf.mp.br/portaldedados/.

23- Available at https://portal.mpf.mp.br/sittel/.

24- Available at https://portal.mpf.mp.br/eevidence/.

- ## Open Sources[25]

Evidently, the open sources indicated in the MPF Asset Recovery Guide continue to be important for tracing the assets of those investigated who operate with cryptocurrencies. Through research in open sources, such as social networks, important data can be obtained which, together with other evidence obtained from other open sources (general or specific to cryptocurrencies) or closed sources of evidence, prove to be useful for the investigation.

With the delimited object of this document, below is the description of specific research tools for cryptocurrencies.

- ## Open Sources Available on the Web

First and foremost, it is important that the researcher has knowledge on the **business template of the cryptocurrency** investigated, whose technical characteristics and practical limitations are of increased importance in the investigation. For each cryptocurrency, there is usually a specific website with a general description of its operation and access to the public ledger. E.g.: Ethereum (ethereum.org/pt-br/), Monero (monero.inf.br/) etc. For a broad overview of existing and continually created cryptocurrencies, you can consult, for example, the website maintained by the company CoinMarketCap (http://www.coinmarketcap.com).

One of the main open source tools used for investigations are those that exploit the public Blockchain technology underlying most cryptocurrencies. In fact, **Blockchain analysis** allows researchers to identify relationships and financial flows between wallets, with a view to researching addresses, transaction amount, submitting and receiving wallets, and other details related to a transaction. This analysis is not associated with the name of an individual, but it indicates a great level of detail concerning the

25- Contributing to the testing of open source tools on cryptocurrencies was server Adriana Shimabukuro, member of the Cryptocurrency Working Group established by SPPEA/PGR.

wallet and its operation and, sometimes, analyzing transactions can support hypotheses that recurring wallets belong to the same person being investigated[26]. Blockchain analysis, combined with other open and closed sources, almost always represents the first step in an investigation into cryptocurrencies.[27]

Websites such as **Blockchain** *(www.Blockchain.com/explorer)* allow for the searching by the number of a Bitcoin, Ethereum and Bitcoin Cash wallet[28], by showing the number of transactions linked to it, the total assets received, final balance and a complete transaction history, enabling you to trace each entry or exit of assets from the wallet. For tools with other crypto options, there are **Blockchair** *(https://blockchair.com/pt)*, **Coin Market** *(https://Blockchain.coinmarketcap.com/)*, **OXT** (*https://oxt.me/)*, **Trade Block** *(https://tradeblock.com/home)*, among others.

In addition to the transactions themselves, it may be important for an investigation to identify who was the **miner** of the Blockchain block. At present, miners are companies with large computational capacity, which sometimes represent a set of several individual miners (mining pool)[29]. As participants receive their share of the pool reward and the mined block can be identified, mining companies can cooperate with any investigations by indicating, for example, which member of the pool paid for mining a given block.

26- Blockchain analysis can be made difficult by the investigator using mixer techniques (tumbler, fogger or blender) that can be contracted as services from a third party or just with software. These techniques combine inputs and outputs from many different users to the same wallet or set of wallets, making transactions difficult to trace. When contracted to a company, fees are charged and, usually, records of contracting users are not kept. This link describes some of the most famous cryptocurrency mixing services: https://beincrypto.com/learn/best-bitcoin-mixers/. Some cryptocurrencies were designed to already contain integrated mixers, such as Dash and Monero (https://monero.inf.br/tecnologia-de-privacidade-do-monero/).

27- As they do not have completely intuitive information, the investigator needs to have knowledge of the business model of the cryptocurrency they are tracing, otherwise, they risk misinterpreting the Blockchain tracing results and missing important details related to a case.

28- In addition to operations with NFTs: https://www.Blockchain.com/pt/nfts.

29- In the context of cryptocurrency mining, a mining pool is the pooling of resources by individual miners, who share their processing power in a network, to divide the reward equally and according to the amount of work each one contributed to fixing blocks of transactions.

In most transactions, it is simple to identify the block miner as their names (or the names of pools or companies) are often “tagged” to the blocks and are already included in the tools described above for analyzing wallets.

In order to monitor wallets with the receipt of notices via e-mail, there are services provided by **Cryptocurrency Alerting** *(https://cryptocurrencyalerting.com/)*, free of charge for up to three alerts, and **Blockonomics** *(https://www.blockonomics.co/)*.

The tool Wallet Explorer (www.walletexplorer.com) provides historical information regarding other addresses held by one single virtual wallet, it links Bitcoin addresses to known entities, including exchanges, mining pools, gaming pages, wallets or darknet.[30] Discontinued in 2016, its methodology was incorporated into the commercial tool of the company Chainalysis, described below.

Wallet Explorer remains, to this day, a powerful tool, especially for those investigative bodies that do not have access to a more sophisticated commercial alternative, especially if, through the data presented by the platform, a relationship with an exchange or other entity that can be identified is identified, even if with historical data, the wallet owner.

With a similar and free-of-charge product, but limited to thirty consultations, there is the solution of the company **Crystal Explorer** *(https://explorer.crystalBlockchain.com).*

30- Wallet Explorer brings together addresses into wallets, mainly by gathering entry addresses of multiple transactions and change. After groups of a given size have been identified, it is necessary that at least one of their addresses be identified through passive or active recognition. An address identified in the group would be sufficient, primarily, to identify all remaining addresses as belonging to that group.

The website **Bitcoin Who's Who** *(www.bitcoinwhoswho.com)* provides more information about a suspicious wallet, such as whether it has been involved in cybercrime based on public information. The IP address of the transaction can be identified, although it is usually hidden by a VPN. The tool **Bitcoin Abuse** (*www.bitcoinabuse.com)* informs the user if others have reported any wallet as associated with illegal activity (ramsomware, spam, fraud, etc.). The result informs the type of illicit activity and, sometimes, the e-mail associated with such activity. With a similar proposal, there is the service **Check Bitcoin Address** *(https://checkbitcoinaddress.com/).*

Some tools allow for the graphical representation of operations with cryptocurrencies, such as **Maltego** *(https://www.maltego.com/blog/cryptocurrency-investigations-with-maltego/).*

If there is information resulting from other evidence, the MPF member can demand cryptocurrency exchanges operating in the country to inform the **registration data of the person responsible for a given wallet**, by using, for this purpose, the various legal provisions that allow this request[31].

The caveat is in those cases where the exchange accepts remote interactions, allowing a customer to create an account by uploading identification documents and, sometimes, a photograph. In these situations, it is possible for the customer to use fraudulent identification or manipulated photos in the ledging process with the exchange.

31- In this regard, for example, art. 15 of Law 12.850/13, art. 17-B of Law 9.613/98 and art. 10, § 3, of Law No. 12.965/14.

Commercial Investigation Tools

Criminals who operate with cryptocurrencies rely heavily on special software and evasive techniques to ensure anonymity and obscure ownership of the cryptocurrency wallet. This is why it is absolutely essential for investigative bodies to use software that can penetrate the countermeasures adopted by those being investigated.

The description of the potential of open-source tools mentioned above already indicates that their use in isolation does not fulfill the ultimate purpose of the investigation, which is the definition of authorship of the criminal act. In the vast majority of cases, therefore, there will be security regarding the flow of resources, but not regarding the identity of those who hold them, since the individuals who operate the wallets remain, almost always, obscured.

Open sources available on the web allow access to the ledging of transaction for most cryptocurrencies, but typically fail to determine the identity of the people behind a given wallet. In addition, linking an individual to an address or wallet is the biggest challenge in investigating cryptocurrencies. Aside from cases in which, as a result of other evidence, the investigator may demand cryptocurrency exchanges operating in the country to provide the registration data of the person responsible for a given wallet, the investigation may reach a dead end due to indeterminacy of authorship, i.e., due to the lack of knowledge of whoever operates a given wallet.

Observing this deficiency in investigations into cryptocurrencies, several companies have started to make paid technological tools available on the market that can, based on a company database, determine who is responsible (person or exchange) for the wallet being investigated.[32]

32- Typically, software suppliers are very open, approachable, and prompt when it comes to the possibility of testing their products before anyone or any entity commits to a purchase.

As a rule, commercial investigation tools are superior because they provide more detailed and faster information than tools available in open sources. Commercial investigation tools commonly allow you to obtain the following set of information and perform, at once, several important actions for analyzing financial data: a) data import and export; b) identification of a greater number of entities; c) perform groupings faster and with better interpretation; d) have a more simplified interface; e) have references to darkweb and open web addresses; f) allow specific queries to obtain technical assistance; g) have several additional features to access information more quickly.[33]

There are several solutions available on the market, such as: **Reactor** of the company Chainalysis *(https://www.chainalysis.com/chainalysis-reactor/),* **Inspector** of the company Cellebrite-Ciphertrace (https://ciphertrace.com/ and https://ciphertrace.com/financial-investigations-and-Blockchain-forensics/), **Coinbase Analytics** of Coinbase (https://www.coinbase.com/pt/analytics); **Blockchain Analytics** of Elliptic (https://www.elliptic.co/solutions/crypto-investigations); and **Crystal Blockchain Analytic** of the company Crystal Blockchain (https://crystalBlockchain.com/).[34]

33- Another functionality presented in some commercial tools is the possibility of linking Bitcoin addresses to a specific wallet based on the addresses requested by the light client, and the registration of IP addresses that can be used to identify a suspect.

34- With a GAFI alert, the use of cryptocurrency analysis tools, while useful, can also pose a challenge for investigations. As each tracing tool contains different open-source data and uses different algorithms to search the blockchain, different results can be provided to researchers by these services. Knowing the tools and their results is essential for the appropriate use of these technologies for investigative purposes. In some cases, countries using these tools have found that different cryptocurrency exchanges and/or platforms are less visible than others, which increases the difficulty of tracing asset flows. Furthermore, analysis tools currently available on the market are only compatible with a limited number of virtual assets (FATF, Guidance on Financial Investigations Involving Virtual Assets. Facing Challenges with Investigations and Confiscation, May 2019, p. 39).

A concern in the use of commercial tools is related to the ability of the investigative body to explain its findings and investigative procedures to the Judiciary Branch. That is to say, the tool needs to present clear information on how it reached a particular investigation, for example, so that the investigative body can evaluate the evidence for its relevance in court. Some tools provide experts within the tool to testify about how the Blockchain analysis was conducted.[35]

Some tools used for data extraction from seized media (e.g., smartphones and computers) can be employed to identify, among the extracted files, programs related to cryptocurrencies[36]. The MPF has access to **Cellebrite Physical Analyzer**, which reveals the existence of cryptocurrency programs. For the extraction of these files, the media should be sent to the SPPEA[37] forensic department, following the initiation of a forensic request in the Forensic System.

- **Financial Intelligence Reports**

Information on cryptocurrency operations can be obtained from the Council for Financial Activities Control – COAF through financial intelligence reports called for directly **(exchange reports**)[38] requested in the Financial Activities Control System – SisCOAF.[39]

35- FATF, Idem, p. 41/42.

36- In this regard: https://cellebrite.com/en/walkthrough-of-parsing-cryptocurrency-applications-in-cellebrite-physical-analyzer/.

37- SPPEA/PGR Service Instruction No. 41/2021 on the handling of digital evidence with visible physical support.

38- Exchange RIFs are those prepared to respond to information requests by national authorities or Financial Intelligence Units. In contrast, spontaneous (ex officio) RIFs are prepared by COAF based on the analysis of reports and complaints.

39- Available at: https://www.gov.br/coaf/pt-br/sistemas/siscoaf-2-1.

Before the entry into force of Law No. 14.478/2022, national exchanges were not classified as “obligated persons” by art. 9 of Law 9.613/1998 – Money Laundering Law. Based on a self-regulation model, some national exchanges began to voluntarily report suspicious operations occurring in their business related to money laundering and terrorist financing to COAF [40].

With the advent of the Cryptocurrency Market Law, exchanges – now named visual asset service providers, PSAVs (art. 5) – became part of the Brazilian Capital Anti-Laundering System[41]. Art. 9 of Law 9.613/1998 was amended to subject PSAVs to the obligations set forth in arts. 10 and 11 of the same law.

The obligations imposed by art. 10 are mainly related to the duty to know your customer (KYC) and the financial transactions carried out by them (KYT):

> Identify your customers and keep records updated, subject to the instructions issued by the competent authorities. In the event where the customer is a legal entity, the identification should encompass the natural persons authorized to represent it, as well as its owners (§ 1) - the idea is to prevent the use of the corporate veil of the company to conceal the ultimate beneficiary (12). The data must be retained for a minimum of five years from the closing of the account or the completion of the transaction (§ 2).
>
> Maintain a ledger of all transactions in national or foreign currency, bonds and securities, credit instruments, metals, visual

40- In this regard, the Code of Conduct and Self-Regulation for companies affiliated with ABCripto: https://www.abcripto.com.br/_files/ugd/55dd41_206786481fc84485817e8d906b54b241.pdf.

41- Two other provisions already included in the Anti-Laundering Law, which were not amended by Law No. 14.478/22, are of interest for financial investigations involving cryptocurrencies, especially at the time of the dilemma of converting cryptocurrencies into fiat currency. Firstly, art. 10-A that creates the SFN Customer Registry – CCS, through which BACEN maintains the centralized ledger of the general registry of account holders and customers of financial institutions, as well as their attorneys. Secondly, art. 11-A provides that international transfers and cash withdrawals must be previously communicated to the financial institution, under the terms, limits, deadlines and conditions established by the Central Bank of Brazil.

assets (inserted by Law No. 14.478/22), or any asset capable of being converted into money, which exceeds the limit established by the competent authority. The data must be retained for a minimum of five years from the closing of the account or the completion of the transaction (§ 2). Furthermore, the ledging of transactions will also be carried out when the natural or legal person, their related entities, have carried out, in the same calendar month, transactions with the same person, conglomerate or group that, as a whole, exceed the limit established by the competent authority (§ 3);

Adopt policies, procedures and internal controls, compatible with its size and volume of operations, in a manner regulated by the competent bodies;

Register and keep one's registration updated with the regulatory or supervisory body and, failing that, with the Council for Financial Activities Control (COAF), in the form and conditions established thereby;

Respond to requests made by COAF within the frequency, form and conditions established thereby, being responsible for preserving, pursuant to the law, the confidentiality of the information provided.

The obligations provided for in art. 11 are related to the duty to report suspicious financial transactions to the Council for Financial Activities Control (COAF):

It is imperative to acknowledge that operations that, subject to the instructions issued by the competent authorities, may constitute serious indications of money laundering. The competent authorities will prepare a list of operations that, due to their characteristics concerning the parties involved, amounts, method of execution, instruments used, or the lack of economic or legal basis, may fit the event provided for therein (§ 1).

Communicate to COAF, refraining from informing any person of such an act, including the person to whom the information refers, within 24 hours, the proposal or execution of all transactions referred to in item II of art. 10, accompanied by the identification referred to in section I of the aforementioned article; and the operations referred to in item I of art. 11;

Communicate to the regulatory or supervisory body of your activity or, failing that, to COAF, within the periodicity, form and conditions established by them, the non-occurrence of proposals, transactions or operations that may be communicated.

It is not uncommon for those being investigated to operate in exchanges based in countries that have weak controls against money laundering and terrorist financing, or even in countries that systematically refuse to cooperate, despite the formal existence of international legal cooperation tools.

In addition to the virtual service providers provided for in Law No. 14.478/2022, operations with cryptocurrencies can be reported to COAF by entities belonging to other sectors required by law, such as banking financial institutions and security brokers and distributors. In fact, traditional entities in legally obliged sectors can report two types of suspicious financial transactions: a) transactions occurring in their financial products by individuals or legal entities being investigated; and b) suspicious operations carried out by the exchanges themselves.

This is because, no matter how much they operate with cryptocurrencies, those investigated always encounter the dilemma of withdrawal (or dilemma of conversion), i.e., they need to convert the cryptocurrency into fiduciary currency[42]. When this conversion occurs in national financial institutions, it is possible that these operations have been communicated to COAF.

Any financial intelligence reports can be analyzed by using the RIF Analysis tool, based on files of the type .CSV forwarded by COAF as an annex to the reports.[43]

With the transnationality inherent to cryptocurrency operations, it is often necessary to seek data from financial intelligence units abroad. To this end, COAF mediates requests to **Egmont Group**. Additional guidance can be found in the following video produced by COAF, *Inteligência Financeira: Aspectos Práticos do Intercâmbio Internacional via Rede Egmont* (Financial Intelligence: Practical Aspects of International Exchange via the Egmont Network)*: https://youtu.be/i5N_LqLmewI.* [44]

42- Because the purpose of an investigation is to gather evidence to prove that a cryptocurrency crime has occurred, investigators may attempt to follow the money until they identify a known cryptocurrency service provider, such as an exchange or payment processor. The critical focal point in a cryptocurrency-related investigation is often to identify the point at which the cryptocurrency is exchanged for fiat currency or another type of cryptocurrency (*FATF, Orientação sobre Investigações Financeiras Envolvendo Ativos Virtuais. Enfrentando Desafios com Investigações e Confisco* (FATF, Guidance on Financial Investigations Involving Virtual Assets. Facing Challenges with Investigations and Confiscation), May 2019, p. 48).

43- The operationalization handbook for RIF Analysis (Information 022/2020-SPPEA/PGR, PGR-00197821/2020) can be requested from SPPEA via e-mail pgr-atendimento-sppea@mpf.mp.br.

44- COAF indicates that for the exchange of information that requires information via the Egmont Network, in addition to the information and documents inserted for national exchange, include the following mandatory requirements in the "Details" field of the Electronic Information System (SEI-C): 1- Description of targets with respective identifying elements. In the event of research on a foreign individual or legal entity, the identification can be made in the text itself, without the need to list the name in the "Main Related Individuals". In this case, include all available information, such as nationality and date of birth for Natural Person - PF and address and registration number for Legal Entity - PJ. 2- Relationship of targets/facts investigated with the requested country. It is important to demonstrate the relationship between the target or fact investigated and the country being consulted. Generic requests, without such binding, will not be submitted. 3- Summary of facts/people investigated. The summary must include at least information on the crime investigated and the modus operandi. If there is more than one target listed, it is important to describe the suspicion regarding each of them (even if it is only a family relationship). 4- Description of the information you want to obtain in the requested country. Specifically, register what is expected from the exchange (e.g. information on any suspicious operations, commercial information, data on the ultimate payee of a company, etc.). If the request is directed to more than one country, please, describe separately what you want from each of them. If the request concerns specific suspicious financial transactions, please, also include available information regarding the foreign financial institution, such as the bank name, account number and branch number.

Closed Sources

Closed sources are understood to be those for which access requires prior judicial authorization (reservation of jurisdiction). This field includes financial, tax, telematics data, etc.

In the cryptomarket, data arising from the lifting of telematics secrecy (a major source of evidence), associated with requests for lifting of fiscal secrecy from the RFB and exchange operations (SIMBA draft templates) may be of interest for the investigation.

- **Lifting of Financial and Tax Secrecy of Cryptocurrency Operations via SIMBA**

Currently, in SIMBA there is the possibility of accessing financial data from all financial markets (credit, exchange, securities, private insurance and pensions, and closed pensions), new payment arrangements (such as PIX and payment initiators), computer systems of special interest to financial investigation, fiscal and telematics data closely intersecting with financial transactions, and operations with cryptocurrencies.[45]

Specifically with respect to transactions involving cryptocurrencies of a civilly identified investigator (name, Individual Taxpayer Identity - CPF or National Roll of Juridical Persons - CNPJ, for example), they can be achieved by requesting data transmitted by exchanges to the Brazilian Federal Revenue Service or, if the MPF knows the exchange involved in the transaction, by obtaining data on transactions intermediated by these electronic platforms (exchanges) and in their internal systems.[46]

45- Available at https://portal.mpf.mp.br/simba/php/Simba.php.

46- As explained above, exchanges have transaction data and documents in a type of company “ledger”.

In the first scenario, this is about a request to lift the tax secrecy of the person being investigated, addressed to the Brazilian Federal Revenue Service. Cryptocurrency exchanges with tax domicile in Brazil are obliged to inform the Brazilian Federal Revenue Service - RFB, on a monthly basis, of the operations carried out by their customers within the platform, whatever the amounts operated might be (IN RFB 1888/2019, art. 6)[47].

The taxpayer (natural person or legal entity) domiciled in Brazil, in turn, has three tax obligations involving cryptocurrencies: a) reporting the operations to the RFB, when, in the previous month, the sum of operations carried out outside national exchanges exceeded BRL 30,000.00 (RFB Normative Instruction 1888/2019, art. 6, §1); b) collecting tax on capital gains, when, in the previous month, a profit was made and the sum of cryptocurrency sales exceeded BRL 35,000.00 (Federal Internal Revenue Department - SRF Normative Instruction 599/2005, art. 1, II and Law 8.981/95, art 21); and c) completing the Income Tax Statement. In the case of the Individual Income Tax - IRPF, cryptocurrencies must be entered in the assets and rights form (codes 81, 82 and 89) and income from cryptocurrencies must be entered in "non-taxable income" or "income subject to exclusive taxation".

At the end of this Operational Guide, there is a draft of the lifting of tax secrecy for operations with cryptocurrencies in SIMBA.

On the other hand, if the MPF knows the exchange involved in the transaction[48], the former may request the lifting of telematics secrecy for operations mediated by these electronic platforms (exchanges) and in their internal systems. This relationship between the investigated individual and exchanges may arise from other evidence, such as, for example, the identification of wallets in the analysis of telematics data obtained in court.

47- For the RFB, cryptocurrency is considered as "the digital representation of value denominated in its own unit of account, whose price can be expressed in local or foreign sovereign currency, electronically transacted using cryptography and distributed ledger technologies, which can be used as an investment, a means of transferring amounts, or access to services, and does not constitute legal tender." (art. 5). Likewise, the RFB considers a cryptocurrency exchange to be "a legal entity, even if not financial, that offers services relating to operations carried out with cryptocurrencies, including intermediation, negotiation or custody, and that can accept any means of payment, including other cryptocurrencies". Included in the concept of intermediation of operations carried out with cryptocurrencies is the provision of environments for carrying out cryptocurrency purchase and sale operations carried out between the users of their services.

48- SPPEA (Expertise, Research and Analysis Unit) has a compiled list of cryptocurrency brokers operating in Brazil.

At the end of this Operational Guide, there is a draft for the lifting of telematics confidentiality of cryptocurrency operations using SIMBA and having a specific exchange as the recipient of the order.

Following Guidance Opinion No. 40/2022, the Brazilian Securities and Exchange Commission has consolidated the understanding that some cryptocurrency operations can be classified as securities. Thus, even though cryptocurrencies are not expressly included among the securities mentioned in the sections of art. 2 of Law No. 6.385/76, market agents must analyze the characteristics of each cryptocurrency in order to determine whether it is a security, which occurs when it: is the digital representation of one of the securities specifically provided for in items I to VIII of art. 2 of Law No. 6.385/76 and/or provided for in Law No. 14.430/2022 (i.e., certificates of receivables in general); or falls within the open concept of security in section IX of art. 2 of Law No. 6.385/76, to the extent that it is a collective investment contract.

For these cases, both the simplified draft and the full draft of SIMBA[49] cover this financial product, by requesting access to data on securities transactions carried out through securities brokerage companies (CTVM) and securities distribution companies (DTVM) that are members of the National Financial System Customer Register - CCS.

With the norms of Law No. 14.478/22, it will be incumbent upon the body or entity of the federal Public Administration, defined in an act of the Executive Branch, to establish which financial assets will be regulated, and it is possible that future regulations will establish new possibilities of access to confidential financial data from operations with cryptocurrencies.

49- For guidance on using SIMBA, please, refer to the booklet available at: https://portal.mpf.mp.br/novaintra/informa/2022/documentos/SIMBACartilhaparaMembros.pdf.

Since transactions with cryptocurrencies are financial operations carried out on electronic platforms, it seems natural that some of the associated telematics data may be sued in court, notably the internet protocol address (IP address) of access to the cryptocurrency broker's application provider; and access records to the internet application maintained by the broker.[50]

In the event of unjustified non-compliance with the court order to hand over transaction data or suspicion regarding the fairness of the exchange's operations, it opens up the possibility of a search and seizure of the exchange's servers to be carried out so that forensic analyzes capable of recovering the data necessary for the investigation or document whether the data is effectively irretrievable or whether it has been deleted. Such an approach, naturally, cannot be applied to services in place on the darknet, where the location of the infrastructure is unknown, or in countries that have a history of refusing international legal cooperation.

An additional problem also exists when it comes to decentralized exchanges. Even today, most exchanges are centralized and store user information on a centralized server. However, since 2012, the cryptocurrency community has been developing decentralized exchange models whereby trading can occur without users having to send their cryptocurrencies to a centralized body and all transactions would become P2P transactions, i.e., between individuals.

50- The migration of financial transactions to digital media meant that various telematics data were associated with financial information. Said telematics data, collected by financial institutions, may be of interest for financial investigation, and may be accessed by judicial authorization. As an example, the following are **telematics data** accessible by court order: a) the internet protocol address (IP address) of access to the financial institution's application provider; b) access records to the internet application maintained by the financial institution, comprising the set of information relating to the date and time of use of the financial institution's internet application from the IP addresses related to the one investigated and reported in the item above; c) the e-mail registered by the user to access the digital financial service; d) the registered terminal (telephone device, computer, etc.); e) type and version of the application used; f) credit card data associated with the digital financial service (holder's name, CPF, telephone number, address, card number, declared income and spending profile); g) photographs and filming of the indicated operations, if they were carried out at automated teller machines (ATM). It is important, in order to rationalize the judicial request, that the MPF points out the transactions in which the provision of linked telematics data is sought, otherwise the response from the financial institution will be significantly delayed. The draft court order for these operations is included in SIMBA.

RFB Normative Instruction 1888/2019 provides a definition of this type of entity in art. 5, sole paragraph, by determining that the concept of intermediation of operations carried out with cryptocurrencies includes the provision of environments for carrying out cryptocurrency purchase and sale operations carried out between the users of their services. Law No. 14.478/22 also considers a virtual asset service provider to be a legal entity that performs, on behalf of third parties, among others, participation in financial services and the provision of services related to the offer by an issuer or sale of virtual assets (art. 5, section V).

One can imagine that decentralized exchanges, with infrastructure distributed across many jurisdictions around the world and no central body overseeing transactions, will make it difficult, for example, to obtain specific information on transactions.[51]

Lifting of Telematics Secrecy

-

In an investigation into cryptocurrencies, there may be a need to formulate requests for the preservation of telematics data and lifting of confidentiality of telematics data other than those associated with financial transactions already included in the SIMBA draft. To this end, the guidelines are compiled on the e-Evidence portal, maintained by the Cyber Crime Support Group, in objective tracks: *HTTPS://PORTAL.MPF.MP.BR/EEVIDENCE*

Reasonable Diligence with Found Seeds and Private Keys

-

As seen previously, access to seeds and private keys gives access to the operation of cryptocurrencies. Unlike traditional investigation, where the amounts are held in centralized financial institutions, here anyone who has access to this information can operate the asset.

51 - FATF, Guidance on Financial Investigations Involving Virtual Assets. Facing Challenges with Investigations and Confiscation, May 2019.

During the criminal investigation, based on the lifting of confidentiality measures described above, it is possible that we will come across seeds, passphrases, private keys and passwords (access keys) even before the initiation of an overt measure. It is common for investigators to store such information in the cloud, which is therefore accessible through a simple telematics lifting.

If access keys are discovered during the covert phase of the investigation, it is important to consider the need to immediately seize the cryptocurrency assets with the possibility of waiting for a more suitable time to launch the police operation.

In these situations, it seems to us that the most appropriate approach is to record everything that is found, in detail, and bring it to the attention of the competent court immediately so that an assessment of convenience/opportunity can be made, by classifying the document with the maximum degree of secrecy.

In fact, such an analysis is fundamental, as investigations may be ongoing and the immediate seizure of assets may alert the targets to the existence of precautionary measures, frustrating other measures.

SEARCH AND SEIZURE OF CRYPTOCURRENCIES

The keys for accessing cryptocurrencies can be stored on a variety of physical electronic devices, such as hardwallets, computers and cell phones, or even printed or written down on paper. Thus, search and seizure diligence can bring very fruitful results in investigations involving cryptocurrencies.

For the investigation to be successful, however, a prior preparation phase and the adoption of certain precautions during the searches are essential, in order to ensure that the cryptocurrencies found can effectively be seized by the State.

PREPARATION FOR THE IN-PERSON SEARCH

In the case of an investigation where there is a suspicion of the use of cryptocurrencies, it is essential that the representative of the Federal Prosecution Service and the Federal Police arrange for the creation of a wallet controlled by the State so that the cryptocurrencies found at the time of the in-person search can be immediately transferred to state custody.

It is impossible to specify which types of cryptocurrencies will actually be found in the searches, but through the remote investigations discussed in a previous topic, it is possible to predict the types of cryptocurrencies usually used by the person being investigated.

In any case, it is suggested that at least Bitcoin and Ethereum addresses be created in advance.

These addresses can be opened in the form of a national exchange account, with judicial authorization, or they can be addresses of their own wallets, preferably hardwallets, whose private keys/seed phrase be in the custody of public agents.[52]

In the latter case, it is essential that those involved in carrying out the search and seizure measure be aware of the risk of potential leakage or improper sharing of private keys or the seed phrase for wallets under the responsibility of the State, as anyone with access to those keys will be able to freely operate the seized cryptocurrencies to any other address. Even worse: protected by Blockchain pseudonymity.

Once a mechanism has been established for the custody of cryptocurrencies that may be seized, it is essential that a person or team (focal point) be designated to be on standby remotely, during the investigations, with access to a computer, internet, state-owned wallet address and some software that allows for remote recovery of cryptocurrency wallets, such as Coinomi[53]. This person or team will be responsible for carrying out the immediate transfer of cryptocurrencies found with the investigation to the state-owned wallet.

This measure is essential for the success of the due diligence, given the possibility of remote operation of cryptocurrencies by any other person who holds a copy of the private keys, which are nothing more than a code.

52- Although there is discussion in the Council of Federal Justice (CJF) regarding the seizure of virtual assets, there is still no regulation that governs their custody. In the CJF regulation project, there is a provision for courts to accredit exchanges, "which will be responsible for creating, upon judicial determination, a wallet to temporarily store virtual assets in investigation processes and procedures". Technically speaking, this is one of the possible solutions, the other being for a public agent or (a group of public agents) to take custody of said assets, as indicated in the previous topic. What seems beyond doubt to us is the fact that its custody should not be the responsibility of the MPF, which does not have the role of being a judicial custodian.

53- https://www.coinomi.com/downloads/

ENFORCEMENT OF IN-PERSON SEARCH

During search and seizure efforts, it is essential that teams be attentive to notes, printed or handwritten, that can characterize seed phrases, sets of 12 to 24 words, or combinations of addresses and private keys to cryptocurrencies, in addition to physical devices (hardwallets) that store private keys.

As highlighted in the initial part of this operational guide, the mere seizure of electronic private key storage devices (hardwallets) does not guarantee the seizure of cryptocurrencies. In order for this to happen, it is necessary to access the private keys and/or the seed phrase.

Thus, even if a seed is found in the home of a target, who has been arrested in an operation, an accomplice who was not affected by the precautionary measure can freely operate the assets, if they are in possession of the same key words. Taking extra care with seed phrases and private keys is recommended, which should not be shared, since, as already warned, anyone in possession of this information will be able to operate the cryptocurrencies.

Example: Search and seizure carried out at 6am with the seizure of access keys. In ideal circumstances, by 6:30 am these resources must have already been transferred to public keys held by the authorities. In other words, before the precautionary measure has been publicized to the target's associates or in the press. If this is not done, an accomplice can, from anywhere in the world, recover the assets and transfer them to addresses that cannot be blocked.

It is essential, therefore, that the recovery of the access keys be followed by the transfer of funds to a wallet held by the authorities or

to the account of a national exchange, in compliance with what has been authorized by the Court.

In the same way as the seizure of traditional assets, the measure must be carried out by the Federal Police, in a documented basis, in order to preserve the chain of custody of evidence and the tracing of assets. It is also important to certify in detail in the due diligence report everything that was carried out on site and the people present.

Another point to be considered very carefully is the compartmentalization of information regarding access keys. As access to such data allows control of assets, it is essential that as few people as possible (both within the Prosecution Service, the Police and the Judiciary) have access to such information.

Finally, considering that private cryptocurrency keys can be stored on computers and cell phones, it is recommended to request priority from the Federal Police forensics sector for the extraction and mirroring of the seized electronic items, so that it is possible to analyze the material with the search for possible passwords and private keys.

SEIZURE AND UNAVAILABILITY OF CRYPTOCURRENCIES

The cases of civil and criminal seizure and unavailability of assets, along with their respective admissibility criteria, were outlined in the Asset Recovery and Management Guide, specifically in chapters V and VI, prepared by a working group appointed by the 2nd and 5th Chambers of Coordination and Review. [54] Such coercive measures constitute powerful tools for combating economic delinquency, with effectiveness that is sometimes greater than traditional custodial sentences.

The specific case will determine which type of asset-restricting measure is applicable and its corresponding legal rationale. Attention should also be paid to the hypotheses of early disposal and to the best practices for asset management, particularly concerning cryptocurrency, as addressed in this handbook.

According to the type of seizure and unavailability adopted, the member of the MPF must request in court the attachment of the defendants' assets, by issuing a writ of attachment of **cryptocurrencies**, **electronic currencies** or **other amounts in any capacity under custody**, including **freezing of any withdrawal orders in legal tender or cryptocurrencies**, up to the determined amount, possibly existing on the nominated exchanges.

54- BRASIL. Federal Prosecution Service. 2nd Chamber of Coordination and Review. Operational Guide – *Persecução Patrimonial e Administração de Bens*, 2017. (Asset Recovery and Asset Management, 2017) Available at: https://portal.mpf.mp.br/novaintra/areas-tematicas/camaras/criminal/publicacoes/roteiros-de-atuacao-restrito/roteiro_atuacao_persecucao_patrimonial.

In addition, it is important to request that the judge adopt some measures to enforce the court order. The first requirement is that the seizure warrant specifies that the MPF and the Federal Police may enforce seizure orders directly by contacting the cryptocurrency exchanges or, if not complied with, by inspecting the companies' headquarters in search of assets. The measure is justified to speed up compliance with the order, if the Judiciary has difficulty implementing it. Secondly, that the exchanges receiving the order transfer the amounts to the wallet previously created and under the control of the State, as discussed in the previous topic of this handbook.

Finally, it should be noted that the seizure does not always need to concern only the defendant's cryptocurrencies, and it is even prudent to carry out the attachment, the accumulation of traditional asset seizure requests[55] with the special requests for the seizure of cryptocurrencies mentioned above.

55- Such as online attachment, provided for in art. 854 of the Code of Civil Procedure and implemented by the Asset Search System of the Judiciary – SISBAJUD; the freezing via RENAJUD of all vehicles registered in the name of the defendants; the freezing of vessels and aircraft contingently registered in the name of the defendants, with the issuance of an official letter to the Port Authority and the National Civil Aviation Agency of Brazil - ANAC to implement the measure; the freezing of real estate registered in the name of the defendants, inserting the attachment order in the CNIB – National Center for Unavailability of Assets.

DISPOSAL OF CRYPTOCURRENCIES

Once the seizure and transfer of cryptocurrencies has been carried out, questions arise regarding the timing of their disposal, particularly whether an early disposal should be carried out or whether it is appropriate to wait for the outcome of the criminal action to convert the cryptocurrencies into fiat currency.

The practical effects of this discussion refer to the great volatility of the price of cryptocurrencies. In a short space of time, sometimes even in a matter of seconds, the price of a given cryptocurrency can undergo severe fluctuations. As an illustration, refer to the change in Bitcoin values in the period from JAN/01/2021 to DEC/31/2022[56] (the values referenced in the left column are in dollars):

56- https://coinmarketcap.com/currencies/bitcoin/?period=7d

According to the graph above, taken from the website Coinmarketcap.com, the lowest price of Bitcoin in 2021 occurred on July 20, when it was traded at $29,807.35[57], and on November 8th the maximum price of $67,566.83 was reached. Thus, there was an appreciation of 226.67% from the lowest to the highest quotation price in 2021, within a period of less than 4 months. However, the last 45 days of the year showed a sharp decline in the price of Bitcoin, which closed the year at $46,306.45.

The high volatility of Bitcoin, which is even more pronounced in other cryptocurrencies, is one of the indicators of its widespread use for speculative purposes. In practice, this situation can lead to significant differences in values when comparing the date of seizure and the date of actual conversion into sovereign currency, which may result in appreciation or depreciation.

It is worth mentioning the existence of stable coins, a type of cryptocurrency that, in theory, is not subject to volatility. Stable coins are cryptocurrencies that link their value to a sovereign currency, issued by the State, typically the dollar. Examples are Tether (USDT), Gemini Dollar (GUSD), Dai (DAI), USD Coin (USDC), Binance USD (BUSD) and True USD (TUSD), cryptocurrencies that pair their value to the dollar, so that a unit of each of these cryptocurrencies is worth 1 dollar. To achieve this parity, there are different techniques, such as the issuance of cryptocurrencies linked to the deposit of sovereign currency, the programming of smart contracts and algorithms that control the purchase and sale of assets[58].

Stable coins have received special attention from authorities, especially state financial market regulatory bodies. In the US, Tether was fined $42.5 million by the Commodity Future Tradings Commission (CTFC), a national administrative body, due to fraud involving its issuance guarantees[59].

57- All values are denominated in U.S. dollars.

58- Additional information can be found at https://www.gemini.com/cryptopedia/what-arestablecoins-how-do-they-work

59- https://www.cftc.gov/PressRoom/PressReleases/8450-21

As previously indicated, the timing of the disposal must be decided between keeping the cryptocurrencies in custody during the process or carrying out their early disposal. In the first situation, only at the end of the criminal action, with the definitive confirmation of the criminal sentence, would its judicial disposal be determined, with the consequent conversion into sovereign currency, based on the exchange rate on the respective date. On the other hand, with early disposal there would be conversion into fiat currency during the process, pursuant to art. 144-A, of the Code of Criminal Procedure.

In search of a solution to define the moment of disposal, the Code of Criminal Procedure, in its art. 144-A, head provision, final part, as worded by Law No. 12.694/2012, authorizes early disposal whenever there is difficulty in maintaining the seized assets:

> *"Art. 144-A: The judge shall order the early disposal for the preservation of the value of the assets whenever they are subject to any degree of deterioration or depreciation, or when there is difficulty in maintaining them" – emphasis added.*

As seen in the topic itself, the seizure and custody of cryptocurrencies require specific preparation and care to avoid frustrating due diligence. Given the digital, cross-border, decentralized nature and irreversibility of operations involving cryptocurrencies, special measures are essential to ensure effective control of the values represented therein.

Whether the cryptocurrencies are under the custody of a national exchange or whether they are in the State's own wallet, there will be risks in their maintenance that are not limited to market risk, i.e., price volatility. Reality is abundant with examples. There are plenty of examples, both involving issues with major exchanges[60], and issues with self-custody by experienced users[61].

60- https://www.seudinheiro.com/2021/bitcoin/bitcoin-africa-do-sul-desaparece-24-06/https://canaltech.com.br/criptomoedas/quadriga-conspiracy-a-suposta-morte-do-ceo-e-o-misterio-de-us-190-milhoes-132453/

61- https://www.correiobraziliense.com.br/mundo/2021/07/4937888-bitcoins-bilionario-que-morreu-afogadodeixa-no-limbo-fortuna-de-rs-11-bilhoes-em-criptomoeda.html https://www.istoedinheiro.com.br/investidor-esquece-senha-de-conta-com-us-240-milhoes-em-bitcoin/

Thus, whether due to the high volatility of prices or the technical specificities involving the security of custody of cryptocurrencies, their specific characteristics demonstrate that they are difficult to maintain, which authorizes, pursuant to art. 144-A, of the CPP, early alienation.

Similarly to other countries, including Switzerland and Germany[62], Brazil also lacks specific legislation regarding the disposal of seized cryptocurrencies.

Despite this, there are technical and legal grounds for early alienation to be carried out based on art. 144-A of the CPP, as seen in the previous topic.

In practical terms, unlike what happens with foreign currencies, exchange-traded credit securities, government debt securities, stocks, and other securities, there is no institution equivalent to *Caixa Econômica Federal* to receive the cryptocurrencies and carry out the exchange at an official rate[63].

Technically, we consider that the two most viable alternatives are: alienation by auction, pursuant to art. 879 et seq. of the CPC; and alienation through national exchanges. In practice, however, we believe it is preferable for the alienation to take place in the second way, i.e., via national exchanges[64], especially when taking into account the principle of efficiency (CPC, art. 8). This is because, in addition to the fee charged by exchanges being lower than the auctioneer's fee, the chance of obtaining a higher sale price is immensely greater in order books than in auctions[65].

62- This is also the case in other countries, which do not have, like Brazil, their own rules on asset attachment on cryptocurrencies. Switzerland and Germany, for example, use their criminal procedural rules regarding seizure and confiscation, as per the questionnaire sent by the Cryptocurrency Working Group to these respective countries, available in a restricted manner at the International Cooperation Unit/PGR. In the first country, the debate arose regarding the disposal at the appreciation of cryptocurrencies, which would be challenging in Brazil, due to the lack of legal regulation, without going into the debate that if this practice would not allow, in the case of large seizures and alienations, that the exchange in charge ended up contributing to the fluctuation of values and even if, in some way, the State would not be associated with a speculative practice that is incompatible with that adopted with other volatile assets, such as securities and foreign currencies (FIAT). Please, refer to Decision 1B_59/2021 of October 18, 2021, of the Swiss Supreme Court at https://archipel.law/en/insights/the-early-liquidation-of-crypto-assets-and-the-need-for-crypto-expertise/

63- Resolution No. 428/2005 of the CJF, art. 1, item VI.

64- Practice also adopted in the United States: https://www.cnbc.com/2021/07/28/us-marshalsservice-hires-custodian-to-hold-crypto-seized-in-criminal-activity.html

65- It is not unknown that there are countries that have already disposed of cryptocurrencies via auctions conducted by specialized houses. Cf.: https://www.irishnews.com/business/2019/10/01/news/wilson-auctionsoff-500-000-of-bitcoin-seized-from-uk-criminal-1726231/

There is no procedure for choosing the exchange through which the disposal will be made. In light of this scenario, it is suggested to employ objective criteria in the selection of exchanges, such as fees charged, trading volume, etc., and to submit the selection to the Judiciary.

