Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

(Bônus) Criptomoedas e crimes

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

Objetivos

- Por que a “atração” do cibercrime por criptomoedas?
- O que seriam tipos comuns de crimes nesse universo?
  - Relação direta com os “porquês”...
  - ... e um alerta para se proteger contra golpes!

Apresentação originalmente realizada no XXVI Congresso Nacional de Criminalística, 2022, Campinas/SP

Notícias em 2022...

Roubo de criptomoedas está em alta. Eis como os crimes são cometidos, e como você pode se proteger (Fev/2022)

https://theconversation.com/crypto-theft-is-on-the-rise-heres-how-the-crimes-are-committed-and-how-you-can-protect-yourself-176027

Lavagem de dinheiro com criptomoedas sobe 30%, diz relatório (Jan/2022)

https://www.bbc.com/news/technology-60072195

Por que?

- Você já deve saber responder isso!
  - Criptomoedas: comum serem **descentralizadas**
    - Maior **resistência a bloqueio de bens**
  - Criptomoedas costumam fornecer algum grau de **(pseudo)anonimato**
    - Assumindo **ausência de intermediários**: política de *Know your Customer* (KYC) reduz ou elimina anonimato
    - Assumindo uso de **ferramentas** adequadas: e.g., Tor, Mixers
    - Apesar de **alguma rastreabilidade** ainda ser possível: Chainalysis, CipherTrace, ...
  - **Política de "imutabilidade"** de transações facilita movimentação de valores ilícitos
    - Opção de "desfazer" é considerada ação extrema (*forks*)

Crimes comuns: roubo de chaves

- Chave privada obtida diretamente do usuário, e usada para realizar transações em seu nome
  - **Acesso indevido a** chave armazenada: conta de e-mail, local físico (desktop, celular, pendrive, carteira...)
  - **Via malware**: spywares, keylogger, trojans, rootkits, ...
    - Ex.: CoinThief (MacOS Trojan, 2013), inserido no código compilado de soluções open source (e.g., Bitvanity, p/ criar "*vanity addresses*"[1]); rouba credenciais em sites e chaves privadas de outros aplicativos
    - Ex. CBHAgent (Win Trojan, 2018), monitora área de transferência; ao detectar endereço de carteira, substitui por endereço do atacante
  - **"Brainwallets"**: chaves privadas geradas com senhas.
    - Adivinhadas se senha é pouco complexa e algoritmo de derivação é inadequado (e.g., hash simples em vez de password hashing)
      - https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys/

[1] Identificadores de carteira contendo um palavra legível em Base58, como "Lover" ou "Rich"

Crimes comuns: invasões

- Ataques a **plataformas de Exchanges**
  - Explorando vulnerabilidades diversas que permitam **intrusão**
  - **Cooptando funcionários** internos (recrutamento é comum...)
  - Explorando más práticas de **governança**
    - Ex.: maleabilidade de assinaturas ECDSA permitia alterar ID de transações no Bitcoin, dificultando rastreio de transações (segwit introduzido em 2017 para mitigar problema)

➔ Mt Gox (conjectura): atacantes pediam 1 saque; Exchange **não percebia** que saque fora realizado ao procurar ID no Blockchain; Exchange repetia transação

- Resultado: várias carteiras afetadas ao mesmo tempo
  - Facilidade de uso vs. mantra "*not your keys, not you coins*"
  - Regulamentação sobre responsabilização nesses casos ainda é tímida...

Crimes comuns: bugs

- Ataques a plataformas de criptomoedas:
  - Bugs em **protocolos base** da plataforma
    - Ex. (Bitcoin): Maleabilidade de transações, mitigado por *Segregated witness* (segwit, 2017) -- removeu assinatura do cálculo do ID da transação
  - Bugs em **contratos inteligentes** internos
    - Ex. (Ethereum, 2016): o "incidente DAO" extraiu 3.6M ETH de um contrato usado para crowdfunding; mitigação feita por um hard fork ("desfazer" aprovado por 89% da rede, mas só 4.5% votantes)
  - Bugs em **pontes (*bridges*)** entre plataformas
    - Ex. (Wormhole, 2022): criação de 120k ETH no Ethereum em troca de valor "equivalente" (porém inexistente) na plataforma Solana; Jump Trading assumiu prejuízo com ETHs próprios
- Mitigação costuma envolver detecção de bugs
  - Programas de ***bug bounty*** são bastante comuns
  - **Ferramentas automatizadas** (ex.: verificação formal) é tema de intensa pesquisa

Crimes comuns: fraudes

- Exchanges de fachada
  - Legítimas em princípio, mas alegam ser vítimas de hacking;
  - Ou **pirâmides** desde o início
  - No Mundo: uma longa lista (até 2020) – https://selfkey.org/list-of-cryptocurrency-exchange-hacks/
  - No Brasil: operação Kryptos (Polícia Federal)
- Scamming :

  - (Spear) Phishing: links para sites falsos enviados via e-mail, SMS, apps de comunicação instantânea, …
    - Ex.: Binance, 2022: https://news.trendmicro.com/2022/02/11/binance-warns-crypto-investors-of-sms-phishing-scam/
  - Pedidos de dinheiro via apps de relacionamento
    - Ex.: www.theverge.com/2022/2/14/22933056/crypto-romance-scammers-139-million-fraud

Crimes comuns: atividades ilícitas

- Malware:
  - Ransomware: solicitação de pagamento usando criptomoedas
    - Não só Bitcoin, mas comumente também plataformas c/ mais privacidade (ex.: Monero)

  - Cryptojacking: recrutamento da máquina da vítima para botnet de mineração
    - Uso indevido de recursos computacionais da máquina infectada
  - Roubo de credenciais e invasão (já mencionados)
- Roubo de eletricidade para “fazendas de mineração”
- Movimentações na margem da legalidade
  - Lavagem de dinheiro e ocultação de patrimônio
  - Evasão de leis/acordos (ex.: embargo a Rússia)

Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

(Bônus) Criptomoedas e crimes

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

Apoio financeiro: d24n.org <https://d24n.org>
ripple impact | university blockchain research initiative

Referências

- B. Tabbaa (2018) "The Mt. Gox Hack— What's in your Bitcoin Wallet?". Medium. URL: https://medium.com/dataseries/the-rise-and-fall-of-mt-gox-whats-in-your-bitcoin-wallet-bd5eb4106f4e
- N. Goline (2018) "Bitcoin 2.0 (parte 2): o que é, pra que surgiu e como funciona o SegWit". Criptofacil. URL: https://www.criptofacil.com/bitcoin-2-0-parte-2-o-que-e-pra-que-surgiu-e-como-funciona-o-segwit/
- A. Madeira (2019) "The Dao, the Hack, the Soft Fork and the Hard Fork". CryptoCompare. URL: https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/
- CoinTime (2022) "Roubo bilionário na Wormhole pode ter criado bolha DeFi na Solana". URL: https://cointimes.com.br/roubo-bilionario-na-wormhole-pode-ter-criado-bolha-defi-na-solana/
- SelfKey (2020) "A Comprehensive List of Cryptocurrency Exchange Hacks". SelfKey Blog. URL: https://selfkey.org/list-of-cryptocurrency-exchange-hacks/
- Polícia Federal (2022) "PF deflagra operação para desarticular esquema de fraudes com criptomoedas". Ministério da Justiça e Segurança Pública. URL: https://www.gov.br/pf/pt-br/assuntos/noticias/2022/03/pf-deflagra-operacao-para-desarticular-esquema-de-fraudes-com-criptomoedas
- Trend Micro (2022) "Binance Warns Crypto Investors of SMS Phishing Scam". Trend Micro Blog - Scam. URL: https://news.trendmicro.com/2022/02/11/binance-warns-crypto-investors-of-sms-phishing-scam/
- E. Roth (2022) "Romance scammers collected $139 million in crypto last year". The Verge. URL: www.theverge.com/2022/2/14/22933056/crypto-romance-scammers-139-million-fraud
- G. Bertolucci (2022). "Justiça brasileira manda todas as corretoras venderem criptomoedas de investidor". Livecoins. URL: https://livecoins.com.br/justica-brasileira-manda-todas-as-corretoras-venderem-criptomoedas-de-investidor/
- A. Greenberg (2019) "A 'Blockchain Bandit' Is Guessing Private Keys and Scoring Millions". Wired. URL: https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys/