Análise dos Mecanismos de Geração e Armazenamento de Chaves em Carteiras de Criptomoedas

Anderson O. de Souza, José Vitor H. da Silva, Nilson M. Lazarin

[1]Bacharelado em Sistemas de Informação – Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ) – Nova Friburgo, RJ – Brazil

anderson.souza.1,jose.heringer@aluno.cefet-rj.br, nlazarin@cefet-rj.br

Abstract. *This paper describes a security analysis of a list of applications known as crypto wallets, focusing on keys generation and storage. This analysis aims to inform future users about the security level implemented, to expose technical details of its internal components, as well as methods for wallet backup and restoration. Six wallets were selected according to the possibility of access to the source code and popularity, then they were evaluated using a set of eight relevant parameters when it comes to security*

Resumo. *Este artigo descreve uma análise de segurança de uma lista de softwares conhecidos como carteiras de cripto ativos, focando na geração e armazenamento de chaves. Esta análise visa informar futuros usuários em relação ao nível de segurança implementado, detalhes técnicos específicos de seus componentes internos, bem como métodos de restauração e backup de chaves. Foram selecionadas seis carteiras de acordo com a possibilidade de acesso ao código-fonte e popularidade, e em seguida avaliadas de acordo com um conjunto de oito parâmetros relevantes no quesito segurança.*

1. Introdução

A criação do Bitcoin desencadeou o surgimento de uma indústria inteiramente nova: a dos cripto ativos. Desde 2008, houve o desenvolvimento de uma grande variedade de tecnologias, com os mais variados propósitos, aliando engenharia de software e criptografia. O público que é, em geral, leigo em relação a ambos os tópicos, gradualmente vem se familiarizando com estas novas tecnologias e tem sido cada vez mais participativo, seja através do investimento em novas criptomoedas ou pela adoção de alguma solução.

Um dos elementos centrais para qualquer usuário dessas soluções, bem como para os que veem como único propósito nos cripto ativos o retorno financeiro, são as carteiras. Estas são nada mais do que softwares utilizados para a custódia de chaves criptográficas, bem como para interagir com as redes blockchain. Desde sua concepção, umas das principais preocupações no que tange às soluções financeiras criptográficas e descentralizadas é a segurança. E as carteiras são um elemento chave neste aspecto, em especial por serem nelas onde estão localizadas as chaves criptográficas que permitem o acesso aos ativos possuídos pelo usuário.

Ao longo dos anos, diversos casos de roubos e vazamento de chaves envolvendo corretoras de cripto ativos foram relatados, como em março de 2014, onde uma falha de segurança na corretora MT.GOX permitiu o roubo de

inúmeras chaves privadas de clientes, causando uma perda de aproximadamente 2600 BTC [Charoenwong and Bernardi 2021].

Devido à complexidade do tópico, bem como a abundância de carteiras disponíveis no mercado, com diferentes níveis de segurança implementados, reconhece-se a necessidade de auxiliar o usuário na escolha de uma solução segura e prática para uso diário. A partir de então surge a necessidade de uma melhor compreensão dos mecanismos de geração e armazenamento de chaves implementados nas carteiras de cripto ativos, permitindo uma tomada de decisão mais segura.

Este trabalho busca apresentar uma análise estática do código-fonte de carteiras de cripto ativos disponíveis no mercado, baseada em alguns parâmetros relevantes de segurança. A maioria das carteiras mais populares disponíveis atualmente implementa padrões de segurança largamente adotados pela indústria, mais notavelmente os BIPs (*Bitcoin Improvement Proposals*). A análise apresentada não apontou nenhuma carteira que possa ser considerada insegura, porém há diferenças objetivas quanto a alguns dos parâmetros de segurança observados, como por exemplo o tamanho e método de geração da entropia utilizada.

Este trabalho está organizado da seguinte forma: na Seção 2 é apresentada uma fundamentação teórica para melhor compreensão do trabalho; na Seção 3 são apresentados alguns trabalhos relacionados que contribuem para a compreensão do tema e para a análise de segurança. na Seção 4 é apresentada a metodologia adotada. na Seção 5 é apresentado o detalhamento de todos os parâmetros técnicos de segurança levantados, bem como alguns pontos relevantes em relação a cada uma das carteiras. Por fim, na Seção 6, são apresentadas as considerações finais.

2. Fundamentação Teórica

Carteiras determinísticas são aquelas nas quais todas as chaves privadas utilizadas são derivadas de uma única semente comum a todas elas. A semente em si é um número gerado por funções criptograficamente seguras, a partir das quais as chaves privadas são derivadas. Portanto, é possível realizar a restauração da carteira somente por meio do backup da semente, sem ter de armazenar também todas as chaves privadas utilizadas [Antonopoulos 2015].

Carteiras hierárquico determinísticas são um tipo específico de carteira determinística, tal como padronizado pelo BIP-32. Nelas as chaves são derivadas da semente por meio de uma estrutura em árvore, permitindo a derivação em inúmeros níveis, causando a criação de ramos inteiros de chaves privadas, as quais podem ser utilizadas para muitos propósitos diferentes. Essas são o tipo mais avançado de carteira determinística e constituem o padrão mais popular para implementação de carteiras de criptomoedas [Wuille 2012].

Códigos mnemônicos são um método de backup de sementes por meio da utilização de uma sequência de palavras. Eles foram projetados para facilitar a exportação e importação de carteiras determinísticas por meio do uso de uma lista que comumente possui 12 palavras escolhidas a partir de uma lista padronizada de 2048 itens, as quais irão gerar 128 bits de entropia [Palatinus et al. 2013].

A aleatoriedade é um componente essencial para muitas operações criptográficas.

A medida de aleatoriedade é chamada de *entropia*, que mede o quão incerto você está em relação a algum valor, e não quantos bits este mesmo valor possui. Uma sequência de 32 bits completamente aleatória possui 32 bits de entropia. Porém, uma sequência de 32 bits que só pode assumir um dentre quatro combinações possíveis de zeros e uns, possui apenas 2 bits de entropia [Ferguson and Schneier 2003].

As *Bitcoin Improvement Proposals* (BIPs) são documentos de design que fornecem informações à comunidade do Bitcoin ou descrevem um novo recurso a ser implementado por seu software, seus processos ou ambiente [Taaki 2013].

BIP-32 é uma BIP informacional que descreve as carteiras hierárquico determinísticas [Wuille 2012]. BIP-39 determina a geração de códigos mnemônicos para a criação de sementes utilizadas na criação de carteiras determinísticas. Seguindo esse padrão é possível obter uma semente a qual o usuário terá maior facilidade de recordar e transcrever. Este documento especifica a forma pela qual a frase mnemônica deve ser gerada, a lista de palavras (dicionário) a ser utilizada em sua geração, bem como sua conversão para a semente binária original [Palatinus et al. 2013].

3. Trabalhos relacionados

Em *Cryptocurrency Wallet: A Review* [Suratkar et al. 2020] é apresentado uma visão geral do funcionamento e dos tipos de carteiras de cripto ativos existentes. Os autores destacam a importância das características no momento de escolha da carteira, funções tais como moedas suportadas, como é feita a gestão das chaves, anonimidade e formas de recuperação da carteira. Porém o artigo não abrange aspectos técnicos de segurança com detalhamento suficiente.

Em *Security Analysis of Cryptocurrency Wallets in Android-based Applications* [He et al. 2020] são propostos ataques em dois aplicativos de cripto carteiras, e os resultados revelam vários riscos sérios de segurança nesses aplicativos, que destacam a necessidade e a importância de desenvolver carteiras de cripto-moeda seguras. Também são apresentadas informações sobre as principais falhas de segurança no sistema Android, assim como dados sensíveis possíveis de obter explorando essas falhas, evidenciando a possibilidade de ataques mesmo em carteiras consideradas seguras.

Em *Cracking Bitcoin wallets: I want what you have in the wallets* [Volety et al. 2019] é apresentada uma proposta de ataque a duas cripto carteiras, entretanto seu foco é a exploração de possíveis falhas no método de recuperação de uma carteira utilizando força bruta. Nas duas aplicações são utilizadas a recuperação através de frases mnemônicas, portanto os autores utilizaram a lista de palavras do BIP-39 para realizar inúmeras tentativas de recuperação com diferentes combinações dessas palavras. Também foi realizada uma investigação para detectar se as carteiras implementam alguma prevenção a esse tipo de ataque, bem como uma análise da viabilidade do ataque.

4. Metodologia

A escolha das carteiras a serem analisadas foi realizada levando em consideração dois fatores: i) acesso ao código-fonte do software; ii) popularidade no GitHub. Dessa forma, conseguimos selecionar as principais carteiras de código aberto do mercado e analisar suas implementações de forma detalhada. A escolha de acordo com o acesso ao código-fonte é motivada pela necessidade de avaliar aspectos técnicos de segurança, conforme

proposta do trabalho. Também levamos em consideração a popularidade do software em si e escolhemos como métrica o número de estrelas que seu repositório possui no GitHub, que é o mais popular site de hospedagem de serviços para desenvolvimento de software e controle de versões utilizando o Git. Para realizar a análise de segurança das carteiras, foram considerados os seguintes parâmetros técnicos de segurança:

