Collaborative Seed Recovery

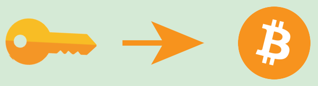
Blockchain Commons

Christopher Allen
Wolf McNally
Shannon Appelcline

ChristopherA@lifewithalacrity.com

1. Why Do You Care?

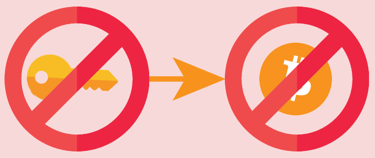
- Holding Bitcoin, Ethereum, or other assets.
- Concerned about a self-sovereign key.
- Know that singular hardware storage is risky.
- Worried about losing your 12 words.



Self-sovereign control of your digital assets gives you independence, but it requires responsible key management!

2. Why is Self-Sovereign Dangerous?

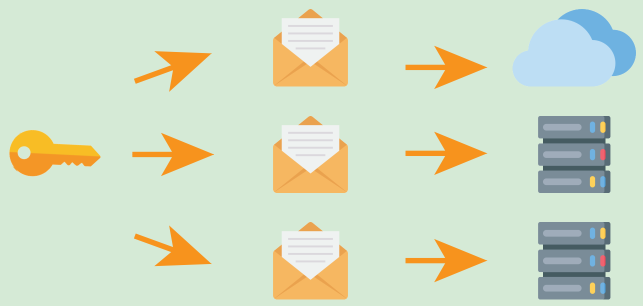
- It's easy to lose a seed.
- It's easy to lose backup words too!
- Hardware devices can become obsolete.
- Theft! Disaster! Loss! So many risks!



Self-sovereign custody reduces the risk of external attack, but you have to also reduce the risk of internal loss.

3. What Does CSR Do?

- Divides seed; recover w/threshold of "shares".
- Backs up first share in platform cloud.
- Stores other shares in share servers.
- Allows recovery with a variety of auth.
- Automates everything to make it simple!



Though it can be hard to protect our self-sovereign seeds alone, we can do so by working together!

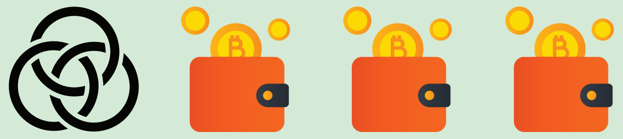
4. What's Innovative in CSR?

- Storing shares physically is risky & hard.
  - Platform clouds automate.
  - Share servers automate.
  - Better protection than physical copies!
- Recovery needs to be secure.
  - A variety of auth improves security.
- Classic shares store small amounts of data.
  - Envelopes will solve that.

The goal of CSR is to expand & automate seed backup. Users should be able to automatically protect their assets!

5. Who is Involved with CSR?

- Working with Bitmark, Foundation, Proxy.
- The goal is an interoperable solution for all.
- We are holding biweekly meetings.
- Discussing specs & demonstrating progress!



The goal of Blockchain Commons is to bring the community together to build interoperable specs & infrastructure.

6. Why Should You Be Involved?

1. You have single keys that need protecting. You want to spread risk & lower liability.
2. You want to run a share server.
3. You want to improve crypto accessibility.
4. You want to advocate your interests.

We want to work with more developers & hardware vendors. Want to be a member of the CSR community? Talk to us!

7. Deep Dive: Envelopes

- Envelopes are the foundation of CSR.
- They are Smart Documents.
- Encrypt secrets; store metadata.
- Lock with Shamir, public keys, and more.
- Permits allow multiple methods of access.

Envelopes today can encrypt data with Shamir & keypairs. They're also future-proofed to allow more access methods.

8. How is CSR Future-Proofed?

- Uses BLAKE3, ChaChaPoly & Schnorr.
- Plans for VSS & distributed key generation.
- Future permits for multisig & crypto-scripts.
- Open arch works for many chains!

CSR is carefully designed for both the present-day and future of cryptography, so that it won't become obsolete!

Images from flaticon.com, attributed as follows: BZZRINCANTATION: hardware wallet; Dinosoft Labs: envelope; Freepik: Bitcoin, key, locks, man, server, sprout, veto; Pixel Perfect: cloud; small.smiles: collaboration; Soodesign: wallet, ultimatearm: risk; Vitaly Gorbachev: woman.