15º Congresso de Inovação, Ciência e Tecnologia do IFSP - 2024

Análise da cibersegurança na implementação de uma carteira cold wallet para transações com criptomoedas

Rafael S. Rocha[1,4], Felipe R. M. Basile[2,4], Leonardo J. R. López [3,4]

[1] Estudante do curso Técnico em Redes de Computadores Integrado ao Ensino Médio, Bolsista CNPq, IFSP, Câmpus Pirituba, rocha.rafael@aluno.ifsp.edu.br.
[2] Docente, IFSP, Câmpus Pirituba, felipe.basile@ifsp.edu.br.
[3] Docente, UMNG, Universidad Militar Nueva Granada, leonardo.ramirez@unimilitar.edu.co.
[4] GITES (Grupo de Informática e Tecnologia em Educação e Sociedade).
Área de conhecimento (Tabela CNPq): 1.03.04.02-9 Arquitetura de Sistemas de Computação.

RESUMO: *Bitcoins* são ativos digitais descentralizados que promovem sigilo e independência financeira, entretanto, o seu uso descuidado é associado a ataques maliciosos. Este projeto visa demonstrar um método sólido, por meio do processo de *hardening*, para garantir a segurança de uma carteira *cold wallet* às transferências do dia-a-dia. Para tal, foram utilizados os *softwares Tails* (*The Amnesic Incognito Live System*), sistema operacional reconhecido pelo sigilo oferecido ao usuário, e a carteira *Electrum*, aplicativo *open-source* conhecido pela sua acessibilidade. A combinação de ambos é constatada a partir do estudo de casos recentes de perdas financeiras envolvendo *exchanges* de reconhecimento internacional nos últimos 10 anos. Para, em seguida, construir uma análise que levará em consideração as vantagens desse método de autocustódia em comparação ao armazenamento terceirizado.

PALAVRAS-CHAVE: bitcoin; confidencialidade, electrum; hardening; privacidade; tails.

Cybersecurity analysis when implementing a cold wallet for cryptocurrency transactions

ABSTRACT: Bitcoins are decentralized digital assets that promote secrecy and financial independence, however, their careless use is associated with malicious attacks. This project aims to demonstrate a solid method, through the hardening process, to associate the security of a Cold Wallet with everyday transfers. To this end, Tails software (The Amnesic Incognito Live System) was used, an operating system recognized for the secrecy offered to the user, and the Electrum wallet, an open-source application known for its accessibility. The combination of both is confirmed by studying recent cases of financial losses involving internationally recognized exchanges over the last 10 years. To then build an analysis that will take into account the advantages of this self-custody method compared to outsourced storage.

KEYWORDS: bitcoin; confidentiality; electrum; hardening; privacy; tails.

INTRODUÇÃO

As criptomoedas surgem como uma proposta descentralizada e alternativa ao sistema financeiro convencional, de acordo com as proposições de precursores importantes como *Adam Back* e

Wei Dai (Aranha, 2020). Seguindo esse princípio, o *bitcoin* foi criado em 2008, por Satoshi Nakamoto, como uma alternativa para os bancos de dados controlados por autoridades centralizadas (Mezquita *et al*, 2019). Apesar de sua recente popularização, a conscientização acerca da segurança desses ativos ainda se configura como um tema pouco explorado.

Incidentes envolvendo criptomoedas ocorrem em várias dimensões, tanto as formas de ataque quanto os tipos de vítimas podem variar. Revistas e jornais, nacionais como *Estadão* e internacionais como a *CNBC*, registram casos envolvendo *exchanges* comprometidas, como a *Poloniex*, a *Poly Network* e a *Binance*, e disseminação de *malwares*, como o *WannaCry* e o *Readline Stealer*. Relatórios indicam que eventos semelhantes resultaram em perdas totais de $3,8 bilhões em criptoativos somente em 2022, como demonstrado pela *Chainanalysis* (2022). Esse fato sublinha a importância de um armazenamento seguro, capaz de proteger os usuários contra ameaças cibernéticas.

Dessa forma, esse artigo pretende propor um método de implementação de infraestrutura tecnológica para a autocustódia de *bitcoins*, para em seguida, realizar uma análise comparativa entre esse procedimento e o meio convencional. Conforme conceitos de cibersegurança associados às 3 dimensões do Cubo de McCumber (McCumber, 1991).