- **Tamanho da Entropia** utilizada na geração de sementes e chaves privadas é um dos fatores mais relevantes no que tange à prevenção de ataques de força bruta.
- **Método de Geração da Entropia** é imprescindível que este dado seja obtido de fontes consideradas criptograficamente seguras, para garantir que realmente teremos a quantidade de bits de entropia necessários.
- **Tamanho da Semente** utilizada para derivação das chaves privadas (no caso de carteiras determinísticas).
- **Método de Geração da Semente** relacionado com o método de geração da entropia utilizada. Considerando a importância deste dado, iremos também avaliar como a entropia é utilizada para sua geração.
- **Tamanho da Chave Privada** também influencia a segurança e este tamanho tem correlação com a sua derivação (no caso das carteiras hierárquico determinísticas).
- **Método de Geração e Derivação das Chaves Privadas** que é aplicável somente no caso de *carteiras hierárquico determinísticas*. Dada a importância e sensibilidade das chaves privadas, o método de geração e derivação influencia diretamente na segurança da carteira.
- **Método de Armazenamento das Chaves Privadas**, pois se trata de um dado muito sensível, derivado a partir da semente (no caso de carteiras hierárquico determinísticas). É a partir dela que o usuário tem acesso aos ativos e realiza transações. Para um dado tão importante, diversas medidas de segurança devem ser adotadas visando impedir seu vazamento.
- **Métodos de Recuperação da Carteira**, pois é fundamental que o usuário final seja capaz de restaurar a carteira em outro dispositivo, caso necessário. Portanto, torna-se necessário avaliar cuidadosamente os métodos de recuperação disponibilizados. A possibilidade de realização de um backup dos dados sensíveis também é imprescindível.

O trabalho consiste em realizar uma avaliação estática de código-fonte em relação aos parâmetros técnicos de segurança elencados, fornecendo os links de acesso aos seus respectivos repositórios para possibilitar a verificação de cada um dos valores listados.

5. Análise

Levando em consideração os critérios de seleção de carteiras mencionados na seção Metodologia, foram escolhidas seis carteiras de cripto ativos para serem analisadas.

Trust Wallet é uma carteira de cripto ativos, disponível para Android, IOS e nos navegadores Chrome e Edge. A mesma possui suporte à várias blockchains. O mecanismo de geração de entropia escolhido, a leitura do arquivo /dev/urandom, gera entropia com um nível de segurança satisfatório. O tamanho da entropia utilizada também possui um valor suficiente para prevenir ataques de força bruta. Implementa os padrões BIP-32 e BIP-39, largamente adotados na indústria, dotando o software de mecanismos de geração de sementes e derivação de chaves robustos e confiáveis, bem como permite a recuperação

	Entropia		Semente		Chaves Assimétricas			Método de
	Tamanho	Geração	Tamanho	Geração	Tamanho	Geração	Persistência	Restauração
Trust	16 à 32 B [1] [2]	/dev/urandom [1] [2]	64 B	BIP-39	32 B	BIP-32	Cifrado (disco)	BIP-39 [1] [2]
OneKey	16 B [1] [2] [3]	getRandomValues [1] [2] [3]	64 B [1] [2] [3]	BIP-39 [1] [2] [3]	32 B	BIP-32	AsyncStorage ou IndexedDB. [1]	BIP-39
Wasabi	16 à 32 B [1] [2]	Random.GetBytes [1] [2]	64 B [1] [2]	BIP-39 [1] [2]	32 B	BIP-32	Cifrado (disco)	BIP-39
Electrum	132 bits	/dev/urandom ou CryptGenRandom [1]	Variável	Criação de frase mnemônica a partir da entropia	32 B	BIP-32	Cifrado (disco) AES-256-CBC	BIP-39
MyEther	16 à 32 B [1] [2]	randomBytes ou getRandomValues [1] [2]	64 B	randomBytes ou getRandomValues. [1] [2]	32 B	BIP-32	Memória	BIP-39
BitPay	16 B	randomBytes ou getRandomValues [1]	64 B	Criação de frase mnemônica a partir da entropia [1]	32 B	BIP-32	MongoDB, indexedDB ou disco [1]	BIP-39

Tabela 1. Comparativo dos parâmetros considerados em cada carteira analisada.

da carteira por completo através de uma sequência de palavras (mnemônicos do BIP-39). Destaque para a quantidade de moedas suportada pela carteira: 120 no total.

OneKey é uma carteira de cripto ativos, disponível em diversas plataformas tais como desktop mobile e web, possuindo também suporte a carteiras baseadas em hardware. Ela também implementa os padrões BIP-32 e BIP-39, conferindo um nível ainda maior de confiabilidade e segurança. A quantidade de moedas suportadas é consideravelmente inferior à da Trust Wallet, porém também conta com suporte à carteiras baseadas em hardware, tais como a Trezor e Ledger.

