SAFEDIME: Proposta de vertente evolutiva do *OPENDIME* para o armazenamento de chaves privadas de bitcoin.

Trilema Nakamoto

trilemabtc@protonmail.com

twitter: trilemabtc

Resumo: O *opendime* é um pequeno USB *stick* que permite ter o conceito de bitcoin ao portador, e quando o lacre é removido, a chave privada é revelada, a proposta de valor do *opendime* é baseada em ter o poder de passar o USB pra frente, sendo possível que qualquer um com acesso físico ao USB ter acesso as chaves privadas apenas violando o lacre. Na configuração inicial o usuário adiciona arquivos aleatórios para gerar entropia necessária para geração da carteira, o *opendime* é fantástico por cumprir o seu papel com maestria, porém nesse projeto, denominado carinhosamente de *safedime*, (a comunidade criará e aceitará o nome que ela achar melhor) tem o propósito de criar um novo conceito diferente: precisa continuar sendo um pequeno USB *stick*, porém, terá prova de criação, apenas o criador poderá abrir as chaves privadas, o idealismo disso não é para ser apenas ao portador, apenas o criador sendo também o portador terá acesso aos bitcoins.

Palavras chaves: Bitcoin, chave privada, segurança digital, hardwallet.

1. INTRODUÇÃO

O safedime, tem um objetivo muito claro, ser o bitcoin "físico" onde nem mesmo você tem acesso as suas chaves privadas, mas quando quiser retirar seus bitcoins para outro lugar, apenas você terá como resgatar suas chaves privadas, via prova de criação (um arquivo-chave). Diferente do que temos até agora o safedime não tem o objetivo de uma pessoa poder "passar ele pra frente" ele tem muito mais a visão de ser um cofre pessoal físico e frio, mas que só quem criou pode abrir, acumule satoshi's, mantenha sua carteira fria, não se preocupe em precisar decorar sua chave privada, o arquivo necessário para abrir a chave privada (arquivo chave) pode ser uma foto sua de família, uma foto de seu filho(a), ou um arquivo qualquer. Você poderá manter o arquivo-chave online ou guardar como quiser, porque seguindo as instruções de criação da carteira, ele só servirá como "senha" para o seu próprio safedime, poderá teoricamente ter dezenas de cópias do arquivo-chave, em tudo quando for nuvens e serviços de hospedagem de arquivos e mesmo assim, ninguém poderá ter acesso ao seus bitcoins mesmo com acesso físico da carteira, se não saber qual arquivo seu que é o arquivo-chave, mesmo assim teremos recomendações extras de segurança sobre como guardar o arquivo-chave, entre outras medidas. O nível de segurança que esse tipo de projeto pode trazer é um dos maiores, mas com um pouco de conhecimento e criatividade do usuário final, esse projeto se torna extremamente seguro, se o usuário final sair contando para os outros qual é e onde está seu arquivo, aí também não adiantaria de nada para a proposta de valor desde projeto.

2. MOTIVAÇÃO

Na busca pela maior liberdade dos indivíduos e da minha própria, pensei na criação de um modelo que possa oferecer uma "tangibilidade para o bitcoin" só que sem o risco de ser confiscável por qualquer pessoa ou entidade que possua fisicamente seu hardware, pesquisando sobre, descobri que basicamente todos os padrões de software e hardware necessários para criação do que estou propondo já existem e é factível a realização desde projeto. A prova de criador é muito empolgante, porque adiciona uma camada essencial de segurança para o "bitcoin físico", diferente da chave privada o arquivo-chave só serve para você, se alguém posta uma privada na internet estará praticamente f*dida, mas poste um arquivo-chave na internet e nada acontece, pois aquilo não serve pra ninguém além de você.

3. CHAVE ASSIMÉTRICA

O bitcoin foi criado para ter sua comunicação ser maneira de criptográfica assimétrica, ou seja, chaves privadas e chaves públicas funcionando como algo perto de uma assinatura digital, isso funciona muito bem, porém, o processo de armazenamento das chaves privadas não acontece de maneira tão assimétrica, qualquer pessoa que tiver acesso as suas chaves privadas poderá subtrair os fundos de sua carteira. Esse projeto trás ao bitcon uma maneira de criação e armazenamento das chaves privadas de bitcoin de maneira assimétrica.

4. CONFIGURAÇÃO

Para configurar um novo safedime, precisará colocar arquivos para gerar entropia da mesma maneira que acontece hoje com o opendime, a sutil diferença acontece com adição de uma nova etapa: "escolha aqui seu arquivo-chave". Nessa etapa, deve conter o botão de upar o arquivo, mas deve conter toda a informação necessária para alertar sobre a importância daquele arquivo e que sem ele lá no futuro seria impossível recuperar os fundos, quando a pessoa adiciona uma arquivo-chave, o sistema irá identificar qual o SHA-256 daquele arquivo, e adicionará essa informação como senha do arquivo criptografado que será gerado quando o lacre do safedime for removido.

5. BACKUP

É recomendável que seja facilitado a criação de mais de um mesmo safedime, com o usuário colocando a mesma entropia e mesmo arquivo-chave, criados de maneira simples na mesma hora, assim recomendando aos usuários para criar pelo menos 3 safedime exatamente iguais, para ter uma maior segurança física, uma vez que a pessoa poderá diversificar onde irá guardar seus safedimes, se o estado ou outra organização tomar seu safedime, mesmo que ele não possa roubar seus fundos, você ainda precisa ter seu safedime para recuperar suas chaves, então é bom ter mais de um, e em lugares diferentes.

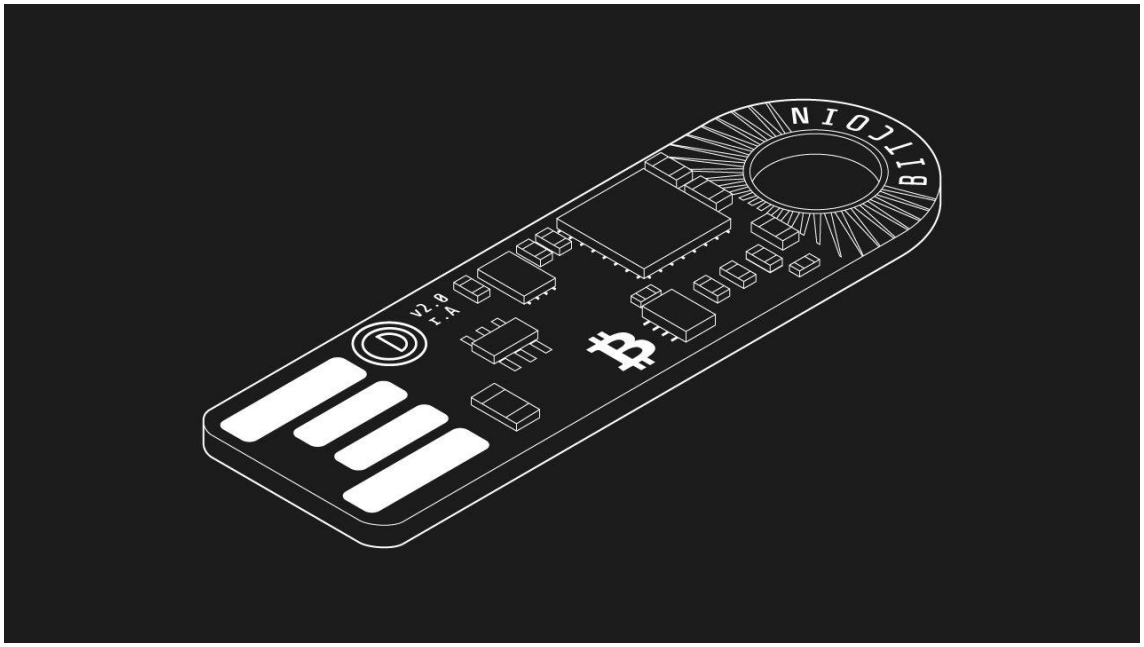
6. ESTADOS DE UM SAFEDIME

Existem quatro estados para um Safedime:

- **Nova unidade** (ainda não tem um endereço bitcoin)
- **Selado** (normal; tem um endereço de pagamento)
- **Não selado** (um arquivo criptografado é gerado, mas apenas o arquivo-chave pode abrir essa criptografia, aí sim alcançará o próximo estado)
- **Revelado** (a chave privada é revelada; varra seus fundos)

O opendime tem 3 estados, o que o safedime faz é adicionar um novo estado, uma ponte para abrir as chaves privadas, apenas via a prova de criador (arquivo-chave)

Figura 1 (design de um USB *stick*)



Fonte: Opendime

7. FORK

Toda a infraestrutura de hardware necessária para a execução de um fork parece estar em pleno funcionamento, o que precisa fazer é programar para quando o lacre for removido ao invés de gerar um arquivo com as chavesprivadas.txt, gere um arquivo criptografado que só possa ser aberto com o arquivo-chave que o usuário configurou lá no início, e que apenas dentro desse arquivo criptografado tenha as chaves privadas da carteira.
A melhor maneira de fazer isso com plena segurança deverá ser criada para não deixar brechas de segurança, mas a comunidade está muito evoluída nesses sentidos, e acredito que o próprio livre mercado fará isso, o melhor projeto de código aberto que consiga fazer isso, junto a comunidade, será mercadologicamente vencedor, inclusive podendo ser a própria *opendime* fazendo o fork dela mesma, já que tem praticamente todos os elementos necessários.