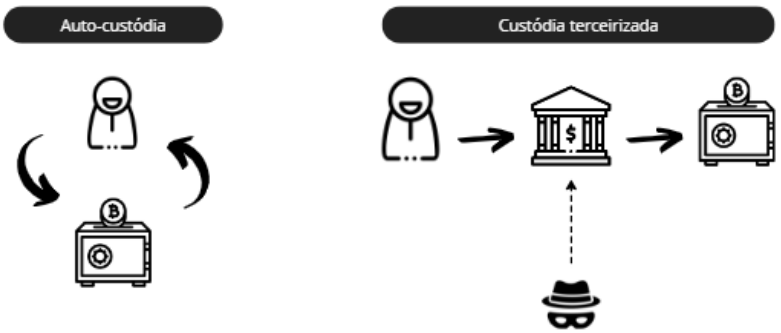

Figura 1: Fluxograma representativo dos conceitos associados à custódia. Fonte: Autor.

MATERIAL E MÉTODOS

A abordagem se dividiu em 3 etapas: o processo de montagem e configuração, o método de transação e, por fim, a análise comparativa. Ambas as tarefas de montagem e configuração remetem a instalação, personalização e ao *hardening* da carteira *Electrum*, que constitui o ponto mais importante da operação. O método de transação se refere a abordagem que usufrui da carteira tipo *watch-only* para transferências de *bitcoins*, com a finalidade de propiciar o resguardo seguro dos ativos. Por último, a análise comparativa considerou as vantagens do processo de autocustódia utilizado em comparação com práticas que incluem intermediadores.

A pesquisa foi inteiramente realizada dentro do ambiente do *SO Tails*, na versão mais recente até então (6.6), um sistema operacional reconhecido por priorizar a privacidade e anonimato do usuário, contando com recursos como o *Persistent Storage* e a conexão *Tor*. Juntamente com o *Tails*, foi utilizado a *Electrum* (versão 4.5.5, a última versão disponível no período da pesquisa), um *software open-source* integrado a esse sistema operacional, reconhecido por sua acessibilidade, baixo consumo de recursos e foco na simplificação do *bitcoin* (Voegtlin, 2011). As aplicações foram executadas em um *notebook Lenovo IdeaPad S145*, equipado com 100GB de armazenamento e 4GB de memória RAM.

Montagem e configuração

A implementação de uma *cold wallet* segura foi realizada utilizando uma combinação estratégica do sistema operacional *Tails* e da carteira *bitcoin Electrum*, ambos escolhidos por suas características avançadas de segurança. O *Tails*, conhecido por seus recursos voltados para a privacidade, oferece um ambiente temporário, sem armazenar informações após o fim da sessão, sendo ideal para a proteção de dados sensíveis como as chaves privadas. Por sua vez, a *Electrum* é

amplamente utilizada devido a sua interface acessível e personalizável, além de não exigir informações pessoais, portanto, preservando a confidencialidade e a autonomia de quem a utiliza.

A primeira etapa de *hardening* requer a instalação segura do sistema operacional através da criação de um *flash-drive USB bootável*, que irá permitir o carregamento do sistema. Para garantir a confiabilidade e integridade do ambiente, esse mesmo dispositivo *USB* deve possuir uma imagem clonada. Após a primeira inicialização, a etapa crucial é a definição de uma senha robusta, sendo recomendada a utilização de palavras aleatórias. Em seguida, há a configuração do *Persistent Storage*, que permite o sistema reter apenas os dados considerados como essenciais pelo usuário (no caso, as carteiras *Electrum*), descartando o que poderia se apresentar como um risco, como imagens ou redes *wi-fi*. Ressalta-se que, durante todo o processo, o dispositivo nunca se conectou à internet.

Por sua vez, a abordagem empregada para a carteira segue o padrão. Se iniciando através da definição do tipo da carteira, selecionando a opção "*standard wallet"* (carteira padrão), a configuração mais comum e apropriada para uma carteira *cold wallet*. O aspecto a ser destacado é o fato de que a carteira, recém-criada, nunca foi conectada à internet, da mesma forma que o sistema, o que confirma a característica de "carteira fria" e a segurança das chaves privadas. Esse isolamento garante que os ativos digitais permaneçam protegidos contra potenciais ameaças externas, oferecendo um nível de segurança reforçado ao usuário.

Método de transação

Com a carteira principal (*cold wallet*) criada, a responsável pela geração das chaves privadas, há a necessidade de criar outra, destinada à visualização e transmissão de transações (*watch-only*). A criação da segunda carteira se dá ao selecionar a opção "*usar uma chave-mestra*", onde deve-se inserir a chave *zpub* da carteira original. O propósito dessa divisão é garantir um ambiente seguro para o armazenamento das criptomoedas, mantendo as chaves privadas *off-line* e fora do alcance de ameaças. A carteira *watch-only*, conectada à internet (estado de *hot wallet*), permite que as operações necessárias sejam realizadas sem comprometer a segurança dos ativos, assegurando que a carteira principal permaneça completamente isolada e protegida.

A realização de uma transação envolve o uso combinado das duas carteiras, garantindo tanto segurança quanto praticidade. Inicialmente, a operação é gerada na carteira *watch-only*. Em seguida, a transação é assinada pela carteira principal, que permanece *off-line* (essa transmissão é realizada a partir de uma leitura de *QR code*, sem o uso de rede). Após essa etapa, a transação é finalmente transmitida através da carteira *on-line*, concluindo-a de maneira segura e eficiente. Dessa forma, as criptomoedas foram movimentadas sem risco de exposição das chaves privadas.

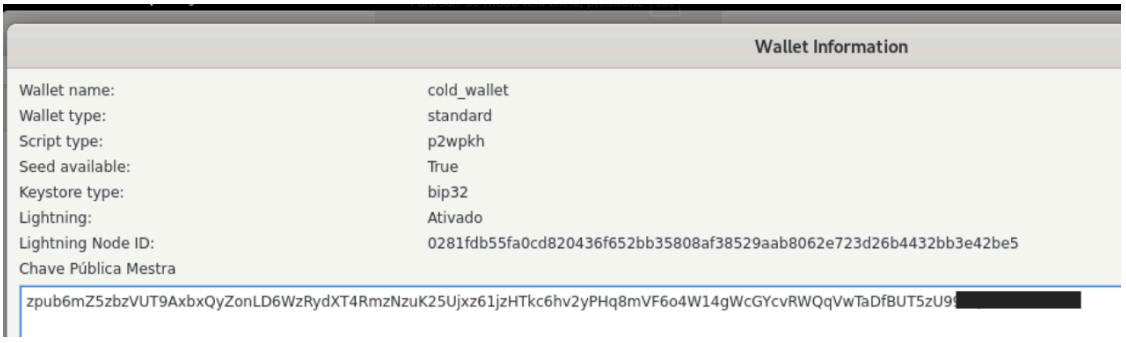

Figura 2: Informações referentes à carteira principal. Fonte: Autor.

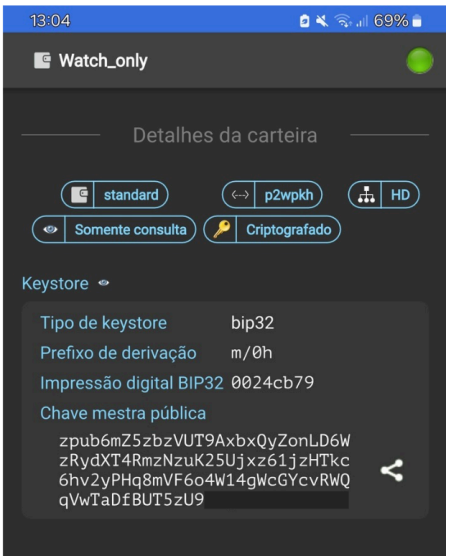

Figura 3: Informações referentes à carteira *watch-only*. Fonte: Autor.

Análise

Ao optar pelo uso dos serviços oferecidos de uma *exchange*, o indivíduo se depara com determinadas vantagens, mas também com desvantagens que podem ser críticas aos seus ativos. Por um lado, o usuário pode encontrar um suporte que simplifica os processos de aquisição e troca de *bitcoins*, o que é favorável para o crescimento e popularização do ativo (Parino *et al*, 2018). Por outro, essa conveniência vem acompanhada de maiores riscos, uma vez que as *exchanges* sempre estarão suscetíveis e vulneráveis a diferentes tipos de ataques, como elucidado na Introdução. Ademais, essas plataformas, em situações adversas, podem impactar diretamente os clientes, como em casos de falhas de segurança, interrupções nos serviços ou até mesmo na perda de fundos devido a ataques.

Em contrapartida, com o método de autocustódia descrito, o indivíduo assume total responsabilidade por seus ativos, sem a necessidade de terceiros para gerenciá-los. Com esse controle, o risco de *malwares* e de outras ameaças é mitigado, já que a carteira principal, onde há o armazenamento dos ativos e da chave privada, permanece no estado “frio”. Desse modo, essa abordagem mitiga os riscos de segurança apontados por Ulrich (2014).

RESULTADOS E DISCUSSÃO

Nakamoto (2008) apresenta e descreve o funcionamento da rede descentralizada, base do sistema de pagamentos digitais, cuja segurança e resiliência são fortalecidas por medidas como o *hardening*. O processo de *hardening* como um todo, que inclui a própria utilização do SO *Tails* e da carteira *Electrum*, assegurou que os dados críticos fossem preservados, alinhando-se ao conceito de Brotherson e Berlin (2017), que definem essa técnica como a prática de configurar sistemas para garantir o mais alto nível de segurança possível. Vale ressaltar que muitos dos problemas previamente identificados em versões anteriores da *Electrum*, conforme registradas nas CVEs, foram corrigidas através de atualizações, fortalecendo ainda mais a segurança do sistema. O resultado do método aplicado pode ser descrito através do Cubo de McCumber, uma ferramenta essencial para a cibersegurança.

O cubo é uma estrutura que abrange três dimensões fundamentais da segurança da informação. A primeira dimensão, “Objetivos de Segurança", trata da confidencialidade, integridade e disponibilidade, assegurando que os ativos estejam inacessíveis a não autorizados, inalterados e sempre disponíveis. A segunda dimensão, "Estados da Informação", envolve armazenamento, processamento e transmissão, com a proteção sendo reforçada por criptografia e autenticação no SO Tails. Por fim, a terceira dimensão aborda "Contramedidas", incluindo políticas, tecnologias e educação, com a implementação de boas práticas para manter a segurança dos ativos e procedimentos padronizados. A tabela a seguir demonstra os principais elementos que foram implementados:

TABELA 1. Exposição das propriedades do Cubo de McCumber aplicadas durante o método.

Camadas	Elementos	Implementação
Princípios da segurança da Informação	Confidencialidade, integridade e disponibilidade	Acesso restrito, desconectividade e acessível sempre que necessário
Estados da informação	Armazenamento	Resguardo seguro através da *Cold Wallet.*
Contramedidas	Tecnologias	Utilização do *Tails* e da *Electrum.*

CONCLUSÕES

Considerando as ferramentas e recursos disponíveis no SO *Tails*, conclui-se que a autocustódia de ativos *bitcoin* com os *softwares Tails* e *Electrum* é uma opção vantajosa quando comparada à custódia terceirizada, no quesito segurança. O usuário, com a utilização da carteira *watch-only*, passa a ter a possibilidade de efetuar as movimentações tradicionais, enquanto mantém a intrínseca segurança de uma carteira *cold wallet*. Ao contrário da custódia terceirizada, que pode expor os ativos a riscos, mesmo que mínimos. A abordagem de uma gestão própria elimina vulnerabilidades associadas a intermediários, oferecendo um controle mais rigoroso sobre a proteção e a gestão dos ativos. Portanto, a combinação do *Tails* e da *Electrum* se torna ideal para proporcionar um ambiente seguro e independente para a administração dos *bitcoins.*

CONTRIBUIÇÕES DOS AUTORES

Rafael Souza Rocha foi responsável pela pesquisa bibliográfica e pelo uso dos softwares mencionados.

Felipe Rodrigues Martinez Basile atuou na orientação e revisão do trabalho.

Leonardo Juan Ramirez López atuou como parceiro internacional no planejamento e desenvolvimento das atividades. Todos os autores contribuíram para a aprovação da versão submetida.

AGRADECIMENTOS

Agradecemos ao IFSP - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - Câmpus Pirituba, e ao CNPq pelo financiamento do projeto de pesquisa realizado.

REFERÊNCIAS

ARANHA, Christian. **Bitcoin, Blockchain e muito dinheiro.** 1. ed. Rio de Janeiro: Valentina, 2020. 160 p.

ChainAnalysis Team. **Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises**. ChainAnalysis, 2024. Disponível em: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/. Acesso em 06 mai, 2024.

BROTHERSTON, Lee; BERLIN, Amanda. **Defensive Security Handbook.** 1. ed. Sebastopol: O'Reilly Media, 2017. 284 p.

McCUMBER, John. **Information Systems Security: A Comprehensive Model.** Proceedings 14th National Computer Security Conference. National Institute of Standards and Technology. Baltimore, MD. October 1991

MEZQUITA, Yeray *et al*. **Blockchain technology in IoT systems: review of the challenges.** Annals of Emerging Technologies in Computing (AETiC), Print ISSN, p. 2516-0281, 2019.

NAKAMOTO, Satoshi. **Bitcoin: A peer-to-peer electronic cash system.** Decentralized business review, p. 21260, 2008.

PARINO *et al*.**Analysis of the Bitcoin blockchain: socio-economic factors behind the adoption.** EPJ Data Science. 2018

ULRICH, Fernando. **Bitcoin: A Moeda na Era Digital.** LVM Editora, 2014.

VOEGTLIN, Thomas. **Electrum**, Copyright 2011-2023+. Documentação oficial do software Electrum. Disponível em: https://electrum.readthedocs.io/en/latest/. Acesso em: 04 dez. 2023