ROTEIRO DE ATUAÇÃO

CRIPTOATIVOS

PERSECUÇÃO PATRIMONIAL

MINISTÉRIO PÚBLICO FEDERAL

ROTEIRO DE ATUAÇÃO CRIPTOATIVOS PERSECUÇÃO PATRIMONIAL

MINISTÉRIO PÚBLICO FEDERAL

MINISTÉRIO PÚBLICO FEDERAL
2ª CÂMARA DE COORDENAÇÃO E REVISÃO

ROTEIRO DE ATUAÇÃO
CRIPTOATIVOS
PERSECUÇÃO PATRIMONIAL

Brasília - MPF 2023

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

Câmara Criminal
Membros titulares
Carlos Frederico Santos
Coordenador
Subprocurador-geral da República

Luiza Cristina Fonseca Frischeisen
Subprocuradora-geral da República

Francisco de Assis Vieira Sanseverino
Subprocurador-geral da República

Membros suplentes
Paulo de Souza Queiroz
Subprocurador-geral da República

Adriana de Farias Pereira
Procuradora regional da República

José Robalinho Cavalcanti
Procurador regional da República

Coordenação e Organização
Grupo de Trabalho Criptoativos
2ª CÂMARA DE COORDENAÇÃO E REVISÃO

Alexandre Senra
Coordenador
Procurador da República

Anamara Osório Silva
Procuradora Regional da República
Secretária Adjunta de Cooperação Internacional/PGR

Eduardo El Hage
Procurador da República

Marisa Varotto Ferrari
Procuradora da República

Thiago Augusto Bueno
Procurador da República

Tiago Misael de Jesus Martins
Procurador da República

Procuradoria-Geral da República
2ª Câmara de Coordenação e Revisão
SAF Sul, Quadra 4, Conjunto C
Fone (61) 3105-5100
70050-900 - Brasília - DF
www.mpf.mp.br

ÍNDICE

INTRODUÇÃO

Esta é a primeira versão de um roteiro para a atuação do Ministério Público Federal na temática dos criptoativos. O objetivo principal é fazer com que o leitor compreenda as discussões, qualificando-o para adotar ou não as propostas de atuação.

O roteiro está organizado em três partes. A primeira reúne informações necessárias à compreensão das discussões e orientações funcionais propostas. A segunda, traz as discussões e as orientações propriamente ditas. A última, conta com modelos que podem ser utilizados por membros do MPF nos casos práticos.

A compreensão deste roteiro de atuação dispensa conhecimento prévio sobre criptoativos, sendo, neste sentido, um roteiro a partir do zero. Todavia, este ainda é um roteiro de atuação, não é um curso sobre criptoativos ou Blockchain. Ele representa, portanto, uma recorte daquilo que importa à atuação do MPF nessa matéria. O mar de conhecimento com um palmo de profundidade, aqui, nada valeria. Em vez disso, o roteiro mergulha em locais estratégicos, na profundidade necessária.

Ao longo do texto, notadamente na primeira parte, o roteiro faz uso de definições operacionais úteis às discussões propostas, sem pretensão de rigor científico. Não encontramos forma mais objetiva para cumprir a finalidade deste roteiro.

Um exemplo. Criptoativos foram definidos como ativos digitais que não podem ser copiados. Não se trata de desconsiderar a importância de elementos como criptografia e tecnologia Blockchain, e sim de demonstrar que eles não são necessários à compreensão do termo “criptoativo” no contexto empregado nesse roteiro.

O roteiro não é completo nem tem a pretensão de o ser. Mesmo dentro do primeiro recorte (aquilo que mais interessa à atuação do MPF), o tema é potencialmente inesgotável. Outros dois recortes subsequentes, então, foram feitos: esta primeira versão se limitou ao subtema da persecução patrimonial, que nos pareceu ser o mais urgente; e o foco é o Bitcoin, ainda que grande parte do que é dito aqui seja aplicável a muitos outros criptoativos.

CRIPTOATIVOS

Criptoativos são ativos digitais que não podem ser copiados. São também o designativo de um gênero.

A seguir, examina-se cada uma dessas proposições.

CRIPTOATIVOS COMO ATIVOS DIGITAIS QUE NÃO PODEM SER COPIADOS

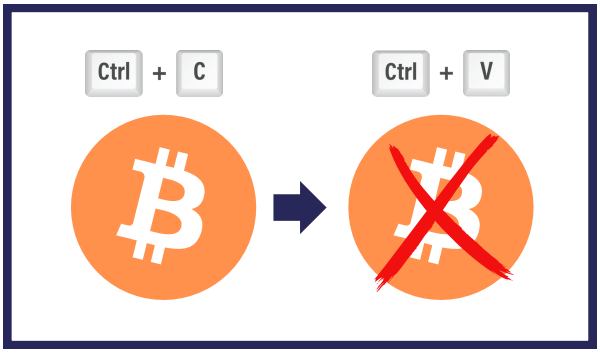
25 de Maio de 2022, a partir do meu computador, em Vitória/ES, envio o pdf deste roteiro, ainda em elaboração, a um colega de MPF. Dessa simples conduta surgem, pelo menos, mais três cópias do pdf. O documento, que antes existia apenas no meu computador, passa a existir também na caixa “itens enviados” do meu e-mail, na caixa “itens recebidos” do e-mail desse colega e no seu computador, assim que ele baixa o arquivo.

Mesmo dia e local, realizo o envio de 0.1 bitcoin da minha carteira para outra carteira. Pouco tempo depois, a minha carteira passa a ter 0.1 bitcoin a menos e a carteira de destino passa a ter 0.1 bitcoin a mais.

Apesar de ter empregado o verbo “enviar” em ambas as situações, as consequências do “envio” foram completamente diversas.

A primeira situação envolveu um objeto digital copiável, enquanto que a segunda envolveu um objeto digital que não pode ser copiado – um objeto digital, neste sentido, escasso.

E se, em vez de um documento em formato .pdf, eu enviasse uma fotografia ou um filme? Estaríamos diante do mesmo problema, consistente na ausência de escassez dessas mídias, que, enquanto bens digitais, podem ser copiadas a um custo muito próximo de zero.



É, portanto, o atributo da escassez que particulariza os criptoativos e não o fato de serem ativos digitais. Jogos e programas de computador, por exemplo, são também ativos digitais, mas podem ser tecnicamente copiados, como a pirataria bem evidencia.

CRIPTOATIVOS COMO O DESIGNATIVO DE UM GÊNERO

Criptoativo é sinônimo de token em sentido amplo e designa um gênero, composto por espécies que podem ser classificadas através de variados critérios.

Vejamos alguns deles.

(a) Conforme sirvam ou não ao pagamento das taxas de uso de uma Blockchain: criptomoedas e demais tokens.

(b) Segundo a finalidade da aplicação a que se vinculam: tokens de DeFi, de jogos, de metaversos etc.

(c) De acordo com a fungibilidade: tokens fungíveis e NFTs.

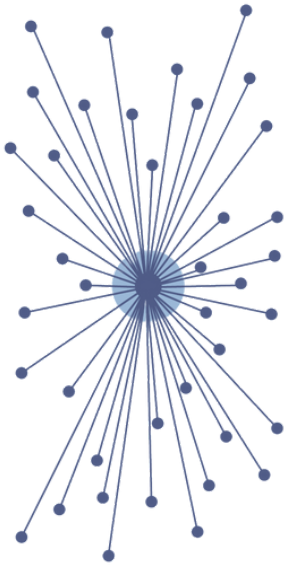
Evidentemente, algumas correlações podem ser traçadas entre essas classificações. Por exemplo: todas as criptomoedas são tokens fungíveis; metaversos usualmente se estruturam sobre tokens fungíveis e sobre NFTs. Mas fazê-lo, neste momento, causaria uma confusão desnecessária.

As espécies que interessam a esse roteiro serão adequadamente tratadas mais à frente.

BLOCKCHAIN

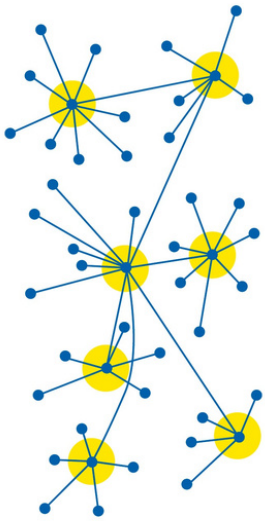
Blockchain é a principal espécie do gênero “tecnologias de registro distribuído”.

Informações podem ser registradas de forma centralizada, em um só ponto da rede, também chamado de provedor, em oposição aos demais pontos dessa rede, chamados de usuários. Ou podem ser registradas de forma descentralizada, entre diversos pontos da rede, que passam aqui a serem chamados de nós.



Provedor

Usuário



Nós

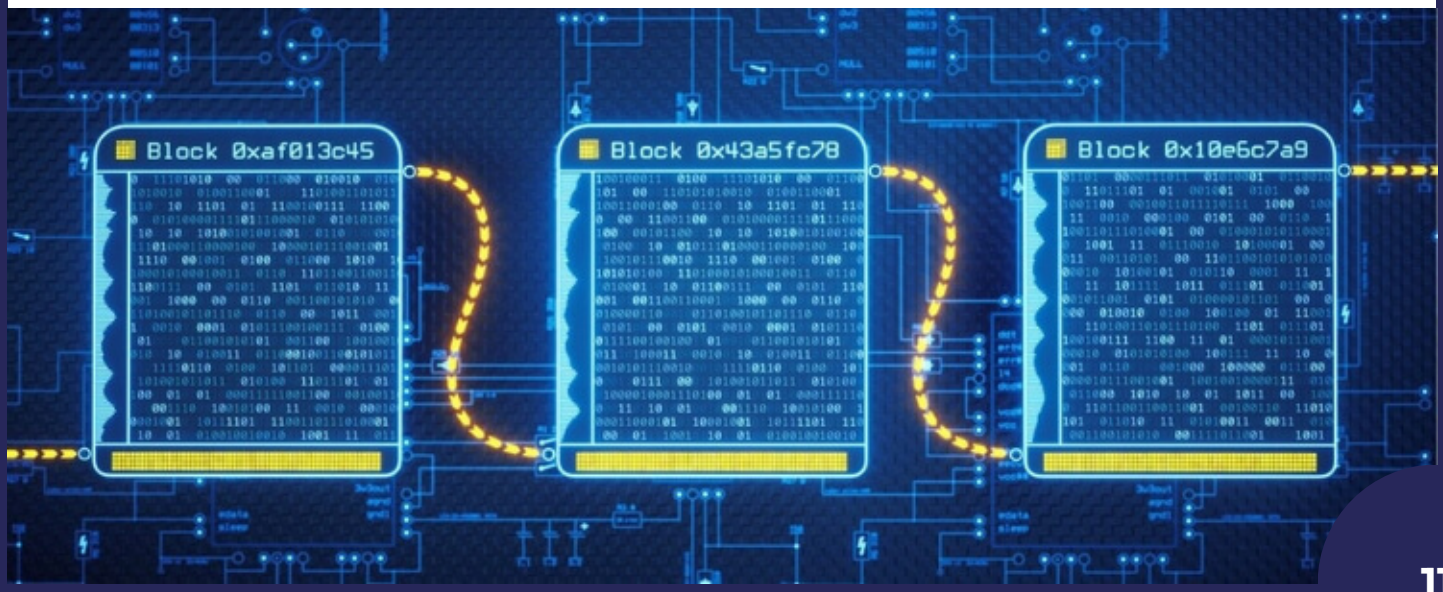
Cada modo de se fazê-lo apresenta as suas vantagens e desvantagens.

Registros centralizados são extremamente baratos e rápidos, mas dependem da confiança na autoridade responsável por esse registro. Registros decentralizados ou distribuídos, por sua vez, são comparativamente mais caros e lentos de serem feitos, mas dispensam a exigência de confiança em qualquer autoridade.

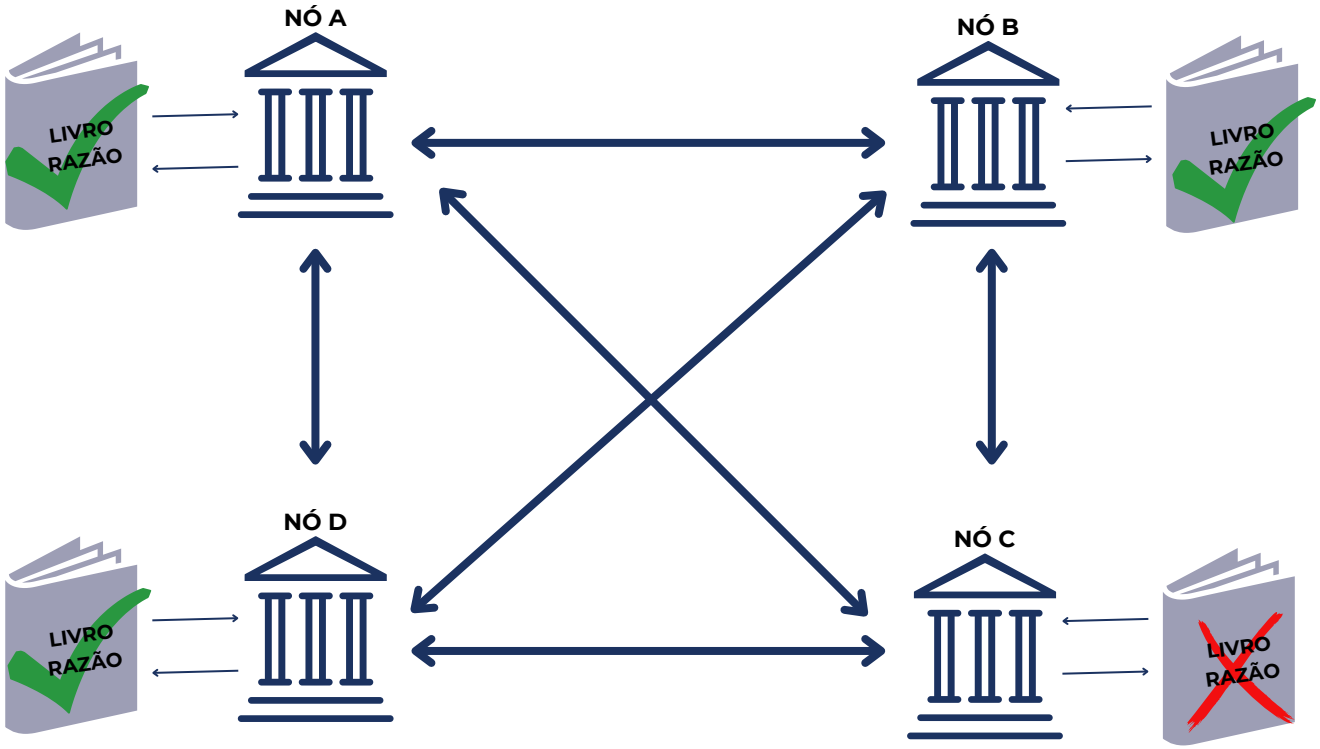
Um exemplo. Transações entre contas de uma mesma exchange de criptoativos são rápidas e baratas, mas a sua veracidade exige que confiemos naquela exchange, responsável pelo registro centralizado das informações. Já transações feitas entre endereços bitcoin são mais caras e lentas, mas dispensam que se confie em qualquer autoridade, porque não existe aí uma autoridade responsável pelo registro, que é mantido de forma distribuída entre os diversos nós da rede.

Apenas uma das repercussões práticas dessa diferença: um registro centralizado pode ser adulterado pela autoridade por ele responsável; um registro distribuído não pode ser adulterado por ninguém.

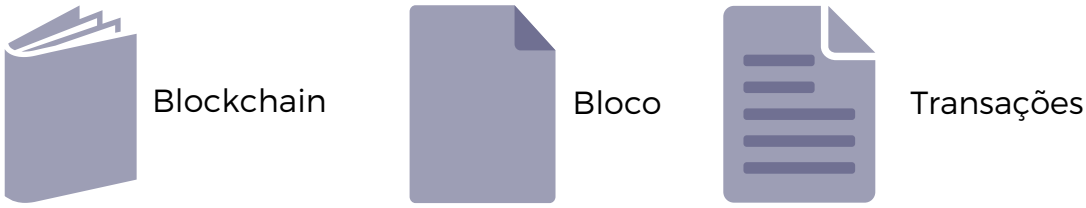
Blockchain é um tipo de registro distribuído, composto por blocos de dados, cronologicamente ordenados, onde cada bloco se liga imediatamente ao anterior e confirma, através de provas matemáticas, as transações contidas em todos os blocos anteriores.



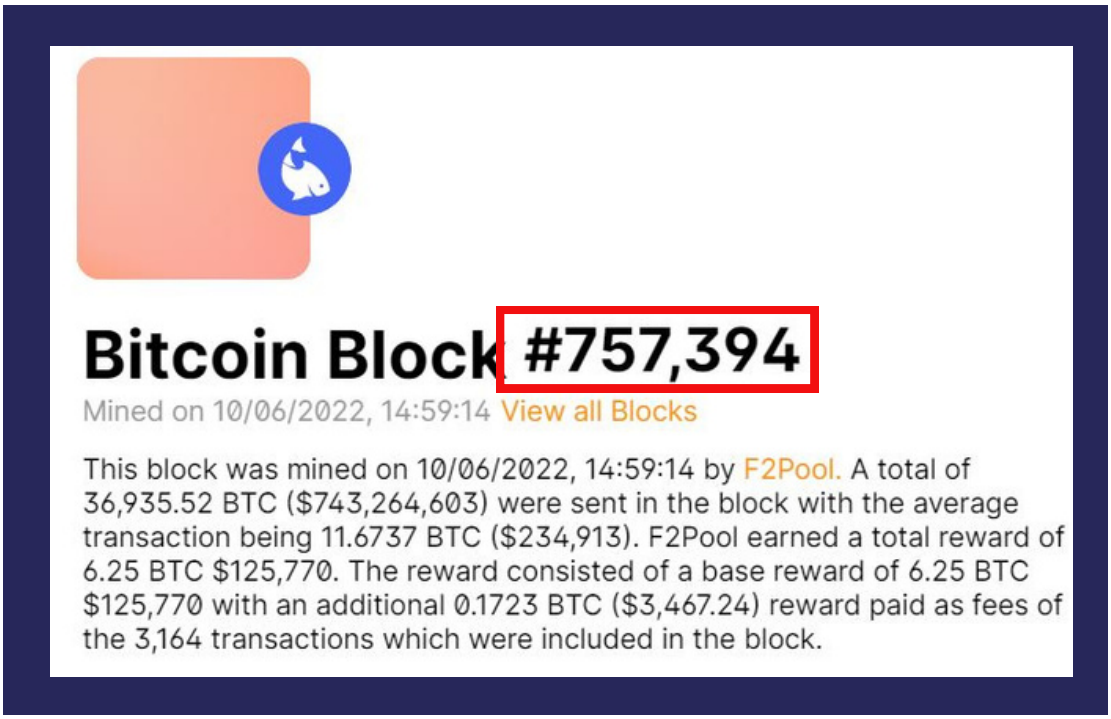
Pense no Blockchain como sendo um livro-razão (ledger) presente em diversas vias ao redor do mundo. Não são cópias feitas a partir de um mesmo original, mas sim vias, de igual importância e originalidade, sincronizadas entre si, onde qualquer alteração indevida feita em uma dessas vias é facilmente percebida e rapidamente repelida pelas demais.



Prosseguindo na metáfora do livro-razão distribuído, imagine que esse livro vai recebendo novas folhas ao longo do tempo e que em cada folha pode existir muitas ou poucas linhas escritas. As folhas correspondem aos blocos do Blockchain. As frases correspondem às transações de cada bloco.



No caso do Bitcoin, desde que o seu primeiro bloco foi minerado (Bloco Zero), às 16h15 (UTC-3) do dia 03/01/2009, uma nova folha é acrescida a cada dez minutos, aproximadamente. Neste exato momento, às 15h do dia 06/10/2022, esse livro já conta com 757.395 folhas.[1]



1- O Bloco número 757.394 corresponde à 757.395 folha do nosso livro porque o Bloco Zero corresponde à primeira folha.

BITCOIN

O Bitcoin foi concebido para ser um sistema de pagamentos sem intermediários.[2] Mas, para prosseguirmos na compreensão do assunto, mais relevante do que saber disso é sabermos que "Bitcoin" é uma palavra ambígua.

Três dos seus significados, a despeito de intimamente relacionados, precisam ser discernidos: Bitcoin-hardware, Bitcoin-software e Bitcoin-criptoativo.

Bitcoin-hardware é o nome dado ao conjunto de dispositivos físicos ao redor do mundo, responsáveis pela segurança do Blockchain contra qualquer tentativa de fraude. É a rede Bitcoin.

Bitcoin-software é o termo utilizado para se referir ao programa que roda nesses dispositivos físicos, de que fazem parte, num recorte simplificado: o Blockchain, um gerador aleatório de pares de chaves e um conjunto de regras.

Numa analogia, o bitcoin-hardware está para o seu notebook, assim como o bitcoin-software está para o Windows ou o Linux que você roda nele. Da mesma forma como notebook e Windows não se confundem, bitcoin-hardware e bitcoin-software não devem ser confundidos.

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

Do Blockchain já falamos. O gerador de pares de chaves abordaremos mais à frente. Falaremos, agora, de algumas das regras do protocolo Bitcoin, começando pela definição do que é o bitcoin-criptoativo.

Bitcoin-criptoativo (BTC) é um ativo digital escasso cuja primeira finalidade é servir como pagamento que o software faz ao hardware para funcionar e cuja segunda finalidade é servir como moeda para o pagamento de taxas por quem queira fazer uso da rede bitcoin.

Examinemos, brevemente, cada uma dessas finalidades.

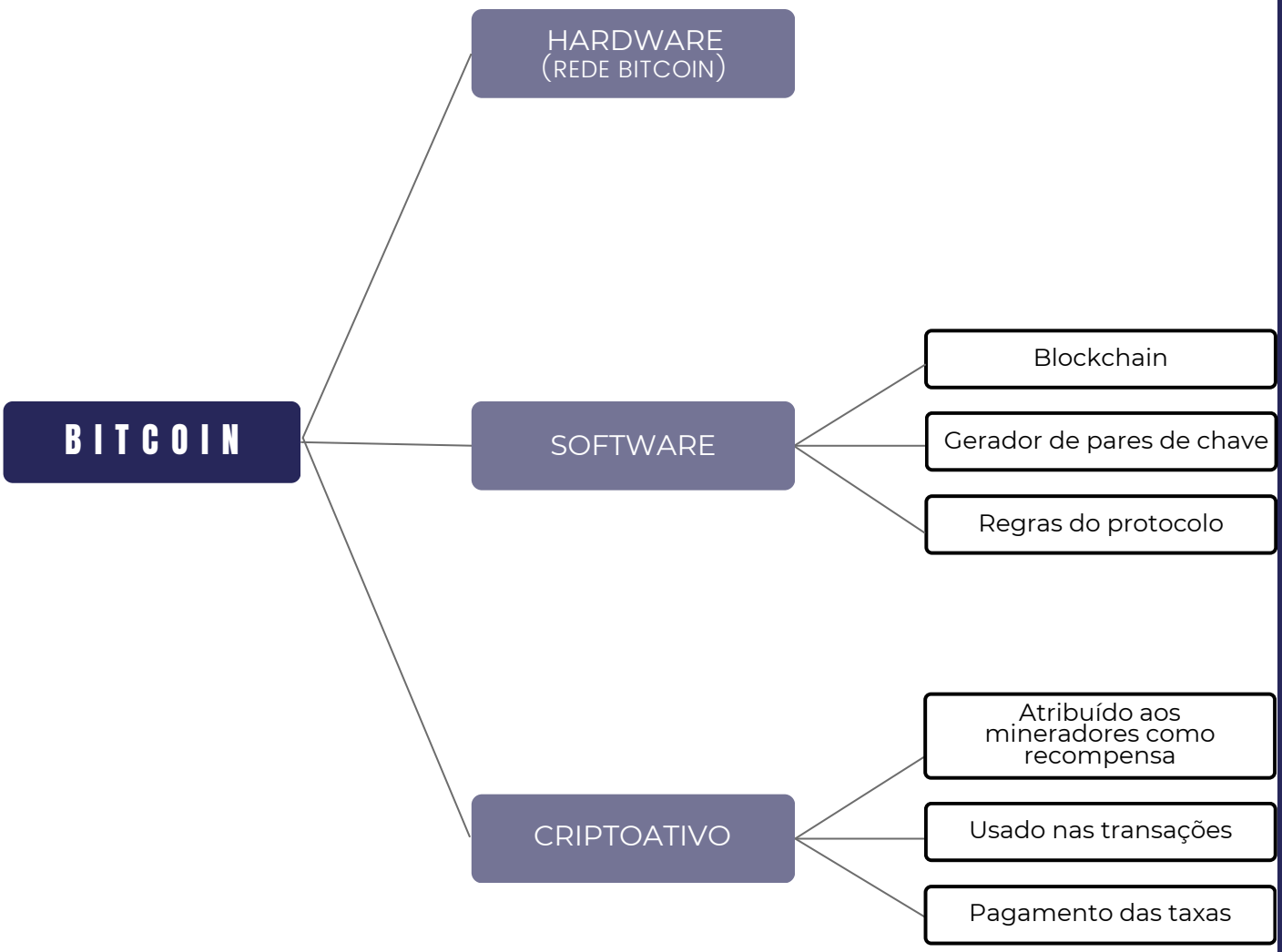
Primeira finalidade: Novos blocos são acrescidos ao Blockchain através de um processo comumente chamado de "mineração", que envolve um elevado gasto de energia elétrica e de potência computacional. Trata-se de um disputa, travada entre mineradores, visando a uma recompensa, consistente nos novos BTC emitidos e atribuídos, a cada novo bloco, a um minerador-vencedor.

Segunda finalidade: Para se enviar BTC através da rede Bitcoin não é preciso ser um minerador nem é necessário ter consigo uma via do Blockchain. No entanto, deve-se pagar uma pequena taxa de transação, necessariamente em BTC.[3] Por isso o BTC é uma criptomoeda, porque ele desempenha, neste contexto, a função de uma moeda.

Sua emissão segue algumas regras do protocolo:

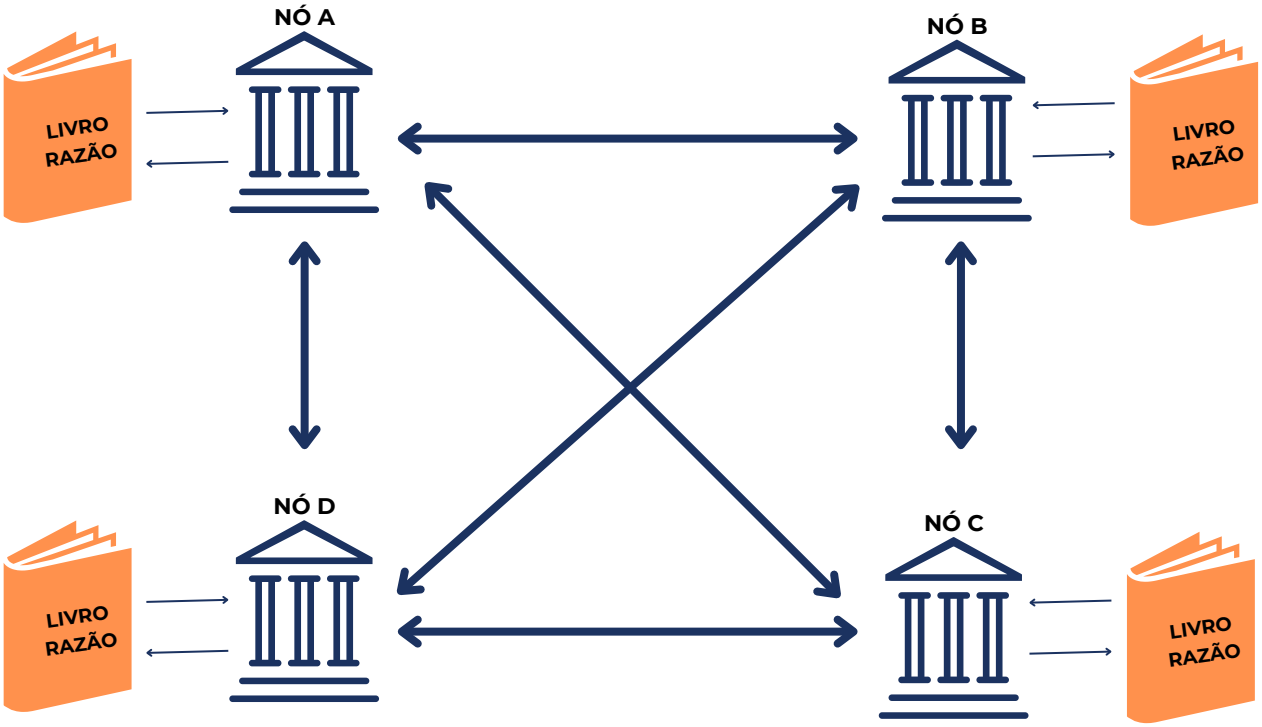
- está limitada a 21 milhões;
- acontece a cada novo bloco minerado;
- inicialmente era de 50 BTC por bloco e atualmente é de 6.25 BTC por bloco, tendo em vista que ela é reduzida pela metade a cada 210.000 novos blocos, em um processo chamado halving.

3- O valor da taxa de transação não depende do valor transacionado e sim de outros dois fatores: do espaço que a transação ocupa no Blockchain e da demanda pelo uso da rede Bitcoin. Quanto maior o espaço ocupado pela transação e quanto maior a demanda pelo uso da rede, maior será a taxa a ser paga.


BITCOIN
HARDWARE
(REDE BITCOIN)
SOFTWARE
Blockchain
Gerador de pares de chave
Regras do protocolo
CRIPTOATIVO
Atribuído aos mineradores como recompensa
Usado nas transações
Pagamento das taxas

ONDE FICAM OS CRIPTOATIVOS

Como bens digitais que são, os criptoativos não estão no mundo físico. Sob a perspectiva do usuário, os criptoativos podem estar com ele ou com terceiros. Sob a perspectiva técnica, os criptoativos não estão com ninguém. Eles são lançamentos em um livro-razão público e distribuído, chamado de Blockchain. Ou estão nesse livro ou simplesmente não existem.



Necessário não se confundir criptoativos com saldo em criptoativos. Criptoativos estão registrados no Blockchain; saldos em criptoativos estão registrados em um banco de dados privado e centralizado, pertencente, por exemplo, a uma exchange.

Um designativo comumente empregado nessa diferenciação é o de transações on-chain e transações off-chain. No primeiro caso, não se precisa confiar em ninguém, apenas no processo de segurança da Blockchain. No segundo caso, é necessário confiar-se na pessoa responsável pelo registro centralizado.

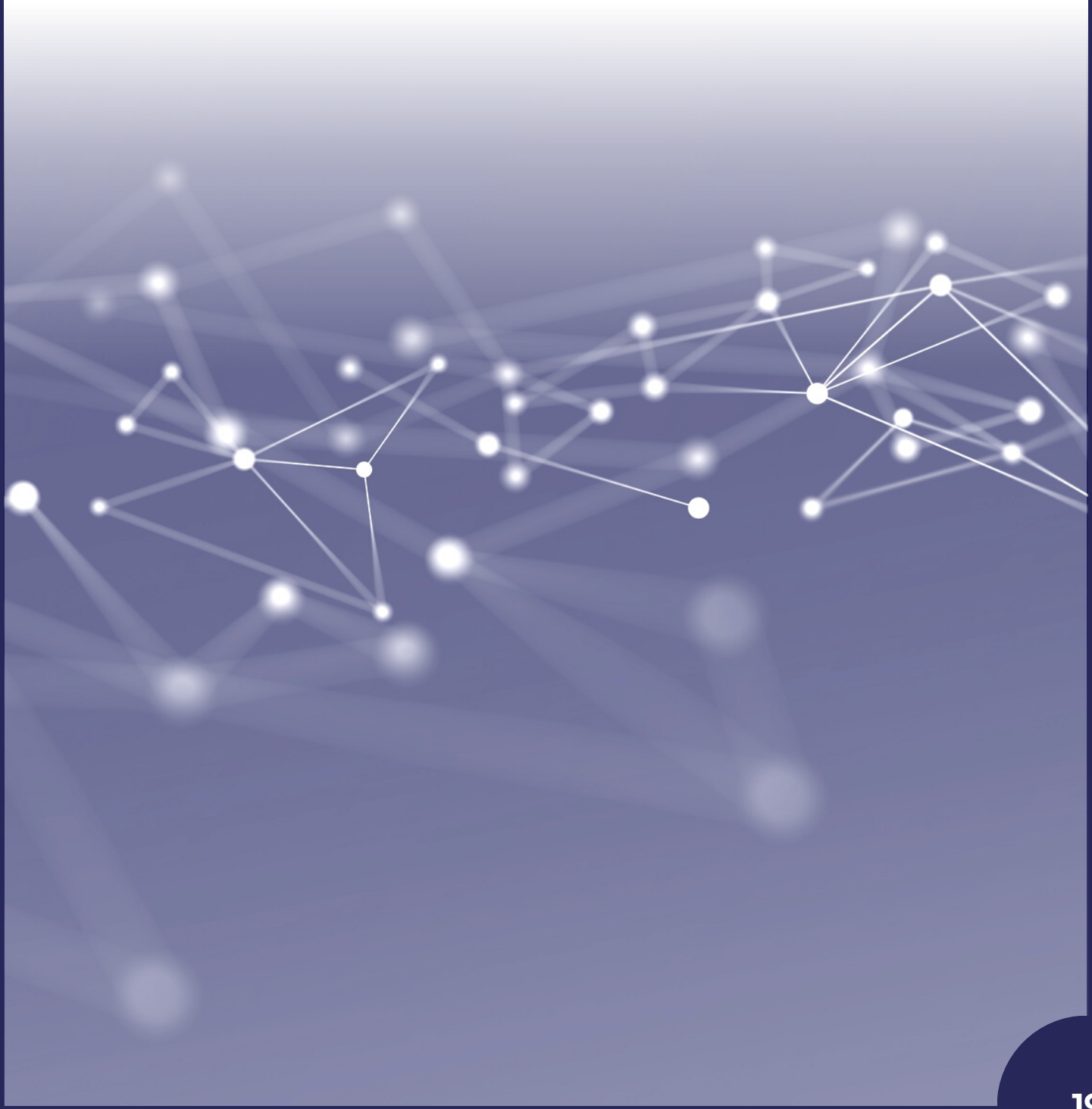
Isso ocorre porque, quando um cliente abre uma conta em uma exchange, as chaves privadas dessa conta ficam em poder da exchange, que se responsabiliza por realizar as operações em nome do cliente – e não em poder do próprio cliente.

Para receber depósitos em criptoativos, a exchange atribui a cada cliente um endereço no Blockchain. Após o criptoativo ser recebido nesse endereço de depósito individual do cliente, a exchange o transfere para endereços mais seguros dela mesma (cold wallets).

Já para enviar saques em criptoativos, a exchange usualmente agrupa saques solicitados por diversos clientes em uma única transação, que tem como origem endereços da exchange similares a contas bancárias de giro e como destino os endereços informados por cada cliente na sua solicitação.

Os endereços de saque da exchange devem possuir criptoativos suficientes para viabilizarem os saques solicitados pelos clientes e não se confundem com os endereços de depósito. Os endereços de depósito são individuais de cada cliente. Os endereços de saque, por sua vez, são comuns.

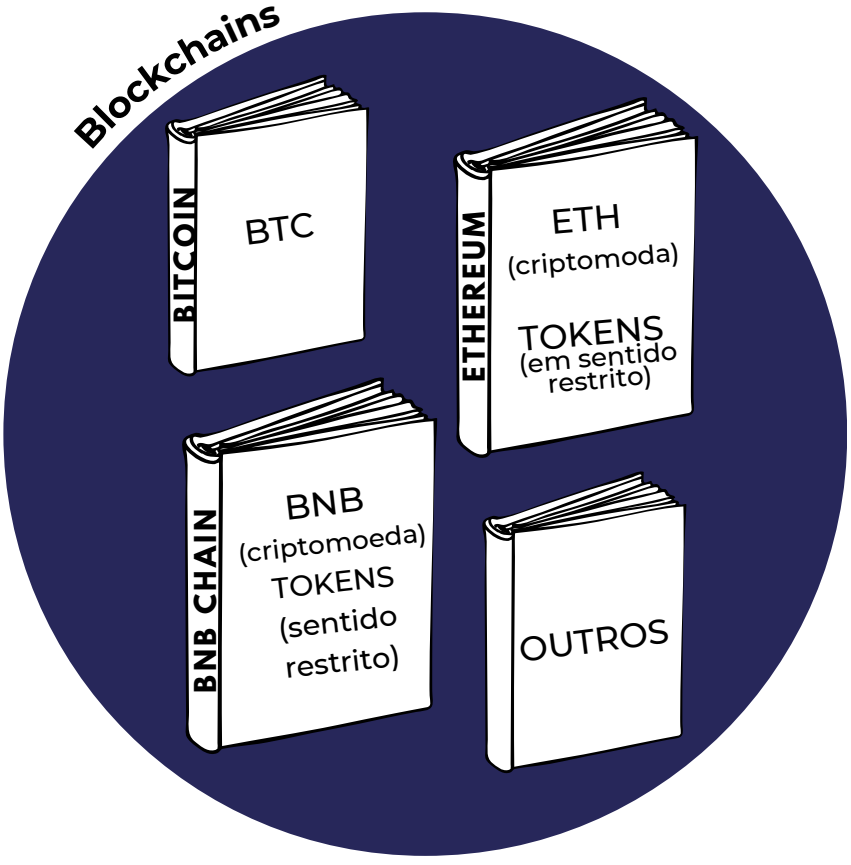
Daí a razão pela qual, para se identificar quais transações foram feitas pela exchange em nome de um determinado cliente não é suficiente olhar para o Blockchain. Torna-se necessário, também, acessar os dados e documentos de transação internos da exchange, espécie de "livro razão" da empresa. Para esse acesso, recomenda-se o modelo de afastamento do sigilo de transações específicas constante do anexo desse Roteiro (Minuta de Afastamento de Sigilo Telemático de Operações com Criptoativos no SIMBA).



PARA ALÉM DO BITCOIN:
BLOCKCHAINS PÚBLICOS E PSEUDÔNIMOS

No início havia apenas o Bitcoin. Um Blockchain com uma única espécie de criptoativo, o BTC, transacionável e empregado como meio de pagamento pelo uso da rede. Hoje existem diversos Blockchains, mantidos por redes diversas.

Há Blockchains que contam com muitos criptoativos transacionáveis, isto é, que podem ser enviados e recebidos. Contudo, em cada um deles, é possível identificar a sua criptomoeda, ou seja, o criptoativo no qual devem ser pagas as taxas de rede.



Blockchain	Criptomoeda	Demais criptoativos	Explorador de blocos
Bitcoin	Bitcoin (BTC)	-	Link
Ethereum	Ether (ETH)	USDT, UNI, ICP, CRV etc	Link
BNB Chain	BNB	BUSD, CAKE, USDT[4] etc	Link

Uma exceção digna de registro é o blockchain do Monero, cujo conteúdo não é publicamente acessível. Monero (XMR) é a criptomoeda desse Blockchain e o principal exemplo das chamadas "moedas de privacidade".[5]

Retomemos o exame dos Blockchains em geral. Apesar de serem públicos, eles são pseudônimos. Significa dizer que da sua simples visualização não é possível, em regra, saber quem são as pessoas envolvidas nas movimentações de criptoativos ali lançadas.

É que a identificação constante do livro não é nominal e sim pelo endereço público (algo como um número de conta). Em outras palavras, podemos facilmente consultar todas as movimentações feitas por determinadas contas, mas não saberemos, pela simples leitura do livro, quem são as pessoas por trás delas. Confira-se:

4 - Criptoativos homônimos podem existir em mais de um blockchain. Existe p. ex., o USDT no blockchain da Ethereum e o USDT na BNB Chain.

5- Moedas de privacidade não serão abordadas em detalhes nesta primeira versão do roteiro.

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... 0.00201913 BTC
358JVUtKdhaTdfKRY8RaHXm4saA... 3.02386829 BTC

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

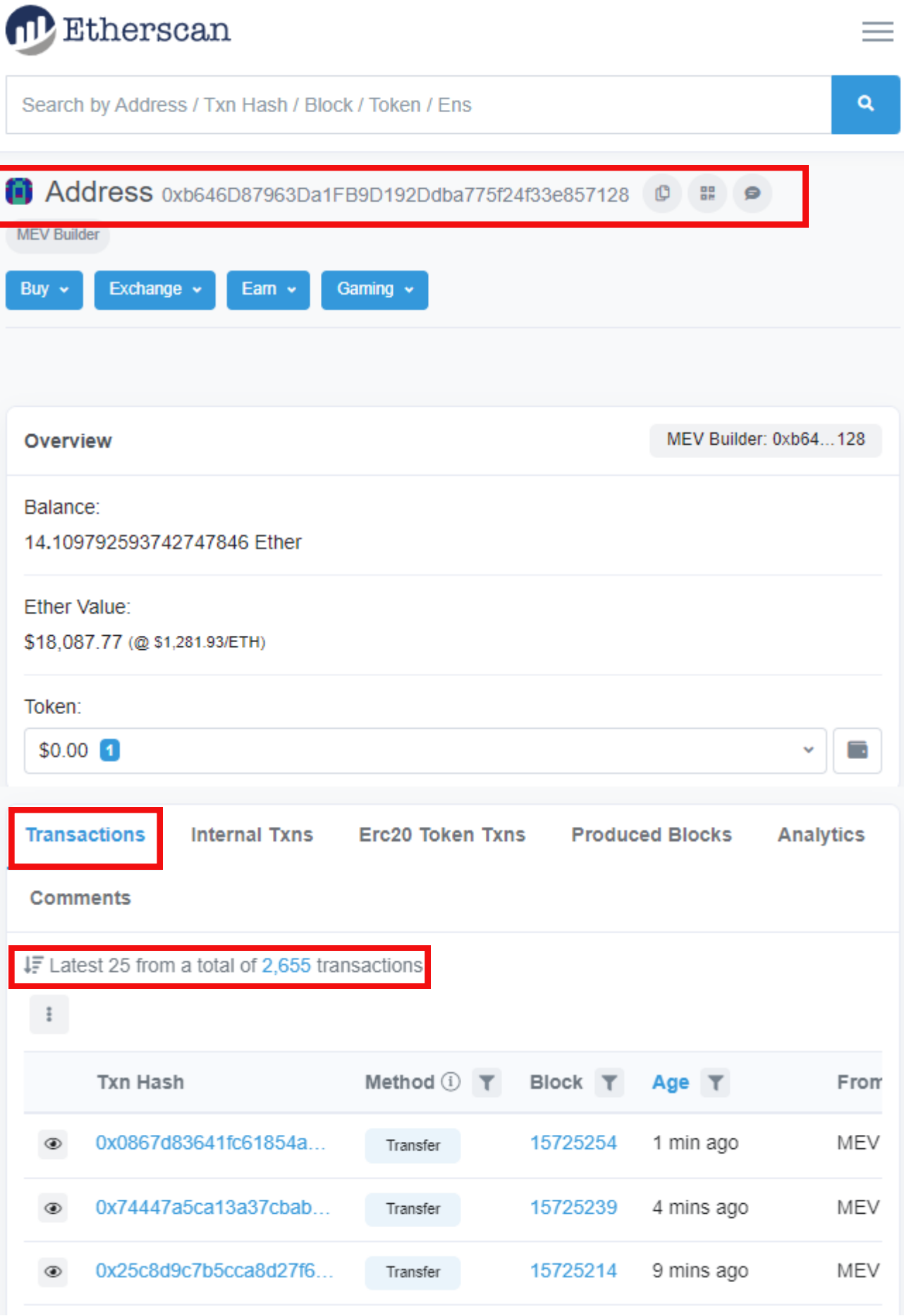
+3.02625922 BTC

Hash a045730dbc010368444ebb4df2aef11d063ee9035ffa3...

2022-10-11 13:06

bc1q5xutv5gr72t7f9cpjwea8rspx45... 3.10129645 BTC

bc1qxy08jgn8lm3kdpe2lh4zj9qgjs2... 0.07467063 BTC
bc1q84m06cqjj8xm77a9j72pz6245r... 3.02625922 BTC

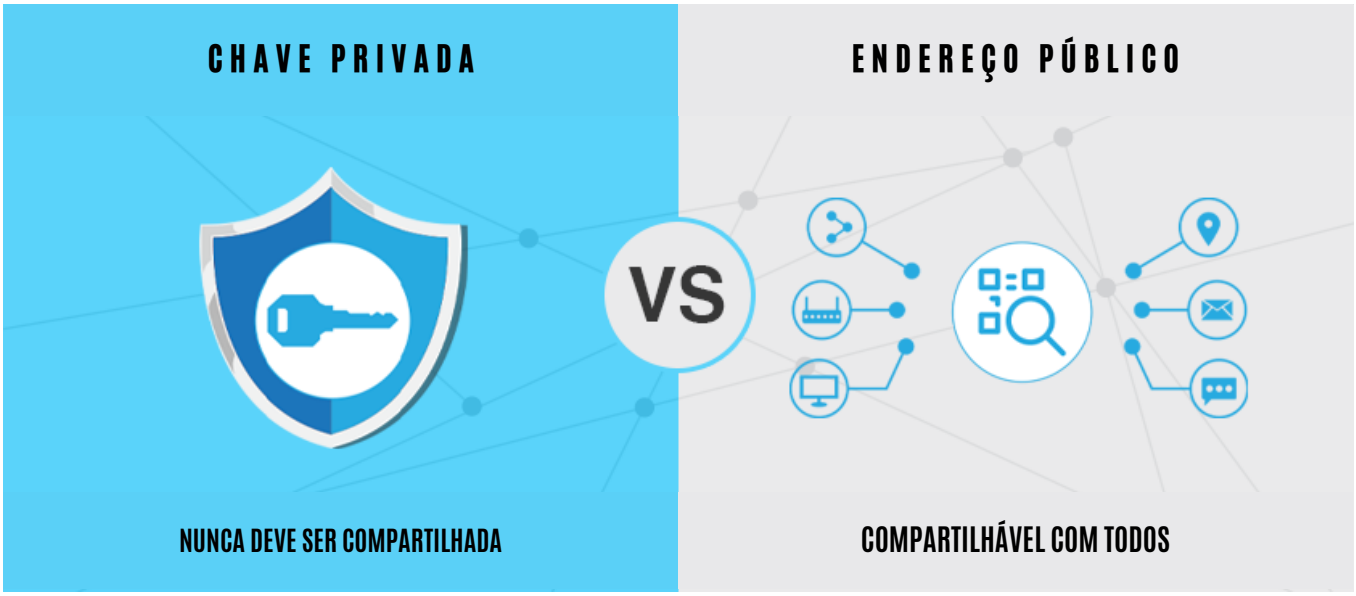

Etherscan
Search by Address / Txn Hash / Block / Token / Ens
Address 0xb646D87963Da1FB9D192Ddba775f24f33e857128
MEV Builder
Buy
Exchange
Earn
Gaming
Overview
MEV Builder: 0xb64...128
Balance:
14.109792593742747846 Ether
Ether Value:
$18,087.77 (@ $1,281.93/ETH)
Token:
$0.00 1
Transactions
Internal Txns
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

ARMAZENAMENTO DE CRIPTOATIVOS

Armazenar criptoativos significa possuir a chave privada que permite movimentá-los.

Para prosseguirmos, há dois termos que devem ser compreendidos: chave privada e endereço público, que formam um par, também chamado de conta. Uma conta de criptoativos nada mais é do que esse par.

Chave privada e endereço público mantém uma relação de correspondência biunívoca. Ou seja: para cada chave privada existe um único endereço público e para cada endereço público existe uma única chave privada.



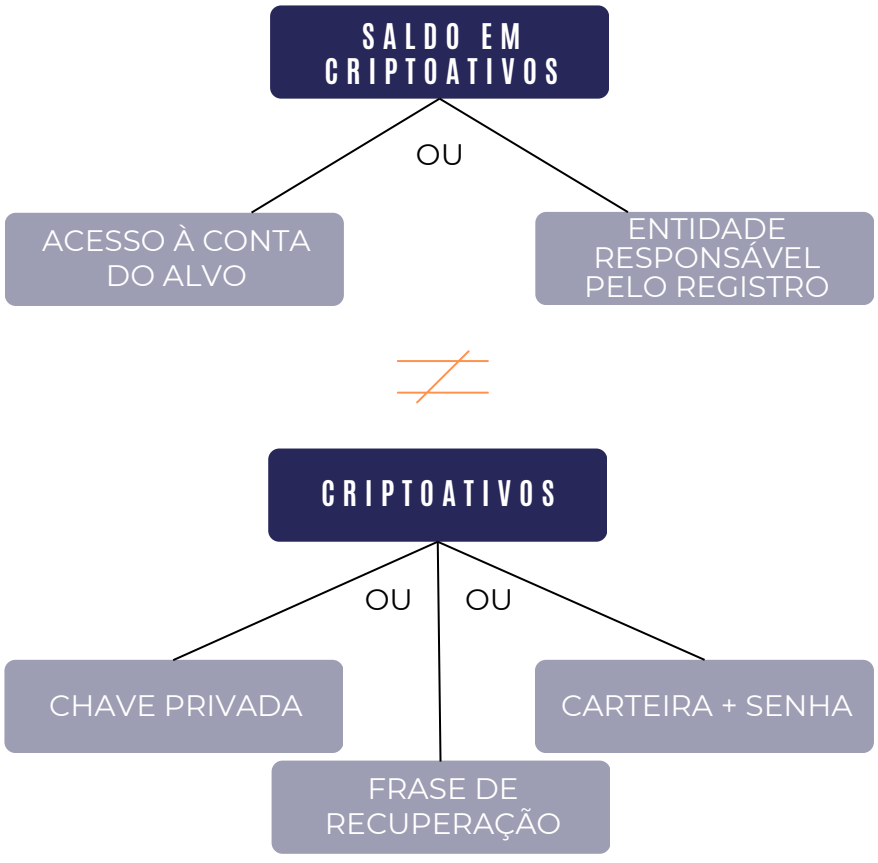
Pense na chave privada como sendo a chave da sua casa e no endereço público como sendo o seu endereço residencial. Considere, ainda, que essa chave privada tem duas particularidades: ela – e somente ela – abre uma porta que não pode ser arrombada e ela é uma chave que vem com o seu endereço nela anotado.

Disso resultam algumas consequências. Destaquemos duas delas. Divulgar o seu endereço público não lhe oferece risco algum de perda dos criptoativos, porque a porta não pode ser arrombada (primeira). Mas divulgar a sua chave privada permite que qualquer pessoa entre na sua casa e subtraia tudo o que de valor ali exista, porque com a chave se tem acesso ao endereço (segunda).

MOVIMENTAÇÃO DE CRIPTOATIVOS

Saldos em criptoativos, como lançamento em registros privados centralizados que são, podem ser movimentados e bloqueados por qualquer pessoa que disponha do acesso à conta do alvo (login + senha + eventuais fatores de múltipla autenticação) ou, mais facilmente, pela própria exchange ou empresa responsável pelo registro.

Criptoativos, por outro lado, podem ser movimentados por quem tenha acesso à chave privada da respectiva conta, à frase de recuperação de uma carteira ou à carteira em si mais a senha de acesso a ela.



Já tratamos da chave privada no tópico anterior. Agora passaremos aos conceitos de carteira, senha de acesso e frase de recuperação.

CARTEIRAS

Carteiras de criptoativos não são como carteiras de dinheiro. Carteiras de dinheiro armazenam dinheiro. Carteiras de criptoativos não armazenam criptoativos, mas sim as chaves privadas que permitem sejam eles movimentados.

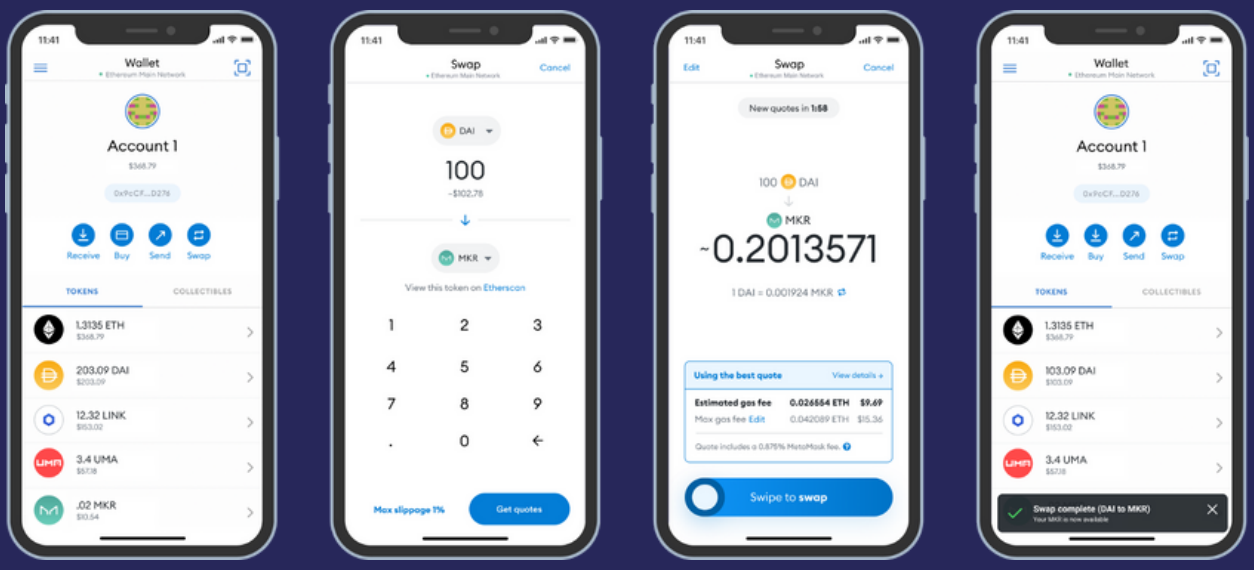
Carteira, neste contexto, também é um termo ambíguo e três sentidos nos importarão:

- carteira como o nome dado a um pedaço de papel (paper wallet), onde se encontrem anotados os dados de uma conta (chave privada e endereço público);

- carteira como o designativo de um dispositivo físico especificamente criado para a custódia de chaves privadas (hardware wallet); e

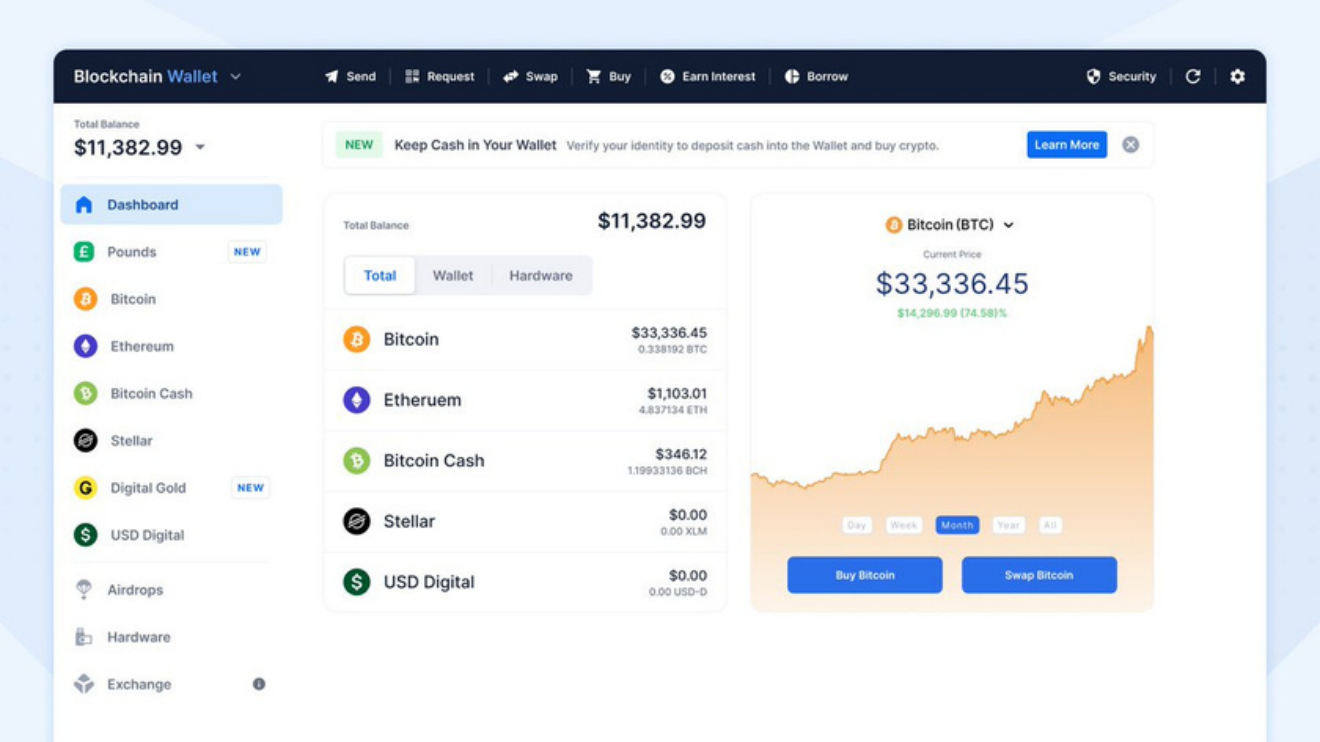
- carteira como o nome dado a um software que auxilia o usuário na guarda das suas chaves privadas e que pode ser executado online (webwallet), estar instalado no computador (desktop wallet) ou no celular (mobile wallet).

HARDWARE WALLET (TREZOR E LEDGER)

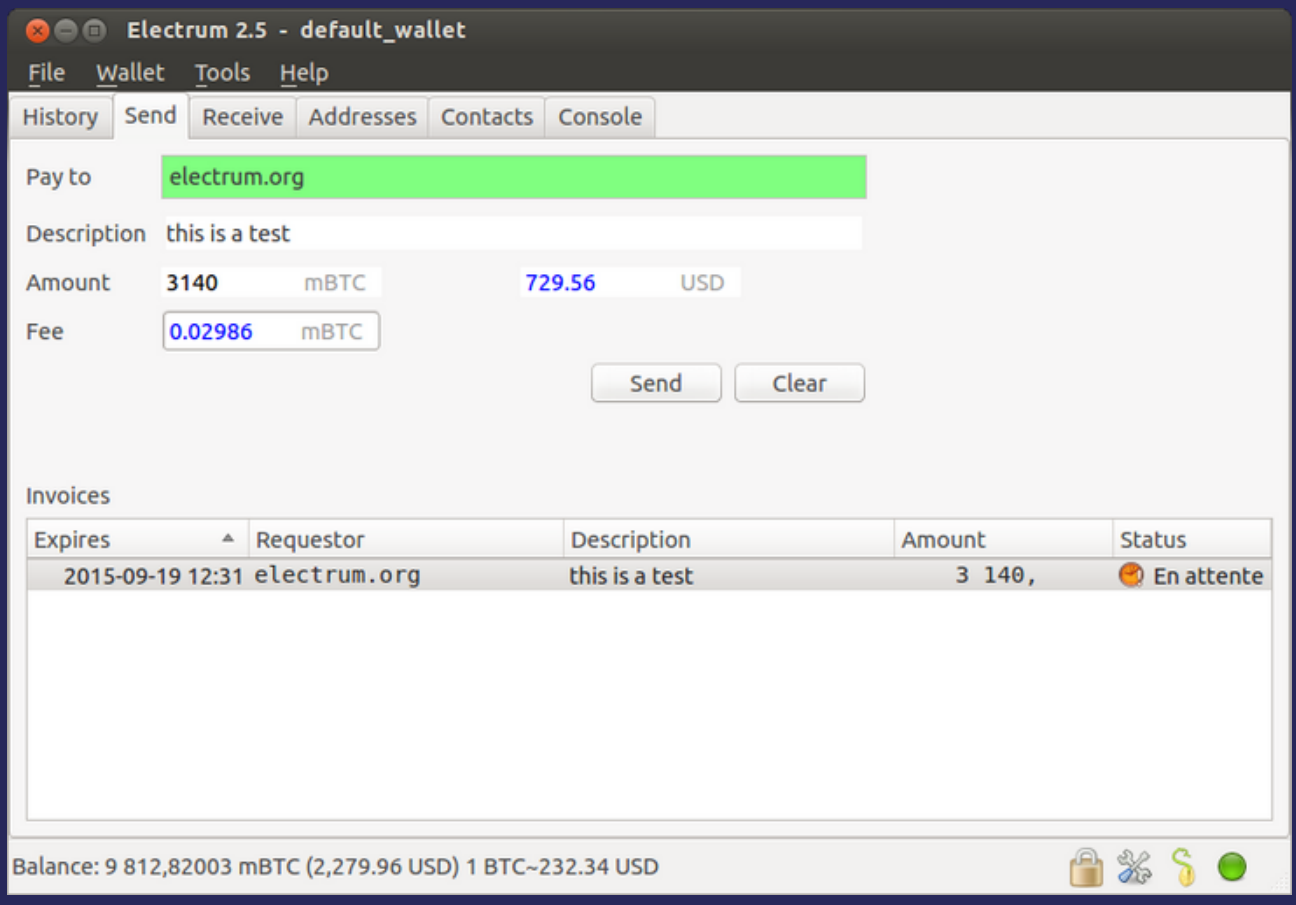


MOBILE WALLET

PAPER WALLET



WEB WALLET



DESKTOP WALLET

As carteiras de papel e as webwallets possuem contraindicações importantes. As primeiras porque só serão seguras se criadas e manejadas por alguém com conhecimento técnico profundo do assunto. As segundas porque armazenam as chaves privadas em nuvem, aumentando o risco de acesso não autorizado a elas.

As demais carteiras são diferenciadas, basicamente, pelo lugar onde ficam armazenadas as chaves privadas. Na hardware wallet as chaves privadas estão em um dispositivo físico específico.[6] Na desktop wallet, no computador. E na mobile wallet, no celular.

Senha de acesso (PIN)

Se sua carteira de dinheiro fosse furtada, você seguramente perderia o dinheiro que ali estivesse guardado. Todavia, se a sua carteira de criptoativos ou se o dispositivo onde ela está instalada fossem furtados, você não perderia os seus criptoativos, a menos que o criminoso soubesse a sua senha ou conseguisse quebrá-la.

Isso ocorre porque, para evitar acessos não autorizados, as carteiras de criptoativos armazenam as chaves privadas de forma criptografada. O que permite que elas sejam descriptografadas é a senha criada pelo usuário, também conhecida como PIN (personal identification number).

Em termos práticos, para a movimentação dos criptoativos de uma conta:

- quem tem a chave privada descriptografada, não precisa da senha;

6- Em adequado uso e funcionamento, as hardware wallets são o tipo mais seguro de carteira por duas razões. Em primeiro lugar, porque elas não permitem que as chaves ali armazenadas toquem em qualquer ambiente online. em segundo lugar, porque elas exigem o acionamento físico de um botão toda vez em que o usuário pretende realizar uma transação.

- quem tem a chave privada criptografada, precisa da senha;

- quem tem só a senha, não tem nada.

Frase de recuperação (seed phrase)

Uma única carteira normalmente compreende várias contas (três, oito, vinte...)[7] e a cada nova conta utilizada pelo usuário mais complexo se tornaria fazer um backup das suas respectivas chaves privadas.

Para contornar essa dificuldade, as carteiras fazem uso da "frase de recuperação" (seed phrase), que se apresenta como uma sequência aleatória de 12, 18 ou 24 palavras, dentre duas mil e quarenta e oito palavras da língua inglesa.

Se a chave privada é como a chave da sua casa, pense na frase de recuperação como um chaveiro com todas as suas chaves (a de casa, a do carro, a do gabinete etc). Ou seja, a frase de recuperação equivale a todas as suas chaves, permitindo a quem a possua ingressar em todos aqueles ambientes e retirar tudo o que ali encontre de valor. Tecnicamente, a frase de recuperação representa uma chave privada mestra (*private master key/ extended private key*) da qual todas as outras derivam.

7- A possibilidade de novas contas serem criadas em uma única carteira é praticamente inesgotável.

NEGOCIAÇÃO DE CRIPTOATIVOS

As duas principais formas de negociação de criptoativos são as seguintes:

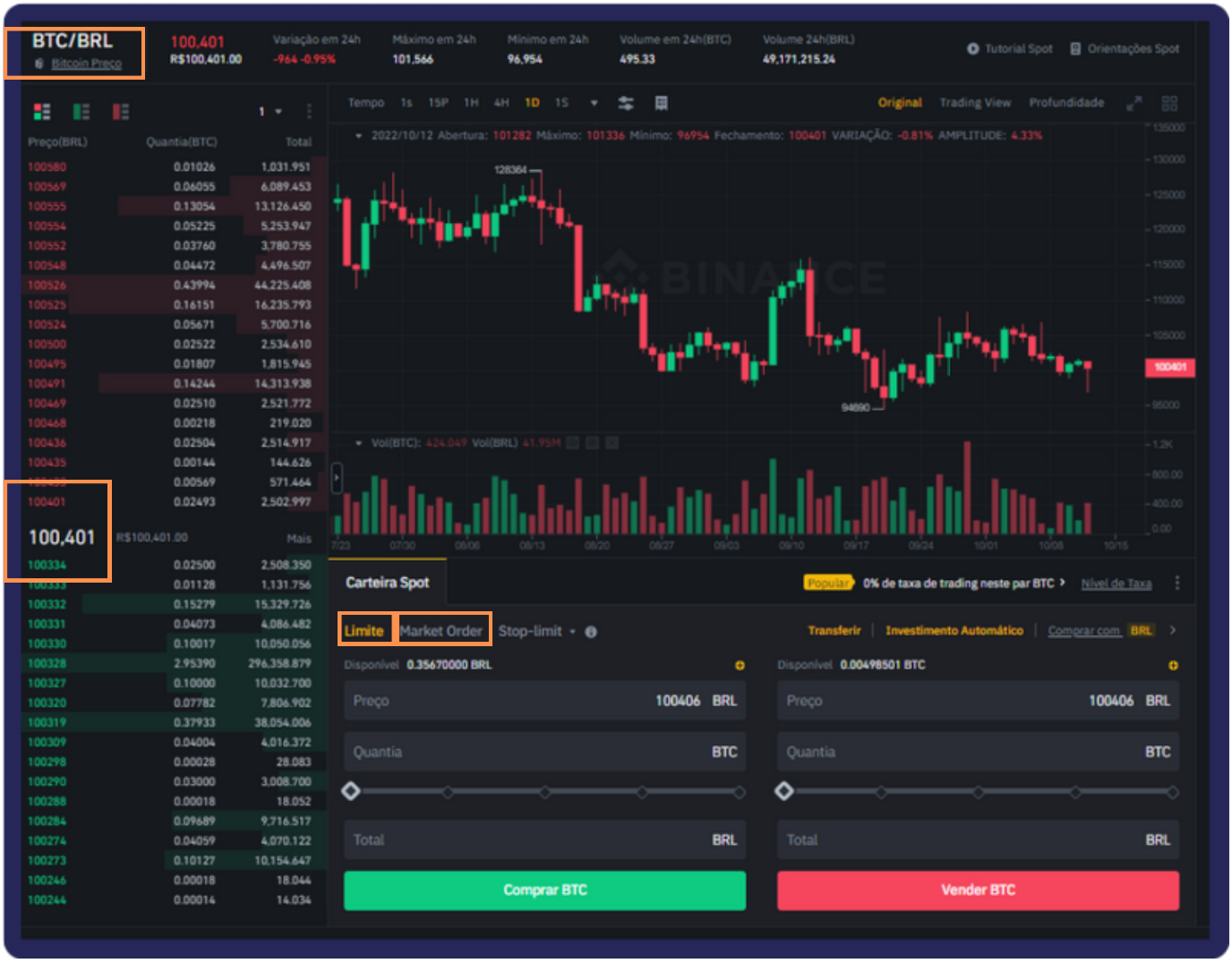
- peer to peer (P2P): negociações não intermediadas, feitas diretamente entre duas carteiras;

- em exchanges: negociações intermediadas, feitas através de livros de ofertas disponíveis em uma plataforma centralizada.

As primeiras transações ficam registradas no Blockchain, sendo, por isso, chamadas de onchain. Já as segundas são lançadas no registro privado da entidade responsável pela plataforma, podendo ser chamadas de offchain.

Livro de ofertas (book) é um instrumento de facilitação do encontro de pessoas com interesses contrapostos, em outras palavras, de quem quer comprar com quer vender determinado ativo. Ou, mais tecnicamente, de quem quer trocar A por B com que quer trocar B ou A, em quaisquer quantidades.

Reproduzimos adiante a imagem de um livro de ofertas para, depois disso, destacarmos alguns elementos desse livro.



1) **Par negociado:** um livro de ofertas sempre diz respeito a dois ativos. Neste caso, BTC e BRL, destinando-se, portanto, facilitar o encontro de quem quer trocar bitcoins por reais, vender, com quem quer comprar bitcoins.

2) **Ordem:** é a formalização de uma intenção.

Tipos de ordem:

- ordem de compra ou ordem de venda;

- ordem a mercado (market order) e ordem limite.

Um exemplo: Se eu quero comprar bitcoin, devo formalizar essa intenção por meio de uma ordem de compra. Se eu me disponho a pagar por ele o que melhor vendedor estiver pedindo,

independentemente do preço, a minha ordem será a mercado; já se eu estabeleço um preço máximo, acima do qual não desejo comprar, a minha ordem terá um limite.

Ordens a mercado são executadas imediatamente, independentemente do preço de mercado. Ordens limite, por outro lado, vão para o livro de ofertas (ordens de venda em vermelho e de compra em verde), onde aguardam o atingimento de um preço de mercado que satisfaça o limite estabelecido.

3) **Spread:** é a diferença entre a melhor ordem de venda e a melhor ordem de compra (100.401 – 100.334 = 67,00).

4) **Operação:** é o nome dado ao encontro de duas ordens contrapostas.

5) **Preço de mercado de um ativo:** é o preço correspondente ao da última operação (R$100.401,00).

LEI DE CRIPTOATIVOS BRASILEIRA

Ativos Virtuais

No final de 2022 foi promulgada no Brasil a primeira lei sobre o mercado de criptoativos. A Lei n. 14.478/22 dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais – nome adotado pela legislação para os criptoativos – e na regulamentação das prestadoras de tais serviços.

A nova lei brasileira considera ativo virtual: "a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento" (art. 3º). [8]

8- A definição de ativos virtuais dada pelo art. 3º da Lei n. 14.478/22 não é mesma adotada pela CVM no Parecer de Orientação n. 40/22. Lá, a CVM adotou o seguinte conceito de criptoativos: ativos representados digitalmente, protegidos por criptografia, que podem ser objeto de transações executadas e armazenadas por meio de tecnologias de registro distribuído (distributed ledger technologies, DLTs). Usualmente, os criptoativos (ou a sua propriedade) são representados por tokens, que são títulos digitais intangíveis. Os criptoativos costumam ser designados como tokens e podem desempenhar diversas funções. A CVM adota a abordagem funcional para enquadramento dos tokens em taxonomia que servirá para indicar o seu tratamento jurídico: Token de Pagamento (cryptocurrency ou payment token): busca replicar as funções de moeda, notadamente de unidade de conta, meio de troca e reserva de valor; Token de Utilidade (utility token): utilizado para adquirir ou acessar determinados produtos ou serviços; e Token referenciado a Ativo (asset-backed token): representa um ou mais ativos, tangíveis ou intangíveis. São exemplos os security tokens, as stablecoins, os non-fungible tokens (NFTs) e os demais ativos objeto de operações de tokenização. Dessa classificação adotada pela CVM, apenas os itens i e iii podem desempenhar "a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento" (art. 3º, Lei n. 14.478/22). São esses aqueles tokens que pode, pela nova lei, serem considerados ativos virtuais.

O mesmo dispositivo determina que não são ativos virtuais:

- **A moeda nacional** (o Real, art. 1º, Lei n. 9.069/95[9]) e as demais moedas estrangeiras, tais como euro, dólar etc;

- **A moeda eletrônica**, definida na Lei nº 12.865/13 como recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento (art. 6º, inciso VI), tais como operações com cartões de crédito e débito, cartões pré-pagos e transações via telefone celular etc. Tais transações são intermediadas por instituições de pagamento, integrantes do Sistema de Pagamentos Brasileiro e do mercado de crédito do Sistema Financeiro Nacional, supervisionadas pelo BACEN e reguladas pelo Conselho Monetário Nacional;

- Instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de **pontos e recompensas de programas de fidelidade**; e

- Representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de **valores mobiliários e de ativos financeiros**[10]. Essa norma é complementada pelo parágrafo único do art. 1º da Lei n. 14.478/22, que exclui da nova lei de criptoativos os ativos representativos de valores mobiliários (Lei nº 6.385/76), não alterando a competência da CVM.

9- Interessante notar que a conformação que o BACEN deu ao **Real Digital**, espécie de moeda digital de banco central (*Central Bank Digital Currency*, CBDC) que possui o mesmo lastro da moeda fiduciária, também a afastaria do conceito de ativo virtual aqui tratado. Ver mais em https://www.bcb.gov.br/estabilidadefinanceira/real_digital.

10- Ativos financeiros constituem bens ou direitos que uma empresa ou pessoa possui e que podem gerar rendimentos, tais como ações, dinheiro, títulos públicos, fundos de investimento, certificados de depósito bancário etc.

Prestadoras de Serviços de Ativos Virtuais

São **Prestadoras de Serviços de Ativos Virtuais – PSAVs** as pessoas jurídicas que executam, em nome de terceiros, pelo menos um dos serviços de ativos virtuais (art. 5º). São as empresas atualmente designadas de **corretoras** ou **exchanges**.

São **serviços de ativos virtuais** definidos na nova legislação:

- A troca entre ativos virtuais e moeda nacional ou moeda estrangeira;
- A troca entre um ou mais ativos virtuais;
- A transferência de ativos virtuais;
- A custódia ou administração de ativos virtuais ou de instrumentos que possibilitem controle sobre ativos virtuais – tais como as chaves privadas de correntistas; ou
- A participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda de ativos virtuais.

Entidade da Administração Pública federal, indicado em ato posterior do Poder Executivo, poderá autorizar a realização de **outros serviços** que estejam, direta ou indiretamente, relacionados à atividade da prestadora de serviços de ativos virtuais.

A Lei n. 14.478/22 submete os PSAVs a importantes leis nacionais ao estabelecer que sua atividade deve observar as seguintes diretrizes, especificadas em ato do órgão federal (art. 4º):

- A livre iniciativa e livre concorrência;
- Boas práticas de governança, transparência nas operações e abordagem baseada em riscos. Esta última, abre espaço para a tendência internacional de regulação defendida pelo FATF/GAFI;

- Segurança da informação e proteção de dados pessoais, remetendo às normas da Lei Geral de Proteção de Dados (Lei n. 13.709/2018);

- Proteção e defesa de consumidores e usuários. A norma é complementada pelo art. 13 da nova lei, ao expressamente estabelecer que as operações conduzidas no mercado de ativos virtuais estarão submetidas, no que couber, ao Código de Defesa do Consumidor (Lei n. 8.078/90);

- Proteção à poupança popular;

- Solidez e eficiência das operações; e

- Prevenção à lavagem de dinheiro (Lei n. 9.613/98) e ao financiamento do terrorismo (Lei n. 13.260/16) e da proliferação de armas de destruição em massa, em alinhamento com os padrões internacionais.

Regulação Federal

Competirá a órgão ou entidade da Administração Pública federal, definido em ato futuro do Poder Executivo, estabelecer quais serão os ativos financeiros regulados, para fins da Lei n. 14.478/22. Esse mesmo órgão deterá o poder de previamente autorizar a funcionar no Brasil as PSAVs, além de estabelecer as hipóteses em que a autorização poderá ser concedida em procedimento simplificado. O art. 6º prevê que ato do Poder Executivo atribuirá a um ou mais órgãos ou entidades da Administração Pública federal a disciplina do funcionamento e a supervisão dos PSAVs.

O art. 8º prevê que as instituições autorizadas a funcionar pelo BACEN poderão prestar exclusivamente o serviço de ativos virtuais ou cumulá-lo com outras atividades, na forma da regulamentação a ser editada por órgão ou entidade da Administração Pública federal indicada em ato do Poder Executivo federal.

Ademais, compete ao órgão ou à entidade reguladora indicada em ato do Poder Executivo Federal (art. 7º):

- Autorizar funcionamento, transferência de controle, fusão, cisão e incorporação de PSAVs;

- Estabelecer condições para o exercício de cargos em órgãos estatutários e contratuais em PSAVs e autorizar a posse e o exercício de pessoas para cargos de administração;

- Supervisionar as PSAVs e aplicar as disposições da Lei nº 13.506/2017 (que trata sobre o processo administrativo sancionador do BACEN e da CVM), em caso de descumprimento da Lei n. 14.478/22 ou de sua regulamentação;

- Cancelar, de ofício ou a pedido, as autorizações das PSAVs; e

- Dispor sobre as hipóteses em que os serviços de ativos virtuais do art. 5º serão incluídos no mercado de câmbio ou em que deverão se submeter à regulamentação de capitais brasileiros no exterior e capitais estrangeiros no País.

Após a sua entrada em vigor, a Lei n. 14.478/22 ainda prevê um subsequente prazo para que as PSAVs se ajustem à regulamentação. Esse prazo será definido pelo órgão federal a ser designado, mas não será inferior a seis meses (art. 9º).

Dispositivos Penais e Normas Complementares

O art. 10 da Lei n. 14.478/22 introduz no Código Penal o art. 171-A, nova forma de estelionato: **“Fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros”.**

Art. 171-A. Organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam ***ativos virtuais, valores mobiliários ou quaisquer ativos financeiros*** *com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento.*

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

A Lei n. 14.478/22 também modifica o parágrafo único do art. 1º da Lei nº 7.492/86 para dele fazer constar o seguinte:

Art. 1º Considera-se instituição financeira, para efeito desta lei, a pessoa jurídica de direito público ou privado, que tenha como atividade principal ou acessória, cumulativamente ou não, a captação, intermediação ou aplicação de recursos financeiros (Vetado) de terceiros, em moeda nacional ou estrangeira, ou a custódia, emissão, distribuição, negociação, intermediação ou administração de valores mobiliários.

Parágrafo único. Equipara-se à instituição financeira:

I - a pessoa jurídica que capte ou administre seguros, câmbio, consórcio, capitalização ou qualquer tipo de poupança, ou recursos de terceiros;

I-A – a pessoa jurídica que ofereça serviços referentes a operações com ativos virtuais, inclusive intermediação, negociação ou custódia;

II - a pessoa natural que exerça quaisquer das atividades referidas neste artigo, ainda que de forma eventual.

Com isso, os PSAVs passam a ser instituições financeiras por equiparação e se submetem a todos os crimes contra o SFN da Lei nº 7.492/86.

As normas antilavagem de dinheiro trazidas pela nova legislação serão analisadas no tópico seguinte.

Por fim, a Lei n. 14.478/22 alterou a Lei Antilavagem para nela incluir o art. 12-A, dispondo sobre a criação do Cadastro Nacional de Pessoas Expostas Politicamente (CNPEP), disponibilizado pelo Portal da Transparência.

A partir de sua vigência, os órgãos e as entidades de quaisquer Poderes da União, dos Estados, do Distrito Federal e dos Municípios deverão encaminhar ao gestor CNPEP, na forma e na periodicidade definidas em regulamento, informações atualizadas sobre seus integrantes ou ex-integrantes classificados como pessoas expostas politicamente (PEPs) na legislação e regulação vigentes. O órgão gestor do CNPEP indicará em transparência ativa, pela internet, órgãos e entidades que deixem de cumprir a obrigação.

As pessoas referidas obrigadas pelo Sistema Antilavagem incluirão consulta ao CNPEP entre seus procedimentos para cumprimento das obrigações previstas nos arts. 10 e 11 da Lei Antilavagem, sem prejuízo de outras diligências exigidas na forma da legislação. § 3º

INVESTIGAÇÃO FINANCEIRA DE CRIMES ENVOLVENDO CRIPTOATIVOS

O emprego do sistema financeiro por criminosos para transferir, guardar ou dissimular o lucro do crime desafia os órgãos de investigação do Estado a coletarem, analisarem e apresentarem provas das movimentações financeiras usadas para tal desiderato, como forma de robustecerem e possibilitarem a persecução penal perante o Poder Judiciário e a recuperação dos ativos envolvidos.

Como método investigativo, a Investigação Financeira se detém sobre os assuntos financeiros relacionados à conduta ilícita, intentando identificar e documentar, para fins de prova, o movimento de dinheiro durante o curso da atividade criminal[11]. Dito de outra forma, a Investigação Financeira é um método que procura conectar pessoas a outras pessoas, locais e eventos através de fatos financeiros[12]. Tal tipo de investigação gira em torno do conceito de dado financeiro, que representa as informações ligadas a dinheiro, ativos, despesas e finanças, presente em quase todos os aspectos da vida de uma pessoa.

Esses dados financeiros foram desmaterializados desde o início da década de 2010, na esteira da crise financeira global de 2008, a partir da migração das relações financeiras tradicionais para meios digitais e do advento de um **criptomercado** paralelo aos sistemas financeiros nacionais.

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.

Os criptoativos representam a mais importante faceta desse dinheiro imaterial, constituído, ao fim e ao cabo, por bits no sistema computacional de alguém, aproximando a investigação financeira de uma investigação informática e exigindo intercessões importantes entre os sigilos financeiros e o sigilo que recobre alguns vestígios digitais.

Como ativo patrimonial, a investigação financeira de crimes envolvendo criptoativos se desenvolve por meio da **mesma metodologia de investigação patrimonial** empregada pelo Ministério Público Federal para rastreio de outros ativos, tal como exposta no Roteiro de Persecução Patrimonial e Administração de Bens elaborado por grupo de trabalho instituído pelas 2ª e 5ª Câmaras de Coordenação e Revisão.[13]

Se a metodologia de investigação é a mesma, as ferramentas tecnológicas empregadas para rastreio patrimonial (busca remota e busca presencial) e as particularidades envolvidas no sequestro e administração dessa espécie de bem demandaram a elaboração de um roteiro de atuação apenas voltados a criptoativos.

METODOLOGIA DE RASTREIO PATRIMONIAL

Utiliza-se o termo Investigação Financeira para o complexo de atividades de coleta, análise e uso de informações financeiras pelos órgãos de aplicação da lei. Embora este documento apresente uma sugestão metodológica para a realização da investigação financeira, parece certo que as medidas adequadas a cada caso devem ser determinadas pelo próprio caso. Somente ele exige as medidas necessárias ao seu próprio sucesso – e esta talvez represente a regra de ouro de qualquer escorço investigativo.[14]

13- BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. Roteiro de Atuação – Persecução Patrimonial e Administração de Bens, 2017. Disponível em: 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. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. Temas Processuais, Prova e Persecução Patrimonial, 2019. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea-de-artigos-temas-processuais-prova-e-persecucao-patrimonial.

Em todo caso, os investigadores financeiros precisam ter em mente que eles devem pacientemente "seguir o dinheiro" (follow the money); nos crimes aqui tratados, se o dinheiro não é seguido, o crime compensa.[15]

Não obstante as dificuldades decorrentes do fluxo globalizado e instantâneo de ativos na contemporaneidade, deve-se sempre ter em mente que o patrimônio é o objetivo do crime praticado. Assim, os criminosos gostam de manter algum grau de controle sobre seus ativos e, como resultado, há geralmente uma "trilha de papel" (paper trail) que pode conduzir a investigação de volta ao infrator. Essa trilha de papel também pode ser seguida para identificar os infratores adicionais e a localização de provas e instrumentos utilizados para cometer os crimes.[16]

Investigadores financeiros desenvolvem hipóteses baseadas em informações disponíveis. A hipótese imaginada determina a extensão e o tipo de informação exigida para provar o seu mérito. Identificar o tipo de informação necessária permite ao investigador determinar onde essas informações estão guardadas (se em fontes abertas ou fechadas, por exemplo). Uma vez que o investigador determinou que informação é necessária e onde ela está armazenada, ele pode prever os métodos e desafios na obtenção da informação (por exemplo, acesso direto a bancos de dados públicos, acesso mediante requisição direta, quebra de sigilos judicial etc). Assim, ele implementa um plano de coleta de dados que leva à obtenção bem-sucedida de informações necessárias à prova da hipótese.[17]

Esse raciocínio pode ser apresentado pelo seguinte gráfico:[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.


Plano de Coleta de Dados
1
Desenvolver a hipótese a partir das evidências disponíveis;
2
Identificar o tipo de informação (evidência) a ser coletada;
3
Identificar o repositório dessas informações (fontes abertas ou fechadas);
4
Identificação do método de coleta
5
Realizar a coleta do dado.

A metodologia para coleta de informações financeiras é baseada em fase sigilosa, encetada para permitir a adoção de medidas de coleta da informação sem o conhecimento do alvo, máxime em decorrência da real possibilidade de rápida dissipação patrimonial e destruição de provas por modernos meios tecnológicos; e em fase ostensiva, na qual essa precaução não se faz mais necessária, v.g., por não ter sido localizado nenhum ativo na fase sigilosa ou por a previsão de que os bens a serem descobertos por medidas adotadas na fase ostensiva compensem o descarte da surpresa das medidas de constrição cautelares.

