DECENTRALISED SEED PHRASE MANAGER

Introduction

A seed phrase is a sequence of random words that stores the data required to access or recover cryptocurrency on blockchains or crypto wallets. It is essential to keep seed phrases safe and secure, as losing them can result in the loss of access to your digital assets. Managing seed phrases presents a significant challenge to both non-technical users and experienced individuals. The responsibility of securing these keys often leads to paranoia or the risk of forgetfulness, potentially resulting in the loss of valuable assets. This light paper introduces a novel solution that addresses these concerns by securely storing seed phrases on-chain in an encrypted format. By leveraging blockchain technology, we aim to relieve the stress associated with seed phrase management, allowing users to confidently participate in the Web3 ecosystem.

Problem

The current way of storing seed phrases relies on two extremes of safety when it comes to trusting the safety of your assets. The first is trusting an organization, an excellent solution when considering convenience. The second is trusting yourself or self-custody if you will. Self-custody is currently the safest way to store your assets but has its limitations as we will look at below.

Current seed phrase managers are centralized, meaning that they are controlled by a single entity. This raises security concerns as if the central entity is hacked or compromised, then all the seed phrases stored on the platform could be at risk. As they say in crypto, ***not your keys, not your password***.

Self-custody as the other alternative has the drawback of being cumbersome to store/ write them down and assumes that every individual can keep these words safe.

Hardware wallets are a solution as well and one of the safest when it comes to self-custody, assuming they never get lost. In 2022 alone about $500 million was estimated to be lost due to losing passwords and seed phrases as well as errors recording seed phrases.

Is there another way we can find a good balance between the convenience of centralized seed phrase storage and the inconvenience of the decentralization that comes with self-custody and can the blockchain help us solve it?

Solution

We propose a **decentralized seed phrase manager**. Using On-Chain Encrypted Storage, our solution provides a secure and convenient approach to seed phrase management. This addresses the security concerns of centralized seed phrase managers by storing seed phrases on a distributed network. it makes it much more difficult for a single entity to hack or compromise all the seed phrases. Furthermore, it offers security from password loss and seed phrase loss that would occur due to miss-typing, misplacing or theft giving users the security and the convenience of the blockchain.

How it works

User will get the seed phrase of 12 or 24 words from the front end of a website. They can write it down or keep it like you would normally.

The application will then generate an encryption key using a Fernet encryption for instance by combining the seed phrase and any other information that only the wallet owner would know such as a hash of their Social Security or Passport number. This key should be kept safely. It can be stored in a centralized cloud storage account which has a relatively easy recovery method such as 2FA because it is not of much value to anyone by itself.

If hacked, the hacker would not know the seed phrase or any other data the user used to encrypt, hence the fernet key is useless to anyone other than the owner of the wallet.

Implementation

This project will use a parameterized smart contract on the Cardano Blockchain that will use the encryption key, hashed personal information and the seed phrase count as parameters. Each word will then be encrypted and stored as a Datum.

An example would be; If there are 12 words of a seed phrase, we will have 12 UTXO's created where each UTXO stores one encrypted word as Datum.

Recovery

In the unfortunate event where a user forgets their wallet password and is unable to retrieve their seed phrase for one or the other reason, they simply need their encrypted key and their private personal data to recover their seed phrase.

On the Cardano blockchain, they can redeem the encrypted key word (basically the UTXO gets unlocked means they know that to be the encrypted key and they can decrypt it because they have the encryption key). Each UTXO is recovered in a similar manner. Technically the user need not unlock the funds, rather but to know it is their word.

Use Cases

A decentralized seed phrase manager could be used for a variety of purposes, including:

- Storing seed phrases for cryptocurrency wallets
- Generating new seed phrases
- Sharing seed phrases with others
- Recovering lost or forgotten seed phrases

Future Work

There are a number of potential future work areas for decentralized seed phrase managers, including:

- Integrating with hardware wallets
- Developing user-friendly interfaces
- Integrating with other decentralized applications

Conclusion

A decentralized seed phrase manager is a promising technology that could help to improve the security and privacy of cryptocurrency wallets. There are several potential future work areas for this technology, and it is likely to see continued development in the years to come.

https://www.businessinsider.in/cryptocurrency/news/investors-likely-to-lose-almost-545-million-worth-bitcoin-in-2022-by-forgetting-passwords-and-various-other-mistakes-suggests-report/articleshow/91126423.cms#:~:text=Bitcoin%20investors%20are%20likely%20to,according%20to%20a%20new%20report.