8. SEGURANÇA

8.1 Projeto

O lacre de segurança é essencial para manter um grande nível padrão de segurança, na prática, se esse tipo de segurança não for implementado, algum invasor ou máquina infectada poderia roubar o arquivo, mesmo que criptografado ele poderia tentar via força bruta achar qual seu arquivo que resolva a "charada criptográfica" para revelar as chaves privadas. Com o lacre protegido via hardware, se torna impossível um ataque de força bruta, mesmo se uma maquina estiver infectada.

8.2 Pessoal

Só recomendo remover o lacre de segurança, apenas no mesmo dia e hora que for remover os fundos, porque mesmo que tudo seja criptografado, os elementos de sua carteira perdem as propriedades de segurança da parte de hardware, ficando apenas com proteção via software, e se todos os elementos para reconstrução da sua chave privada estiverem em uma mesma maquina ou com mesmo atacante, seus recursos estariam vulneráveis.

8.3 Para Nerds

(lembrete de segurança, não entrar muito nisso sem não entender exatamente o que está fazendo)

Leve modificação de arquivo

Mesmo a parte do arquivo-chave sendo uma etapa adicional de segurança, a maestria na segurança só poderá ser atingida, por usuários mais avançados e criativos, pode por exemplo, abrir uma foto em um bloco de notas, e na última virgula, substituir por 1 ponto, então você configuraria o safedime com esse arquivo modificado, e depois de configurar retira o ponto e volta pra virgula, assim você continua como uma foto inofensiva mas agora nem esse arquivo resgata suas chaves privadas de imediato, só bastaria você trocar a última virgula por um ponto novamente, e aquilo se torna o arquivo-chave novamente (lembrando que esse é só um exemplo, e que é preciso tomar cuidado em alterar arquivos, uma virgula errada ou até um espaço a mais, e a pessoa nunca mais recuperaria os recursos). Nesse exemplo, tudo que você precisaria era da foto, e também lembrar que tem que trocar a última virgula por ponto na antes de restaurar a chave privada do seu safedime.

Senha

Não quer esconder o arquivo-chave em uma foto? É possível esconder até mesmo na sua mente, um arquivo.txt contendo apenas uma senha, sempre vai gerar o mesmo SHA256sum se usar a mesma senha, independente de quando foi criado, se você decorar uma senha boa e forte e usar em um arquivo.txt com essa senha como arquivo-chave, poderá apagar o arquivo-chave depois de configurado, já que pode recuperar esse arquivo-chave fazendo um novo arquivo da mesma maneira. (novamente uma vírgula errada, e já era).

PGP

Para usuários mais avançados temos o PGP, para criptografar arquivos, mas se você chegou nesse ponto na segurança da informação, nem mesmo precisa de um safedime.

9. CONSIDERAÇÕES FINAIS

O quão bom é o projeto ou o quão ele ou as vertentes que surgirão a partir dele gerarão de valor pra humanidade, só depende da livre iniciativa e o livre mercado dizer essa resposta ao longo do tempo, tudo que ajudar a desenvolver o bitcoin de maneira saudável é bem-vindo, espero que minha contribuição tenha utilidade para um mundo mais descentralizado e melhor. Lembrando que só é possível enxergar longe, estando nos ombros de gigantes. As considerações sobre segurança devem ser tomadas, só compre algo que foi inspirado nesse projeto se for de profissionais qualificados e se possível com muito tempo de experiencia nesse tipo de coisa, se a indústria quiser comercializar isso, fique à vontade, para criar e desenvolver em cima disso, as ideias são livres e não são cobradas, e se quem se capitalizar quiser pagar royalties, fique à vontade para entrar em contato, verifique meu pgp, eu acredito no livre mercado e que as coisas se auto regulam, o valor que você gera para sociedade de alguma maneira volta. Somente criando isso com grande nível de segurança de software e hardware será possível que a ideia vá para frente, no desenvolvimento de uma sociedade melhor e mais funcional.

Referências

OPENDIME, URL: **opendime.com** e **https://github.com/opendime** 2021.

OLIVEIRA, Ronielton Rezende. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Segurança Digital [Revista online]**, v. 31, p. 11-15, 2012.

NAKAMOTO, Satoshi. Bitcoin whitepaper. **URL: https://bitcoin.org/bitcoin.pdf - (Дата обращения: 17.07. 2019)**, 2008.