MÓDULO 4

ESTUDOS DE CASO

por Alexandre Senra

I CASOS

(1) 02/12/2019

https://dje.tjsp.jus.br/cdje/consultaSimples.do?cdVolume=14&nuDiario=2944&cdCaderno=11&nuSeqpagina=3561

(2) 28/04/2020

https://portaldobitcoin.uol.com.br/em-prisao-domiciliar-antigo-lider-da-unick-forex-diz-que-fara-live-para-anunciar-novos-projetos/

- **10/12/2020**

  https://www1.folha.uol.com.br/mercado/2020/12/vitimas-de-madoff-receberao-quase-us-500-mi-em-indenizacoes.shtml

(3) 16/06/2020

https://cointelegraph.com.br/news/national-justice-council-plans-to-block-bitcoin-on-exchanges-in-brazil

(4) 28/08/2020

https://portaldobitcoin.uol.com.br/justica-de-goias-faz-acordo-trabalhista-de-r-350-mil-e-usa-bitcoin-como-pagamento/

(5) 05/11/2020

https://olhardigital.com.br/2020/11/05/noticias/justica-dos-eua-confisca-quase-us-1-bilhao-em-bitcoins/

(6) 26/11/2020

https://livecoins.com.br/justica-expede-oficio-a-bitcoin-org-em-processo-de-divorcio/

II BUSCA, APREENSÃO E DEPÓSITO DE CRIPTOATIVOS

(1) Criptoativos (existentes) estão sempre armazenados em carteiras.

(2) Carteira é o nome dado a duas coisas diversas:

- ao par chave privada e endereço público → carteira de papel, bastando, para se ter acesso aos criptoativos, a chave privada.
- à aplicação que armazena chaves privadas criptografadas, sendo necessário, para se ter acesso aos criptoativos:
    - arquivo armazenado no dispositivo que roda a aplicação (ou na nuvem) + senha;
    - OU seed words (palavras-sementes).

(3) Hot wallet X cold storage (~~cold wallet~~).

(4) Criptoativos do alvo podem estar numa carteira em poder dele próprio ou de exchanges. O que fazer?

(5) Se estiverem em poder dele mesmo:

- Carteira de papel → procura-se pela chave privada.
- Carteiras hardware, desktop ou mobile → procura-se pela seed OU pela senha + apreensão do dispositivo.

- Carteira web→ procura-se pela seed OU pela senha.

(6) Se estiverem em poder de exchanges:

- Nacionais: oficia-se à Receita Federal do Brasil (RFB) e às exchanges.
  - À RFB para que informe a eventual existência de operações com criptoativos realizadas pelo alvo (v. IN RFB 1888/2019).
  - Às exchanges para que informem eventual existência de saldo em nome do alvo e procedam ao seu imediato bloqueio, em sendo o caso.
- Estrangeiras: cooperação internacional.
  - https://www.infomoney.com.br/minhas-financas/ministerio-da-justica-bloqueia-r-130-milhoes-em-moedas-virtuais/

(7) Cautela com buscas ostensivas:

- Com a chave privada ou as palavras-semente qualquer outra pessoa também tem acesso aos fundos e, alertada, pode realizar a transferência dos criptoativos para uma nova e inacessível carteira.

(8) Deve-se fazer a transferência dos criptoativos para uma carteira do Poder Público o quanto antes.

- Ideal: hardware wallet.

(9) Um furto de 5.15 btc e o que podemos aprender com ele.

- Endereço público da carteira de papel que foi gerada para armazenar os criptoativos apreendidos: 1DS74UWUBRCj8C3eMVS7iXdUz8tXRcUbAV

- Lógica da coisa (= por que a carteira de papel é, *teoricamente*, tão segura?):
  - Você baixa o gerador aleatório de chaves privadas. Não precisa confiar em nenhuma aplicação. E essas chaves, depois de geradas, serão armazenadas fisicamente.
- Alguns possíveis problemas práticos, que comprometem a segurança desse procedimento:
  - Gera-se a carteira online.
  - Gera-se carteira offline e depois se reconecta o computador na internet.
  - Cria-se a carteira offline, não se reconecta na internet, mas se faz uso de um gerador que, em verdade, não era aleatório. Destaque-se que a fundação bitcoin.org não recomenda nenhum site que gere carteiras de papel.
  - Terceiros podem acabar tendo acesso físico à chave privada, onde ela tiver sido anotada ou guardada.

(10) Como se fazer, então, a apreensão e o depósito de criptoativos?

- Paper wallet → não. É muito segura na teoria. Na prática, o procedimento apresenta muitas vulnerabilidades.
- Web wallet → não. Chave privada fica armazenada na nuvem, ainda que de forma criptografada.
- Hardware wallet → ideal.
- Mobile ou desktop wallet → possível.
  - Referências em **https://bitcoin.org/pt_BR/escolha-sua-carteira**
- Muito cuidado no armazenamento da senha e, mais ainda, no armazenamento da seed.

(11) Brainwallet: é um tipo de carteira de papel. (https://www.bitaddress.org/)

III ALEGAÇÃO DE INVESTIMENTOS EM CRIPTOATIVOS COMO SUPOSTA JUSTIFICATIVA PARA UM ACELERADO ACRÉSCIMO PATRIMONIAL

Sugere-se seja requisitado que o alvo informe:

- Na hipótese de transações P2P: TXIDs ou endereços públicos das carteiras envolvidas.
- Caso tenha operado em exchanges nacionais: indicação do nome das exchanges.
- Caso tenha operado em exchanges não-nacionais: indicação do nome das exchanges + extrato do período das negociações ou justificativa da impossibilidade de fornecê-lo.

IV ALIENAÇÃO DE CRIPTOATIVOS

Sugere-se seja priorizada a venda por exchange nacional (em detrimento do leilão).

V QUERO PRATICAR. POR ONDE COMEÇAR?

(1) Abra uma conta numa exchange brasileira (onde você depositará BRL).

Ref.: https://bitvalor.com/

(2) Abra uma conta numa exchange estrangeira (onde você vai operar com um número muito maior de funcionalidades).

Ref.: https://coinmarketcap.com/pt-br/rankings/exchanges/

(3) Baixe uma mobile wallet, onde você armazenará seus criptoativos com segurança.

Ref.: https://bitcoin.org/pt_BR/escolha-sua-carteira

- Não deixe grandes volumes em exchanges.
- Deixe a seed fisicamente armazenada em segurança.
- Fique na aula até o final das perguntas e participe do desafio, tendo a chance de ganhar BRL 50,00 em BTC. **Update:** o desafio já foi vencido, mas você ainda pode praticar tentando resolvê-lo.
- Quem tiver interesse em se aprofundar no tema, não deixe de acompanhar as Lives sobre o assunto (https://www.instagram.com/alexandresenra_/).

VI DESAFIO

(1) Criei uma brainwallet (no https://www.bitaddress.org/) com o nome deste curso (“Criptoativos e blockchain para o MPU”). Seu endereço público é: **1AW4wp488DMovMk8XKXz7QABUqdBooYvCk**

(2) Transferi para ela o equivalente a BRL 50,00 em BTC.

(3) Agora você tem a oportunidade de ficar com esse saldo, bastando que você seja o primeiro a terminar estas etapas:

- gere a mesma chave privada que eu;

- importe essa chave privada em alguma aplicação (carteira);
- transfira o saldo para outra carteira, cuja chave privada só você possua.