Boray's User manual

Group-T

Contents

Introduction

Borays is a next-generation cryptocurrency wallet designed to deliver unmatched security by leveraging a unique two-device signing mechanism. Unlike conventional wallets that store a complete private key on a single device, Borays divides the signing authority between two trusted devices—Device A and Device B—ensuring that no transaction can be executed without the explicit consent of both. This architecture mitigates the risk of key compromise, malware-based exploits, and unauthorized access, making Borays ideal for users who demand higher standards of operational security.

Developed as part of an academic project at the University of Wollongong, Borays combines the strength of the Elliptic Curve Digital Signature Algorithm (ECDSA) with Paillier homomorphic encryption to enable collaborative transaction signing without exposing sensitive key material. Each device independently manages part of the cryptographic process, and only through encrypted interaction can a transaction be authorized and broadcast to the blockchain.

This user manual is intended for general users, crypto enthusiasts, and security-conscious individuals who may or may not possess in-depth technical knowledge. It outlines the setup, operation, troubleshooting, and best practices for using Borays in a practical environment. Clear instructions and a step-by-step structure make it easy for first-time users to get started while providing deeper insights for advanced users.

Borays supports token transactions on the Ethereum blockchain and is designed for mobile or cross-platform environments. Whether you're sending assets, checking balances, or pairing devices, this manual will serve as your comprehensive guide to secure cryptocurrency management.

System Overview

Borays is a secure, dual-device cryptocurrency wallet system designed to ensure robust protection of digital assets through distributed cryptographic processing. It employs multiple layers of advanced security, combining cutting-edge cryptographic primitives with a user-friendly interface.

- At the core of Borays is the **Two-Party ECDSA Signing** mechanism. Instead of storing the entire private key on a single device, Borays splits the key across two devices—Device A and Device B—ensuring that no individual device can sign a transaction on its own. This cryptographic split minimizes the risk of key leakage, side-channel attacks, and malware exploits.
- To enable secure interaction between the two devices during transaction signing, Borays integrates the **Paillier Homomorphic Encryption** scheme. This allows Device A and Device B to compute partial signatures over encrypted values, preserving the confidentiality of each device's private share throughout the communication process. Even if communication is intercepted, no usable private key information can be extracted.
- **Mnemonic-Based Recovery** offers users a practical way to back up and restore their wallet. A unique 24-word mnemonic phrase is generated during wallet creation. The first 12 words are used on Device A and the remaining 12 on Device B. Together, they reconstruct the same wallet address while still adhering to the dual-authentication model.

- **Dual Device Authentication** forms a foundational security feature of Borays. Every transaction must be explicitly approved by both devices before it is signed and broadcast to the blockchain. This drastically reduces the risk of unauthorized access, accidental spending, or remote attacks—even in cases where one device is compromised.

Borays also incorporates support for Ethereum-based token transfers, including ERC-20 assets, and is designed for modular extensibility—enabling future enhancements such as biometric authentication, NFT management, and smart contract interaction.

Quick Start Guide

This section provides a simplified, step-by-step walkthrough for first-time users to set up and begin using the Borays Wallet on two separate devices. Follow these instructions carefully to ensure a secure wallet configuration.

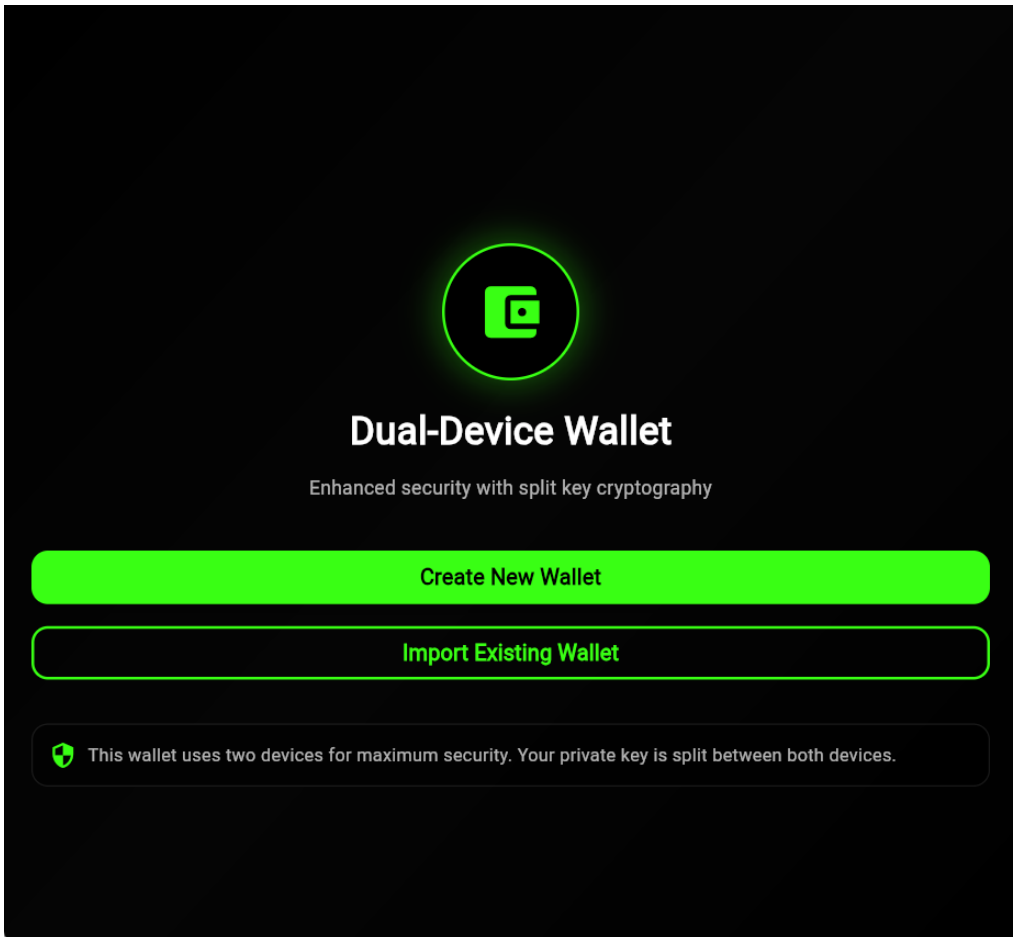

Figure 1 Home page

Step 2: Create a New Wallet on Device A

1. Launch the app on **Device A**.
2. Tap on **"Create Wallet"** from the home screen.

3. The system will generate a **24-word mnemonic recovery phrase**.

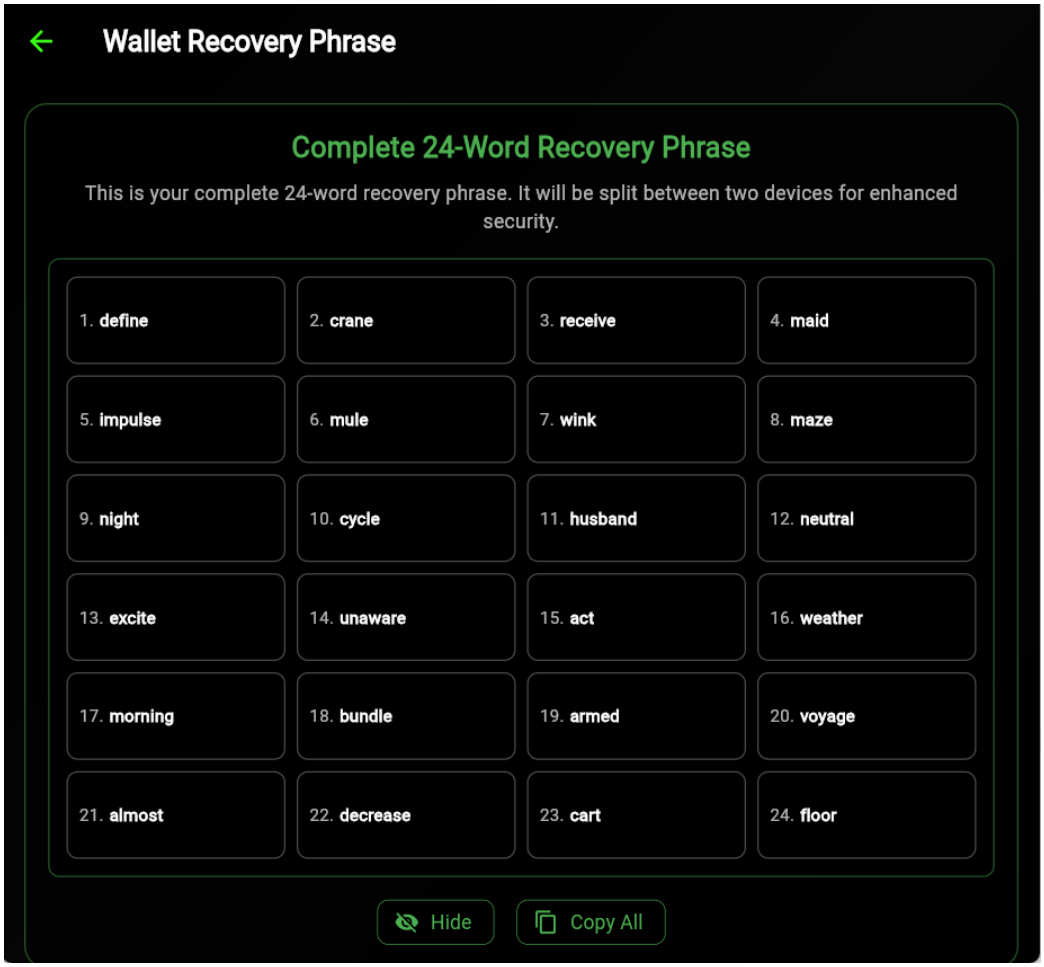

Figure 2 Complete 24-word recovery phrase

Step 3: Backup the Mnemonic Phrase

1. Write down all **24 mnemonic words** in the exact order displayed.
2. **Split the phrase**:
    - Use **Words 1–12** on Device A.
    - Use **Words 13–24** on Device B.
3. Keep the full phrase secure and never share it online.

