



# MANUAL DE APOIO À INVESTIGAÇÃO DE CRIPTOATIVOS



COORDENAÇÃO GERAL DE REPRESSÃO À CORRUPÇÃO,  
CRIMES FINANCEIROS E LAVAGEM DE DINHEIRO  
DIVISÃO DE REPRESSÃO AOS CRIMES FINANCEIROS  
DFIN/CGRC/DICOR/PF

# **MANUAL DE APOIO À INVESTIGAÇÃO DE CRIPTOATIVOS**

## **Conteudistas**

Aline Pedrini Cuzzuol

Andre Lovatti

Antonio Boson Almeida Junior

Janaina Pereira Lima Palazzo

Saul Tranches Junior

## **Colaboradores**

Alvaro Jose Rinaldi Fogaça

Pedro Alexandre Ferreira da Cunha

## SUMÁRIO

1. INTRODUÇÃO .....	5
2. ASPECTOS HISTÓRICOS.....	9
3. NOÇÕES SOBRE ATIVOS VIRTUAIS .....	17
3.1. Ativo Virtual .....	17
3.2. Blockchain .....	18
3.2.1. Classificação de Blockchain .....	30
3.3. Chave Privada, Chave Pública, Endereço .....	31
3.4. Carteiras de Ativos Virtuais .....	33
3.4.1. Classificação quanto à guarda das chaves privadas .....	33
3.4.1.1. Carteiras de Custódia de Terceiros (ou Carteiras Custodiais) .....	34
3.4.1.2. Carteiras de Custódia Própria (ou não-custodiais) .....	35
3.5. Frase Secreta (Seed).....	37
3.6. Outras classificações de carteiras .....	38
3.7. Transação de ativos virtuais – elementos e funcionamento .....	40
4. ASPECTOS NORMATIVOS .....	44
4.1. A Recomendação 15 do GAFI .....	44
4.2. Instrução Normativa 1888/2019 da Receita Federal do Brasil .....	46
4.3. Parecer de Orientação nº 40 da Comissão de Valores Mobiliários.....	47
4.4. Lei 14.478/2022 .....	48
4.5. Decreto nº 11.563 .....	50
4.6. Solução de Consulta COSIT RFB 217/2023 .....	51
4.7. Solução de Consulta COSIT RFB 218/2023 .....	51
4.8. Lei 14754/2023 .....	52
4.9. Instrução Normativa 2.219/2024 da Receita Federal do Brasil .....	52
5. INVESTIGAÇÃO E PERSECUÇÃO PATRIMONIAL .....	55
5.1. Identificar .....	56
5.2. Rastrear .....	72
5.2.1. Rastreamento On-Chain .....	73
5.2.2. Rastreamento Off-Chain .....	78

<b>5.3. Apreender e Custodiar.....</b>	<b>84</b>
<b>5.3.1. Planejar e preparar a deflagração da operação .....</b>	<b>85</b>
<b>5.3.1.1. Constituição da Equipe de Coordenação da Deflagração .....</b>	<b>86</b>
<b>5.3.1.2. Indicação de Ponto Focal .....</b>	<b>87</b>
<b>5.3.1.3. Indicação de Apoio Técnico.....</b>	<b>87</b>
<b>5.3.1.4. Fornecimento de meios de atuação .....</b>	<b>88</b>
<b>5.3.1.5. Pedidos Judiciais .....</b>	<b>90</b>
<b>5.3.1.6. Criação de Carteira Oficial de Custódia.....</b>	<b>91</b>
<b>5.3.2. Apreensão de Ativos Virtuais .....</b>	<b>93</b>
<b>5.3.2.1. Sequestro de Saldos Representativos de Ativos Virtuais sob Custódia de Terceiros (Fluxo 1) .....</b>	<b>94</b>
<b>5.3.2.2. Apreensão de Ativos Virtuais sob Custódia Própria (Fluxos 2 e 3) .....</b>	<b>95</b>
<b>5.3.2.3. Transferências de Apreensão.....</b>	<b>102</b>
<b>5.3.3. Alienar .....</b>	<b>104</b>
<b>5.3.3.1. Sugestão de rito de alienação .....</b>	<b>107</b>
<b>6. CONSIDERAÇÕES FINAIS .....</b>	<b>112</b>
<b>7. BIBLIOGRAFIA.....</b>	<b>113</b>
<b>8. ANEXOS.....</b>	<b>117</b>

## 1. INTRODUÇÃO

Nos últimos anos, os ativos virtuais têm ganhado destaque não apenas como uma inovação tecnológica e financeira, mas também como um desafio significativo para as autoridades de aplicação da lei em todo o mundo. A Polícia Federal, como uma das principais instituições responsáveis pela segurança e ordem pública no Brasil, enfrenta a tarefa complexa de investigar crimes que envolvem ativos virtuais. Este manual é, portanto, uma ferramenta essencial para capacitar os servidores da Polícia Federal a compreenderem e lidarem eficazmente com esses novos desafios.

Este manual tem como objetivo apoiar o trabalho de policiais que necessitam identificar, apreender, custodiar, alienar e destinar ativos virtuais no contexto de investigações de polícia judiciária. Para isso, reúne fundamentos teóricos e diretrizes investigativas. Inclui também remissões para modelos de representação, informações de polícia judiciária e ofícios para Prestadoras de Serviços de Ativos Virtuais.

A importância deste manual reside em vários aspectos cruciais:

- **Compreensão Técnica:** Ativos virtuais, como Bitcoin e Ethereum, operam em redes descentralizadas e utilizam tecnologias avançadas de criptografia. Para investigar crimes relacionados a esses ativos, é fundamental que os agentes da lei possuam um conhecimento técnico sólido sobre como essas tecnologias funcionam.
- **Identificação de Crimes:** Ativos virtuais podem ser utilizados em uma variedade de atividades ilícitas, incluindo lavagem de dinheiro, financiamento ao terrorismo, fraudes e tráfico de drogas.
- **Cooperação Internacional:** Devido à natureza global dos ativos virtuais, as investigações frequentemente requerem cooperação com outras agências de aplicação da lei e entidades reguladoras internacionais.
- **Atualização Contínua:** O campo dos ativos virtuais está em constante evolução. Portanto, este manual será uma fonte viva de conhecimento, sendo atualizado regularmente para refletir as mudanças tecnológicas e regulatórias.

Tem-se ainda por objetivo sintetizar e reunir boas práticas já identificadas e empregadas em casuísticas de sucesso acompanhadas e apoiadas pela Divisão de Repressão aos Crimes Financeiros (DFIN/CGRC/DICOR/PF) de modo que a expertise

adquirida pelas equipes de trabalho sirva como modelo e seja replicado como solução às diversas investigações que se encontram em curso no âmbito da Polícia Federal.

A ideia foi elaborar um guia prático e de leitura acessível para aqueles que, mesmo sem nenhum conhecimento técnico sobre ativos virtuais, precisem definir balizas de atuação para as investigações, deflagração de operações, custódia, alienação e destinação de ativos virtuais.

Preferimos, para efeitos deste manual, passar a usar o termo “Ativos Virtuais” em substituição ao termo “Criptoativos”, apenas por adequação ao termo usado pela Lei 14.478/2022. Por natureza, porém, os termos têm o mesmo significado. Portanto, caso o leitor encontre o termo “Criptoativo”, tal como no próprio nome deste documento, deve considerar que seu termo sinônimo é “Ativo Virtual” cuja definição será abordada adiante.

A necessidade de enfrentar a questão dos ativos virtuais pela Polícia Federal não é recente. Desde 2017, a demanda por ações específicas nessa área tem sido tratada pela CGRC/DICOR/PF, através da DFIN/CGRC/DICOR/PF. Em resposta, essa divisão desenvolveu uma série de ações de capacitação com o objetivo de sensibilizar, informar e preparar o efetivo para lidar com o uso dessa tecnologia por criminosos. Essas iniciativas culminaram na criação da disciplina “Investigação e Análise de Criptoativos” no Curso de Investigação e Análise Financeira (CIAF), a partir da sua XIV edição.

Em 2019, a DFIN/CGRC/DICOR/PF submeteu à aprovação da DICOR o “Projeto de Criptoativos”, estruturado em três eixos principais: Estudos de Caso, investigação e Capacitação. Este projeto foi classificado como prioritário tanto pela DICOR quanto pelo Ministério da Justiça e Segurança Pública. Desde então, diversas iniciativas foram implementadas para ampliar a capacidade de atuação da Polícia Federal de maneira eficiente e proativa diante dos desafios impostos pela nova tecnologia.

Como resultado, foram disponibilizados ao efetivo diversos recursos, incluindo o Guia de Orientação para Apreensão de Criptoativos, um Curso EAD sobre conhecimentos básicos e identificação do uso e apreensão de criptoativos, e a Capacitação Avançada do Grupo Lince para o uso de ferramentas comerciais de rastreamento. Além disso, foram realizados webinários para a difusão de tipologias comuns utilizadas por criminosos e a Capacitação Avançada CIAF Cripto, que atualmente integra o Plano de Desenvolvimento de Pessoal (PDP) da Academia Nacional de Polícia, com previsão de duas edições anuais.

Complementando essas iniciativas, a DFIN desenvolveu a ferramenta tecnológica de análise “CIAF CRIPTO”, que auxilia na interpretação dos dados fornecidos pela PSAV (Exchange) Binance, responsável por cerca de 80% do mercado brasileiro. Adicionalmente, foi instituído o Laboratório LINCE, dedicado à investigação de casos relacionados a ativos virtuais e ao apoio às investigações em todo o Brasil.

Apesar desses esforços, dada a complexidade e os desafios na identificação e rastreamento de ativos virtuais, há uma constante necessidade de atualização e disseminação de conhecimento para suprir as lacunas relacionadas ao uso de ativos virtuais por organizações criminosas.

Nesse contexto, os aspectos técnicos relativos à custódia e transferência de ativos virtuais continuam a gerar insegurança entre os servidores da Polícia Federal. Mesmo com a publicação, em 2021, de um consistente Manual de Busca e Apreensão de Ativos Virtuais pela DITEC, que orienta a atuação dos Peritos Federais e esclarece os requisitos mínimos de segurança para a atuação policial, ainda persistem dúvidas sobre a atuação segura dos investigadores.

Diante desses desafios, este manual foi elaborado para fornecer uma compreensão abrangente e detalhada sobre os ativos virtuais, abordando desde sua origem até os procedimentos específicos de investigação e apreensão. Nos capítulos que se seguirão, serão explorados os seguintes tópicos:

- **Aspectos Históricos dos Ativos virtuais:** Este capítulo traçará a evolução dos ativos virtuais, desde a concepção inicial de moedas digitais até o desenvolvimento das principais criptomoedas atuais. Analisaremos os marcos históricos e as inovações tecnológicas que moldaram o cenário dos ativos virtuais.
- **Noções básicas sobre Ativos Virtuais:** Capítulo em que serão apresentadas definições e características básicas sobre criptoativos, tipos, tecnologia blockchain, e carteiras.
- **Aspectos Normativos dos Ativos virtuais no Brasil:** Abordaremos a legislação e regulamentação vigente no Brasil relacionada aos ativos virtuais. Este capítulo fornecerá uma visão detalhada das normas que regem o uso, a negociação e a fiscalização dos ativos virtuais no país, destacando as principais leis e diretrizes emitidas por órgãos reguladores.

- **Investigação e Persecução Patrimonial de Ativos virtuais:** Focaremos nas metodologias e técnicas de investigação aplicáveis aos ativos virtuais. Este capítulo incluirá estratégias para rastreamento de transações, identificação de atividades ilícitas e cooperação internacional, além de ferramentas e recursos disponíveis para os investigadores. Além disso, detalharemos os procedimentos para a apreensão segura e alienação de ativos virtuais incluindo os aspectos legais e operacionais.

Esses capítulos foram estruturados para fornecer uma base sólida de conhecimento e práticas recomendadas, capacitando os servidores da Polícia Federal a lidar de maneira eficaz e segura com os desafios impostos pelos ativos virtuais.



## 2. ASPECTOS HISTÓRICOS

A ideia de criar uma moeda descentralizada e livre de uma autoridade central remonta ao ano de 1998 e foi proposta inicialmente por *Nick Szabo*<sup>1</sup> com o nome “*Bit Gold*”, considerado o antecessor do Bitcoin<sup>2</sup>. Szabo também é apontado como o idealizador dos “contratos inteligentes”.

Anos depois, em 29 de dezembro de 2005, Szabo publicou no blog “*Unenumerated*” o artigo “*Bit Gold*”<sup>3</sup> no qual se refere à ideia previamente concebida em 1998. De acordo com Szabo, um problema inerente ao dinheiro fiduciário é que seu valor depende da confiança depositada em um terceiro, papel exercido por uma autoridade central dotada de prerrogativa para tal.

O problema, em poucas palavras, é que nosso dinheiro atualmente depende da confiança em uma terceira parte. Como muitos episódios inflacionários e hiperinflacionários durante o século XX demonstraram, este não é um estado de coisas ideal.

No mesmo artigo, Szabo apresentou as principais etapas do sistema Bit Gold, bem como as ideias dos algoritmos de prova de trabalho que são usadas atualmente pelo sistema do Bitcoin e de outras criptomoedas<sup>4</sup>.

---

<sup>1</sup> De acordo com a Binance, Nick Szabo é “o pai do Bit Gold”. Acessível em <https://www.binance.com/en/square/post/669178305602>. Acessado em 24/08/2024.

<sup>2</sup> De acordo com a Binance, “Nick Szabo inventou o Bit gold em 1998, um esboço para uma criptomoeda descentralizada usando “mineradores de bit gold” para resolver ‘quebra-cabeças matemáticos complexos’. Acontece que o Bit Gold usa o algoritmo de prova de trabalho do Bitcoin: Hashcash de Adam Back. É importante ressaltar que Szabo se refere ao Bit gold como o ‘design antecessor’ do Bitcoin”. Acessível em <https://www.binance.com/pt-BR/square/post/7692072862561?ref=49193790>. Acesso em 24/08/2024.

<sup>3</sup> O artigo original é acessível através da ferramenta WaybackMachine em <https://unenumerated.blogspot.com/2005/12/bit-gold.html>. Acesso em 24/08/2024. O artigo também foi replicado no sítio eletrônico <https://nakamotoinstitute.org>, acessível em <https://nakamotoinstitute.org/library/bit-gold/>. Acesso em 24/08/2024.

<sup>4</sup> Criptomoedas são um tipo específico de ativo virtual que funciona como uma forma de moeda digital, utilizando criptografia e uma rede descentralizada (geralmente baseada em blockchain) para garantir a

Minha proposta para Bit Gold é baseada na computação de uma sequência de bits a partir de uma sequência de bits de desafio, usando funções chamadas de 'função de quebra-cabeça do cliente', 'função de prova de trabalho' ou 'função de benchmark segura'. A sequência de bits resultante é a prova de trabalho.

Em 31 de outubro de 2008, 10 anos após a ideia inicial de Szabo, e quase três anos de sua publicação no blog *Unenumerated*, um pequeno artigo intitulado "*Bitcoin: A Peer-to-Peer Electronic Cash System*", de autoria de *Satoshi Nakamoto*, foi encaminhado para uma lista de discussão de criptografia denominada "*The Cryptography Mailing list*"<sup>5</sup> hospedada no sítio eletrônico metzdowd.com.

Em linhas gerais, esse artigo propunha a adoção de uma solução para contornar as deficiências inerentes aos processos de pagamentos eletrônicos, intermediados por instituições financeiras e baseados na confiança. Nakamoto sugeriu a possibilidade de que duas partes envolvidas em um negócio jurídico pudessem realizar pagamentos ou transferências de recursos sem a necessidade da intermediação de uma instituição financeira. Neste caso, a confiança seria substituída pela prova criptográfica em meio eletrônico e pela ideia de moeda eletrônica<sup>6</sup>, assim constituída como um encadeamento de assinaturas digitais. Esse artigo de Nakamoto é amplamente aceito como o documento que instituiu as bases do Bitcoin, estabelecendo os fundamentos teóricos e tecnológicos que o amparam.

---

segurança das transações, controlar a criação de novas unidades e verificar a transferência de ativos. Ativo Virtual é gênero; criptomoeda é espécie.

<sup>5</sup> Atualmente este artigo pode ser lido no sítio eletrônico <https://satoshi.nakamotoinstitute.org>, acessível em <https://satoshi.nakamotoinstitute.org/emails/cryptography/1/>. Acesso em 24/08/2024.

<sup>6</sup> O termo "moeda eletrônica" empregado por Satoshi Nakamoto diverge da definição de moeda eletrônica adotada pelo Banco Central do Brasil, tal qual previsto na Lei 12.865/2013, a saber: "moeda eletrônica - recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento."

Em 12 de janeiro de 2009 ocorreu a primeira transação de Bitcoin quando *Satoshi Nakamoto* transferiu 10 Bitcoins (10 BTC) para *Hal Finney*<sup>7</sup>, operação que pode ser visualizada<sup>8</sup> na rede blockchain, cujo excerto dessa transação histórica apresentamos.

Advanced Details			
Hash	f418-9e16	ID do Bloco	170
Posição	1	Hora	12 Jan 2009 01:30:25
Idade	15y 2m 15d 16h 20m 43s	Entradas	1
Valor de entrada	50.00000000 BTC	Saídas	2
	\$0.00	Valor de saída	50.00000000 BTC
Comissão	0 BTC		\$0.00
	\$0.00	Comissão/B	-
Comissão/VB	-	Tamanho	275 Bytes
Peso	1.100	Weight Unit	-
Coinbase	No	Testemunha	No
RBF	No	Locktime	0
Versão	1		

Overview

JSON

De

1 Satoshi 2 50.00000000 BTC • \$0.00

Para

1 Hal Finney 10.00000000 BTC • \$0.00

2 Satoshi 2 40.00000000 BTC • \$0.00

Figura 1-Primeira transação de Bitcoin da história extraída do bloco gênese do Bitcoin

Em 2010, respectivamente em março e julho, foram criadas as primeiras negociadoras<sup>9</sup> de criptomoedas, a Bitcoinmarket.com e a Mt.Gox, ambas extintas. Atualmente, as dez principais negociadoras de criptomoedas do mundo<sup>10</sup>, de acordo com

<sup>7</sup> De acordo com a Binance, Hal Finney é o pioneiro por trás do Bitcoin e da criptografia digital. Acessível em <https://www.binance.com/pt-BR/square/post/10667997231001>. Acessado em 24/08/2024.

<sup>8</sup> Acessível em <https://www.blockchain.com/pt/explorer/transactions/btc/f4184fc596403b9d638783cf57adfe4c75c605f6356fb-c91338530e9831e9e16>. Acesso em 18/04/2024.

<sup>9</sup> Preferimos não usar o termo “Corretora” por dois motivos: evitar confusão com corretoras de valores mobiliários; esse termo pode não abranger todos os serviços prestados por uma empresa atuante no mercado de ativos virtuais

<sup>10</sup> A CoinMarketCap classifica e pontua as corretoras com base no seguinte: Fator de Tráfego no Site; Média de Liquidez; Volume, assim como a Confiança de que o volume informado pela corretora é legítimo. Os pesos

o sítio eletrônico [coinmarketcap.com](https://coinmarketcap.com), são, nesta ordem: Binance, Coinbase, Okx, Bybit, Upbit, Kraken, Gate.io, HTx-antiga Huobi, Bitfinex e, KuCoin. As negociadoras brasileiras Mercado Bitcoin e Foxbit aparecem, respectivamente, no 77º e 84º lugares, segundo o mesmo ranking.

Passaremos, para efeitos deste manual, a usar o termo “Prestadora de Serviços de Ativos Virtuais” (PSAV) para nos referirmos a qualquer empresa que atue no mercado de ativos virtuais realizando: troca entre ativos virtuais e moeda nacional ou moeda estrangeira; troca entre um ou mais ativos virtuais; transferência de ativos virtuais; custódia ou administração de ativos virtuais ou de instrumentos que possibilitem controle sobre ativos virtuais e; participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda de ativos virtuais. Trata-se de um termo mais abrangente em relação ao termo “negociadora” e alinhado com os ditames da Lei 14.478/2022.

A partir de 2011 começaram a surgir as primeiras criptomoedas alternativas ao Bitcoin, as chamadas “Altcoins”, termo que é usado para identificar todas as criptomoedas diferentes do Bitcoin. Atualmente existem milhares de altcoins criadas por motivações variadas. De fato, algumas altcoins surgiram com o intuito de aperfeiçoar as funcionalidades do Bitcoin, outras para explorar novas funcionalidades, ou ainda apenas como objeto de especulação ou usadas para captar recursos como instrumentos de fraudes financeiras.

A primeira altcoin foi a Namecoin que surgiu em abril de 2011 a partir da bifurcação<sup>11</sup> do código fonte do Bitcoin. Logo depois, em outubro de 2011, surgiu a altcoin Litecoin, também derivada de bifurcação do código fonte do Bitcoin. E em seguida a Dogecoin, em dezembro de 2013.

---

são atribuídos aos fatores mencionados acima e a Corretora recebe a pontuação de 0,0 a 10,0. Acessível em <https://coinmarketcap.com/pt-br/rankings/exchanges/>. Acesso em 24/08/2024.

<sup>11</sup> Em linhas gerais as altcoins são criadas de três maneiras: i) por meio de uma bifurcação ou “fork” que nada mais é do que um novo projeto a partir de um código fonte pré-existente; ii) por meio da criação de uma blockchain própria na qual a nova moeda é chamada de moeda nativa; iii) por meio do uso de blockchain pré-existente que serve de suporte para as novas criptomoedas.

Em 2014 surgiu o token<sup>12</sup> Tether (USDT), sendo a primeira “Stablecoin”<sup>13</sup>, termo que se refere ao ativo virtual que se diz estável, pois mantém seu valor vinculado a uma moeda fiduciária. O Tether (USDT) está pareado com o dólar americano, significando dizer que 1 Tether (USDT) corresponde a 1 dólar americano. Foi inicialmente emitido na blockchain de Bitcoin, mas, atualmente é emitido em larga escala nas blockchains Ethereum e Tron, dentre outras.

Atualmente, a altcoin mais expressiva do mercado é a Ether, que é a criptomoeda nativa da blockchain Ethereum, criada em 2015. A blockchain Ethereum difere da blockchain do Bitcoin porque além de permitir transferências de ativos, tal como esta, também permite a criação de aplicativos, de tokens fungíveis e não fungíveis (NFT), de jogos, a realização de ofertas iniciais de criptomoedas (ICO), dentre outras funcionalidades. Trata-se, como veremos adiante, de uma blockchain de segunda geração, diferente da blockchain do Bitcoin, que é de primeira geração.

A partir de 2017, com o advento da rede Ethereum, surgiram os NFT, abreviação de Non-fungible Token ou token não fungível, isto é, uma representação digital de um item exclusivo cujo detentor exerce direito de propriedade sobre ele. Por exemplo, uma arte gráfica digital. Dito de outro modo, é o direito de propriedade sobre algo infungível garantido por uma certificação digital da blockchain.

Os chamados contratos inteligentes (Smart Contracts), apesar de idealizados por Nick Szabo ainda no fim do século passado, só se tornaram possíveis a partir do surgimento da rede Ethereum. Esses contratos inteligentes nada mais são do que programas computacionais executáveis de modo automático, caso uma condição seja satisfeita, de acordo com a regra “se-então”. Para esclarecer o funcionamento dos contratos

---

<sup>12</sup> Token é unidade digital de valor emitida em uma rede blockchain, a partir de contratos inteligentes, que representa algum tipo de ativo ou direito. Ele pode ser utilizado para diversas finalidades, como meio de troca, acesso a serviços ou produtos, ou mesmo para representar a propriedade de um ativo físico ou digital

<sup>13</sup> Stablecoin é um tipo de ativo virtual projetado para manter um valor estável, geralmente atrelado a um ativo de referência, como uma moeda fiduciária (por exemplo, o dólar americano), um bem físico (como ouro) ou uma cesta de ativos. O objetivo das stablecoins é mitigar a volatilidade associada a outros ativos virtuais, como Bitcoin e Ethereum, tornando-as mais adequadas para uso como meio de troca e reserva de valor em aplicações cotidianas.

inteligentes, Szabo usou o exemplo da máquina de venda automática de refrigerantes<sup>14</sup>: se o comprador paga o preço então tem acesso ao refrigerante; se o comprador paga a maior deve então receber o troco e ter acesso ao refrigerante; se o comprador não paga, então não tem acesso ao refrigerante. Nesse tipo de relação qualquer pessoa que detém moedas ou notas suficientes seria capaz de participar da troca com a máquina.

Szabo propôs que este modelo fosse replicado para qualquer tipo de bem valioso suscetível de controle por meio digital. Szabo ainda ofereceu outro exemplo, aplicável à venda de carros compostos por sistemas de segurança digital. Imaginemos um carro vendido em prestações. Inicialmente o comprador, mediante o cumprimento de protocolos contratuais (exemplo: pagar o sinal), teria acesso às chaves criptográficas que permitem dar partida no carro. Se, no entanto, as prestações deixarem de ser liquidadas, o comprador perderia, em dado momento e segundo as regras contratuais, o controle sobre as chaves criptográficas de partida que retornariam, então, à posse do vendedor. Isso tudo seria efetivado de forma automática.

O gráfico a seguir apresenta a cronologia histórica dos ativos virtuais.

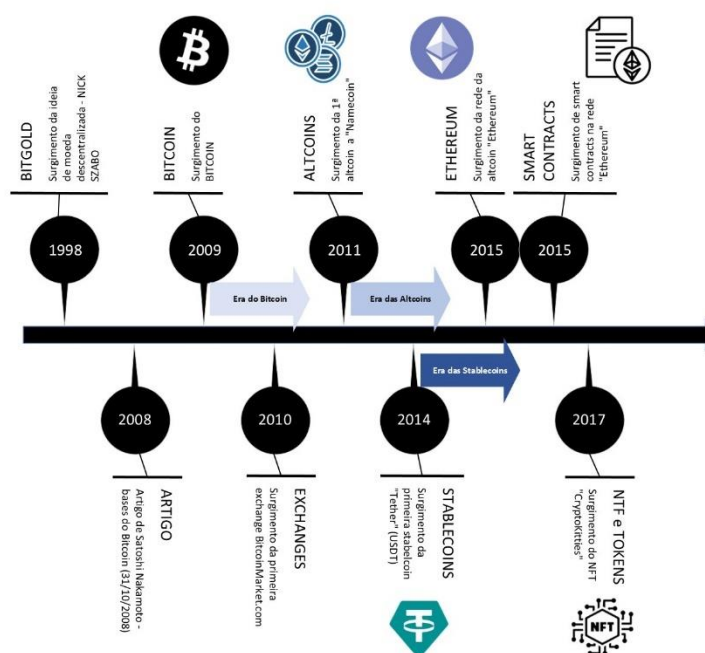


Figura 2-Cronologia histórica dos ativos virtuais

<sup>14</sup> Acessível em <https://nakamotoinstitute.org/library/the-idea-of-smart-contracts/>. Acessado em 26/08/2024.

---

## Glossário dos principais termos citados neste capítulo

---

**Altcoin:** termo que se refere a todas as criptomoedas que surgiram após o Bitcoin. Elas são alternativas ao Bitcoin e geralmente apresentam variações em suas tecnologias, funções, ou protocolos de consenso. Exemplos: Ethereum (ETH), Litecoin (LTC) e Ripple (XRP).

---

**Ativo Virtual:** uma representação digital de valor que pode ser transacionada, armazenada ou trocada eletronicamente. Esses ativos podem incluir criptomoedas, tokens e outros tipos de ativos digitais que utilizam tecnologias blockchain para garantir sua segurança e descentralização. Ativos virtuais não têm uma existência física e não são necessariamente lastreados por moeda fiduciária. É gênero do qual são espécies: criptomoedas, tokens fungíveis, tokens não fungíveis, finanças descentralizadas etc.

---

**Bitcoin:** primeira criptomoeda descentralizada, criada em 2009 por uma entidade desconhecida sob o pseudônimo de Satoshi Nakamoto. Utiliza tecnologia blockchain para permitir transações seguras e descentralizadas sem a necessidade de uma autoridade central. O Bitcoin opera em um protocolo de proof-of-work (PoW), onde a mineração de novos blocos requer a solução de problemas matemáticos complexos.

---

**Blockchain:** tecnologia de registro distribuído que armazena dados de forma descentralizada e imutável. Consiste em uma cadeia de blocos de transações, onde cada bloco está ligado ao anterior por meio de hashes criptográficos. A blockchain é usada como a base de vários ativos virtuais, garantindo que as transações sejam verificadas e seguras sem depender de uma entidade centralizada. Também pode ser entendido como o próprio registro. Portanto, podemos usar o termo “a blockchain” para nos referirmos à tecnologia e; podemos usar o termo “o blockchain” para nos referirmos ao conjunto de registros públicos de transações gravadas em blocos. Existem diversas blockchains independentes, cada uma com suas respectivas criptomoedas nativas. Exemplos: Blockchain Bitcoin, Blockchain Ethereum, Blockchain Tron.

---

**Contrato Inteligente (Smart Contract):** é um programa autoexecutável assentado em uma blockchain que contém regras e instruções para realizar transações automaticamente quando condições predefinidas são atendidas. São encontrados em plataformas como o Ethereum e podem ser usados para criar tokens, realizar empréstimos descentralizados, ou automatizar qualquer tipo de processo financeiro.

---

**Criptoativo:** termo abrangente que inclui qualquer tipo de ativo digital que utilize a tecnologia blockchain ou criptografia para garantir sua segurança e autenticidade. É sinônimo de Ativo Virtual.

---

**Criptomoeda:** é uma espécie de ativo digital que utiliza técnicas de criptografia para garantir a segurança das transações e o controle da criação de novas unidades. As criptomoedas são descentralizadas,

---

---

geralmente operando em redes de blockchain, e podem ser usadas como meio de troca, reserva de valor ou unidade de conta. Exemplos incluem Bitcoin (BTC) e Ethereum (ETH).

---

**Ethereum:** é uma plataforma de blockchain descentralizada que permite a execução de contratos inteligentes sobre ela. Criada por Vitalik Buterin em 2015, oferece um ambiente para desenvolver aplicativos descentralizados (dApps). A moeda nativa da rede Ethereum é o Ether (ETH), que também é usada como combustível (gas) para executar contratos inteligentes na rede.

---

**Prestadora de Serviço de Ativo Virtual (PSAV):** é uma entidade ou empresa que oferece serviços relacionados à negociação, troca, custódia ou gerenciamento de ativos virtuais. Esses serviços podem incluir negociadoras de criptomoedas, vulgarmente conhecidas como exchanges, custodiantes, ou processadores de pagamento que aceitam ou facilitam transações com criptoativos. Sua definição legal é determinada pelo artigo 5º da Lei 14.478/2022 e acompanha o conceito difundido pelo GAFI.

---

**Stablecoin:** é um tipo de ativo virtual projetado para manter um valor estável, geralmente atrelado a um ativo subjacente, como uma moeda fiduciária (ex: dólar americano), uma commodity (ex: ouro) ou uma cesta de ativos. O objetivo das stablecoins é reduzir a volatilidade inerente às criptomoedas tradicionais, como o Bitcoin, tornando-as mais adequadas para uso como meio de troca e reserva de valor. Atualmente são amplamente usadas no ambiente criminoso.

---

**Tether (USDT):** é um token com característica de stablecoin que busca manter um valor estável, atrelado ao dólar americano na proporção de 1:1. Ele é suportado por reservas de ativos fiduciários que garantem sua paridade com o dólar. Tether é amplamente utilizada em mercados de ativos virtuais para transferir valor rapidamente sem a volatilidade associada a outras criptomoedas. O Tether (USDT) é emitido pela empresa Tether Limited, que é uma subsidiária do grupo iFinex Inc., também responsável pela operação da negociadora de ativos virtuais Bitfinex. A Tether Limited é responsável por garantir que cada unidade de USDT emitida seja lastreada por reservas de ativos que incluem moedas fiduciárias, como o dólar americano, e outros ativos financeiros.

---

**Token:** são ativos virtuais emitidos em redes de blockchain através de contratos inteligentes. Eles podem representar uma ampla variedade de direitos e propriedades. O mais conhecido deles no ambiente da investigação criminal da Polícia Federal é o Tether (USDT).

---

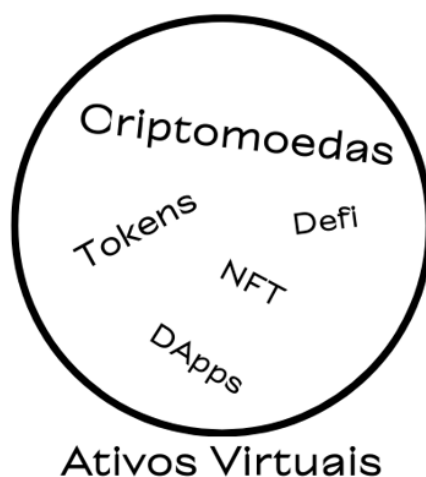


### 3. NOÇÕES SOBRE ATIVOS VIRTUAIS

Neste capítulo, serão apresentadas as noções fundamentais sobre ativos virtuais, incluindo uma análise das características que os diferenciam dos ativos tradicionais. Serão discutidos conceitos-chave como blockchain, chaves assimétricas, descentralização, carteiras, frase secreta, tokens e contratos inteligentes.

#### 3.1. Ativo Virtual

Ativo Virtual é uma representação digital de valor que pode ser transacionada, armazenada ou trocada eletronicamente. Esses ativos podem incluir criptomoedas, tokens e outros tipos de ativos digitais que utilizam tecnologias blockchain para garantir sua segurança e descentralização. Ativos virtuais não têm uma existência física e não são necessariamente lastreados por moeda fiduciária. É gênero do qual são espécies: criptomoedas, tokens fungíveis, tokens não fungíveis, finanças descentralizadas, aplicações descentralizadas etc.



*Figura 3-Espécies de Ativo Virtual*

A Lei 14.478/2022, conhecida como a Lei de Ativos Virtuais, trouxe a seguinte definição:

Ativo virtual é a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realizar pagamentos ou com a finalidade de investimento.

Trata-se de conceito enunciado no glossário de definições do Grupo de Ação Financeira Internacional (GAFI) a partir do qual a legislação brasileira se inspirou. Com

efeito, desde ao menos 2014, através do relatório “*Virtual Currencies Key Definitions and Potential AML/CFT Risks*”<sup>15</sup>, o GAFI já trazia o conceito de moeda virtual e sua diferenciação em relação à moeda eletrônica:

A moeda virtual é uma representação digital de valor que pode ser negociada digitalmente e funciona como um meio de troca; e/ou uma unidade de conta; e/ou uma reserva de valor, mas não tem curso legal em qualquer jurisdição. Não é emitida nem garantida por qualquer jurisdição e cumpre as funções acima somente por acordo dentro da comunidade de usuários da moeda virtual. A moeda virtual é distinta da moeda fiduciária (também conhecida como “moeda real”, “dinheiro real” ou “moeda nacional”), que é a moeda e o papel-moeda de um país designada como moeda com curso legal; circula; e é habitualmente utilizada e aceita como meio de troca no país emissor. É distinta de dinheiro eletrônico, que é uma representação digital de moeda fiduciária usada para transferir valor eletronicamente denominado em moeda fiduciária. O dinheiro eletrônico é um mecanismo de transferência digital para moeda fiduciária – ou seja, transfere eletronicamente valor com curso legal.”

Em 2019 o termo “moeda virtual” foi substituído por “ativo virtual”, oportunidade em que a definição foi ratificada pelo GAFI no documento “*Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*”<sup>16</sup> nos seguintes termos:

Ativo virtual é uma representação digital de valor que pode ser negociado ou transferido digitalmente e pode ser usado para fins de pagamento ou investimento. Os ativos virtuais não incluem representações digitais de moedas fiduciárias, títulos e outros ativos financeiros que já são abrangidos em outras partes das Recomendações do GAFI.

### 3.2. Blockchain

---

<sup>15</sup> Acessível em <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html>. Acesso em 19/08/2024.

<sup>16</sup> Acessível em <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html>. Acesso em 19/08/2024.

As transações de ativos virtuais são feitas em um meio eletrônico amparado pela tecnologia conhecida como blockchain. A blockchain nada mais é, sob a ótica tecnológica, do que um ambiente eletrônico distribuído de registro público de transações. Mas também, é a nomenclatura utilizada para o próprio registro. Portanto, quando falamos em blockchain podemos estar nos referindo à tecnologia ou ao próprio conjunto de registros. Daí derivam as falas “a blockchain” (tecnologia) e “o blockchain” (conjunto de registros).

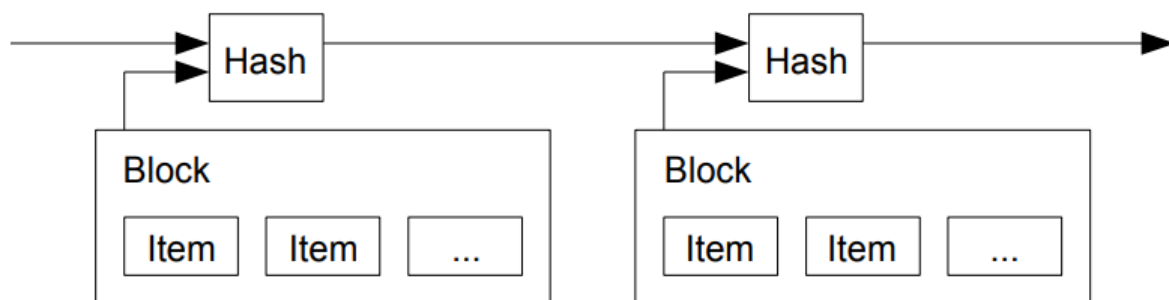
Foi inicialmente idealizada para resolver o problema cronológico inerente às transações financeiras comuns de modo a torná-las mais seguras. De fato, existe um problema cronológico intrínseco às operações financeiras que se traduz pela dificuldade de se garantir a ordem correta das transações. Para esclarecer, imaginemos uma transação em que uma pessoa “A” tenha em sua conta bancária R\$ 1.000,00 e queira fazer dois pagamentos online simultâneos. No primeiro, “A” tenta comprar um celular de R\$ 1.000,00 e no segundo “A” tenta comprar um tênis de R\$ 1.000,00. Neste caso o banco de “A” evitará o problema de gasto duplo porque antes de efetivar a transação verificará o saldo de “A” e processará a primeira transação que estiver na ordem. Caso não houvesse esta autoridade central (banco) para validar a transação, teoricamente o gasto duplo seria possível, mesmo havendo dinheiro suficiente para a realização de apenas uma das compras.

Note que quem detém o conhecimento histórico-cronológico sobre as transações de “A”, além dele próprio, é o banco com o qual se relaciona, sendo este o possuidor dos mecanismos de verificação de gasto duplo. A burla somente não ocorre no mundo real porque a transação é garantida por uma autoridade central confiável (banco), e somente por esta.

Considerando esse teórico problema, Satoshi Nakamoto sugeriu que as transações fossem registradas publicamente de modo que os participantes da transação (contrapartes) concordassem com uma única história da ordem das transações, eliminando a necessidade de verificação de “gasto duplo” por uma autoridade central. Nas palavras do próprio Nakamoto:

*The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.<sup>17</sup>*

Para tal solução, Nakamoto idealizou a criação de uma cadeia de blocos que se inicia com um hash<sup>18</sup> de um bloco de itens (transações). Este hash é amplamente publicizado provando sua existência. As próximas transações são registradas em um novo bloco de itens que inclui, além do seu próprio hash, o hash anteriormente publicado, formando então uma cadeia. Vejamos a figura difundida por Nakamoto<sup>19</sup> para representar a cadeia de blocos.



*Figura 4-Cadeia de Blocos segundo Nakamoto*

Tendo em consideração a ideia de Nakamoto, podemos definir a blockchain como um banco de dados digital avançado no qual transações são registradas como um livro-razão digital público, composto pela prova das transações anteriores e a prova da transação atual, garantindo a integridade dos registros.

Os blocos que compõem a blockchain são formados por lotes de transações (Nakamoto as chama de itens) em que cada uma delas tem um tamanho digital. A quantidade de transações em um bloco pode variar conforme as especificações técnicas da rede blockchain a que se refere. Por exemplo, atualmente cada bloco de Bitcoin carrega

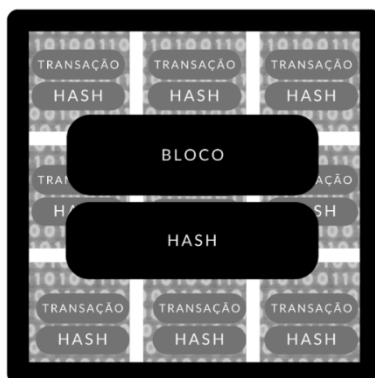
---

<sup>17</sup> Bitcoin: A Peer-to-Peer Electronic Cash System. Acessível em <https://bitcoin.org/bitcoin.pdf>. Acessado em 26/08/2024.

<sup>18</sup> Hash é um algoritmo matemático eletrônico que transforma um dado de entrada em um conjunto alfanumérico com comprimento fixo de caracteres e é utilizado para verificar a integridade de arquivos digitais, dentre outras utilidades.

entre 1.5 e 1.8 megabytes<sup>20</sup>, isto é, cada bloco compila um conjunto de transações que quando somadas alcançam esse tamanho digital, independentemente da quantidade de transações, pois, como dito, cada uma delas pode ter um tamanho diverso.

Cada uma das transações detém seu próprio hash e, por sua vez, o bloco formado pelo conjunto de transações também detém seu próprio hash. Portanto, podemos afirmar que o hash do bloco é o resultado da solução do algoritmo matemático de todas as transações contidas no lote.

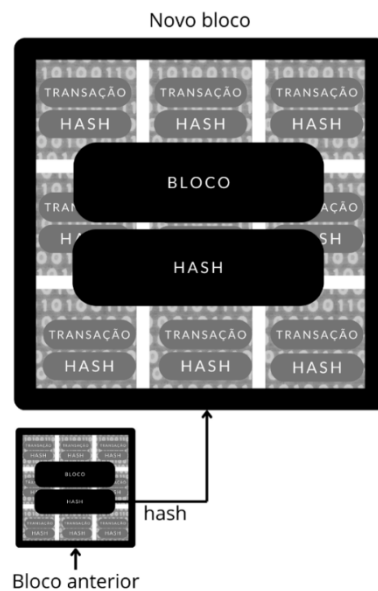


*Figura 5-Ilustração de bloco de transação da blockchain*

Quando novas transações forem realizadas formarão um novo bloco que conterà não só as transações deste lote, mas também o hash (e somente o hash) do bloco anterior. Dito de outro modo e em linguagem leiga, o hash do bloco atual é a soma do lote atual com o hash do bloco anterior. Mas, como o bloco anterior também é a soma do lote dele próprio com o seu respectivo lote imediatamente anterior, podemos afirmar que quando um bloco é validado, sendo ele, por exemplo, o 100º bloco, na verdade estarão sendo validados o bloco atual e todos os blocos anteriores, sendo que: o 1º bloco pela 100ª vez, o 2º bloco pela 99ª, o 3º bloco pela 98ª vez, e assim por diante até chegar ao 100º bloco que estará sendo validado pela 1ª vez. Quando o 101º bloco sobrevier, o 100º bloco será validado pela 2ª vez, pois estará contido na validação do 101º bloco que será validado pela 1ª vez.

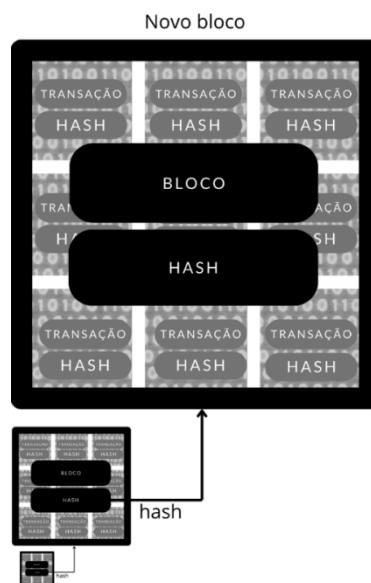
---

<sup>20</sup> Fonte: [https://ycharts.com/indicators/bitcoin\\_average\\_block\\_size](https://ycharts.com/indicators/bitcoin_average_block_size). Acesso em 19/08/2024.



*Figura 6-Ilustração representativa da cadeia de blocos*

E assim por diante.



*Figura 7-Ilustração representativa da cadeia de blocos*

Sendo assim, cada bloco na blockchain contém um conjunto de transações e um “retrato” digital do bloco anterior, que é dado pelo hash, de modo a formar uma cadeia contínua de blocos que garante a autenticidade e integridade dos registros, tornando-os imutáveis e resistentes a adulterações.

A blockchain é dotada de diversas características dentre as quais destacam-se:

**Distribuição:** para contornar o problema cronológico já mencionado, a solução dada foi a supressão do poder da autoridade central de validação, de modo a distribuir este poder para uma rede de nós independentes, que nada mais são do que computadores detentores de uma via<sup>21</sup> completa atualizada de toda a cadeia de blocos. Cada um dos nós é detentor de uma via da cadeia de bloco e, portanto, cada um deles tem poder de validar as novas transações adicionadas à blockchain.

Segundo Baran<sup>22</sup>, redes de comunicação podem ser classificadas como centralizadas, descentralizadas e distribuídas, conforme a figura a seguir.

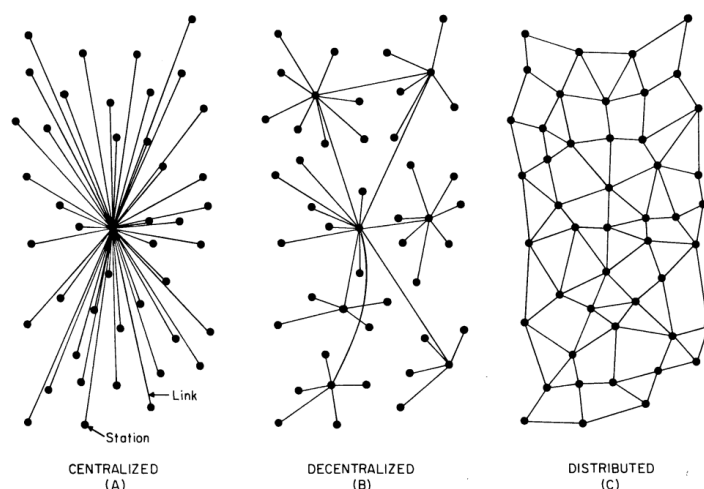


FIG. 1 — Centralized, Decentralized and Distributed Networks

*Figura 8-Tipos de rede, segundo Baran*

A rede centralizada, também chamada de estrela, é altamente vulnerável porque se o nó central for eliminado haverá o comprometimento de toda a rede. A rede descentralizada, por sua vez, não compreende apenas um nó central, mas uma divisão de responsabilidade entre alguns nós mais importantes do que outros. Contudo, essa rede também pode ser comprometida em decorrência de ataque contra alguns nós. Na rede distribuída não há prevalência de responsabilidade entre os nós, tampouco um nó central.

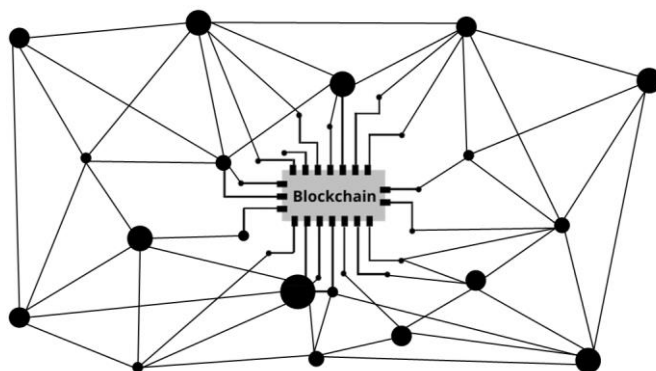
---

<sup>21</sup> Prefere-se o termo “via” ao termo “cópia”, porquanto, a via se refere a um documento original, produzido com a mesma validade jurídica que o documento original principal, enquanto a cópia é uma reprodução de um documento original que não possui o mesmo valor jurídico que a via original, a menos que seja autenticada.

<sup>22</sup> BARAN, Paul. On Distributed Communications (Introduction to distributed communication network). Economic Policy, v. 5, p. 193-208, 2009.

De fato, todos os nós detêm idêntico nível hierárquico de modo que as comunicações somente seriam interrompidas em caso de ataque sobre todos os nós simultaneamente.

Ao invés de depender de um único ponto de controle, como um servidor centralizado, a blockchain é mantida por uma rede de computadores interconectados (nós), ou seja, configura uma rede distribuída na qual os nós se comportam simultaneamente como provedores e usuários da rede e são capazes de verificar se as novas transações são válidas no que se refere à ordem, porquanto carregam a via completa e atualizada de toda a cadeia. Com efeito, uma vez que uma transação é feita na blockchain os nós realizam a verificação (validação) da transação através de esforços para solução de problemas matemáticos para, ao cabo, atestar ou não sua integridade. Não haveria efetividade em tentar congelar transações emitindo ordem para um único nó, pois todos os nós detêm vias dos registros e essas vias contêm a integralidade dos registros. Assim sendo, a rede continuaria a funcionar de qualquer maneira. A figura a seguir representa a rede distribuída da blockchain.



*Figura 9-Ilustração da rede distribuída da blockchain*

Vejamos um exemplo ilustrativo da atividade da rede distribuída, analisando uma mesma transação da blockchain com diferença de pouco mais de 1 minuto entre as visualizações. Note-se, na figura a seguir, que no primeiro momento havia 24 confirmações e pouco mais de 1 minuto depois já havia 33 confirmações. Essa diferença entre confirmações é o resultado de novas validações feitas pelos nós intervenientes que fazem o papel distribuído de substituição de uma autoridade central de certificação.



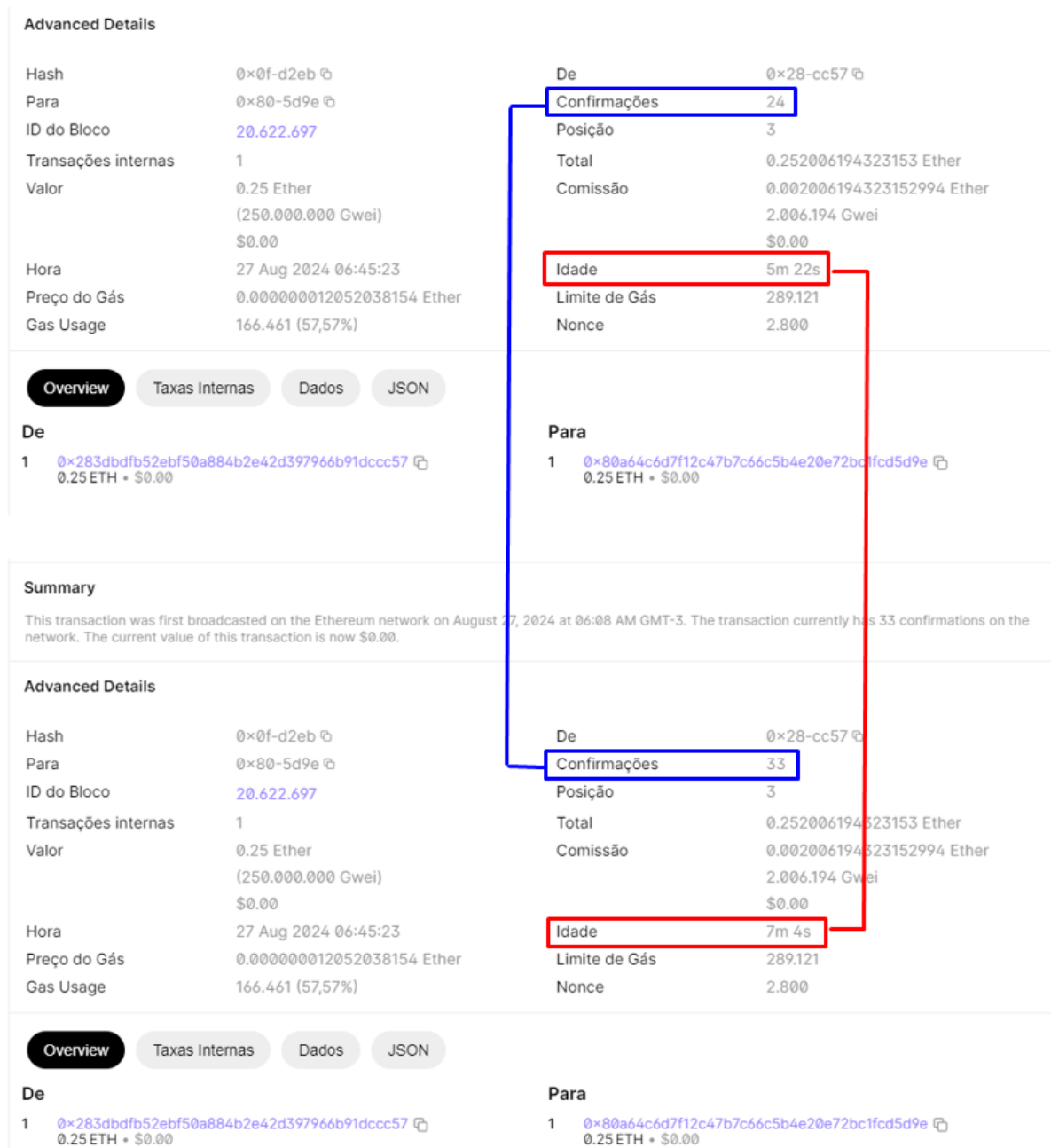


Figura 10-Excerto do blockchain Ethereum mostrando as validações ao longo do tempo

Vejamos mais um exemplo, agora com uma transação mais antiga componente de um bloco que já foi validado 1.901.638 de vezes.

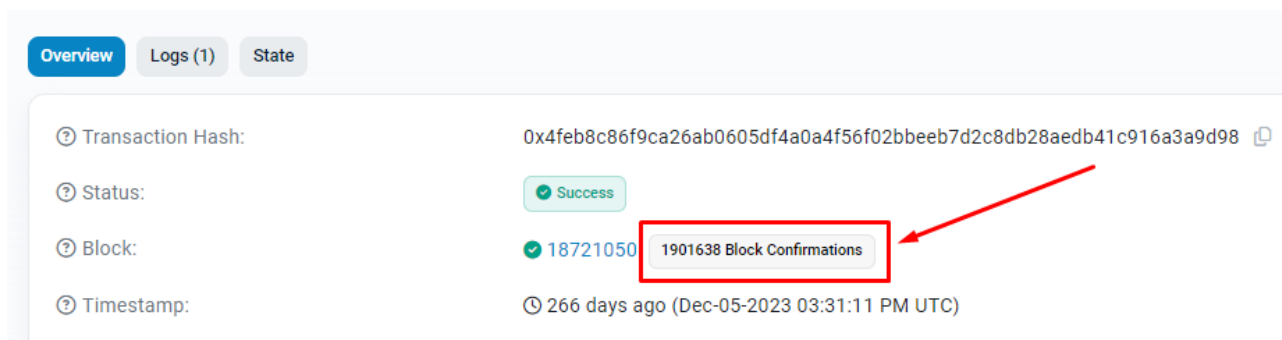


Figura 11-Excerto do blockchain Ethereum mostrando validações

**Transparência:** Os dados dos blocos e das transações que os compõem são públicos e abrangem: o hash da transação; o número do bloco no qual a transação está inserida; as confirmações da transação; a data da realização da transação; o endereço público do remetente; o endereço público do destinatário; o valor da transação na moeda transacionada e seu respectivo valor em moeda fiduciária; a taxa da transação; dentre outras informações. Vejamos um exemplo de registro de transação e seus dados publicizados.

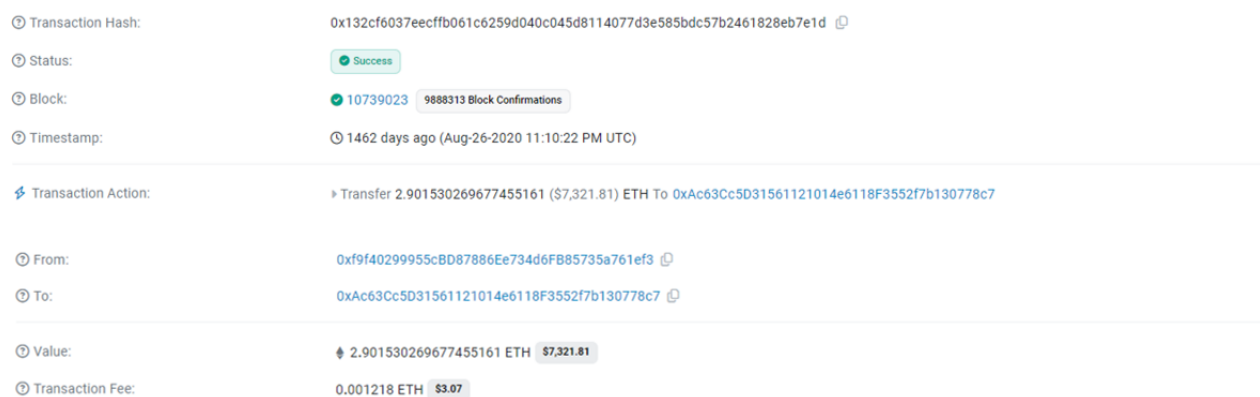


Figura 12-Excerto de registro de transação no blockchain

As transações podem ser examinadas nas redes blockchain correspondentes por meio de exploradores de blockchain, que são ferramentas online projetadas para permitir que os usuários acessem informações detalhadas sobre transações, blocos, endereços e outras atividades registradas em blockchain. Esses exploradores funcionam como motores de busca especializados para blockchains, proporcionando a qualquer pessoa o acesso a dados armazenados em uma rede de maneira transparente e em tempo real.

Os exploradores de blockchain permitem pesquisas por endereços, pelo hash da transação, pelo número do bloco, dentre outros critérios. Recentemente, o motor de

busca Google passou a indexar os dados de transações das redes blockchain e a partir de então é possível fazer pesquisas nesta ferramenta usando como critério de pesquisa o hash da transação ou o endereço público envolvido para descobrir a rede blockchain relacionada e desta forma usar um explorador de blockchain específico para a referida rede. Recomendamos que as eventuais explorações sejam feitas através dos seguintes exploradores:

- [Blockchair.com](https://blockchair.com/);
- <https://blockchain.coinmarketcap.com/>;
- <https://etherscan.io/>
- <http://www.blockchain.com/explorer> (apesar do nome, este sítio eletrônico não é a blockchain, mas sim apenas um explorador de blockchain)
- [tronscan.org](https://tronscan.org)

**Segurança:** decorre de um conjunto de atributos intrínsecos à arquitetura da blockchain, a saber:

- Imutabilidade*, pois, uma vez que o bloco de dados é acrescentado à blockchain sua alteração ou supressão se torna praticamente impossível, especialmente por conta das funções criptográficas de hash de transações e dos próprios blocos que se interconectam. Desse modo, quanto mais antiga for a idade do bloco, mais próxima do impossível será sua alteração;
- Distribuição*, pois, conforme já mencionado, a rede não é controlada por uma entidade central, mas sim pelos nós que detêm as vias da cadeia de blocos, e assim sendo, um ataque de sucesso dependeria do controle da maioria absoluta dos nós pelo atacante. Desse modo, quanto maior a rede, menor a chance de ocorrer um ataque de sucesso;
- Consenso de Rede*, que está intimamente ligado à descentralização e é o processo pelo qual os nós concordam sobre a validade de uma transação ou de um bloco. O consenso

é obtido através de algoritmos de consenso dentre os quais se destacam *Proof of Work (PoW)* e *Proof of Stake (PoS)*;

- iv) *Criptografia*, pois, os dados são assinados digitalmente por chaves criptográficas privadas que se vinculam às chaves públicas por meio de algoritmos matemáticos de assimetria, a exemplo do algoritmo ECDSA<sup>23</sup> (Elliptic Curve Digital Signature Algorithm) usado para o Bitcoin e Ethereum;
- v) *Auditabilidade*, pois a transparência proporciona visibilidade por qualquer pessoa e por consequência permite auditorias independentes e a verificação da integridade dos dados.

**Anonimato relativo (pseudonimato):** as identidades dos usuários são encobertas por uma camada alfanumérica codificada (o endereço). O anonimato é dito relativo porque o fluxo de ativos entre diferentes endereços públicos pode ser rastreado e ferramentas de análise de blockchain podem mapear essas transações, identificando padrões e relacionando diferentes endereços e, ao cabo, revelando uma identidade. Ademais, quando os usuários compram ou vendem criptomoedas em PSAVs centralizadas, eles geralmente são obrigados a cumprir políticas de Conheça Seu Cliente (KYC), fornecendo informações de identificação pessoal. Se um endereço de ativo virtual usado em uma transação puder ser vinculado a um usuário que tenha passado por um processo de KYC, a identidade real do usuário pode ser revelada.

**Abrangência global:** é possível enviar ativos a partir de qualquer lugar do mundo para qualquer lugar do mundo dispondo apenas de acesso à internet, não existindo fronteiras geográficas que limitem as transações a serem efetuadas.

**Disponibilidade:** as transações envolvendo ativos virtuais realizadas por meio da blockchain estão disponíveis 24 horas por dia, 7 dias por semana, oferecendo maior flexibilidade e disponibilidade em comparação com o mercado financeiro tradicional.

**Diversidade:** existem várias redes blockchain e isso se justifica porque os ativos virtuais são criados para atender interesses específicos. Por exemplo, a blockchain

---



<sup>23</sup> Para saber mais acesse <https://www.youtube.com/watch?v=6TI5YOpnrgI>. Acessado em 28/08/2024.

do Bitcoin tem como finalidade ser uma alternativa ao mercado financeiro tradicional, enquanto a blockchain Ethereum objetiva ser uma plataforma de contratos inteligentes, e, por consequência, de tokens e NFTs. Outras ainda são construídas para oferecer pagamentos velozes e de baixo custo, com intervalos curtos entre os blocos em busca de escalabilidade e desempenho. As blockchains ainda diferem em seus modelos de governança que podem refletir os valores da comunidade visada, mais ou menos centralizadas. A tendência atual é pela construção de blockchains dotadas de interoperabilidade e integração, de modo a permitir compartilhamento de informações entre redes.

No que se refere ao conjunto de registros, os principais blockchain de interesse investigativo são:


- I) o blockchain do Bitcoin, que pode ser explorado pelo motor de busca em <http://www.blockchain.com/explorer>
- II) o blockchain Ethereum, que pode ser explorado pelo motor de busca em <https://etherscan.io/>;
- III) o blockchain Tron, que pode ser explorado pelo motor de busca em <https://tronscan.org/#/>.

Na tabela a seguir discriminamos as principais características dessas três redes blockchain.

Blockchain	Características
Bitcoin 	Meio de transferência de ativos digitais. Não suporta contratos inteligentes. É o ativo mais valorizado e mais popular, amplamente usado como reserva de valor.
Ethereum 	Permite a execução de contratos inteligentes, transações com tokens, NFTs e Finanças Descentralizadas (DeFi) <sup>24</sup> . Suporta USDT através da emissão do token ERC-20.

---

<sup>24</sup> Defi (Decentralized Finance) corresponde a um ecossistema de aplicações financeiras construídos sobre blockchains públicas, como a rede Ethereum. Essas aplicações têm como objetivo substituir, replicar e expandir as funcionalidades do sistema financeiro tradicional de forma aberta e descentralizada, sem intermediários e plenamente auditável.

Tron 	Permite a execução de contratos inteligentes, transações com tokens, NFTs e Finanças Descentralizadas (DeFi). Suporta USDT através da emissão do token TRC-20. A rede Tron é o principal meio de transação do token USDT, devido ao baixo custo desta rede.
---	---

*Quadro 1- Características das 3 principais blockchains*

Blockchain, como mencionado, pode ainda ser definido, sob a ótica tecnológica, como um banco de dados de registros; sob a ótica financeira como um instrumento de transações de ativos; sob a ótica comercial como plataforma de novas soluções e oferta de serviços; e sob a ótica da segurança jurídica como certificadora.

Para entender com mais profundidade o funcionamento de Blockchain recomendamos assistir aos vídeos acessíveis por este link: <https://andersbrownworth.com/blockchain/>

### **3.2.1. Classificação de Blockchain**

Quanto à classificação, tendo como critério a completude da linguagem de programação empregada na construção, temos duas gerações de blockchain. Em resumo, as blockchains podem ser completas ou incompletas, entendidas, respectivamente, como aquelas que não trazem e aquelas que trazem limitações para programação sobre elas. São chamadas de primeira (incompleta) e de segunda (completa) gerações.

A primeira geração de blockchain, representada pelo Bitcoin, apresenta limitações em sua capacidade de programação. Lançado em 2009, o Bitcoin estabeleceu as bases para a tecnologia, concentrando-se principalmente em transações financeiras. Utilizando um modelo de prova de trabalho (Proof of Work), a rede garante segurança e descentralização. Essa geração introduziu a ideia de uma moeda digital que opera sem intermediários, empregando criptografia robusta para proteger as transações. Contudo, devido ao seu foco funcional como meio de pagamento, a tecnologia do Bitcoin restringe a programação, uma vez que essa funcionalidade não faz parte de seu escopo.

A segunda geração adveio com o lançamento do Ethereum em 2015 e expandiu o conceito de blockchain para além de meras transações de cunho financeiro. A rede Ethereum introduziu os contratos inteligentes, permitindo que códigos autônomos fossem executados diretamente na blockchain, o que possibilitou a criação de aplicações descentralizadas (dApps), tokens e NFTs. Essa geração diversificou as possibilidades de uso da tecnologia, permitindo que desenvolvedores criassem soluções inovadoras em

diversas áreas, como finanças, jogos e identidade digital. A blockchain do Ethereum permite programação sobre ela e por esse motivo é considerada completa e de segunda geração.

As blockchains de segunda geração (completas) permitem, portanto, a criação de contratos inteligentes (smart contracts) sobre elas. Contratos inteligentes não devem ser compreendidos como contratos segundo o significado do Direito Civil. São tão somente programas de computador que se valem da estrutura da blockchain de segunda geração para funcionarem. Sendo assim, programadores podem utilizar a estrutura da blockchain de segunda geração para desenvolver novos negócios, por meio de contratos inteligentes, tais como a criação de tokens fungíveis, tokens não-fungíveis, jogos, finanças descentralizadas etc.

Em linhas gerais, reservados os casos excepcionais, a blockchain do Bitcoin é fechada, significando dizer que somente suporta o tráfego de Bitcoin. Por outro lado, as blockchains de segunda geração, como a Ethereum e Tron, são abertas (completas, pois permitem a inserção de contratos inteligentes) e por elas trafegam, por exemplo, criptomoedas nativas (criptomoeda específica da rede usada para pagar taxas de transações na rede) e tokens, que são ativos virtuais que nascem dos contratos inteligentes, dentre outros ativos virtuais.

### **3.3. Chave Privada, Chave Pública, Endereço**

As diversas arquiteturas das blockchains utilizam algoritmos de criptografia assimétrica para garantir a integridade dos dados. A criptografia assimétrica é conhecida também como criptografia de chave pública e difere da criptografia simétrica, conhecida como de chave privada. Na criptografia simétrica apenas uma chave é usada tanto para codificar quanto para decodificar uma mensagem. Já na criptografia assimétrica, duas chaves são usadas: uma chave pública, usada para codificar, e uma chave privada, para decifrar.

Os ativos virtuais utilizam o algoritmo de criptografia assimétrica ECDSA (Elliptic Curve Digital Signature Algorithm) que é altamente seguro e eficiente do ponto de vista computacional para criar um par de chaves. Este algoritmo trabalha com uma relação matemática entre as duas chaves que compõem o par, de modo que a chave pública deriva da chave privada. A partir de uma chave privada é possível conhecer a chave pública e por conseguinte o endereço. Mas, o inverso não é verdadeiro porque a chave pública deriva da chave privada numa relação unidirecional. Isto é, não seria possível conhecer a chave

privada a partir da chave pública. Por esse motivo, como veremos adiante, não há qualquer problema em revelar o endereço dos seus ativos virtuais.

Muito embora no ambiente dos ativos virtuais as chaves públicas sejam conhecidas como endereços, tecnicamente são duas coisas distintas. De fato, a chave pública é criada a partir da chave privada formando o sobredito par. Já o endereço é uma representação simplificada da chave pública após a aplicação de processos de criptografia e de hash sobre esta. Trata-se, portanto, de uma “etiqueta” criptografada da chave pública, com representação mais simples e mais curta. Portanto, quando estiver se referindo à sequência alfanumérica que determina a origem e o destino de uma transação com ativos virtuais, chame-a de endereço público. Tecnicamente, não a chame de chave pública.

Os endereços e as chaves privadas são reconhecidos por conjuntos de caracteres alfanuméricos que obedecem à determinados padrões conforme a rede blockchain. A seguir, apresentamos exemplos de conjuntos de endereços públicos de Bitcoin, Ethereum e Tron.

 BITCOIN	<b>Endereço público:</b> <b>bc1qpzgsyjfj05jpazqs7uavcz38w3v6elhrqzk7syt</b>
 ETHEREUM	<b>Endereço público:</b> <b>0x8d94a325b6A6b4cf2D2FeA81632EddfDB0DFCDC5</b>
 TRON	<b>Endereço público:</b> <b>TCtz8eWk2btjw8mPDF2zgMRQR2ZSp8qCZU</b>

*Quadro 2-Exemplo de endereços públicos das 3 principais blockchains*

O endereço público tem a função de identificar a origem ou destino dos ativos virtuais. Pode-se afirmar que se parece com o número de uma conta bancária do mercado financeiro tradicional, que poderia ser fornecida a uma determinada pessoa para receber uma quantia. Por exemplo, se você deseja enviar bitcoins para alguém, necessitará saber o endereço do destinatário, tal como necessitamos saber a chave PIX em transações com moeda fiduciária. Essa identificação seria inserida como o endereço de destino da transação e, uma vez concluída, os ativos seriam transferidos para o endereço especificado.

A chave privada, por outro lado, é utilizada para acessar os ativos associados a um endereço. Dando continuidade à analogia iniciada no parágrafo anterior, a chave



privada se parece com a senha da conta bancária que nos permite acessar nossos ativos fiduciários. Dessa forma, para que os ativos virtuais associados a um endereço sejam enviados para um outro endereço qualquer, é necessário que o responsável pela transação possua a chave privada relativa ao endereço de onde se originarão os ativos enviados.

Deve-se ressaltar a criticidade inerente à chave privada. Enquanto o endereço pode ser compartilhado sem maiores preocupações, a chave privada é um elemento que dá acesso total e irrestrito aos ativos atrelados ao endereço à qual ela se refere, devendo ser mantida em completo sigilo, sob pena de se perder completamente os ativos.

Merece destaque, ante ao exposto, o fato de que o efetivo controle do ativo virtual se dá pelo controle da chave privada referente ao endereço ao qual ele está associado, aspecto que será relevante para a compreensão de conceitos, cenários e procedimentos apresentados nos capítulos que subsequentes.

### **3.4. Carteiras de Ativos Virtuais**

As carteiras de ativos virtuais são recursos tecnológicos de software e hardware desenvolvidos para auxiliar a gestão e operação de ativos virtuais. Através de uma carteira, consegue-se, por exemplo, de forma mais amigável e simples, gerenciar de forma segura um conjunto de chaves, ter acesso ao saldo de endereços de diversas blockchains, realizar transações em diferentes blockchains, observar o histórico de transações em diferentes blockchains, além de se ter à disposição alguns importantes recursos de segurança.

Por se tratar de um recurso utilizado por alguém para realizar a efetiva manipulação de ativos virtuais, a compreensão das possíveis características desse elemento é de suma importância para o investigador policial, bem como algumas de suas classificações e tipos. Esses aspectos podem influenciar diretamente nos procedimentos e diligências que deverão ser realizados durante a fase de investigação e recuperação de ativos.

#### **3.4.1. Classificação quanto à guarda das chaves privadas**

Como visto anteriormente, a chave privada é um elemento crítico que determina o real controle sobre os ativos associados a um endereço. Esse aspecto é de suma importância para a compreensão da relação de efetiva propriedade de ativos virtuais.

Consequentemente, a classificação das carteiras quanto à forma como é realizada a guarda dessas chaves privadas torna-se também de suma importância.

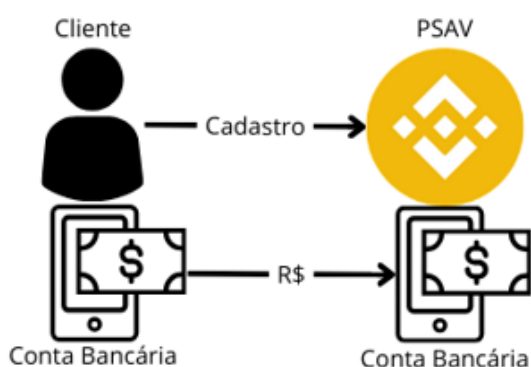
#### **3.4.1.1. Carteiras de Custódia de Terceiros (ou Carteiras Custodiais)**

Uma Carteira de Custódia de Terceiros é aquela em que um terceiro, geralmente uma Prestadora de Serviço de Ativos Virtuais (PSAV), mantém a guarda das chaves privadas dos ativos virtuais do usuário da carteira. Isso significa que o usuário de uma carteira desse tipo não tem controle direto sobre suas chaves privadas, e, por consequência, ele aceita a terceirização da responsabilidade da guarda das chaves privadas dos seus ativos. Dito de outro modo, o provedor do serviço tem controle completo sobre os ativos do usuário.

Para esclarecer alguns aspectos acerca do uso de uma Carteira de Custódia de Terceiros, relata-se brevemente as etapas de abertura de conta e compra de ativos virtuais através de uma PSAV.

1. O processo de abertura de uma conta em uma instituição Prestadora de Serviços de Ativos Virtuais é simples, assemelhando-se ao processo de abertura de uma conta digital em uma instituição financeira tradicional, exigindo-se a inserção de alguns dados cadastrais, validação documental e conferência biométrica, por exemplo.
2. A partir da abertura da conta na referida PSAV, torna-se possível o envio de moeda fiduciária para a conta recentemente aberta através de diferentes meios de pagamentos.
3. Quando a moeda fiduciária sai da conta bancária do usuário e vai para a conta bancária da PSAV (por meio de TED, PIX, etc) o dinheiro segue para uma conta bancária bolsão da PSAV que registra, de forma escritural, o crédito em favor do usuário. Este saldo em moeda fiduciária permite ao usuário emitir ordens para a PSAV de compra de ativos virtuais.
4. Uma vez emitida uma ordem dessa natureza, o montante ordenado será debitado do saldo em moeda fiduciária do usuário na PSAV e, em contrapartida, será acrescido em seu portfólio um saldo representativo do ativo virtual recém adquirido. Importante notar que até este ponto, o

usuário não tem, de fato, ativos virtuais, mas tão somente uma representação deles através da conversão da moeda fiduciária no ativo virtual pretendido com a taxa cambial do dia e hora da conversão.



Ordens que o cliente poderá emitir para a PSAV cumprir:

- 1) Manter a moeda fiduciária parada na conta da PSAV
- 2) Mandar de volta para a conta bancária origem
- 3) Mandar converter em ativo virtual (saldo representativo)
- 4) Uma vez convertido em saldo representativo, mandar transferir para um endereço público

*Figura 13-Ordens que o cliente pode dar para a PSAV*

Na figura acima podemos compreender o que o cliente poderá determinar que a PSAV cumpra. Somente no caso da hipótese 4 é que haveria de fato a posse de ativos virtuais no endereço público que recebeu.

A utilização desse tipo de carteira pode influenciar na atividade policial dadas as características inerentes. De fato, a abertura de uma conta em uma PSAV pressupõe a inserção de dados cadastrais e pessoais; o acesso a uma conta em uma PSAV é geralmente realizado através de um login e senha (podendo ou não contar com duplo fator de autenticação) utilizando-se o site ou aplicativo da instituição, independentemente do dispositivo utilizado para se realizar o acesso; o controle total dos ativos recai sobre a instituição na qual a conta foi aberta, uma vez que ela fará a guarda das chaves privadas; os ativos do usuário ficam à mercê da capacidade de liquidez e da segurança da infraestrutura da PSAV. Assim, se a instituição for à falência ou alegar que sofreu um ataque hacker, o usuário não terá acesso aos seus ativos, uma vez que não possui as chaves privadas.

#### **3.4.1.2. Carteiras de Custódia Própria (ou não-custodiais)**

As Carteiras de Custódia Própria têm como característica principal o fato de o usuário ter o controle total sobre suas chaves privadas e, portanto, sobre seus ativos. Ou seja, o próprio usuário tem a responsabilidade de armazenar e gerenciar suas próprias chaves privadas.

Carteiras de Custódia Própria podem assumir diferentes formas, destacando-se as *hardwallets* e as carteiras em formatos de softwares. As *hardwallets* são dispositivos físicos projetados especificamente para armazenar chaves privadas de forma segura. Conectadas a um computador por um cabo, permitem, através da utilização de uma interface desenvolvida por cada fabricante, visualizar os endereços, realizar transferências etc. Na figura a seguir, apresentam-se as *hardwallets* mais populares no momento da elaboração deste manual.



*Figura 14 Hardwallets mais populares do mercado; à esquerda e no centro a Trezor, à direita a Ledger.*

Já as Carteiras de Custódia Própria em formato de software nada mais são do que programas de computador ou aplicativos de dispositivos móveis, que podem ser acessados e instalados assim como qualquer outro software.

Deve-se ressaltar algumas características da utilização desse tipo de carteira que podem influenciar a atividade policial: a criação de uma carteira de custódia própria não envolve a inserção de nenhum dado pessoal; o acesso à carteira pode estar protegido por senha, PIN e/ou duplo ou múltiplo fator de autenticação; as chaves privadas estão, de fato, armazenadas no dispositivo no qual a Carteira de Custódia Própria foi configurada. Consequentemente, por exemplo, se o usuário perder o PIN/senha que dá acesso àquela carteira, ou se o dispositivo onde se encontrava a carteira for roubado ou ainda se ele quebrar, o acesso à carteira ficará impossibilitado de ser realizado, a não ser que o usuário tenha a Frase Secreta, o que será mencionado adiante.

O PIN/senha e o dispositivo no qual a Carteira de Custódia Própria foi configurada são elementos indispensáveis para o acesso à carteira e consequentemente às chaves privadas que permitirão a gestão dos ativos a elas associadas. É exatamente por esse aspecto que as Carteiras de Custódia Própria dispõem de um mecanismo de backup para o caso de o acesso à carteira ter sido perdida. Esse mecanismo de backup é a Frase Secreta.

### 3.5. Frase Secreta (Seed)

A Frase Secreta (Seed Phrase, ou Frase-Semente, ou Frase de Recuperação) é um recurso de recuperação de uma Carteira de Custódia Própria. Se um usuário perder o acesso à sua carteira devido a uma falha no dispositivo físico, roubo, esquecimento do PIN/senha ou qualquer outro motivo, a Frase Secreta pode ser utilizada para restaurar o acesso aos ativos da carteira. Ressalte-se, então, que possuir a Frase Secreta de uma carteira representa acesso total e irrestrito aos fundos da carteira à qual ela se refere.

Uma Frase Secreta consiste em uma sequência, normalmente, de 12, 18 ou 24 palavras aleatórias selecionadas a partir de um conjunto pré-definido de 2048 palavras do idioma inglês. Exemplos de Frases Secretas podem ser visualizados na imagem a seguir.

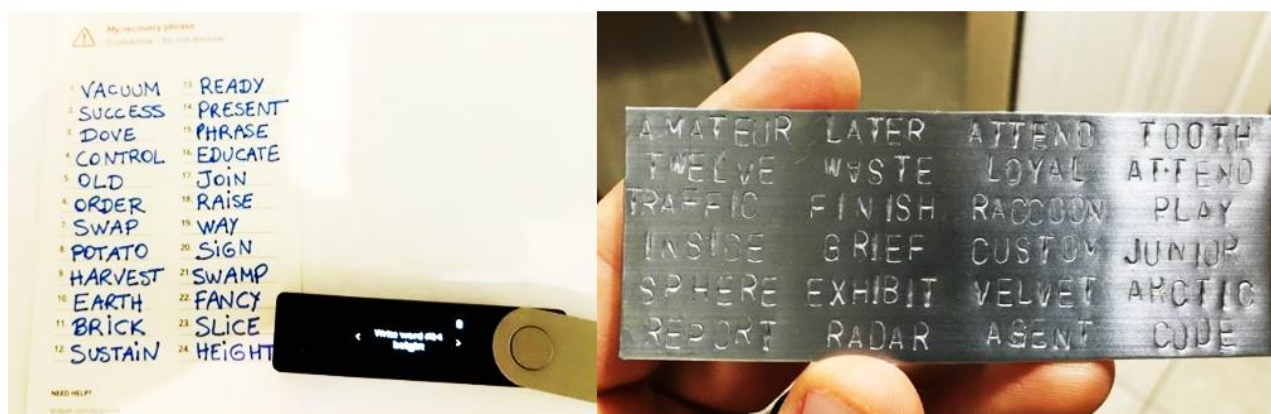


Figura 15 - Exemplos de Frases Secretas anotadas em papel e em uma placa metálica.

A Frase Secreta é apresentada para o usuário durante o processo de criação da Carteira de Custódia Própria, momento em que o usuário deverá anotá-la em local seguro, observando a ordem de disposição das palavras. A inversão ou substituição de palavras impactará negativamente o processo de recuperação da carteira. A recuperação de uma carteira através da Frase Secreta se dá pela possibilidade de derivação, a partir dela, de todas as chaves públicas e privadas da carteira à qual aquela Frase Secreta se refere. Em outras palavras, se o investigador obtém a Frase Secreta, poderá acessar todo o conjunto de pares de chaves, privadas e públicas, constantes daquela carteira.

Na prática, o processo de recuperação de uma carteira a partir de uma Frase Secreta pode ser genericamente descrito pelos seguintes passos.

1. Escolher a Carteira de Custódia Própria onde será feita a recuperação.

2. Selecionar a opção referente à recuperação de carteiras.
3. Inserir a Frase Secreta da carteira que se deseja recuperar.

Após o processo descrito acima, tratando-se de uma Frase Secreta válida, o responsável pelo processo de recuperação terá sob seu controle uma Carteira De Custódia Própria idêntica à que foi criada quando a Frase Secreta foi originalmente gerada e anotada.

Vale ressaltar que não há qualquer impedimento para que uma mesma carteira seja recuperada, a partir de sua Frase Secreta, indeterminadas vezes. Sendo assim, por exemplo, a carteira de uma organização criminosa pode ter uma cópia de sua Frase Secreta na posse de vários integrantes ao redor do mundo, e todos eles serão capazes de recuperar a carteira da organização e de lá transferir os ativos antes que as forças policiais o façam.

### **3.6. Outras classificações de carteiras**

A distinção já realizada entre Carteiras de Custódia de Terceiros e Carteiras de Custódia Própria, baseada em quem exerce o controle das chaves privadas, é essencial para que se compreenda os procedimentos de apreensão de ativos virtuais e de sequestro de saldos representativos de ativos virtuais pela polícia judiciária.

No entanto, outras classificações são comumente utilizadas para descrever carteiras de ativos virtuais. Nesta seção, faz-se menção a outros termos utilizados para classificar carteiras, principalmente no que se refere ao tipo de dispositivo suporte utilizado para “hospedar” a carteira e ao fato de ele estar ou não conectado à internet.

Hot Wallets (ou carteiras quentes): um Hot Wallet é um tipo de carteira de ativos virtuais que mantém as chaves privadas dos usuários em um dispositivo ou plataforma conectada à internet, permitindo acesso rápido e fácil aos fundos para realizar transações frequentes. Por sua conexão constante à rede, hot wallets são mais vulneráveis a ataques cibernéticos e intrusões maliciosas em comparação com cold wallets, que operam offline. Exemplos de hot wallets incluem carteiras web, carteiras móveis e carteiras desktop, abordadas nos subitens a seguir.

- Carteiras web: tipo de carteira que permite aos usuários armazenar e gerenciar ativos virtuais por meio de um navegador da web, utilizando uma interface online fornecida por um serviço de carteira. As chaves

privadas são frequentemente armazenadas nos servidores da empresa que oferece o serviço, o que pode facilitar o acesso e a recuperação de fundos, mas também aumenta a exposição a riscos de segurança, como ataques hackers e violações de dados. Carteiras web são convenientes para transações frequentes e acesso rápido aos ativos virtuais, mas a segurança depende da robustez das medidas de proteção adotadas pelo provedor do serviço.

- Carteiras mobile: uma carteira mobile é um tipo de software wallet projetada especificamente para ser instalada e operada em dispositivos móveis, como smartphones e tablets, permitindo aos usuários armazenar, gerenciar e transacionar ativos virtuais de forma conveniente e rápida. As chaves privadas são armazenadas localmente no dispositivo móvel e a carteira geralmente inclui recursos adicionais de segurança, como autenticação biométrica e PIN. Embora ofereça alta acessibilidade e seja ideal para uso diário e transações em movimento, a segurança da carteira mobile depende da integridade do dispositivo e das práticas de segurança adotadas pelo usuário, tornando-a mais vulnerável a malware e ataques físicos se o dispositivo for perdido ou comprometido.
- Carteiras desktop: uma carteira desktop é um tipo de software wallet que é instalado e operado em um computador pessoal, permitindo aos usuários armazenar, gerenciar e transacionar ativos virtuais diretamente do seu desktop ou laptop. As chaves privadas são armazenadas localmente no disco rígido do computador, proporcionando controle total do usuário sobre seus ativos. Carteiras desktop oferecem recursos de segurança e conveniência, incluindo backups e criptografia de chave privada. No entanto, a segurança da carteira desktop depende da proteção do computador contra malwares, vírus e outros tipos de ataques cibernéticos, além de ataques físicos se o dispositivo for perdido ou comprometido.

Cold Wallets: um Cold Wallet é um tipo de carteira de ativos virtuais que armazena as chaves privadas do usuário em um dispositivo ou meio que não está conectado à internet, proporcionando uma camada adicional de segurança contra ataques



cibernéticos e invasões. Como resultado, Cold Wallets são altamente recomendadas para o armazenamento de grandes quantidades de ativos virtuais a longo prazo, pois minimizam os riscos de acesso não autorizado. Exemplos de cold wallets incluem hardware wallets e paper wallets, abordadas nos subitens a seguir.

- **Paper Wallets (carteiras de papel):** é um método de armazenamento de ativos virtuais que envolve a impressão dos endereços públicos e respectivas chaves privadas em um pedaço de papel físico, geralmente na forma de códigos QR. Essa forma de armazenamento é completamente offline, oferecendo alta segurança contra ataques digitais e malwares, desde que o papel seja protegido contra perda, danos físicos e acesso não autorizado. A criação de uma Paper Wallet requer um ambiente seguro para garantir que as chaves não sejam expostas durante o processo de geração e impressão. Existem sites maliciosos especializados em oferecer a criação de paper wallets, gerando, no momento da criação por um usuário, uma cópia do paper e, uma vez que o endereço tenha recebido os ativos virtuais, o criminoso os subtrairá, pois detentor da cópia.
- **Hardwallets:** dispositivo físico especializado que armazena as chaves privadas de ativos virtuais de forma segura e offline, oferecendo proteção robusta contra ataques cibernéticos e malware. Essas carteiras geralmente vêm na forma de dispositivos USB que podem ser conectados a computadores ou dispositivos móveis para realizar transações, garantindo que as chaves privadas nunca saiam do dispositivo, mesmo durante a assinatura de transações. A segurança é reforçada através de mecanismos de autenticação de múltiplos fatores e criptografia avançada.

### **3.7. Transação de ativos virtuais – elementos e funcionamento**

O processo de transferência de ativos virtuais, se estudado a fundo e tecnicamente, envolve etapas complexas, cada uma desempenhando um papel crucial para garantir a segurança e a integridade das transações. Desde a criação e assinatura da transação até a validação, mineração e confirmação, cada passo é projetado para operar de maneira descentralizada, confiável e transparente, sem a necessidade de intermediários. No entanto, para o usuário final desse tipo de ativo e para o investigador



que atua nessa área é suficiente compreender alguns aspectos referentes à dinâmica geral desse tipo de transação.

A abordagem apresentada aqui dividirá uma transação de ativos virtuais em três etapas: montagem da transação; transmissão para a rede; registro na blockchain.

### **Montagem da Transação**

A criação de uma transação geralmente é feita com o auxílio de um aplicativo de carteira digital. Nas várias carteiras disponíveis no mercado, existe uma interface específica para o envio de ativos, permitindo que o usuário especifique o tipo de ativo a ser transferido, o endereço de destino, o valor desejado e a taxa de rede a ser aplicada. Os endereços de origem da transação são, em sua maioria, selecionados automaticamente pela carteira, uma vez que os endereços públicos são gerados no momento de sua criação. O usuário tem a opção de ajustar a taxa de rede, o que pode acelerar o processamento da transação. No entanto, é importante ter cautela para não aplicar uma taxa excessivamente alta, o que poderia reduzir de forma significativa o valor dos ativos transferidos. Após a configuração da transação, ela deve ser assinada utilizando as chaves privadas associadas aos endereços de origem. Em quase todas as carteiras disponíveis no mercado, essa assinatura é facilitada pelo uso de um PIN ou senha, configurados pelo usuário durante a criação da carteira, evitando a necessidade de manipular diretamente os complexos conjuntos de caracteres alfanuméricos das chaves. Por fim, uma vez assinada, a transação é transmitida para a rede.

### **Transmissão para a Rede**

Uma vez que a transação tenha sido montada e assinada na carteira do remetente, ela é transmitida para a rede descentralizada de computadores que compõem a blockchain. Esses computadores, chamados de nós, recebem a transação e a retransmitem para outros nós na rede.

### **Registro na Blockchain**

Dependendo do tipo de mecanismo de consenso utilizado pela blockchain, um único nó da rede é selecionado para realizar o registro de um novo bloco de transações. Algumas informações importantes serão verificadas, como, por exemplo, se o remetente realmente tem a quantidade de criptomoedas que deseja enviar e se a assinatura digital é

válida. Assim que o bloco que contém uma transação for adicionado à blockchain, a transação é dita confirmada.

---

## Glossário dos principais termos citados neste capítulo

---

**Autoridade Central:** É uma entidade única e controladora, como um governo ou banco central, responsável por regular e emitir moeda fiduciária. No contexto de criptoativos, a ausência de uma autoridade central é uma característica fundamental das redes descentralizadas.

---

**Carteiras de Ativos Virtuais:** São softwares ou dispositivos que permitem armazenar e gerenciar criptoativos, como criptomoedas. Essas carteiras gerenciam chaves privadas e públicas, permitindo enviar e receber criptoativos.

---

**Carteiras de Custódia de Terceiros:** São carteiras onde um provedor de serviços ou uma instituição mantém e gerencia os criptoativos do usuário em nome dele, sendo responsável pela segurança das chaves privadas.

---

**Carteiras de Custódia Própria:** São carteiras nas quais o próprio usuário tem total controle sobre suas chaves privadas, sendo responsável pela segurança dos seus ativos. Essas carteiras permitem que o usuário gerencie seus criptoativos diretamente, sem depender de terceiros.

---

**Cold Wallets:** São carteiras de criptoativos armazenadas offline, usadas para garantir a segurança de grandes quantidades de criptoativos, protegendo-os de ameaças online, como hackers.

---

**Criptografia Assimétrica:** Também conhecida como criptografia de chave pública, é um método que utiliza um par de chaves — uma chave pública e uma chave privada. A chave pública pode ser compartilhada para criptografar dados, enquanto a chave privada é mantida secreta e usada para descriptografar esses dados.

---

**Exploradores de Blockchain:** São ferramentas online que permitem aos usuários visualizar e pesquisar dados de transações, blocos e endereços em uma blockchain. Exploradores fornecem transparência ao mostrar o histórico e detalhes das transações de forma pública.

---

**Frase Secreta (Seed):** É uma sequência de palavras aleatórias geradas durante a criação de uma carteira de criptoativos, que atua como uma chave de recuperação. A frase secreta pode ser usada para restaurar uma carteira em caso de perda de acesso.

---

---

**Gasto Duplo:** É o risco de um ativo digital ser gasto mais de uma vez. Em redes descentralizadas, como as de criptomoedas, o gasto duplo é evitado com a ajuda da tecnologia blockchain, que registra todas as transações de forma imutável.

---

**Hardwallets:** São dispositivos físicos, como USBs, projetados para armazenar chaves privadas de criptoativos offline. Elas são consideradas uma das formas mais seguras de armazenamento, pois estão protegidas de ataques online.

---

**Hash:** É o resultado de uma função criptográfica que converte uma entrada de qualquer tamanho em uma sequência fixa de caracteres. O hash é usado para garantir a integridade e segurança dos dados em uma blockchain, já que pequenas alterações na entrada produzem resultados completamente diferentes.

---

**Hot Wallets:** São carteiras de criptoativos conectadas à internet, permitindo acesso rápido e fácil para transações, mas sendo mais vulneráveis a ataques cibernéticos em comparação às cold wallets.

---

**Moeda Fiduciária (Fiat Currency):** É uma moeda emitida por um governo, sem lastro físico, como o ouro ou a prata. O valor de uma moeda fiduciária depende da confiança no governo que a emite. Exemplos incluem o dólar (USD), o euro (EUR) e o real (BRL).

---

**Nós:** São computadores que participam de uma rede blockchain, mantendo uma via completa dos registros e validando transações. Os nós contribuem para a segurança, integridade e funcionamento da rede.

---

**PIN (Personal Identification Number):** É um código numérico curto configurado pelo usuário para proteger o acesso à carteira de criptoativos, servindo como uma camada adicional de segurança.

---

**Tron:** É uma plataforma descentralizada baseada em blockchain que visa criar um sistema global gratuito de conteúdo digital de entretenimento, utilizando tecnologia de armazenamento distribuído. A Tron também possui sua própria criptomoeda chamada TRX.

---

## 4. ASPECTOS NORMATIVOS

O ambiente regulatório dos ativos virtuais ainda se encontra em processo de desenvolvimento. Neste capítulo apresentaremos, em linha cronológica, as normas que tratam sobre ativos virtuais no Brasil, limitando-se apenas aos seus principais aspectos.

Em linhas gerais, podemos determinar como marco inicial de regulação no Brasil o ano de 2019, quando a Receita Federal do Brasil expediu duas instruções normativas para disciplinar a obrigatoriedade de prestação de informações relativas às operações realizadas com ativos virtuais. Para efeito didático, todavia, nossa cronologia começará um pouco antes, com a alteração da Recomendação 15 do Grupo de Ação Financeira Internacional (GAFI), em outubro de 2018.

Já em tempo mais recente, em consonância com as recomendações do GAFI, foi promulgada a Lei 14.478/2022, com vigência a partir de junho de 2023, a qual dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais, mas que ainda carece de regulamentação.

O ecossistema de ativos virtuais ainda é permeado por normas infralegais ditadas pela Comissão de Valores Mobiliários, em cumprimento a sua atribuição de regulação do mercado de capitais, tendo-se em vista a possibilidade, em alguns casos, de classificação dos ativos virtuais como valor mobiliário.

### 4.1. A Recomendação 15 do GAFI

De acordo com o “*Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*”, em outubro de 2018 o GAFI “adotou alterações às suas Recomendações para esclarecer explicitamente que se aplicam a atividades financeiras que envolvem ativos virtuais, e adicionou duas novas definições no Glossário, ‘ativo virtual’ (AV) e ‘provedor de serviços de ativos virtuais’ (PSAV)”.

Com efeito, a Recomendação 15 foi alterada, passando a exigir que os provedores de serviços de ativos virtuais fossem regulamentados para fins de combate à lavagem de dinheiro e ao financiamento ao terrorismo, bem como passassem a estar sujeitos aos mecanismos de monitorização e supervisão. Vejamos o texto da Recomendação 15.

Recomendação 15 antes da alteração de 2018	Recomendação 15 após a alteração de 2018

<p>15. Novas tecnologias</p> <p><i>Os países e instituições financeiras deveriam identificar e avaliar os riscos de lavagem de dinheiro e financiamento do terrorismo que possam surgir em relação a (a) desenvolvimento de novos produtos e práticas de negócios, inclusive novos mecanismos de entrega, e (b) o uso de novas tecnologias ou em desenvolvimento para produtos novos ou já existentes. No caso de instituições financeiras, tal avaliação de riscos deveria ocorrer antes do lançamento desses novos produtos, práticas de negócios ou do uso de novas tecnologias ou em desenvolvimento. As instituições deveriam adotar medidas apropriadas para gerenciar ou mitigar tais riscos.</i></p>	<p>15. Novas tecnologias</p> <p><i>Os países e instituições financeiras deveriam identificar e avaliar os riscos de lavagem de dinheiro e financiamento do terrorismo que possam surgir em relação a (a) desenvolvimento de novos produtos e práticas de negócios, inclusive novos mecanismos de entrega, e (b) o uso de novas tecnologias ou em desenvolvimento para produtos novos ou já existentes. No caso de instituições financeiras, tal avaliação de riscos deveria ocorrer antes do lançamento desses novos produtos, práticas de negócios ou do uso de novas tecnologias ou em desenvolvimento. As instituições deveriam adotar medidas apropriadas para gerenciar ou mitigar tais riscos. Deverão tomar medidas adequadas para gerir e mitigar esses riscos. Para gerir e mitigar os riscos emergentes dos <b>ativos virtuais</b>, os países devem garantir que os <b>provedores de serviços de ativos virtuais</b> sejam regulamentados para efeitos de AML/CFT<sup>25</sup>, licenciados ou registrados e sujeitos a sistemas eficazes para monitorizar e garantir o cumprimento das medidas relevantes previstas nas recomendações do GAFI.</i></p>
--	---

Consoante o glossário de termos do GAFI, Ativo Virtual:

É uma representação digital de valor que pode ser negociado ou transferido digitalmente e pode ser usado para fins de pagamento ou investimento. Os ativos virtuais não incluem representações digitais de moedas fiduciárias, títulos e outros ativos financeiros.”

Da mesma fonte se extrai o conceito de Provedor de Serviços de Ativos Virtuais que:

Significa qualquer pessoa física ou jurídica que não esteja coberta pelas Recomendações e, como empresa, conduz uma ou mais das seguintes atividades ou operações para ou em nome de outra pessoa física ou jurídica:

- troca entre ativos virtuais e moedas fiduciárias;
- troca entre uma ou mais formas de ativos virtuais.

<sup>25</sup> AML – Anti Money Laundering; CFT – Counter Financing of Terrorism

Como veremos adiante, esses conceitos foram absorvidos pela Lei 14.478/2022.

Em junho de 2019, o GAFI publicou o documento intitulado “*Guidance for a Risk-Based Approach - Virtual Assets And Virtual Asset Service Providers*” no qual, especificamente no Anexo A, foram inseridas notas interpretativas da Recomendação 15 e definições. Em outubro de 2021 o referido documento foi atualizado. Trata-se de leitura importante para o entendimento sobre a temática.

#### **4.2. Instrução Normativa 1888/2019 da Receita Federal do Brasil**

A Instrução Normativa 1888/2019, da Receita Federal do Brasil (RFB) foi publicada no Diário Oficial da União em 07 de maio de 2019 com o objetivo de instituir e disciplinar a obrigatoriedade de prestação de informações relativas às operações realizadas com ativos virtuais à Secretaria Especial da Receita Federal do Brasil.

Essa norma trouxe pela primeira vez no Brasil os conceitos legais, sob a ótica da RFB, de ativos virtuais e de exchange de ativos virtuais em seu artigo 5º, nas próprias palavras:

*Art. 5º Para fins do disposto nesta Instrução Normativa, considera-se:*

*I - 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; e*

*II - Exchange de criptoativo: a pessoa jurídica, ainda que não financeira, que oferece serviços referentes a operações realizadas com ativos virtuais, inclusive intermediação, negociação ou custódia, e que pode aceitar quaisquer meios de pagamento, inclusive outros ativos virtuais.*

Para além disso a norma definiu: quem são as pessoas obrigadas a prestar as informações; quais tipos de operações estão sujeitas à prestação de informações; quais características das operações devem ser informadas; o prazo de prestação da informação contado a partir da data da operação; as penalidades pela infração de ausência de

prestação de informações; previsão de retificação das informações; o canal de prestação de informações e; por fim, atribuiu a definição do leiaute por meio de Ato Declaratório Executivo (ADE).

O mencionado leiaute foi definido inicialmente pelo ADE Copes nº 1, de 18 de junho de 2019 e foi seguido por modificações pelos Atos 2 e 5 de 2019, todos já revogados. Atualmente, encontra-se em vigor o Ato Declaratório Executivo Copes nº 1/2013 que dispõe sobre o leiaute e sobre o Manual de Orientação do Leiaute da obrigatoriedade de prestação de informações relativas às operações realizadas com ativos virtuais à Secretaria Especial da Receita Federal do Brasil, produzindo efeitos a partir de 01 de janeiro de 2024. É importante que o policial conheça o leiaute definido pela RFB, considerando-se que será fonte de dados em investigações e seu entendimento é fundamental. É inviável apresentar o leiaute neste manual, pois composto por diversos modelos de tabelas, uma para cada situação. Sugere-se, portanto, que o interessado acesse a página dos leiautes, cujo excerto é apresentado a seguir.

gov.br

Ministério da Fazenda

Órgãos do Governo

Acesso à Informação

Legislação

Acessibilidade

Entrar com o gov.br

Receita Federal

O que você procura?

> Assuntos > Mais Orientações Tributárias > Declarações e Demonstrativos > Criptoativos > Arquivos > Ato Declaratório Executivo Copes nº 1/2023

Ato Declaratório Executivo Copes nº 1/2023

Publicado em 18/12/2023 12h26 | Atualizado em 18/12/2023 12h28

Compartilhe: f X in

Título	Autor	Tipo	Data de modificação
Ato Declaratorio Executivo Copes 1_2023.pdf	Receita Federal	Arquivo	18/12/2023 12h29
manual-de-orientacao-do-leiaute-criptoativos-versao-1.2.pdf	Receita Federal	Arquivo	18/12/2023 12h29
leiaute-criptoativos-exchanges_ver_1.2.xlsx	Receita Federal	Arquivo	18/12/2023 12h29
leiaute-criptoativos-sem-exchanges_ver_1.2.xlsx	Receita Federal	Arquivo	18/12/2023 12h29
leiaute-criptoativos-exchanges-exterior_ver_1.2.xlsx	Receita Federal	Arquivo	18/12/2023 12h29

Figura 16-Excerto do sítio eletrônico da Receita Federal do Brasil, disponível em <https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos/arquivos/ato-declaratorio-executivo-copes-ndeg-1-2023>

4.3. Parecer de Orientação nº 40 da Comissão de Valores Mobiliários

Em 11 de outubro de 2022 a Comissão de Valores Mobiliários (CVM) publicou o Parecer de Orientação CVM Nº 40 que dispõe sobre os Ativos virtuais e o Mercado de Valores Mobiliários.

Em linhas gerais, a CVM estabeleceu, por meio desse instrumento, o limite de sua atuação e consolidou seu entendimento sobre o tema. Seguindo essa linha, a CVM considera que um ativo virtual, a depender de sua natureza e da forma como é ofertado, pode caracterizar um valor mobiliário nos termos do inciso IX da Lei 6.385/76, ou seja, pode ser um Contrato de Investimento Coletivo (CIC) ofertado publicamente e, assim sendo, estaria sujeito ao regramento dessa autarquia.

A CVM explica que alguns tokens podem representar direitos de remuneração por empreendimento, direitos de receber relacionados a estruturas semelhantes à securitização ou ainda direitos de voto, situações que aproximariam os tokens do conceito de valor mobiliário na modalidade CIC.

Para essa determinação, deve-se aplicar o já conhecido Teste Howey ou, nas próprias palavras da CVM, verificar se o token detém as seguintes características: i) investimento; ii) formalização; iii) caráter coletivo do investimento; iv) expectativa de benefício econômico; v) esforço de empreendedor ou de terceiro e; vi) oferta pública.

#### **4.4. Lei 14.478/2022**

Em 22 de dezembro de 2022 o direito brasileiro absorveu a Lei 14.478/2022 que dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais.

Essa lei, além de trazer normas de regulação ao ecossistema dos ativos virtuais, alterou a Lei de Lavagem de Dinheiro, a Lei de Crimes Financeiros e o Código Penal. Vejamos as modificações mais profundas nessas leis e os principais aspectos trazidos pela nova norma.

De fato, a Lei 9.613/98 – Lei de Lavagem de Dinheiro – foi modificada pela Lei 14.478/2002 nos seguintes aspectos relacionados aos ativos virtuais:

- Inseriu uma causa de aumento de pena no §4º do artigo 1º para quem cometer o crime de Lavagem de Dinheiro por meio de utilização de ativo virtual;
- Inseriu o inciso XIX do artigo 9ª de modo que as prestadoras de serviços de ativos virtuais passaram a ser pessoas obrigadas ao



mecanismo de controle, conforme os ditames dos artigos 10 (identificação) e 11 (comunicação);

- Modificou o inciso II do artigo 10, passando a determinar que as pessoas obrigadas deverão manter registros de transações de ativos virtuais;

Por sua vez, a Lei 7.492/86 – Lei de Crimes Financeiros - passou a classificar como instituição financeira equiparada, nos termos do inciso I-A, inserido pela Lei 14.478/2022, a pessoa jurídica que ofereça serviços referentes a operações com ativos virtuais, inclusive intermediação, negociação ou custódia. Dito de outro modo, a partir da vigência da Lei 14.478/2022, uma pessoa física ou jurídica que atue no mercado de ativos virtuais pode ser considerada, para os efeitos da Lei de Crimes Financeiros, como uma instituição financeira e, assim sendo, estaria sujeita às tipificações ali previstas, especialmente o artigo 16 da Lei 7.492/86.

O Código Penal passou a vigorar com o acréscimo do tipo do artigo 171-A, cuja ementa é “Fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros” com reclusão de 4 a 8 anos para quem 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.

Especificamente quanto às regulações trazidas pela Lei 14.478/2022 ao ecossistema de ativos virtuais, merecem destaque os seguintes pontos:

- Prévia autorização de funcionamento exigida para as prestadoras de serviços de ativos virtuais funcionarem no Brasil;
- Definição de ativo virtual, muito semelhante à definição encontrada no glossário do GAFI;
- Atribuição ao órgão regulador, até então não definido, para determinar quais seriam os ativos financeiros regulados;
- Discriminação de diretrizes a serem observadas para atuação no mercado;

- Definição de prestadora de serviços de ativos virtuais, muito semelhante à definição encontrada no glossário do GAFI;
- Regulação e supervisão a serem atribuídas a um ou mais órgãos da Administração Pública Federal por ato do Poder Executivo;
- Discriminação de competências do(s) órgão(s) encarregado pelo referido ato;
- Prazo não inferior a 6 meses para adequação das prestadoras que já estiverem em atividade no Brasil
- Vacatio legis de 180 dias tendo como termo inicial 22 de dezembro de 2022, portanto, com vigência em 20 de junho de 2023.

#### **4.5. Decreto nº 11.563**

O Decreto 11.563/2023 foi publicado em 14 de junho de 2023, dias antes do início da vigência da Lei 14.478/2022. Essa norma estabeleceu competências ao Banco Central do Brasil (BCB).

Contudo, esse decreto se limitou a informar que o BCB é o órgão competente para: I - regular a prestação de serviços de ativos virtuais, observadas as diretrizes da lei e; II - regular, autorizar e supervisionar as prestadoras de serviços de ativos virtuais; mas não trouxe qualquer regulação ao mercado no que tange às transações com ativos virtuais, deixando, ao menos por enquanto, um vácuo legal no ecossistema.

Segundo publicação do Banco Central do Brasil, datada de 20/05/2024, os próximos passos de abrangência da regulação serão:

- desenvolvimento de uma segunda consulta pública sobre as normas gerais de atuação dos prestadores e de autorização ainda no segundo semestre;
- estabelecimento do planejamento interno em relação à regulamentação de stablecoins, em especial nas esferas de competência do Banco Central sobre pagamentos e o mercado de câmbio e capitais internacionais;

- desenvolvimento e aperfeiçoamento do arcabouço complementar para recepcionar as entidades (exemplo: atuação das VASPs no mercado de câmbio e capitais internacionais, regulamentação prudencial, prestação de informações ao BC, contabilidade, tarifas, suitability etc.).

#### **4.6. Solução de Consulta COSIT RFB 217/2023**

A Solução de Consulta 217 foi emitida pela Coordenação-Geral de Tributação da Receita Federal do Brasil, e trata de obrigações acessórias ligadas a operações com ativos virtuais, mais especificamente NFTs (Non-Fungible Tokens), que representam imóveis físicos. A questão principal discutida é se essas operações devem ser reportadas à Receita Federal, conforme a Instrução Normativa RFB nº 1.888/2019, e se há a obrigação de apresentação da Declaração de Informações sobre Atividades Imobiliárias (Dimob).

A Receita Federal concluiu nessa consulta que os NFTs que representam imóveis não se enquadram no conceito de criptoativo previsto na Instrução Normativa RFB nº 1.888/2019, pois não possuem as características de moeda virtual ou criptoativo usualmente transacionado. Consequentemente, empresas que intermedeiam operações envolvendo tais NFTs não estão obrigadas a prestar informações sobre essas operações à Receita Federal com base nesta instrução normativa.

Além disso, a solução também esclarece que, apesar de a empresa em questão intermediar a alienação de NFTs e confirmar a titularidade de tais tokens para fins de locação, essas atividades não configuram intermediação imobiliária propriamente dita. Assim, a empresa também não está obrigada a apresentar a Dimob, já que suas operações não se enquadram nas atividades previstas na Instrução Normativa RFB nº 1.115/2010.

#### **4.7. Solução de Consulta COSIT RFB 218/2023**

Já a solução de consulta 218, também emitida pela Coordenação-Geral de Tributação da Receita Federal do Brasil (RFB) e datada de 21 de setembro de 2023, trata das obrigações acessórias de uma pessoa jurídica que disponibiliza uma plataforma digital para transações com utility tokens. O foco está em determinar se a empresa está obrigada a prestar informações à Receita Federal sobre essas transações, conforme a Instrução Normativa RFB nº 1.888/2019.

A Receita Federal concluiu que a pessoa jurídica, mesmo que não financeira, que oferece uma plataforma onde os usuários realizam transações peer-to-peer com utility

tokens, se enquadra no conceito de exchange de ativos virtuais. Assim, a empresa deve prestar informações à Receita sobre as transações com utility tokens, tanto aquelas realizadas diretamente por ela quanto pelos seus usuários, conforme previsto no artigo 6º da referida instrução normativa. Além disso, a emissão de utility tokens também deve ser informada à Receita.

A consulta também esclareceu que, além de transações de compra e venda, operações como permuta, doação, aluguel, emissão e outras formas de transferência de ativos virtuais devem ser reportadas. A empresa é responsável por analisar e reportar essas operações, com base no § 2º do artigo 6º da IN RFB nº 1.888/2019.

#### **4.8. Lei 14754/2023**

A lei em questão relaciona-se aos ativos virtuais principalmente no Art. 3º, que aborda a tributação das aplicações financeiras no exterior de pessoas físicas residentes no Brasil. Nela, os ativos virtuais (incluindo criptomoedas) e as carteiras digitais são classificados como aplicações financeiras no exterior e, portanto, sujeitas à tributação.

Os rendimentos provenientes dessas aplicações, como a variação da criptomoeda em relação à moeda nacional, devem ser declarados na Declaração de Ajuste Anual (DAA) e estão sujeitos ao Imposto de Renda de Pessoa Física (IRPF). A Receita Federal regulamentará o enquadramento dos ativos virtuais e carteiras digitais, especificando como eles devem ser tratados para fins tributários. A tributação ocorrerá tanto sobre os rendimentos (como juros) quanto sobre os ganhos de capital, como na alienação ou liquidação das criptomoedas.

Resumindo, a lei incluiu os ativos virtuais como parte das aplicações financeiras no exterior, estabelecendo regras claras sobre como seus rendimentos e variações cambiais devem ser declarados e tributados.

#### **4.9. Instrução Normativa 2.219/2024 da Receita Federal do Brasil**

A Instrução Normativa 2.219/2019, da Receita Federal do Brasil (RFB) foi publicada no Diário Oficial da União em 18 de setembro de 2024 com o objetivo de instituir e disciplinar a obrigatoriedade de prestação de informações relativas a cadastros, operações financeiras, previdência privada e repasse de valores recebidos por meio dos instrumentos de pagamento.

Especificamente no que se refere ao uso dos ativos virtuais, a IN 2219/2019 RFB inova ao determinar que as instituições de pagamento devem prestar informações relativamente aos serviços prestados para PSAVs estrangeiras que têm atuação no Brasil, em periodicidade semestral.

Portanto, nos casos em que as operações com ativos virtuais são realizadas com exchanges estrangeiras e que eventualmente não seriam reportadas com base na IN 1.888/2019, será possível obter informações que devem ser prestadas mediante a comunicação das operações financeiras com fundamento na IN 2.219/2024.

---

### **Glossário dos principais termos citados neste capítulo**

---

**Contrato de Investimento Coletivo (CIC):** É uma forma de contrato em que investidores aportam recursos de maneira conjunta em um empreendimento ou negócio, com a expectativa de obter lucros futuros decorrentes dos esforços de terceiros. Esse tipo de contrato é um valor mobiliário sujeito ao regramento da Comissão de Valores Mobiliários (CVM) no Brasil e tem previsão legal na Lei no inciso IX do artigo 2º da Lei 6.385/76. No contexto de criptoativos, um CIC pode ser configurado quando um projeto oferece tokens ou participações que conferem aos investidores o direito a uma parcela futura de lucros

---

**Dimob (Declaração de Informações sobre Atividades Imobiliárias):** É uma declaração obrigatória no Brasil, apresentada à Receita Federal por pessoas jurídicas que atuam no setor imobiliário. Ela registra as operações de vendas, aluguéis e intermediação de imóveis realizadas no ano anterior. A Dimob é essencial para fiscalizar e garantir que as transações imobiliárias sejam devidamente declaradas para fins de tributação.

---

**Peer-to-Peer (P2P):** É um modelo de rede descentralizada em que os participantes se conectam diretamente entre si para compartilhar recursos ou informações sem a necessidade de uma autoridade central ou intermediário. No contexto de criptoativos, redes P2P são essenciais para o funcionamento das blockchains, permitindo que os nós validem e verifiquem transações diretamente. O modelo P2P também é usado em plataformas de empréstimos e trocas de criptomoedas, onde as transações ocorrem diretamente entre os usuários.

---

**Teste Howey (Howey Test):** É um critério legal estabelecido pela Suprema Corte dos Estados Unidos para determinar se uma transação é considerada um "contrato de investimento" e, portanto, sujeita às leis de valores mobiliários. De acordo com o Teste Howey, uma transação é um contrato de investimento se envolve: (1) um investimento de dinheiro, (2) em uma empresa comum, (3) com a expectativa de lucros, (4) derivada dos esforços de terceiros. Esse teste é frequentemente aplicado para determinar se um criptoativo ou token é uma security (valor mobiliário) ou não.

---

---

**Utility Tokens:** São tokens emitidos por um projeto ou empresa que conferem ao detentor o direito de acessar produtos ou serviços específicos dentro de um ecossistema, mas não representam participação em lucros ou direitos de governança. Diferentemente dos security tokens, os utility tokens geralmente não são considerados valores mobiliários e têm como principal função habilitar o uso de uma plataforma ou serviço.

---

## 5. INVESTIGAÇÃO E PERSECUÇÃO PATRIMONIAL

Para melhor entendimento deste capítulo devemos, inicialmente, estabelecer uma diferenciação fundamental entre dois institutos: Ativos Virtuais e Saldo Representativo de Ativos Virtuais. Nesse sentido:

Ativos Virtuais, como dito, são representações digitais de valor que podem ser negociadas ou transferidas eletronicamente e usadas como forma de pagamento, investimento, ou como utilidade em certas redes. Os ativos virtuais incluem criptomoedas (como Bitcoin e Ethereum), tokens (como tokens de utilidade ou tokens de segurança), e outros ativos digitais com valor intrínseco ou representado, como os tokens não-fungíveis (NFT). Eles são criados e transacionados com base na tecnologia de blockchain e por este motivo podemos afirmar que o Ativo Virtual está na blockchain.

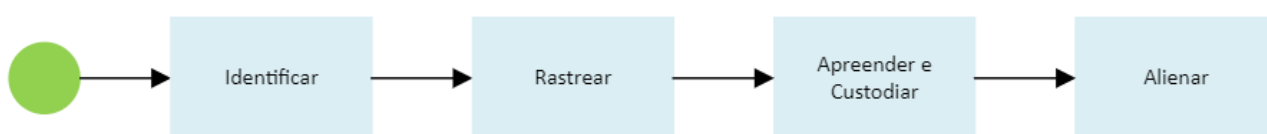
Saldo Representativo de Ativos Virtuais se refere ao valor que uma entidade, como uma PSAV, mantém em nome de um usuário, relacionado a um ou mais ativos virtuais. O Saldo Representativo pode ser entendido como um crédito representado em ativo virtual que o usuário tem direito junto a uma entidade. Esse saldo é gerido por terceiros (como uma PSAV centralizada), e o usuário confia que o saldo registrado digitalmente corresponde a ativos virtuais reais que podem ser resgatados ou negociados. Assemelha-se ao saldo que temos neste momento em nossa conta bancária junto a uma instituição financeira do mercado de crédito de moeda fiduciária. Assim como o saldo em reais é gerido pelo banco que o representa em moeda fiduciária em nosso extrato eletrônico, o Saldo Representativo de Ativos Virtuais é administrado pela PSAV, porém, com representação em ativo virtual.

Em resumo, a principal diferença está no fato de que o ativo virtual é a propriedade digital propriamente dita, enquanto o saldo representativo de ativos virtuais é uma representação contábil ou escritural desse ativo, geralmente mantida por uma entidade intermediária, como uma PSAV, em nome do usuário.

Cumpra lembrar que, quando o cliente se cadastra em uma plataforma como a Binance e envia moeda fiduciária para "comprar" Bitcoin, na realidade, a Binance não adquire diretamente o Bitcoin em nome do usuário. O que ocorre é que a plataforma registra internamente que o usuário possui um saldo equivalente à criptomoeda pretendida. Esse saldo não corresponde necessariamente a Bitcoins mantidos em uma carteira vinculada ao usuário, mas sim a um registro escritural nos sistemas da empresa.

Em caso de falência da Binance, o usuário não poderia simplesmente resgatar seus Bitcoins, já que esses ativos não existiriam de fato sob sua posse. O que ele possui é um saldo representativo que, em casos de insolvência da empresa, pode se tornar irrecuperável, assim como ocorreria com a falência de um banco ou assim como ocorreria com a falência de uma empresa aérea com as milhas. Contudo, o cliente poderá instruir a Binance a transferir esse saldo representativo para um endereço público de uma carteira de sua propriedade, na blockchain. Somente após a efetivação dessa transação o usuário passaria a ter, de fato, a posse dos ativos virtuais, em vez de um mero saldo representativo.

Feita essa diferenciação, a qual será útil para o investigador, passemos a comentar sobre importantes técnicas que podem ser usadas em investigações criminais. Para facilitar a apresentação das ideias neste manual e destacar os pontos de atenção que devem orientar a atuação das equipes policiais em casos que envolvam ou possam envolver o uso de ativos virtuais ou saldos representativos de ativos virtuais, estruturamos as investigações de polícia judiciária em quatro tarefas, listadas a seguir.



*Figura 17-Etapas investigativas e de persecução patrimonial*

Essas tarefas podem não ocorrer na ordem apresentada e, em alguns casos, podem até não se aplicar. Cabe ao investigador adaptar os aspectos relevantes de cada uma delas ao caso concreto, de forma a obter o melhor resultado.

### **5.1. Identificar**

A tarefa de identificar o uso de ativos virtuais ou de saldo representativo de ativos virtuais pode ser subdividida em duas, a saber:

- Identificar indícios do uso ou propriedade de ativos virtuais ou de saldos representativos de ativos virtuais;
- Identificar se há indícios da espécie de ativo virtual ou da representação do saldo.

#### **Identificar indícios do uso**



Em muitos casos, a identificação é obtida de forma imediata, ainda no início da investigação. Situações como investigações decorrentes de procedimentos precedentes com compartilhamento de provas ou notícias-crime que indiquem o uso de ativos virtuais ou cadastros em PSAVs, por exemplo, podem revelar de forma direta o uso de tais ativos ou de saldos pelo alvo. Nesses casos, essa subtarefa estaria superada.

Contudo, devemos considerar a possibilidade de haver apenas indícios superficiais, que levem a uma suspeita inicial e incerta. Nesse cenário, o investigador deverá recorrer a outros meios investigativos para cumprir a subtarefa.

Para tanto, o investigador poderá se valer dos seguintes meios de investigação (lista não-exauriente):

- Pesquisas em fontes abertas: especialmente redes sociais de difusão de negócios financeiros;
- Pesquisas em redes sociais;
- Análise de Relatório de Inteligência Financeira;
- Análise Bancária decorrente de afastamento de sigilo;
- Análise Fiscal;
- Análise Telemática;
- Análise de Material Apreendido (documentos, celulares, HDs de computadores);
- Requisições cadastrais para PSAVs

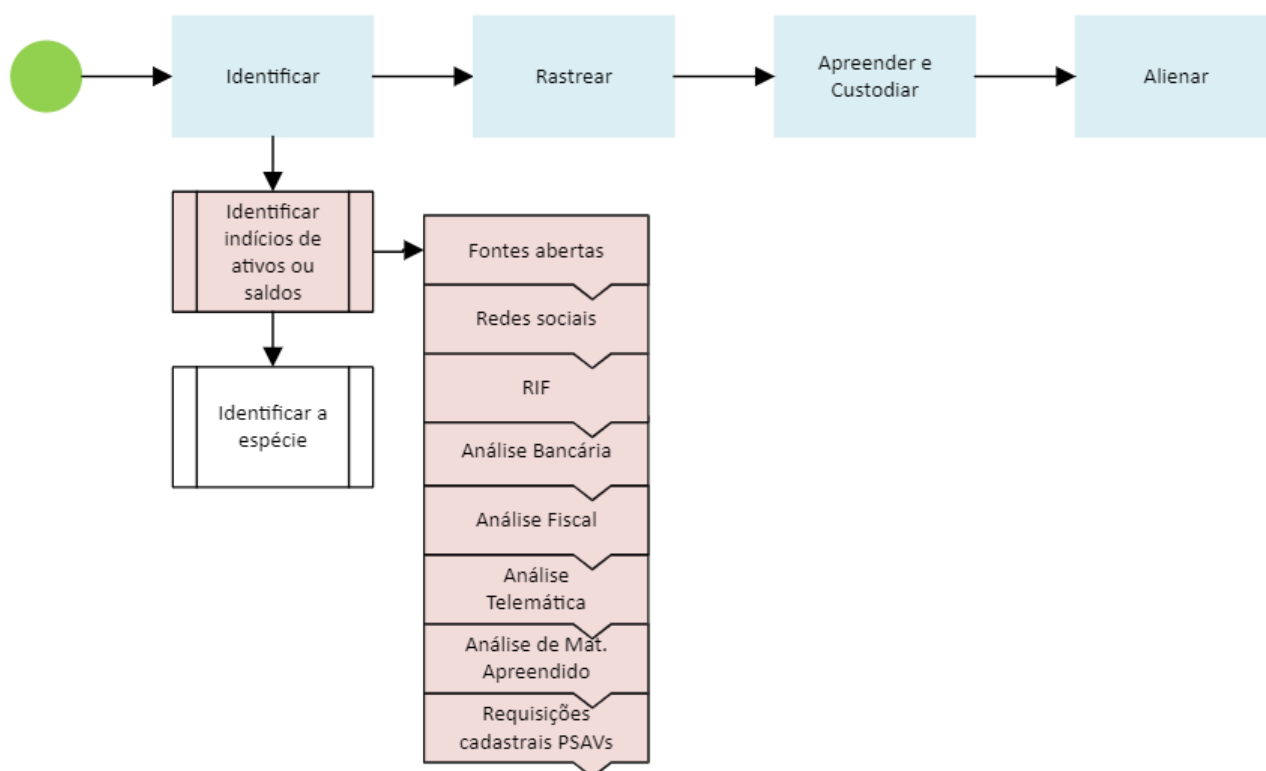


Figura 18-Subtarefas da identificação de ativos virtuais

Quanto à obtenção de identificação por meio de fontes abertas e rede sociais o investigador deverá realizar pesquisas diretamente nas plataformas ou usar o suporte de motores de busca específicos. Trata-se de tema relacionado ao ambiente da OSINT para o qual remetemos o leitor. Cabe enfatizar, todavia, que o investigador deverá ter em mente a diferenciação entre ativos e saldos, explicitada anteriormente. Algumas pessoas publicam endereços públicos na internet outras ensinam a fazer cadastros em PSAVs. A diferenciação é importante na medida em que permitirá ao investigador dar o próximo passo de modo mais seguro quanto à obtenção de informações.

Já por ocasião da análise de Relatórios de Inteligência Financeira o policial deve estar atento, no campo de “Informações Adicionais” aos termos relacionados com o ambiente dos ativos virtuais, tais como: ativo, virtual, corretora, ativos virtuais, criptomoedas, bit, bitcoin, digital, digitais etc. Vejamos exemplos de textos “Informações Adicionais”, com menção ao mercado de ativos virtuais, extraídos do Banco de Dados de RIF da DRLD/CGRC/DICOR/PF, sem identificação do titular envolvido. Repare que o RIF traz informações importantes que indicam saldo representativo junto a PSAVs e não necessariamente a propriedade de fato de ativos virtuais em endereços públicos:

*“Cliente de Cuiabá MT. Consta ser motorista com **RENDA** de R\$ 5.000,00. No período de 2 meses movimentou R\$ 345.656,08 a **CREDITO** e R\$*

345.625,76 a **DEBITO**, com destaque para TED de terceiros e enviadas a uma corretora de ativos virtuais. Movimentação incompatível com a **REND**A cadastrada. Principais **CREDITOs**: (...). Principais **DEBITOs**: R\$ 330.340,52 - XXXXXXXX **SERVICOS DIGITAIS** LTDA, CNPJ AAAAAAAAAAAAAA - Caixa Econômica Federal, 2 TEDs. KYC (Gerente): "Cliente tem dificuldade em relatar a **ORIGEM** do recurso, e a forma de investimentos."

Cliente de Curitiba PR. Consta ser Administrador com **REND**A de R\$ 18.236,00. No período de 3 meses movimentou R\$ 828.120,76 a **CREDITO** e R\$ 835.010,49 a **DEBITO**, com destaque para 88 TED de/para diversos terceiros, PF e PJ, incluindo pessoas de outros Estados e corretoras de ativos virtuais. Movimentação incompatível com a **REND**A cadastrada. Principais **CREDITOs**: R\$ 177.333,33 - XXXXXXXX **SERVICOS DIGITAIS** S/A, CNPJ AAAAAAAAAAAAAA, 2 TEDs. R\$ 146.052,33 - **MERCADO BITCOIN SERVICOS DIGITAIS LTDA**, CNPJ 18213434000135."

Igual atenção deve ser despendida por ocasião da análise de extratos bancários tanto pelo SIMBA quanto pela ferramenta CIAF-Bancário. A ferramenta CIAF-Bancário pode ser bastante útil porque já traz uma pasta nomeada como "Exchange de Criptomoedas" cuja função é indicar automaticamente se o titular das operações transacionou com PSAVs (somente aquelas que constam de lista inserida na aplicação), recebendo ou enviando valores em moeda fiduciária (reais brasileiros). Do mesmo modo, isso indicará possível saldo representativo de ativos virtuais. Somente a PSAV saberá informar precisamente se tal saldo a ela dirigido foi convertido em ativo virtual (envio para um endereço público).



Figura 19-Excerto da tela da aplicação CIAF-Bancário

Os indícios também podem decorrer de afastamentos de sigilos fiscais específicos. Conforme mencionado no capítulo destinado aos aspectos normativos, através das instruções normativas 1888/2019 e 2219/2024, a Receita Federal do Brasil (RFB) coleta dados de transações de ativos virtuais tanto de pessoas físicas quanto de PSAVs. Após o deferimento do pedido de afastamento do sigilo fiscal de investigado, a Receita Federal poderá fornecer uma ampla variedade de dados relativos ao mercado de ativos virtuais e que, não raras as vezes, serão de interesse dos investigadores.

Demais disso, vale esclarecer quais informações constarão do banco de dados da Receita Federal. No caso de PSAVs brasileiras e pessoas físicas ou jurídicas que realizaram transações via P2P (operações que não foram realizadas em PSAVs, mas sim diretamente entre usuários por meio de carteiras de custódia própria), deverão ser reportadas as seguintes informações:

- a) a data da operação;
- b) o tipo da operação (compra e venda, permuta, doação, etc.);
- c) os titulares da operação;
- d) os ativos virtuais usados na operação;
- e) a quantidade de ativos virtuais negociados, em unidades, até a décima casa decimal;
- f) o valor da operação, em reais, excluídas as taxas de serviço cobradas para a execução da operação, quando houver;
- g) o valor das taxas de serviços cobradas para a execução da operação, em reais, quando houver.

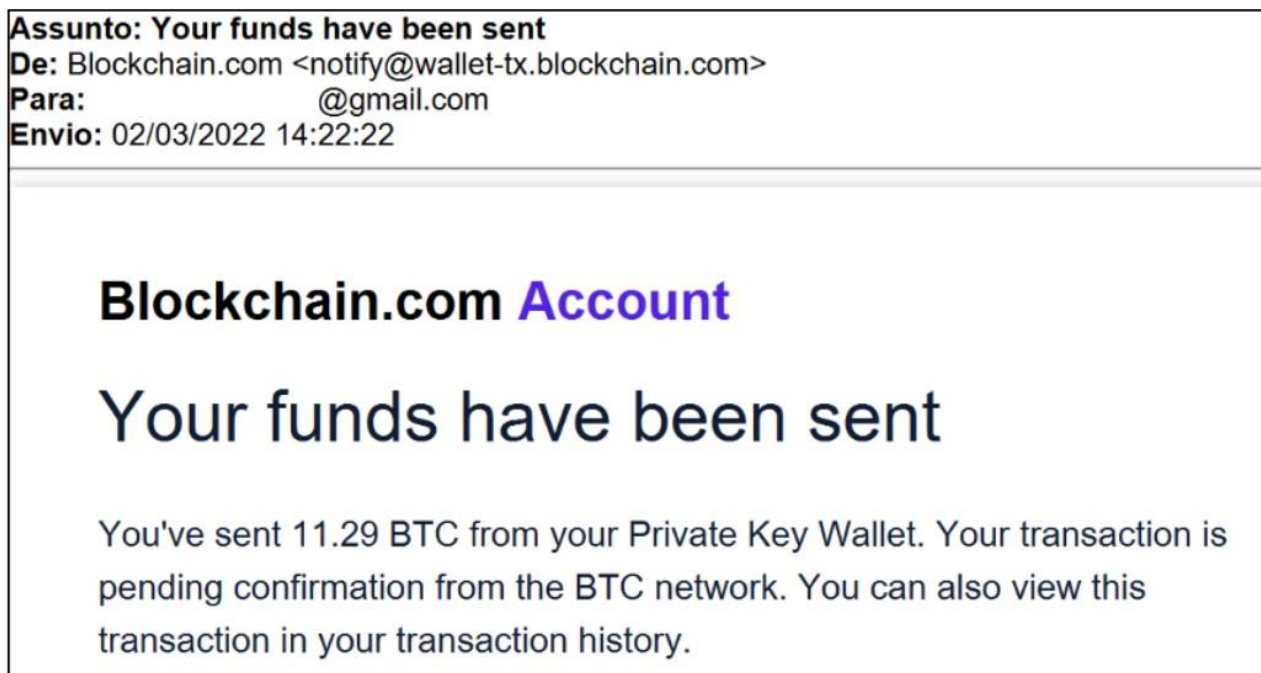
Já no caso de a pessoa física ou jurídica ter realizado operações em PSAV domiciliada no exterior, além das informações acima constará a identificação da PSAV internacional em que foi realizada a operação.

Importante, salientar, que existe um prazo para que as PSAVs brasileiras, pessoas físicas e jurídicas que se enquadram na obrigatoriedade da IN-1.888 façam esse reporte, que é o último dia útil do mês calendário subsequente àquele em que ocorreu o conjunto de operações realizadas com ativos virtuais.

E, por fim, destacamos que as PSAVs brasileiras também devem reportar até o dia 31 de dezembro de cada ano, relativamente a seus clientes:

- a) saldo em moedas fiduciárias, em reais;
- b) O saldo de cada espécie de ativos virtuais, em unidade dos respectivos ativos virtuais; e
- c) O custo, em reais, de obtenção de cada espécie de criptoativo, declarado pelo usuário de seus serviços, se houver

A análise telemática de caixa de e-mail e nuvem digital é um terreno riquíssimo para a identificação do uso de ativos virtuais ou a presença de saldos relacionados ao investigado. De fato, a experiência revela que geralmente as PSAVs enviam mensagens para o e-mail do investigado quando este acessa a aplicação de carteira ou realiza alguma transação. O investigado também tende a fazer capturas de tela (print screen) do celular ao realizar transações e guardá-las no próprio dispositivo que, caso esteja sincronizado com algum ambiente digital de guarda de dados (nuvem), tal como Icloud, Drive ou OneDrive, os arquivos poderão ser acessados ampliando as possibilidades de identificação. A seguir são apresentados arquivos digitais encontrados em caixas de email e nuvens, com preservação da identidade do investigado.



*Figura 20-Exemplo de arquivo indicativo de ativo virtual*

### Verificação de Login

Seu código de verificação

**839684**

O código de verificação será válido por 30 minutos. Não compartilhe este código com ninguém.

Não reconhece esta atividade? [Redefina a sua senha e entre em contato](#) com o nosso [suporte imediatamente](#).

*Esta é uma mensagem automática, não responda.*

Siga nossas redes sociais!

Para se manter protegido, você pode configurar um código de phishing aqui [here](#)

**Aviso de risco:** O trade de criptomoedas está sujeito ao alto risco de mercado. A Binance fará o seu melhor esforço para escolher moedas de alta qualidade, mas não será responsável por suas perdas. Por favor, faça trade com cautela.

**Atenção:** Fique atento a sites de phishing e sempre se certifique de que você está visitando o site oficial da Binance.com ao digitar dados sensíveis.

Para mais informações sobre como processamos os dados, por favor consulte a nossa [Política de Privacidade](#).

**-59.47300000 ETH**

Type	General
Status	Completed
Withdraw Address	0x52dec4b08c932d015a7bb4f1123f53a1424a34e9
Fee	0.00700000 ETH
TxID	0xc9683038749a9040c8441afdead00b44a8d1d81c37b016e74ba880bf71305904
Date	16:44:56 05/06/2021

Figura 21-Exemplos de arquivos indicativos de ativo virtual

Transaction

SENT

11.943 BTC

Value when sent: \$97,383.46  
Transaction fee: 0.00007006 BTC

Description

What's this for?

To

1QF9YTNZqEDb1Ro7tSUJeoKFXA2nAEnZSB

From

My Bitcoin Wallet

Date

October 04, 2019 @ 7:20pm

Status

Pending (0/3 Confirmations)

VIEW ON BLOCKCHAIN.COM

←

Operation details

Sent

-50.00021672 BTC

-\$1,169,897.52

• Not confirmed

Account

Bitcoin 1 (segwit)

Date

December 17, 2020, 12:57 PM

Network fees

0.00021672 BTC ≈ \$5.07

Transaction ID

a5eba3b1df7731ebcd6fd4f3c90d0b47d1111ea2ec1c5f3b9c8724b075b658e4

From (1)

3BDpvpq7VpnLqsoxc13oy56htWE5ZYBYdA

To (2)

[Why multiple addresses?](#)  
16i42nrmujZw2JpZY2uLPo9HzRBNoA6Fd8  
32Nuo9J2tHHGcbWHZLjYxsp2D5gqsNbwh4

Figura 22-Exemplos de arquivos indicativos de ativo virtual

A análise de materiais apreendidos, especialmente de celulares e HDs de computadores, é terreno fértil para identificar o uso de ativos virtuais ou de saldos representativos. Através dessas análises, é possível coletar mensagens ou arquivos digitais que contenham endereços públicos, hashes de transações, ou até capturas de tela que reúnam essas informações. Além disso, é comum encontrar confirmações de transações enviadas por aplicativos de mensagens, como Telegram, WhatsApp ou WeChat, o que amplia as possibilidades de rastreamento e comprovação das atividades envolvendo ativos virtuais.

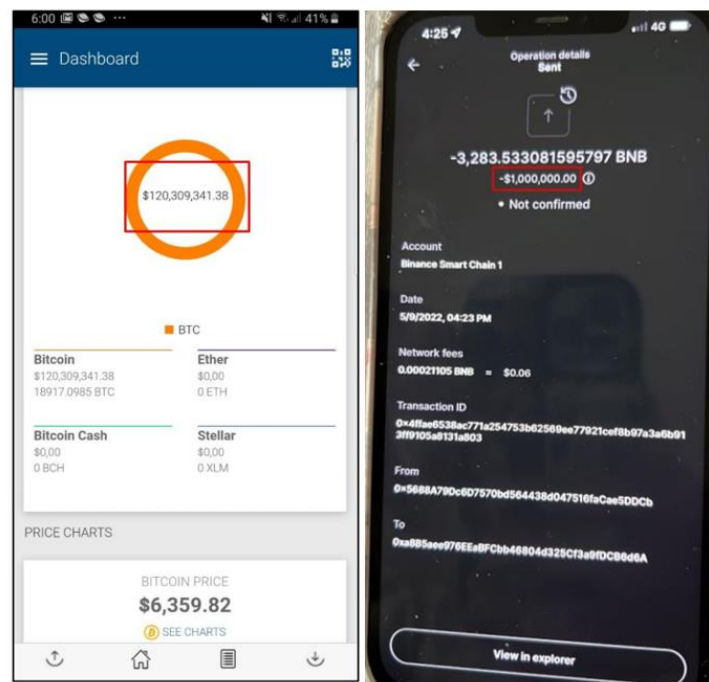


Figura 23-Exemplos de anexos de mensagens obtidos em análise de material apreendido

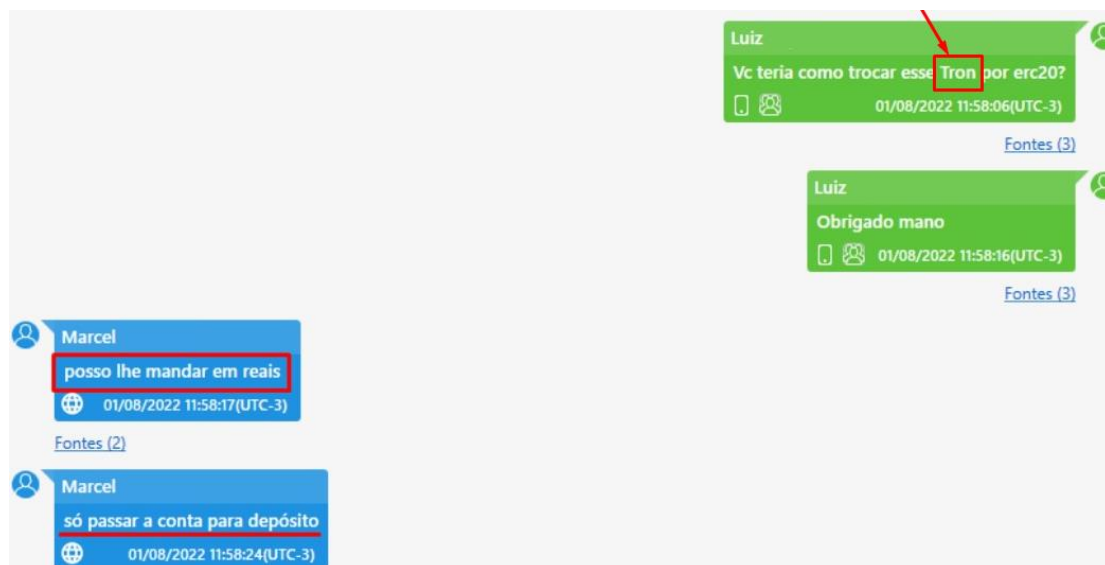


Figura 24-Exemplo de mensagem indicativa de uso da Blockchain Tron

Destacamos ainda na técnica de análise de material apreendido que a ferramenta Indexador e Processador de Evidências Digitais (IPED) oferece a busca por expressões regulares (REGEX) relacionadas ao mundo dos ativos virtuais. Em outras palavras, o IPED pode encontrar determinados padrões de endereços públicos ou até mesmo Frases Secretas de recuperação (Seed) de forma automática, bastando que o investigador habilite a função na aplicação. Significa dizer que se houver endereços públicos ou frases de recuperação no conjunto de arquivos indexados, o IPED tende a encontrar e indicar esses arquivos instantaneamente, sem necessidade de o investigador percorrer arquivo por arquivo em busca da identificação ou aplicar critérios de pesquisa por palavra-chave.

Em acréscimo, através de requisições direcionadas às PSAVs, o investigador poderá obter informações cadastrais dos alvos investigados caso eles possuam relacionamento com a empresa. Geralmente as PSAVs informam: nome completo, número telefônico, endereço de email vinculado, data de nascimento, CPF, Passaporte, e os endereços de ativos virtuais. A seguir, exemplos de cadastros da Binance e do Mercado Bitcoin.

Basic Information				
User ID	Email	Mobile	Registration time	Name
23827036	josedetaldomanual@hotmail.com	+55112223333	2018-01-21 18:28:28	JOSE DE TAL DO MANUAL
API Information				
Rule ID	API Name	Trade IP	Withdraw IP	Create Time
16	AntBot	0.0.0.0	0.0.0.0	2022-03-01 19:11:23(UTC)

Asset Ticker	Asset Name	Total Position	Estimated BTC Value	Deposit Wallet Address	Label/Tag/Memo
BNB	BNB	0	0		
BRL	Brazilian Real	0	0		
BTC	Bitcoin	0	0	14MBZT6s25FiiANRK9FzuPpTFKPCLHF5sY	
CAKE	PancakeSwap	0	0		
USDT	TetherUS	0.00000067	0.000000000321332		

Figura 25-Excerto de dados cadastrais da Binance com dados anonimizados





Figura 26-Excerto de dados cadastrais da Mercado Bitcoin




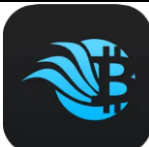



Lembramos que saldo representativo de ativos virtuais não é o ativo virtual em si. Se determinado investigado tem saldo em PSAV significa dizer que esta tem uma obrigação civil de pagamento correspondente para o investigado.

Enfatizamos, que esse meio de obtenção de provas pode submeter a investigação a um risco de vazamento, dado que a PSAV pode iniciar procedimentos para encerrar o relacionamento com o cliente. Assim, além de realizar uma avaliação de risco, é preciso fazer constar expressamente nos ofícios a determinação para que seja mantido o sigilo do inquérito, bem como para que a PSAV se abstenha de adotar quaisquer procedimentos tendentes a cientificar o cliente da existência de uma investigação em seu desfavor.

A seguir colacionamos os nomes e endereços das principais PSAVs que atuam no país, acompanhadas de seus e-mails ou meios de contato para o encaminhamento de ofícios/requisições judiciais:

PSAV logo	PSAV/Site/Contato Law Enforcement
	BINANCE <a href="https://www.binance.com/pt-BR">https://www.binance.com/pt-BR</a> Plataforma KODEX <a href="https://app.kodexglobal.com/signin">https://app.kodexglobal.com/signin</a>
	BITFY <a href="https://bitfy.app/">https://bitfy.app/</a> <a href="mailto:juridico@ripio.com">juridico@ripio.com</a> <a href="mailto:juridico@bitcointrade.com.br">juridico@bitcointrade.com.br</a> Whatsapp: +55 11 93239-8261 / + 55 11 3239-8261
	BISCOINT <a href="https://biscoin.io/">https://biscoin.io/</a> <a href="mailto:suporte@biscoin.io">suporte@biscoin.io</a>

	<b>BITBALCAO</b> <a href="https://bitbalcao.com.br/">https://bitbalcao.com.br/</a> 19-99713-6118 / 19 99713-6118
	<b>BITBLUE</b> <a href="https://bitblue.com/">https://bitblue.com/</a>  <i>juridico@bitblue.com</i>
	<b>RIPIO TRADE</b> <a href="https://ripio.com.br/ripiotrade/">https://ripio.com.br/ripiotrade/</a> <i>juridico@ripio.com</i> <i>juridico@bitcointrade.com.br</i>
	<b>BITYPREÇO</b> <a href="https://bitypreco.com/">https://bitypreco.com/</a> priscila@bitpreco.com compliance@bitpreco.com
	<b>BITNUVEM</b> <a href="https://bitnuvem.com/suporte@bitnuvem.com">https://bitnuvem.com/suporte@bitnuvem.com</a> 19-9624-4268 (11) 9756-5867 <b>WHATSAPP</b> 19 99755-2945
	<b>COINBASE</b> <a href="https://www.coinbase.com/pt-br/">https://www.coinbase.com/pt-br/</a> Plataforma KODEX <a href="https://app.kodexglobal.com/signin">https://app.kodexglobal.com/signin</a> <i>int.subpoenas@coinbase.com</i> <i>giovanna.nahhat@coinbase.com</i>
	<b>COINEXT</b> <a href="https://coinext.com.br/">https://coinext.com.br/</a> <i>juridico@coinext.com.br</i>
	<b>FLOW</b> <a href="https://www.flowbtc.com.br/">https://www.flowbtc.com.br/</a> <i>compliance@flowbtc.com.br (usar este)</i> <i>helen@flowbtc.com.br (mandar com cópia)</i> <i>mariana@flowbtc.com.br (mandar com cópia)</i>
	<b>FOXBIT</b> <a href="https://foxbit.com.br/">https://foxbit.com.br/</a> <i>victor.gomes@foxbit.com.br</i>
	<b>MERCADO BITCOIN</b> <a href="https://www.mercadobitcoin.com.br/">https://www.mercadobitcoin.com.br/</a> <i>juridico@mercadobitcoin.com.br</i>
	<b>NOVADAX</b> <a href="https://www.novadax.com.br/">https://www.novadax.com.br/</a> <i>compliance@novadax.com</i>
	<b>KRAKEN</b> <a href="https://www.kraken.com/pt-br">https://www.kraken.com/pt-br</a> <a href="https://support.kraken.com/hc/pt-br/forms/648008">https://support.kraken.com/hc/pt-br/forms/648008</a>

	PHEMEX <a href="https://phemex.com/pt/">https://phemex.com/pt/</a> <a href="mailto:support@phemex.zendesk.com">support@phemex.zendesk.com</a>
	NOXBITCOIN <a href="https://noxbitcoin.com.br/">https://noxbitcoin.com.br/</a> <a href="mailto:hi@noxbitcoin.com.br">hi@noxbitcoin.com.br</a>
	BITCOINTOYOU <a href="https://bitcointoyou.com/">https://bitcointoyou.com/</a> <a href="mailto:contato@bitcointoyou.com">contato@bitcointoyou.com</a> <a href="mailto:juridico@bitcointoyou.com">juridico@bitcointoyou.com</a>
	BRASIL BITCOIN <a href="https://brasilbitcoin.com.br/">https://brasilbitcoin.com.br/</a> <a href="mailto:suporte@brasilbitcoin.com.br">suporte@brasilbitcoin.com.br</a>
	BIT RECIFE <a href="https://www.bitrecife.com.br/">https://www.bitrecife.com.br/</a> <a href="mailto:postmaster@bitrecife.com.br">postmaster@bitrecife.com.br</a>
	BIT CÂMBIO <a href="https://bitcambio.com.br/#/">https://bitcambio.com.br/#/</a> <a href="mailto:juridico@grupocitar.com.br">juridico@grupocitar.com.br</a>
	CAPITAL DIGITAL ABERTO <a href="https://capitaldigitalaberto.com.br/">https://capitaldigitalaberto.com.br/</a> <a href="mailto:contato@capitaldigitalaberto.com.br">contato@capitaldigitalaberto.com.br</a> <a href="mailto:juridico@capitaldigitalaberto.com.br">juridico@capitaldigitalaberto.com.br</a>

*Quadro 3-Lista das principais PSAVs e contatos Law Enforcement*

Por se tratar de um mercado dinâmico e extremamente volátil, é possível que os meios de contato citados anteriormente sejam alterados, seja pela fusão de empresas ou pelo encerramento da atividade. Dessa forma é possível buscar informações mais atualizadas no portal CIAF através do link:

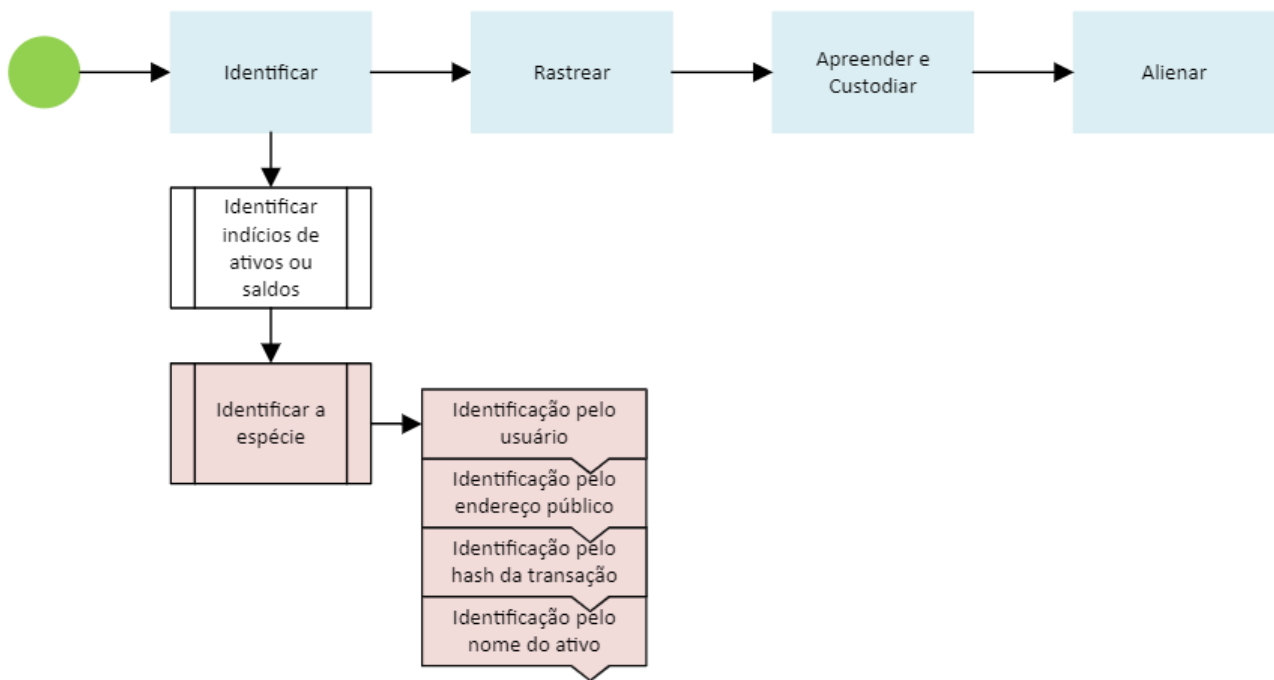
<https://pfgovbr.sharepoint.com/sites/PortalCIAF/SitePages/Principais-Corretoras-Exchanges-que-operam-no-Brasil.aspx>

### **Identificar a espécie**

Para descobrir qual a espécie necessitamos ao menos de uma dessas referências:

- Identificação pelo usuário;
- Identificação pelo endereço público;
- Identificação pelo hash da transação;

- Identificação pelo nome do ativo virtual



*Figura 27-Subtarefas de identificação da espécie de ativo virtual*

Consoante mencionado no tópico anterior, o investigador poderá obter dados cadastrais junto às PSAVs. Tais dados cadastrais abrangem não somente a qualificação pessoal como também os endereços públicos que a PSAV atribuiu ao investigado para receber ativos virtuais da blockchain, inclusive separados por tipos de ativos virtuais, conforme a compatibilidade da rede blockchain.

Em outros casos, a verificação do formato do endereço público obtido permitirá determinar o ativo ao qual o endereço está atrelado. De fato, endereços públicos de diferentes blockchains têm formatos específicos. Apenas ao analisar o formato, já seria possível identificar a qual rede o endereço pertence e, conseqüentemente, qual ativo virtual pode estar sendo utilizado. Segue tabela com alguns dos padrões:

Ativo Virtual	Formato de endereço público	Exemplo de endereço público
Bitcoin (BTC)	Legacy (P2PKH), começa com "1"	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Bitcoin (BTC)	SegWit (P2SH), começa com "3"	3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy
Bitcoin (BTC)	Bech32 (Native SegWit), começa com "bc1"	bc1qar0srrr7xfkvy5l643lydnw9re59gtzwwf8txh

Ethereum (ETH)	Começa com "0x"	0xde0B295669a9FD93d5F28D9Ec85E40f4cb697Bae
Litecoin (LTC)	Legacy (P2PKH), começa com "L"	LZVjx63zLqBppDcNoRZZsXzAq9czKegKsn
Litecoin (LTC)	SegWit (P2SH), começa com "M"	MQMcJhpWHYVeQArcZR3sBgyPZxxRygs7vT
Litecoin (LTC)	Bech32 (Native SegWit), começa com "ltc1"	ltc1qar0srrr7xfkvy5l643lydnw9re59gtzwwf8txh
Ripple (XRP)	Começa com "r"	rEb8TK3gBgk5auZkwc6sHnwrGVJH8DuaLh
Bitcoin Cash (BCH)	Legacy, começa com "1" ou "3"	1BpEi6DfDAUFd7GtittLSdBeYJvcoaVggu
Bitcoin Cash (BCH)	CashAddr, começa com "q" ou "p"	qpm2qsznhks23z7629mms6s4cwef74vcwvy22gdx6a
Cardano (ADA)	Começa com "addr"	addr1q9xlwqf6hl0j5g9fh3pgw4tnxu5h9n5l9n4uvmfppwz4mfgsm4qdq7aztg2fhxj0k
Binance Coin (BNB) (BEP-2)	Começa com "bnb"	bnb1grp0955h0yk8usrnvzp4eq4gzuwvps7e5u8pe
Binance Smart Chain (BSC) (BEP-20)	Igual ao Ethereum, começa com "0x"	0xde0B295669a9FD93d5F28D9Ec85E40f4cb697Bae
Monero (XMR)	Começa com "4" ou "8"	48Y4q3DsYKjHoafD9g7oNKnZ9PYWDpgYTGJMiHUgmkBbYhTnYZ kVzRXYbRoDpgV7G2XsiNtQFwD2pkM3RSBFCrdCjx1FJ5
Dash (DASH)	Começa com "X" ou "7"	XxXxC6tptWAqkWoZunxPqXU6Zxxmgxro
Zcash (ZEC)	Transparent Address (t-addr), começa com "t1" ou "t3"	t1RyvYvZP8Gt5fXzUE8AHuB9xNgtRa8MoC
Zcash (ZEC)	Shielded Address (z-addr), começa com "zs"	zs1m3pm5e42dn0zwpw50xz0xs2xsvjx40dz63tjhhrlpvayq5z8mrhs3fplr6gs0qd
Polkadot (DOT)	Começa com "1"	1zugcCF9WLfN3vxQGHq1w4EHk7PjL35XkqC4FGiEkA
Stellar (XLM)	Começa com "G"	GBRPYHIL2C5SXI2RJKH4NBDFYA5JDJYE4RB5WJAKI5SAI2FZTTVGTLTG
Tron (TRX)	Começa com "T"	TJRy4Psh4prK1ysus7zBkoP9NxxTibzYwb
VeChain (VET)	Começa com "0x"	0xdceaf1652a131F32a821468Dc03A92df0edd86Ea
Dogecoin (DOGE)	Começa com "D"	D8B7xsQBTzcqFz3FgoD9YpDoEugzQHBsV4

Solana (SOL)	Comprimento variável (geralmente 32 ou 44 caracteres)	5gPhzVBD6CxrEgKQxQLu5RAuYxnS2Jkrt89qPgsKQwaU
-----------------	---	--

Quadro 4-Padrões de endereços conforme o ativo virtual ou blockchain

Para além da identificação da espécie de ativo virtual a partir do padrão de formato do endereço podemos usar exploradores de blockchain e até mesmo o Google para determiná-la. Com efeito, o Google passou a indexar os endereços públicos e bastaria inserir o endereço no campo de pesquisa. O resultado indicaria as blockchains atreladas.

Google

0x264bd8291fAE1D75DB2c5F573b07faA6715997B5

X

TodasImagensVideosShoppingNotíciasMapsLivrosMaisFerramentas

Endereço da blockchain

Rede	Saldo	Última atualização	Buscador
Ethereum	1982.996917072307317237 ETH	20 de out. de 2024, 5:45 PM BRT	Etherscan.io
Arbitrum	0.470001485719226000 ETH	12 de set. de 2024, 7:31 PM BRT	Arbiscan.io
Polígono	3516.837479659551033274 MATIC	09 de ago. de 2024, 5:57 PM BRT	Polygonscan.com

Figura 28-Pesquisa de endereço público no Google com resultado indicando as redes blockchain

Podemos usar também exploradores de blockchain, já mencionados anteriormente, que são motores de busca que apresentam a espécie de ativo virtual vinculado ao endereço aplicado. Os mais conhecidos são Etherscam.io para Ethereum, Blockchain.com para Bitcoin, Tronscan.org para Tron.

*Figura 29-Pesquisa de endereço público no explorador Etherscan*

Os hashes das transações também poderão ser usados como critério de pesquisa nos exploradores de blockchain com resultado semelhante.

É importante destacar que recorrentemente temos visto, a partir de análises de material apreendido, especialmente de celulares, o uso do termo USDT que se refere ao token Tether (USDT), um token stablecoin que afirma manter paridade com o dólar americano. Já mencionamos que tokens são construídos a partir de contratos inteligentes (programações de computador) inseridos em blockchains completas, abertas, de segunda geração. Sendo assim, ressaltamos que o USDT é emitido em diversas redes blockchain, incluindo Ethereum (ERC-20), Tron (TRC-20) e Binance Smart Chain (BEP-20), entre outras. Portanto, podemos ver transações de Tether (USDT) em variadas blockchains, considerando a emissão em diversas delas. Imaginemos um Banco Central mundial que pudesse emitir dólares em determinados países. Numa metáfora, os países seriam as redes blockchain e os dólares seriam o Tether (USDT).

Recentemente, observou-se um crescimento acentuado no uso do Tether (USDT) globalmente, especialmente na rede Tron, que se destaca por suas taxas de transação mais baixas em comparação com a rede Ethereum. Esse fenômeno também é evidente no Brasil, onde investigações conduzidas pela Polícia Federal revelam o uso do Tether (USDT) para realizar pagamentos à margem do Sistema Financeiro Nacional ou em

transações ilícitas de todo tipo, seja como pagamento de drogas, contrabando, crimes cibernéticos e até mesmo pedofilia. Essa tendência é corroborada pelas estatísticas publicadas pela Receita Federal do Brasil, que estão apresentadas no gráfico a seguir.

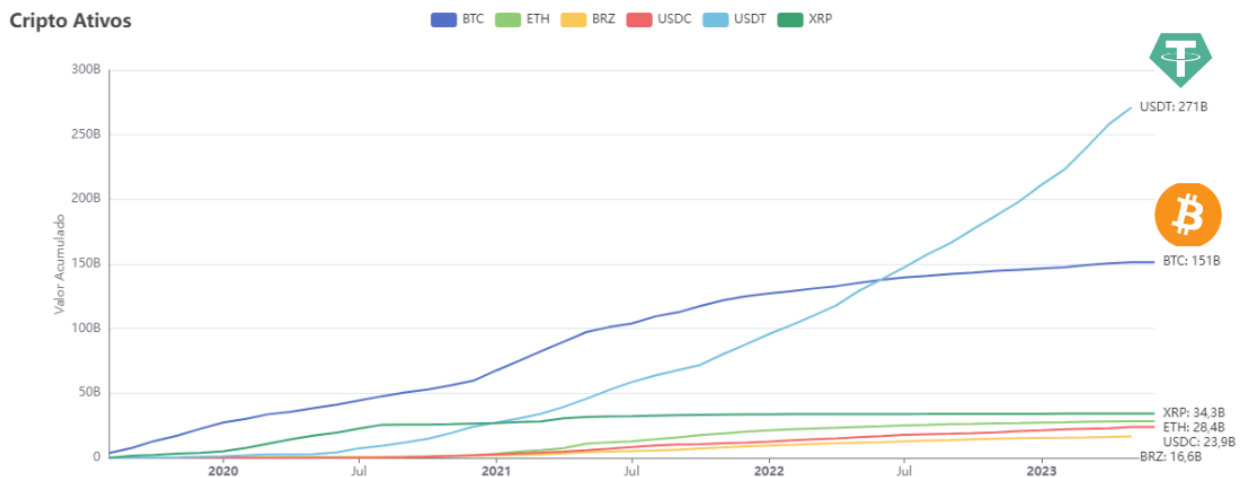


Figura 30-Excerto de comunicação da Receita Federal - disponível em <https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2023/outubro/criptoativos-receita-federal-detecta-crescimento-vertiginoso-na-movimentacao-de-stablecoins>

Essas considerações são fundamentais, pois a identificação de um endereço público em uma determinada rede não implica necessariamente que o investigado esteja transacionando a criptomoeda nativa daquela rede. Na verdade, o investigado pode estar utilizando o Tether (USDT) na mesma rede, ou seja, movimentando o token Tether (USDT) que opera dentro da infraestrutura dessa blockchain. Lembramos que a blockchain Ethereum (assim como outras) é aberta, completa sob a ótica da programação. Nada impede que sejam criados nela tokens por meio de contratos inteligentes compatíveis com essa blockchain e por consequência ali negociados. Esse assunto será aprofundado no tópico destinado ao rastreamento. Uma lista completa dos ativos virtuais mais importantes é encontrada no sítio [coinmarket.com](https://coinmarket.com).

## 5.2. Rastrear

O rastreamento pode ser dividido em dois tipos principais: On-chain e Off-chain, e ambos desempenham papéis fundamentais na análise e investigação de transações com ativos virtuais.



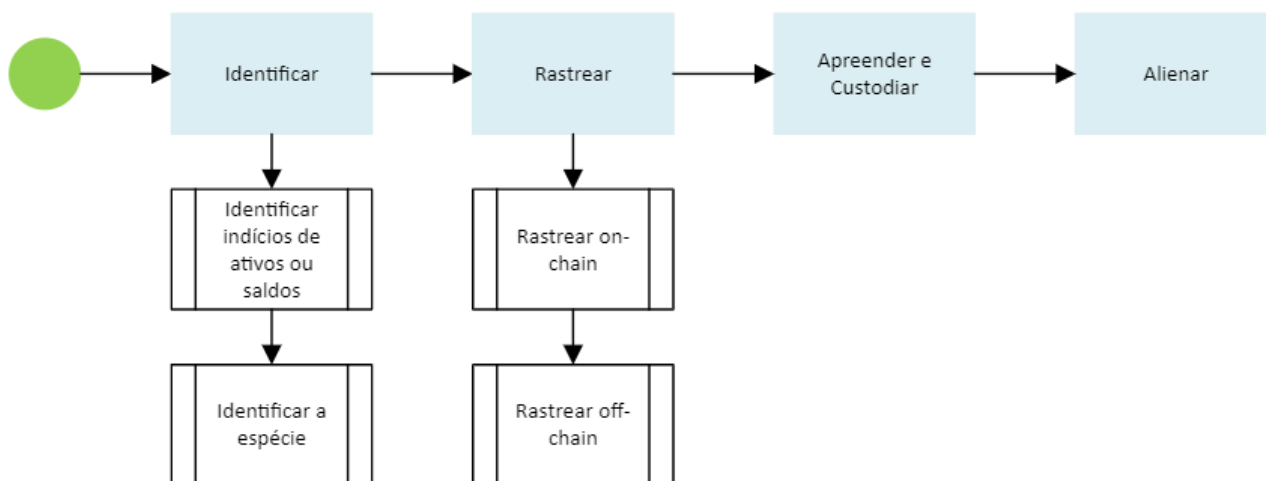


Figura 31-Tarefas do comando “Rastrear”

### 5.2.1. Rastreamento On-Chain

Em linhas gerais, o Rastreamento On-Chain refere-se à análise de transações e dados registrados diretamente na rede blockchain e pode ser realizado conforme as subtarefas a seguir apresentadas.

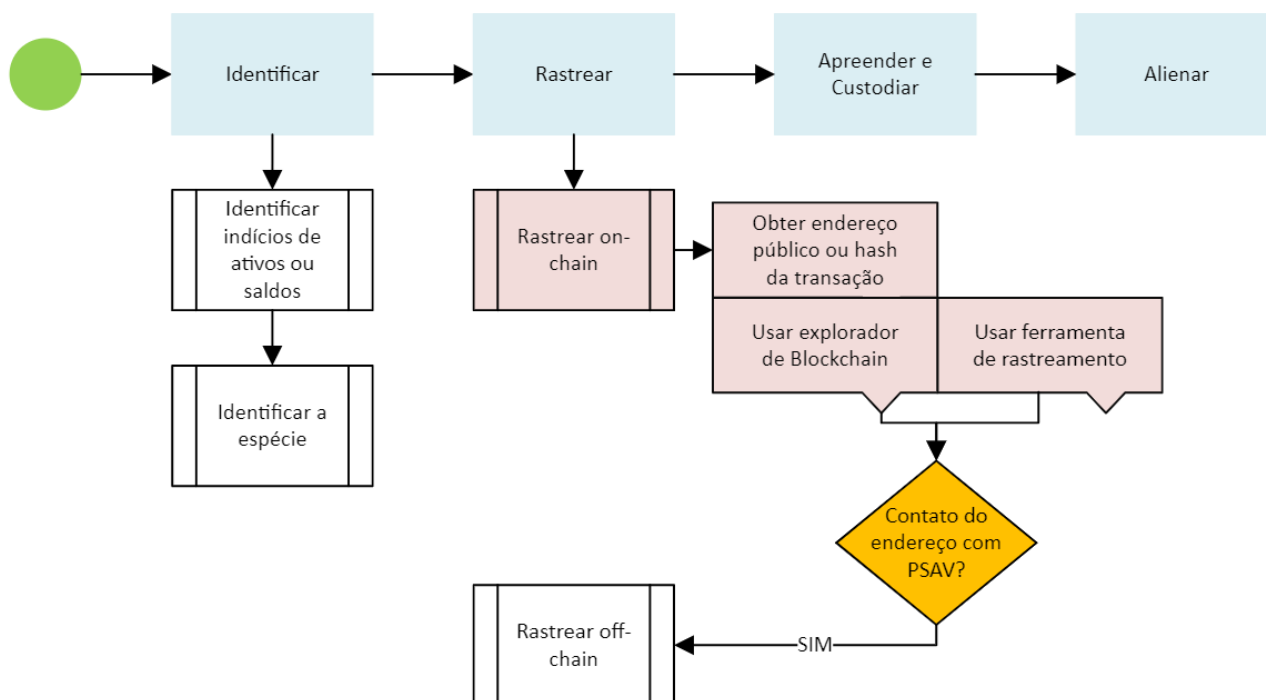


Figura 32-Subtarefas do Rastreamento On-Chain

Sabemos que as transações de ativos virtuais, como Bitcoin, Ethereum ou Tether (USDT), são armazenadas de forma pública e transparente em suas respectivas redes blockchains, permitindo que qualquer pessoa acesse essas informações. Portanto, o

Rastreamento On-Chain se relaciona com a propriedade de fato de ativos virtuais e não com o saldo representativo que porventura alguma pessoa tenha junto a uma PSAV.

São características do Rastreamento On-Chain:

- Transparência: porque as transações são públicas e imutáveis;
- Descentralização: não depende de uma entidade central para fornecer os dados, diferente de uma quebra bancária;
- Rastreabilidade: permite o acompanhamento contínuo de ativos pelo histórico de transações, desde a sua origem até o destino, incluindo os intermediários, ao menos até determinados pontos;
- Anonimato relativo: identificar o proprietário de um endereço pode ser difícil sem informações adicionais, mas o pseudonimato aqui se aplica considerando que se o endereço público decorre de uma informação precedente que o vincule ao investigado, podemos atribuí-lo, assim como as transações verificadas.

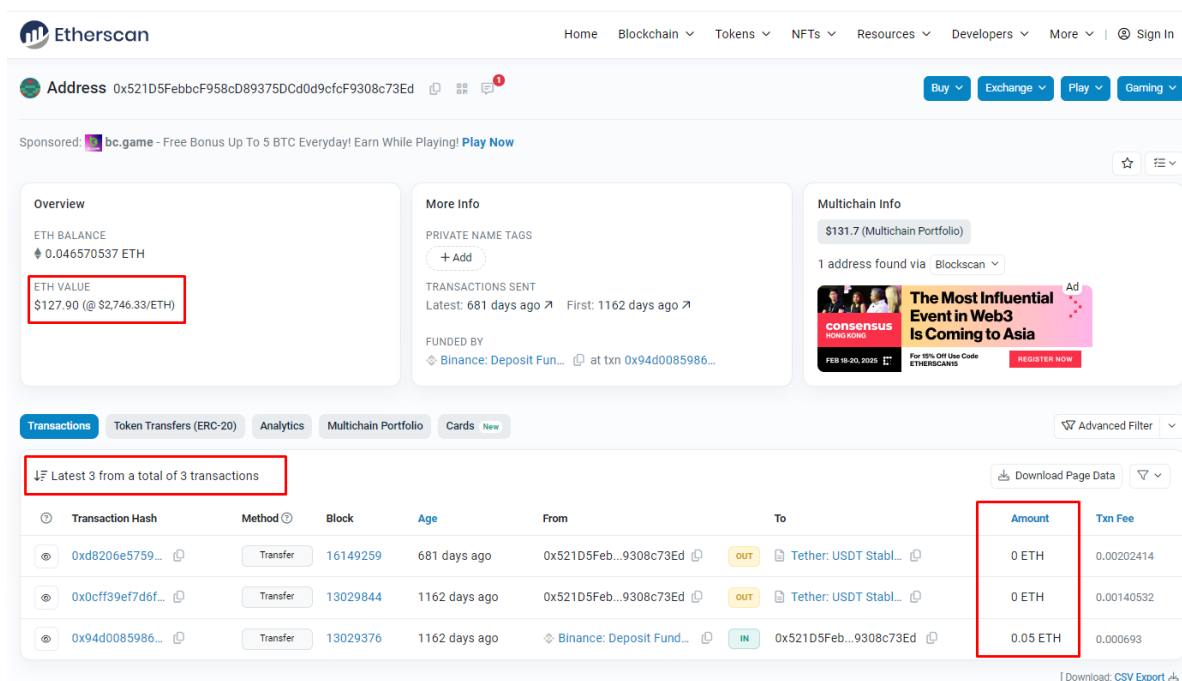
O Rastreamento On-Chain permite verificar:

- Transações: Identificação de todas as transferências de um criptoativo entre diferentes endereços públicos.
- Saldos: Verificação dos saldos de endereços públicos.
- Interações com Smart Contracts: como sabido, em blockchains como Ethereum, é possível analisar interações com contratos inteligentes, como tokens Tether (USDT).

O Rastreamento On-Chain pode ser feito através de exploradores de blockchain ou ferramentas de rastreamento, com a inserção do endereço público ou o hash da transação, sendo estes os pontos de partida para encontrar as origens e destinos, e por consequência analisar os fluxos sob a ótica investigativa.

Como já mencionado, os principais exploradores de blockchain são: [blockchain.com](https://blockchain.com), [etherscan.io](https://etherscan.io) e [tronscan.org](https://tronscan.org). Na figura a seguir, por exemplo, foi inserido um endereço público de Ethereum no explorador [etherscan.io](https://etherscan.io). Note que a interface inicial

do explorador apresenta as transações com a criptomoeda nativa da rede, a Ether, representada pela sigla ETH. Pelo que se verifica, há um pequeno saldo em ETH correspondente a USD 127,00 e o movimento foi mínimo com apenas três transações.



The screenshot displays the Etherscan interface for a specific Ethereum address. The 'Overview' section shows an ETH balance of 0.046570537 and a value of \$127.90. The 'Transactions' section shows three transactions, with the 'Amount' column highlighted. The transactions are:

Transaction Hash	Method	Block	Age	From	To	Amount	Txn Fee
0xd8206e5759...	Transfer	16149259	681 days ago	0x521D5FebbcF958cD89375D0d0d9cfF9308c73Ed	Tether: USDT Stabl...	0 ETH	0.00202414
0x0cf39ef7d6f...	Transfer	13029844	1162 days ago	0x521D5FebbcF958cD89375D0d0d9cfF9308c73Ed	Tether: USDT Stabl...	0 ETH	0.00140532
0x94d0085986...	Transfer	13029376	1162 days ago	Binance: Deposit Fund...	0x521D5FebbcF958cD89375D0d0d9cfF9308c73Ed	0.05 ETH	0.000693

Figura 33-Excerto de pesquisa de endereço público na rede Ethereum na aba Transactions (que traz apenas as transações na moeda nativa ETH)

Todavia, o investigador não deve se ater somente aos movimentos da criptomoeda nativa, geralmente usada para pagar taxas de transações. Como sabido, a blockchain Ethereum comporta tokens decorrentes de contratos inteligentes, especialmente o token Tether (USDT), que mencionamos estar intimamente relacionado com práticas criminosas. Portanto, o investigador deverá também verificar a aba “Token Transfers (ERC-20)” a fim de encontrar os movimentos de USDT.

Podemos agora verificar na figura abaixo que houve cinco movimentações de tokens Tether (USDT) relacionadas a este endereço, sendo três delas de entrada e duas delas de saída. Em resumo, houve a entrada, neste endereço, de cerca de USDT 6,5 milhões (6,5 milhões de dólares americanos, por conta da paridade da stablecoin), os quais foram enviados para a PSAV Binance, que poderá nos alimentar de informações a partir de um pedido judicial da escrituração interna, afinal de contas, não sabemos o que ocorreu daí para adiante, pois, uma vez que os ativos virtuais ingressam na PSAV poderão tomar caminhos diversos: conversão em saldo representativo; liquidação em moeda fiduciária para uma conta bancária; ou ainda enviados para outro endereço.

Transactions

Token Transfers (ERC-20)

Analytics

Multichain Portfolio

Cards

New

Advanced Filter

Transactions involving tokens marked as suspicious, unsafe, spam or brand infringement are currently hidden. To show them, go to Site Settings.

Transactions with zero token value are currently hidden. To show them, go to Site Settings.

Latest 5 ERC-20 Token Transfer Events

Download Page Data

Transaction Hash	Method	Block	Age	From	To	Amount	Token
0xd8206e5759...	Transfer	16149259	681 days ago	0x521D5Feb...9308c73Ed	OUT Binance 14	499.925011	Tether USD (USDT)
0x848b89c02c...	Transfer	13260292	1126 days ago	Coinbase 5	IN 0x521D5Feb...9308c73Ed	499.925011	Tether USD (USDT)
0x0c9f39ef7d6f...	Transfer	13029844	1162 days ago	0x521D5Feb...9308c73Ed	OUT Binance 14	5,998,385.769901	Tether USD (USDT)
0xe0286c549f7...	Transfer	13007958	1165 days ago	0xcA7A2fca...0f27002F	IN 0x521D5Feb...9308c73Ed	3,000,000	Tether USD (USDT)
0x0c4627b52e...	Transfer	12993111	1168 days ago	0x0500d67C...388351BFc	IN 0x521D5Feb...9308c73Ed	2,998,385.769901	Tether USD (USDT)

Download CSV Export

Figura 34-Excerto de pesquisa de endereço público na rede Ethereum na aba Token Transfers (ERC-20) (representativo de Tether USDT)

A representação em linha de tempo cronológica dessas transações pode ser vista na próxima figura. Note que o investigado (endereço pesquisado) recebeu Tether USDT de duas pessoas anônimas. Por outro lado, ele recebeu Tether USDT da PSAV Coinbase e enviou para a Binance. Essas PSAVs poderão responder os pedidos judiciais de quebra visando à obtenção dos dados das contrapartes envolvidas. Note-se que 6 milhões em Tether USDT foram para a Binance e somente ela poderá nos informar o que ocorreu daí em diante.

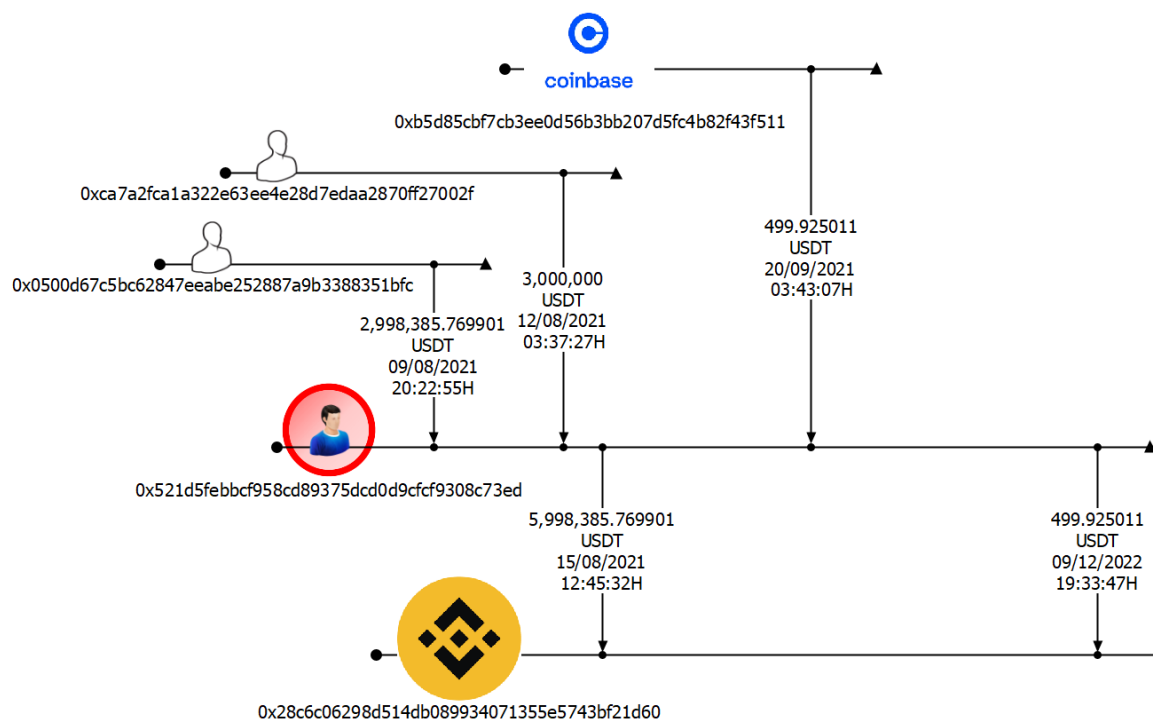


Figura 35-Linha de Tempo de transações com ativos virtuais Tether USDT-destino final = Binance

Para além dos exploradores de blockchain, existem ferramentas comerciais e gratuitas que permitem realizar o rastreamento, com destaques para: Chainalysis (paga), TRM (paga), Arkham (gratuita), Metasleuth (gratuita), e Blockpath (gratuita). Essas ferramentas auxiliam a traçar os fluxos bem como identificar até mesmo entidades ou pseudônimos que estejam atrelados a determinados endereços. Ou seja, essas ferramentas poderão trazer dados mais apurados das contrapartes envolvidas, mitigando o anonimato. Abaixo podemos verificar as telas de rastreamento das ferramentas Metasleuth e Arkham, nesta ordem, usando como critério o mesmo endereço já aplicado no Etherscam.

Na primeira figura, repare que, diferentemente do explorador Etherscam, a ferramenta Metasleuth já atribuiu ao endereço do investigado, representado no centro do gráfico, um logotipo da Binance, assim como no endereço de destino. Portanto, podemos concluir que o endereço público do investigado, que é aquele que foi usado como critério de pesquisa, é um endereço de recebimento que a Binance lhe atribuiu quando da realização do seu cadastro original. Esta informação é importante na medida em que podemos requisitar informações cadastrais junto à Binance para confirmar a relação do investigado com o endereço ou até mesmo encontrar interposição de pessoas, caso o endereço esteja cadastrado em nome de um “laranja”.

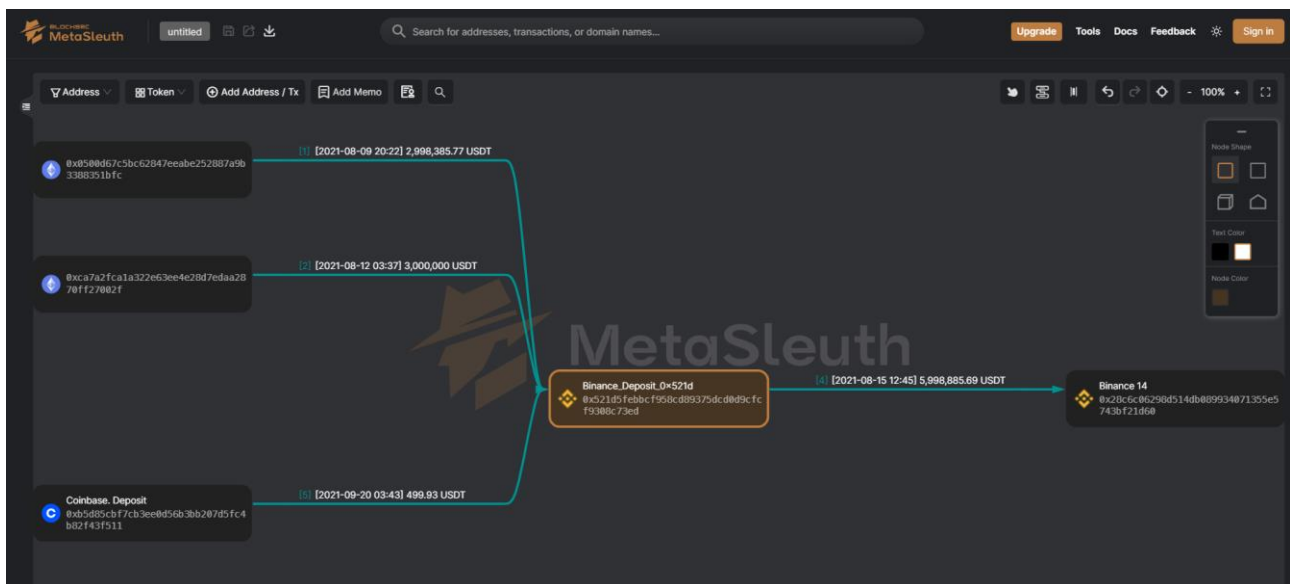


Figura 36-Excerto da tela de rastreamento On-Chain da Metasleuth

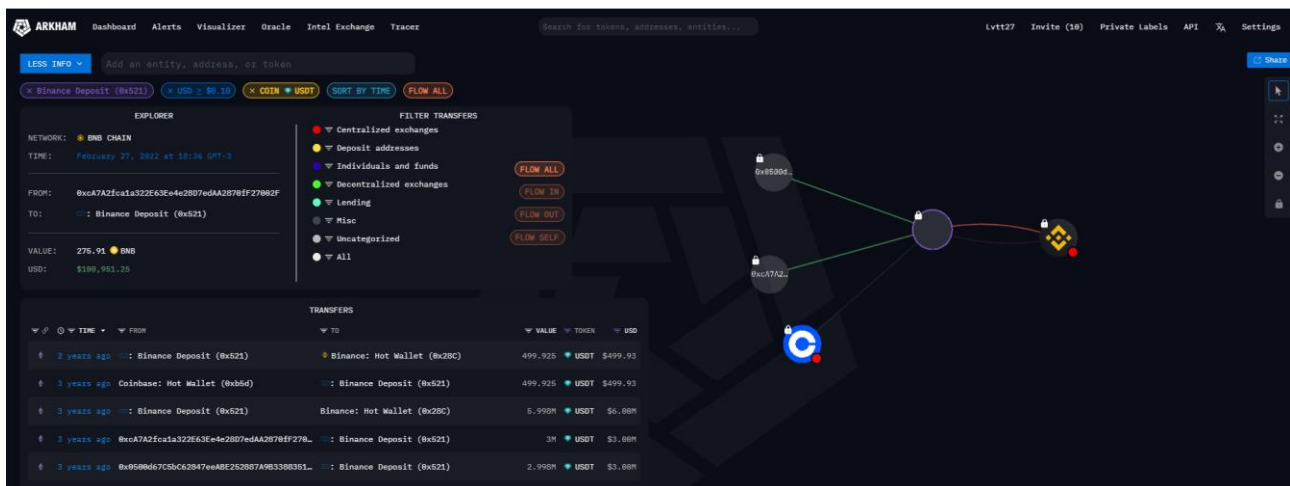


Figura 37-Excerto da tela de rastreamento On-Chain da Arkham

A Divisão de Repressão aos Crimes Financeiros (DFIN) vem realizando cursos para os servidores policiais na temática ativos virtuais (CIAF-Cripto), onde a técnica de Rastreamento On-Chain é apresentada e aprofundada. Por ora, resta-nos informar que é possível realizar rastreamentos com resultados bastante satisfatórios, os quais podem ser aperfeiçoados de acordo com a capacidade tecnológica da ferramenta utilizada e com as informações colacionadas.

### 5.2.2. Rastreamento Off-Chain

Conforme visto no tópico anterior, a análise do caminho percorrido pelos ativos através do Rastreamento On-Chain, por vezes, culminará na identificação de um endereço associado a um endereço público atrelado a uma PSAV, momento em que a análise On-Chain deve ser paralisada para dar lugar à análise Off-Chain. O fluxo a seguir apresenta os passos que poderão ser transpostos.

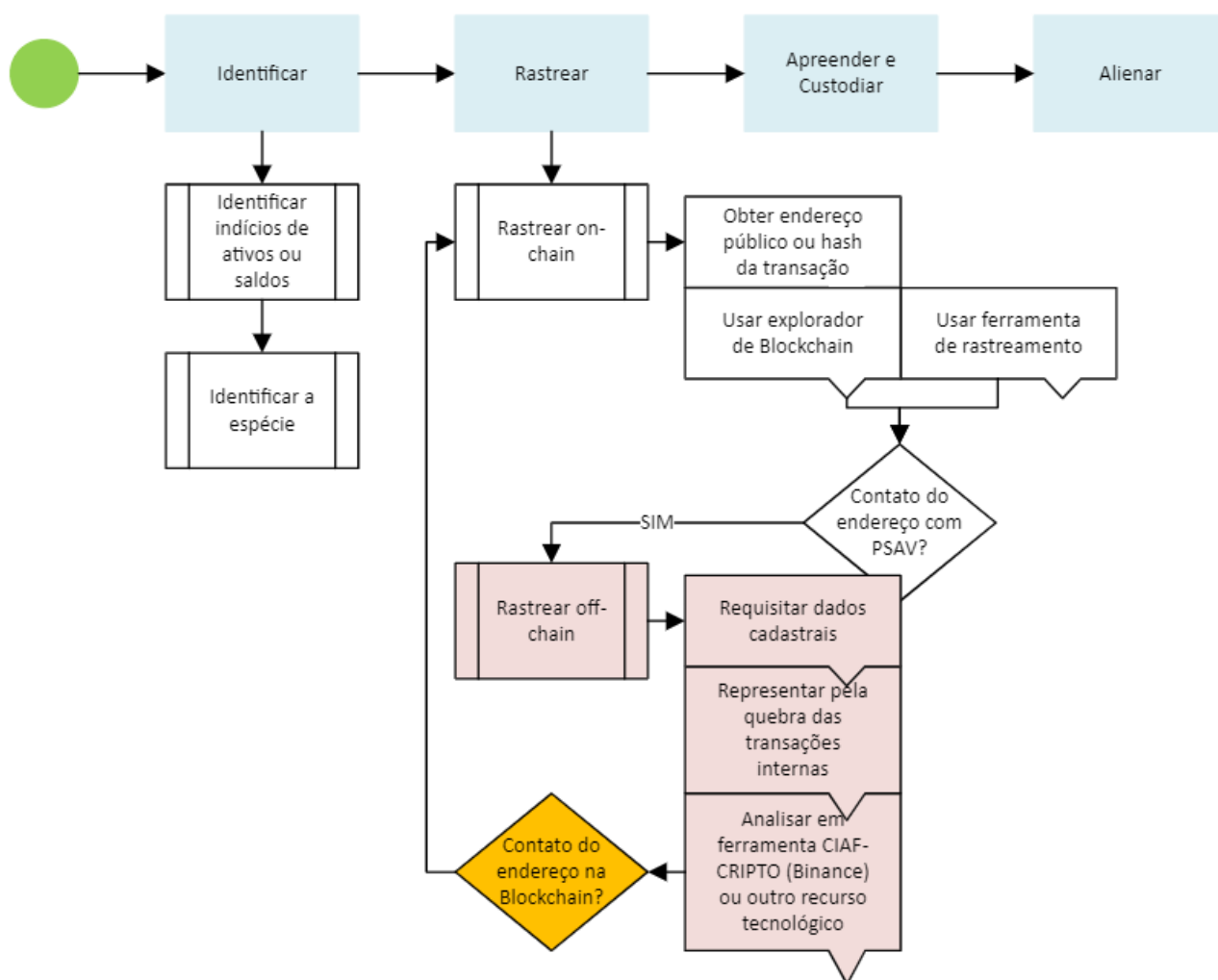
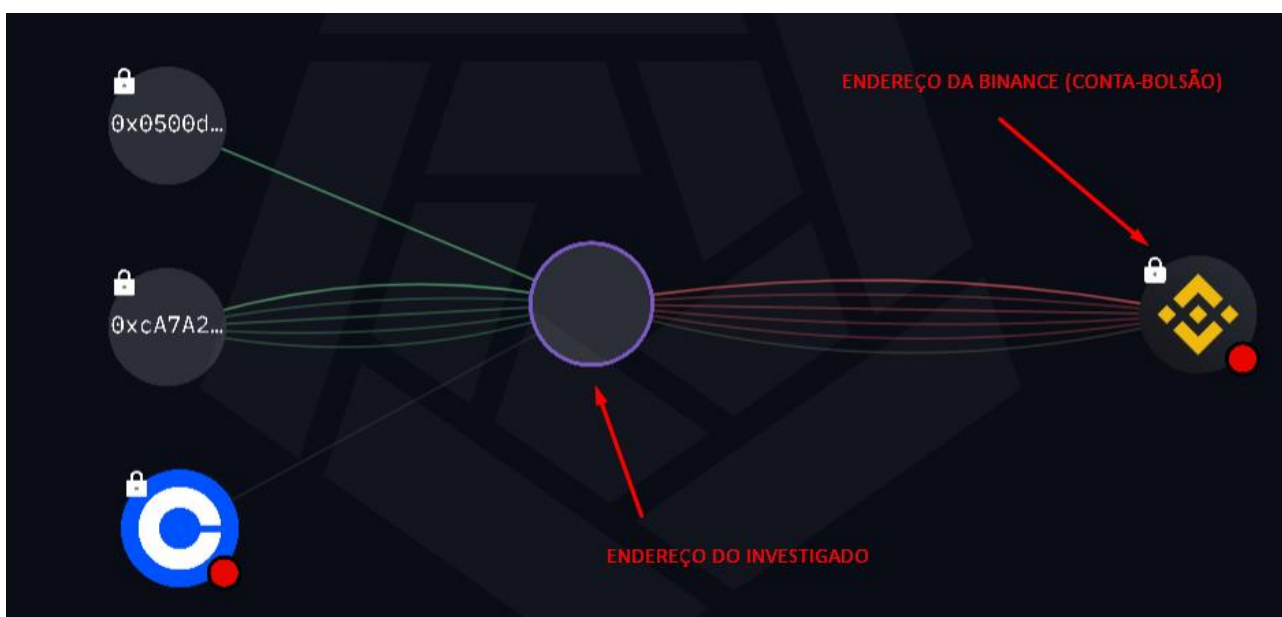


Figura 38-Rastreamento Off-Chain

Frisamos que a partir da identificação de que um determinado endereço está associado a uma conta em uma PSAV, o Rastreamento On-Chain deve ser paralisado e deve-se proceder à análise Off-Chain dos dados da referida conta, sob pena de serem analisadas transações que não condizem com a realidade dos fatos<sup>26</sup>, isso porque o

<sup>26</sup> Tenhamos em mente que quando um usuário envia ativos virtuais para um endereço de depósito em uma PSAV, o ativo não permanece parado nesse endereço. Em vez disso, a PSAV movimenta internamente os fundos conforme necessário, agrupando e misturando-os com os fundos de outros usuários. Por exemplo, muitas PSAVs mantêm parte dos fundos depositados em carteiras frias, desconectadas da internet, por razões de segurança. Trata-se de endereços públicos da PSAV semelhantes a contas-bolsão ou contas-ônibus. Essas movimentações internas realizadas pela PSAV são registradas na blockchain como qualquer outra transação, isto é, as saídas e entradas desse endereço bolsão são registradas, mas não necessariamente dizem respeito ao investigado; muito pelo contrário, dizem respeito a uma infinidade de clientes da PSAV. Portanto, não faz sentido continuar rastreando os fundos depois que eles foram depositados em um serviço, pois o proprietário do endereço de depósito geralmente não é o responsável por

endereço da PSAV na verdade é uma espécie de conta-bolsão ou conta-ônibus a partir do qual ou para o qual são originados ou destinados recursos de inúmeros clientes. Note na figura abaixo que o investigado (endereço central) recebeu recursos dos endereços localizados à esquerda do fluxo. Depois disso, os ativos foram enviados para um endereço da Binance. Neste ponto o investigador deverá parar seu rastreamento On-Chain pelo simples fato de que o endereço Binance é usado pela PSAV para receber e enviar ativos virtuais de/para inúmeros clientes, os quais não necessariamente se relacionam com o investigado.



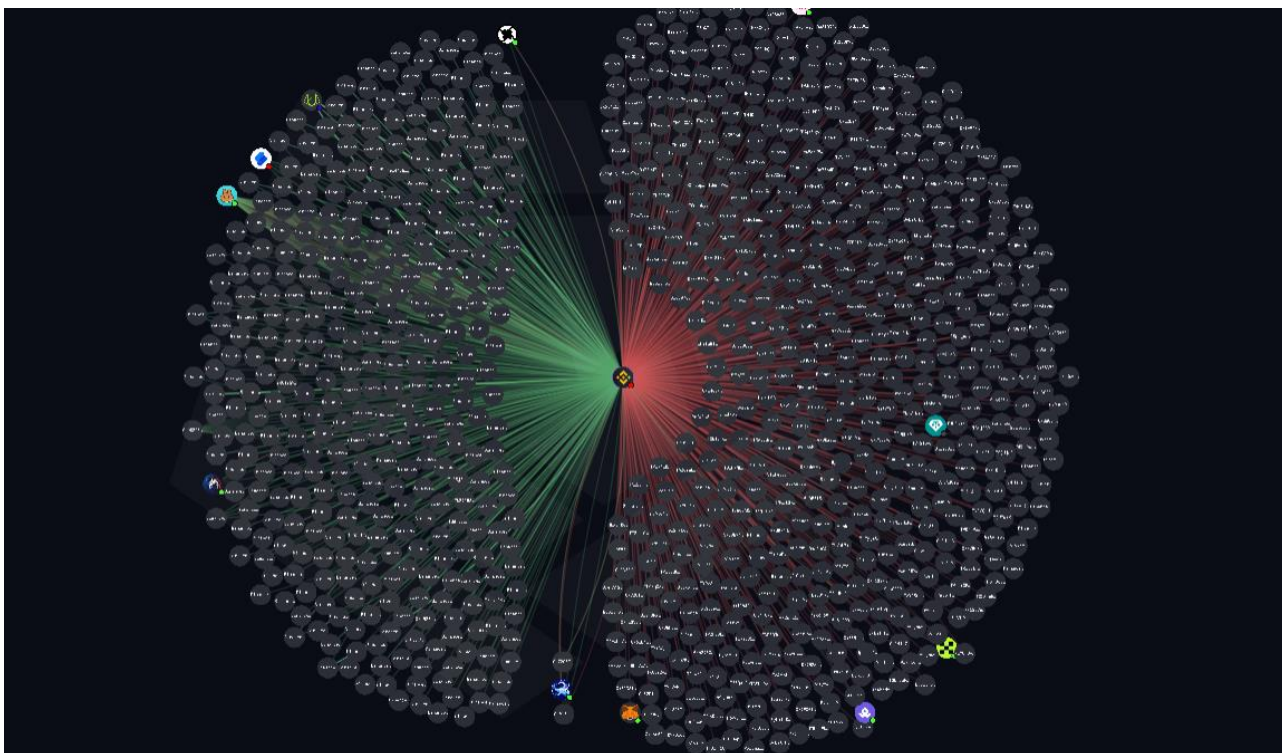
*Figura 39-Indicação de um endereço bolsão da Binance*

Podemos verificar o que estamos por afirmar quando “explodimos” o endereço da Binance na ferramenta de Rastreamento On-Chain. Na figura a seguir podemos verificar o endereço “explodido” com centenas, senão milhares de transações. À esquerda estão os endereços de origem e à direita estão os endereços de destino de ativos.

---

movê-los após esse ponto. Apenas a própria PSAV sabe quais depósitos e saques estão associados, de fato, a clientes específicos, e essas informações são mantidas nos bancos de dados da PSAV, que não são visíveis nas blockchains ou em ferramentas de análise. Para evitar que investigadores sigam erroneamente os fundos depois que eles foram depositados em um serviço, o Rastreamento On-Chain deve ser paralisado quando um endereço associado a um serviço é identificado.





*Figura 40-Endereço da BINANCE "explodido" - não é viável realizar Rastreamento On-Chain nesse tipo de endereço porque não saberíamos apontar quais transações dizem respeito ao investigado, pois somente a PSAV teria como informar o que o investigado fez com os ativos que enviou para esse endereço.*

O Rastreamento Off-Chain é comumente definido como a análise dos dados mantidos pelas PSAVs acerca das operações realizadas por seus clientes através de sua plataforma. Trata-se do cotejamento de informações que não estão registradas na blockchain, mas sim em bancos de dados privados mantidos pelas empresas que prestam o serviço.

Os dados Off-Chain mantidos pelas PSAVs possuem natureza heterogênea. A lista a seguir exemplifica as informações que geralmente podem ser encontradas em posse dessas empresas.

- Dados cadastrais utilizados para o registro conta.
- Saldo em moeda fiduciária e em ativos virtuais mantidos pelo correntista.
- Métodos de pagamentos utilizados.
- Depósitos e saques em moeda fiduciária.
- Depósitos e saques em ativos virtuais.

- Logs de acessos.

Dada a natureza dos dados expostos acima e à forma como a sua guarda é realizada – em bancos de dados privados -, é pacífico que, diferentemente dos dados registrados em blockchain, o acesso a todos eles, com exceção dos dados cadastrais, submetem-se à reserva de jurisdição, devendo a autoridade policial representar pelo afastamento do sigilo dos dados da pessoa investigada antes de acessá-los.

No que se refere à natureza do sigilo cujo afastamento deve ser buscado para garantir a legalidade do acesso aos dados listados acima, entende-se que a quebra de sigilo bancário em conjunto com a quebra do sigilo telemático do investigado seria suficiente. No entanto, a fim de que a investigação possa se desenvolver em um cenário tão seguro quanto possível, recomenda-se que a autoridade policial represente também de forma explícita pelo afastamento do sigilo dos dados mantidos por PSAVs em que o investigado seja correntista, no intuito de se evitar qualquer questionamento futuro acerca da autorização de acesso a dados que possam ter natureza ainda não pacificada entre alguns dos atores envolvidos no processo de persecução penal.

Obtidas as ordens necessárias para o acesso aos dados Off-Chain, a equipe de investigação deve encaminhar as autorizações de afastamento de sigilo e requisitar os dados pertinentes à PSAV através do seu canal de comunicação<sup>27</sup> Law Enforcement, pelo fato de não haver, ainda, sistema destinado à transmissão oficial desses dados entre as PSAVs e as instituições de persecução penal.

A estrutura dos dados que serão disponibilizados pelas PSAVs varia de empresa para empresa. Sendo assim, tem sido observado o envio de dados em formato csv, excel ou mesmo pdf, o que dificulta em demasia o desenvolvimento de ferramentas de análises Off-Chain que possam auxiliar o investigador. Todavia, faz-se menção à ferramenta tecnológica de análise “CIAF CRIPTO”, desenvolvida pela DFIN, que auxilia na interpretação dos dados fornecidos pela Binance (e somente para esta empresa),

---

<sup>27</sup> Algumas PSAVs, no entanto, contrataram a plataforma Kodex, que é um serviço de comunicação centralizado com as PSAVs que aderiram à contratação. Por exemplo, fazem parte desta plataforma as PSAVs: Binance (maior do mundo), Bitbuy, Bitfinex, Bitget, Coinbase, Coinsquare, MoonPay. Significa dizer que para essas PSAVs as ordens judiciais poderão ser encaminhadas pela plataforma Kodex. Para as demais PSAVs as comunicações deverão ser feitas individualmente pelos seus contatos Law Enforcement.

responsável por cerca de 80% do mercado brasileiro. Para a análise dos dados Off-Chain fornecidos pelas demais PSAVs, recomenda-se a utilização de editores de texto, planilhas eletrônicas e ferramentas de Business Intelligence, conforme cada caso.

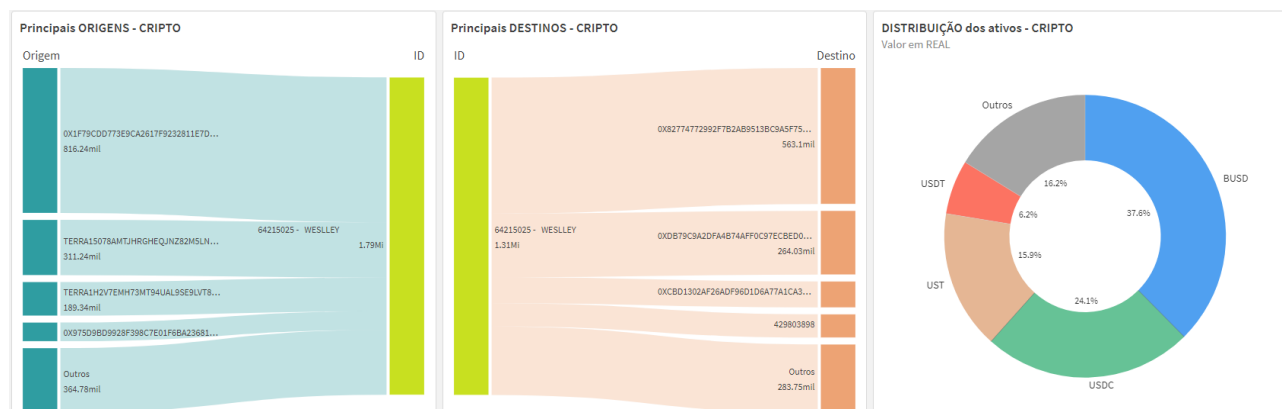


Figura 41-Exemplo de objetos da ferramenta CIAF Cripto que apontam as principais origens e destinos de criptoativos, bem como a distribuição dos ativos transacionados.

O Rastreamento Off-Chain permite ao investigador avaliar, dentre outros aspectos inerentes ao caso concreto:

- A utilização de laranjas, testas de ferros e pessoas interpostas, através da análise dos dados utilizados no cadastro da conta, por exemplo, e-mail e telefone apontados para a execução do duplo fator de autentificação.
- O saldo em moeda fiduciária e em ativos virtuais disponível na conta no momento do envio dos dados.
- Os principais ativos transacionados e blockchains utilizadas pelo investigado.
- A conversão de saldos em moeda fiduciária para ativos virtuais, e vice-versa.
- As transações em moeda fiduciária e em ativos virtuais realizadas com outros correntistas da mesma instituição.
- As transações de ativos virtuais realizadas entre o endereço investigado e endereços de carteiras privadas ou endereços associados a outras PSAVs.

- A identificação dos principais remetentes e destinatários da conta analisada.
- Os dispositivos utilizados para acessar a conta analisada.
- A localização geográfica dos dispositivos utilizados para acessar a conta analisada, no momento do acesso.

Finalmente, cumpre salientar que nem sempre a análise Off-Chain de uma conta em uma PSAV, identificada a partir de uma análise On-Chain que vinha sendo previamente realizada, será o ponto final do rastreamento de ativos virtuais. Determinadas as contas e endereços que figuram como principais remetentes e destinatários em uma análise Off-Chain, tanto para transações em moeda fiduciária quanto para transações em ativos virtuais, pode se mostrar necessário que a equipe policial dê início a novos rastreamentos On-Chain e Off-Chain, a fim de dar continuidade à identificação do caminho percorrido pelos ativos ou das pessoas que tiveram participação nesse processo.

### **5.3. Apreender e Custodiar**

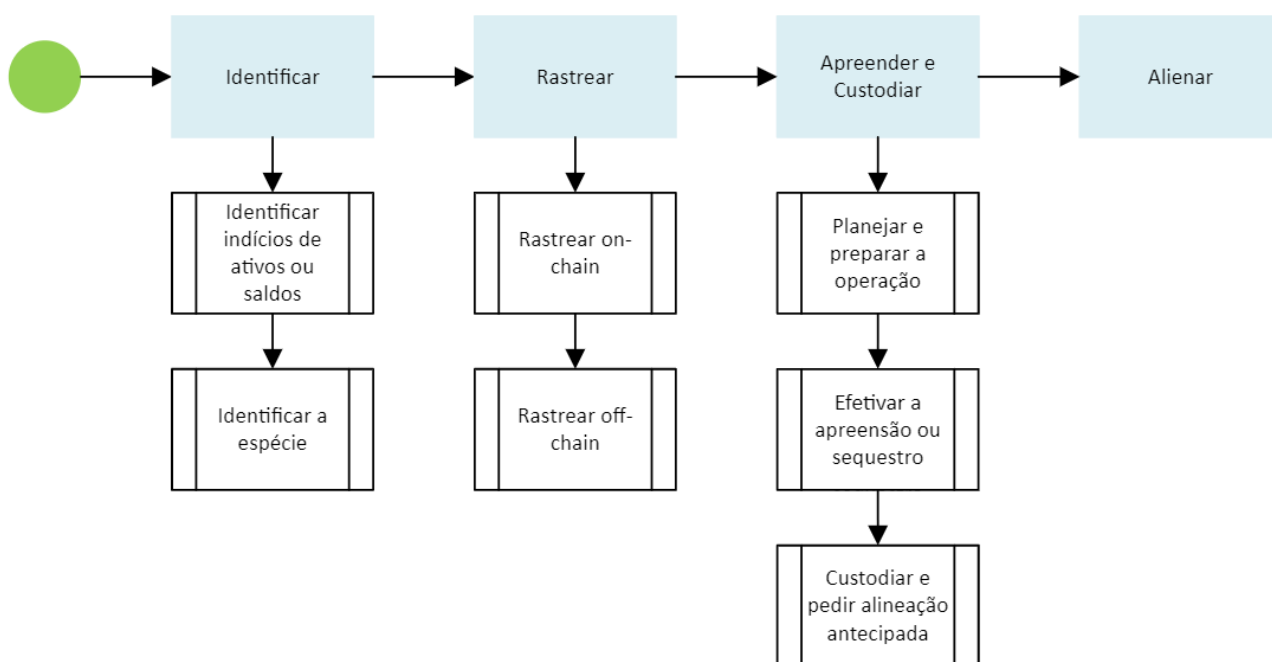
A deflagração de operações policiais que possam envolver a apreensão de ativos virtuais ou saldos representativos demanda a realização de alguns procedimentos prévios, de forma a reduzir os riscos e aumentar a eficácia do processo de recuperação desse tipo de ativo.

Tais preparativos são necessários pelos ainda pouco conhecidos procedimentos a serem realizados com os ativos virtuais ou saldos representativos porventura encontrados em posse dos alvos, mas também em função da portabilidade que é intrínseca a esses bens e que exige da polícia ação intempestiva.

Além disso, fatores diretamente relacionados ao modo de custódia dos ativos virtuais ou de saldos representativos influenciarão na forma como a apreensão deve ser realizada. Como já mencionado, no mundo dos ativos virtuais as carteiras digitais podem ser classificadas em dois tipos principais: carteiras de custódia própria e carteiras de custódia de terceiros. A diferença entre elas está no controle das chaves privadas, que são essenciais para acessar os ativos virtuais na blockchain. Lembrando: uma Carteira de Custódia Própria é aquela em que o usuário tem controle total sobre suas chaves privadas, e, conseqüentemente, sobre seus ativos. Essa carteira pode ser um aplicativo de software, uma carteira de hardware ou até uma carteira de papel. Numa Carteira de Custódia de

Terceiros, a chave privada e o controle dos ativos são gerenciados por uma entidade externa, como uma PSAV. Tal diferenciação é determinante para efeito de apreensão/sequestro porque os procedimentos variam conforme o tipo de carteira.

Diante dessas considerações, recomendamos a adoção do seguinte procedimento para a apreensão de ativos virtuais ou sequestro de saldos representativos. O processo é dividido em três etapas principais: a fase de planejamento, a fase de execução das medidas de apreensão, e a fase de custódia e solicitação de alienação. Cada uma dessas fases será detalhada adiante através de suas subtarefas.



*Figura 42-Tarefas do comando "Apreender e Custodiar"*

### 5.3.1. Planejar e preparar a deflagração da operação

O Planejamento e Preparação envolve a constituição de equipes e indicação de específicas atribuições a determinados policiais capacitados na temática. Envolve também os pedidos judiciais e a criação de uma Carteira Oficial de Custódia para recepção dos ativos virtuais apreendidos. O gráfico a seguir apresenta as subtarefas.

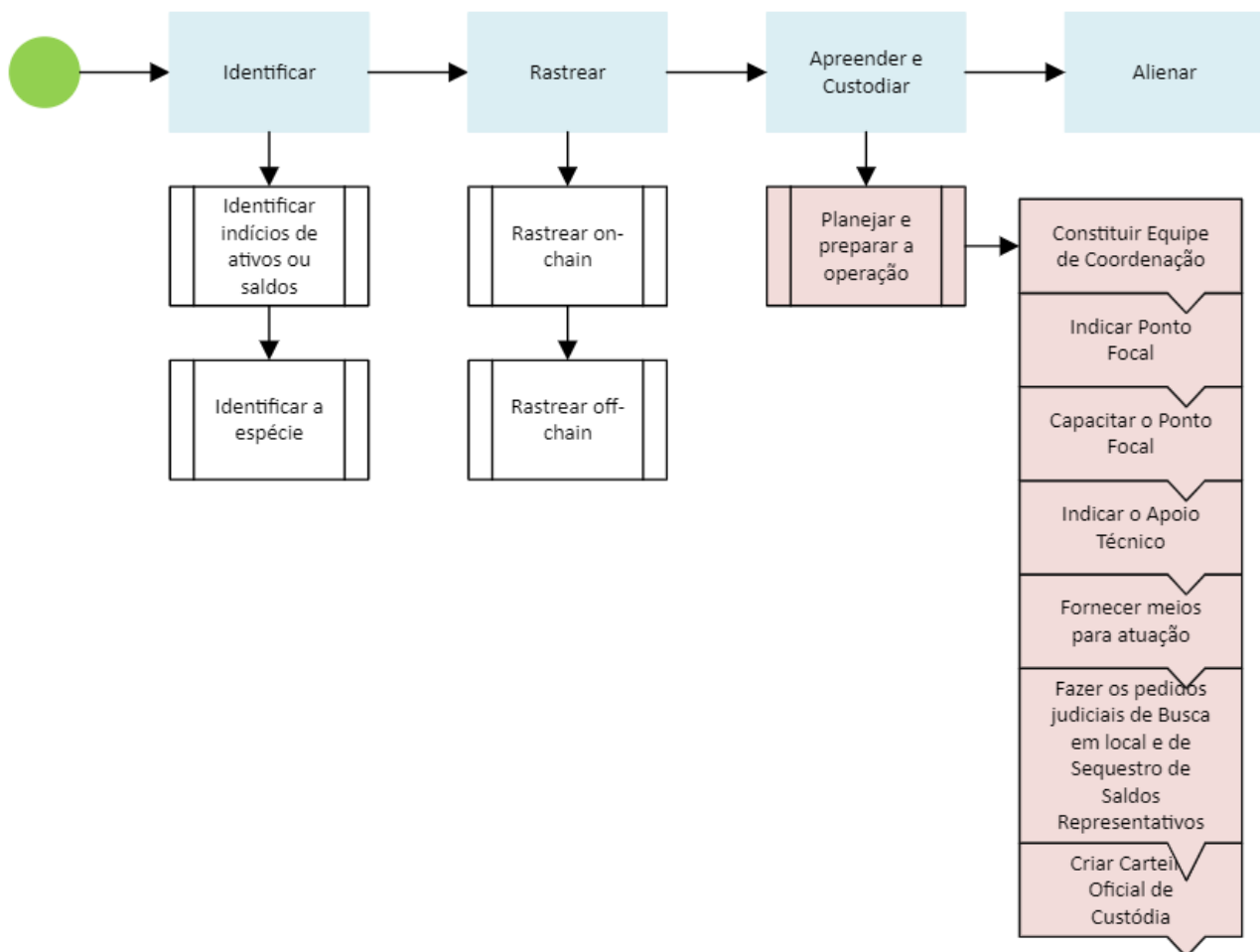


Figura 43-Subtarefas da tarefa "Planejar e Preparar"

#### 5.3.1.1. Constituição da Equipe de Coordenação da Deflagração

Entende-se por Coordenação da Deflagração a equipe composta pelos policiais responsáveis por organizar as diligências de busca e apreensão. Geralmente é constituída pela autoridade policial e pelos policiais que participaram ativamente da investigação.

No que se refere à apreensão de ativos virtuais ou sequestro de saldos representativos, a Coordenação da Deflagração, para além das demais atribuições ordinárias que envolvem uma operação policial, deverá:

- Indicar pontos focais de equipes projetadas de acordo com as necessidades;
- Encontrar meios de capacitar previamente os pontos focais;
- Indicar o Apoio Técnico;

- Fornecer meios para atuação dos pontos focais e Apoio Técnico.

#### **5.3.1.2. Indicação de Ponto Focal**

O Ponto Focal atuará na equipe de busca e apreensão, no ambiente da diligência e deve ser entendido como o/a policial previamente capacitado/a que, por seu maior conhecimento na temática, torna-se referência para os demais integrantes da equipe policial encarregada do cumprimento da medida judicial de busca.

Especialmente no que se refere à busca de elementos referentes a ativos virtuais – Frase Secreta, Chave Privada, Carteiras, Endereços -, a utilização de pontos focais nas equipes é estratégia importante para que nenhum elemento relevante passe despercebido durante as diligências.

É imperativo, portanto, que a equipe de Coordenação da Deflagração da operação policial encontre meios para capacitar policiais para atuarem como pontos focais nas equipes de busca e apreensão, ao menos naquelas equipes relacionadas aos alvos principais, sob a ótica de maior probabilidade de se encontrar ativos virtuais.

O Ponto Focal seria o primeiro filtro para identificação, no próprio local de busca, dos elementos relativos a ativos virtuais e, diante do seu conhecimento prévio, estaria habilitado a orientar os demais componentes da equipe, bem como estabelecer um contato técnico e efetivo com o Apoio Técnico – abordado no tópico subsequente.

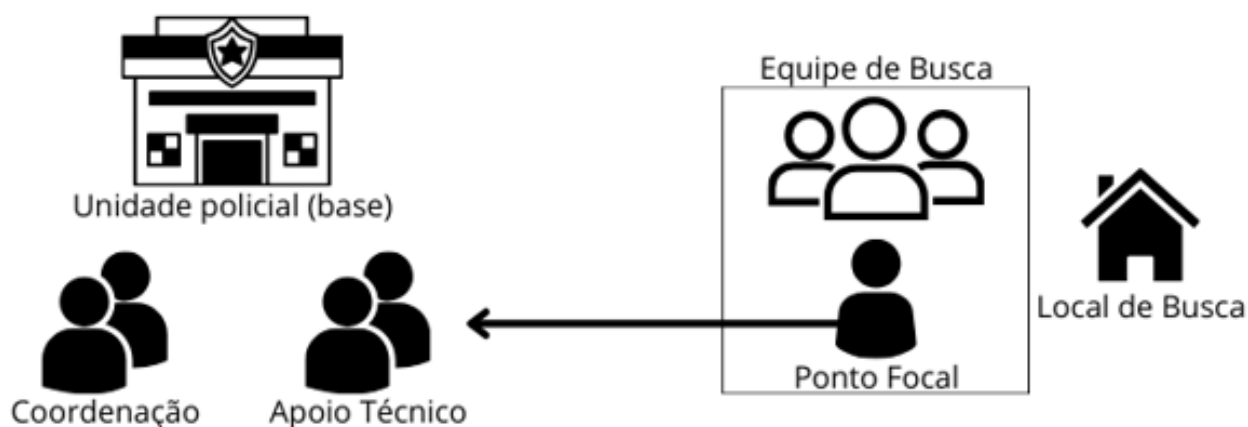
Ratifica-se que a preocupação acerca da utilização dos pontos focais nas equipes projetadas deve-se ao fato de que, tratando-se da apreensão de ativos virtuais, os procedimentos necessários à efetiva recuperação do bem devem ser realizados tão brevemente quanto possível. Caso contrário, abre-se uma janela de oportunidade para que outros membros da organização investigada intervenham e tornem a apreensão desses ativos impossível. Dessa forma, o momento da identificação do elemento no local de busca e a rapidez do tratamento dado a ele são fatores que influenciarão de maneira determinante na eficácia da apreensão.

#### **5.3.1.3. Indicação de Apoio Técnico**

A expressão "Apoio Técnico" refere-se ao policial ou à equipe com maior experiência e capacitação em procedimentos relacionados a ativos virtuais, cuja função é atuar na base da unidade, em conjunto com a equipe de Coordenação da operação. Sua

principal atribuição é fornecer suporte aos Pontos Focais das equipes em campo, garantindo a eficácia das ações projetadas.

Dado que a operação policial em questão poderá abranger vários locais de busca, onde há potencial para se encontrar elementos relacionados a ativos virtuais, entende-se que a equipe de Apoio Técnico seria mais eficaz se permanecesse na base (unidade policial) durante a deflagração. Neste ambiente controlado e livre dos riscos inerentes aos locais de busca, a equipe de Apoio Técnico, equipada com todos os recursos necessários, poderia resolver as dúvidas das equipes em campo e conduzir os procedimentos de apreensão de ativos virtuais, seja realizando-os diretamente, seja orientando remotamente os colegas para executá-los.



*Figura 44-Esquema de divisão das equipes e respectivos locais de atuação*

#### **5.3.1.4. Fornecimento de meios de atuação**

Os meios de atuação abrangem:

- Ambiente de atuação do Apoio Técnico: geralmente o apoio técnico é fornecido pela DFIN;
- Aquisição, sempre que possível, pois altamente recomendável, de hardwallet para efetivar a apreensão;
- Parte do briefing de deflagração explicitada por policial com conhecimento técnico;
- Download prévio e estudo do funcionamento de carteiras pelos Pontos Focais;



- Treinamento prévio com os Pontos Focais com policial técnico: em geral o treinamento prévio é dado por policial da DFIN;
- Contato e alinhamento prévio com as PSAVs que receberão ordens de sequestro de saldos representativos de ativos virtuais: contato prévio pelo canal Law Enforcement.

Especificamente quanto a esta última tarefa, a identificação das PSAVs que são utilizadas pelos investigados deve ser realizada através dos diferentes meios de investigação disponíveis (RIF, quebra de sigilo bancário, quebra de sigilo fiscal, quebra de sigilo telemático etc.) e é parte fundamental do processo de sequestro de saldos representativos, uma vez que não existe, até a data em que este manual foi escrito, banco de dados centralizado que contenha registro de todas as PSAVs onde uma pessoa física ou jurídica possua conta, tal como existe o Cadastro de Clientes do Sistema Financeiro Nacional (CCS) para os relacionamentos bancários.

Não existe também sistema governamental de transmissão das ordens de sequestro proferidas pelo Judiciário, assim como o Sisbajud, de modo que cada ordem, para cada PSAV, deve ser encaminhada manualmente de forma individual.

Algumas PSAVs, no entanto, contrataram a plataforma Kodex, que é um serviço de comunicação centralizado com as PSAVs que aderiram à contratação. Por exemplo, fazem parte desta plataforma as PSAVs: Binance (maior do mundo), Bitbuy, Bitfinex, Bitget, Coinbase, Coinsquare, MoonPay. Significa dizer que para essas PSAVs as ordens judiciais poderão ser encaminhadas pela plataforma Kodex. Para as demais PSAVs as comunicações deverão ser feitas individualmente pelos seus contatos Law Enforcement.

O momento de envio das ordens de sequestro para cada uma das PSAVs deve ser ponderado pela equipe de investigação - se antes ou concomitantemente à deflagração. O envio precoce da ordem de sequestro pode aumentar as chances de um sequestro de ativos mais efetivo, porém, pode também aumentar as chances de o investigado suspeitar a existência de investigação que se desenrola a seu respeito, podendo reduzir a efetividade das buscas que seriam ainda realizadas.

Note-se que as PSAVs necessitam, para fazer as buscas em seus sistemas, de informações cadastrais relacionadas ao investigado. A experiência revela que esses dados abrangem especialmente, em lista não exauriente: Nome, CPF, CNH, Data de

nascimento, Passaporte, endereço eletrônico (email), telefone. Sugere-se, portanto, que seja criada uma tabela conforme modelo abaixo, contendo esses dados, que deverá ser encaminhada junto com a ordem judicial.

Nome	CPF	CNH	Data de nascimento	Passaporte	Email	Telefone
------	-----	-----	--------------------	------------	-------	----------

*Quadro 5-Modelo de tabela a ser encaminhada para a PSAV*

Por fim, chama-se atenção, como dito, para o fato de atualmente cada PSAV possuir um canal de comunicação distinto, às vezes pouco eficiente, às vezes acessado a partir de cadastros prévios, às vezes alterado constantemente etc. Dessa forma, para garantir o sucesso da comunicação com as instituições, sugere-se que previamente à deflagração sejam validados - através das diligências julgadas mais adequadas - os canais de comunicação com cada uma das PSAVs utilizadas pelos alvos. Por exemplo, dias antes o policial poderá transmitir mensagens através do canal encontrado indagando sobre o procedimento que deverá adotar e precavendo a PSAV sobre a ordem futura, sem, contudo, obviamente, revelar dados sobre a investigação.

#### **5.3.1.5. Pedidos Judiciais**

No ambiente de busca, o procedimento de recuperação/acesso a carteiras de ativos virtuais e a apreensão dos ativos a elas “associados” exigirá, na maior parte das vezes, a utilização de elementos – notadamente Frases Secretas (Seed), chaves privadas e logins/senhas - encontradas nos locais de buscas em dispositivos eletrônicos, anotadas em papel ou mesmo fornecidos pelo alvo do mandado. Em alguns desses cenários será necessário, ainda, que o policial execute a transferência de apreensão dos ativos diretamente a partir da carteira utilizada pelo alvo, no próprio dispositivo utilizado pelo alvo.

Dada a especialização referente aos ativos virtuais e ao armazenamento de suas chaves de acesso, recomenda-se a formulação de pedidos específicos na representação pela busca e apreensão, a fim de que as carteiras que armazenam as chaves privadas possam ser acessadas de forma imediata e que as transferências do controle dos ativos para a polícia esteja amparada por autorização judicial.

Desse modo, ao redigir a representação referente a busca e apreensão, sugere-se o pedido de acesso imediato ao conteúdo das mídias eletrônicas, dispositivos físicos de armazenamento de chaves de ativos virtuais (coldwallets, hardware wallets ou carteira

frias) arrecadados e/ou apreendidos no endereço da diligência, especialmente em relação aos smartphones e a nuvem relacionada a serviços vinculados aos celulares apreendidos.

Recomenda-se que a autoridade policial represente para que conste expressamente na decisão judicial de busca e apreensão, além de outros aspectos julgados necessários ao caso concreto, pelo menos as seguintes autorizações, visando a total segurança jurídica dos policiais e da investigação quanto à realização dos procedimentos de apreensão de ativos virtuais.

- Autorização de acesso aos dispositivos eletrônicos e seu conteúdo, inclusive àqueles dados mantidos em nuvem.
- Autorização de acesso às carteiras de ativos virtuais mantidas em celulares, em computadores, em hardwallets, em papel, em Prestadoras de Serviços de Ativos Virtuais entre outros formatos, inclusive através da utilização de PINs, senhas, SEEDs, chaves privadas entre outros elementos encontrados no local de busca ou fornecidos pelo alvo do mandado.
- Autorização para que a Polícia Federal possa realizar a efetiva transferência dos ativos virtuais das carteiras do alvo para uma carteira de custódia oficial sob controle da Polícia Federal.

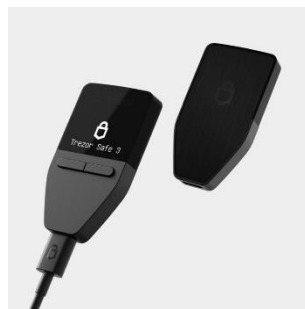
#### **5.3.1.6. Criação de Carteira Oficial de Custódia**

Para fazer a custódia dos ativos virtuais que vierem a ser efetivamente transferidos de carteiras dos alvos dos mandados de busca e apreensão, a equipe de Coordenação, já mencionada, deverá previamente providenciar a criação de uma carteira de ativos virtuais, denominada Carteira Oficial de Custódia.

Para servir como dispositivo suporte à Carteira Oficial de Custódia, recomenda-se a utilização de uma hardwallet, em face dos avançados recursos de segurança oferecidos por esse tipo de dispositivo. Dentre os principais modelos de hardwallet disponíveis no mercado, destaca-se e recomenda-se a utilização de modelos da marca Ledger, já consolidada no mercado pelos requisitos de segurança apresentados e quantidade de blockchains e ativos virtuais suportados.



*Figura 45-Ledger Wallet (Hardwallet)*



*Figura 46-Trezor Wallet (Hadwallet)*

Ressalta-se que, na impossibilidade de se adquirir uma hardwallet, é possível a utilização de um aparelho celular ou computador para a criação da Carteira Oficial de Custódia, através da instalação de um software de carteira (Soft Wallet).

No atual momento, a Trust Wallet, Metamask, Exodus, e Electrum, por exemplo, são aplicações de carteiras tidas como confiáveis pela comunidade, podendo ser utilizadas para a criação da Carteira Oficial de Custódia, se suas características técnicas forem adequadas ao caso concreto. Todavia, recomenda-se fortemente que a equipe de Coordenação, por ocasião da criação da Carteira Oficial de Custódia, mantenha contato com a Divisão de Repressão aos Crimes Financeiros (DFIN) para se certificar previamente qual aplicação usar, pois esta unidade estará atualizada e alinhada com as melhores práticas adotadas, considerando possíveis vulnerabilidades supervenientes de alguma das aplicações.

Deve-se atentar, pelo menos, para os seguintes aspectos antes da criação da Carteira Oficial de Custódia:

- Jamais crie uma carteira do tipo Paper Wallet, considerando que existem sites de criação de carteiras desse tipo na internet que em realidade buscam fornecer uma carteira e depois subtrair os ativos porventura transferidos para ela;

- O dispositivo/aplicativo utilizado para a criação da Carteira Oficial de Custódia deve ser confiável (hardwallet adquirida em meio oficial, celular retornado às configurações de fábrica livre de malwares, software de carteira validado pela comunidade etc.);
- A Carteira Oficial de Custódia deve oferecer suporte aos ativos com maior chance de serem apreendidos;
- O procedimento de criação da Carteira Oficial de Custódia deve ser circunstanciado em documento que especifique os policiais envolvidos, bem como outros elementos julgados importantes como, por exemplo, lacres utilizados para guardar a SEED, lacres utilizados para guardar o PIN/senha, local onde será guardado os envelopes lacrados, chaves públicas etc.

### **5.3.2. Apreensão de Ativos Virtuais**

A apreensão de ativos virtuais ou sequestro de saldos representativos pode ocorrer em dois diferentes cenários, a depender do tipo de custódia praticada pelos alvos e dos elementos que venham a ser encontrados pelas equipes projetadas durante a deflagração. Relembremos que os ativos virtuais ou saldos representativos podem estar custodiados ou por terceiros (Custódia de Terceiros), sob a segurança das PSAVs, ou pelo próprio dono (Custódia Própria) e, estando com o dono, podemos obter ou não elementos que facilitem o acesso à carteira, tal como uma Frase Secreta (Seed). Para cada uma dessas situações existe um procedimento específico a cumprir, os quais, arbitrariamente, nomeamos de Fluxos 1, 2 e 3, conforme apresentado na figura abaixo.

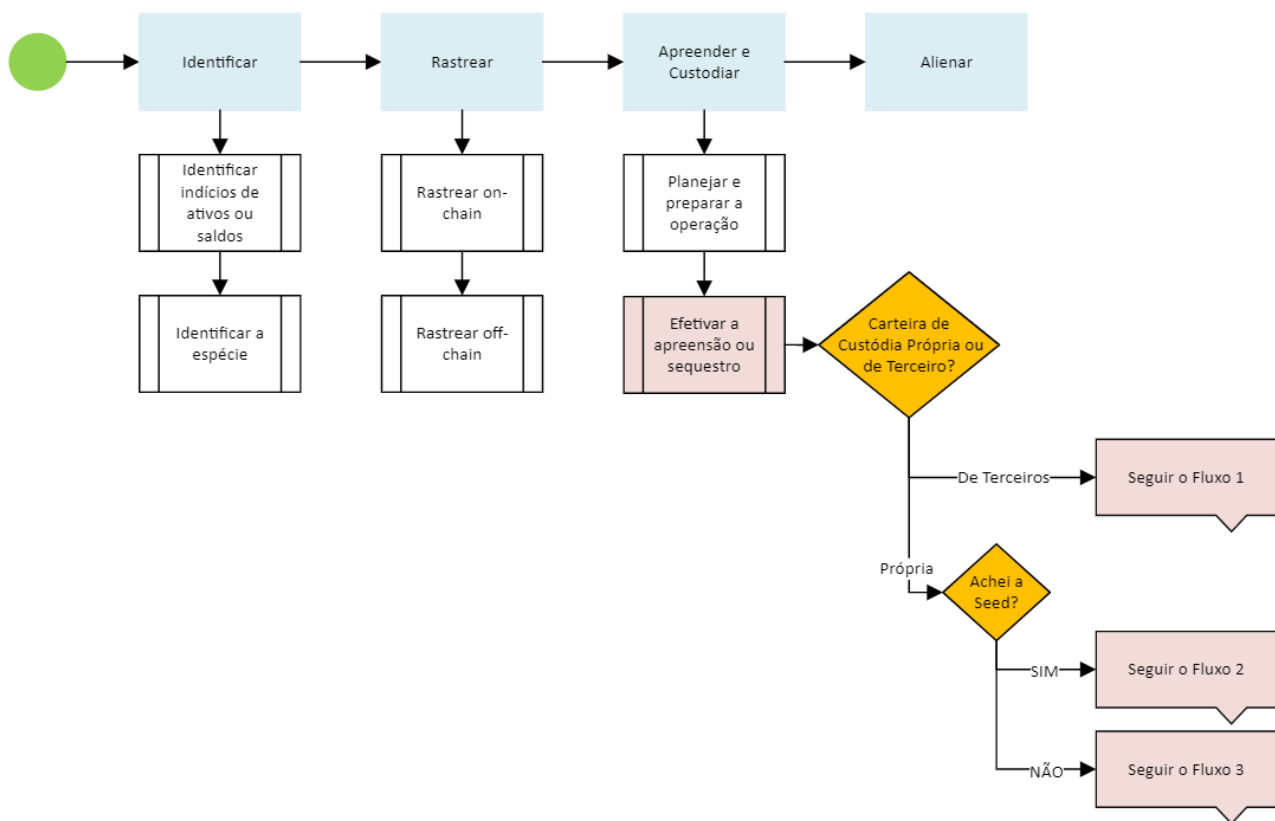


Figura 47-Subtarefas da efetivação da apreensão

#### 5.3.2.1. Sequestro de Saldos Representativos de Ativos Virtuais sob Custódia de Terceiros (Fluxo 1)

No que se refere aos saldos representativos de ativos virtuais custodiados por terceiros (Custódia de Terceiros - mantidos pelos alvos em PSAVs), o sequestro deve ser efetivado por meio de encaminhamento da ordem judicial e consequente bloqueio/congelamento da conta do usuário na PSAV.

Este é o meio menos difícil de persecução patrimonial porque, em linhas gerais, basta encaminhar a ordem judicial de sequestro para que a PSAV cumpra. Todavia, esse procedimento pode se tornar extremamente complicado porque devemos considerar que existem PSAVs estrangeiras que só cumprem ordens do Judiciário brasileiro mediante Cooperação Internacional (MLAT). Para além disso, é plausível considerar que nem mesmo este canal possa ser eficaz para PSAVs hostis, sediadas em jurisdições pouco colaborativas.

Especial atenção, portanto, deve ser dada às PSAVs que não cumprirão imediatamente as determinações do Poder Judiciário brasileiro, seja pela jurisdição onde

se encontram (situação em que podem exigir MLAT<sup>28</sup>), seja pela própria natureza de operação da empresa (no caso de uma empresa criada especificamente para impedir a atuação estatal).

No primeiro caso, a equipe de investigação deve considerar o custo-benefício de fazer o procedimento MLAT, sem, contudo, deixar de lado a possibilidade de apreensão na diligência de busca pelo acesso direto à carteira por meio de aplicação de internet.

No segundo caso, na situação em que a PSAV é hostil ao ponto de nem mesmo cumprir por MLAT, restaria às equipes projetadas diligenciar para conseguir acesso às contas dos alvos nessas instituições a partir da obtenção de Frases Secretas (Seed), de logins, senha, isto é, tentar apreender na diligência de busca por meio de acesso à carteira (procedimento que será discutido no próximo tópico), e uma vez obtido o acesso à conta do alvo, os ativos poderiam ser transferidos para a Carteira Oficial de Custódia.

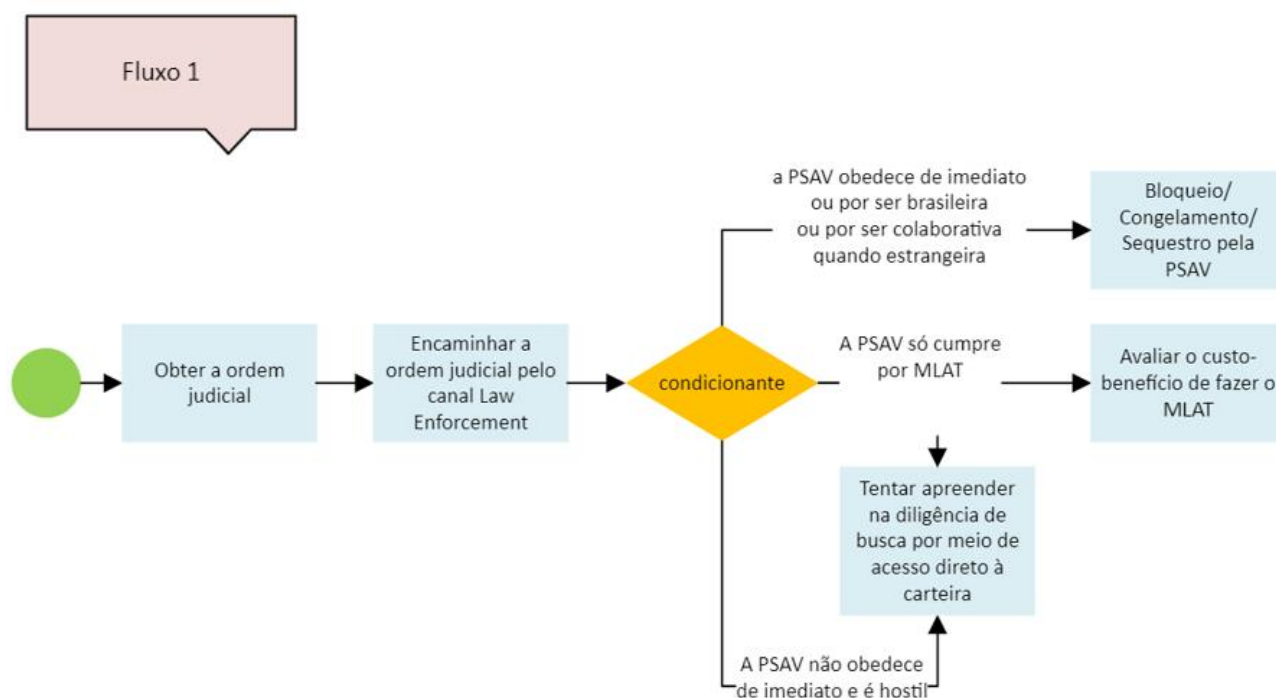


Figura 48-Fluxo para sequestro de saldos representativos junto a PSAVs

### 5.3.2.2. Apreensão de Ativos Virtuais sob Custódia Própria (Fluxos 2 e 3)

<sup>28</sup> Mutual Legal Assistance Treaties - MLAT

Quando se tratar de ativos mantidos pelos alvos em carteiras de Custódia Própria, por outro lado, são diferentes as abordagens necessárias à apreensão. Nesse caso, o cenário se subdivide em dois, a saber:

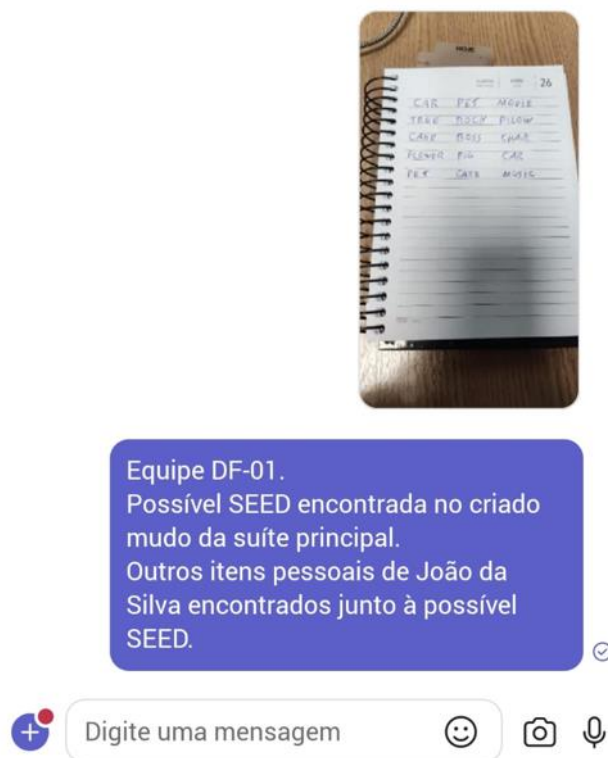
- Ativos virtuais custodiados em carteiras cuja Frase Secreta (Seed)/chave privada foi localizada.
- Ativos virtuais custodiados em carteiras cuja Frase Secreta (Seed)/chave privada não foi localizada.

Deve-se ter em mente que existe hierarquia de importância quanto aos elementos a serem buscados. Com efeito, encontrar uma Frase Secreta (Seed) em local de busca permitirá acesso total e irrestrito aos ativos associados à carteira à qual ela pertence. A Chave Privada dará acesso ao endereço público vinculado. O PIN com login para uma aplicação da internet poderá fornecer acesso à carteira e, por fim, não encontrando qualquer um desses elementos, mas encontrando um endereço público, poderemos associá-lo ao investigado.

No que se refere à apreensão de ativos virtuais em carteiras de custódia própria cuja Frase Secreta (Seed)/Chave privada foi identificada/encontrada leva-se em conta que a utilização da Frase Secreta (Seed) ou da Chave Privada para a recuperação dos ativos do alvo pode ser realizada de qualquer lugar, não se exigindo que esse procedimento seja feito no local de busca onde o elemento foi encontrado. Dessa forma, considera-se mais seguro e eficaz que esse elemento seja enviado para a equipe de Apoio Técnico, já mencionada, lotada na base, através da plataforma Teams, para que esta equipe realize os protocolos adequados em zona segura e tecnicamente dotada de todos os meios necessários.

Recomenda-se ainda que sejam explicitadas, na mensagem de envio do elemento encontrado no local de buscas, circunstâncias acerca da sua localização (cômodo onde foi encontrado, proprietário etc.), tal como exemplificado na figura abaixo.





*Figura 49-Exemplo de envio de SEED para a equipe de Apoio Técnico.*

No que se refere ao auto de arrecadação confeccionado no local de busca, chama-se atenção para o fato de não dever ser nele registradas todas as palavras da possível Frase Secreta (Seed) encontrada, o que a tornaria vulnerável, uma vez que esse é um documento que será inserido nos autos da investigação e acabará chegando ao conhecimento de pessoas diversas. Lembramos: a Frase Secreta (Seed) permite a abertura da carteira e acesso a todas as contas.

Ainda no local de busca, antes do envio do elemento encontrado para a equipe de Apoio Técnico lotada na base, recomenda-se que o Ponto Focal da equipe seja consultado, a fim de se estabelecer um primeiro filtro acerca do que é ou não um elemento indicativo de posse de ativos virtuais. Também, recomenda-se que o chefe de equipe seja comunicado do envio a ser realizado, no intuito de deixá-lo ciente acerca da possível apreensão de ativos virtuais a ser feita.

Na base, a equipe de Apoio Técnico estará a postos para proceder à recuperação da carteira e executar a apreensão dos ativos para a Carteira Oficial de Custódia, a partir da Frase Secreta (Seed)/chave privada encontrada.

A imagem a seguir busca ilustrar o fluxo que poderia ser seguido na apreensão de ativos virtuais a partir de Frases Secretas e Chaves Privadas identificadas em locais de buscas.

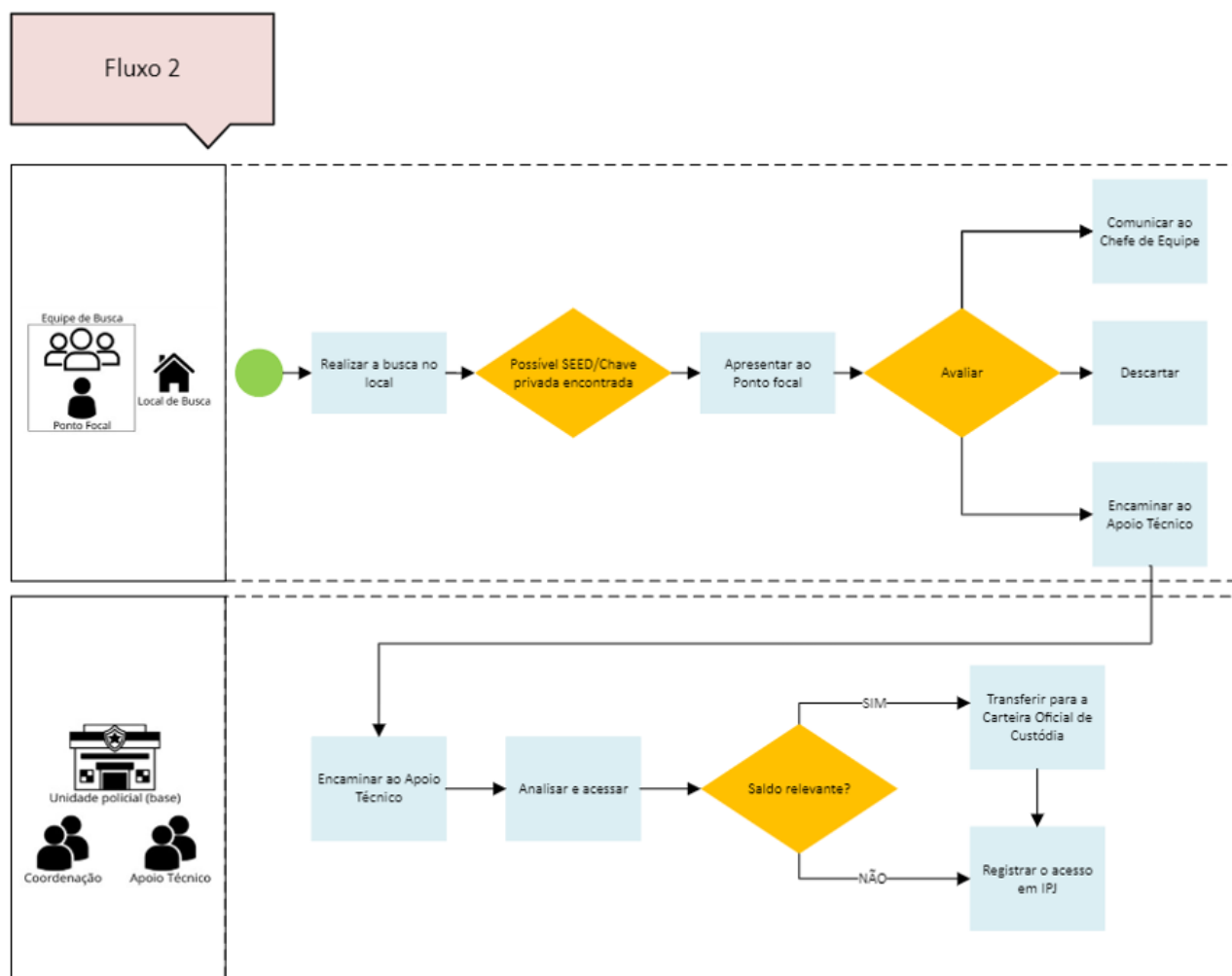


Figura 50-Fluxo de apreensão de ativos virtuais a partir do encontro de SEED/Chave privada no local de busca.

No que se refere à forma de arrecadação física do elemento encontrado, chama-se mais uma vez atenção para a criticidade que envolve a Frase Secreta e a Chave Privada. Esses tipos de itens não devem ser arrecadados de forma que fiquem visíveis para qualquer pessoa, por exemplo, em sacos plásticos transparentes. A utilização de envelopes pardos e quaisquer outros meios de proteção, como a simples dobra da folha de papel onde a possível Seed está anotada, contribui para a segurança dos ativos e da equipe policial responsável pelo cumprimento do mandado judicial.

O processo de recuperação de uma carteira de ativos virtuais a partir de uma Frase Secreta (Seed) pode ser genericamente descrito através dos passos listados a seguir:

1. Eleger o meio capaz de realizar o procedimento de restauração da carteira: i) adquirir e configurar uma hardwallet se optar por este meio ii) baixar, instalar e configurar o software de computador se optar por este meio; iii) baixar, instalar e configurar a aplicação de celular se optar por este meio.
2. Selecionar a opção “Restaurar Carteira”: na interface da carteira escolhida no passo de número 1, provavelmente haverá uma opção similar a “Restaurar Carteira” ou “Frase Secreta”. Vejamos três exemplos nas aplicações Exodus, Green Wallet e Trust Wallet.

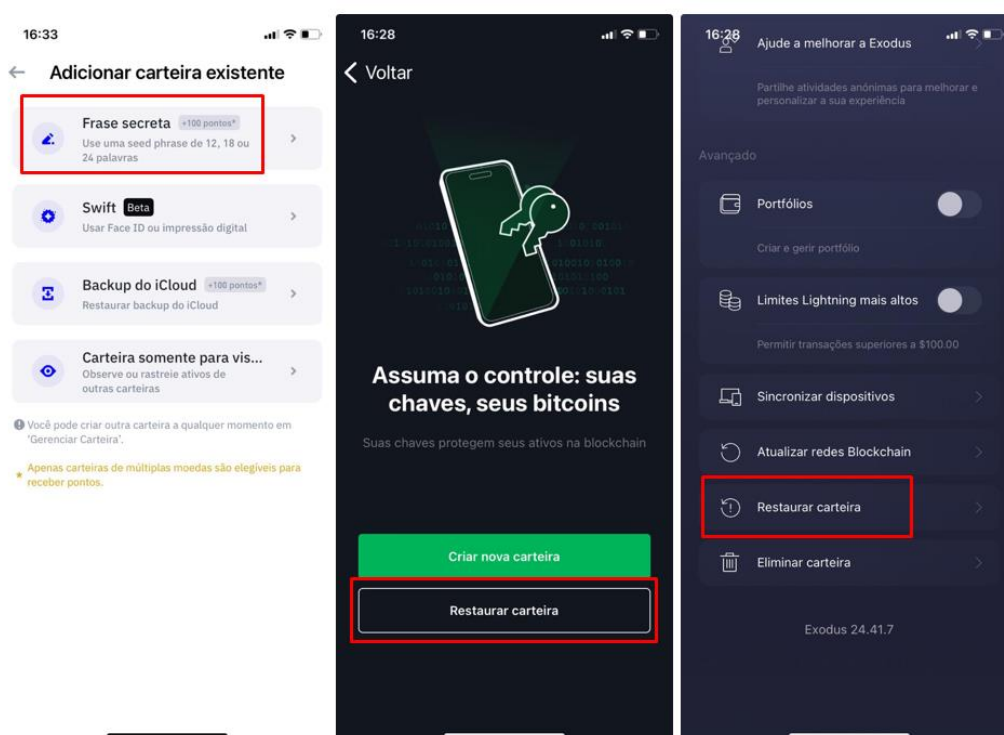


Figura 51-Exemplos de opções de restauração de carteiras a partir de uma SEED nas aplicações, da esquerda para a direita: Trust Wallet, Green Wallet e Exodus.

3. Inserir a Frase Secreta: selecionada a opção de recuperação de carteira mencionada no passo 2, deverá ser apresentado ao usuário uma interface para inserção das palavras que compõem a Frase Secreta a ser recuperada. Como sabido, a Frase Secreta é composta

por sequências ilógicas de 12, 18 ou 24 palavras do idioma inglês dentre 2048<sup>29</sup> palavras fixas.

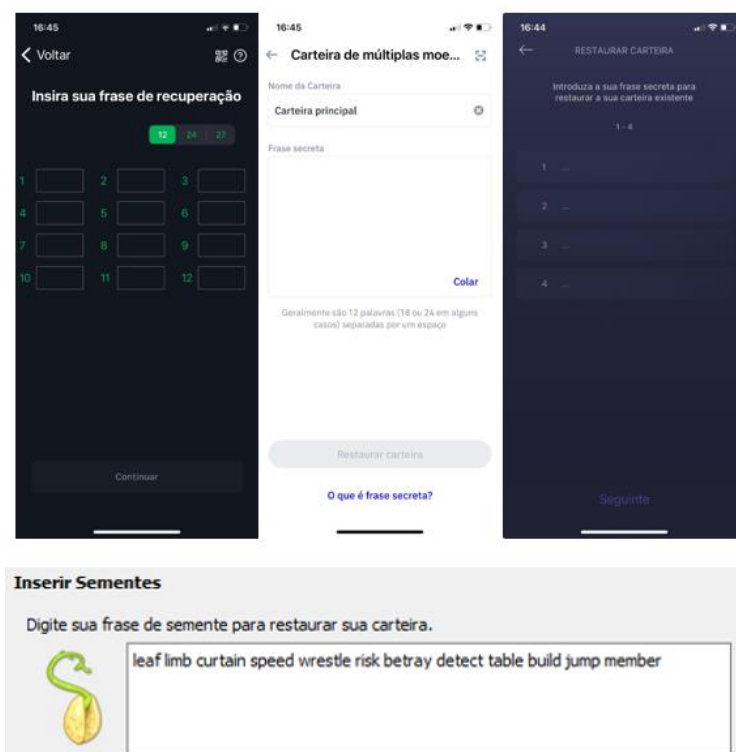


Figura 52-Exemplos de campos destinados à inserção das palavras da Frase Secreta nas aplicações, da esquerda para a direita: Green Wallet, Trust Wallet, Exodus e Electrum

4. Configuração de senha/PIN: algumas carteiras, em meio ao processo de recuperação, obrigam o usuário a configurar uma senha ou PIN que será utilizada para autorizar transações ou desbloquear o acesso à carteira localmente.
5. Acesso restaurado: a carteira escolhida para recuperação derivará as chaves públicas e privadas a partir da Frase Secreta inserida e sincronizará com as blockchains as transações já realizadas, saldos e tokens associados. Após a sincronização, o usuário terá acesso completo à carteira originalmente associada à Frase Secreta utilizada para recuperação.

---

<sup>29</sup> A lista das 2048 palavras pode ser encontrada em <https://www.bitcoinsafety.com/blogs/bitcoin/seed-phrase-list>. Acesso em 18/10/2024.

Nos passos descritos acima, quando o elemento encontrado for uma chave privada, ao invés de uma Frase Secreta, a opção a ser utilizada para recuperação do ativo assemelha-se, geralmente, a “Importar chave privada”.

Especial atenção merece ser dada ao passo de número 1 da lista apresentada anteriormente, uma vez que a escolha da carteira a ser utilizada para recuperar a Frase Secreta pode determinar o sucesso ou insucesso do procedimento.

A maioria das carteiras modernas usa um padrão chamado de BIP-39 para gerar Frases Secretas, o que permite que elas sejam compatíveis entre si. No entanto, existem carteiras que podem utilizar outros padrões ou formatos de geração da Frase Secreta e derivação das chaves públicas e privadas. Portanto, é crucial garantir que a carteira escolhida para ser restaurada a partir de uma Frase Secreta seja compatível com o padrão da Frase Secreta no momento da sua geração.

A busca por essa garantia de compatibilidade poderia ser facilitada pela utilização de alguns softwares de análises de Frases Secretas. Porém, o uso desse tipo de solução ainda não é incentivado devido ao fato de, até o momento em que este manual foi escrito, não ter sido ainda avaliada nenhuma das soluções disponíveis quanto à segurança dos dados nelas inseridos. Dessa forma, recomenda-se que se busque pela identificação da carteira utilizada na geração da Frase Secreta (verificando-se nos dispositivos do investigado os softwares de carteiras instalados, por exemplo), ou mesmo que se realize a recuperação da referida Frase Secreta em diferentes carteiras, dentre as mais populares do mercado, cobrindo assim diferentes cenários de recuperação complementares entre si.

Se no local de busca forem identificadas carteiras de Custódia Própria de posse dos alvos, porém não sejam encontradas suas respectivas Frases Secretas ou Chaves Privadas, a apreensão não poderá ser feita de forma remota pela equipe de Apoio Técnico na base, e deverá ser, por consequência, realizada no próprio local de busca pelo Ponto Focal com apoio dos demais integrantes da equipe.

Nessas circunstâncias, para acessar os ativos da carteira identificada, a equipe projetada deverá diligenciar para conseguir o PIN/senha que a desbloqueia. Com a carteira desbloqueada, o Ponto Focal da equipe de busca deverá realizar as apreensões julgadas pertinentes pela equipe de investigação, realizando as transferências dos ativos para a Carteira Oficial de Custódia criada previamente pela equipe de Coordenação.

O procedimento de apreensão realizado no local de busca poderá contar com a orientação da equipe de Apoio Técnico, inclusive através de chamadas realizadas por meio da plataforma Teams.

A imagem a seguir busca ilustrar o fluxo que poderia ser seguido na apreensão de ativos virtuais associados a carteiras cujas Frase Secretas (Frase Secreta)/chaves privadas não foram identificadas ou encontradas.

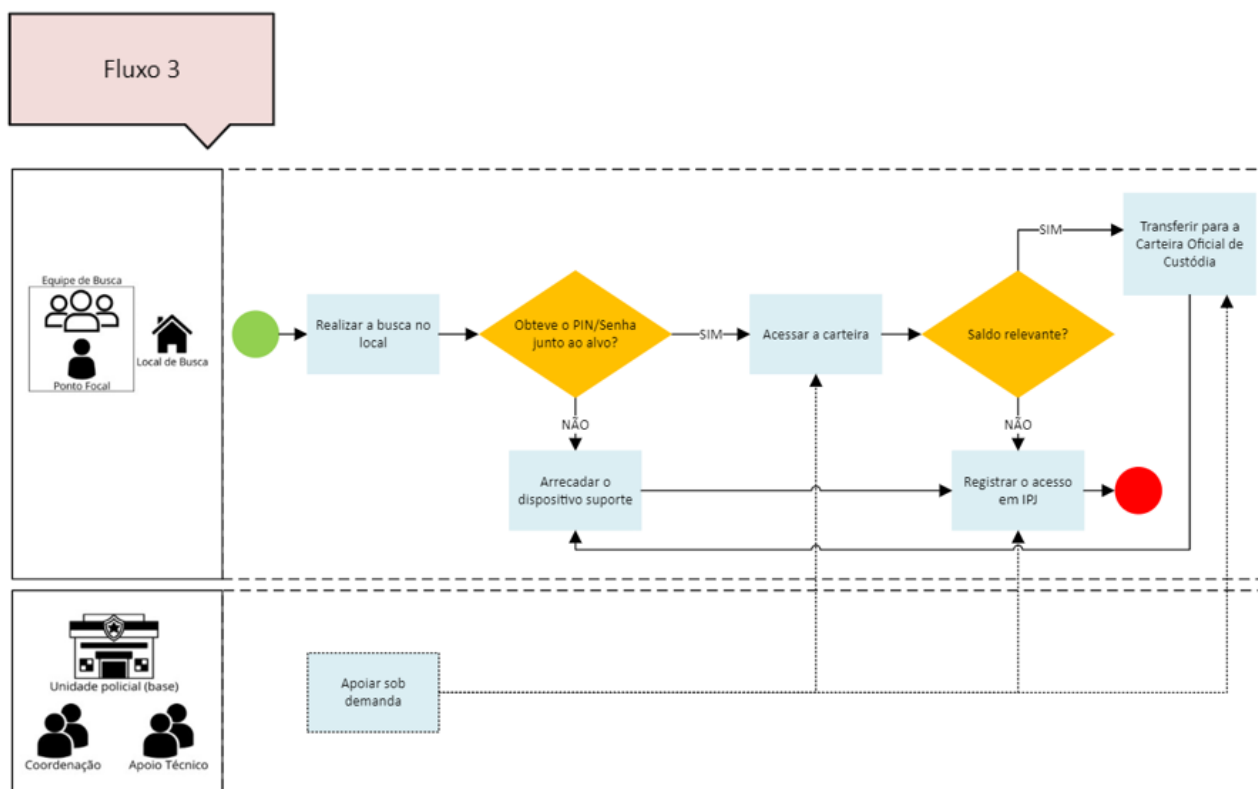


Figura 53-Fluxo de apreensão de ativos virtuais a partir de carteiras de custódia própria identificadas no local de busca, quando as respectivas Frase Secreta e chaves privadas não forem encontradas.

Por fim, chama-se atenção para o fato de que, se a Frase Secreta/chave privada não tiver sido localizada pela equipe de busca ou se localizada, o PIN/senha não tiver sido identificado, não será possível acessar os ativos e consequentemente não será possível realizar as transferências de apreensão. Apesar disso, a arrecadação do dispositivo onde a carteira estava configurada pode se mostrar útil: se o alvo, por qualquer motivo que seja, tiver perdido acesso à Frase Secreta da carteira cujo dispositivo foi arrecadado, consequentemente ele também não poderá movimentar os ativos a ela associados.

### 5.3.2.3. Transferências de Apreensão

No que se refere às efetivas transferências dos ativos virtuais da carteira do alvo para a Carteira Oficial de Custódia, realizada por um servidor policial, boas práticas podem ser estabelecidas no intuito de se reduzir a possibilidade de ocorrência de erros humanos que resultem na dilapidação dos ativos virtuais a serem apreendidos.

- Em nenhuma hipótese deve ser considerada a possibilidade de se digitar o endereço de destino da transferência de apreensão. Deve-se, em todo e qualquer caso, utilizar o recurso copiar/colar ou o escaneamento de QR Codes gerados por meio de softwares confiáveis e difundidos pela equipe de Coordenação. A utilização de um endereço de destino incorreto pode acarretar a perda definitiva dos ativos.
- Antes de se transferir todos os ativos virtuais da carteira do alvo, especialmente nos casos em que se esteja lidando com ativos de valor substancial, recomenda-se a realização de uma transferência de homologação, de valor reduzido, no intuito de garantir a conformidade do endereço de destino e dos procedimentos adotados para a transação de apreensão. O procedimento de transferência de homologação é recomendado inclusive para as apreensões realizadas na base, pela equipe de Apoio Técnico. Após a verificação da conformidade da transferência “de teste”, o envio da totalidade dos recursos a serem apreendidos para a Carteira Oficial de Custódia pode ser executado.
- Como já fora abordado neste manual, o procedimento de transação de ativos virtuais tem como característica o pagamento de uma taxa. A depender da carteira que esteja sendo utilizada, a definição dessa taxa pode ser de livre escolha do usuário, baseada em valores pré-definidos entre outros formatos. Fato é que o policial responsável pela apreensão deve sempre ter a preocupação de ponderar a taxa que está sendo empregada na transação, a fim de se evitar que transferências com taxas exorbitantes sejam realizadas, o que implicaria na dilapidação dos ativos a serem efetivamente apreendidos.

Em acréscimo, seja pela dificuldade em se registrar o hash da transação no auto de arrecadação ou pelo fato de a transação de apreensão ter sido realizada na base, pela equipe de Apoio Técnico, considera-se que a melhor forma de registrar o procedimento

de apreensão de ativos virtuais seja a confecção de uma Informação de Polícia Judiciária (IPJ) destinada especificamente a circunstanciar a forma como se obteve o acesso aos ativos do alvo e como foram feitos os procedimentos de apreensão.

Para tanto, considera-se que o policial responsável pelo procedimento deve registrar em IPJ, no mínimo, as seguintes informações.

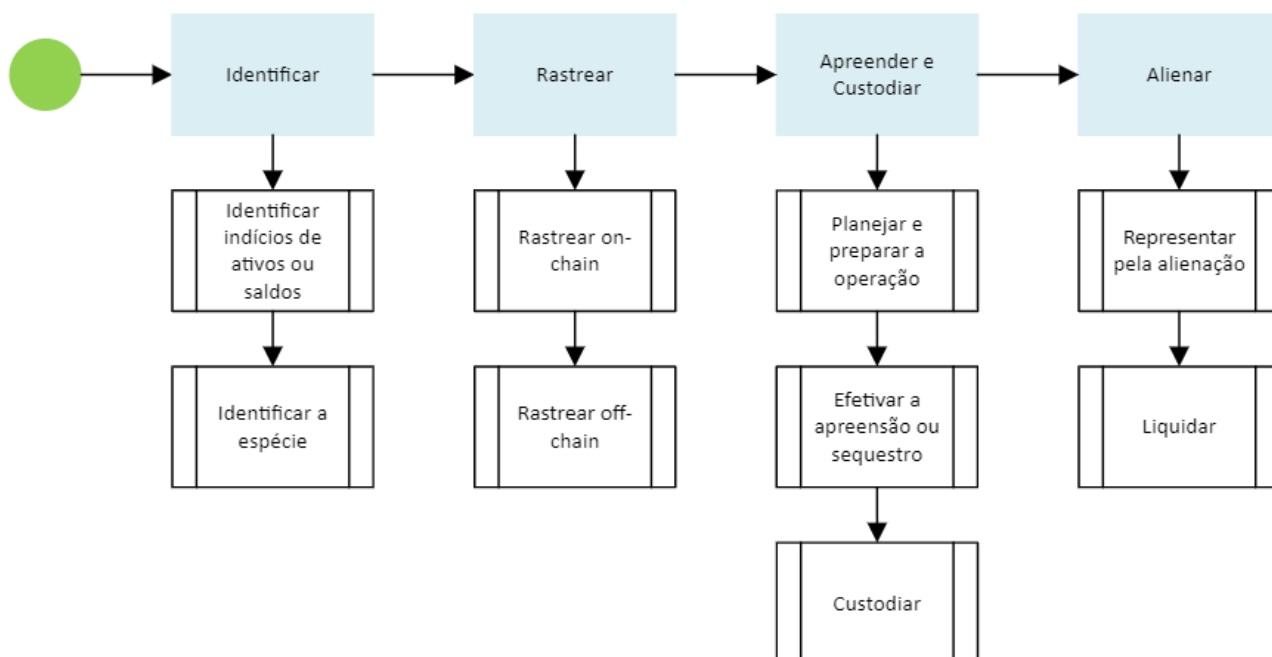
- Descrição do elemento que deu acesso aos ativos virtuais apreendidos, através da menção da equipe que o encontrou, local onde foi encontrado, seu proprietário etc.
- Descrição do procedimento realizado para se ter acesso aos ativos virtuais.
- Descrição do saldo identificado da carteira do alvo.
- Hash de cada uma das transações de apreensão realizadas.
- Descrição do quantitativo apreendido de cada tipo de ativo.
- Descrição das taxas de transferências utilizadas.
- Relação e assinatura dos policiais responsáveis/testemunhas dos procedimentos.

Encontra-se disponibilizado nos anexos deste manual, para referência, uma sugestão/modelo de IPJ que discrimina o processo de apreensão de ativos virtuais realizado a partir de uma Frase Secreta encontrada em local de busca.

### **5.3.3. Alienar**

Os ativos virtuais são caracterizados por uma alta volatilidade, com grandes oscilações de valor. Ao contrário dos mercados regulamentados de valores mobiliários, onde existem mecanismos eficazes para prevenir manipulações, no mercado de ativos virtuais esses controles são menos presentes, permitindo que os preços sejam mais suscetíveis a flutuações imprevisíveis.





*Figura 54-Tarefas de Alienação*

A característica anteriormente destacada implica na observância do artigo I, letra b, da Recomendação N. 30 do CNJ, e que trata da alienação antecipada de bens apreendidos em procedimentos criminais quando indica aos juízes criminais que:

b) ordenem, em cada caso justificadamente, a alienação antecipada da coisa ou bem apreendido para preservar-lhe o respectivo valor, quando se cuide de coisa ou bem apreendido que pela ação do tempo ou qualquer outra circunstância, independentemente das providencias normais de preservação, venha a sofrer depreciação natural ou provocada, ou que por ela venha a perder valor em si, venha a ser depreciada como mercadoria, venha a perder a aptidão funcional ou para o uso adequado, ou que de qualquer modo venha a perder a equivalência com o valor real na data da apreensão.

Além da já mencionada volatilidade dos preços, que por si só justificaria o pedido de alienação antecipada dos ativos virtuais, destaca-se também a complexidade e as dificuldades relacionadas à custódia desses bens. Essa particularidade exige atenção especial e reforça a necessidade de concentrar esforços para que a alienação ocorra no menor prazo possível.

A citada precariedade da custódia de criptomoedas atrai a previsão contida no Art. 144-A do Código de Processo Penal, no sentido de que 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.

Atualmente, em que pese os sucessivos pedidos judiciais realizados por autoridades policiais para que o juízo disponibilize carteiras próprias do juízo, ou mesmo, para que indiquem PSAVs para a custódia de ativos virtuais apreendidos em operações de polícia judiciária, tal demanda nunca foi atendida, ficando a custódia a cargo das equipes policiais encarregadas da investigação.

Desse modo, considerando toda a precariedade e risco advindo do manuseio de carteiras em que se concentram as senhas privadas dos ativos virtuais arrecadados, bem como a facilidade de acesso e transferência do equivalente em ativos em caso de ataques hackers ou mesmo de servidores ou pessoas mal-intencionadas que porventura tenham acesso a tais dispositivos, recomendamos, fortemente, que em caso de apreensão de ativos virtuais, o pedido de alienação antecipada seja feito o quanto antes.

Em alguns casos observamos que os juízes autorizam a alienação de forma concomitante ao pedido de apreensão/sequestro. Entretanto, na maior parte dos casos, é preciso reformular tal intento após o momento da deflagração.

Em princípio, vislumbram-se duas formas juridicamente possíveis para se efetivar a venda dos ativos virtuais:

- a) Leilão ou
- b) Alienação direta em PSAV(s).

Apesar de o leilão ser a forma tipicamente prevista no CPP (Art. 120, § 5º, 133, caput; 144-A, § 1º), em virtude da pouca experiência dos leiloeiros com essa tecnologia, os juízes em geral têm autorizado que a alienação antecipada ocorra em PSAV(S).

A alienação direta em PSAV(s), por sua vez, a despeito de não estar prevista expressamente no CPP, pode ser admitida por uma interpretação teleológica do Código de Processo Civil, aplicável ao processo penal por força do art. 3º do CPP. É que o CPC não só admite a alienação por iniciativa própria da parte contrária (CPC, art. 880, caput) como a prioriza sobre o leilão. Demais disso, a alienação direta em PSAV é, inequivocadamente, a forma economicamente mais vantajosa para se concretizar a alienação porque não

depende do pagamento da comissão do leiloeiro e viabiliza a venda dos ativos virtuais pelo valor de mercado, trazendo, neste particular, menor risco ao resultado.

Assim sendo, nos casos em que o juiz atenda aos pedidos da alienação dos ativos de forma antecipada, a referida PSAV será responsável por apresentar um plano de liquidação e, após sua apresentação e autorização pelo juízo, os valores obtidos com a venda sejam recolhidos em conta judicial.

#### 5.3.3.1. Sugestão de rito de alienação

Traçadas as ideias anteriores, elencamos abaixo uma sugestão de rito para a alienação dos ativos virtuais apreendidos.

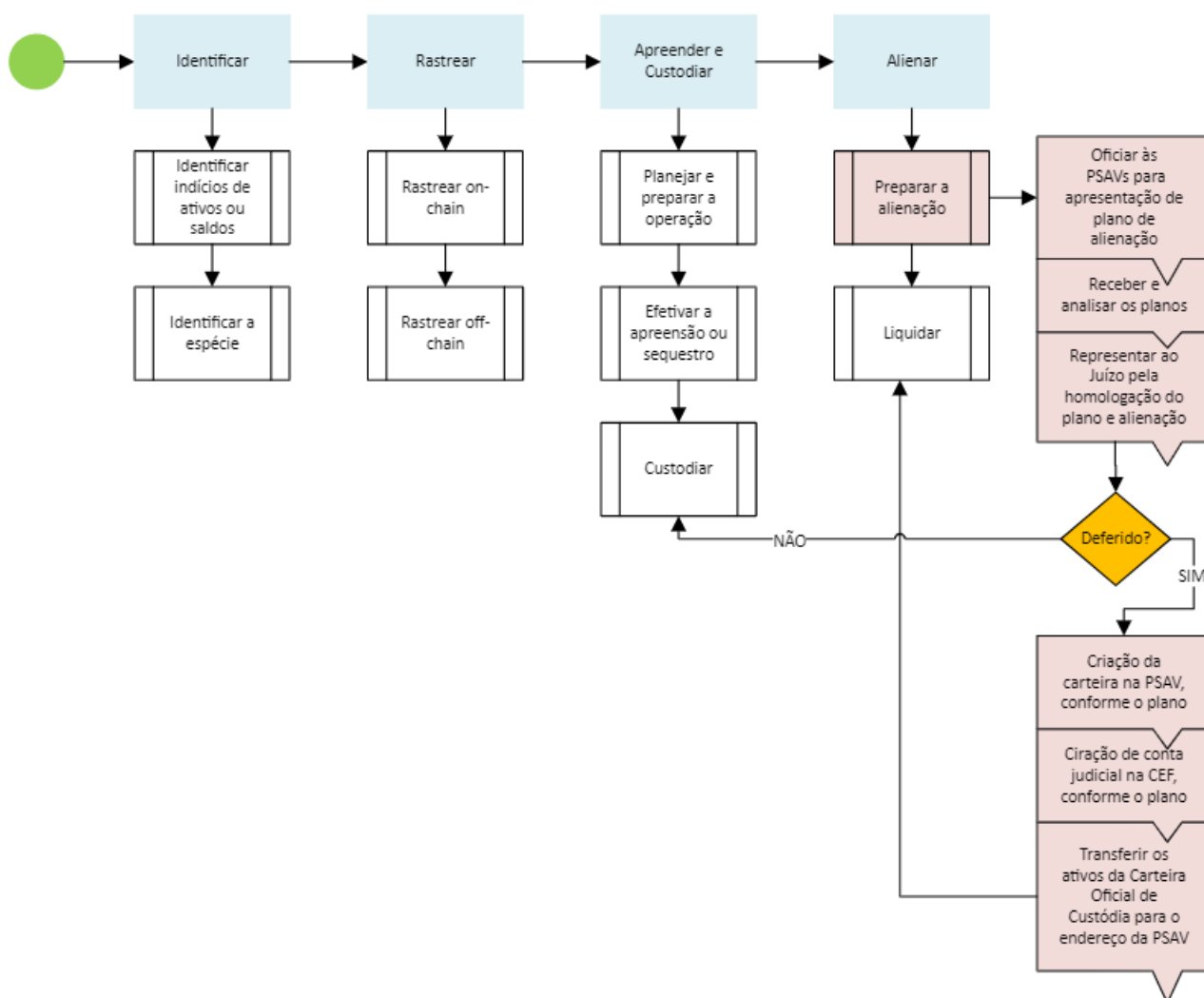


Figura 55-Sugestão de rito de alienação conforme a experiência compilada pela DFIN

Destacamos que a provocação do Judiciário pode ocorrer tanto por impulso da autoridade policial, que preside o inquérito, quanto pelo membro do Ministério Público responsável.

O modelo a seguir apresentado já foi replicado em algumas investigações, mas nada impede que, a depender do caso concreto, a opção adotada seja diversa. Assim, após justificar a alienação antecipada com os fundamentos do tópico anterior, entre outros, devem ser acrescentados os seguintes pedidos de ações a serem realizadas pelo juízo em caso de deferimento da alienação:

Expedição de ofícios, pelo Juízo competente, às 05 (cinco) PSAVs nacionais mais bem colocadas no mercado nacional na negociação de ativos virtuais (cf. consulta a ser feita, na data da apresentação da proposta em juízo, no site: <https://biscoin.io/exchanges/btc/brl>), informando a quantidade de ativos virtuais apreendidos e estipulando um prazo de 30 dias para que respondam aos ofícios e para que apresentem um plano detalhado para alienação das criptomoedas apreendidas, incluindo as taxas cobradas (a serem descontadas dos valores obtidos com as alienações, sem qualquer tipo de ônus para o poder público), os procedimentos a serem adotados e o tempo estimado para tanto, requerendo-se ainda:

Com a apresentação das respostas, escolha da PSAV a partir das informações fornecidas, com exclusão daquelas que não responderam aos ofícios no prazo a ser estipulado.

Que o critério prioritário de escolha do juízo não seja necessariamente o valor das taxas cobradas, mas considere também o market share (participação no mercado), já que, ao contrário do mercado de capitais, no mercado de ativos virtuais o livro de ofertas não é único para todo o mercado, mas sim formado dentro de cada PSAV, de sorte que, quanto maior a participação de uma PSAV no mercado, maior o número de interessados em comprar os ativos virtuais.

Seja homologado o plano de alienação antecipada escolhido pelo juízo dentre os apresentados.

Autorização para que a PSAV escolhida abra uma carteira em nome do Juízo, para a realização da transferência das criptomoedas em posse da Polícia Federal para referida carteira;

Após a alienação, os valores resultantes da venda dos ativos virtuais sejam transferidos imediatamente para conta vinculada ao Juízo na Caixa Econômica Federal.

Após a resposta das PSAVs, pugna-se pela intimação do investigado, por meio de sua defesa devidamente constituída, para informar, justificadamente, se tem alguma objeção à alienação antecipada dos ativos virtuais, bem como ao rito ora proposto.

Por fim, requer a determinação à Caixa Econômica Federal a abertura de conta judicial, vinculada aos autos, para transferência dos valores da alienação dos ativos virtuais apreendidos.

Vale dizer, ainda, que autoridades policiais optam por primeiro oficializar as PSAVs nacionais para, somente após as respostas dos órgãos, fazerem a submissão direta dos planos de alienação para escolha da proposta e homologação, o que não invalida, nem torna incorreta a representação realizada pelo profissional.

Demais disso, apontamos que à conta criada para depósito dos valores decorrentes da alienação antecipada dos criptoativos pode, nos casos em que houver a prática do crime de lavagem de dinheiro associada, ser vinculada ao FUNAPOL, pela utilização do código correspondente.

---

## Glossário dos principais termos citados neste capítulo

---

---

**Arkham:** É uma plataforma de rastreamento de blockchain que se especializa em analisar e desanonimizar transações em criptoativos. Arkham oferece insights sobre fluxos de ativos, monitoramento de carteiras e identificação de comportamentos suspeitos.

---

**Blockpath:** É uma plataforma que oferece ferramentas para o rastreamento de transações e análise de carteiras em diversas blockchains. Blockpath ajuda na visualização de fluxos de criptoativos e no acompanhamento de endereços de forma transparente.

---

**Chainalysis:** É uma empresa especializada em ferramentas de rastreamento e análise de blockchain. Ela fornece software de compliance e monitoramento para governos, exchanges e outras instituições, ajudando a identificar atividades ilícitas e rastrear transações em criptoativos.

---

---

**Criptomoeda Nativa:** Refere-se à principal criptomoeda de uma blockchain específica. Por exemplo, o Ether (ETH) é a criptomoeda nativa da Ethereum, e o Bitcoin (BTC) é a criptomoeda nativa da blockchain Bitcoin.

---

**Electrum:** É uma carteira de criptoativos focada em Bitcoin. É uma das carteiras mais antigas e populares, conhecida por sua leveza e velocidade. Electrum é uma carteira não custodial e oferece recursos avançados como suporte a multisig e integração com hardwallets.

---

**Ether (ETH):** É a criptomoeda nativa da blockchain Ethereum. Ether é usada para pagar as taxas de transação (conhecidas como "gas fees") e também funciona como uma unidade de valor dentro do ecossistema Ethereum.

---

**Exodus:** É uma carteira de criptoativos multi-cripto que suporta diversas blockchains. Ela oferece uma interface intuitiva e permite aos usuários armazenar, enviar, receber e trocar criptoativos diretamente dentro do aplicativo.

---

**Ferramentas de Rastreamento:** São plataformas ou softwares que permitem o monitoramento e análise de transações de criptoativos em blockchain. Essas ferramentas são usadas para investigar atividades ilícitas, monitorar movimentações de grandes quantidades de criptoativos, ou verificar a origem e o destino de fundos em blockchains públicas.

---

**Metamask:** É uma carteira digital usada principalmente para interagir com a blockchain Ethereum. Ela pode ser usada como uma extensão de navegador ou aplicativo móvel, permitindo o armazenamento de Ether e tokens ERC-20, além de permitir a interação com contratos inteligentes e DApps.

---

**Metasleuth:** É uma ferramenta de análise de blockchain focada em investigar e rastrear transações em múltiplas redes blockchain. Usada para análise de dados e rastreamento de criptoativos, ajuda a identificar padrões de comportamento em blockchains públicas.

---

**OSINT (Open Source Intelligence):** É o processo de coleta de informações utilizando fontes públicas e abertas, como redes sociais, sites, fóruns e outros meios disponíveis ao público. No contexto de criptoativos, o OSINT pode ser usado para investigar transações suspeitas, identificar endereços ou atividades de carteiras, e monitorar comportamentos de mercado.

---

**Rastreamento Off-Chain:** Refere-se à investigação e análise de transações que ocorrem fora de uma blockchain, como em exchanges centralizadas ou transações privadas. O rastreamento off-chain foca em dados fora da rede blockchain, como registros de exchanges ou informações financeiras externas.

---

---

**Rastreamento On-Chain:** Refere-se à análise e rastreamento de transações que ocorrem diretamente na blockchain. Este tipo de rastreamento permite visualizar e monitorar o histórico de transações e movimentações de ativos em tempo real, utilizando o livro-razão público da blockchain.

---

**REGEX (Regular Expression):** É uma técnica usada em programação para identificar padrões específicos de caracteres dentro de um texto. Em criptoativos, REGEX pode ser utilizado para extrair e analisar endereços de carteiras, hashes de transações e outras informações estruturadas.

---

**Saldo Representativo de Ativos Virtuais:** Refere-se à representação de quantidade de criptoativos que um usuário possui em sua carteira digital. Esse saldo é registrado pela Prestadora de Serviços de Ativos Virtuais.

---

**TRM (TRM Labs):** É uma empresa de inteligência financeira e compliance que oferece ferramentas de monitoramento e rastreamento de criptoativos. Suas soluções são usadas para combater crimes financeiros, prevenir lavagem de dinheiro e analisar riscos relacionados a transações em blockchain.

---

**Trust Wallet:** É uma carteira digital de criptoativos não custodial que permite aos usuários armazenar e gerenciar várias criptomoedas. Trust Wallet oferece suporte a diferentes blockchains e tokens, e os usuários têm controle total sobre suas chaves privadas.

---

## 6. CONSIDERAÇÕES FINAIS

O ambiente dos criptoativos apresenta um desafio único para investigadores, em razão de sua natureza descentralizada, anônima e global. No entanto, com as ferramentas corretas, técnicas avançadas e uma compreensão profunda dos mecanismos por trás das blockchains, é possível traçar um caminho claro para identificar fluxos de transações, rastrear ativos e, em muitos casos, associar identidades a endereços e carteiras.

A aplicação de metodologias como o Rastreamento On-Chain e Off-Chain, o uso de criptografia assimétrica e a análise de dados públicos disponíveis em exploradores de blockchain oferece um panorama detalhado e preciso das movimentações dentro deste ecossistema digital. No entanto, é crucial que os investigadores estejam constantemente atualizados sobre as novas tecnologias, tendências e legislações emergentes, uma vez que o setor dos criptoativos é dinâmico e em constante evolução.

É igualmente importante que as investigações sigam princípios éticos e legais, respeitando as regulações locais e internacionais e garantindo que as análises sejam conduzidas de forma transparente e imparcial. Com o crescimento exponencial dos ativos virtuais e a integração desses ativos ao sistema financeiro tradicional, o trabalho de investigação desempenha um papel fundamental na manutenção da segurança, legalidade e confiança nesse novo paradigma econômico.

O uso adequado de ferramentas especializadas, combinado com o conhecimento técnico, pode transformar o processo de investigação, trazendo à luz informações essenciais para a tomada de decisões e a mitigação de riscos. O papel do investigador será cada vez mais estratégico nesse cenário, onde inovação, segurança e privacidade caminham lado a lado.

Nesse contexto, a Coordenação Geral de Repressão à Corrupção, Crimes Financeiros e Lavagem de Dinheiro e a Divisão de Repressão aos Crimes Financeiros apresentam este manual de suporte para o corpo policial.



## 7. BIBLIOGRAFIA

ARAÚJO, Eugênio Rosa de. Finanças públicas e direito penal: O conceito de evasão de divisas no parágrafo único do artigo 22 da Lei no 7.492/1986 (LGL\1986\17). Revista da Seção Judiciária do Rio de Janeiro, Rio de Janeiro, v. 19, n. 33, p. 89-96, abr. 2012.

BANCO CENTRAL DO BRASIL. Circular 3624/2013. Disponível em: <[https://www.bcb.gov.br/pre/normativos/circ/2013/pdf/circ\\_3624\\_v1\\_O.pdf](https://www.bcb.gov.br/pre/normativos/circ/2013/pdf/circ_3624_v1_O.pdf)>.

BARAN, Paul. On Distributed Communications (Introduction to distributed communication network). Economic Policy, v. 5, p. 193-208, 2009.

BITCOIN SAFETY. \*Seed phrase list\*. Bitcoin Safety, 2023. Disponível em: <<https://www.bitcoinsafety.com/blogs/bitcoin/seed-phrase-list>>.

BITENCOURT, Cezar Roberto. Tratado de direito penal econômico. São Paulo: Saraiva, 2012.

BLOCKCHAIN ACADEMY BRAZIL. COMMENTS to the BCBS Discussion Paper entitled "Designing a prudential treatment for crypto-asset". Destinatário: the Basel Committee on Banking Supervision. São Paulo, 13 março 2020. Carta. Disponível em: <<https://www.bis.org/bcbs/publ/comments/d490/blockchainacademybrazil.pdf>>.

BLOCKCHAIN.COM. Transação Bitcoin f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16. Disponível em: <<https://www.blockchain.com/pt/explorer/transactions/btc/f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16>>.

BRASIL. Decreto nº 11.563, de 13 de junho de 2023. Regulamenta a Lei nº 14.478, de 21 de dezembro de 2022, para estabelecer competências ao Banco Central do Brasil sobre a prestação de serviços de ativos virtuais. Diário Oficial da União, Brasília, DF, 14 jun. 2023. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2023/decreto/D11563.htm](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11563.htm)>.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, Brasília, DF, 31 dez. 1940. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848.htm](https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm)>.

BRASIL. Receita Federal. Criptoativos: Receita Federal detecta crescimento vertiginoso na movimentação de stablecoins. Receita Federal, 2023. Disponível em: <<https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2023/outubro/criptoativos-receita-federal-detecta-crescimento-vertiginoso-na-movimentacao-de-stablecoins>>.

BRASIL. Receita Federal. Instrução Normativa RFB nº 2.219, de 17 de setembro de 2024. Atualiza as regras da e-Financeira e amplia a obrigatoriedade de envio de informações financeiras por novas entidades. Diário Oficial da União, Brasília, DF, 18 set. 2024. Disponível em: <<https://normas.receita.fazenda.gov.br>>.

BRASIL. Lei nº 7.492, de 16 de junho de 1986\*. Define os crimes contra o sistema financeiro nacional. Diário Oficial da União, Brasília, DF, 17 jun. 1986. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/leis/l7492.htm](https://www.planalto.gov.br/ccivil_03/leis/l7492.htm)>.

BRASIL. Lei nº 9.613, de 3 de março de 1998\*. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores. Diário Oficial da União, Brasília, DF, 4 mar. 1998. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/leis/l9613.htm](https://www.planalto.gov.br/ccivil_03/leis/l9613.htm)>.

BRASIL. Lei nº 14.478, de 21 de dezembro de 2022\*. Dispõe sobre diretrizes para o mercado de criptoativos no Brasil. Diário Oficial da União, Brasília, DF, 21 dez. 2022. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_Ato2022-2026/2022/Lei/L14478.htm](https://www.planalto.gov.br/ccivil_03/_Ato2022-2026/2022/Lei/L14478.htm)>.

BRASIL. Lei nº 14.754, de 12 de dezembro de 2023. Dispõe sobre a tributação de aplicações em fundos de investimento no País e da renda auferida por pessoas físicas residentes no País em aplicações financeiras, entidades controladas e trusts no exterior. Diário Oficial da União, Brasília, DF, 13 dez. 2023. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_Ato2023-2026/2023/Lei/L14754.htm](https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14754.htm)>.

BRASIL. Receita Federal. Solução de Consulta COSIT nº 217, de 21 de setembro de 2023. Trata da não obrigatoriedade de reporte de operações com NFTs na Declaração de Criptoativos. Diário Oficial da União, Brasília, DF, 29 set. 2023. Disponível em: <<https://normas.receita.fazenda.gov.br>>.

BRASIL. Receita Federal. Solução de Consulta COSIT nº 218, de 21 de setembro de 2023. Esclarece sobre obrigações acessórias relacionadas a plataformas de transação de utility tokens. Diário Oficial da União, Brasília, DF, 29 set. 2023. Disponível em: <<https://normas.receita.fazenda.gov.br>>.

BROWNORTH, Anders. Blockchain demo. Disponível em: <<https://andersbrownworth.com/blockchain/>>.

COINCODEX. Nick Szabo: the Father of Bit Gold. Binance Square, 2023. Disponível em: <<https://www.binance.com/en/square/post/669178305602>>.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Orientação N. 40. Disponível em: <<https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html>>.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Supervisão Baseada em Risco: Relatório Semestral julho - dezembro 2017. Disponível em: <[http://www.cvm.gov.br/export/sites/cvm/menu/acesso\\_informacao/planos/sbr/Relatorio\\_Se\\_mestral\\_julhodezembro\\_2017.pdf](http://www.cvm.gov.br/export/sites/cvm/menu/acesso_informacao/planos/sbr/Relatorio_Se_mestral_julhodezembro_2017.pdf)>.

CRYPTO DAWAR. Nick Szabo, The Real Satoshi Nakamoto: o estudo de caso definitivo. Binance Square, 2023. Disponível em: <<https://www.binance.com/pt-BR/square/post/7692072862561?ref=49193790>>.

DURAN, CV; Steinberg, D.; CUNHA FILHO, M. C. "Criptoativos no Brasil: o que são e como regular? Recomendações aos Projetos de lei 2060/2019 e 2303/2015". Faculdade de Direito da Universidade de São Paulo, 2019.

FATF-GAFI. Guidance for a risk-based approach to virtual assets and virtual asset service providers. Financial Action Task Force, 2019. Disponível em: <<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html>>.

FATF-GAFI. Guidance for a risk-based approach - Virtual Assets and Virtual Asset Service Providers: AML – Anti Money Laundering; CFT – Counter Financing of Terrorism. Financial Action Task Force, 2019.

FATF-GAFI. Virtual currencies: key definitions and potential AML/CFT risks. Financial Action Task Force, 2014. Disponível em: <<https://www.fatf-gafi.org/en/publications/Methodsandrends/Virtual-currency-definitions-aml-cft-risk.html>>.

FLÁVIO NETO, Luís. Criptomoedas e hipóteses de (não) realização da renda para fins tributários: o encontro das "tecnologias disruptivas" da economia digital com a "tradição" dos institutos jurídicos brasileiros. In: ZILVETTI, Fernando Aurelio; FAJERSZTAJN, Bruno; SILVEIRA, Rodrigo Maito da. Direito Tributário Princípio da Realização no Imposto sobre a Renda: Estudos em Homenagem a Ricardo Mariz de Oliveira. São Paulo: IbdT, 2019.

GOMES, Daniel de Paiva. Bitcoin: a tributação de investimentos em criptomoedas. 2019. 305f. Dissertação (Mestrado) - Curso de Direito, Fundação Getúlio Vargas, Escola de Direito de São Paulo, São Paulo, 2019.

GRUPENMACHER, Giovana Treiger. As plataformas de negociação de criptoativos: uma análise comparativa com as atividades das corretoras e da bolsa sob a perspectiva da proteção do investidor e da prevenção à lavagem dinheiro. 2019. 219 f. Dissertação (Mestrado) - Curso de Direito, Fundação Getúlio Vargas, Escola de Direito de São Paulo, São Paulo, 2019.

JOCHUMSEN, Rina. \*Hal Finney: o pioneiro por trás do Bitcoin e da criptografia digital\*. Binance Square, 2023. Disponível em: <<https://www.binance.com/pt-BR/square/post/10667997231001>>.

MANUAL DE PROCEDIMENTOS PERICIAIS – Perícia de Informática – Busca e Apreensão de Criptoativos. Polícia Federal. DITEC – Instituto Nacional de Criminalística. 1ª edição. 2021.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>.

NAKAMOTO, Satoshi. E-mail exchanges on cryptography. Satoshi Nakamoto Institute, 2008. Disponível em: <<https://satoshi.nakamotoinstitute.org/emails/cryptography/1/>>.

PARENTONI, Leonardo; [Coord.] GONTIJO, Bruno Miranda; LIMA, Henrique Cunha Souza. [Orgs.]. Direito tecnologia e inovação. Vol. 1. Belo Horizonte: Editora D'Plácido, 2018.

PÉRICO, Augusto e col. Evadindo divisas com bitcoins? Uma matriz para a avaliação do risco de prática de evasão de divisas. São Paulo, 2020.

RECEITA FEDERAL DO BRASIL. Ato Declaratório Executivo COPE/S nº 1, de 2023. Disponível em: <<https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos/arquivos/ato-declaratorio-executivo-copes-ndeg-1-2023>>.

RECEITA FEDERAL DO BRASIL. Instrução nº 1.888 de 03 de maio de 2019. Disponível em: <<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=100592>> Acesso em: 21 de outubro de 2024.

RECEITA FEDERAL DO BRASIL. Instrução nº 2.180 de 11 de março de 2024. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=100592>.

REGULANDO CRIPTOATIVOS. Projeto Multidisciplinar da Faculdade Getúlio Vargas. [Coord] ESTELLITA, Heloisa; PRADO, Viviane. Vários autores. 2020.

ROTEIRO DE ATUAÇÃO CRIPTOATIVOS – Persecução Patrimonial. 2ª Câmara de Coordenação e Divisão. 2023.

SALAMA, Bruno Meyerhof. O mercado de criptomoedas começa a ser regulado: FATF publicou um novo guia de análise de risco de lavagem de capitais e financiamento de terrorismo para o setor de ativos virtuais. [S. l.], 14 ago. 2019. Disponível em: <https://www.infomoney.com.br/columnistas/bruno-meyerhof-salama/o-mercado-de-criptomoedas-comeca-a-ser-regulado>.

SCHMIDT, Andrei Zenkner; FELDENS, Luciano. O crime de evasão de divisas: a tutela penal do sistema financeiro nacional na perspectiva da política cambial brasileira. Rio de Janeiro: Lumen Juris, 2006.

SZABO, Nick. The idea of smart contracts. Satoshi Nakamoto Institute, 1997. Disponível em: <<https://nakamotoinstitute.org/library/the-idea-of-smart-contracts/>>.

SZABO, Nick. Bit Gold. Satoshi Nakamoto Institute, 2005. Disponível em: <<https://nakamotoinstitute.org/library/bit-gold/>>.

YCHARTS. \*Bitcoin Average Block Size\*. Disponível em: <[https://ycharts.com/indicators/bitcoin\\_average\\_block\\_size](https://ycharts.com/indicators/bitcoin_average_block_size)>.

## **8. ANEXOS**

Considerando possíveis atualizações nos modelos atualmente utilizados pela Polícia Federal, encaminhamos o leitor à página oficial da instituição, onde estarão disponíveis, dentre os seguintes modelos:

- Modelo de Briefing
- Modelos de Representação;
- Modelos de IPJ de Apreensão

Segue o link da página de Criptoativos da DFIN na qual constarão os modelos:

**[https://pfgovbr.sharepoint.com/:u:/r/sites/PortalCIAF/SitePages/Criptom  
oedas.aspx](https://pfgovbr.sharepoint.com/:u:/r/sites/PortalCIAF/SitePages/Criptom<br/>oedas.aspx)**