Guardian WallETH

Idea

Building a social recovery wallet that can provide better security and a user-friendly recovery process. We want to design a solution that reduces the number of losses and thefts taking place, without requiring all cryptocurrency users to turn personal security into a full-time hobby, which is highly valuable for the industry.

Problem

Wallet security issues have been a thorn in the side of the blockchain ecosystem almost since the beginning. Cryptocurrency losses and thefts are rampant even now after a decade of bitcoin launch.

One analysis of the Bitcoin ecosystem suggests that 1500 BTC may be lost every day - over ten times more than what Bitcoin users spend on transaction fees, and over the years adding up to 20% of the total supply. The stories and the numbers alike point to the same inescapable truth: **the importance of the wallet security problem is great, and it should not be underestimated**.

Hardware wallets

1. If you buy a hardware wallet, you are trusting a number of actors that were involved in producing it - the company that designed the wallet, the factory that produced it, and everyone involved in shipping it who could have replaced it with a fake.
2. **Still a single point of failure**: if someone steals your hardware wallet right after they stand behind your shoulder and catch you typing in the PIN, they can steal your funds. If you lose your hardware wallet, then you lose your funds

Mnemonic phrases

1. Many wallets, hardware, and software alike have a setup procedure during which they output a *mnemonic phrase*, which is a human-readable 12 to 24-word encoding of the wallet's root private key.
2. If you lose your wallet but you have the mnemonic phrase, you can input the phrase when setting up a new wallet to recover your account, as the mnemonic phrase contains the root key from which all of your other keys can be generated.
3. **Mnemonic phrases are good for protecting against loss, but they do nothing against theft.** Maintaining a mnemonic phrase and not accidentally throwing it away is itself a non-trivial mental effort.

MultiSig Wallets

1. You could have wallets with 3 keys and you need approval from two of them to perform a transaction.
2. This is reasonably secure: there is no single device that can be lost or stolen which would lead to you losing access to your funds.
3. But usability is a challenge as you need approval from two keys to perform each transaction.

Solution

What we need is a wallet design that satisfies three key criteria:

- **No single point of failure**: there is no single thing (and ideally, no collection of things that travel together) that, if stolen, can give an attacker access to your funds, or if lost, can deny you access to your funds.
- **Low mental overhead**: as much as possible, it should not require users to learn strange new habits or exert mental effort to always remember to follow certain behavior patterns.
- **Maximum ease of transacting**: most normal activities should not require much more effort than they do in regular wallets (eg. Status, Metamask...)

Social recovery

A social recovery system works:

1. There is a single "signing key" that can approve transactions
2. There is a set of at least 3 (or a much higher number) ***guardians***, of which a majority can cooperate to change the signing key.

Architecture

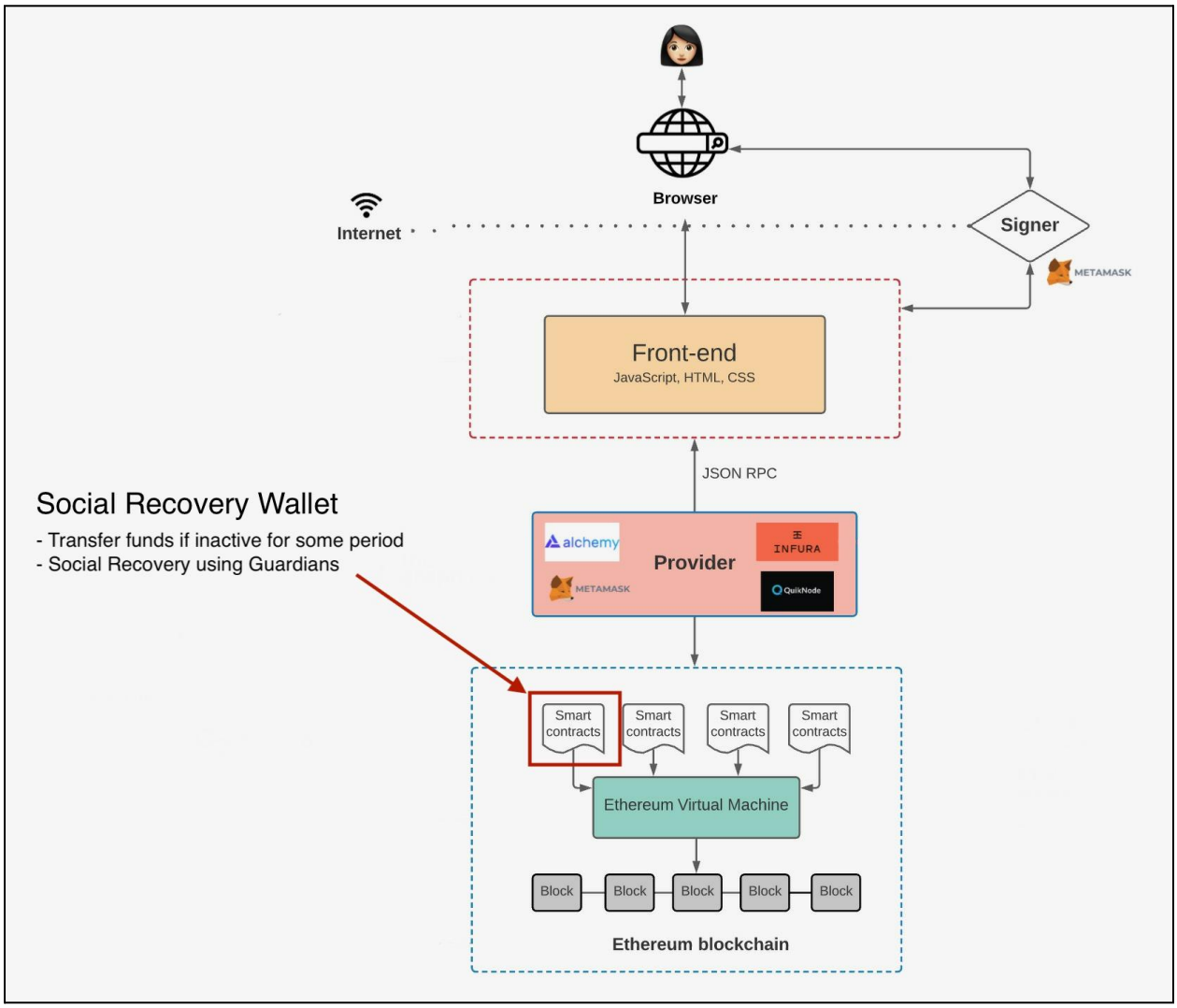

Figure 1: Architecture of the dApp

Core Features and Functionality:

- Social Recovery Wallet
- Transfer of ownership after an inactivity period.
- Set a limit for transactions
- Lock Wallet for some time
- Multisig Wallet

Social Recovery Wallet

It has seen that often people lose access to their hot crypto wallets (one of the non-custodial wallets, e.g. MetaMask) when

- they lose their computing device
- their computing devices crash because of hardware failure or software failure
- they upgrade their computing device
- if an account is compromised, etc.

The above scenarios can happen at any time and if the user of the wallet doesn't have their secret recovery phrase then it means the user has lost all their funds. However unlikely this situation might seem, this is a real possibility and has happened to lots of people.

The concept of guardians will be incorporated into our smart contract wallet so we can always retrieve those funds. At the time of registration, the user will be prompted to add guardians (at least three). For the guardian to be added, they will need to provide their wallet address and a password. The guardian will use this password when he or she votes to transfer ownership of the smart contract wallet to another non-custodial wallet. A hash of the wallet address and the password will be stored on the blockchain. By doing so, we will ensure that no private information is kept on the blockchain.

We will utilize ***zero-knowledge proof*** in order to prevent the address of the guardian from being revealed on-chain.

