Social wallet recovery

- Timo Glastra, timo@animo.id

Introduction

Wallet recovery has been a hot topic in the digital identity space for a long time. A question you often get when people realize all data is stored on your own devices is “But what if I lose my phone?”.

An easy solution to this answer would be to store a backup of your wallet on a centralized server, and for ease of use also store the key to decrypt the wallet on this centralized server. You’ll have your wallet recovered on your new device in a matter of seconds.

During RWOT, I’d like to explore the possibilities of social wallet recovery in a manner that you don’t have to trust a single third party provider, and also aren’t dependent on keeping a seed phrase secure.

What

Last year Vitalik shared a post on the advantages of social recovery. This mainly focused on crypto currency wallet recovery. A wallet contract stores a public signing key, and there are a number of guardians that can change the public key (if x out n guardians approve).

This topic focuses on social recovery without the need for a contract on a blockchain, but rather by directly setting up social recovery between a number of peers. A peer could be anything in this case. It could be another device of yours, a friend, family, or a vendor that offers key shard storage as a service. The goal is that no one involved in the process could recover the wallet on their own, but together, a key or wallet can be recovered.

There’s two topics of focus:

- Social key recovery (Using for example shamir secret sharing)
- Social wallet data recovery

Key recovery could be used for a number of use cases, it could be leveraged for constructing a high-privilege private key that can rotate the public keys in a did document, but it could also be a key that can decrypt your encrypted wallet backup.

The approach for wallet data recovery is a bit more complex, as there’s more data that needs to be stored. It could be possible to store your encrypted wallet backup at centralized services such as Google Drive, Dropbox, One Drive. Distributing the shards over multiple services reduces the risk of losing access to your wallet backup. Another approach is to also shard the wallet data and share this across peers. The synology NAS allows you to backup your drive to a lot of different providers such as cloud providers, external hard drives, but also encrypted backups on the Synology's of your friends an family. This ensures you're never locked out of your own data.

Research Questions

- How to exchange shards between multiple peers?
  - Can a DIDComm protocol help with the process of sharing and recovering shards? If so, the user probably lost access to their did, how do you know you should share the shard? Is this an Out of band approach?
- Is it possible to shard a larger binary blob across multiple peers to allow for wallet recovery?
- What are the risks and opportunities of social recovery?
- What methods with regards to sharding and storage can be leveraged?
  - E.g. Friends/Family, Trusted Services, Other devices, QR codes, etc..?

Resources

- Global.ID Trustees
- What If I lose my Phone - Sovrin
- A beginner's guide to Shamir's Secret Sharing
- Shamir Secret Sharing Implementation