Current wallet recovery mechanisms always come with a big trade-off. Either you rely 100% on yourself (push the responsibility to the user), or you sacrifice sovereignty by trusting your private key to some centralised entity.

In this document, I present Sovereign Social Recovery, a non-custodial recovery mechanism that tries to bring the best of both worlds.

Quick Philosophical Notes:

One of the core values of crypto is the empowerment towards the individual. Empowerment can mean many things, but one particular that we can all agree with, is the true ownership of assets. That is why winning the fight of non-custodial wallets is (in my opinion) one of the most important challenges there is. If crypto flourishes with the majority of the users using custodial wallets, the only thing we accomplished is changing the name of “JPMorgan Chase” to “Binance”.

1. Introduction

A recovery mechanism is simply the act of getting access to your funds in case the main device is lost.

We can split the current recovery mechanisms into two main conceptual categories:

Custodial

A custodial recovery mechanism means to delegate the responsibility of managing the private key to someone else (usually the wallet’s company).

Pros:

- Ease of use

: If a user looses his/her device, a simple two factor authentication restores the account.

- Delegation of responsibility:

A lot of users don’t want the responsibility of keeping the seed phrase under their control (they want to call somebody if something goes wrong).

Cons:

- Censorship:

The most obvious one is that your funds are completely censorable. Killing one of the core principles of crypto.

- Centralising Power:

Another super under-hyped issue with having a custodial wallet, is that the companies behind have complete access to the funds. While today is not a problem, in the future, it can make these companies operate the same way as banks do today. They can start lending the money in order to earn more interests, and re-create the same system that we have today. While this may sound impossible now, I find it very likely to happen in the future. Power corrupts.

Any wallet service that has access to your private key, is by default custodial.

Non-Custodial

In a non-custodial mechanism, you can share the recovery responsibility with other parties, but the key point here is that no one should be able to take away your funds without your consent.

Some basic examples are:

Seed-phrase backup:

Probably this is the most common one. In this scenario, you write some words (usually 12 or 24) and keep them safe. In the case that you loose your main device, you can easily restore your wallet by entering those words. This is compatible with almost all wallets, so you can easily migrate from one to another.

Pros:

- Sovereign:

Only you have access to your funds (unless you get hacked).

- Liberal:

You can easily migrate your wallet to another one, just by entering the seed phrase.

Cons:

- UX:

It doesn't feel that modern to write down on a piece of paper (metal?) some words.

- Safety:

It adds extra security concerns. If someone steals the seed phrase, they immediately have access to your funds. If you loose it with your device, there is no way to recover your funds again.

- Responsibility:

You are 100% responsible. If something goes wrong, there is no one to call. Responsibility is usually good, but for systems that hold so much economic value, the responsability should be on the applications and systems, not so much on the user.

Multi-Sig:

Multi-sigs wallet like Gnosis are extremely safe and have provided enormous value to the ecosystem. I believe these type of wallets are very adequate for managing DAO's reserves and people with large amounts of crypto that want to park their funds there. For everyday users, they are not very practical.

There is another newer option called social recovery. This option can be custodial, non-custodial, or semi-custodial as you will see.

Social Recovery

Social Recovery is a mechanism to get access to your funds (in case you loose the main device) by having guardians. I believe this mechanism is a good way forward, but still has many flaws. Allow me to explain them.

1. Extra Security Considerations:

By having guardians you are adding extra security complexity. If the majority of your guardians conspire against you, they would be able to steal the funds. And I am not talking from a maxi perspective, I am talking from a pragmatic one. Not only can they steal by having bad intensions, but they can also get socially engineered, or even loose their own wallets.

1. Extra Complexity:

A lot of users don't have a couple of people to trust their life savings with. Even if they have members they can trust in a moral way, very likely not in a "keep you wallet safe" way.

Some counter-arguments I receive about this are the following:

1. Use a centralised guardian:

Using a centralised guardian is just a normal centralised wallet. The mental model we need to have is, if a government forces the guardians to take the user's funds, can they ? If they can, then is it really non-custodial ?

1. Put yourself as a guardian:

Another point that I commonly hear is to have another wallet as backup. I think this setup does not make sense at all. If you have one wallet as a backup, then that wallet is your weakest link. Why then use your social recovery wallet instead of your only guardian wallet ? You are only introducing more risks.

