Funding the Commons & Earth
Commons Hackathon

Stellar

SecuredSmartWallet

Making crypto accessible to non-crypto users

*With Smart Wallet policies
and a new paradigm*

Nicolas Beaudouin

Table of contents

01

Why crypto is not accessible?

Most people won’t do self-custody

02

Solution and compromises

Two tools that helps accessibility to crypto

03

Smart Wallet integration

Integration as policies

04

Future of the solution

What’s next ?

01

Why crypto is not accessible ?

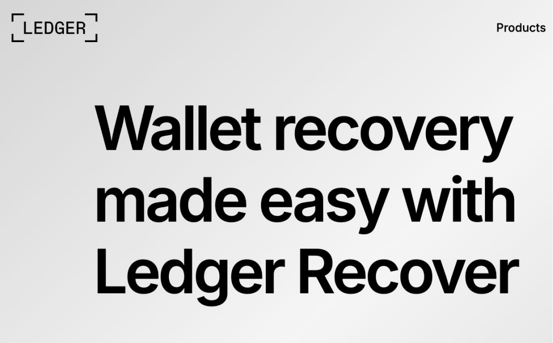
Why my grandma, your non-nerd friends
don’t have a crypto wallet ?

We created banks to secure our money and facilitate exchange

But now Crypto enable an **integrity** layer for **money** and allows to get away from institutions and banks.

What do people really want ?

The self-custody problem

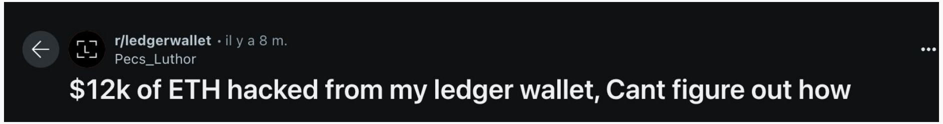


LEDGER

Products

Wallet recovery made easy with Ledger Recover

People lose their seed. So ledger made a business out of it
→ *This solution may put your keys at risk !*



r/ledgerwallet • il y a 8 m.
Pecs_Luthor

$12k of ETH hacked from my ledger wallet, Cant figure out how

Hardware wallet prevent you from getting your key stolen **NOT from being scammed**

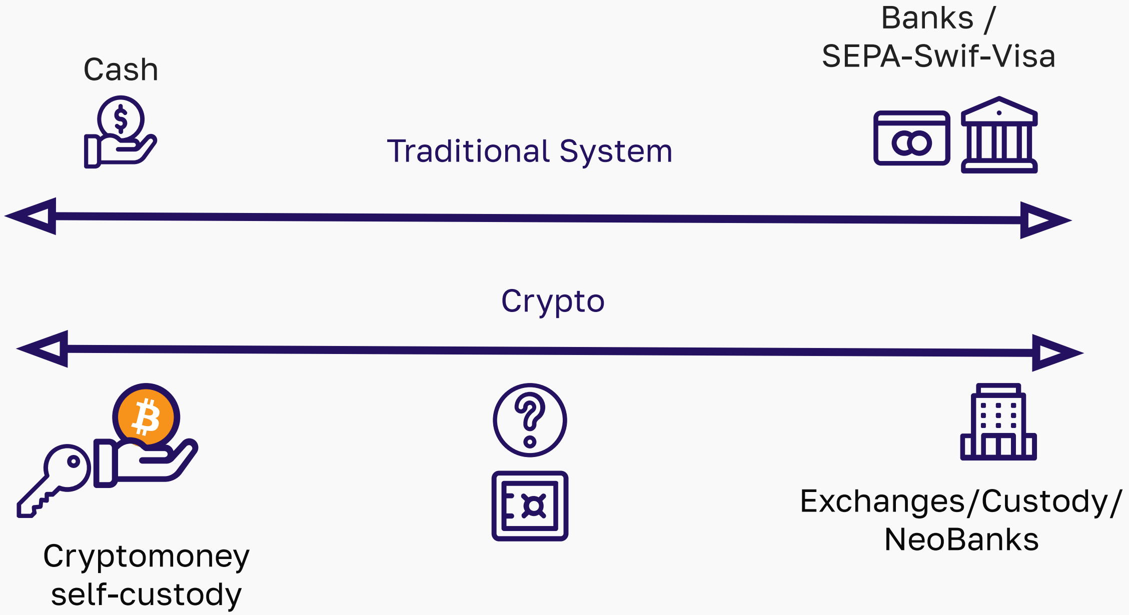
Still many people lose funds because of unsafe transactions

Overview

→ **Self-custody** (but full responsibility)

→ **Low regulation**

→ **Easily exchangeable** (Low fees or no fees)



Cash

Banks / SEPA-Swif-Visa

Traditional System

Crypto

Cryptomoney self-custody

Exchanges/Custody/ NeoBanks

→ **Custody** (but with partial responsibility)

→ **Regulated** (given specific countries)

→ **Easily exchangeable** (but with fees)

02

Solution and compromises

- Time based Social Recovery
- Securer: external multisig for high security

Social Recovery has a problem

You are no longer fully in control of your funds
There is a collusion risk...

Compromised solution:
Inactivity time based recovery system

(As long as you keep sending, you keep full control)
Solutions for savings accounts in implementation

```
[
        {
        [alice_backup, bob, companyX],
        threshold: 2, time: 10 days
        },
        {
        [alice_backup, companyX], threshold: 1,
        time: 15 days
        }
]
```

Securer: external entity multisig

(optional ofc)

External security with **censorship compromise** during the *Inactivity time* (set in recovery)

Keeping control of your assets with *time compromise* *(based on recovery)*

Providing the option for **partial responsibility** and potential **insurance** coverage (on your asset property - against theft...)

03

Implementation in smart wallet

Stellar has a great auth system and a great smart wallet implementation ;) Let’s add on top of it.

Policies

External contract that will be call during auth:

- For each call for securer
- For recovery action for recovery function

Recovery

Last_active_time

We have to regularly send a transaction for showing activity (this could be sign when signing new tx):

- Imagine we have a recovery time of 1 week
- Alice can pre-sign 4 transactions if she knows she will not connect again for a month
- Her phone can send them in the background every week (or she can subscribe to a service)

  → if she lost her phone she will only have to have a 1 week loan / or wait 1 week

  → She keeps the control all the time

Securer

Dynamic Signer Addresses

To provide the best security possible a Securer company would want to be able to **change his validating keys** in case of one being compromise.
(Without having every client to sign a new transactions)

Moreover, he may have **more than one signers** to keep high availability.

This is why this function is implemented as an external policy rather than using the embedded multisig of the Smart Wallet

04

Future of the solution

What’s next ?

Improvement

Tests

More tests and thorough implementation are needed - only 6-5 days have been spent on understanding the smart wallet and integrate the functions

Client

Client sdk for automatic authorization entries

Wallet integration

Integration in on going wallet for “non-crypto” users

Business

Developing the idea on a real market of users as a securer *(I know a potential market but we need more tools :* ***regulatory and privacy*** *tools)*

Thank you!

Do you have any questions?

pro@nicolasbeaudouin.com
https://nicolasbeaudouin.com

Credits: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**