No início da fase sigilosa, grande parte dos dados se encontram em fontes abertas de informação. Toda investigação começa devagar e toma fôlego a medida que informações e dados vão sendo acumulados[19]. Para a reunião dessas informações, o investigador lança mão primeiro das chamadas fontes abertas (open sources), consistentes em toda a informação publicamente disponível através da internet, mídias sociais, mídia impressa e eletrônica, bem como os registos mantidos por órgãos públicos ou por órgãos privados, mas de acesso ao público[20].

Não é a intenção desse trabalho sobre criptoativos, que apenas relembra conceitos metodológicos sobre investigação patrimonial, descrever as fontes de pesquisa abertas, mas tão somente apresentar a sua existência e utilidade no contexto da Investigação Financeira. Para consulta às fontes abertas no Brasil e no exterior, recomenda-se a consulta ao Roteiro de Persecução Patrimonial e Administração de Bens, capítulo III, itens 4 e 5.

Com a reunião das informações contidas em fonte aberta, pode-se buscar acesso a fontes fechadas, entendidas como aquelas a que o investigador não tem acesso, via pesquisa direta ou requisição, sem necessidade de intervenção judicial. As fontes fechadas são normalmente identificadas como sujeitas a sigilo legal, tais como os dados bancários, fiscais, telefônicos, telemáticos etc.

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

No MPF, os modelos adotados para acesso a dados financeiros e fiscais se encontram nas minutas do Sistema de Investigação de Movimentações Bancárias – **SIMBA**[21] e da Sistemática de Investigação Fiscal – **SIFISCO**[22], ao passo que o recebimento de dados telefônicos, acaso interessem à investigação, podem ser recebidos no Sistema de Investigação de Registros Telefônicos – **SITTEL**[23]. Por sua vez, os modelos de pedidos de afastamento de sigilo de dados telemáticos se encontram compiladas no portal e-Evidence, mantido pelo Grupo de Apoio à Criminalidade Cibernética.[24]

A sequência apresentada de coleta de dados em fontes abertas para depois seguir para as fontes fechadas foi adotada apenas para fins didáticos. O que ocorre na prática, em verdade, é uma retroalimentação das fontes. Isso porque informações voltam a ser coletadas em meio aberto a medida que novas informações são trazidas pelas fontes fechadas e vice-versa.

Com a coleta dessas fontes de prova, pode convir ao caso a realização de uma fase ostensiva com interrogatórios dos alvos, de seus familiares, associados formais ou informais, busca e apreensão em sua residência (art. 240, § 1º, b e h, CPP), em suas empresas, escritórios, apreensão de computadores para perícia, apreensão de livros contábeis para auditoria etc.

FERRAMENTAS PARA RASTREIO PATRIMONIAL DE CRIPTOATIVOS

Conforme metodologia apresentada no Roteiro de Persecução Patrimonial do MPF, o rastreio de criptoativos se inicia, normalmente, com a consulta a fontes abertas de registro das transações, que possuem relevada importância no contexto de criptoativos que adotem um livro razão público.

21- Disponível em https://portal.mpf.mp.br/simba/php/Simba.php.

22- Disponível em https://portal.mpf.mp.br/portaldedados/.

23- Disponível em https://portal.mpf.mp.br/sittel/.

24- Disponível em https://portal.mpf.mp.br/eevidence/.

- **Fontes Abertas**[25]

Evidentemente, as fontes abertas indicadas no Roteiro de Persecução Patrimonial do MPF continuam sendo importantes para o rastreio patrimonial de investigados que operam com criptoativos. Por meio de pesquisas em fontes abertas, tais como redes sociais, pode-se obter dados importantes que, em conjunto com os demais elementos de prova obtidos com outras fontes abertas (gerais ou específicas para criptoativos) ou fontes de prova fechadas revelam-se úteis para a investigação.

Com o delimitado objeto do presente documento, segue a descrição das ferramentas de pesquisa específicas para criptoativos.

- **Fontes Abertas Disponíveis na Web**

Em primeiro lugar, é importante que o investigador possua conhecimento sobre o **modelo de negócio do criptoativo** investigado, cujas carasterísticas técnicas e limitações práticas possuem importância redobrada na investigação. Para cada criptoativo, normalmente há um site específico com a descrição geral do seu funcionamento e acesso ao livro razão público. Ex: Ethereum (ethereum.org/pt-br/), Monero (monero.inf.br/) etc. Para uma visão ampla das criptomoedas existentes e continuamente criadas, pode-se consultar, por exemplo, o site mantido pela empresa CoinMarketCap (http://www.coinmarketcap.com).

Uma das principais ferramentas de fontes abertas usadas para investigações são aquelas que exploram a tecnologia de Blockchain pública subjacente à maioria dos criptoativos. De fato, **a análise de Blockchain** permite que investigadores identifiquem relacionamentos e fluxos financeiros entre carteiras, com vistas a pesquisar endereços, valor das transações, carteiras remetentes e destinatárias, e outros detalhes relacionados a uma transação. Essa análise não está associada ao nome de uma pessoa física, mas indica

25- Contribuiu para o teste das ferramentas de fontes abertas sobre criptoativos, a servidora Adriana Shimabukuro, membro do GT de Criptoativos instituído pela SPPEA/PGR.

um grande nível de detalhe sobre a carteira e sua movimentação e, às vezes, analisar as transações pode subsidiar hipóteses de que carteiras recorrentes pertencerem ao mesmo investigado[26]. A análise de Blockchain, combinada com outras fontes abertas e fechadas, representam, quase sempre, o primeiro passo em uma investigação com criptoativos.[27]

Sites como o **Blockchain** *(www.Blockchain.com/explorer)* permitem busca por o número de uma carteira de Bitcoin, Ethereum e Bitcoin Cash[28], mostrando o número de transações a ela vinculada, o total de ativos recebido, saldo final e um completo histórico de transações, permitindo rastrear cada entrada ou saída de ativos da carteira. Para ferramenta com outras opções de criptos, há **Blockchair** *(https://blockchair.com/pt)*, **Coin Market** *(https://Blockchain.coinmarketcap.com/)*, **OXT** (*https://oxt.me/)*, **Trade Block** *(https://tradeblock.com/home)*, dentre outros.

Além das transações em si, pode ser importante para uma investigação identificar qual foi o **minerador** do bloco de Blockchain. Atualmente, os mineradores são empresas com grande capacidade computacional, que, por vezes, representam o conjunto de vários mineradores individuais (pool de mineração)[29]. Como os participantes recebem a sua parte da recompensa do pool e o bloco minerado pode ser identificado, as empresas de mineração podem cooperar com eventuais investigações indicando, por exemplo, a qual

26- A análise de Blockchain pode ser dificultada pelo investigado com o emprego de técnicas de mixer (tumbler, fogger ou blender) que podem ser contratadas como serviços de um terceiro ou apenas com um software. Essas técnicas combinam entradas e saídas de muitos usuários diferentes para uma mesma carteira ou conjunto de carteiras, de modo a dificultar o rastreio das transações. Quando contratados a uma empresa, taxas são cobradas e, normalmente, não são mantidos os registros de usuários contratantes. Nesse link são descritos alguns dos mais famosos mixing services de criptoativos: https://beincrypto.com/learn/best-bitcoin-mixers/. Alguns criptoativos foram desenhados para já constar com mixers integrados, tais como Dash e Monero (https://monero.inf.br/tecnologia-de-privacidade-do-monero/).

27- Por não possuir informações completamente intuitivas, o investigador precisa ter um conhecimento do modelo de negócio do criptoativo que está rastreando, sob pena de interpretar erroneamente os resultados do rastreamento do Blockchain e perder detalhes importantes relacionados a um caso.

28- Além de operações com NFTs: https://www.Blockchain.com/pt/nfts.

29- No contexto da mineração de criptomoeda, um pool de mineração é o aglomerar de recursos por parte dos mineradores individuais, que compartilham o seu poder de processamento numa rede, para dividir a recompensa de forma igual e de acordo com a quantidade de trabalho com que cada um contribuiu para a fixação de blocos de transações.

integrante do pool remunerou pela mineração de determinado bloco. Na maioria das transações, é simples identificar o minerador do bloco pois os seus nomes (ou os nomes dos pools ou empresas) são muitas vezes "etiquetados" aos blocos e já constam das ferramentas acima descritas para análise das carteiras.

Para o monitoramente de carteiras com o recebimento de avisos via e-mail, há os serviços prestados pela **Cryptocurrency Alerting** *(https://cryptocurrencyalerting.com/)*, gratuito até três alertas, e **Blockonomics** *(https://www.blockonomics.co/)*.

A ferramenta Wallet Explorer (www.walletexplorer.com) fornece a informação histórica sobre outros endereços possuídos por uma só carteira virtual, vincula endereços de Bitcoin a entidades conhecidas, incluindo exchanges, "pools" de mineração, páginas de jogos, carteiras ou darknet.[30] Descontinuada em 2016, sua metodologia foi incorporada à ferramenta comercial da empresa Chainalysis, adiante descrita.

A **Wallet Explorer** permanece, até hoje, como uma ferramenta poderosa, especialmente para aqueles órgaos de investigação que não têm acesso a uma alternativa comercial mais sofisticada, especialmente se através dos dados apresentados pela plataforma for identificada relação com alguma exchange ou outra entidade que possa identificar, ainda que com dados históricos, o proprietário da carteira.

Com produto semelhante e gratuito, mas limitado a trinta consultas, há a solução da empresa **Crystal Explorer** *(https://explorer.crystalBlockchain.com)*.

30- O Wallet Explorer agrupa endereços em carteiras, reunindo principalmente endereços de entrada de múltiplas transações e de troco. Depois de grupos de determinada dimensão serem identificados, é necessário que, pelo menos, um dos seus endereços seja identificado através de reconhecimento passivo ou ativo. Um endereço identificado no grupo seria suficiente, em princípio, para identificar todos os endereços restantes como pertencentes a esse grupo.

O site **Bitcoin Who's Who** *(www.bitcoinwhoswho.com)* fornece mais informações sobre alguma carteira suspeita, tais como se ela foi envolvida com crimes virtuais a partir de informações públicas. Pode-se identificar o endereço de IP da transação, embora ele normalmente esteja encoberto por alguma VPN. A ferramenta **Bitcoin Abuse** (*www.bitcoinabuse.com)* informa ao usuário se outros reportaram alguma carteira como associada a atividade ilegal (ramsomware, spam, fraude etc.). O resultado informa o tipo de ilícito e, por vezes, o email associado a tal atividade. Com proposta semelhante, há o serviço **Check Bitcoin Address** *(https://checkbitcoinaddress.com/).*

Algumas ferramentas permitem a representação gráfica de operações com criptoativos, tais como o **Maltego** *(https://www.maltego.com/blog/cryptocurrency-investigations-with-maltego/).*

Havendo informação decorrente de outros elementos de prova, o membro do MPF pode demandar as exchanges de criptoativos em atuação no País para que informem os **dados cadastrais da pessoa responsável por determinada carteira**, usando, para tanto, os diversos dispositivos de lei que permitem essa requisição[31] .

A ressalva se dá naqueles casos em que a exchange aceita interações à distância, permitindo que um cliente faça uma conta com o upload de documentos de identificação e, por vezes, fotografia. Nessas situações, é possível que o cliente empregue identificação fraudulenta ou fotos manipuladas no processo de registro juntos à exchange.

31- Nesse sentido, por exemplo, o art. 15 da Lei 12.850/13, o art. 17-B da Lei 9.613/98 e o art. 10, § 3º, da Lei n. 12.965/14.

- **Ferramentas Comerciais de Investigação**

Os criminosos que operam com criptoativos dependem intensamente de softwares especiais e técnicas evasivas para garantir o anonimato e obscurecer a titularidade da carteira de criptoativos. Daí porque é absolutamente fundamental o emprego pelos órgãos de investigação de softwares que possam penetrar nas contramedidas adotadas pelos investigados.

A descrição das potencialidades das ferramentas de fontes abertas feita acima já indicam que o seu emprego isolado não atende ao fim último da investigação que é a definição de autoria do fato criminoso. Por elas, na grande maioria dos casos, ter-se-á segurança sobre o fluxo dos recursos, mas não sobre a identidade de quem os titulariza, posto que as pessoas físicas que movimentam as carteiras permanecem, quase sempre, obscurecidas.

As fontes abertas disponíveis na web permitem acesso a registros das transações da maioria dos criptoativos, mas falham, normalmente, em determinar a identidade das pessoas por trás de determinada carteira. E vincular um indívíduo a um endereço ou carteira é o maior desafio da investigação com criptoativos. Afora os casos em que, em decorrência de outros elementos de prova, o investigador pode demandar as exchanges de criptoativos em atuação no país para que informem os dados cadastrais da pessoa responsável por determinada carteira, a investigação pode entrar em um beco sem saída por indeterminação da autoria, ou seja, pelo desconhecimento de quem opera determinada carteira.

Observando essa deficiência nas investigações sobre criptoativos, diversas empresas passaram a disponibilizar no mercado ferramentas tecnológicas pagas que conseguem, com base em um banco de dados da empresa, determinar quem é o responsável (pessoa ou exchange) pela carteira investigada.[32]

32- Por norma os fornecedores de software são muito abertos, próximos e expeditos quando se trata da possibilidade de testar os seus produtos antes de alguém, ou alguma entidade, se comprometer com uma compra.

Em regra, as ferramentas comerciais de investigação são superiores, pois fornecem mais informação e de forma mais detalhada e rápida que as ferramentas existentes em fontes abertas. As ferramentas comerciais de investigação, normalmente, permitem obter o seguinte conjunto de informações e realizar, de uma só vez, várias ações importantes para a análise dos dados financeiros: a) importação e exportação de dados; b) identificação de um maior número de entidades; c) realizar agrupamentos de forma mais rápida e de melhor interpretação; d) possuem interface mais simplificada; e) possui referências a endereços da darkweb e da web aberta (open web); f) permitem consultas específicas para obter assistência técnica; g) têm várias funcionalidades adicionais para alcançar informações de forma mais célere. [33]

São várias as soluções disponíveis no mercado, tais como: o **Reactor** da empresa Chainalysis *(https://www.chainalysis.com/chainalysis-reactor/)*, o **Inspector** da empresa Cellebrite-Ciphertrace (https://ciphertrace.com/ e https://ciphertrace.com/financial-investigations-and-Blockchain-forensics/), a **Coinbase Analytics** da Coinbase (https://www.coinbase.com/pt/analytics); a **Blockchain Analytics** da Elliptic (https://www.elliptic.co/solutions/crypto-investigations); e a **Crystal Blockchain Analytic** da empresa Crystal Blockchain (https://crystalBlockchain.com/). [34]

33- Outra funcionalidade apresentada em algumas ferramentas comerciais é a possibilidade de vincular endereços de Bitcoin a uma carteira específica com base nos endereços solicitados pelo cliente light, e o registro de endereços IP que podem ser usados para identificação de um suspeito.

34- Com alerta o GAFI, o uso de ferramentas de análise de criptoativos, embora útil, também pode representar um desafio para as investigações. Como cada ferramenta de rastreamento contém dados de código aberto diferentes e usa diferentes algoritmos para pesquisar o Blockchain, resultados diferentes podem ser fornecidos aos pesquisadores por esses serviços. Conhecer as ferramentas e seus resultados é essencial para o aproveitamento adequado dessas tecnologias para fins investigativos. Em alguns casos, os países que utilizam essas ferramentas descobriram que diferentes Exchanges e/ou plataformas de criptoativos são menos visíveis do que outras, o que aumenta a dificuldade de seguir os fluxos dos ativos. Além disso, as ferramentas de análise atualmente disponíveis no mercado são compatíveis apenas com um número limitado de ativos virtuais (FATF, Orientação sobre Investigações Financeiras Envolvendo Ativos Virtuais. Enfrentando Desafios com Investigações e Confisco, maio de 2019, p. 39).

Uma preocupação no emprego de ferramentas comerciais está relacionada com a capacidade do órgão de investigação de explicar suas descobertas e procedimentos investigativos ao Poder Judiciário. Vale dizer, a ferramenta precisa apresentar informações claras sobre como chegou a determinado investigado, por exemplo, para que o órgão de investigação possa avaliar a prova a sua pertinência em juízo. Algumas ferramentas disponibilizam especialistas na ferramenta para testemunhar a respeito do modo como a análise de Blockchain foi conduzida.[35]

Algumas ferramentas utilizadas para extração de dados de mídias apreendidas (por exemplo, smartphones e computadores) podem ser usados para identificação, dentre os arquivos extraídos, de programas relacionados a criptoativos[36]. O MPF possui acesso ao **Cellebrite Physical Analyzer**, que revela a existência de programas de criptoativos. Para a extração desses arquivos, deve-se encaminhar a mídia para o setor de perícia da SPPEA[37], a partir da abertura de um pedido de perícia no Sistema Pericial.

- **Relatórios de Inteligência Financeira**

Informações sobre operações com criptoativos podem ser obtidas junto ao Conselho de Controle de Atividades Financeiras – COAF por meio de relatórios de inteligência financeira demandados diretamente **(relatórios de intercâmbio)**[38] solicitados no Sistema de Controle de Atividades Financeiras – SisCOAF.[39]

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

36- Nesse sentido: https://cellebrite.com/en/walkthrough-of-parsing-cryptocurrency-applications-in-cellebrite-physical-analyzer/.

37- Instrução de Serviço SPPEA/PGR n. 41/2021 sobre manuseio de vestígios digitais com suporte físico visível.

38- RIFs de intercâmbio são aqueles elaborados para atendimento à solicitação de informações por autoridades nacionais ou por Unidades de Inteligência Financeira. Ao contrário, RIFs espontâneos (de ofício) são os elaborados por iniciativa do COAF a partir da análise de comunicações e denúncias.

39- Disponível em: https://www.gov.br/coaf/pt-br/sistemas/siscoaf-2-1.

Antes da entrada em vigor da Lei n. 14.478/2022, as exchanges nacionais não estavam enquadradas como "pessoas obrigadas" pelo art. 9º da Lei 9.613/1998 – Lei de Lavagem de Dinheiro. A partir de um modelo de autoregulação, algumas exchanges nacionais passaram a comunicar voluntariamente ao COAF operações suspeitas ocorridas em seu negócio relacionada à lavagem de dinheiro e financiamento ao terrorismo[40].

Com o advento da Lei do Mercado de Criptoativos, as exchanges – agora nomeadas prestadores de serviços de ativos vistuais, PSAVs (art. 5º) – passaram a integrar o Sistema Antilavagem de Capitais brasileiro[41]. O art. 9º da da Lei 9.613/1998 foi alterado para sujeitar as PSAVs às obrigações previstas nos arts. 10 e 11 da mesma lei.

As obrigações impostas pelo art. 10 são, principalmente, relacionadas ao dever de conhecer o seu cliente (KYC) e as transações financeiras por eles realizadas (KYT):

> Identificar seus clientes e manter cadastro atualizado, nos termos de instruções emanadas das autoridades competentes. Na hipótese de o cliente ser pessoa jurídica, a identificação deverá abranger as pessoas físicas autorizadas a representá-la, bem como seus proprietários (§ 1º) – a ideia é evitar o uso do véu corporativo das empresa para ocultar o beneficiário final (12). Os dados devem ser conservados por, no mínimo, cinco anos a partir do encerramento da conta ou da conclusão da transação(§ 2º).
>
> Manter registro de toda transação em moeda nacional ou estrangeira, títulos e valores mobiliários, títulos de crédito,

40- Nesse sentido, o Código de Conduta e Autorregulação das empresas vinculadas à ABCripto: https://www.abcripto.com.br/_files/ugd/55dd41_206786481fc84485817e8d906b54b241.pdf.

41- Dois outros dispositivos já constantes da Lei Antilavagem, que não foram alterados pela Lei n. 14.478/22, possuem interesse para as investigações financeiras que envolvam criptoativos, especialmente no momento do dilema da conversão de criptoativos em moeda fiduciária. Em primeiro lugar, o art. 10-A que cria o Cadastro de Clientes do SFN – CCS, por meio do qual o BACEN mantém o registro centralizado do cadastro geral de correntistas e clientes de instituições financeiras, bem como de seus procuradores. Em segundo lugar, o art. 11-A prevê que as transferências internacionais e os saques em espécie deverão ser previamente comunicados à instituição financeira, nos termos, limites, prazos e condições fixados pelo Banco Central do Brasil.

metais, ativos virtuais (inserido pela Lei n. 14.478/22), ou qualquer ativo passível de ser convertido em dinheiro, que ultrapassar limite fixado pela autoridade competente. Os dados devem ser conservados por, no mínimo, cinco anos a partir do encerramento da conta ou da conclusão da transação(§ 2°). Ademais, o registro das transações será efetuado também quando a pessoa física ou jurídica, seus entes ligados, houver realizado, em um mesmo mês-calendário, operações com uma mesma pessoa, conglomerado ou grupo que, em seu conjunto, ultrapassem o limite fixado pela autoridade competente (§ 3°);

Adotar políticas, procedimentos e controles internos, compatíveis com seu porte e volume de operações, na forma disciplinada pelos órgãos competentes;

Cadastrar-se e manter seu cadastro atualizado no órgão regulador ou fiscalizador e, na falta deste, no Conselho de Controle de Atividades Financeiras (COAF), na forma e condições por eles estabelecidas;

Atender às requisições formuladas pelo COAF na periodicidade, forma e condições por ele estabelecidas, cabendo-lhe preservar, nos termos da lei, o sigilo das informações prestadas.

As obrigações previstas no art. 11 são relacionadas ao dever de comunicação de operações financeiras suspeitas ao Conselho de Controle de Atividades Financeiras (COAF):

Dispensar especial atenção às operações que, nos termos de instruções emanadas das autoridades competentes, possam constituir-se em sérios indícios de lavagem de capitais. As autoridades competentes elaborarão relação de operações que, por suas características, no que se refere às partes envolvidas, valores, forma de realização, instrumentos utilizados, ou pela falta de fundamento econômico ou legal, possam configurar a hipótese nele prevista (§ 1°).

Comunicar ao COAF, abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, no prazo de 24 horas, a proposta ou realização de todas as transações referidas no inciso II do art. 10, acompanhadas da identificação de que trata o inciso I do mencionado artigo; e das operações referidas no inciso I do art. 11;

Comunicar ao órgão regulador ou fiscalizador da sua atividade ou, na sua falta, ao COAF, na periodicidade, forma e condições por eles estabelecidas, a não ocorrência de propostas, transações ou operações passíveis de serem comunicadas.

Não é incomum que investigados operem em exchanges sediadas em países que possuem controles fracos contra a lavagem de dinheiro e financiamento ao terrorismo, ou mesmo em países que sistematicamente se recusam a cooperarem, a despeito da existência formal de ferramentas de cooperação jurídica internacional.

Além das prestadoras de serviços virtuais previstas na Lei n. 14.478/2022, operações com criptoativos podem ser comunicadas ao COAF por entidades pertencentes a outros setores obrigados por lei, tais como instituições financeiras bancárias e corretoras e distribuidoras de valores mobiliários. De fato, as tradicionais entidades dos setores obrigados legalmente podem notificar duas sortes de operacões financeiras suspeitas: a) operações ocorridas em seus produtos financeiros por pessoas físicas ou jurídicas investigadas; e b) operações suspeitas realizadas pelas próprias exchanges.

Isso ocorre porque, por mais que operem com criptoativos, os investigados sempre encontram o dilema de saque (ou dilema da conversão), ou seja, precisam converter o criptoativo em moeda fiduciária[42]. Quando essa conversão ocorre em instituições financeiras nacionais, é possível que essas operações tenham sido comunicadas ao COAF.

Eventuais relatórios de inteligência financeira podem ser analisados por meio da ferramenta RIF Análise, a partir dos arquivos do tipo .CSV encaminhados pelo COAF em anexo aos relatórios.[43]

Com a transnacionalidade inerente às operações com criptoativos, muitas vezes se faz necessário buscar dados de unidades de inteligência financeira no exterior. Para tanto, o COAF intermedeia os pedidos ao **Grupo de Egmont**. Orientações adicionais estão no seguinte vídeo produzido pelo COAF, *Inteligência Financeira: Aspectos Práticos do Intercâmbio Internacional via Rede Egmont: https://youtu.be/i5N_LqLmewI*.[44]

42- Como o propósito de uma investigação é acumular evidência para provar que um crime envolvendo criptoativos ocorreu, os investigadores podem tentar seguir o dinheiro até que identifiquem um conhecido provedor de serviço com criptoativos, tal como uma exchange ou um processador de pagamento. O ponto focal crítico em uma investigação relacionada a criptoativos geralmente é a identificação do ponto em que o criptoativo é trocado por moeda fiduciária ou por outro tipo de criptoativo (FATF, Orientação sobre Investigações Financeiras Envolvendo Ativos Virtuais. Enfrentando Desafios com Investigações e Confisco, maio de 2019, p. 48).

43- O manual de operacionalização do RIF Análise (Informação 022/2020-SPPEA/PGR, PGR-00197821/2020) pode ser solicitado à SPPEA por meio do e-mail pgr-atendimento-sppea@mpf.mp.br.

44- O COAF indica que para o intercâmbio de informações que demandam informações via Rede Egmont, além das informações e documentos inseridos para o intercâmbio nacional, incluir no campo "Detalhes" do Sistema Eletrônico de Informações (SEI-C) os seguintes requisitos obrigatórios: 1- Descrição dos alvos com os respectivos elementos identificadores Na hipótese de pesquisa sobre pessoa física ou jurídica estrangeira, a identificação poderá ser feita no próprio texto, não havendo a necessidade de listar o nome nos "Principais Relacionados". Neste caso, incluir todas as informações disponíveis, tais como nacionalidade e data de nascimento para PF e endereço e número de registro para PJ. 2- Relacionamento dos alvos/fatos investigados com o país requerido. É importante demonstrar o relacionamento existente entre o alvo ou o fato investigado com o país que está sendo consultado. Pedidos genéricos, sem tal vinculação, não serão enviados. 3- Resumo dos fatos/pessoas investigadas. O resumo deve contemplar ao menos informações sobre o crime investigado e o modus operandi. Caso haja mais de um alvo listado, é importante descrever a suspeição sobre cada um deles (mesmo que seja somente uma relação de parentesco). 4- Descrição da informação que se pretende obter no país requerido. Registrar especificamente o que se espera do intercâmbio (ex: informações sobre eventuais movimentações suspeitas, informações comerciais, dados sobre o beneficiário final de uma empresa, etc). Caso o pedido for direcionado para mais de um país, descrever separadamente o que se quer de cada um deles. Se o pedido versar sobre transações financeiras suspeitas específicas, favor incluir também as informações disponíveis sobre a instituição financeira estrangeira, tais como o nome do banco, o número da conta e o da agência.

Fontes Fechadas

Por fontes fechadas se entende, suscitamente, aquelas para as quais o acesso precisa ser precedido de autorização judicial (reserva de jurisdição). Estão nesse campo os dados financeiros, fiscais, telemáticos etc.

No criptomercado, os dados decorrentes de afastamentos de sigilo telemático (grande fonte de prova), associado aos pedidos de afastamento de sigilo fiscal da RFB e ao das operações das exchanges (modelos de minuta do SIMBA) podem ser de interesse para a investigação.

- **Afastamento de Sigilo Finaceiro e Fiscal de Operações com Criptoativos via SIMBA**

Atualmente, no SIMBA há possibilidade de acesso a dados financeiros constantes de todos os mercados financeiros (crédito, câmbio, valores mobiliários, seguros e previdência privados, e previdência fechada), novos arranjos de pagamento (como o PIX e os iniciadores de pagamento), sistemas informáticos de especial interesse à investigação financeira, dados fiscais e telemáticos dotados de intersecção estreita com transações financeiras, e operações com criptoativos.[45]

Especificamente em relação às transações envolvendo criptoativos de investigado identificado civilmente (nome, CPF ou CNPJ, por exemplo), elas podem ser alcançadas pela solicitação dos dados transmitidos pelas exchanges à Receita Federal do Brasil ou, caso o MPF conheça a exchange envolvida na transação, pela obtenção de dados de transações intermediadas por essas plataformas eletrônicas (exchanges) e em seus sistemas internos.[46]

45- Disponível em https://portal.mpf.mp.br/simba/php/Simba.php.

46- Como explicado acima, as exchanges possuem os dados e documentos de transação em uma espécie de "livro razão" da empresa.

No primeiro cenário, trata-se de pedido de afastamento de sigilo fiscal de investigado, dirigido à Receita Federal do Brasil. Exchanges de criptoativos com domicílio tributário no Brasil encontram-se obrigadas a informar à RFB, mensalmente, as operações realizadas por seus clientes dentro da plataforma, quaisquer que tenham sido os valores operados (IN RFB 1888/2019, art. 6°).[47]

O contribuinte (pessoa física ou jurídica) domiciliado no Brasil, por sua vez, possui três obrigações tributárias envolvendo criptoativos: a) informar operações à RFB, quando, no mês anterior, o somatório das operações realizadas fora de exchanges nacionais tenha excedido R$ 30.000,00 (IN RFB 1888/2019, art. 6°, §1°); b) recolher imposto sobre o ganho de capital, quando, no mês anterior, tenha obtido lucro e o somatório das alienações de criptoativos tenha superado R$ 35.000,00 (IN SRF 599/2005, art. 1°, II e Lei 8.981/95, art. 21); e c) preencher Declaração do Imposto de Renda. No caso do IRPF, criptoativos deverão estar lançados na ficha bens e direitos (cód. 81, 82 e 89) e rendimento com criptoativos deverão estar lançados em "rendimentos não tributáveis" ou em "rendimentos sujeitos à tributação exclusiva".

Ao final desse Roteiro de Atuação consta minuta de afastamento de sigilo fiscal de operações com criptoativos no SIMBA.

Por outro lado, caso o MPF conheça a *exchange* envolvida na transação[48], ele poderá solicitar o afastamento do sigilo telemático das operações intermediadas por essas plataformas eletrônicas (*exchanges*) e em seus sistemas internos. Essa relação entre investigados e *exchanges* pode exsurgir de outros elementos de prova, como, por exemplo, a identificação de carteiras na análise dos dados telemáticos obtidos judicialmente.

47- Para a RFB, considera-se criptoativo "a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal" (art. 5°). De igual modo, a RFB considera exchange de criptoativo "a pessoa jurídica, ainda que não financeira, que oferece serviços referentes a operações realizadas com criptoativos, inclusive intermediação, negociação ou custódia, e que pode aceitar quaisquer meios de pagamento, inclusive outros criptoativos". Incluem-se no conceito de intermediação de operações realizadas com criptoativos, a disponibilização de ambientes para a realização das operações de compra e venda de criptoativo realizadas entre os próprios usuários de seus serviços.

48- A SPPEA possui a lista compilada das corretoras de criptoativos em atuação no Brasil.

Ao final desse Roteiro de Atuação, consta minuta de afastamento de sigilo telemático de operações com criptoativos utilizando o SIMBA e tendo por destinatário da ordem uma exchange específica.

A partir do Parecer de Orientação n. 40/2022, a Comissão de Valores Mobiliários consolidou o entendimento de que algumas operações com criptoativos podem se configurar como valores mobiliários. Assim, ainda que os criptoativos não estejam expressamente incluídos entre os valores mobiliários citados nos incisos do art. 2° da Lei n° 6.385/76, os agentes de mercado devem analisar as características de cada criptoativo com o objetivo de determinar se é valor mobiliário, o que ocorre quando ele: é a representação digital de algum dos valores mobiliários previstos taxativamente nos incisos I a VIII do art. 2° da Lei n° 6.385/76 e/ou previstos na Lei n° 14.430/2022 (i.e., certificados de recebíveis em geral); ou se enquadra no conceito aberto de valor mobiliário do inciso IX do art. 2° da Lei n° 6.385/76, na medida em que seja contrato de investimento coletivo.

Para esses casos, tanto a minuta simplificada quanto a minuta completa do SIMBA[49] abarcam esse produto financeiro, ao pedir o acesso aos dados das transações de títulos e valores mobiliários realizados por meio de sociedades corretoras de títulos e valores mobiliários (CTVM) e sociedades distribuidoras de títulos e valores mobiliários (DTVM) integrantes do CCS.

Com as normas da Lei n. 14.478/22, competirá a órgão ou entidade da Administração Pública federal, definido em ato do Poder Executivo, estabelecer quais serão os ativos financeiros regulados, sendo possível que a futura regulamentação estabeleça novas possibilidades de acesso a dados financeiros sigilosos de operações com criptoativos.

49- Para as orientações sobre o uso do SIMBA, consulte-se a cartilha da disponível em: https://portal.mpf.mp.br/novaintra/informa/2022/documentos/SIMBACartilhaparaMembros.pdf.

Uma vez que as operações com criptoativos são operações financeiras realizadas em plataformas eletrônicas, parece natural que alguns dos dados telemáticos associados possam ser demandados judicialmente, notadamente o endereço de protocolo de internet (endereço IP) de acesso ao provedor de aplicação da corretora de criptoativos; e os registros de acesso à aplicação de internet mantida pela corretora.[50]

Em caso de descumprimento injustificado da ordem judicial de entrega dos dados das operações ou de suspeita quanto à lisura das operações da exchange, abre-se a possibilidade de ser realizada uma busca e apreensão dos servidores da exchange para que neles sejam feitas análises forenses aptas a recuperar os dados necessários à investigação ou documentar se os dados são efetivamente irrecuperáveis ou se foram apagados. Tal abordagem, naturalmente, não pode ser aplicada a serviços instalados na darknet, onde a localização da infraestrutura é desconhecida, ou em países que têm histórico de recusar cooperação jurídica internacional.

Um problema adicional existem também quando se trata de exchanges descentralizadas. Ainda hoje, a maioria das exchanges é centralizada e armazena informações de usuários em um servidor centralizado. Todavia, desde 2012, a comunidade de criptoativos vem desenvolvendo modelos de exchanges descentralizadas nas quais a negociação pode ocorrer sem que os usuários precisem enviar seus criptoativos a um órgão centralizado e todas as transações se tornariam transações P2P, ou seja, entre particulares.

50- A migração das transações financeiras para suportes digitais significou que variados dados telemáticos foram associados a informações financeiras. Esses dados telemáticos, coletados pelas instituições financeiras, podem ser de interesse para a investigação financeira, sendo passíveis de acesso por autorização judicial. A título de exemplo, são **dados telemáticos** passíveis de acesso por ordem judicial: a) o endereço de protocolo de internet (endereço IP) de acesso ao provedor de aplicação da instituição financeira; b) os registros de acesso a aplicação de internet mantida pela instituição financeira, compreendendo o conjunto de informações referentes à data e hora de uso da aplicação de internet da instituição financeira a partir dos endereços IP relacionados ao investigado e informados no item acima; c) o e-mail cadastrado pelo usuário para acesso ao serviço financeiro digital; d) o terminal cadastrado (aparelho telefônico, computador etc.); e) tipo e a versão do aplicativo utilizado; f) dados do cartão de crédito associado ao serviço financeiro digital (nome do titular, CPF, telefone, endereço, número do cartão, renda declarada e perfil de gastos); g) fotografias e filmagens do momento das operações indicadas, caso tenham sido realizadas em caixas automáticos (ATM). Importante, para racionalização do pedido judicial, que o MPF aponte as transações em que se busca o fornecimento dos dados telemáticos atrelados, sob pena de se atrasar em muito a resposta por parte da instituição financeira. A minuta de pedido judicial dessas operações consta do SIMBA.

A IN RFB 1888/2019 traz uma definição sobre esse tipo de entidade no art. 5º, parágrafo único, ao determinar que se incluem no conceito de intermediação de operações realizadas com criptoativos, a disponibilização de ambientes para a realização das operações de compra e venda de criptoativo realizadas entre os próprios usuários de seus serviços. A Lei n. 14.478/22 também considera prestador de serviço de ativos virtuais aquela pessoa jurídica que executa, em nome de terceiros, dentre outros, a participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda de ativos virtuais (art. 5º, inciso V).

Pode-se imaginar que exchanges descentralizadas, com infraestrutura distribuída em muitas jurisdições ao redor do mundo e nenhum órgão central que supervisiona transações, dificultará, por exemplo, a obtenção de informações específicas sobre transações.[51]

- **Afastamento de Sigilo Telemático**

Em uma investigação sobre criptoativos, pode haver necessidade de se formular pedidos de preservação de dados telemáticos e afastamento de sigilos de dados telemáticos diversos daqueles associados a transações financeiras já constantes da minuta do SIMBA. Para tanto, as orientações estão compilados no portal e-Evidence, mantido pelo Grupo de Apoio à Criminalidade Cibernética, em trilhas objetivas: *https://portal.mpf.mp.br/eevidence*.

- **Cautelas com Seeds e Chaves Privadas Encontradas**

Conforme visto anteriormente, o acesso a seeds e chaves privadas dá acesso à possibilidade de movimentação dos criptoativos. Diferentemente da investigação tradicional, onde os valores estão custodiados em instituições financeiras centralizadas, aqui qualquer um que tenha acesso a essas informações poderá movimenta-los.

49- FATF, Orientação sobre Investigações Financeiras Envolvendo Ativos Virtuais. Enfrentando Desafios com Investigações e Confisco, maio de 2019.

Durante a investigação criminal, a partir de medidas de afastamento de sigilo acima descritas, é possível que nos deparemos com seeds, passphrases, chaves privadas e senhas (chaves de acesso) antes mesmo da deflagração de uma medida ostensiva. É comum investigados guardarem tais informações na nuvem, estando, portanto, acessíveis por meio de uma simples quebra telemática.

Se na fase velada da investigação forem encontradas chaves de acesso, é importante ponderar a necessidade de se apreender os criptoativos imediatamente com a possibilidade de se aguardar momento mais apropriado para deflagração da operação policial.

Nessas situações, nos parece que a postura mais adequada é registrar tudo o que for encontrado, de forma pormenorizada, e levar ao conhecimento do juízo competente imediatamente para que uma avaliação de conveniência/oportunidade possa ser feita, classificando-se a peça com o grau máximo de sigilo.

De fato, tal análise é fundamental, na medida em que diligências podem estar em curso e a imediata apreensão dos ativos pode alertar os alvos da existência de cautelares, frustrando outras medidas.

BUSCA E APREENSÃO DE CRIPTOATIVOS

As chaves para acesso a criptoativos podem estar armazenadas em variados dispositivos físicos eletrônicos, como hardwallets, computadores e celulares, ou até mesmo impressas ou anotadas em papel. Assim, a diligência de busca e apreensão pode trazer resultados bastante frutíferos em investigações que envolvam criptoativos.

Contudo, para o sucesso da diligência é imprescindível uma fase prévia de preparação e a adoção de alguns cuidados durante as buscas, de modo a assegurar que os criptoativos encontrados possam efetivamente ser apreendidos pelo Estado.

PREPARAÇÃO PARA A BUSCA PRESENCIAL

Tratando-se de investigação em que exista a suspeita de utilização de criptoativos, é essencial que o representante do Ministério Público Federal e a Polícia Federal providenciem a criação de uma carteira controlada pelo Estado para que os criptoativos encontrados no momento da busca presencial possam ser imediatamente transferidos para a custódia estatal.

É impossível precisar quais tipos de criptoativos serão de fato encontrados nas buscas, mas por meio das diligências remotas tratadas em tópico anterior, é possível prever as espécies de criptoativos usualmente utilizadas pelo investigado.

De todo modo, sugere-se que sejam previamente criados endereços, pelo menos, de Bitcoin e de Ethereum.

Esses endereços podem ser abertos na forma de uma conta em exchange nacional, mediante autorização judicial, ou podem ser endereços de carteiras próprias, preferencialmente hardwallets, cujas chaves privadas/frase de recuperação estejam sob a custódia de agentes públicos.[52]

Neste último caso, é fundamental que os envolvidos no cumprimento da medida de busca e apreensão saibam do risco de eventual vazamento ou compartilhamento indevido das chaves privadas ou da frase de recuperação das carteiras sob a responsabilidade do Estado, pois qualquer pessoa com acesso a essas chaves poderá movimentar livremente os criptoativos apreendidos para qualquer outro endereço. Pior: protegido pelo pseudonimato do Blockchain.

Estabelecido um mecanismo para a custódia dos criptoativos porventura apreendidos, é imprescindível que seja designada uma pessoa ou equipe (ponto focal) para ficar de prontidão remotamente, durante as diligências, com acesso a computador, internet, endereço da carteira estatal e algum software que permita a recuperação remota de carteiras de criptoativos, como por exemplo, o Coinomi[53]. Essa pessoa ou equipe será responsável por realizar a imediata transferência de criptoativos encontrados com investigados para a carteira estatal.

Essa medida é essencial para o sucesso das diligências, tendo em vista a possibilidade de movimentação remota dos criptoativos por qualquer outra pessoa que detenha cópia das chaves privadas, que nada mais são do que um código.

52- Apesar de haver discussão no Conselho da Justiça Federal (CJF) a respeito da apreensão de ativos virtuais, não há, ainda, regulamentação que discipline a sua custódia. No projeto de regulamentação do CJF, existe previsão para que os tribunais façam o credenciamento de exchanges, "que serão responsáveis por criar, mediante determinação judicial carteira (wallet) para armazenar temporariamente os ativos virtuais em processos e procedimentos de investigação". Tecnicamente, essa é uma das soluções possíveis, sendo a outra a de algum agente público ou (um grupo de agentes públicos) assumir a custódia desses ativos, como se indicou no tópico anterior. O que nos parece fora de dúvidas é o fato de que a sua custódia não deve ficar a cargo do MPF, que não possui o munus de ser depositário judicial.

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

EXECUÇÃO DE BUSCA PRESENCIAL

Durante as diligências de busca e apreensão é imprescindível que as equipes estejam atentas a anotações, impressas ou manuscritas, que possam configurar frases de recuperação (seed phrases), conjuntos de 12 a 24 palavras, ou combinações de endereços e chaves privadas de criptoativos, além de dispositivos físicos (hardwallets) que armazenam as chaves privadas.

Como se destacou na parte inicial desse roteiro de atuação, a mera apreensão de dispositivos eletrônicos de armazenamento de chaves privadas (hardwallets) não garante a apreensão dos criptoativos. Para que isso ocorra, é necessário que se chegue às chaves privadas e/ou à seed phrase.

Assim, mesmo que uma seed seja encontrada na casa de um alvo, que tenha sido preso numa operação, um comparsa que não foi atingido pela medida cautelar pode livremente movimentar os ativos, caso esteja de posse das mesmas palavras chaves. Recomenda-se redobrado cuidado com seed phrases e chaves privadas, que não devem ser compartilhadas, pois, como já alertado, qualquer pessoa de posse dessas informações poderá movimentar os criptoativos.

Exemplo: Medida de busca e apreensão realizada às 6h com a apreensão de chaves de acesso. Em circunstâncias ideais, às 6h30min esses recursos já têm que ter sido transferidos para chaves públicas em poder das autoridades. Isto é, antes que a medida cautelar tenha sido publicizada para comparsas do alvo ou na imprensa. Caso isso não seja feito, um comparsa pode, de qualquer lugar do mundo, recuperar os ativos e transferi-los para endereços que não poderão ser objeto de bloqueio.

Desta forma, é essencial que à recuperação das chaves de acesso se siga a transferência dos fundos para uma carteira em poder das

autoridades ou para a conta de alguma exchange nacional, em conformidade com o que tenha sido autorizado pela Justiça.

Nos mesmos moldes em que se dá com a apreensão de ativos tradicionais, deve a medida ser conduzida pela Polícia Federal, de forma documentada, de modo a preservar a cadeia de custódia das evidências e o rastreamento dos ativos. Importante, ainda, certificar de forma detalhada no relatório da diligência tudo o que foi realizado no local e as pessoas presentes.

Outro ponto a ser considerado com bastante atenção é a compartimentalização das informações referentes às chaves de acesso. Como o acesso a tais dados permite o controle dos ativos, é fundamental que o menor número possível de pessoas (tanto no âmbito do Ministério Público, da Polícia e do Poder Judiciário) tenha acesso a tais informações.

Por fim, considerando que chaves privadas de criptoativos podem estar armazenadas em computadores e celulares é recomendável solicitar prioridade ao setor de perícias da PF para a extração e espelhamento dos itens eletrônicos apreendidos, para que seja possível a análise do material com a busca de possíveis senhas e chaves privadas.

SEQUESTRO E INDISPONIBILIDADE DE CRIPTOATIVOS

Os casos de sequestros e indisponibilidades, cíveis e criminais, de ativos e suas respectivas hipóteses de cabimento foram delineados no Roteiro de Persecução Patrimonial e Administração de Bens, especificamente nos capítulos V e VI, elaborado por grupo de trabalho instituído pelas 2ª e 5ª Câmaras de Coordenação e Revisão[54]. Tais medidas de coação constituem-se em poderosas ferramentas de combate à delinquência econômica com eficácia por vezes superior às tradicionais penas privativas de liberdade.

O caso concreto determinará qual espécie de medida restritiva patrimonial é cabível e a sua respectiva fundamentação jurídica. Deve-se atentar também para as hipóteses de alienação antecipada e para as boas práticas para administração dos bens, tratadas, no que diz respeito a criptoativos, no presente manual.

De acordo com o tipo de sequestro e indisponibilidade adotado, o membro do MPF deve requerer em juízo a constrição dos bens dos demandados, expedindo-se mandado de constrição de **criptoativos**, **moedas eletrônicas** ou **outros valores a qualquer título custodiados**, inclusive o **congelamento de eventuais ordens de saque em moeda corrente ou criptoativos**, até o valor determinado, eventualmente existentes nas *exchanges* nomeadas.

54- BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. Roteiro de Atuação – Persecução Patrimonial e Administração de Bens, 2017. Disponível em: https://portal.mpf.mp.br/novaintra/areas-tematicas/camaras/criminal/publicacoes/roteiros-de-atuacao-restrito/roteiro_atuacao_persecucao_patrimonial.

Em acréscimo, é importante solicitar que o magistrado adote algumas medidas para efetivação da ordem judicial. A primeira é que conste do mandado de sequestro que o MPF e a Polícia Federal poderão dar cumprimento às ordens de sequestros diretamente em contato com as corretoras ou, caso não atendidas, vistoriar a própria sede das empresas em busca de ativos. A medida se justifica para dar agilidade ao cumprimento da ordem, caso o Poder Judiciário tenha dificuldade em operacionalizá-la. Em segundo lugar, que as exchanges destinatárias da ordem realizem a transferência dos valores para a carteira previamente criada e sob o controle do Estado, conforme abordado em tópico anterior desse manual.

Por fim, anote-se que o sequestro nem sempre precisa recair apenas sobre os criptoativos do demandado, sendo, inclusive, prudente para efetivação da constrição, a cumulação de pedidos tradicionais de sequestro de ativos [55] com os especiais pedidos de sequestro de criptoativos acima referidos.

55- Tais como a penhora on line, prevista no art. 854 do Código de Processo Civil e instrumentalizada pelo Sistema de Busca de Ativos do Poder Judiciário – SISBAJUD; o bloqueio via RENAJUD de todos os veículos registrados em nome dos demandados; o bloqueio de embarcações e aeronaves eventualmente registradas em nome dos requeridos, com a expedição de ofício à Capitania dos Portos e à ANAC para efetivar a medida; o bloqueio de bens imóveis registrados em nome dos demandados, inserindo a ordem de restrição na CNIB – Central Nacional de Indisponibilidade de Bens.

ALIENAÇÃO DE CRIPTOATIVOS

Efetuada a apreensão e transferência dos criptoativos, surgem questões referentes ao momento de sua alienação, particularmente se deve ser realizada alienação antecipada ou se cabe aguardar o desfecho da ação penal para a conversão dos criptoativos em moeda fiduciária.

Os efeitos práticos dessa discussão se referem à grande volatilidade do preço dos criptoativos. Em um curto espaço de tempo, por vezes até mesmo em questão de segundos, o preço de um determinado criptoativo pode sofrer severas oscilações. De forma ilustrativa, veja-se a alteração dos valores do Bitcoin no período de 01.jan.2021 a 31.12.2022[56] (os valores em referência na coluna da esquerda são em dólares):

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

De acordo o gráfico acima, extraído do site Coinmarketcap.com, o menor valor da cotação do Bitcoin em 2021 ocorreu em 20 de julho, quando foi negociado a $29.807,35[57], sendo que em 08 de novembro foi alcançado o valor máximo de $67.566,83. De tal forma, houve uma valorização de 226,67% do menor para o maior valor da cotação em 2021, em um intervalo de menos de 4 meses. No entanto, os últimos 45 dias do ano mostraram uma forte queda na cotação do Bitcoin, que fechou o ano em $46.306,45.

A grande volatidade do Bitcoin, que se mostra ainda mais acentuada em outros criptoativos, é um dos indicativos de sua utilização maciça com cunho especulativo. Esse quadro pode produzir, na prática, grandes diferenças de valores comparando-se a data da apreensão e a data da efetiva conversão em moeda soberana, o que pode implicar em valorização ou não.

Cabe indicar a existência das stable coins, modalidade de criptoativos que, em tese, não estão sujeitos à volatidade. As stable coins são criptoativos que atrelam seu valor a uma moeda soberana, emitida pelo Estado, normalmente o dólar. Exemplos são Tether (USDT), Gemini Dollar (GUSD), Dai (DAI), USD Coin (USDC), Binance USD (BUSD) e True USD (TUSD), criptoativos que pareiam seu valor ao dólar, de modo que uma unidade de cada um desses criptoativos vale 1 dólar. Para alcançar essa paridade existem técnicas diferentes, como a emissão de criptoativos atrelados ao depósito de moeda soberana, a programação de smart contracts e de algoritmos que controlam a compra e venda dos ativos.[58]

As stable coins tem merecido especial atenção das autoridades, em especial dos órgãos estatais de regulação do mercado financeiro. Nos EUA, o Tether foi multado em $42,5 milhões pela Commodity Future Tradings Commission (CTFC), órgão administrativo nacional, por conta de fraudes envolvendo as garantias de sua emissão.[59]

57- Todos os valores estão fixados em dólares americanos.

58- Maiores informações podem ser encontradas em https://www.gemini.com/cryptopedia/what-arestablecoins-how-do-they-work

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

Conforme indicado antes, quanto ao momento da alienação há de se definir entre manter os criptoativos custodiados no curso do processo ou realizar sua alienação antecipada. Na primeira situação somente ao final da ação penal, com a confirmação definitiva da sentença penal condenatória, seria determinada sua alienação judicial, com a consequente conversão em moeda soberana, pela cotação da respectiva data. Por outro lado, com a alienação antecipada haveria a conversão em moeda fiat ainda no curso do processo, na forma do art. 144-A, do Código de Processo Penal.

Em busca de uma solução para a definição do momento da alienação, o Código de Processo Penal, em seu art. 144-A, caput, parte final, na forma da redação dada pela Lei nº 12.694/2012, autoriza a alienação antecipada sempre que houver dificuldade para a manutenção dos bens apreendidos:

> *"Art. 144-A: O juiz determinará a alienação antecipada para preservação do valor dos bens sempre que estiverem sujeitos a qualquer grau de deterioração ou depreciação, ou quando houver dificuldade para sua manutenção" – grifo nosso.*

Como visto no tópico próprio, a apreensão e custódia de criptoativos exigem preparação e cuidados específicos para se evitar a frustração das diligências. Dado o caráter digital, transfronteiriço, descentralizado e a irreversibilidade das operações envolvendo criptoativos, medidas especiais são imprescindíveis para assegurar o efetivo controle dos valores neles representados.

Estejam os criptoativos sob a custódia de uma exchange nacional, estejam eles em carteira própria do Estado, haverá riscos na sua manutenção que não se limitam ao risco de mercado, ou seja, à volatilidade do preço. A realidade é pródiga em exemplos. Tanto de problemas envolvendo grandes exchanges [60], quanto de problemas envolvendo a custódia própria por usuários experientes [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/

Dessa forma, seja em razão da alta volatividade dos preços ou das especificidades técnicas envolvendo a segurança da custódia dos criptoativos, suas características próprias demonstram serem bens de difícil manutenção, o que autoriza, nos termos do art. 144-A, do CPP, a alienação antecipada.

Assim como outros países, dentre eles Suíça e Alemanha[62], também o Brasil não conta com uma legislação específica sobre a alienação de criptoativos apreendidos.

Apesar disso, há fundamentos técnicos e jurídicos para que a alienação antecipada seja realizada com base no art. 144-A do CPP, conforme visto no tópico anterior.

Em termos práticos, diversamente do que ocorre com moedas estrangeiras, títulos de crédito negociados em Bolsa, títulos da dívida pública, ações e demais valores mobiliários, não existe uma instituição equivalente à Caixa Econômica Federal para receber os criptoativos e realizar o câmbio em uma cotação oficial[63].

Tecnicamente, consideramos que as duas alternativas mais viáveis sejam: alienação por leilão, na forma do art. 879 e ss. do CPC; e alienação por intermédio de exchanges nacionais. Na prática, no entanto, entendemos preferível que a alienação se dê da segunda forma, ou seja, via exchanges nacionais[64], sobretudo quando se tem em conta o princípio da eficiência (CPC, art. 8º). É que, além da taxa cobrada por exchanges ser inferior à taxa do leiloeiro, a chance de se obter um maior preço de venda é imensamente maior em livros de ofertas do que em leilões[65].

62- Assim também ocorre em outros países, que não possuem, tal qual o Brasil, um regramento próprio sobre constrição patrimonial de criptoativos. A Suíça e a Alemanha, por exemplo, utilizam suas normas processuais penais sobre apreensão e confisco, conforme questionário enviado pelo GT Criptoativos a esses respectivos países, disponível de forma restrita na Secretaria de Cooperação Internacional/PGR. Nesse primeiro país, surgiu o debate sobre a alienação na alta dos criptoativos, o que seria problemático no Brasil, por falta de regulamentação legal, isso sem entrar no debate de que se essa prática não permitiria, em caso de grandes apreensões e alienações, que a exchange encarregada acabasse por concorrer para a flutuação dos valores e ainda se, de alguma forma, o Estado não estaria associado a uma prática especulativa e incompatível à adotada com outros ativos voláteis, como valores mobiliários e moedas estrangeiras (FIAT). Confira a Decisão 1B_59/2021 de 18 de outubro de 2021, da Suprema Corte Suíça em thttps://archipel.law/en/insights/the-early-liquidation-of-crypto-assets-and-the-need-for-crypto-expertise/

63- Resolução nº 428/2005 do CJF, art. 1, inciso VI.

64- Praxe também adotada nos Estados Unidos: https://www.cnbc.com/2021/07/28/us-marshalsservice-hires-custodian-to-hold-crypto-seized-in-criminal-activity.html

65- Não se desconhece a existência de países que já realizaram a alienação de criptoativos via leilões conduzidos por casas especializadas. Cf.: https://www.irishnews.com/business/2019/10/01/news/wilson-auctionsoff-500-000-of-bitcoin-seized-from-uk-criminal-1726231/

Não há procedimento previsto para a escolha da exchange por meio da qual será feita alienação. Diante desse cenário, sugere-se a utilização de critérios objetivos na escolha das exchanges, tais como taxa cobrada, volume de negociação etc, e a submissão da escolha ao Juízo.

Destaca-se, por fim, ser desejável a adoção de estratégias, a serem pensadas com a exchange, visando à obtenção do melhor preço médio. A seguir, o exemplo da estratégia que foi judicialmente homologada, em 14/07/2021, para a alienação de quase 30 bitcoins, apreendidos nos autos do proc. N° 5004543-34.2019.4.02.5001, tramitado na Justiça Federal do Espírito Santo. Naquele caso, os parâmetros propostos para a venda foram assim estabelecidos:

1. Os BTC serão alienados de forma fracionada (10 lotes, sendo os 09 primeiros de 3 BTC e o último no valor remanescente);

2. A venda de cada um dos lotes será feita pelo lançamento de uma única ordem de venda no livro de ofertas, no valor total do lote em BTC, com preço limite não inferior a 2% do preço de mercado, assim entendido como o preço correspondente ao da última operação realizada via livro de ofertas;

3. Na eventualidade de a ordem de venda com preço limite não ser completamente preenchida em até trinta minutos, nova ordem de venda poderá ser lançada, no valor remanescente do lote, com observância da mesma diretriz anterior (item 2);

4. Encerrada a venda de um lote, poderá ser realizado o lançamento da ordem relativa ao próximo lote, sem a necessidade de observância de intervalo mínimo, mas sempre com respeito aos mesmos parâmetros definidos no item 2.

O objetivo foi o de não afetar negativamente o preço do bitcoin no livro de ofertas da exchange, o que aconteceria caso fosse realizada a alienação de todos os bitcoins de uma só vez ou em um intervalo muito pequeno de tempo.

DEFI E SUAS PARTICULARIDADES

DeFi é o acrônimo de Decentralized Finances (finanças descentralizadas) e denomina uma especial categoria de aplicações executadas[66] em ambientes descentralizados – os chamados DApps (decentralized applications) –, cuja finalidade é viabilizar serviços financeiros, como empréstimos, seguros e provisão de liquidez.

Para compreendermos o que são DApps, retomemos a comparação que fizemos entre, de um lado, o bitcoin-hardware/bitcoin-software e, do outro, o notebook/seu sistema operacional (Windows ou Linux). Nessa comparação, o bitcoin-software é como um sistema operacional que apresenta funcionalidades, mas que não foi concebido para acomodar a instalação de programas.

A partir do Ethereum, primeiro Blockchain programável a surgir, esse cenário muda drasticamente, e o Windows da nossa comparação passa a ser um sistema operacional pensado e concebido para comportar a instalação de programas que rodam sobre ele.

Nesse novo cenário comparativo, o Ethereum-hardware se assemelha ao Notebook, o Ethereum-software ao Windows e os DApps a quaisquer programas que rodam no Windows, como o Word, o Google Chrome e o Zoom.

Assim como os programas do nosso exemplo (Apps) podem ser classificados em diversas categorias, com base no serviço que

66- Programas, aplicativos e aplicações são, neste contexto, palavras sinônimas.

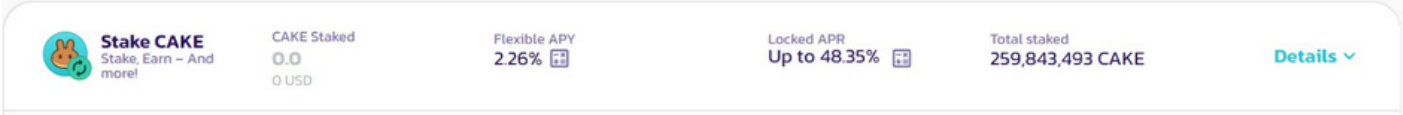
viabilizam (edição de textos, navegação na web, conferência remota etc), os DApps também podem ser assim classificados. Uma das espécies resultantes do emprego desse critério classificatório são os DApps de DeFi.

Programas que rodam localmente, no seu notebook, como o Word e o Chrome, dependem de instalação local. Programas que rodam de forma descentralizada, por sua vez, dependem de instalação no Blockchain. Instalar um programa no computador mundial descentralizado chamado Ethereum (EVM: Ethereum Virtual Machine) significa rigorosamente a mesma coisa que fazer o implante (deploy) de um contrato inteligente no Blockchain do Ethereum.

Para prosseguirmos, então, um esclarecimento adicional deve ser feito: contratos inteligentes são programas que rodam em Blockchains. No sentido comum do termo, portanto, não são contratos, muito menos inteligentes. São simplesmente programas que executam aquilo que foram programados a fazer (autoexecutáveis).

Em um "contrato inteligente", toda vez que a condição A se verifica, o resultado B é produzido. São programas escritos na forma do condicional IF → THEN.

O exemplo a seguir evidenciará porque a compreensão do assunto nos interessa.



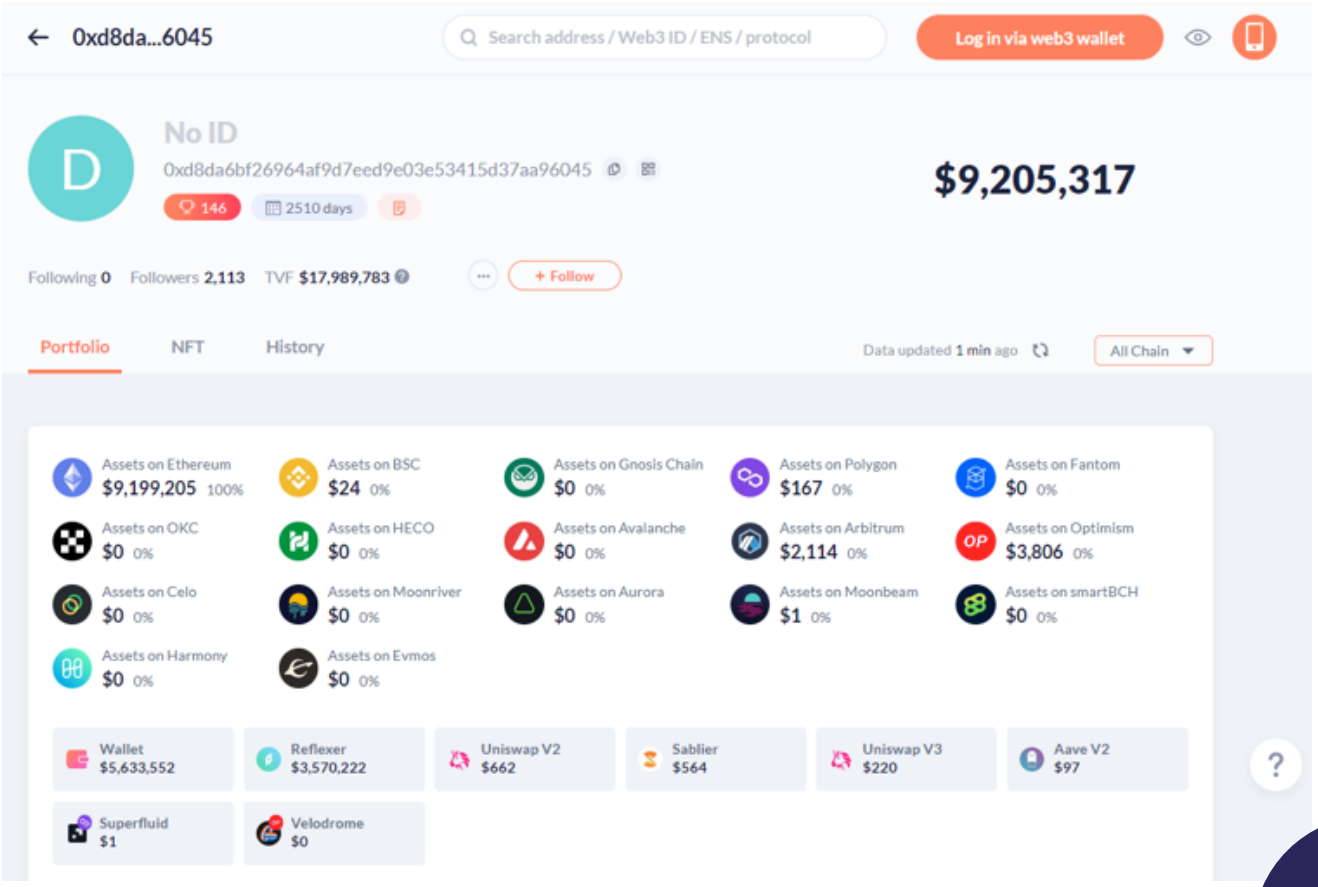
A imagem reproduz uma aplicação de DeFi que, para quem travar (stake) tokens CAKE (IF), confere rendimentos (yield) anualizados de até 48.35%, em tokens CAKE (→ THEN).

Por stake entenda-se o envio de tokens CAKE da sua conta para a conta do contrato inteligente que irá remunerá-lo.

A consequência prática é a de que, a partir desse envio, os tokens não mais estarão no seu endereço e sim no endereço do contrato inteligente. A sua chave privada passará a permitir, então, não mais o imediato envio desses tokens para outro endereço, e sim a recuperação desses tokens, algo com um resgate dos tokens aplicados.

Imaginemos, então, que seja essa a situação do alvo de uma investigação patrimonial. Mesmo que o seu endereço público seja conhecido, os tokens "aplicados" não serão ali encontrados, porque estarão nos endereços de contratos inteligentes de DApps de DeFi.

Essa dificuldade, entretanto, é contornável. Tokens pertencentes ao alvo, temporariamente localizados em algum dos principais endereços de contratos inteligentes de DeFi, podem ser facilmente encontrados mediante o uso de ferramentas online gratuitas, como o https://debank.com/ e o https://apeboard.finance/.



Em outras palavras, pertencem ao alvo não apenas os criptoativos que constem dos seus endereços públicos, mas também aqueles vinculados aos seus endereços públicos que, temporariamente, constem de contratos inteligentes de DeFi.

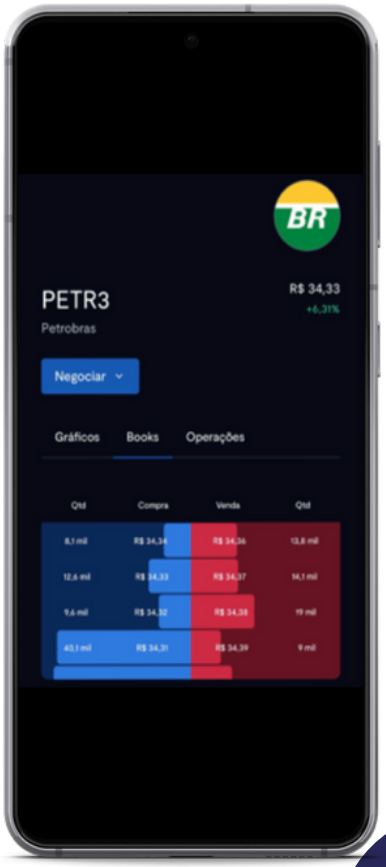
Diante disso, qualquer ato de investigação ou constrição patrimonial que recaia sobre criptoativos custodiados pelo alvo deve considerar a possibilidade de que uma parcela considerável deles esteja temporariamente em outros endereços públicos.

NFTS E SUAS PARTICULARIDADES

NFT é a sigla de non-fungible tokens. Tokens não-fungíveis em tradução literal. Se tokens são ativos digitais que não podem ser copiados, tokens não-fungíveis são ativos digitais que, além de não poderem ser copiados, são únicos, insubstituíveis.

Criptomoedas e tokens fungíveis em geral podem ser negociados nos livros de ofertas de exchanges, assim como ações são negociadas via livro de ofertas na B3. NFTs, por outro lado, não podem – da mesma forma que imóveis e obras de arte, não poderiam - ser negociados via livro de ofertas, ainda que a legislação o permitisse.

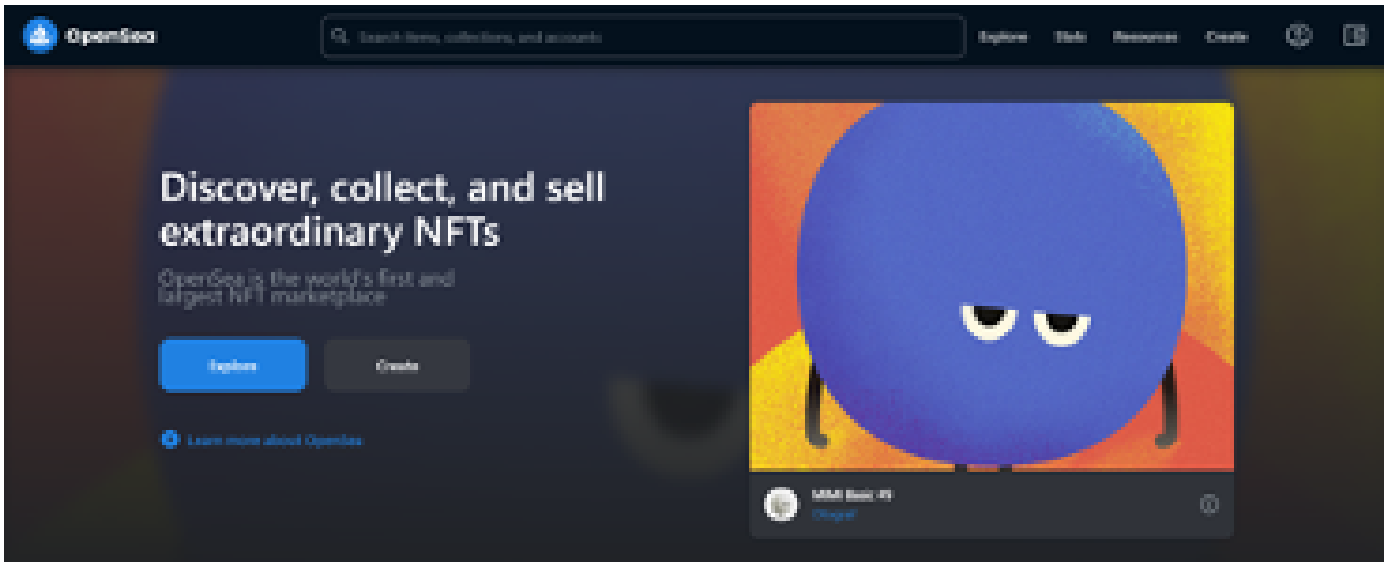
Isso ocorre porque imóveis e obras de arte são bens únicos, ou seja, não-fungíveis. E o livro de ofertas é um instrumento de reunião de interesses contrapostos relativos a um par de coisas fungíveis. Confira-se o exemplo a seguir.



Na imagem ao lado vemos o livro de ofertas (book) do par de negociação BRL (real) e PETR3 (ações ordinárias da Petrobrás). Recorrem a ele as pessoas que querem trocar real por ações ou ações por real, ambos bens fungíveis, não-únicos. Um real equivale a outro real. Uma ação equivale a outra ação.

Imóveis e obras de arte podem ser colocados à venda diretamente por seus proprietários ou esses mesmos proprietários podem recorrer a um intermediário, como uma imobiliária e uma galeria de artes. NFTs, similarmente, podem ser colocados à venda diretamente pelos seus proprietários. O mais comum, no entanto, é que sejam colocados à venda através de um intermediário, uma plataforma que, sem fazer a custódia desses NFTs, dê a eles maior visibilidade e, sobretudo, segurança na negociação.

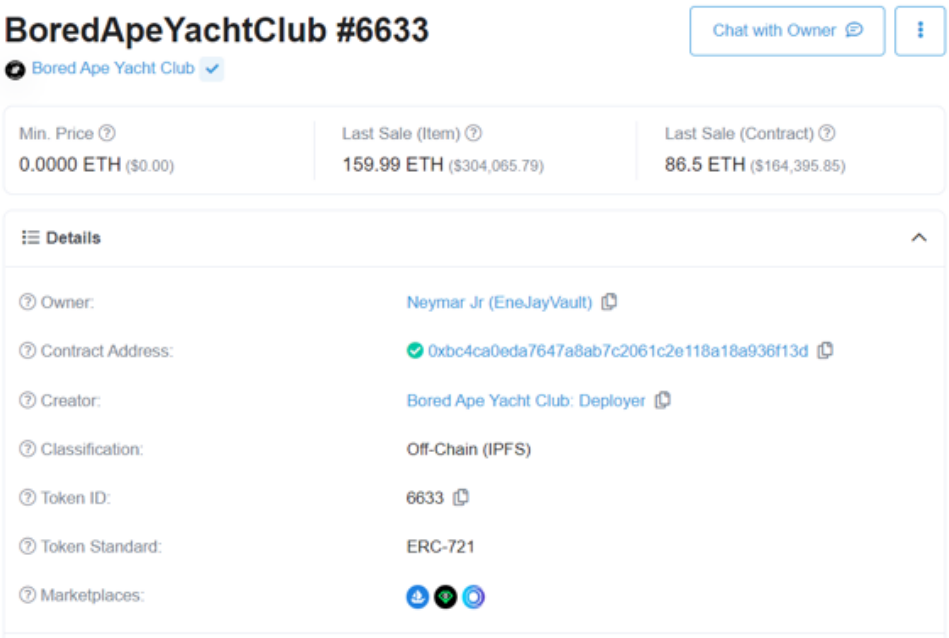
A essas plataformas dá-se o nome de marketplaces e a principal delas, com amplíssima vantagem, é o Opensea (https://opensea.io/).



Não existe nada que particularize a custódia de NFTs. A diferença prática entre tokens fungíveis e NFTs que nos interessa consiste na forma de alienação, com os primeiros tendo por local mais propício à alienação os livros de ofertas de exchanges e os segundos podendo ser alienados via marketplaces.

NFTs não são figurinhas. São, em vez disso, um objeto digital único. E esse objeto digital único não é a mídia que possa estar a ele associada, mas sim um identificador único na Blockchain.

A imagem acima não é um NFT. É a mídia associada ao BAYC #6633, NFT que faz parte da coleção Bored Ape Yatch Club e que atualmente pertence ao jogador de futebol Neymar. Tecnicamente, a imgem reproduzida acima pode ser livremente copiada por terceiros e nada tem de infungível.



O print acima, por outro lado, expõe os dados do referido NFT. Um token com identificação única (6633), vinculado a um contrato inteligente (0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d), implantado em um Blockchain (Ethereum) .

NFTs são a infungibilidade do mundo real[67] trazida para o mundo digital. Em termos menos românticos, são tokens numerados.

Assim como documentos originais, imóveis e obras de arte são fundamentalmente distintos entre si – a despeito de serem todos bens infungíveis – NFTs também podem sê-lo.

Alguns desses NFTs poderão não ter valor algum de mercado (p. ex. documentos), enquanto que outros poderão ter um imenso valor (p. ex. imóveis virtuais e itens de coleções famosas).

Ao que nos interessa. A maneira mais efetiva de alienar NFTs encontrados em carteiras do alvo é através de marketplaces, dada a sua não-fungibilidade, não se devendo recorrer a exchanges nesse caso.

67- Curiosamente, essa imagem do macaco nem no Blockchain está. Ela está em um serviço de armazenamento distribuído chamado IPFS, e o que o NFT em verdade faz é apontar para a sua localização (off-chain).

MODELOS

AFASTAMENTO DE SIGILO FISCAL DE OPERAÇÕES COM CRIPTOATIVOS NO SIMBA

Desta forma, requer o Ministério Público Federal, com base no art. 198 do Código Tributário Nacional, a decretação do afastamento do sigilo fiscal das pessoas físicas e jurídicas relacionadas no quadro abaixo, pelo período informado:

(quadro gerado pelo SIMBA com nome, CPF/CNPJ e período)

Em relação a esses investigados, devem ser encaminhados pela Receita Federal do Brasil, no prazo de 30 (trinta) dias, a contar do recebimento da ordem judicial, todas as informações do investigado relativas a criptoativos de que disponha, tais como: a) declarações de operações com criptoativos (informadas pelo próprio contribuinte ou por exchanges nacionais); b) documentos relacionados ao pagamento de imposto sobre o ganho de capital decorrente da alienação de criptoativos e c) declarações do imposto de renda com informações a respeito de criptoativos.

Para a operacionalização da ordem judicial, requer-se que:

I – Conste da ordem judicial a obrigação da Receita Federal do Brasil enviar os dados e documentação complementar, no formato .txt, .cvs, .xlsx ou, na impossibilidade destes, em .pdf, por meio do SIMBA, em referência ao caso Simba 001-MPF-00XXXX-XX, utilizando o programa "VALIDADOR BANCÁRIO SIMBA", na opção "TRANSMISSÃO DE DOCUMENTOS", cujas orientações encontram-se no endereço eletrônico https://asspaweb.pgr.mpf.mp.br;

II – Conste da ordem judicial que, em caso de dúvidas por parte das instituições destinatárias, o endereço eletrônico para contato com a Secretaria de Perícia, Pesquisa e Análise – SPPEA/PGR é pgr-simba@mpf.mp.br.

AFASTAMENTO DE SIGILO TELEMÁTICO DE OPERAÇÕES COM CRIPTOATIVOS NO SIMBA (EXCHANGES)

Desta forma, requer o Ministério Público Federal, com base na Lei n. 12.965/14 (Marco Civil da Internet), a decretação do afastamento do sigilo telemático das pessoas físicas e jurídicas relacionadas no quadro abaixo, pelo período informado:

(quadro gerado pelo SIMBA com nome, CPF/CNPJ e período)

I. Em relação a esses investigados, devem ser encaminhados pela corretora de criptoativos (...), no prazo de 30 (trinta) dias, a contar do recebimento da ordem judicial:

a) todos os dados e documentos cadastrais seus e de procuradores eventualmente habilitados para o uso de contas suas;

b) informações sobre todas as operações por eles realizadas (seja em criptoativo seja em moeda fiduciária), em planilha contendo campo com o valor em REAL correspondente a cada operação com criptoativos ao tempo em que realizada;

c) sobre cada operação deverá ser informado também o valor correspondente em dólar norte-americano no momento da transação e o saldo remanescente após a transação, bem como:

- Data e hora;
- Identificação do ativo e quantidade;
- Identificação de remetente e do destinatário (incluindo conta bancária ou endereço cripto);
- Valor correspondente em REAL (na data e hora da transação);
- Rede (cripto) e Banco (correspondente bancário), a depender da hipótese (envolvimento de criptoativos e/ou moeda fiduciária na operação);
- Hash ID da transação.

d) informação sobre o saldo atual de cada um dos investigados, discriminado por moeda fiduciária ou espécie de criptoativo, neste último caso com valor atual referenciado em REAL.

II. Para a operacionalização da ordem judicial, requer-se que:

a) Conste da ordem judicial a obrigação da corretora de criptoativos enviar os dados e documentação complementar, no formato .txt, .cvs, .xlsx ou, na impossibilidade destes, em .pdf, por meio do SIMBA, em referência ao caso Simba 001-MPF-00XXXX-XX, utilizando o programa "VALIDADOR BANCÁRIO SIMBA", na opção "TRANSMISSÃO DE DOCUMENTOS", cujas orientações encontram-se no endereço eletrônico https://asspaweb.pgr.mpf.mp.br;

b) Conste da ordem judicial a obrigação das corretoras de criptoativos manterem o sigilo da decisão judicial de quebra, abstendo-se de dar ciência do processo ou da diligência a seus clientes, sob as penas da lei;

c) Conste da ordem judicial que, em caso de dúvidas por parte das instituições destinatárias, o endereço eletrônico para contato com a Secretaria de Perícia, Pesquisa e Análise – SPPEA/PGR é pgr-simba@mpf.mp.br.

BUSCA E APREENSÃO

O MINISTÉRIO PÚBLICO FEDERAL requer, nos termos do art. 240, §1°, alíneas “b”, “c”, “e”, “f” e “h”, do Código de Processo Penal, a expedição de mandados de busca e apreensão criminal com a finalidade de apreender quaisquer documentos, mídias e outras provas encontradas relacionadas aos crimes (...), notadamente, mas não limitado a:

a) registros e livros contábeis, formais ou informais, comprovantes de recebimento/pagamento, prestação de contas, ordens de pagamento, agendas, cartas, atas de reuniões, contratos, cópias de pareceres e quaisquer outros documentos relacionados aos ilícitos narrados nesta manifestação;

b) HDs, laptops, smartphones, pen drives, mídias eletrônicas de qualquer espécie, arquivos eletrônicos de qualquer espécie, agendas manuscritas ou eletrônicas, dos investigados ou de suas empresas, quando houver suspeita que contenham material probatório relevante, como o acima especificado;

c) arquivos eletrônicos pertencentes aos sistemas e endereços eletrônicos utilizados pelos representados, além dos registros das câmeras de segurança dos locais em que se cumpram as medidas;

d) valores em espécie em moeda estrangeira ou em reais de valor igual ou superior a R$ 20.000,00 ou US$ 5.000,00 e desde que não seja apresentada prova documental cabal de sua origem lícita; e

e) dispositivos físicos de armazenamento de chaves de criptoativos (coldwallets, hardwallets ou carteiras frias).

O MPF requer, ainda, que os celulares e tablets apreendidos sejam encaminhados para a Perícia da Polícia Federal imediatamente após a deflagração da operação policial, a fim de que seus dados sejam extraídos e juntados aos autos, devendo ser apresentadas em prazo razoável as análises dos demais aparelhos.

Requer, outrossim, seja determinado por este juízo que os dados sejam extraídos por meio da “extração por sistemas de arquivos”, se possível, uma vez que permite a coleta de um número maior de informações do dispositivo.

Requer, além disso, em relação a todos os equipamentos, mídias eletrônicas e dispositivos físicos de armazenamento de chaves de criptoativos (coldwallets, hardwallets ou carteiras frias) apreendidos, a autorização para acesso a seus conteúdos, e, especialmente em relação aos smartphones, o acesso a todos os dados armazenados na nuvem relacionados a serviços vinculados aos celulares apreendidos.

Quanto aos dispositivos físicos de armazenamento de chaves de criptoativos (coldwallets, hardwallets ou carteiras frias), requer que conste expressamente do mandado de busca e apreensão a autorização para acesso ao seu conteúdo, devendo a autoridade policial diligenciar para a imediata transferência dos ativos encontrados para carteira sob custódia estatal.

CAUTELAR PATRIMONIAL

Isto posto, o MINISTÉRIO PÚBLICO FEDERAL requer a decretação do SEQUESTRO dos bens dos demandados, solidariamente, até o valor de (...).

Para operacionalização da medida de sequestro, o MPF requer:

a) a comunicação da decisão de sequestro às instituições financeiras, por intermédio da técnica de penhora online, prevista no art. 854 do novo Código de Processo Civil e instrumentalizada pelo Sistema de Busca de Ativos do Poder Judiciário – SISBAJUD, relativamente a todas as contas-correntes e aplicações financeiras de titularidade dos requeridos[68], de forma a assegurar que não sejam resgatadas ou transferidas sob qualquer forma. Em caso de não implementação da medida, requer-se desde já a reiteração automática de ordens de bloqueio;

b) cumulativamente, requer a expedição de mandado de sequestro dos criptoativos eventualmente existentes sob custódia das seguintes corretoras (...). Para a efetivação do mandado de sequestro, requer-se igualmente que:

1. conste do mandado que o MPF e a Polícia Federal poderão dar cumprimento às ordens de sequestros diretamente em contato com as corretoras ou, caso não atendidas, vistoriar a própria sede das empresas em busca de ativos;

2. o MPF e a Polícia Federal poderão tem acesso a dispositivos eletrônicos ou de armazenamento, aos e-mails ou telefones, vinculados para fim do duplo fator de autenticação, para realizar a transferência dos valores para a carteira descrita em anexo sob o controle do Estado, para fins de custódia provisória desses criptoativos; e

68- Incluindo ativos mobiliários, como títulos de renda fixa e ações, custódia de ações, títulos privados, títulos públicos e derivativos, aplicações em fundos de investimento, VGBL, PGBL, aplicações em LCA e LCI, aplicações em CDBs, RDBs, COE, ouro e afins, previdência privada e cartas de consórcio.

3. o MPF e a Polícia Federal possam realizar a transferência de valores custodiados, adotando as medidas de execução operacional para o cumprimento da ordem judicial, inclusive a criação de carteira de custódia de criptoativos, a liquidação pelo valor de mercado do dia do criptoativo e a transferência do resultado para conta judicial atrelada aos autos, mediante ordem judicial;

4. o MPF e a Polícia Federal possam transferir para a carteira virtual descrita no documento em anexo os valores em criptoativos eventualmente apreendidos nos mandados de busca e apreensão expedidos no processo n. (...), nessa mesma data protocolado.

c) requer-se o bloqueio via RENAJUD de todos os veículos registrados em nome dos demandados até o valor de (...), cujo ano de fabricação seja superior a 2010 – como objetivo de se evitar bloqueios de veículos antigos sem valor de mercado. Solicita-se que seja inserida anotação no RENAJUD, especificando a restrição como "transferência do veículo, seu licenciamento anual e circulação na via pública";

d) requer-se o bloqueio de embarcações e aeronaves eventualmente registradas em nome dos requeridos, com a expedição de ofício à Capitania dos Portos e à ANAC para efetivar a medida;

e) requer-se o bloqueio de bens imóveis registrados em nome dos demandados até o valor de R$, inserindo a ordem de restrição na CNIB – Central Nacional de Indisponibilidade de Bens[69], instituída na forma do Provimento da Corregedoria Geral de Justiça pelo Provimento n. 39/2014;

f) requer a expedição de mandado à Junta Comercial dos Estados da Federação em que se situam as empresas demandadas, comunicando-lhe a indisponibilidade de todas as cotas integralizadas do capital social das pessoas jurídicas indicadas na tabela acima;

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

g) inserção dos bens no Sistema Nacional de Bens Apreendidos – SBNA do Conselho Nacional de Justiça, na forma da Resolução n. 63, de 16 de dezembro de 2008;

h) a avaliação judicial dos bens imóveis e automotivos eventualmente apreendidos, intimando-se o MPF e o proprietário de seu resultado, e sua homologação judicial;

i) a alienação antecipada dos imóveis e automotivos eventualmente apreendidos, nos moldes do art. 144-A do Código de Processo Penal e da Resolução n. 92/09 do Conselho da Justiça Federal, com vistas a preservar o seu valor, tendo em vista se tratar de bem sujeito a grau acentuado de deterioração e depreciação, bem como por implicar dificuldades e custos do Estado em sua manutenção;

j) o depósito do produto da alienação em conta vinculada ao juízo até a decisão final condenatória da ação penal principal, procedendo-se à sua conversão em renda para a União (art. 91, inciso I, CP);

l) autorize a transmissão da decisão a autoridades estrangeiras em pedidos de cooperação jurídica internacional, com o objetivo de bloquear e repatriar eventuais bens identificados no exterior.

m) autorize o sequestro de bens considerados de alto valor, como obras de arte, veículos e joias encontrados em posse/propriedade dos requeridos, no valor especificado acima, quando do cumprimento dos mandados de busca e apreensão solicitados no processo protocolado nessa data.

73

MPF

Ministério Público Federal