Finally, it is worth highlighting that it is desirable to adopt strategies, to be thought out with the exchange, aiming to obtain the best average price. Below is an example of the strategy that was judicially approved, as of JUL/14/2021, for the disposal of almost 30 bitcoins, seized in case file No. 5004543-34.2019.4.02.5001, processed in the Federal Court of Espírito Santo State. In that case, the parameters proposed for the sale were established as follows:

1.The BTC will be sold in fractions (10 lots, the first 9 of which will be 3 BTC and the last of the remaining value);

2. The sale of each of the lots will be made by launching one single sell order in the order book, for the total amount of the lot in BTC, with a limit price of not less than 2% of the market price, thus understood as the price corresponding to the last operation carried out via order book;

3. In the event where the sales order with limit price is not completely filled within thirty minutes, a new sales order may be launched, for the remaining amount of the lot, subject to the same previous guideline (item 2);

4. Once the sale of a lot has ended, the order for the following lot may be launched, without the need to observe a minimum interval, but always respecting the same parameters defined in item 2.

The goal was not to negatively affect the Bitcoin price in the exchange's order book, which would occur if all the bitcoins were disposed of at once or in a very short period of time.

DEFI AND ITS PARTICULARITIES

DeFi is the acronym for Decentralized Finances and names a special category of applications run[66] in decentralized environments – the so-called DApps (decentralized applications) –, whose purpose is to enable financial services, such as loans, insurance and liquidity provision.

In order to understand what DApps are, let us go back to the comparison we made between, on the one hand, bitcoin-hardware/bitcoin-software and, on the other, the notebook/its operating system (Windows or Linux). In this comparison, bitcoin software is like an operating system that has functionalities, but was not designed to accommodate the installation of programs.

Starting with Ethereum, the first programmable Blockchain to emerge, this scenario changes drastically, and the Windows in our comparison becomes an operating system thought of and designed to support the installation of programs that run on it.

In this new comparative scenario, Ethereum-hardware resembles the Notebook, Ethereum-software resembles Windows and DApps resemble any programs that run on Windows, such as Word, Google Chrome and Zoom.

Just as the programs in our example (Apps) can be classified into different categories, based on the service they provide (text editing, web browsing,

66- In this context, programs, apps, and applications are synonymous words.

remote conferencing, etc.), DApps can also be classified as such. One of the species resulting from the use of this classification criterion is DeFi DApps.

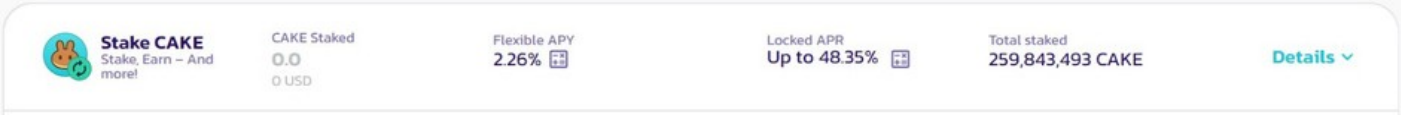
Programs that run locally on your notebook, such as Word and Chrome, depend on local installation. Programs that run in a decentralized manner, in turn, depend on installation on the Blockchain. Installing a program on the decentralized world computer called Ethereum (EVM: Ethereum Virtual Machine) means strictly the same thing as deploying a smart contract on the Ethereum Blockchain.

To proceed, an additional clarification should be made: smart contracts are programs that run on blockchains. In the common sense of the term, therefore, they are not contracts, let alone intelligent ones. They are simply programs that execute what they were programmed to do (self-executing).

In a “smart contract”, every time condition A is met, result B is produced. These are programs written in the form of the conditional IF → THEN.

The following example will show why understanding the subject interests us.

The image depicts a DeFi application where, for those who stake CAKE tokens, it offers annualized yields of up to 48.35% in CAKE tokens (→ THEN).

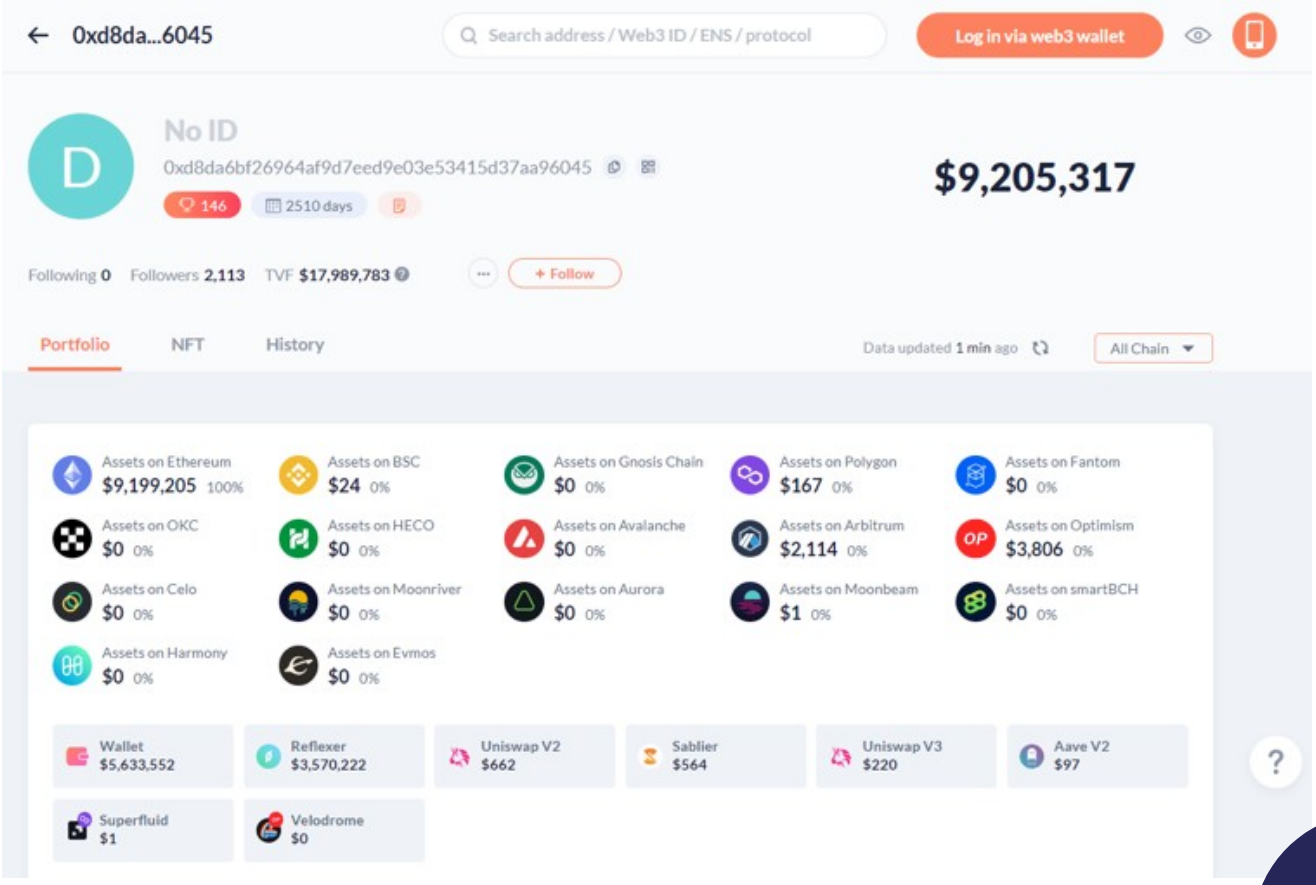


By staking, we mean submitting CAKE tokens from your account to the smart contract account that will remunerate you.

The practical consequence is that, from this submission, the tokens will no longer be at your address but at the address of the smart contract. Your private key will then no longer allow the immediate submission of these tokens to another address, but rather the recovery of these tokens, something with a redemption of the applied tokens.

Let us imagine, then, that this is the situation of the target of an asset investigation. Even if your public address is known, the “placed” tokens will not be found there, because they will be in the smart contract addresses of DeFi DApps.

This difficulty, however, is surmountable. Tokens belonging to the target, temporarily located at one of the main DeFi smart contract addresses, can be easily found by using free online tools, such as https://debank.com/ and https://apeboard.finance/.



In other words, not only the cryptocurrencies that appear in their public addresses belong to the target, but also those linked to their public addresses that, temporarily, appear in DeFi smart contracts.

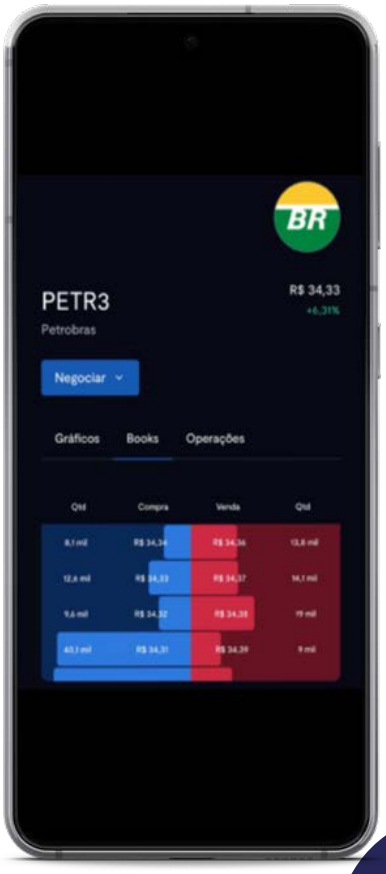
At that, any act of investigation or asset attachment that concerns cryptocurrencies held by the target must consider the possibility that a considerable portion of them are temporarily at other public addresses.