With all of these points in consideration, let me introduce Sovereign Social Recovery.

II. Sovereign Social Recovery

Sovereign social recovery has a very similar implementation as social recovery but with one big difference: it predetermines the next owner in advance.

The big problem with social recovery as pointed out previously, is that guardians can change the owner to a new address. This new address is an input parameter in a function, allowing the guardians to choose whatever address they please.

With sovereign social recovery, the guardians can only recover the wallet to the predetermined address, which the real owner holds.

Let's go through an example:

- Alice creates a smart contract wallet in her mobile device. The signing key (private key) is encrypted in the mobile's hardware (the seed phrase is not shown to avoid social engineering attacks).
- Alice chooses a set of guardians or the wallet defaults to a centralised one (it doesn't matter, guardians are not able to

access Alice's funds).

- The recovery owner key pair is created and the address is stored in a "recoveryOwner" variable in the wallet's contract. The seed phrase can be shown to Alice or saved in different cloud providers. This seed phrase is NOT THAT CRITICAL, Alice can loose it and nothing happens (she can replace the recovery owner). It is completely worthless if someone steals it (except the guardians).

Here is a semi pseudo-code sample for a better understanding:

It can also be recovered in a safer way. Just in case an attacker has the recovery key and it is just waiting for the owner to loose the device:

*You can add an additional function so the guardians can't lock the wallet forever pretty easily (it can be implemented in multiple ways).

Let's recap the main security considerations:

1. The only way that guardians can access the wallet's funds is by maliciously betraying the user AND stealing the recovery seed phrase. The probabilities that the guardians do the former are not that low, if you add the later, it becomes extremely unlikely.
2. If the user looses access to the recovery seed phrase, nothing happens. The user can generate a new one and change the recovery owner.
3. If an attacker steals the recovery seed phrase, he cannot do anything with it (except if he partners up with guardians).
4. The user can have centralised custodians as guardians, family members, etc… The funds are completely safe. Having a couple of centralised guardians will provide the same UX as using a custodial wallet, with the difference that this wallet is 100% non-custodial.
5. The main seed phrase is never shown to the user in order to avoid social engineering attacks.

Another way that the funds can get drained, is if an attacker gets access to the mobile app. This applies to almost every wallet (Metamask, Coinbase, etc…). Because this is a smart contract wallet, we can add extra safety filters like multi-sig, spending limit, etc… Where the owner key is always required to sign. In case an attacker access the wallet device, he will have only the ability to steal a limited amount of money, or not at all (if multi-sig). But even in a multi-sig that requires m of n, the owner signature is ALWAYS required.

The last consideration is abstracting away the recovery address seed phrase to the user. This can be done by encrypting it in a cloud provider (multiple). From a user experience, it will feel better than using gmail.

This combo will abstract all the responsibility away from the user, while providing a safe and non-custodial wallet mechanism.

Some negative considerations:

What if the user looses the device and the recovery seed phrase at the same time !!!

Although highly unlikely that both scenarios happen at the same time (looses the phone, and looses access to multiple cloud providers at the same time?), some more complex filters can be implemented. For example, an option that guardians can unlock the wallet to a new address (like social recovery) ONLY IF the wallet has been inactive for more than x (180 ?) amount of days. This has tradeoffs (what if the guardians kidnap the user ?).

We are going back to showing the seed phrase !!!

Again, we don't have to. The recovery seed phrase can be completely abstracted away from the user, and stored in different cloud providers (even centralised custodians, this key is useless by itself!).

But, you are being paranoid ! My guardians would never steal from me !!!

I understand that your guardians will not maliciously steal from you. But by having guardians you are introducing more security risks than using a centralised wallet. What if they get socially engineered ? What if the majority of them loose their wallet ? What if…. I really don't believe people (at least me) would be comfortable with those trade-offs. And, a traditional social-recovery wallet with only one centralised guardian is EXACTLY THE SAME as a custodial wallet. That guardian can take your funds away.

Conclusion

This mechanism tries to bring the sovereignty of being a 100% non-custodial wallet but without scarifying the UX of a centralised one. I believe we are in a point that we need to stop pushing responsibilities to the users, and instead create systems that feel invisible while maintaining the core values that we care about.

I would love to hear some negative feedback from all of you

.

If you are interested in this proposal, you can contact me through twitter:https://twitter.com/ro_herrerai