



Storecoin ecosystem wallet

Securing the wallet, token issuance, and ongoing token distribution

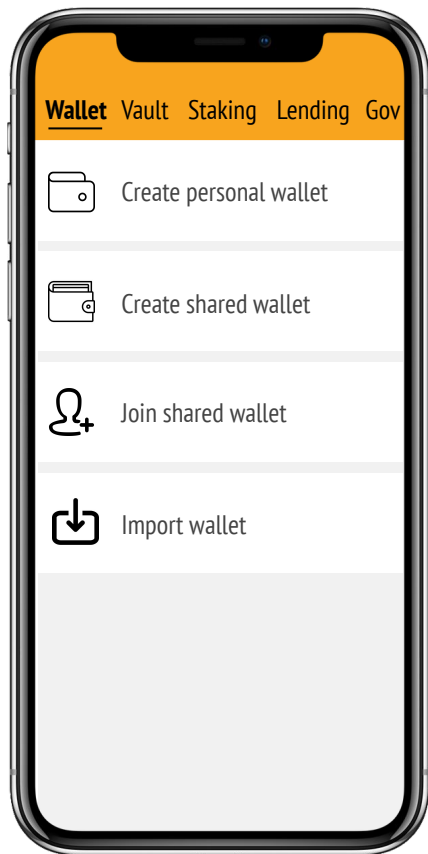


May 2019

Questions answered in this presentation

- 1) How Store issues tokens probably with lawyers? See slides 22-28.
- 2) How those tokens can be owned by a user with a cloud solution? See slides 5-13 for using cloud-based Vault. Token ownership flow is same as in slides 22-28.
- 3) How they can do it with their own machine? See slide 5 for self-secured wallet. Token ownership flow is common as in slides 22-28.
- 4) How seed phrases/backup phrases can be backed up in cold storage using this cloud tool? See slide 14 and 15 for generating and confirming the seed words for the wallet. Slides 16 and 17 describe the flow of backing up the seed words in the cold storage.
- 5) How ongoing token distributions can be sent from Storecoin to this tool? See slides 22-28 and description in slide 28.

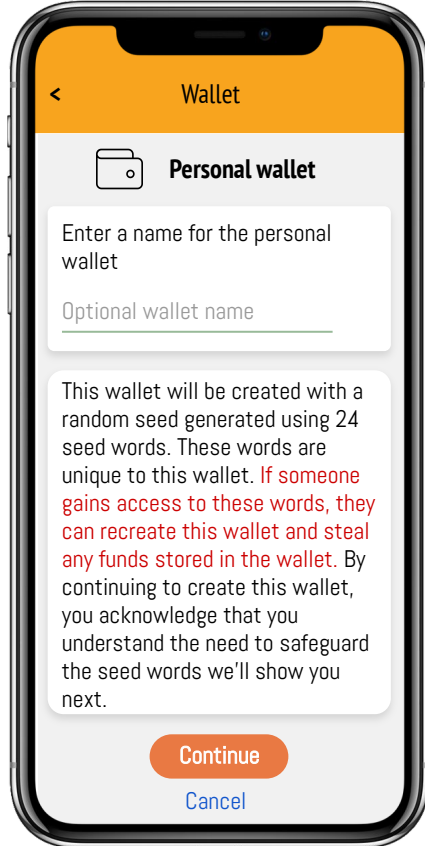
Create new wallet



1 User selects the **Wallet** option in the app.

2 User selects **Create personal wallet** option to create a personal wallet, which requires a single signature of the user. User can create a shared wallet, which requires multi-sig. In this flow we describe the steps for a personal wallet.

Enter a name for the wallet (optional)



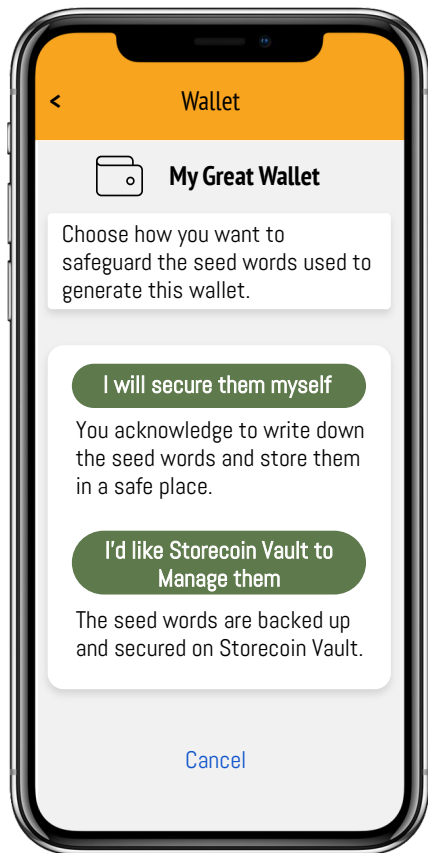
1

User can enter a name for the wallet. This is optional. Typically a single wallet can hold multiple cryptocurrencies, so unless the user creates multiple wallets in the same app for better manageability of ownership of coins, a name is not necessary.

