Me and the whole Coinsafe team have been working on a Shamir secret sharing implementation in a non-custodial mobile wallet. Our implementation allows you to recover your 12 word mnemonic phrase using your trusted devices essentially making it safe for everyone to hold private keys of their cryptocurrencies instead of trusting custodial services. I'm excited to announce that we are live in testnet beta for both Android and iOS.

Over the past couple of months we tried to tackle all the attack vectors in integrating secret sharing in a mobile wallet and make it simple to use for a non-technical user.

Some key achievements of our technical architecture :

1. Applying secret sharing at the mnemonic level instead of private key level in order to support multiple cryptocurrencies. This is not possible with a smart contract based recovery approach as in such approaches a user's funds are held in a smart contract which means there can only be support for ETH & ERC20 tokens.

2. Successfully handling the case of 'trusted devices collusion' which ensures that your funds remain secure even if all your trusted devices collude. We handled this problem by ensuring that :

a. You first encrypt your mnemonic using a symmetric key to get an encrypted text

. This symmetric key is mapped with your email address hash and is safely stored in Coinsafe's database.

b. You apply secret sharing on this encrypted text to generate shares that are to be shared with your trusted devices/friends.

M (original mnemonic) +X (symmetric key) → M' (encrypted text)

M' (Encrypted text) -> Secret sharing -> S1, S2, S3, S4, S5 (Secrets)

This means that even if your trusted devices/friends collude, they would only get an encrypted text and in order to gain access to your original mnemonic, they would need to hack your email as well to gain access to the decrypting symmetric key. The probability of both of them happening together is substantially low. Full details in our first blog post.

1. Making sure only you know your trusted devices - this is essential as we don't want Coinsafe or any other third party to have the ability to send recovery request to your trusted devices on your behalf.

This is accomplished because our architecture only needs to know the hash of your trusted device wallet public keys. Full details in our second blog post

.

1. Using a wallet public, private key pair for secure communication between you and your trusted devices while 'setting up key recovery' and 'recovering forgotten key'. This public, private key pair is derived from the user's mnemonic phrase but is not tied to any cryptocurrency. It's just used to do encrypted communication between the user and their trusted devices.

Feedback we are looking for :

- UI/UX improvement in our implementation of secret sharing in the app with the goal of allowing even our Moms to secure her funds by selecting friends/devices she trusts.
- Possible security issues with our architecture, if any.
- Collaborations/partnerships we can do to reach to a wider user base. This can be collaborations with other software/hardware wallet companies, institutions or high networth individuals who are looking to safeguard the private keys of their crypto etc.

Relevant Links :

Coinsafe Twitter

Coinsafe Website

App Beta versions :

Android

iOS