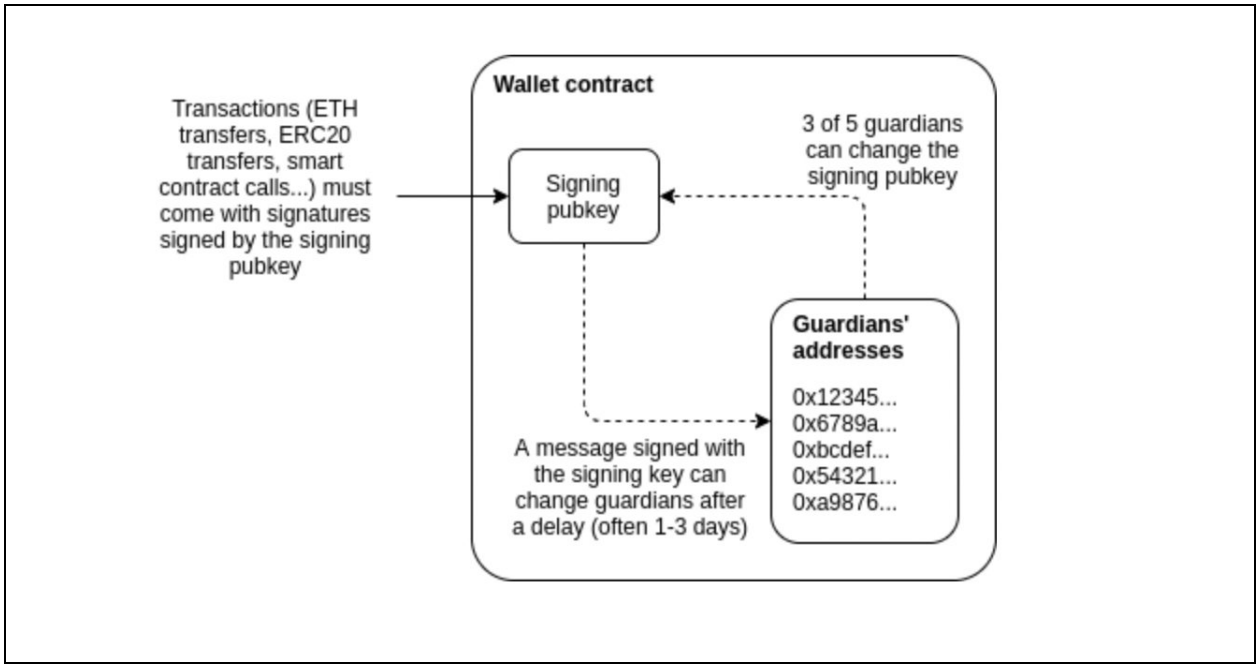

Figure 2: Wallet Recovery Using Guardians

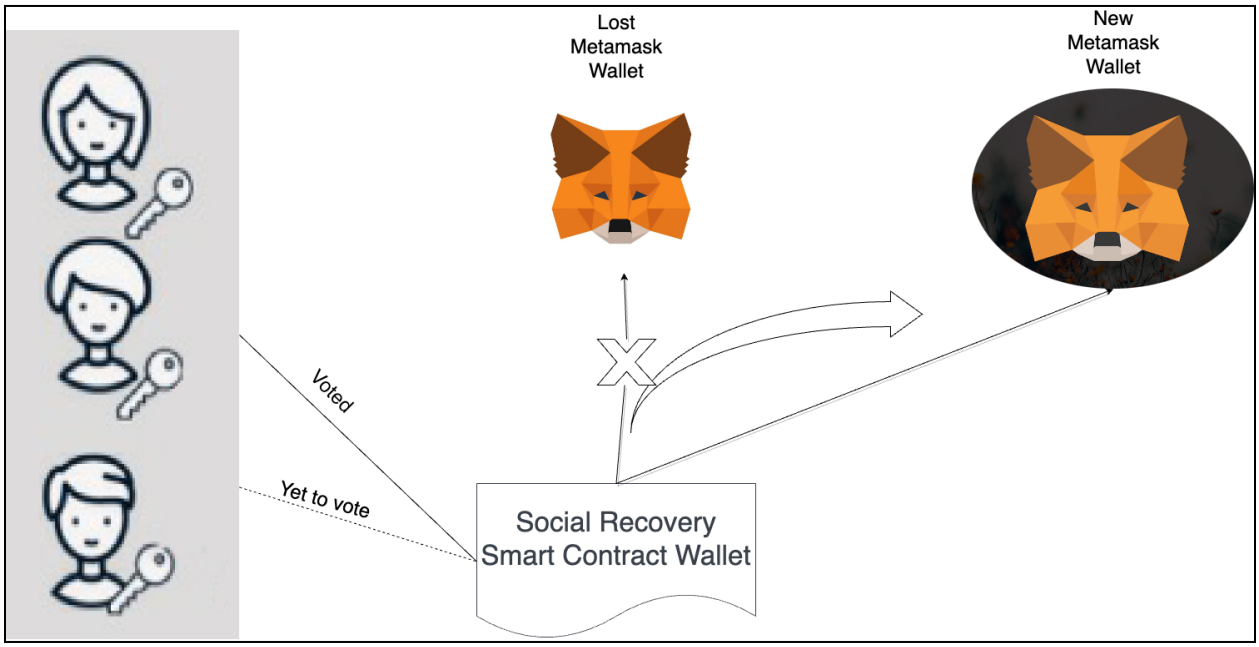

Figure 3: Wallet Recovery Mechanism

Transfer of ownership after an inactive period

It has been observed that people usually use multiple non-custodial wallets for different purposes. Their multiple wallets include two or three primary wallets, which they access frequently, and they maintain a backup of these mnemonic keys and can recover them with minimal effort. In the case of other wallets that they do not use regularly, their credentials are prone to theft, resulting in the loss of the funds associated with those wallets.

As a solution, we are asking users to provide an inactive period. Following this period, ownership of this smart contract wallet is transferred to one of the primary wallets they use on a daily basis.

The user will be asked for this information during the creation of the smart contract wallet. Once they enter the inactive period, they will be asked to enter the primary wallet address to which they would like ownership of this smart wallet transferred once this set inactive period is over.

Set withdrawal limit

In some cases, it may be desirable to limit transactions, such as:

- During their travels
- Visiting a new location
- An unsafe environment worries them

However, they would still want to carry out their day-to-day transactions.

We offer them a feature to limit their withdrawals, so they can avoid falling into one of the scenarios above. This feature would be enabled by entering a transaction limit on the front end of the application.A limit can only be removed after four hours after it has been set.

Lock Wallet

Occasionally, a user may wish to lock their wallet completely in order to prevent any activity from taking place in the wallet. Users can use this feature by clicking on the lock button and entering the time for which they wish to lock their wallet. Consequently, they can rest assured that their wallets will not be misused.

Multi Signature Wallet

In some cases, it is desirable to have multiple levels of approval for spending cryptocurrencies. As the name suggests, multi-signature wallets require authorisation of transactions through multiple keys, meaning that a group of users is required to sign to approve a transaction.

Numerous people claim that the multisignature user experience is not sufficiently simplified for average users, so only those with a thorough understanding of the process should bother using it. As a result, we provide this feature as an optional feature aimed at advanced users. This is because normal users are not interested in navigating through multiple transactions every time a transaction needs to be conducted. The purpose of this feature is to attract a group of users/organizations that are interested in using this smart contract wallet but they are located throughout different geographical regions.

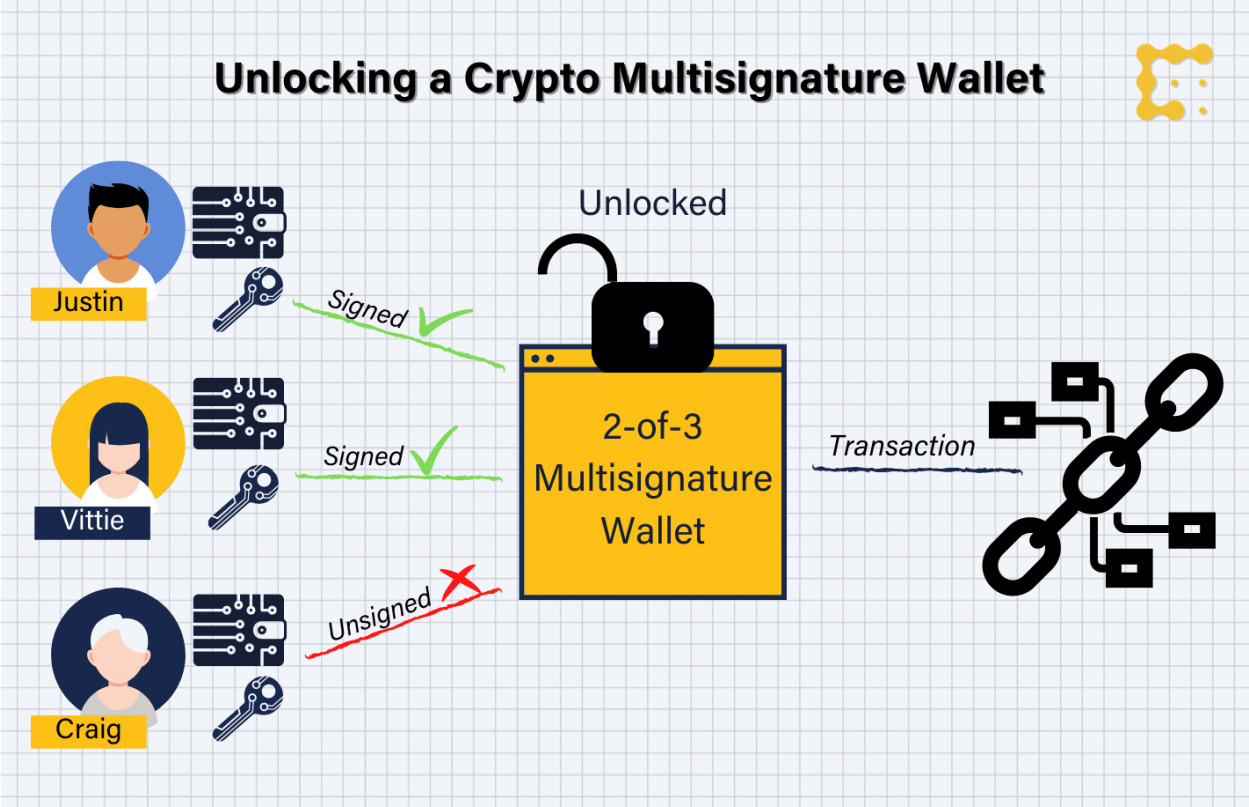

Figure 4: Unlocking a Multi Signature Wallet

Terminology

- **Smart Contract Wallet** - It's a wallet with funds secured by smart contracts. This is a bit different from conventional wallets, where funds are secured by private keys. For more, please read here.

- **Guardian -** A Guardian can be anyone a user trusts. In most cases, it is the user's friends, family, and colleagues.
- **Zero Knowledge Proof -** In a zero-knowledge proof, you prove the truth of a statement without revealing its contents or how you discovered it. In order to achieve this, zero-knowledge protocols rely on algorithms that take some data as input and return a true or false value.
- **Social Recovery Methods -** The recovery process can be expedited with the help of friends, family, colleagues, or others whom you can rely on.
- **Non-custodial Wallets -** It is a type of Blockchain wallet that lets you be your own bank. This implies that users have full control over their funds and the associated private key. If you want to know more about blockchain wallets, you can read here.
- **Primary Wallets -** It is a subset of wallets owned and used by a user for day-to-day transactions.
- **Inactive Period -** You have not made any transactions on your account during this period. It is possible that you have forgotten about the account or that you have lost access to it.

Future Work

- Money Lending among friends
-