2

How the wallet is generated and the need for securing the seed words is emphasized. This can be elaborated further as shown in <https://www.cryptouxhandbook.com/creating-a-wallet>. Here, we only capture the need for letting the user know that the seed words must be secured.

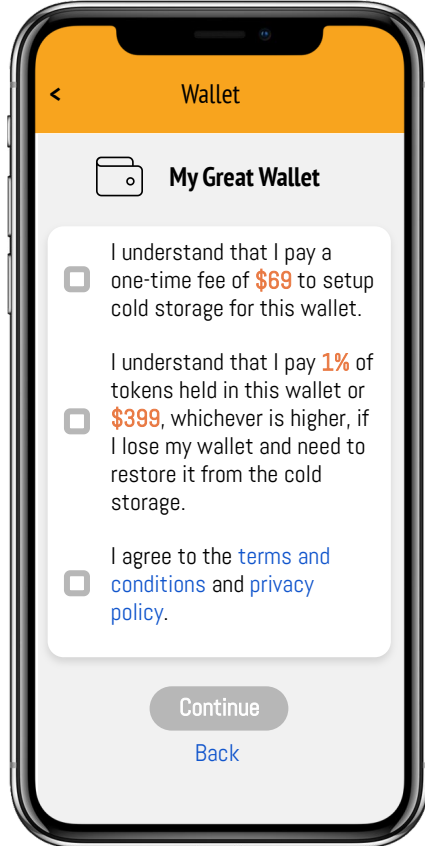
Select how the seed words are secured



The seed words are secured in one of the two ways:

- 1 - The user can write down the seed words and store them securely on a hardware wallet like Trezor (<https://trezor.io/>), Cryptosteel (<https://cryptosteel.com/>), etc. We'll not discuss these options here. If the user selects this option, they will continue to the next step in slide 14 directly.
- 2 - The seed words are stored securely on a cloud-based Vault service. This option is discussed in the next few slides. We assume that the user selects this option for securing the personal wallet.

Cloud-based Vault for cold storage



The Vault service is not a multi-sig wallet where it co-signs transactions. It is only a cold storage facility to safeguard users' wallets. It stores seed words in secure cold storage facilities scattered around the world.

1

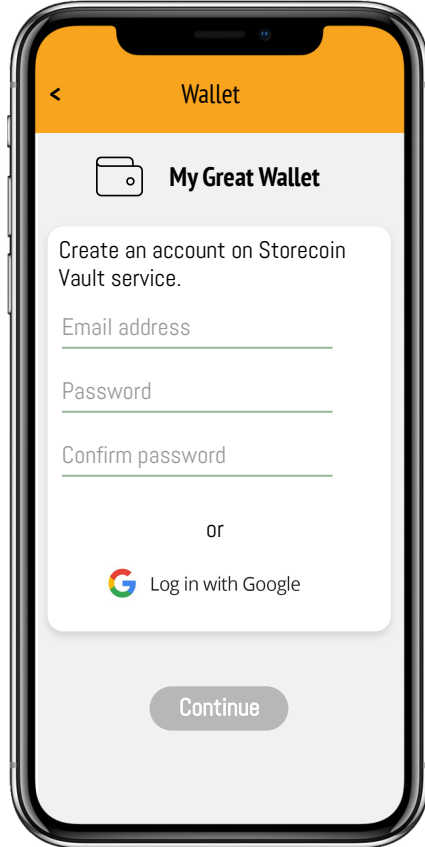
There is a one time fee to set it up, which the user pays in the next step. If the user loses the wallet and needs to restore it from the seed words stored in the cold storage, there is an additional fee as described here.

The fees listed here are for illustration purposes only.

2

The Continue option is enabled when the user checks all the boxes.

Account creation for the cloud-based Vault for cold storage

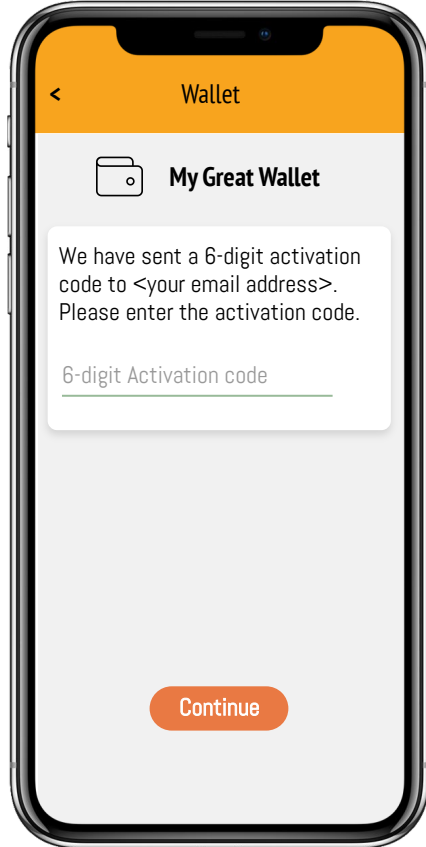


1

The user needs to create an account on the Vault service. The user can sign up with an email address and password or optionally, login with a single sign-on with a Google account.

If the user signs up with the Google account, the email address associated with the Google account is used automatically. User is then requested to create a password, so subsequently they can login with the email address and password.

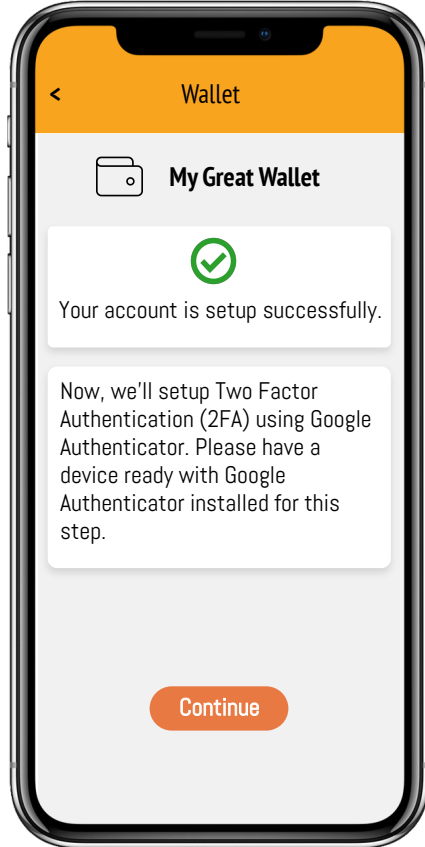
Activation code to continue creating the account



1

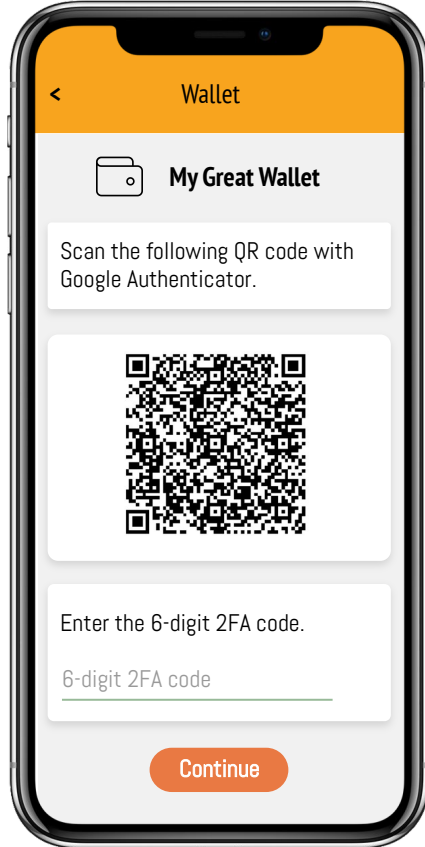
User enters the activation code sent to their email to continue creating the account. It is possible to click on the activation link in the email to complete the account setup process (which is standard), but this step shows how the same can be done within the app.

Setup 2FA for improved security



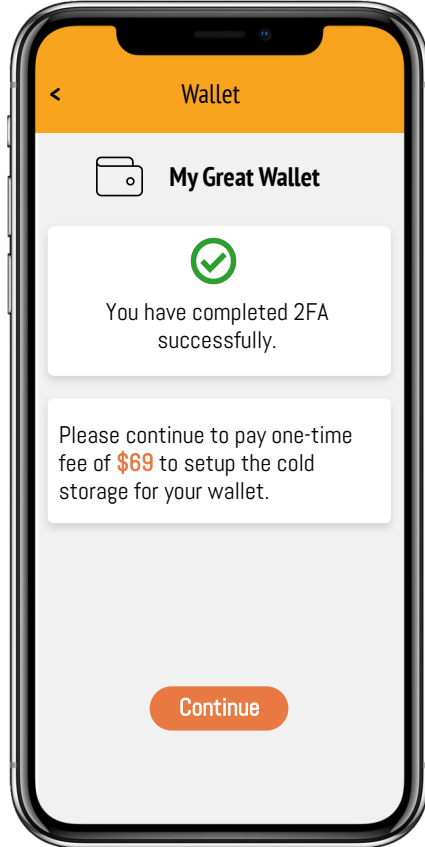
- 1 After the account is created, 2FA is setup for improved security. Every access to the account in the future requires 2FA.

Scan 2FA QR code with Google Authenticator (GA)



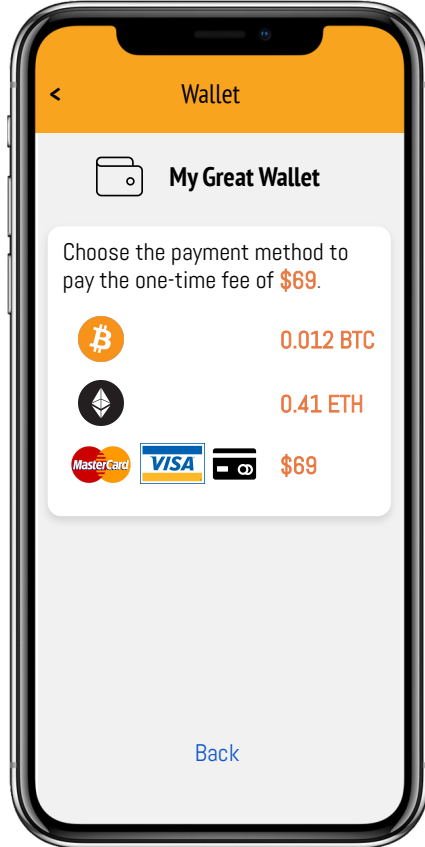
- 1 The user scans the 2FA QR code with Google Authenticator, which generates a 6-digit 2FA code. In this flow, we show the 2FA step with GA on the same device, but this step could be completed on a different device, if the user has installed GA on that device.
- 2 The user enters the 6-digit 2FA code to complete 2FA setup.

Continue to the payment step to pay for the cold storage



- 1 This step completes setting up the account with 2FA support. The user now proceeds to the payment step.

Payment to setup the cloud-based Vault for cold storage

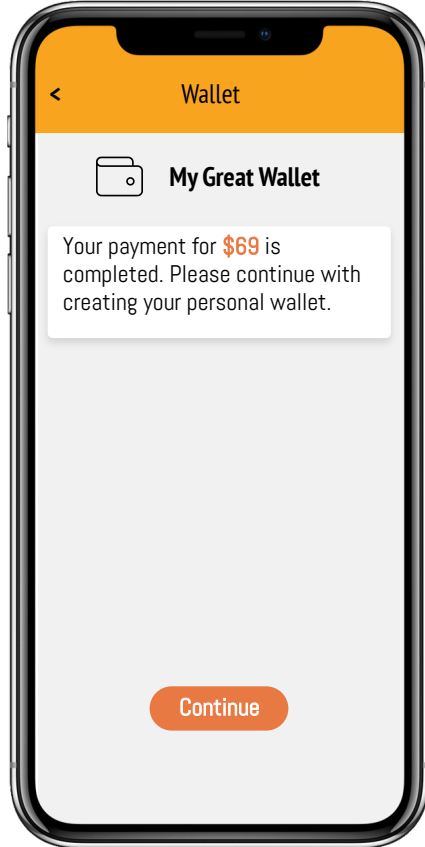


The user can pay the setup fee with BTC, ETH, or credit/debit cards. The payment processing and flow details are not described here for brevity. It is assumed that the payment is successful.

- 1 If the user pays with BTC, ETH, any cryptocurrency, the user can continue only after transaction confirmation is received.

Since the user is setting up a new wallet, we assume that the user cannot pay with STORE yet. However, if the user owns multiple wallets, they can pay with STORE also.

Payment is completed



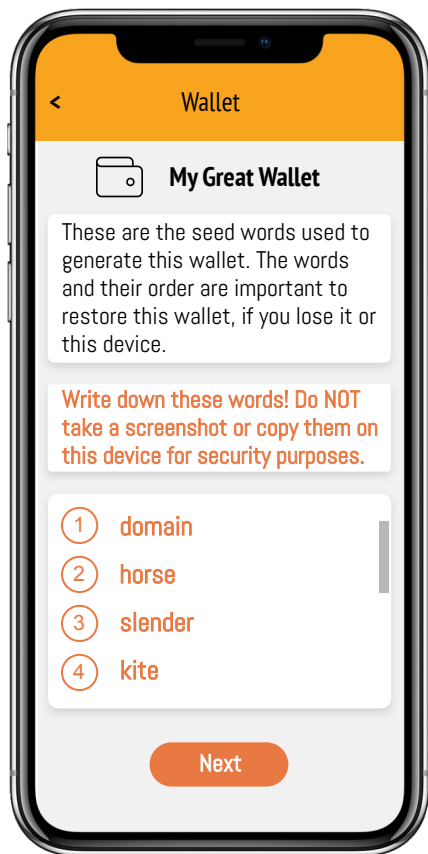
1

The user can close the app and come back later to know the status of the payment completion. The app supports notifications (not described here) so the user can be notified when the payment is completed. The user will also receive email confirmations separately.

Once the payment is successfully completed, the user can continue with creating the personal wallet.

If the user decides to secure their wallets themselves in slide 4, they will go the next step directly.

Display the seed words used to create the wallet



Request the user to write down the seed words. For improved security, warn them not to take screenshots or copy them on the same device because if someone can access the device, they may steal the seed words. Better warnings and other details may be needed here.

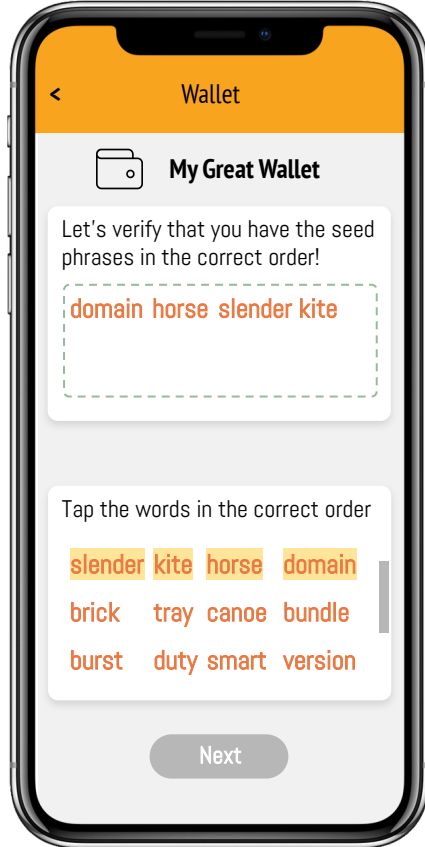
1

Even if the user selects the Vault option to backup the wallet, they will be asked to confirm the seed words. This is to get an acknowledgement from the user on the seed words, before they are backed up.

2

Display the seed words used to generate this wallet. The order of the words are displayed explicitly. The user can scroll down the list to write down all the 24 seed words.

Make sure that the user verifies the seed words in the same order



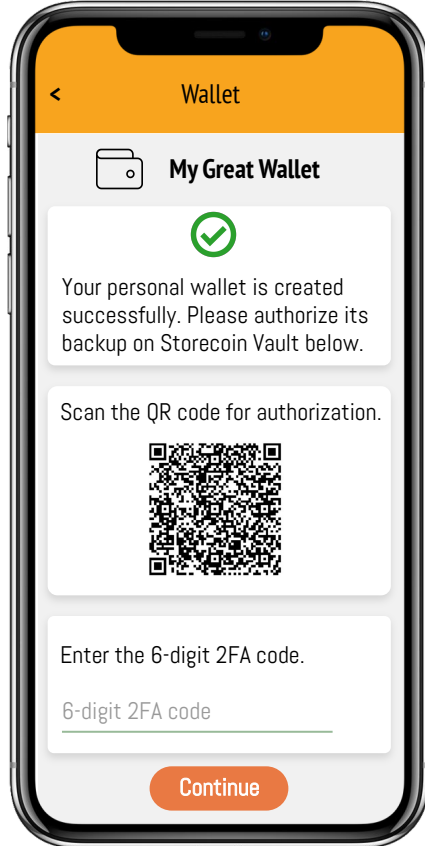
1

The user verifies the seed words even if they have selected the Vault option. The seed words are displayed in a random order at the bottom of the screen. The user is required to tap the words in the correct order. As the user taps the words, they appear here in the same order.

2

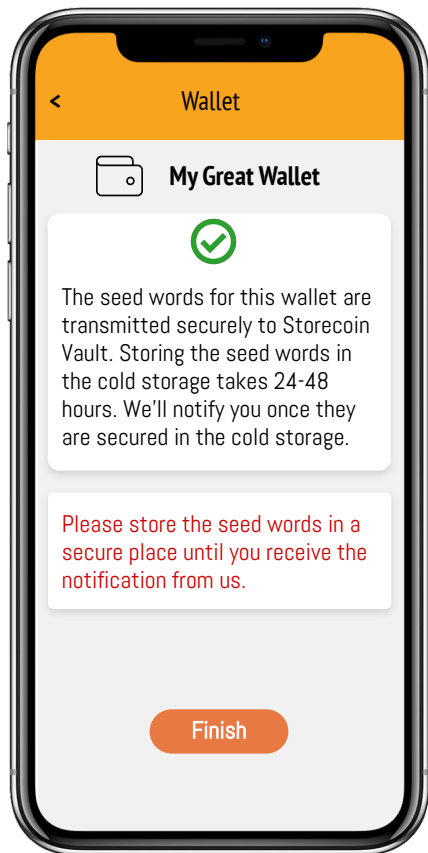
The words already selected are highlighted. The user can toggle the selection by tapping again on the same word. The user is allowed to continue after all the seed words are tapped in the correct order.

The wallet is successfully created



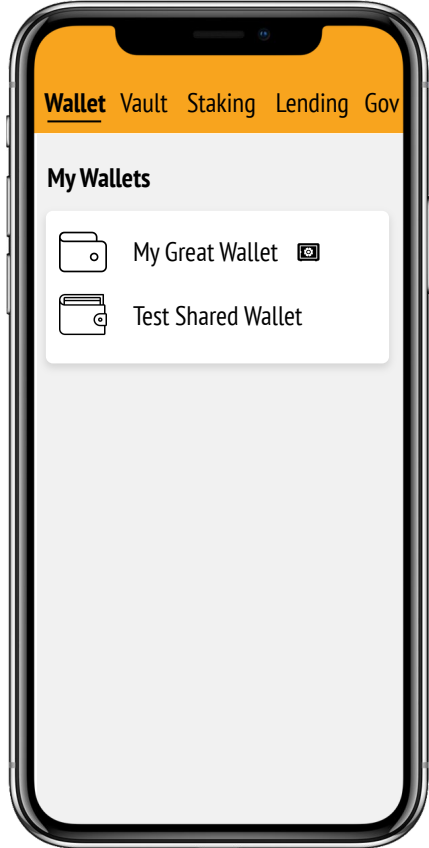
- 1 The wallet is created successfully on this device, but it is still not backed up on Storecoin Vault. If the user chose to safeguard the seed words themselves, they are responsible for securing them as previously described.
- 2 For backing up the seed words on Storecoin Vault, the user needs to authorize the service. This is done with the 2FA.
- 3 User enters the 2FA code to authorize Storecoin Vault to backup the seed words in its cold storage.


Cold storage takes some time to complete



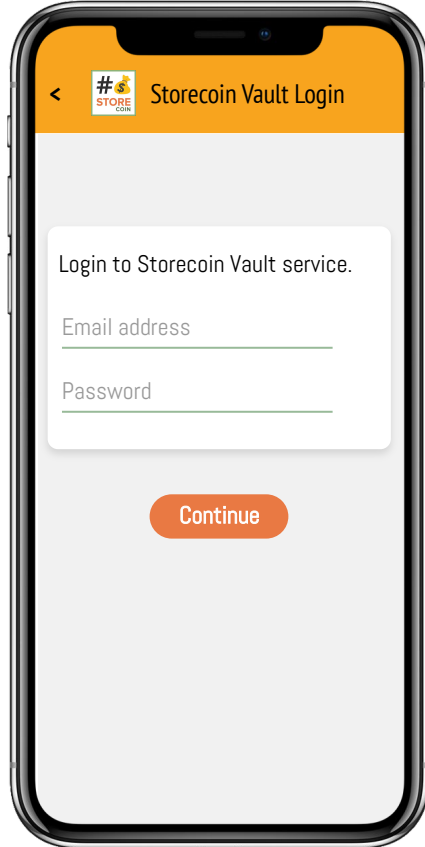
- 1 The seed words for this wallet are sent to the Storecoin Vault service securely with an end-to-end encryption between the app and the Vault API endpoint. The process of securing the seed words in the Vault takes some time because it involves manual operations. The user will be notified in-app as well as on email when the backup is completed.
- 2 The user is requested to save the paper copy in the interim. There may be corner cases where the Vault may not be able to store the seed words for this wallet, so a “retry” may be necessary in such circumstances. The retry flow is not discussed here.
- 3 This completes the flow of creating a wallet and queuing the backup request to the Storecoin Vault service.

Listing wallets on this device



- 1 Once wallets are created, the **Wallets** selection shows the available wallets.
- 2 The personal and shared wallets are displayed. Each of these wallets may either be secured by the user or on Storecoin Vault .

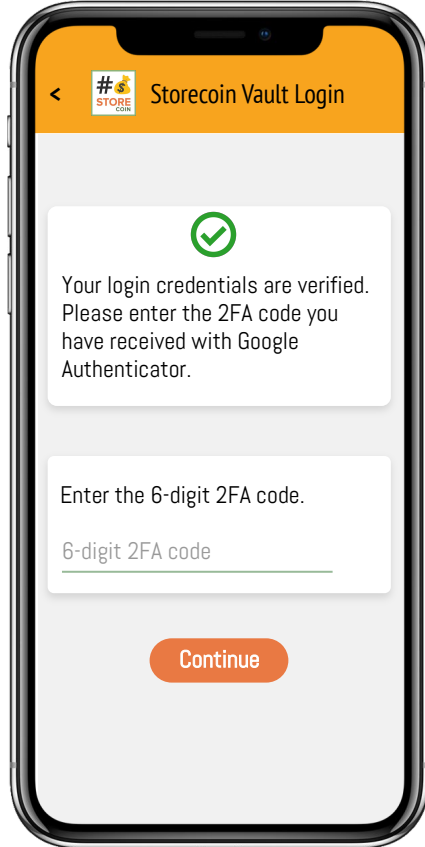
Account login flow



1

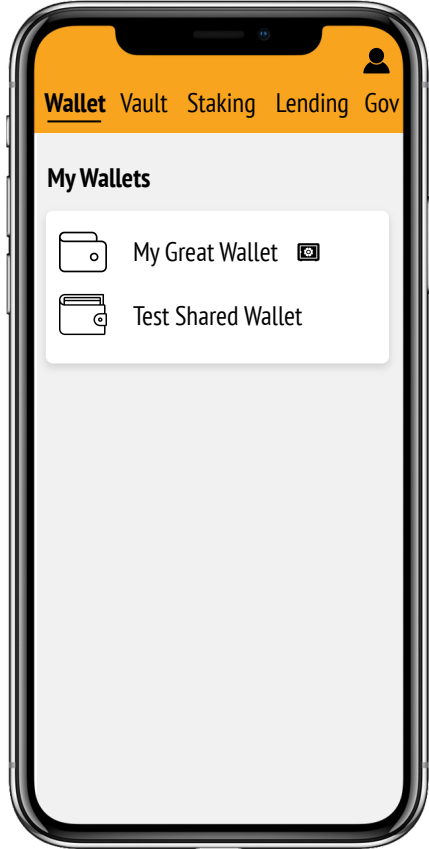
The login flow begins with entering the username (email address) and password. After successful authentication, 2FA is used to confirm that the user is the authorised owner of this account.

Account login requires 2FA verification also



- 2 The user enters the 2FA code from Google Authenticator to complete the login flow.

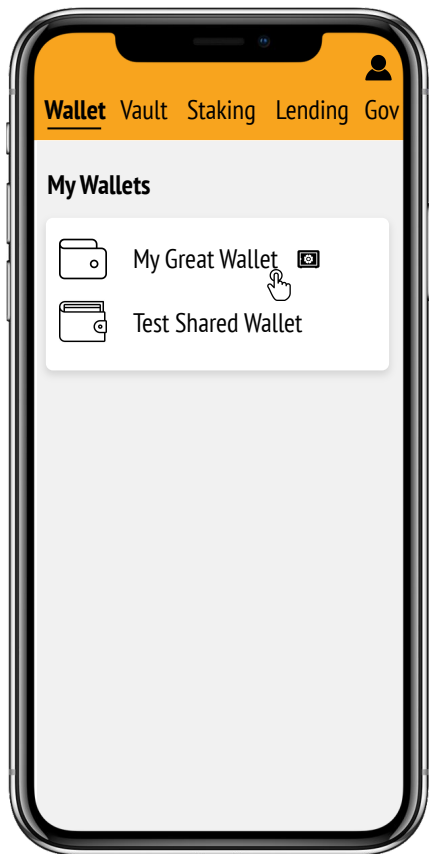
Account login requires 2FA verification also



3

The authenticated session shows the user icon. If the user session is expired, the user icons disappears. The user must repeat the login flow to reestablish the user session.

STORE token issuance to an address owned by the tokenholder



Use case:

- The user participates in Storecoin token sale and purchases certain number of tokens.
- Storecoin only knows about the user's email address.
- Storecoin wants to issue the purchased STORE tokens to the user.
- The user receives an email from Storecoin requesting an address to issue STORE tokens.

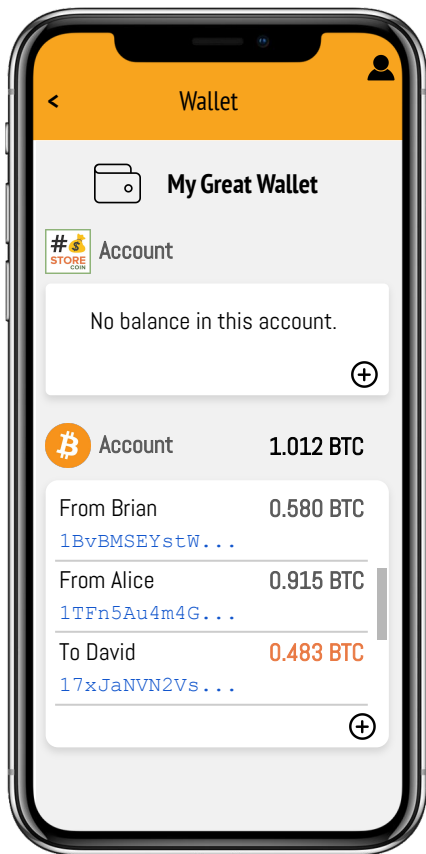
Pre-requisites:

- User has created an account on Storecoin Vault even if they have chosen to self-secure their wallet. This includes 2FA setup.
- Storecoin Vault has confirmed the email address used to create the account. This should be the same email address that the user used while participating in the token sale.
- The user has logged in. If not, the login flow described previously is triggered as part of token issuance flow.


1

The user selects the wallet that would receive STORE tokens.

Multiple coins associated with the wallet are displayed

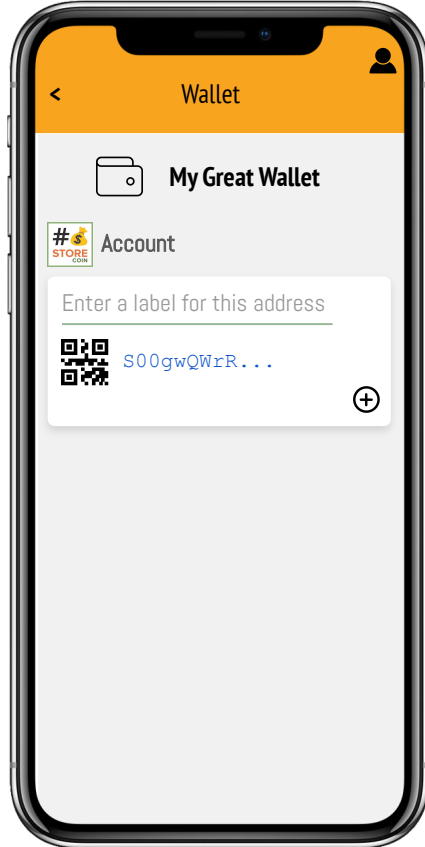


HD (Hierarchical Deterministic) spec* allows storing multiple coin types in the same wallet. So, a wallet can hold STORE, BTC, ETH, or any supported coins.

- 1 We assume the STORE account has no STORE tokens deposited yet. The user can create a new receive address by clicking on  for any coin.

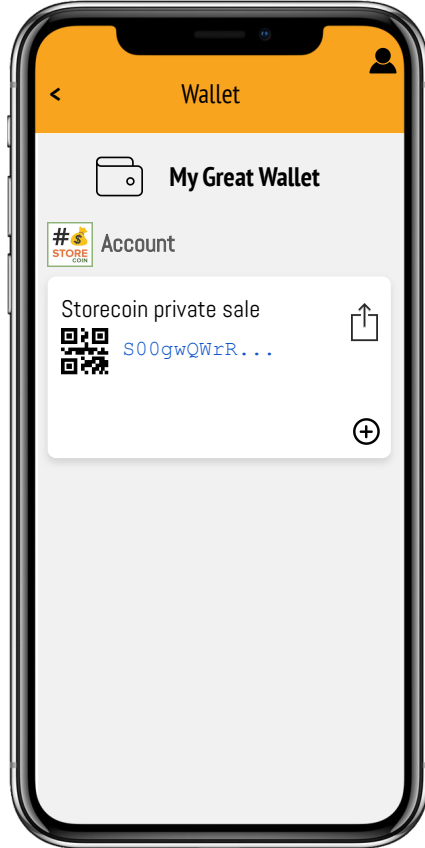
- 2 This shows an example of a BTC account showing both coins sent and received from this account. The account balance is displayed at the top of the account. Each address can have a user-provided label for easy identification. Note that BIP-44 doesn't support labeling the addresses, so this feature is specific to our implementation.

Create a new receive address to receive STORE token



- 1 User clicks on ⊕ to create a new address. The address format is specific to the coin to which it belongs.
- 2 A new address is created. User has an option to label the address. User can create multiple addresses. Each address comes with a QR code for easy sharing when payment is requested.

Optionally enter a label for the new address



- 1 User labels the address for easy reference. In this case, the address is generated to receive STORE tokens from the private sale.
- 2 A share or forward icon is displayed for all unused addresses. The user can request payment using this action.

Share the new address with Storecoin to receive STORE token



- 1 The user can share the receive address in multiple ways depending on who they are requesting the payments from. In this case, the address will be shared with Storecoin.
- 2 After selecting the sharing method, user clicks on **Share**.

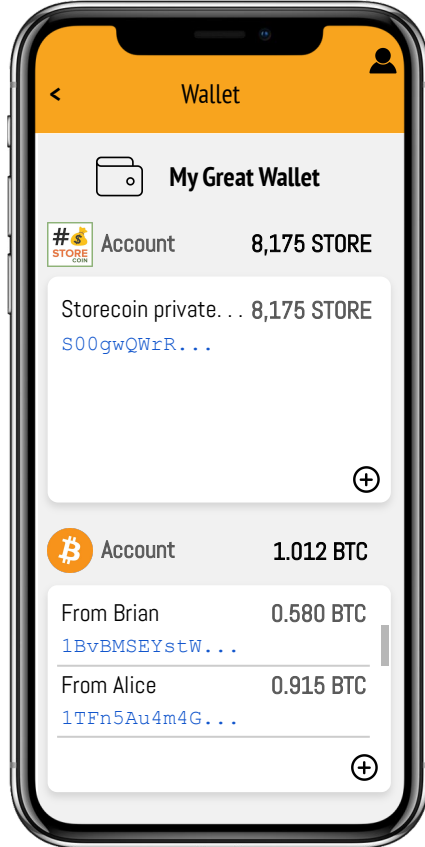
Share the new address with Storecoin to receive STORE token



- 1 A confirmation message is displayed after sharing the address successfully with the intended recipient.

Storecoin legal team or whoever is responsible for the coin issuance with use the receive address and the email address to issue the tokens purchased by the user to the specified address. Once the tokens are issued the user is notified both on email and in the app.

STORE tokens issued will show up in the wallet



After the STORE tokens are issued to the receive address, STORE account shows the updated balance in the account.

Any ongoing token issuance is performed similarly, namely:

- 1
 - the user gets a notification to receive STORE tokens from Storecoin. This notification can be in-app or on email
 - the user either creates new receive addresses (preferred for security reasons) or shares one of the existing receive addresses with Storecoin
 - The tokens are deposited into the shared address.

It is possible to automate creating and sharing receive addresses when the app receives notifications on token issuance.