Blockchain Based

DECENTRALIZED WALLET.

Aliasgar Merchant

Blockchain Based Wallet

Table of Contents

Blockchain Based Wallet

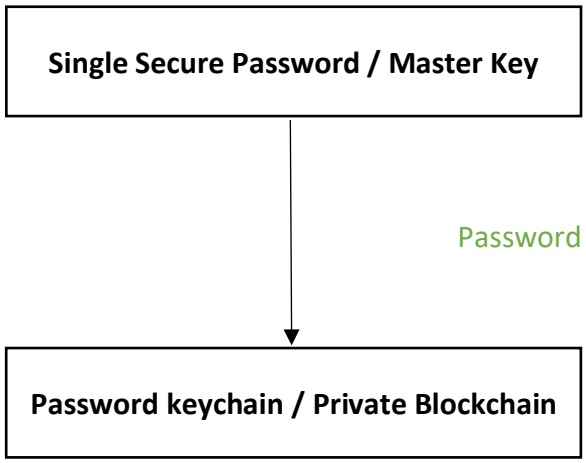
Abstract

Blockchain Based Wallet is an open source software which can be used to store **passwords**, **credit card information** and **other secret information** securely over Blockchain. None of the user information is ever stored in any database. Hence the user exercises complete control over his/her personal information.

This white paper will serve as an informative guide discussing various aspects of the wallet and demonstration of how to use it. If you have any issues or concerns – please feel free to connect to the developers over GitHub. The software wallet is open source and code can be found over GitHub – readily available for audit.

Blockchain Based Wallet

Master Key



Blockchain Based Wallet

Details about Master Key

- Bitcoin wallet.
- BIPS 32 standard.

Blockchain Based Wallet

Features

- Store password / critical information over Blockchain making it highly secured.
- Nothing is stored centrally on any database. (No loss or breach of data.)
- Everything is synced over various platforms like – android, IOS, chrome, Safari and IE.
- Password can be securely shared with friends, family, and co-workers. However, this need downloading application. (This facilitates revoking of password as and when needed.)
- The mnemonic phrase used during registration can be used to reset the master key.

Following things can be stored in the secured vault:

- Passwords.
- Secured Notes.
- Credit Card information.
- Random Password Generator. (Follow the respective rules of website for password generation.)

- For mobile application, access into vault or auto-fill is through face id or touch id. For all other use cases password maybe needed. (Password timeout can be set manually. By default, it is set to 30 mins.)

  Password Generator:

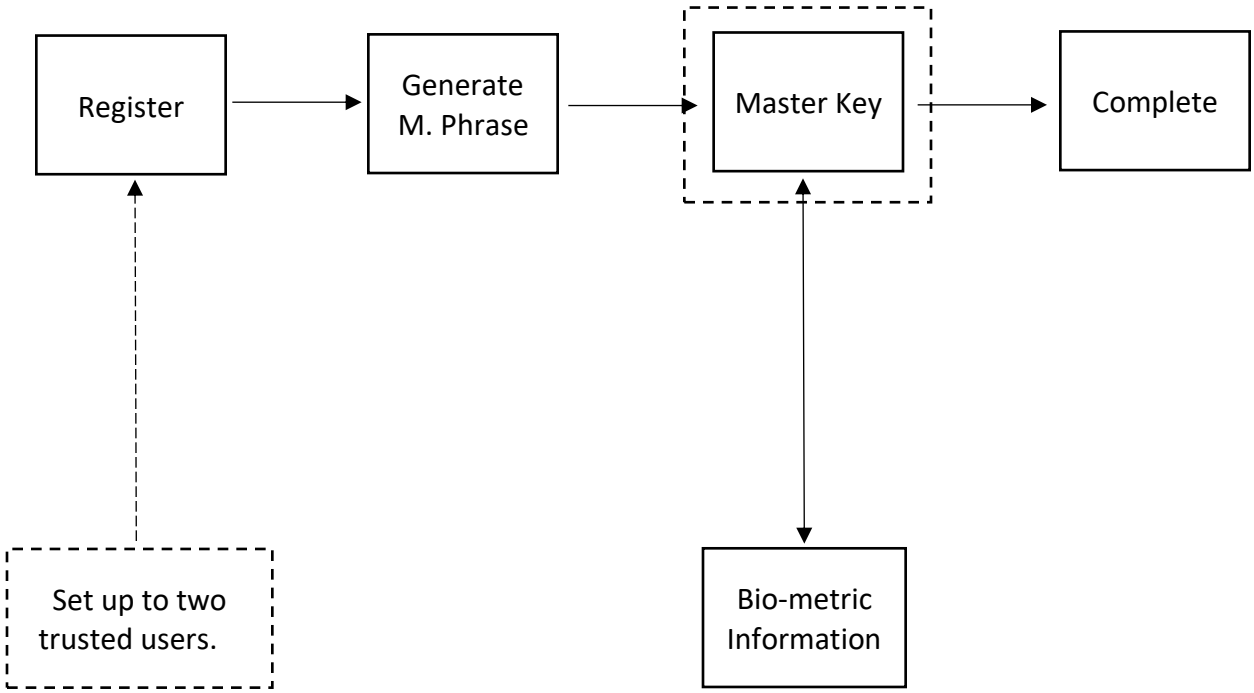
- Length (Slide bar) [up to 64 chars.]
- A-Z (Toggle)
- a-z (Toggle)
- 1-9 (Toggle)
- -*/@# (Toggle)

- Auto fill and auto login.

Blockchain Based Wallet

Registration Flow

1. User clicks on register.
2. Generate mnemonic phrase.
BIPS 32 standard. This serves as a first factor authentication for any major changes.
3. Then user enters a master key.
This is a complicated set of passwords usually chosen by user. Users are forced to choose a complicated password.
4. The password is then masked behind the biometric information of user.
5. The registration process is completed and ready for use.



Blockchain Based Wallet

Forget (Lost) password flow

For mnemonic phrase – once lost can never be retrieved.

Unless (as suggested) it can be securely stored in the vault of a friend/trusted user.

1. User clicks on forgot password.
2. Enter passphrase. (If forgotten request from trusted user.)
3. Information i.e. password is sent to the user via approved mode of communication like phone or email.
(Time token based random number is generated and displayed to trusted user – for additional 2 factor authentication.
4. User successfully reset the password and can now log in.

In case a password is being requested by a trusted user passphrase needs to be entered.
The user has up to 8 hours (between 30 mins and 8 hours as configured.)

Blockchain Based Wallet

Flow of application

1. User registers. (first time user)
2. User logs in. (Biometric Auth)
3a. On a website / application prompt user to save user id and password.
3b. Safely store the credentials and other important information in vault.
4. Access the vault to retrieve needed information.