Wasabi Wallet é uma carteira de Bitcoins focada em privacidade. Está disponível exclusivamente para as plataformas desktop Windows, macOS e Linux. Suporta apenas Bitcoin. Foi implementada em C# e está disponível apenas para plataformas desktop. Todos os parâmetros de segurança analisados possuem valores adequados e são aderentes a padrões já estabelecidos na indústria.

Electrum é uma carteira que suporta exclusivamente Bitcoin e está disponível para plataformas desktop e para Android. A principal característica que distingue esta carteira das demais está relacionada ao tamanho da sua entropia. Ela não segue o BIP-39 e possui 4 bits de entropia a mais em comparação com as demais carteiras, porém com uma implementação e funcionamento similar, suportando frases mnemônicas e utiliza a mesma lista de palavras do BIP-39.

MyEtherWallet é uma carteira para navegadores e dispositivos Android e iOS. Implementada utilizando o framework JavaScript VueJs, ela fornece suporte às principais moedas baseadas em ETH. De maneira geral, esta carteira implementa os mesmos padrões e convenções dos projetos analisados anteriormente. Entretanto, por ser uma aplicação *client side*, ela possui uma alta dependência de bibliotecas de terceiros para implementar os padrões BIPs, incluindo uma forma de geração de carteira feita completamente através de uma biblioteca externa. O nível de segurança em relação à geração da entropia e semente é satisfatório, e seu principal diferencial está relacionado ao armazenamento de chaves privadas. No momento de sua inicialização a carteira realizará a geração de chaves privadas e a mesma permanecerá em memória.

BitPay é uma das principais aplicações de código aberto quando se trata de criptomoedas. Ela é extremamente completa quanto a funcionalidades, possuindo suporte a plataformas desktop e móveis. Assim como as anteriores, está carteira implementa de maneira ade-

quada todos os padrões recomendados e possui um nível de segurança satisfatório.

6. Considerações finais

Todas as carteiras analisadas neste trabalho cumprem os requisitos de segurança listados de forma satisfatória. Os padrões BIP-32 e BIP-39 são amplamente adotados pelos softwares e todos utilizam fontes criptograficamente seguras de entropia. São todos projetos já estabelecidos e seguros, apesar de haver diferenças em alguns dos parâmetros de segurança listados, como pode ser observado na Tabela 1.

Levando em consideração que não há diferenças significativas entre as carteiras no que tange à segurança, todas as carteiras analisadas podem ser consideradas seguras para o uso. Cabe ao usuário verificar quais moedas são suportadas por cada uma delas e sua disponibilidade em diferentes plataformas. Este é um trabalho em andamento, a próxima etapa da pesquisa irá analisar se a Trust Wallet pode ser aplicada em blockchains permissionadas tal como a BigChainDB, de forma a permitir uma integração com o Middleware Velluscinum [Mori Lazarin et al. 2023].

Referências

Antonopoulos, A. M. (2015). *Mastering bitcoin*. O'Reilly, Sebastopol CA, 1º edition.

Charoenwong, B. and Bernardi, M. (2021). A decade of Cryptocurrency 'hacks': 2011 – 2021. 91. http://doi.org/10.2139/ssrn.3944435.

Ferguson, N. and Schneier, B. (2003). *Practical cryptography*. Wiley, New York.

He, D., Li, S., Li, C., Zhu, S., Chan, S., Min, W., and Guizani, N. (2020). Security analysis of cryptocurrency wallets in android-based applications. *IEEE Network*, 34(6):114–119. https://doi.org/10.1109/MNET.011.2000025.

Mori Lazarin, N., Machado Coelho, I., Pantoja, C. E., and Viterbo, J. (2023). Velluscinum: A middleware for using digital assets in multi-agent systems. In Mathieu, P., Dignum, F., Novais, P., and De la Prieta, F., editors, *Advances in Practical Applications of Agents, Multi-Agent Systems, and Cognitive Mimetics. The PAAMS Collection*, pages 200–212, Cham. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-37616-0_17.

Palatinus, M., Rusnak, P., Voisine, A., and Bowe, S. (2013). BIP 39: Mnemonic code for generating deterministic keys. https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki.

Suratkar, S., Shirole, M., and Bhirud, S. (2020). Cryptocurrency wallet: A review. In *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, pages 1–7. DOI: 10.1109/ICCCSP49186.2020.9315193.

Taaki, A. (2013). BIP 1: Bip purpose and guidelines. https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki.

Volety, T., Saini, S., McGhin, T., Liu, C. Z., and Choo, K.-K. R. (2019). Cracking Bitcoin wallets: I want what you have in the wallets. *Future Generation Computer Systems*, 91:136–143. https://doi.org/10.1016/j.future.2018.08.029.

Wuille, P. (2012). BIP 32: Hierarchical Deterministic Wallets. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki.