Criptomoedas

Orientações gerais para equipes de busca

V. 01 | 2019

POLÍCIA FEDERAL | CGRC

Conceitos iniciais

O que são criptomoedas?

São uma espécie de ativos virtuais; um pedaço de código que pode ser usado para armazenar e transferir valor. Funcionam como um tipo de "dinheiro digital", permitindo transferências diretas entre duas partes, da mesma forma que duas pessoas podem transacionar moeda corrente, mas sem a mediação de um agente centralizador (como um banco, por exemplo). Elas não são ilegais, podendo ser usadas de maneira lícita.

Como elas funcionam?

Através de um processo chamado criptografia de chaves públicas, que garante a segurança das transações. No caso do Bitcoin, todas as transações realizadas ficam disponíveis *online* em um livro público (similar a um livro razão) conhecido como o *Blockchain*. Deste modo, se você tem em mãos um endereço de Bitcoin, você pode verificar quantas bitcoins estão armazenadas lá e quais transações com ativos virtuais esse endereço já fez.

Como armazenar criptomoedas?

Quando falamos em armazenar criptomoedas, na verdade estamos falando em armazenar um par de chaves de criptografia que dão acesso a elas. Aplicativos de carteiras (*wallets*) armazenam e gerenciam essas chaves.

Uma chave privada não pode ser exposta ou perdida, sob o risco de um terceiro dispor livremente dos ativos virtuais vinculados a essa chave. No entanto, ela pode ser recuperada através de um *seed* – um conjunto aleatório de 12, 18 ou 24 palavras que permite o backup e a recuperação de uma carteira sem precisar de qualquer outra informação. É uma forma que o criminoso tem de poder acessar sua carteira, apenas memorizando a sequência de palavras.

Carteiras digitais (*apps*)

São interfaces acessadas por meio de dispositivos eletrônicos (smartphone, laptop, web, etc.) que permitem ao usuário gerar chaves e um endereço público, bem como gerenciá-las.

Carteiras de papel

Um pedaço de papel no qual é impresso ou registrado um par de chaves e o endereço a ele associado.

Carteiras de hardware

Dispositivos eletrônicos exclusivos para o armazenamento de chaves que dão acesso a criptomoedas, com um nível mais elevado de segurança.

Como comprar criptomoedas?

A maneira mais fácil de começar a transacionar com ativos virtuais é baixar um aplicativo de carteira (*wallet*) para o smartphone ou computador. Uma vez baixado, o aplicativo gera um par de chaves e, então, o usuário se torna titular de um endereço no qual os ativos virtuais serão "depositados".

Uma carteira digital pode ser usada como se fosse uma conta bancária convencional, recebendo fundos e realizando transferências. Uma vez que você tenha uma carteira, você pode "preenchê-la" comprando ativos virtuais das seguintes maneiras:

1

LocalBitcoins.com

2

3

foxbit

MERCADO BITCOIN

BITCOINTRADE

BINANCE

B2U

kraken

Transação direta 1

Vários websites estão disponíveis onde você compra ativos virtuais em uma transação direta com outra pessoa. Assim, o vendedor lhe envia/entrega os ativos virtuais dele em troca de moeda corrente, que pode ser entregue inclusive em espécie. Exemplos são o LocalBitcoins, o LiberalCoins e o Paxful.

Caixas Eletrônicos (ATMs) de ativos virtuais 2

Você coloca dinheiro na máquina e informa o endereço que receberá o valor correspondente em criptomoeda. São mais populares no exterior, mas já existem no Brasil.

Exchanges 3

São websites legítimos, onde você abre uma conta e paga por ativos virtuais por meio de uma transferência bancária ou com seu cartão de crédito/débito. Muitos exigem que você providencie cópias de seus documentos de identificação para poder abrir sua conta e realizar transações.

O que buscar?

A seguir, uma lista –não exaustiva– de elementos que podem ser identificados em buscas. O acesso a dispositivos eletrônicos durante a busca **deverá ser objeto de autorização judicial específica** e contar com apoio pericial quando necessário, garantindo-se a manutenção da cadeia de custódia.

Carteiras digitais (*wallets*)

Acessadas por dispositivos eletrônicos, permitem gerar e gerenciar chaves e endereços.

XAPO JAXX EDGE BRD BTC.COM EXODUS COINOMI

ELECTRUM BITCOIN WALLET BLOCKCHAIN WALLET COINBASE MYCELIUM GREEN ADDRESS

Carteiras de hardware

Dispositivos eletrônicos para o armazenamento de chaves.


COOLWALLET


TREZOR

LEDGER

KEEPKEY


SAFE-T

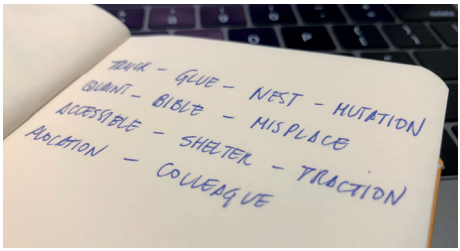
O que buscar?

Carteiras de papel

Pedaço de papel contendo as chaves e o endereço a ele associado.

Seeds

Conjunto aleatório de palavras que permite o backup e a recuperação de uma carteira.



Endereços

Extensos códigos alfanuméricos utilizados para o recebimento de valores, podem ser visualizados como QR codes. Um endereço de Bitcoin, que é a criptomoeda mais popular, possui entre 26-35 caracteres e começam com um 1, 3 ou bc1. Permite verificar o saldo e as transações já efetuadas.

`1CkpWik3TL2fq4cvQ5g1wEEDvHrkU4T3py`

Chaves privadas

Chaves privadas de Bitcoin possuem 51 ou 52 caracteres alfanuméricos que normalmente começam com 5, L ou K.

`5J2eNfaJx4WPtkoHCWgUCnXbvTfdJeDxXsLkZAhVRNHo8wWpdMn`

O que buscar?

Relacionamento com *exchanges*

Identificar no material do investigado registros de contas abertas junto a exchanges ou de transações efetuadas com exchanges.

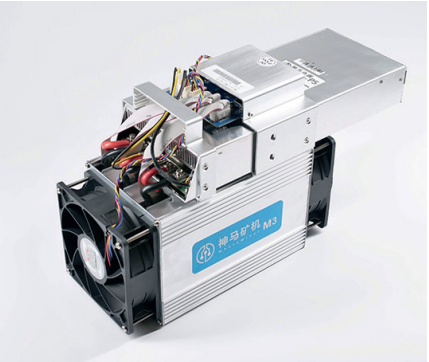
Principais exchanges

NO BRASIL
Foxbit, Mercado Bitcoin, BitcoinTrade, Negocie Coins, Bitcoin2You, entre outras.

NO EXTERIOR
Binance, OKEx, Coinbase, ZB.COM, Kraken, Bitfinex, Huobi, entre outras.

Equipamentos de mineração

Dispositivos que podem ser comprados por qualquer um e utilizam poder computacional para "gerar" criptomoedas. Atualmente, é uma atividade desenvolvida por grandes grupos, que utilizam potentes máquinas e muita energia elétrica, não sendo comum que um indivíduo se dedique à atividade de forma caseira.



Equipamento de mineração Whatsminer M3

Arquivos digitais

*Estão associados ao uso de carteiras (*wallets*). Podem ser localizados em um dispositivo informático e contêm as chaves de criptografia necessárias para que se obtenha controle das criptomoedas.*

Tipos de arquivos

Padrão de cliente Bitcoin Core:
`wallet.dat`

Formato zj protobuf:
`.wallet`

Onde encontrar?

Localização padrão do diretório dos arquivos (por sistema operacional)

Windows Vista/7/8:
`C:\Usuários\UserName\Appdata\Roaming\Bitcoin`

Mac
`~/Library/ApplicationSupport/Bitcoin/`

Linux
`~/.bitcoin/`

Apreensão de criptomoedas

O que eu devo apreender?

Havendo suspeita de utilização de criptomoedas em contexto criminoso, e **existindo autorização judicial específica no mandado de busca e apreensão**, deverão ser apreendidas quaisquer evidências que representem a utilização de ativos virtuais – carteiras, endereços públicos e chaves, bem como dispositivos eletrônicos contendo histórico de acesso a websites relacionados a criptomoedas e arquivos associados a carteiras. A ideia é apurar se o investigado é titular de ativos virtuais e, em caso positivo, apreendê-los ou rastrear o fluxo das transações efetuadas.

Como você pode apreender os ativos virtuais?

Se você controlar a chave privada, você controla o ativo virtual e pode dispor dele livremente. **Apreender um ativo virtual significa, inicialmente, assumir o controle da chave privada**. Isso pode ser feito (1) através da descoberta da *seed* ou da própria chave, que podem estar registradas ou armazenadas em local acessível, em meio físico ou digital; ou (2) pelo acesso a uma carteira (*wallet*), que deverá estar instalada em algum dispositivo eletrônico, normalmente protegido por senha adicional. Em caso de dificuldade de acesso no local da busca, o dispositivo deverá ser apreendido e encaminhado à perícia.

Para efetivar a apreensão e prevenir a perda do controle dos ativos **é necessário também transferi-los imediatamente para uma carteira controlada pelo Estado**. É importante agir rapidamente durante uma apreensão, pois é provável que o investigado ou seus associados tenham backups de suas chaves privadas ou de suas *seeds*, o que permitirá a movimentação dos ativos a partir de outros dispositivos eletrônicos.

Assim, enquanto a questão da apreensão de ativos virtuais não for objeto de regulamentação específica, **sugere-se que a Autoridade Policial represente ao juízo solicitando autorização para apreensão dos ativos virtuais porventura identificados durante o cumprimento do mandado**, com a transferências dos ativos identificados para uma carteira controlada pelo Estado.

Ativos que estejam sob a custódia de uma *exchange* poderão ser alvos de ordem judicial de bloqueio de ativos.

Por que eu preciso saber sobre criptomoedas?

As redes de criptomoedas e sua popularidade continuam a crescer e, devido à sua natureza descentralizada e ao fato de que não são reguladas, é impossível "desligá-las".

Ao contrário da identificação e apreensão de dinheiro em espécie, com as quais as equipes policiais já estão familiarizadas, o uso criminoso de ativos virtuais apresenta novos desafios ao cumprimento da lei: um pedaço de código pode ser usado para armazenar e transferir dinheiro. Nesse contexto, as equipes de busca precisam saber o que procurar.

Como criminosos usam criptomoedas?

Pagamentos ilícitos na *dark web*

Ativos virtuais são a principal moeda de troca na *dark web*. Nela, é possível pagar para adquirir drogas, armas e até mesmo contratar um assassino.

Armazenamento de valor

Aplicativos de carteiras de ativos virtuais podem efetivamente ser usados como uma "conta bancária" para armazenar os produtos dos crimes, convertendo-se moeda corrente em ativos virtuais.

Transferência de dinheiro

Criptomoedas podem ser transferidas para qualquer lugar do mundo com um simples comando, sem a possibilidade de se controlar ou regular, convertendo-se em um poderoso instrumento de lavagem de dinheiro.

Referências de conteúdo: Bitcoin for search officers (N8 Policing Research Partnership, 2017); A guide for bitcoin investigators (EC3 Europol, 2017).
Créditos das imagens: Marco Verch/Flickr (capa); torange.biz (p. 7)

CGRC POLÍCIA FEDERAL