NFTS AND THEIR DISTINCTIVE FEATURES

NFT is the acronym for non-fungible tokens. If tokens are digital assets that cannot be copied, non-fungible tokens are digital assets that, in addition to being unable to be copied, are unique and irreplaceable.

Cryptocurrencies and fungible tokens in general can be traded on the order books of exchanges, similar to how stocks are traded via order books on the B3. NFTs, on the other hand, cannot – in the same way as real estate and works of art – be traded via an order book, even if legislation would allow it.

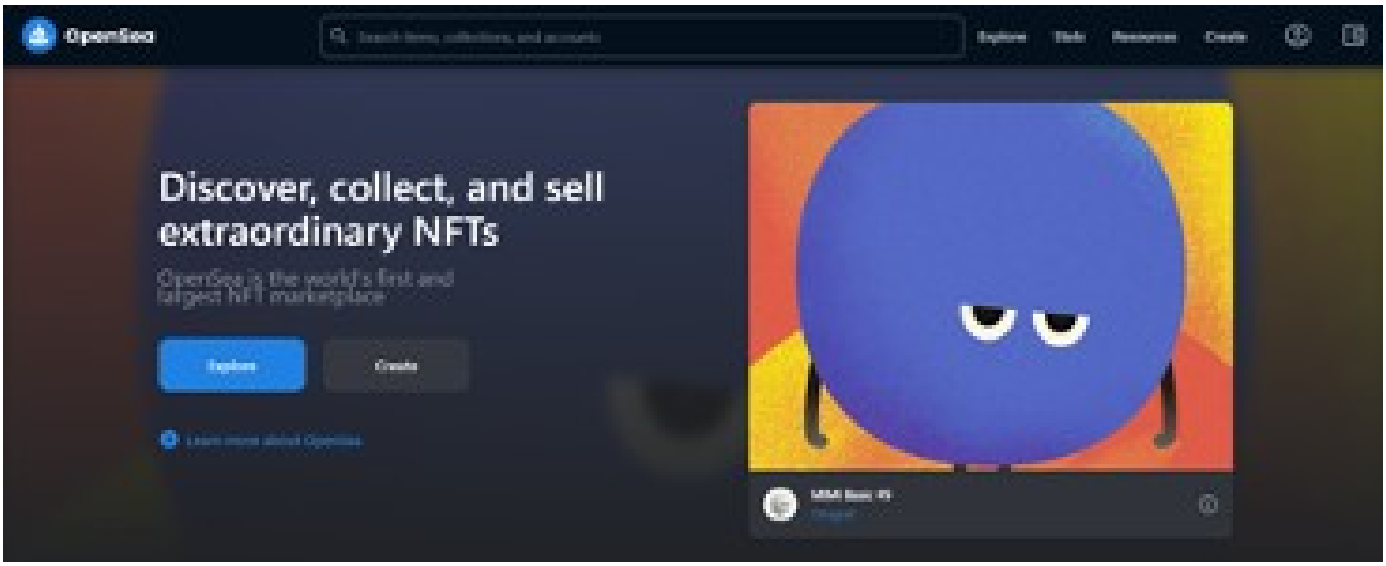
This is because real estate and works of art are unique assets, i.e., non-fungible. And the order book is an instrument for bringing together opposing interests regarding a pair of fungible things. Please, refer to the following example.



In the image to the side, we can see the order book (book) for the trading pair BRL (Brazilian real) and PETR3 (common shares of Petrobras). People refer to it when they want to exchange real for shares or shares for real, both of which are fungible, non-unique assets. One real is equivalent to another real. One share is equivalent to another share.

Real estate and works of art can be listed for sale directly by their owners, or these same owners can turn to an intermediary, such as a real estate agency or an art gallery. NFTs, similarly, can be offered for sale directly by their owners. The most common, however, is that they are offered for sale through an intermediary, a platform that, without taking custody of these NFTs, gives them greater visibility and, above all, security in trading.

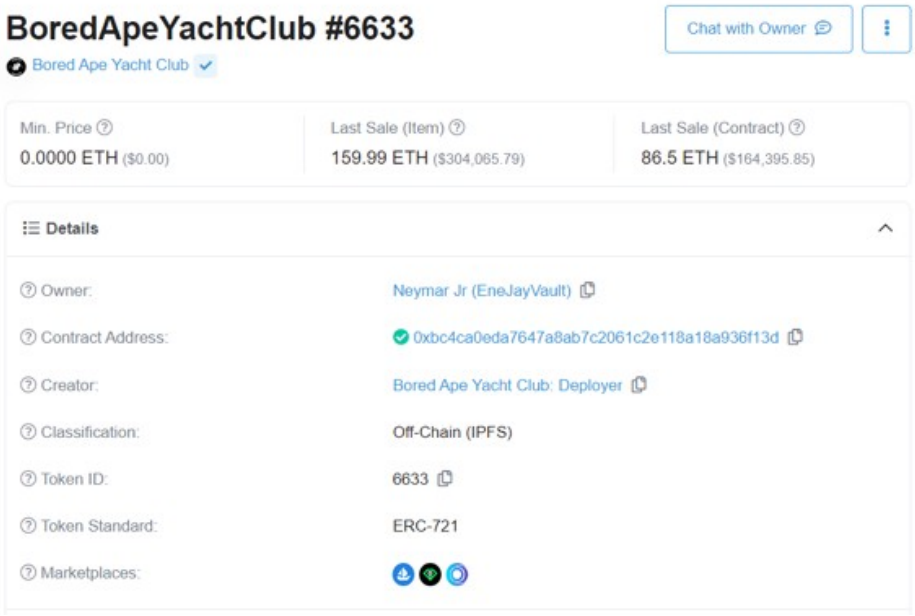
These platforms are called marketplaces and the main one, with a huge advantage, is Opensea (https://opensea.io/).



There is nothing that particularizes the custody of NFTs. The practical difference between fungible tokens and NFTs that interest us consists of the form of disposal, with the former having exchange offering books as the most suitable place for disposal and the latter being able to be disposed of via marketplaces.

NFTs are not trading cards. They are, instead, a unique digital object. And this unique digital object is not the media that may be associated with it, but rather a unique identifier on the Blockchain.

The image above is not an NFT. It is the media associated with BAYC #6633, an NFT that is part of the Bored Ape Yatch Club collection and that currently belongs to football player Neymar. Technically, the image reproduced above can be freely copied by third parties and it is not non-fungible at all.



The screenshot above, on the other hand, showcases the data of said NFT. A token with a unique ID (6633), linked to a smart contract (0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d), implemented on a blockchain (Ethereum)[67].

NFTs are the non-fungibility of the real world brought into the digital world. Just like original documents, real estate and works of art are fundamentally different from each other – despite being all non-fungible assets – NFTs can also be.

Some of these NFTs may have no market value (e.g. documents), while others may have immense value (e.g. virtual properties and items from famous collections).

To what interests us. The most effective way to dispose of NFTs found in the target's wallets is through marketplaces, given their non-fungibility, and exchanges should not be used in this case.

67- Interestingly, this image of the monkey is not even on the Blockchain. It is in a distributed storage service called IPFS, and what the NFT actually does is point to the location (off-chain).

TEMPLATES

LIFTING OF TAX SECRECY OF OPERATIONS WITH CRYPTOCURRENCIES IN SIMBA

The Federal Prosecution Service, therefore, requests, based on Article 198 of the National Tax Code, the order for the lifting of tax secrecy for the individuals and legal entities listed in the table below, for the specified period:

(table generated by SIMBA with name, CPF/CNPJ and period)

Regarding these individuals under investigation, the Brazilian Federal Revenue Service must provide, within thirty (30) days from the receipt of the court order, all the information related to cryptocurrency that it possesses, such as: a) statements of cryptocurrency operations (reported by the taxpayer or national exchanges); b) documents related to the payment of tax on capital gains from the disposal of cryptocurrencies, and c) income tax returns with information on cryptocurrencies.

For the judicial order to be operational, it is requests that:

I – The court order states that the Federal Revenue Service of Brazil is obliged to submit the data and additional documentation, in .txt, .cvs format, .xlsx or, if this is not possible, in .pdf, through SIMBA, in reference to Simba case 001-MPF-00XXXX-XX, using the program “VALIDADOR BANCÁRIO SIMBA”, in the option “TRANSMISSION OF DOCUMENTS”, whose guidelines can be found at the electronic address https://asspaweb.pgr.mpf.mp.br;

II – The court order must include that, in case of doubt from the behalf of the recipient institutions, the e-mail address for contact with the Expertise, Research and Analysis Unit - SPPEA/PGR is pgr-simba@mpf.mp.br.

LIFTING OF TELEMATICS SECRECY OF OPERATIONS WITH CRYPTOCURRENCIES IN SIMBA (EXCHANGES)

The Federal Prosecution Service requests, therefore, based on Law No. 12.965/14 (Brazilian Civil Rights Framework for the Internet), the order for the lifting of telematics secrecy for the individuals and legal entities listed in the table below, for the period informed:

(table generated by SIMBA with name, CPF/CNPJ and period)

I. Concerning these individuals under investigation, the cryptocurrency exchange (...) must provide, within thirty (30) days from the receipt of the court order:

a) all your registration data and documents and those of attorneys who may be authorized to use your accounts;

b) information regarding all operations carried out by them (whether in cryptocurrency or in fiat currency), in a spreadsheet containing a field with the amount in REAL corresponding to each operation with cryptocurrencies at the time it was carried out;

c) For each transaction, the corresponding amount in US dollars at the time of the transaction and the remaining balance after the transaction must also be informed, as well as:

- Date and Time;
- Asset identification and quantity;
- Sender and recipient identification (including bank account or crypto address);
- Corresponding amount in REAL (on the date and time of the transaction);
- Network (crypto) and Bank (banking correspondent), depending on the hypothesis (involvement of cryptocurrencies and/or fiat currency in the operation);
- Hash ID of the transaction.

d) information on the current balance of each of those investigated, broken down by fiat currency or type of cryptocurrency, in the latter case with a current amount referenced in REAL.

II.For the judicial order to be operational, request is made that:

a) The court order states that the cryptocurrency brokerage must submit the data and additional documentation, in .txt, .cvs format, .xlsx or, if this is not possible, in .pdf, through SIMBA, in reference to Simba case 001-MPF-00XXXX-XX, using the program “VALIDADOR BANCÁRIO SIMBA”, in the option “TRANSMISSION OF DOCUMENTS”, whose guidelines can be found at the electronic address https://asspaweb.pgr.mpf.mp.br;

b) The court order states that cryptocurrency brokers must maintain the secrecy of the judicial decision to breach, refraining from informing their clients of the process or due diligence, under the penalties of the law;

c) The court order must include that, in case of doubt from the behalf of the recipient institutions, the e-mail address for contact with the Expertise, Research and Analysis Unit - SPPEA/PGR is pgr-simba@mpf.mp.br.

SEARCH AND SEIZURE

The FEDERAL PROSECUTION SERVICE requests, pursuant to art. 240, §1, paragraphs “b”, “c”, “e”, “f” and “h”, of the Code of Criminal Procedure, the issuance of search and criminal seizure warrants with the purpose of seizing any documents, media and other evidence found related to the crimes (...), notably, but not limited to:

a) ledgers and accounting books, formal or informal, proof of receipt/payment, rendering of accounts, payment orders, agendas, letters, minutes of meetings, contracts, copies of opinions and any other documents related to the offenses narrated in this statement;

b) HDs, laptops, smartphones, flash drives, electronic media of any kind, electronic files of any kind, handwritten or electronic diaries, of those being investigated or their companies, when there is a suspicion that they contain relevant evidentiary material, as specified above;

c) electronic files belonging to the systems and electronic addresses used by those represented, in addition to records from security cameras in the places where the measures are carried out;

d) amounts in cash in foreign currency or reais of an amount equal to or greater than BRL 20,000.00 or US$ 5,000.00 and provided that full documentary proof of their lawful origin is not presented; and

e) physical storage devices for cryptocurrency keys (cold wallets, hard wallets, or cold wallets).

The MPF also requests that the seized cell phones and tablets be sent to the Federal Police Forensic Examination immediately after the police operation is initiated, so that their data can be extracted and added to the case files, where the analyses of the other devices should be presented within a reasonable timeframe.

It also requests that this court determine that the data be extracted through “file system extraction”, if possible, as it allows the collection of a greater amount of information from the device.

It also requests, with respect to all the equipment, electronic media, and physical storage devices for cryptocurrency keys (cold wallets, hard wallets, or cold wallets) seized, authorization to access their contents, and especially with respect to smartphones, access to all cloud-stored data related to services linked to the seized phones.

Regarding the physical storage devices for cryptocurrency keys (cold wallets, hard wallets, or cold wallets), request is made that the search and seizure warrant explicitly authorizes access to their content, and the police authority must take steps for the immediate transfer of the assets found to the state custody wallet (...).

PRECAUTIONARY ASSET SEIZURE

That said, the FEDERAL PROSECUTION SERVICE requests the order for the SEIZURE of the defendants' assets, jointly and severally, up to the amount of (...).

To operationalize the seizure measure, the MPF requests:

a) communication of the seizure decision to financial institutions, through the online seizure technique, provided for in art. 854 of the new Code of Civil Procedure and implemented by the Asset Search System of the Judiciary – SISBAJUD, with respect to all current accounts and financial investments held by the defendants[68], in order to ensure that they are not redeemed or transferred in any way. If the measure is not implemented, the automatic reiteration of freezing orders is henceforth requested;

b) cumulatively, request is made for the issuance of a warrant for the seizure of cryptocurrencies that may be in the custody of the following brokers (...). To execute the seizure warrant, request is also made that:

1. The order states that the MPF and the Federal Police may comply with attachment orders directly by contacting brokers or, if not met, inspect the companies' headquarters in search of assets;

2. the MPF and the Federal Police may have access to electronic or storage devices, e-mails or telephones, linked for the purpose of double-factor authentication, to transfer the amounts to the wallet described in the annex under the control of the State, for the purposes of provisional custody of these cryptocurrencies; and

68- Including securities assets, such as fixed income securities and shares, custody of shares, private securities, public securities and derivatives, investments in investment funds, VGBL, PGBL, investments in LCA and LCI, investments in CDBs, RDBs, COE, gold and related, private pension and consortium letters.

3. the MPF and the Federal Police can carry out the transfer of amounts in custody, by adopting operational execution measures to comply with the court order, including the creation of a cryptocurrency custody wallet, settlement at the day's market value of the cryptocurrency and the transfer of the result to a judicial account linked to the records, upon court order;

4. the MPF and the Federal Police can transfer to the virtual wallet described in the attached document the amounts in cryptocurrencies contingently seized in the search and seizure warrants issued in process No. (...), on the same date filed.

c) Request is made for the freezing through RENAJUD of all vehicles registered in the name of the defendants up to the amount of (...), provided that the year of manufacture is above 2010 - with the goal of avoiding the freezing of older vehicles without market value. Request is made that a note be inserted in RENAJUD, specifying the restriction as "transfer of the vehicle, its annual licensing and circulation on public roads";

d) the freezing of vessels and aircraft that may be registered in the name of the defendants is requested, with the issuance of an official letter to the Port Authority and ANAC to implement the measure;

e) the freezing of real estate registered in the name of the defendants is requested up to the amount of BRL, by inserting the restriction order in the CNIB – National Central Registry of Unavailability of Assets[69], established in compliance with the Provision of the Inspector-General of Justice by Provision No. 39/2014;

f) request is made for the issuance of a warrant to the Board of Trade of the States of the Federation where the defendant companies are located, informing it of the unavailability of all paid-up shares of the share capital of the legal entities indicated in the table above;

69- https://www.indisponibilidade.org.br/autenticacao/

g) inclusion of assets in the National System for Seized Assets – SBNA of the National Council of Justice, pursuant to Resolution No. 63, of December 16, 2008;

h) the judicial appraisal of real estate and automobiles contingently seized, by notifying the MPF and the owner of the result, and its judicial approval;

i) the early disposal of properties and automobiles contingently seized, pursuant to art. 144-A of the Code of Criminal Procedure and Resolution No. 92/09 of the Council of Federal Justice, with a view to preserving its value, considering that it is an asset subject to a high degree of deterioration and depreciation, furthermore, because it involves difficulties and costs for the State in its maintenance;

j) the deposit of the disposal proceeds into an account linked to the court until the final decision sentencing the main criminal action, converting it into income for the Federal Government (art. 91, item I, CP);

l) Authorize the transmission of the decision to foreign authorities in requests for international legal cooperation, with the aim of blocking and repatriating any assets identified abroad.

m) authorize the seizure of assets considered to be of high value, such as works of art, vehicles and jewelry found in the possession/property[73] of the defendants, in the amount specified above, when executing the search and seizure warrants requested in the process filed on that date.

MPF

Ministério Público Federal

Federal Prosecution Service