SAFEDIME: Proposal for an evolutionary aspect of the *OPENDIME* for bitcoin private key storage.

Trilema Nakamoto

trilemabtc@protonmail.com

twitter: trilemabtc

Abstract: Opendime is a small USB stick that allows you to have the concept of bitcoin to the bearer, and when the seal is removed, the private key is revealed, the value proposition of opendime is based on having the power to pass the USB forward, making it possible for anyone with physical access to the USB to access the private keys just by breaking the seal. In the initial configuration, the user adds random files to generate the entropy needed to generate the portfolio, the opendime is fantastic for fulfilling its role masterfully, but in this project, affectionately called safedime, (the community will create and accept the name it sees fit) has the purpose of creating a new different concept: it needs to remain a small USB stick, however, it will have proof of creation, only the creator will be able to open the private keys, the idealism of this it's not meant to be bearer only, only the creator being also the bearer will have access to bitcoins.

Keywords: Bitcoin, private key, digital security, hardwallet.

1. INTRODUCTION

Safedime has a very clear objective, to be the “physical” bitcoin where you don't even have access to your private keys, but when you want to remove your bitcoins elsewhere, only you will be able to redeem your private keys, via proof of creation (a key file).
Unlike what we have so far, safedime does not have the objective of a person being able to "pass it forward", it has much more the vision of being a physical and cold personal safe, but that only those who created it can open it, accumulate satoshi's, keep your cool wallet, don't worry about having to memorize your private key, the file needed to open the private key (key file) can be a family photo of you, a photo of your child, or any other file. You can keep the key file online or save it as you like, because following the wallet creation instructions, it will only serve as a “password” for your own safedime, you can theoretically have dozens of copies of the key file, in everything when it is clouds and file hosting services and even so, no one will be able to access your bitcoins even with physical wallet access, if they do not know which file is the file. -key, even so, we will have extra security recommendations on how to save the key file, among other measures. The level of security that this type of project can bring is one of the greatest, but with a little knowledge and creativity from the end user, this project becomes extremely secure, if the end user starts telling others what and where his file is, then it wouldn't do any good for the value proposition of this project either.

2. MOTIVATION

In the search for greater freedom for individuals and for my own, I thought about creating a model that could offer a "tangibility for bitcoin" but without the risk of being confiscated by any person or entity that physically owns its hardware, researching about, I found that basically all the software and hardware standards needed to create what I'm proposing already exist and it's feasible to carry out this project. The creator proof is very exciting because it adds an essential layer of security to the “physical bitcoin”, unlike the private key the key file is just for you, if someone posts a toilet on the internet they're pretty much f*cked up, but they post a key file on the internet and nothing happens, because that doesn't work for anyone but you.

3. ASYMMETRIC KEY

Bitcoin was created to have its communication be a way of asymmetric cryptography, that is, private keys and public keys working as something close to a digital signature, this works very well, however, the process of storing private keys does not happen in such a way asymmetric, anyone who has access to your private keys can steal the funds from your wallet. This project brings to bitcon a way to create and store bitcoin private keys asymmetrically.

4. CONFIGURATION

To configure a new safedime, you will need to place files to generate entropy in the same way that happens today with opendime, the subtle difference happens with the addition of a new step: “choose your key file here”. In this step, it must contain the button to upload the file, but it must contain all the necessary information to warn about the importance of that file and that without it there in the future it would be impossible to recover the funds, when the person adds a key file, the system will identify which is the SHA-256 of that file, and will add this information as the password of the encrypted file that will be generated when the safedime seal is removed.

5. BACKUP

It is recommended that the creation of more than one safedime be facilitated, with the user placing the same entropy and the same key file, created simply at the same time, thus recommending users to create at least 3 exactly the same safedime, to have greater physical security, since the person can diversify where they keep their safedime, if the state or other organization takes their safedime, even if they can't steal your funds, you still need to have your safedime to retrieve your keys, so it's good to have more than one, and in different places.

6. STATES OF A SAFEDIME

There are four states for a Safedime:

• New unit (does not have a bitcoin address yet)

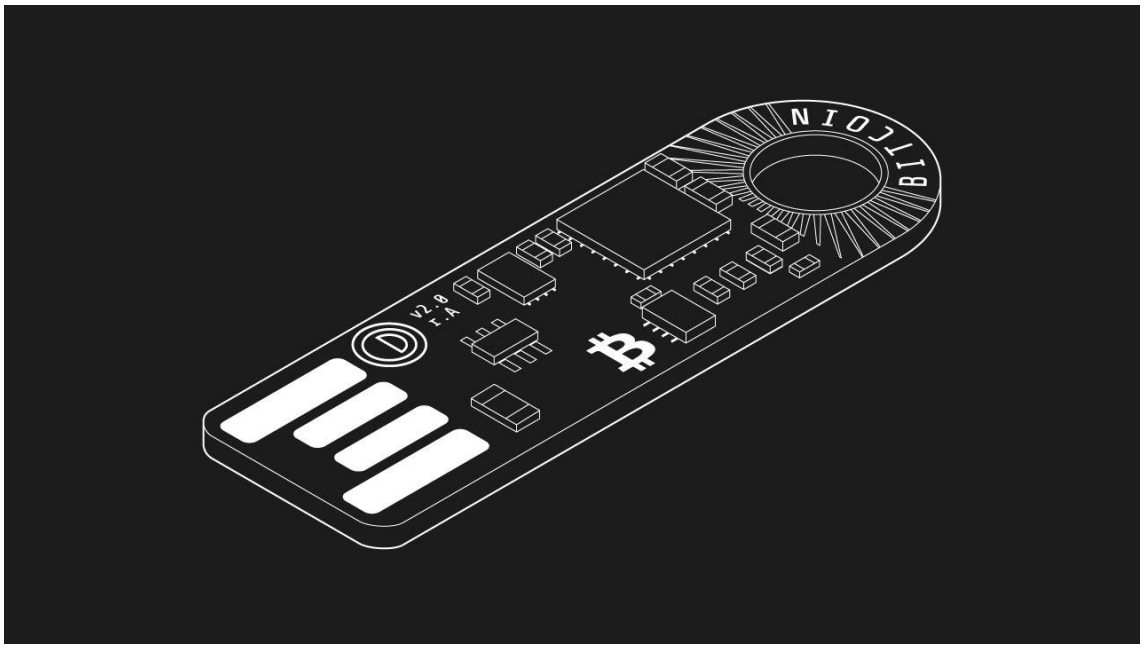
• Sealed (normal; has a payment address)

• Unsealed (an encrypted file is generated, but only the key file can open this encryption, then it will reach the next state)

• Revealed (private key is revealed; sweep your funds)

Opendime has 3 states, what safedime does is add a new state, a bridge to open the private keys, just via the creator proof (key file)

Figure 1 (design of a USB *stick*)



Font: Opendime

7. FORK

All the hardware infrastructure needed to run a fork seems to be in full operation, what you need to do is program so when the seal is removed instead of generating a file with privatekeys.txt, generate an encrypted file that can only be open with the key file that the user configured there at the beginning, and that only inside this encrypted file has the private keys of the wallet. The best way to do this with full security is to be designed to leave no security breaches, but the community is very evolved in these respects, and I believe the free market itself will do that, the best open source project that manages to do this, together with the community, will be a winner in the market, even being able to be the opendime itself making its own fork, since it has practically all the necessary elements.

8. SECURITY

8.1 Project

The security seal is essential to maintain a high standard level of security, in practice, if this type of security is not implemented, some intruder or infected machine could steal the file, even if encrypted, it could try via brute force to find out which file would solve the “cryptographic riddle” to reveal the private keys. With the seal secured via hardware, a brute force attack is impossible, even if a machine is infected.

8.2 Personal

I only recommend removing the security seal, only on the same day and time that you remove the funds, because even if everything is encrypted, the elements of your wallet lose the security properties of the hardware part, leaving only protection via software, and if all the elements for rebuilding your private key are on the same machine or with the same attacker, your resources would be vulnerable.

8.3 For Nerds

(safety reminder, don't go into this too much without understanding exactly what you're doing)

Slight file modification

Even though the key file part is an additional security step, mastery of security can only be achieved, by more advanced and creative users, you can, for example, open a photo in a notepad, and in the last comma, replace with 1 point, so you would configure safedime with this modified file , and after setting it removes the period and returns to a comma, so you continue as a harmless photo but now even this file doesn't rescue your private keys right away, you just need to change the last comma for a period again, and that becomes the file -key again (remembering that this is just an example, and that you have to be careful in changing files, a wrong comma or even an extra space, and the person would never recover the resources). In this example, all you would need was the photo, and also remember that you have to change the last comma for dot in before restoring your safedime's private key.

Key

Don't want to hide the key file in a photo? It is possible to hide even in your mind, a .txt file containing only one password, will always generate the same SHA256sum if you use the same password, regardless of when it was created, if you memorize a good strong password and use it in a file. txt with this password as the key file, you can delete the file-key once configured, as you can retrieve this key file by making a new file in the same way. (again a wrong comma, and that's it).

PGP

For more advanced users we have PGP, to encrypt files, but if you've reached that point in information security, you don't even need a safedime.

9. FINAL CONSIDERATIONS

How good the project is or how it or the strands that will emerge from it will generate value for humanity, only depends on free enterprise and the free market saying this answer over time, everything that helps to develop bitcoin in a way healthy is welcome, I hope my contribution will be useful for a more decentralized and better world. Remembering that it is only possible to see far, standing on the shoulders of giants. Security considerations must be taken, only buy something that was inspired by this project if it is from qualified professionals and if possible with a lot of experience in this type of thing, if the industry wants to market it, feel free to create and develop on top of it, ideas are free and are not charged, and if those who capitalize want to pay royalties, feel free to get in touch, check my PGP, i believe in the free market and that things regulate themselves, the value you generate for society somehow comes back. Only by creating this with a high level of software and hardware security will it be possible for the idea to go forward, in the development of a better and more functional society.

References

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.