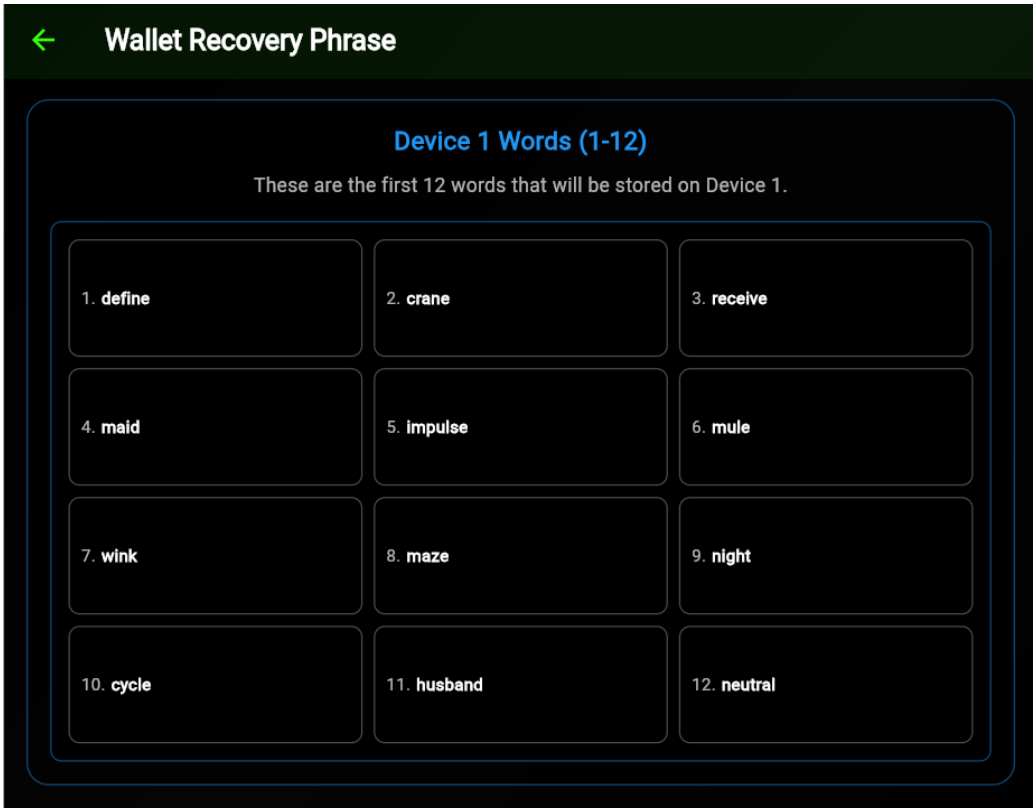

Figure 3 Device-1 recovery phrase

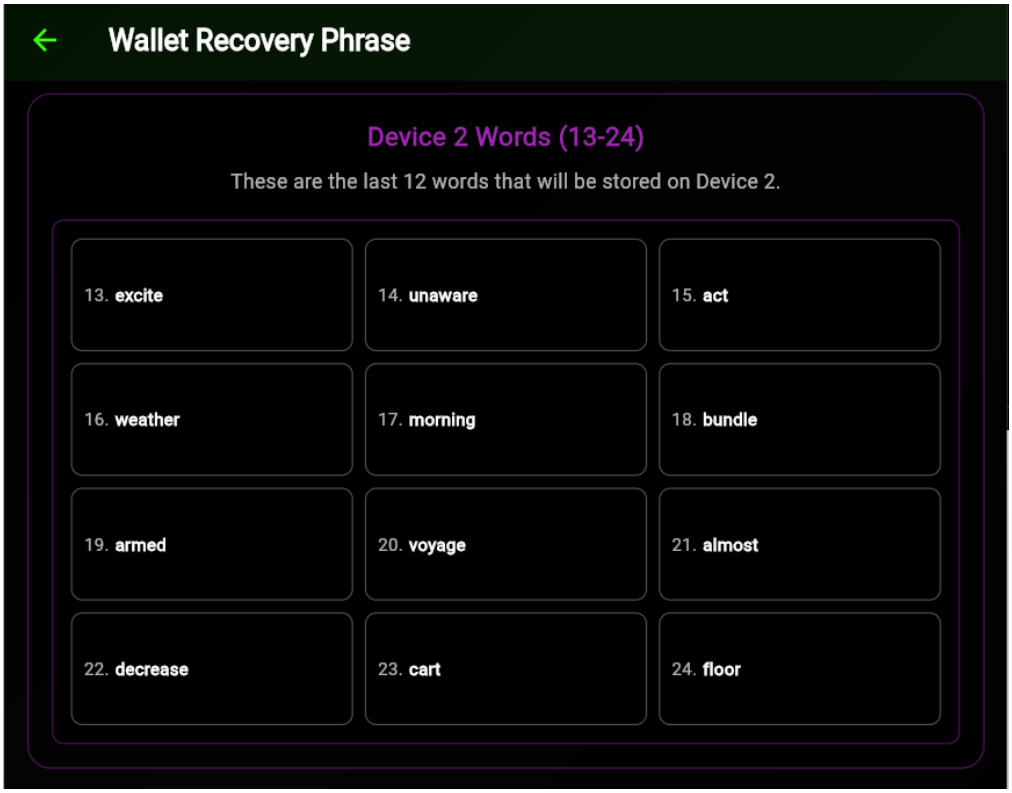

Figure 4 Device-1 recovery phrase

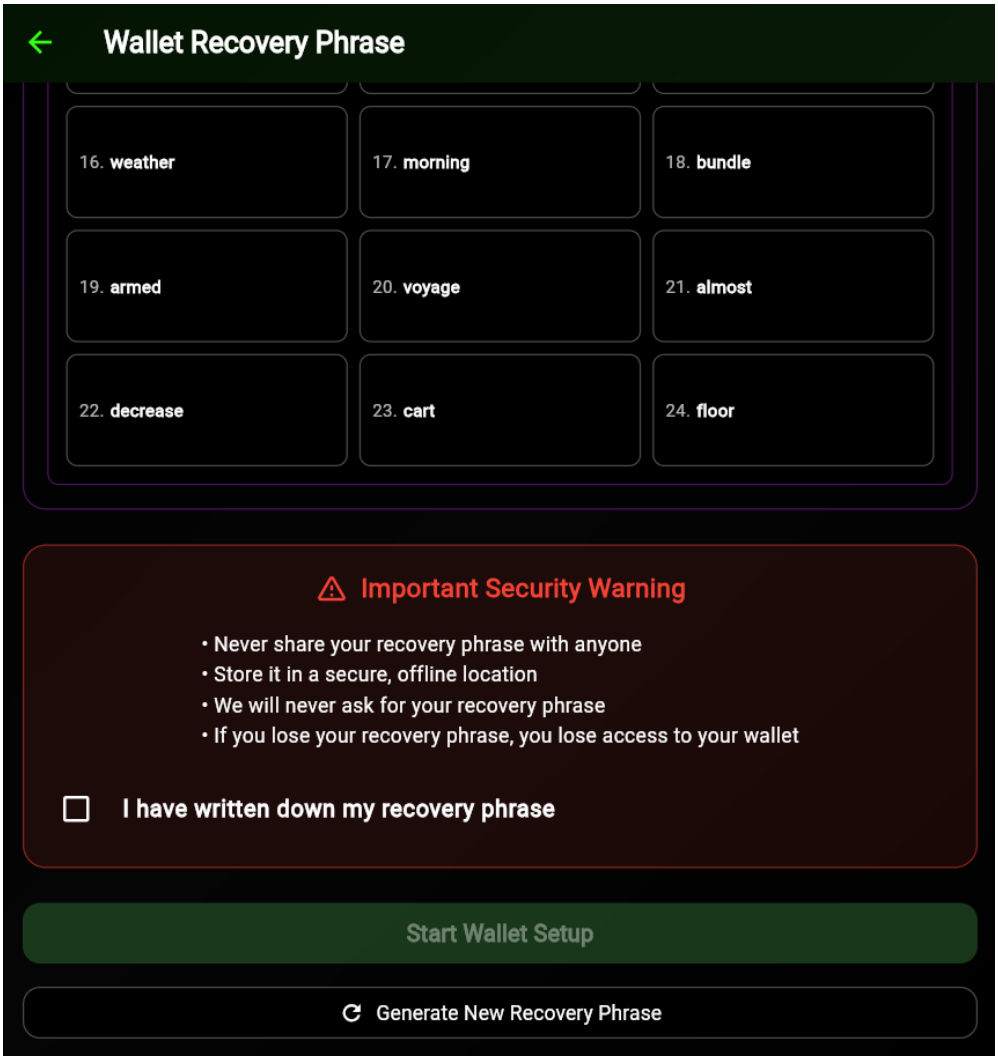

Figure 5 Setup wallet phase

📝 *Tip: Store your phrase offline (paper or encrypted USB) for recovery purposes.*

Step 4: Set Secure Passwords on Both Devices

Each device will prompt you to set a **local access password**.

- Use a strong combination of letters, numbers, and symbols.
- This password is required to access your portion of the wallet.

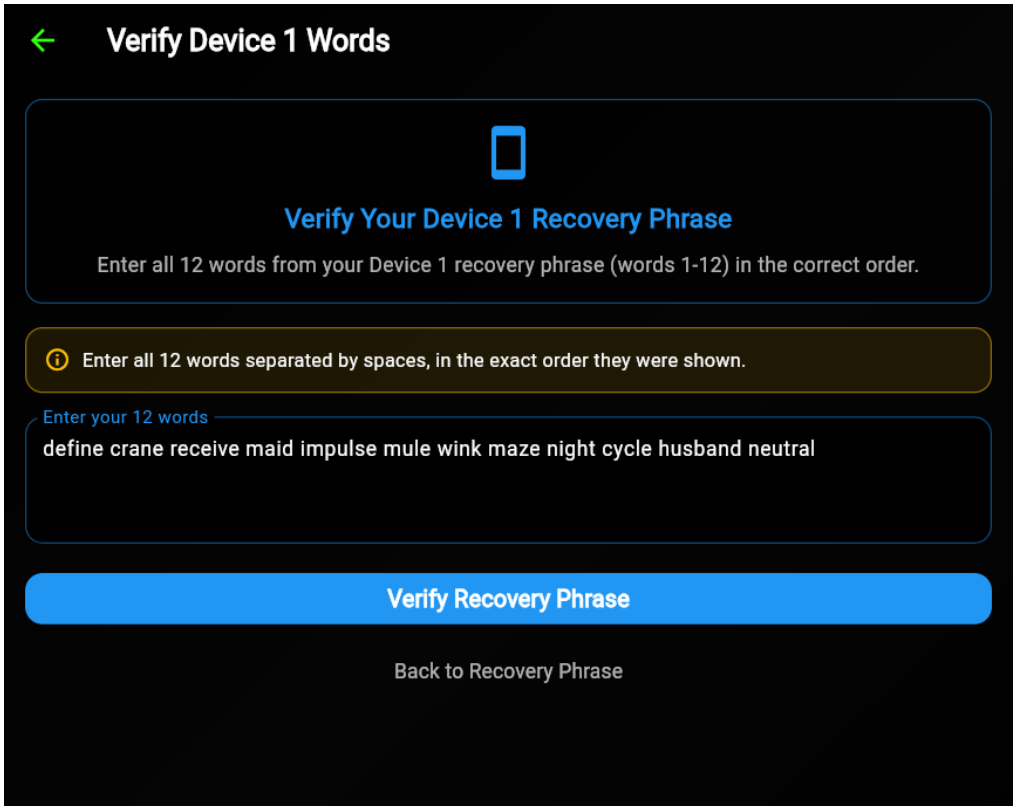

Figure 6 Device-1 Setup phase

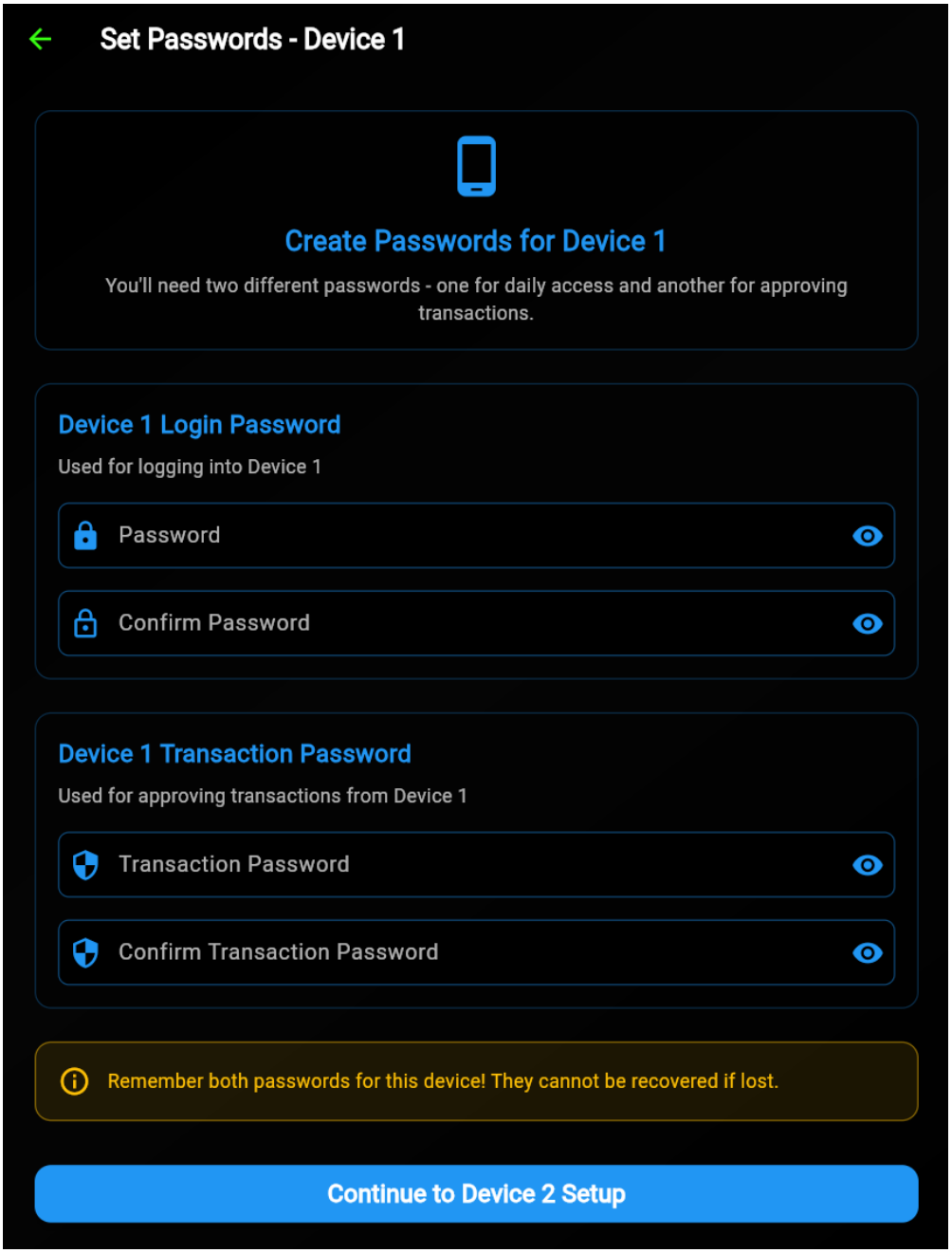

Figure 7 Device-1 Password setup phase

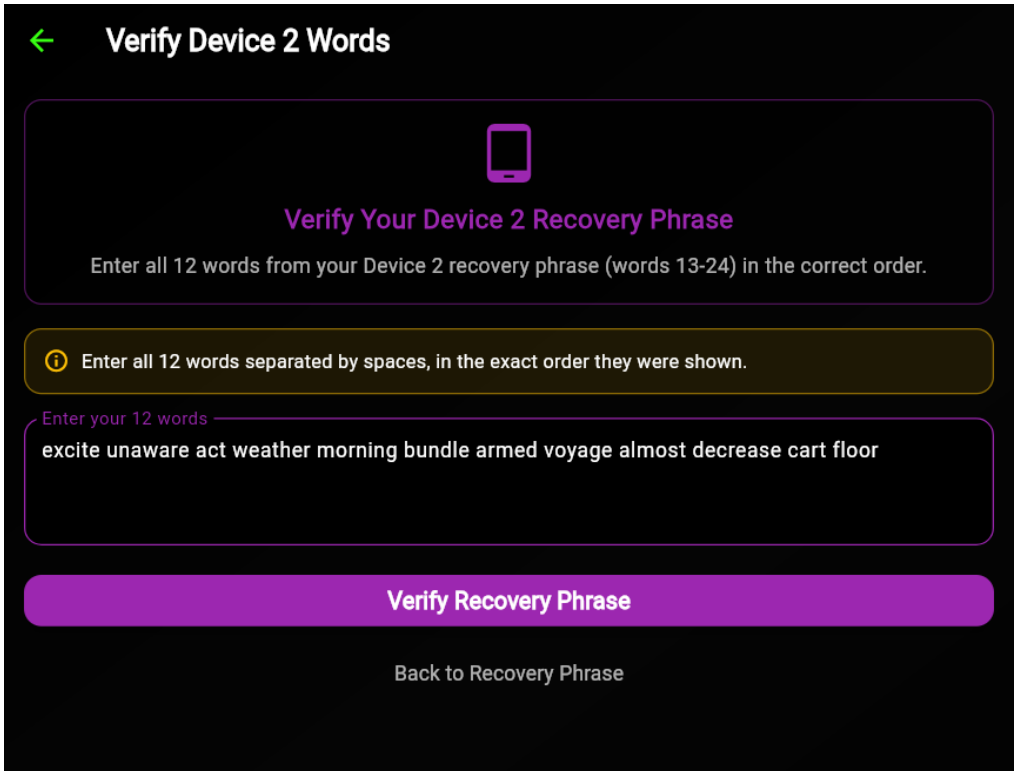

Figure 8 Device-2 Setup phase

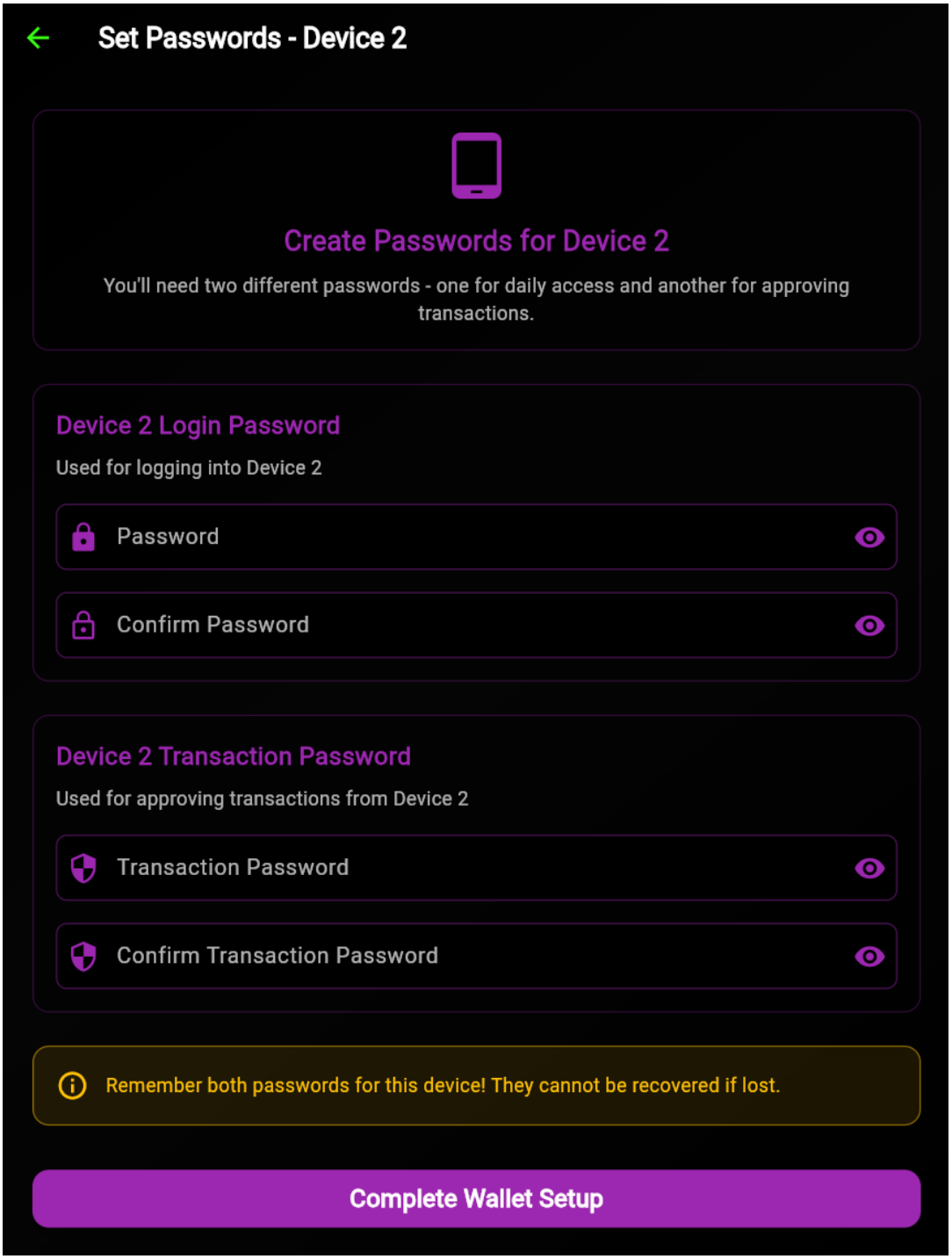

Figure 9 Device-2 Password setup phase

Step 6: Start Using Borays

Once both devices are paired:

- You can now **Send** and **Receive** tokens.
- Device A can initiate transactions.
- Device B must approve each transaction request for it to be valid.

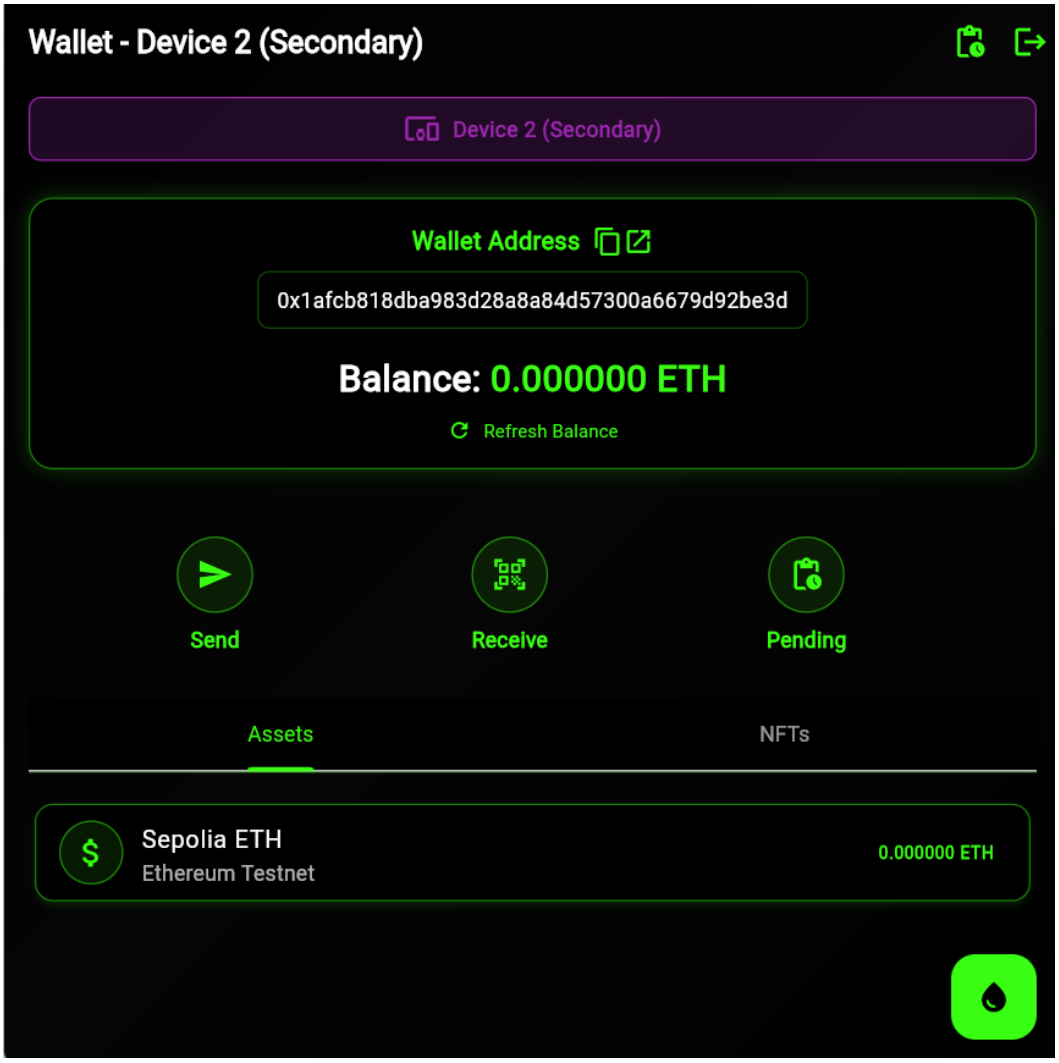

Figure 10 Device-2 Dashboard

We can use the import method to login to device-1, which is explained later in this document.

Importing a wallet

If you've previously created a Borays wallet and need to restore it on a new or reset device, use the Import from Seed feature. This allows either Device A or Device B to be independently recovered using their respective portion of the 24-word mnemonic phrase.

Step 2: Select "Import from Seed"
Tap the Import from Seed button to begin the recovery process.

Figure 11 Device import page

Step 3: Enter Your 12-Word Mnemonic Segment
Enter the 12-word portion of the recovery phrase assigned to this device:

On Device A: enter Words 1–12

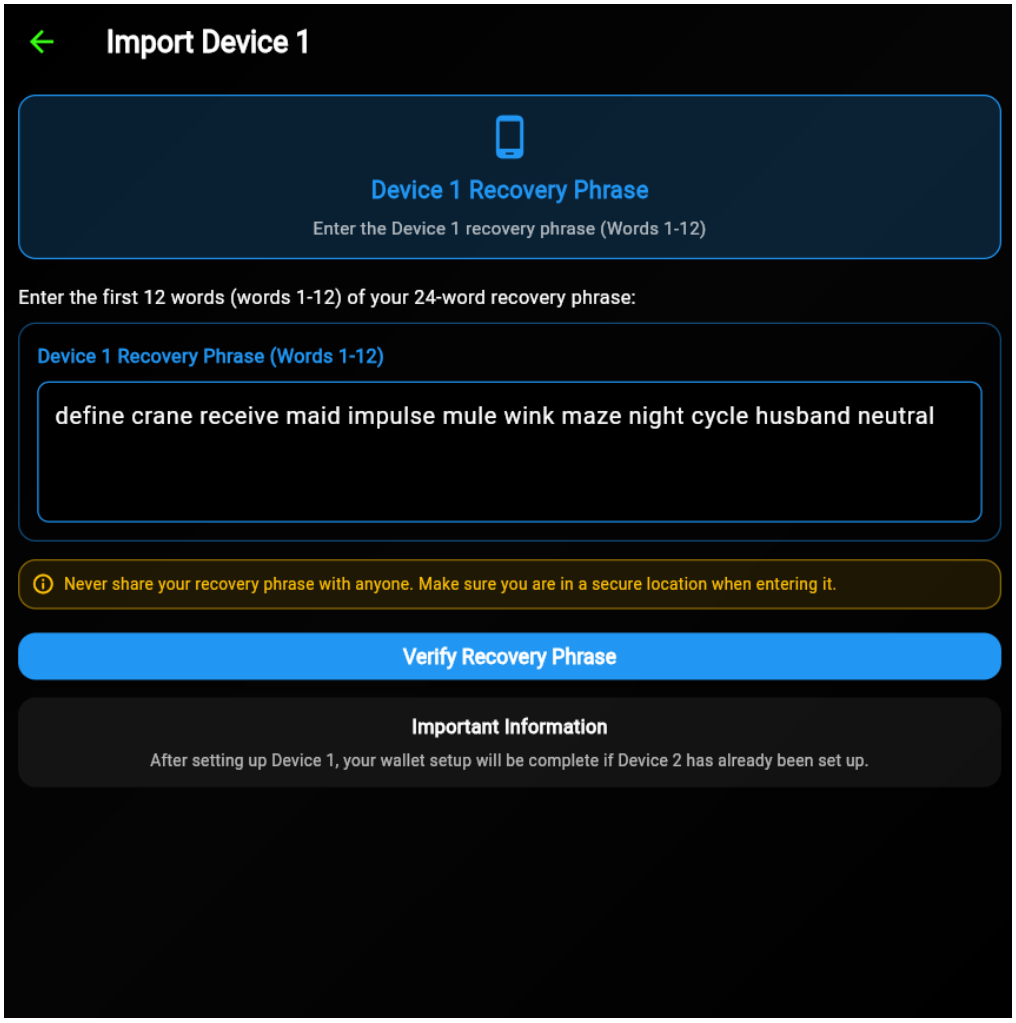

Figure 12 Device-1 Import page

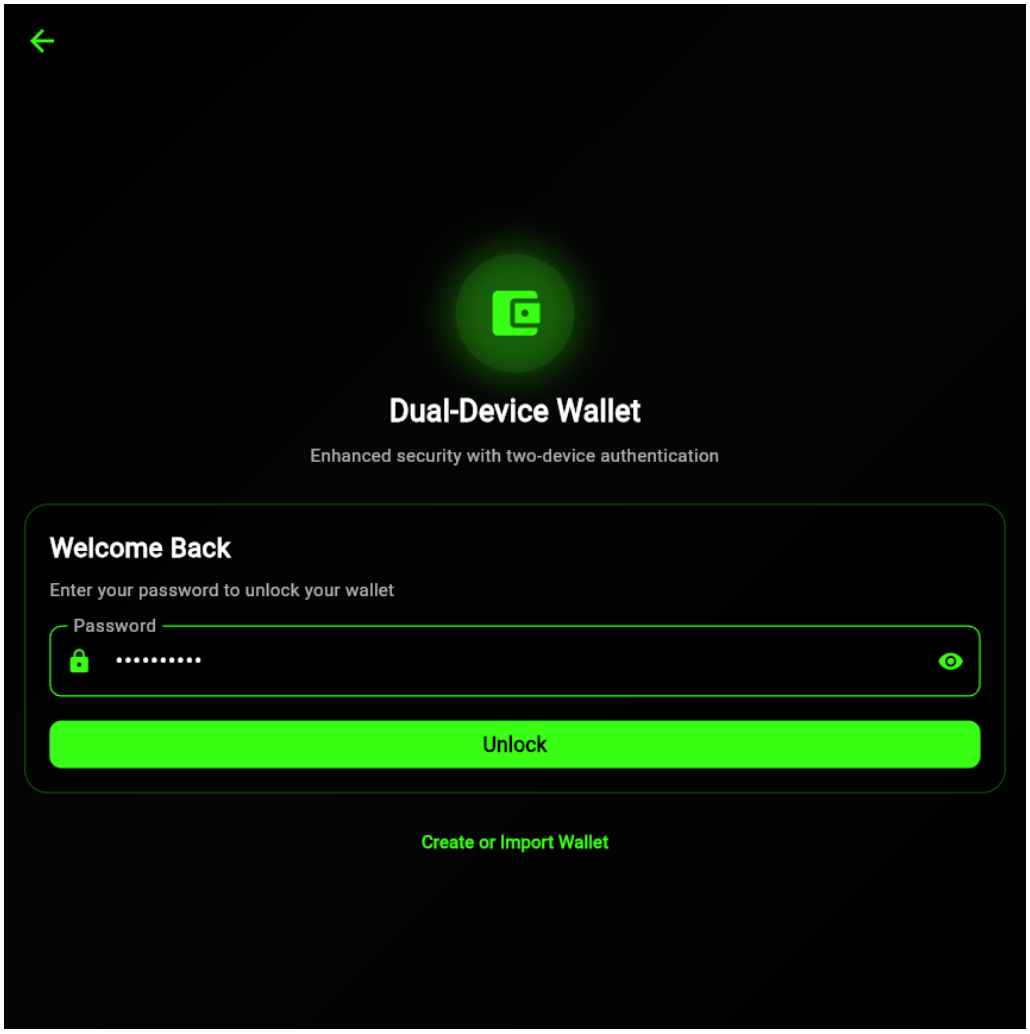

Figure 13 Device-1 password page

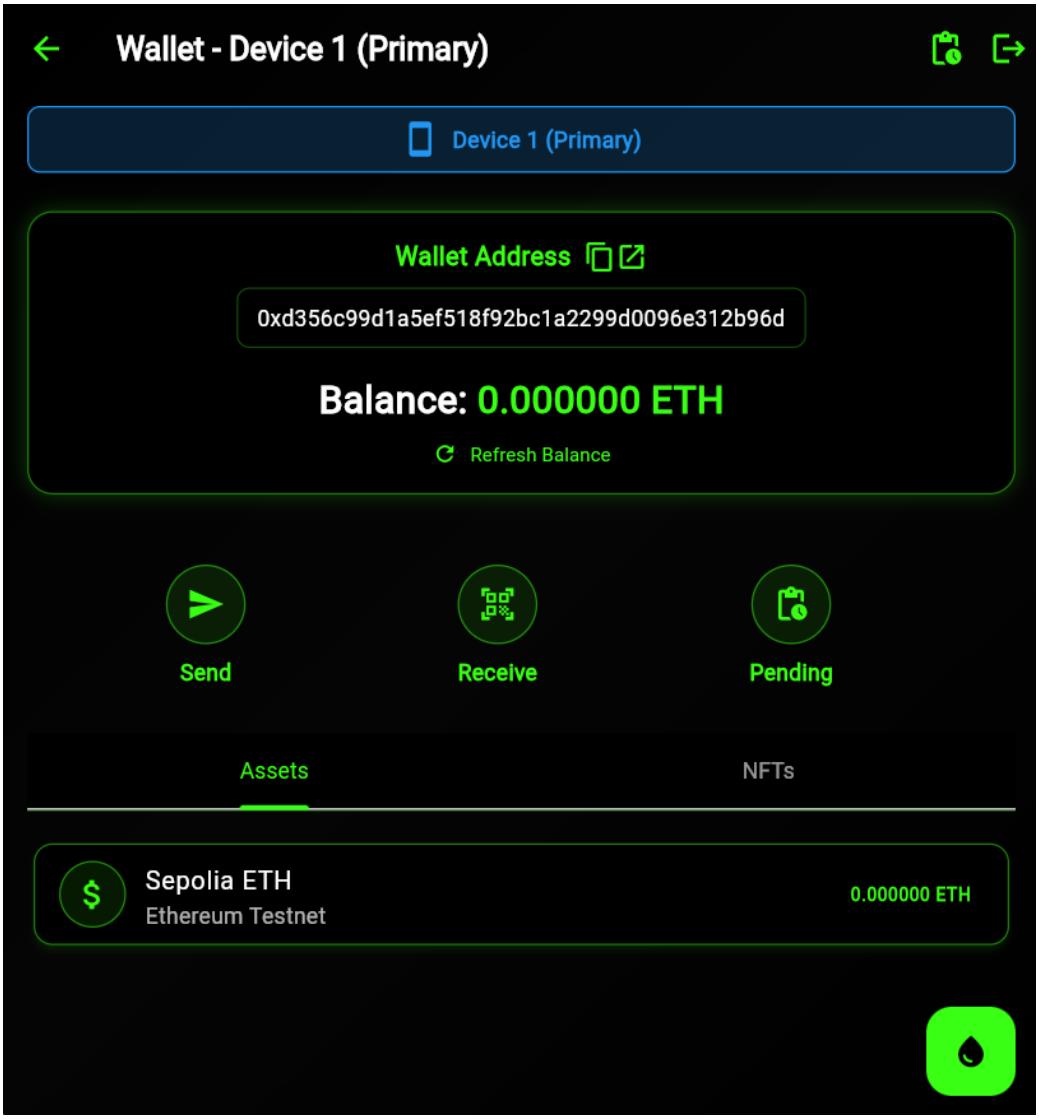

Figure 14 Device-1 Dashboard imported successfully

On Device B: enter Words 13–24

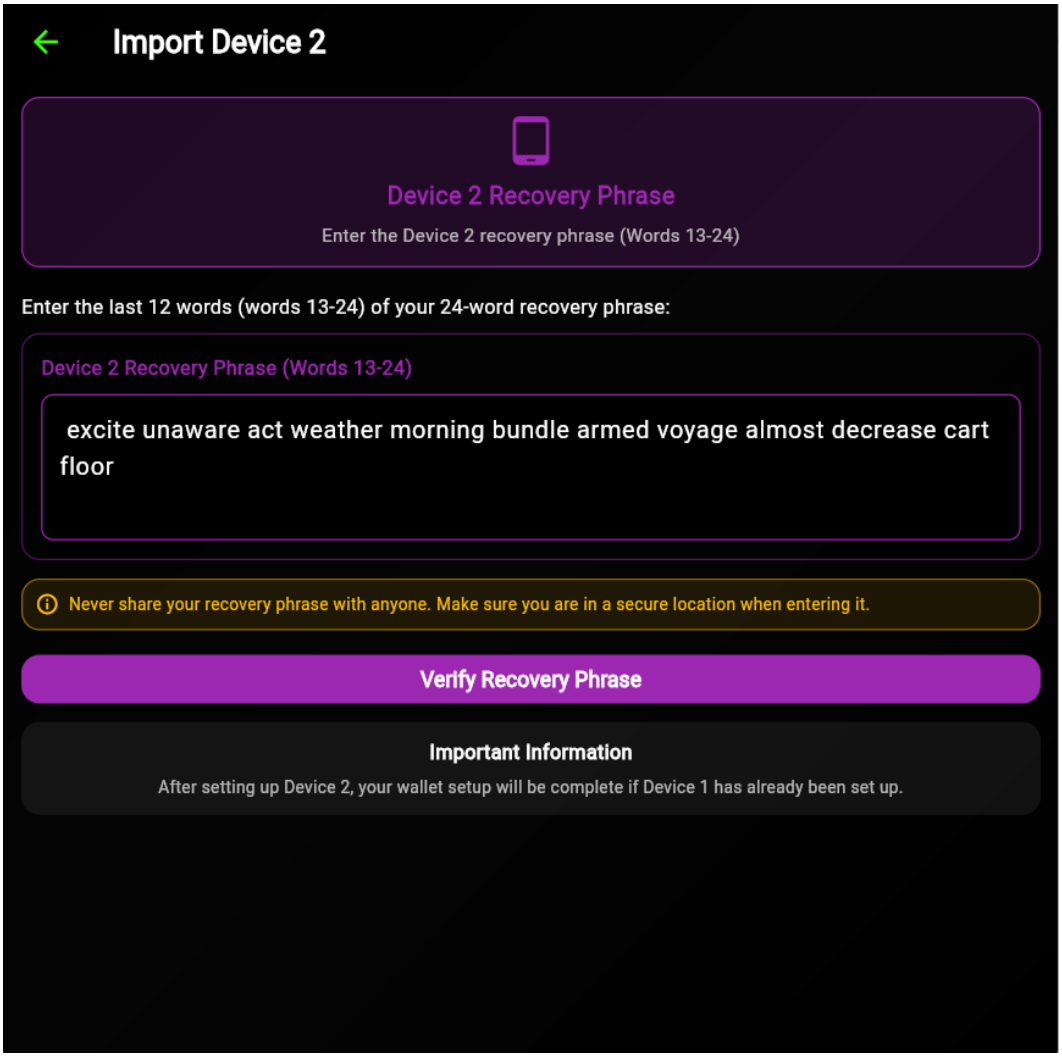

Figure 15 Device-2 Import page

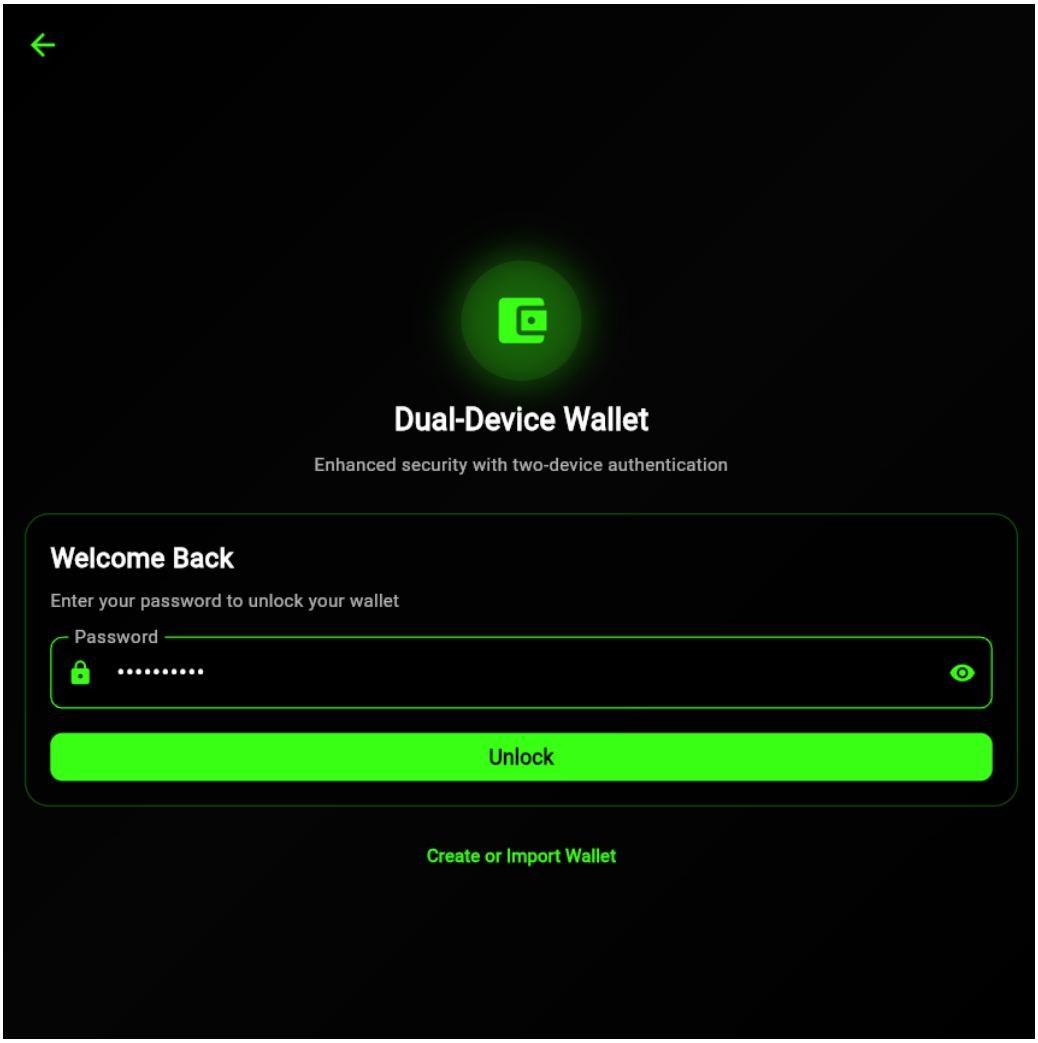

Figure 16 Device-2 password page

📝 Double-check spelling and word order. Import will fail if the phrase is incorrect.

Step 5: Wallet Address Verification
After successful import and password setup:

The device will reconstruct its assigned portion of the wallet.

The wallet address will be displayed.

If the correct mnemonic was used, the address will match the one from the original wallet setup.

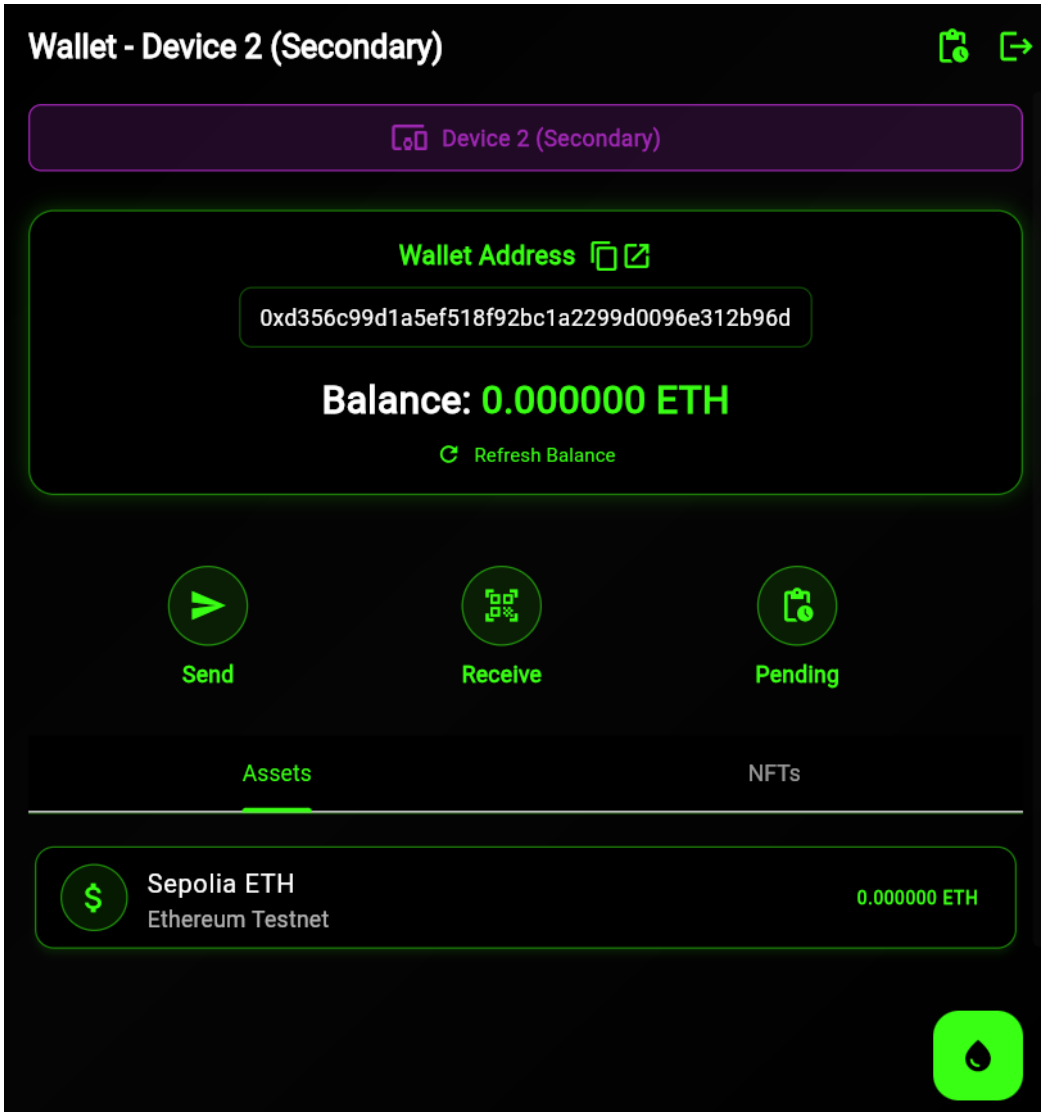

Figure 17 Device-2 Imported successfully

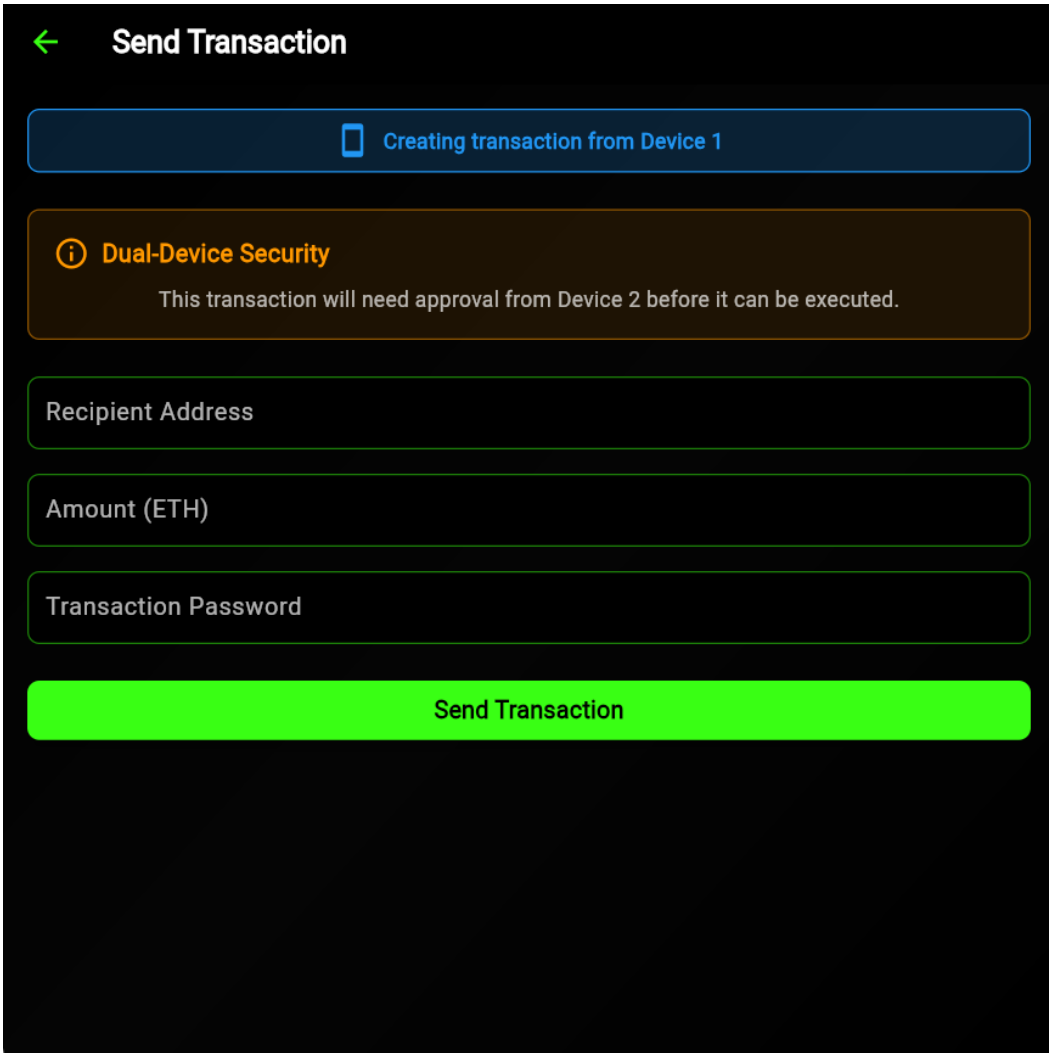

Figure 18 Device-1 Transaction page

Figure 19 Device-1 Receive page

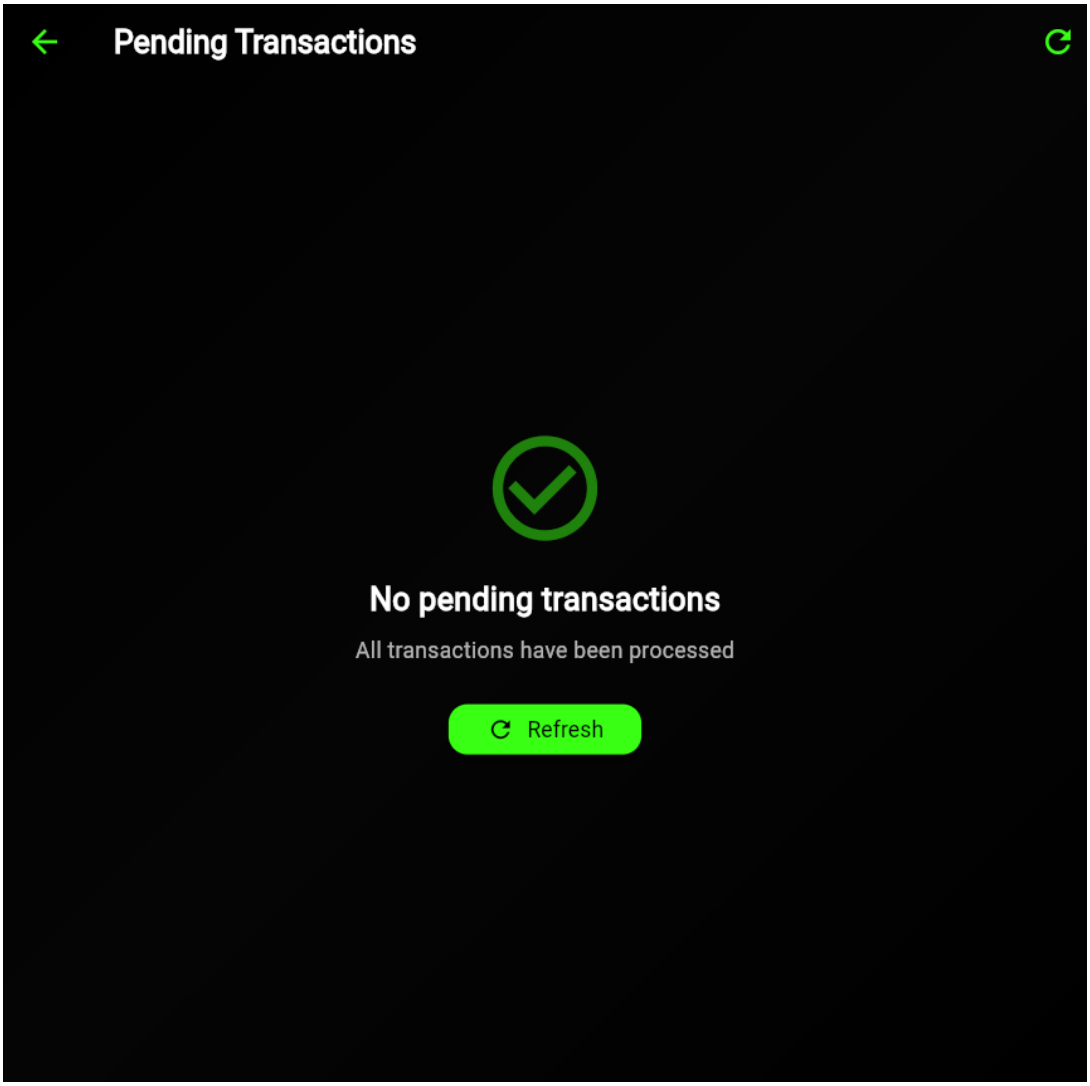

Figure 20 Device-1 pending transaction page

These pages will be same for both the wallets in device 1 and 2.

Receiving Cryptocurrency

You can test this out by following the below link:

https://cloud.google.com/application/web3/faucet/ethereum/sepolia

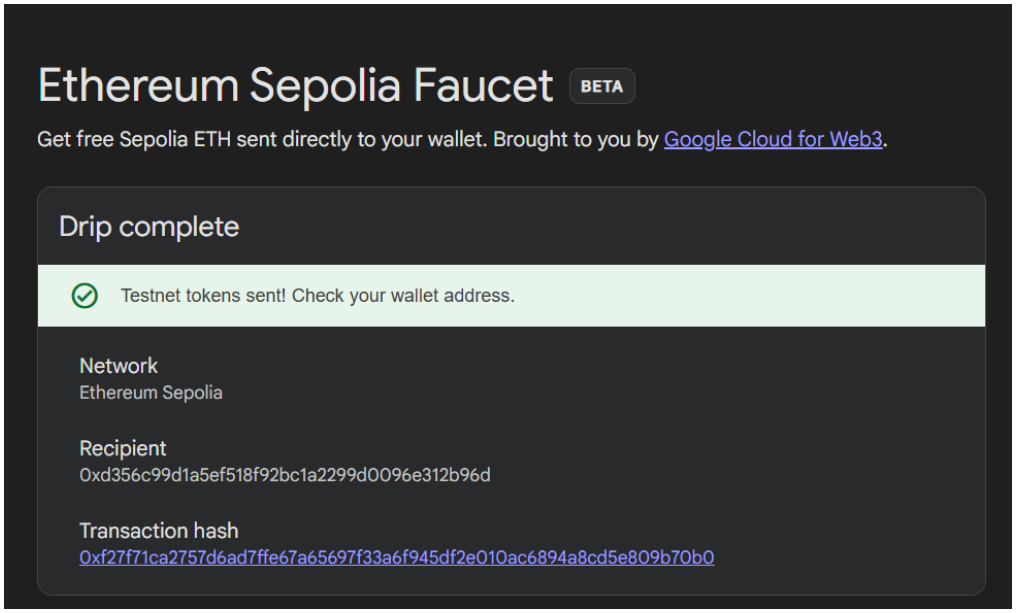

Figure 21 Ethereum test tokens

Then press enter, after that you can check the balance of Ethereum in your wallet

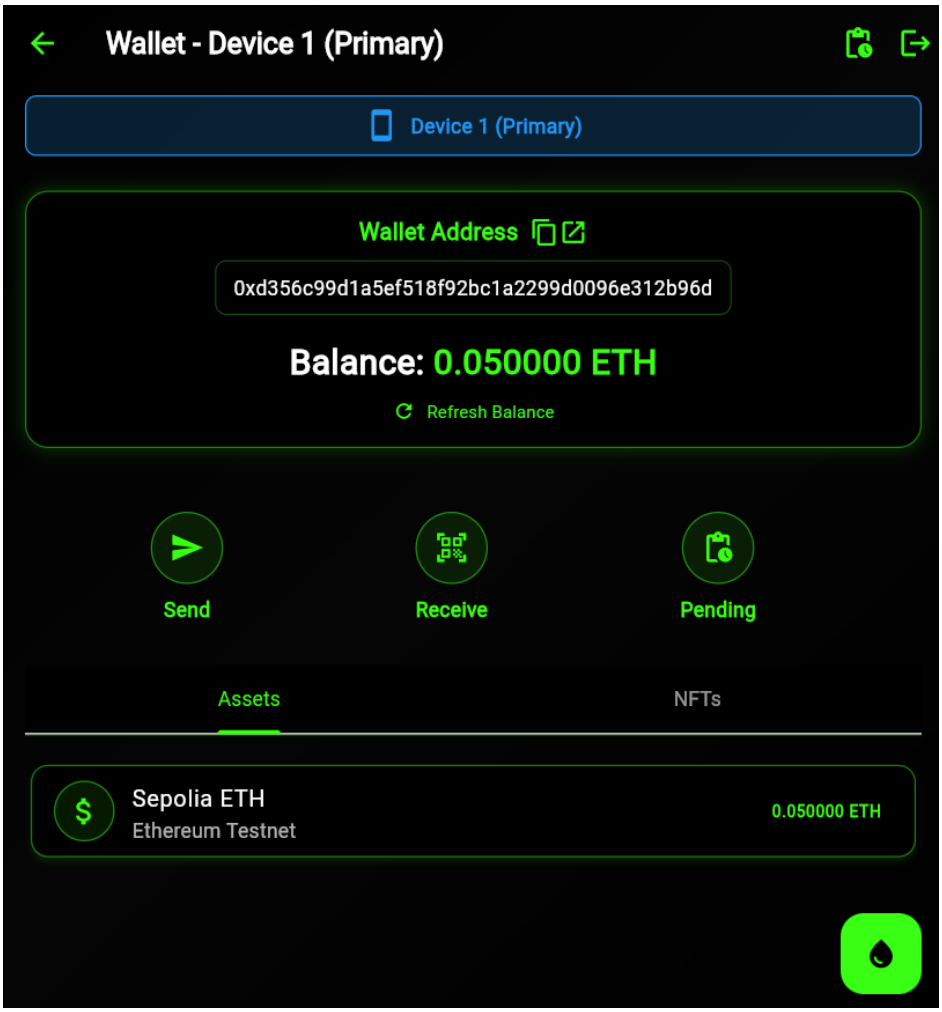

Figure 22 Ethereum received successfully

Then you can enter any wallet address to whom you want to send the Ethereum.

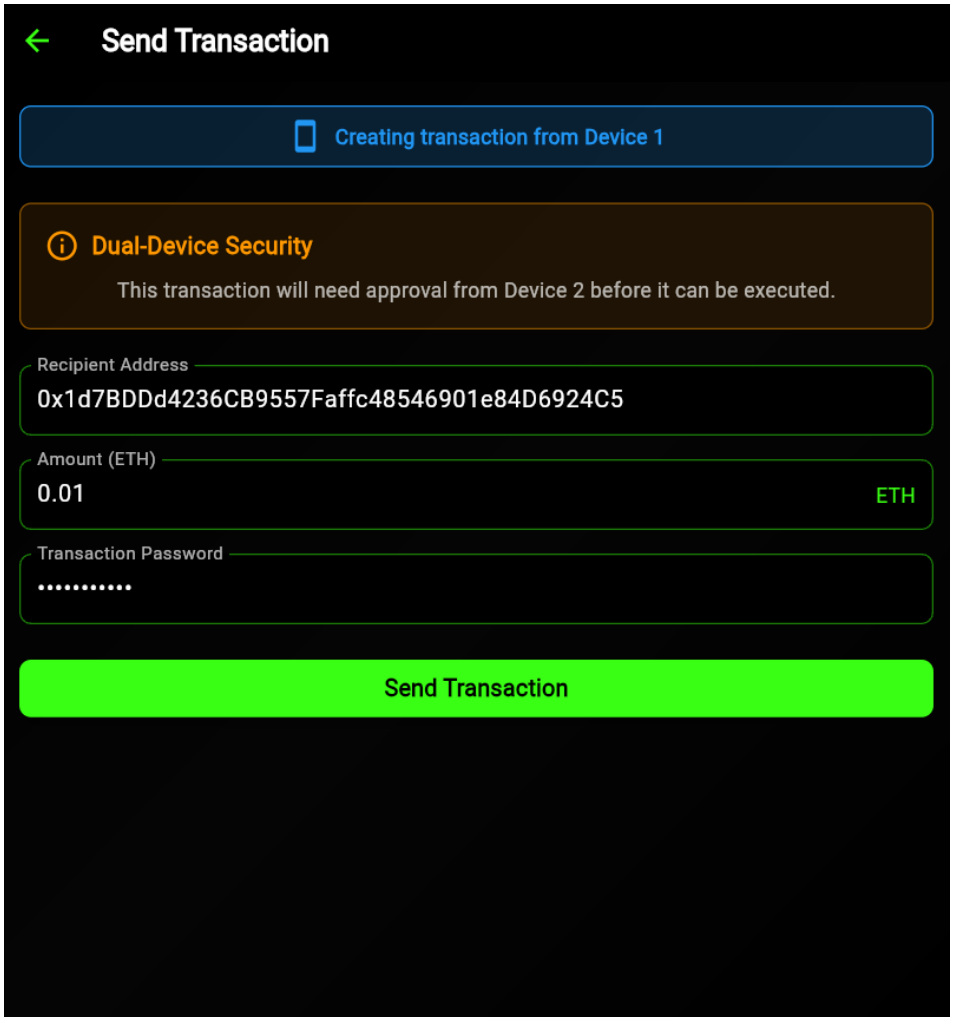

Figure 23 Sending Ethereum

Here, I have entered the address of another wallet to send Ethereum. I have also given the amount and password to process the transaction.

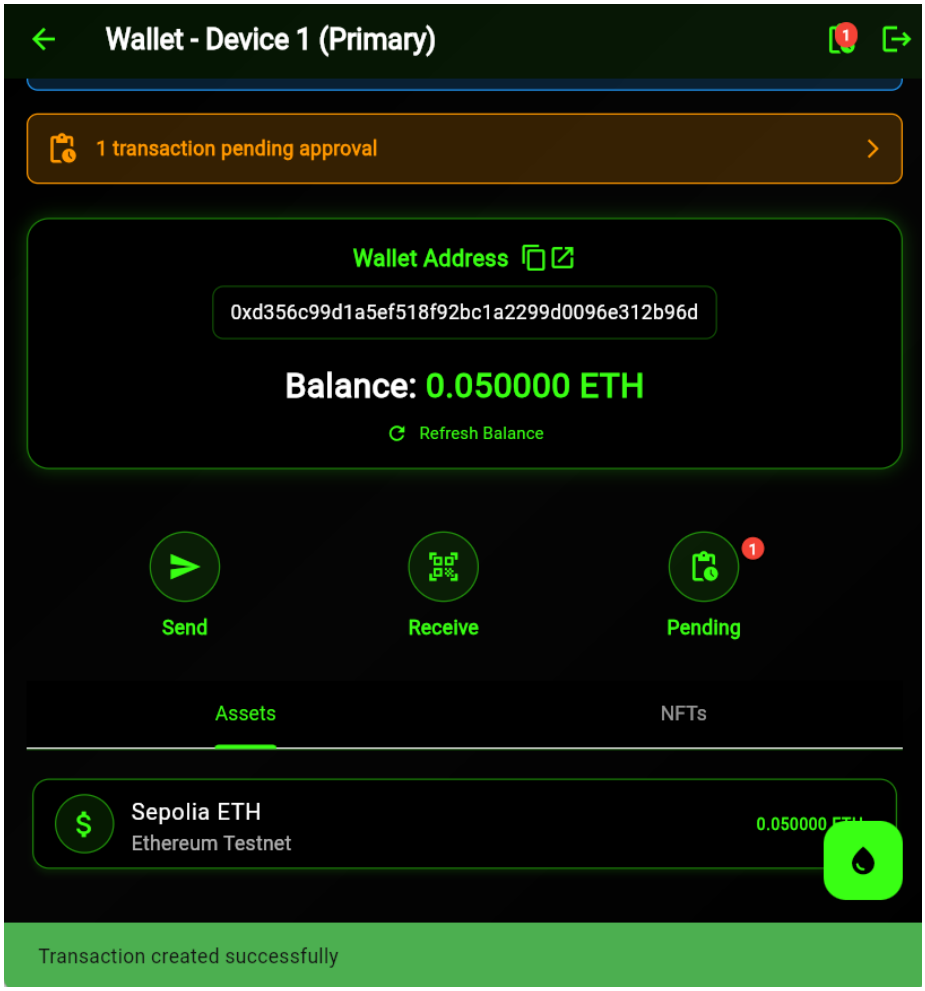

Figure 24 Transaction Initiated from device-1

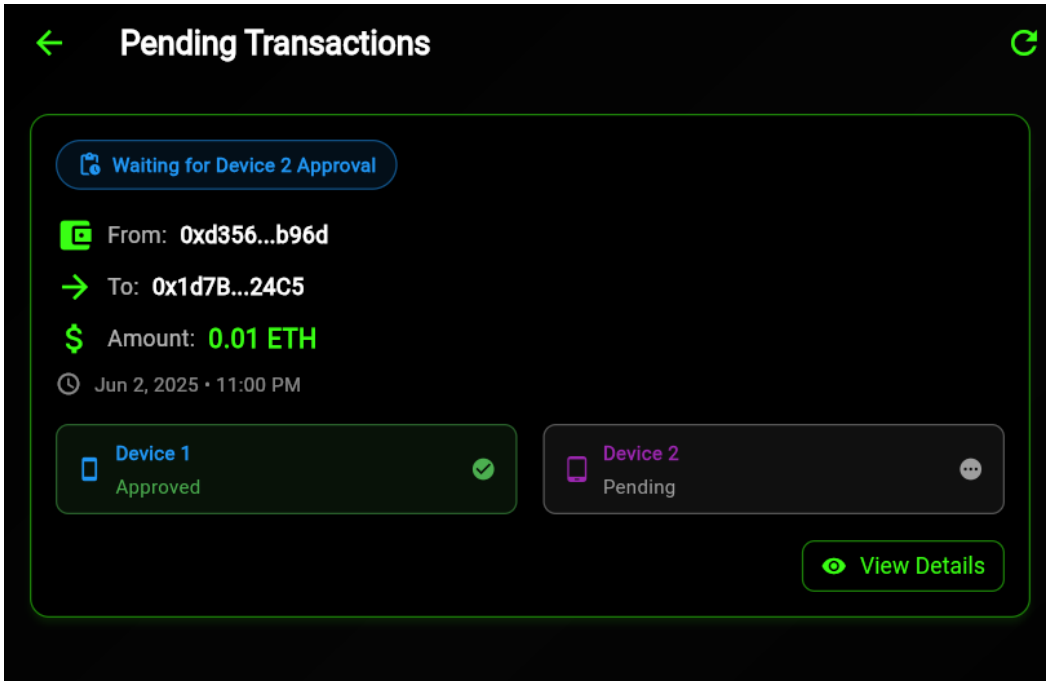

Figure 25 Pending Transaction in device-2

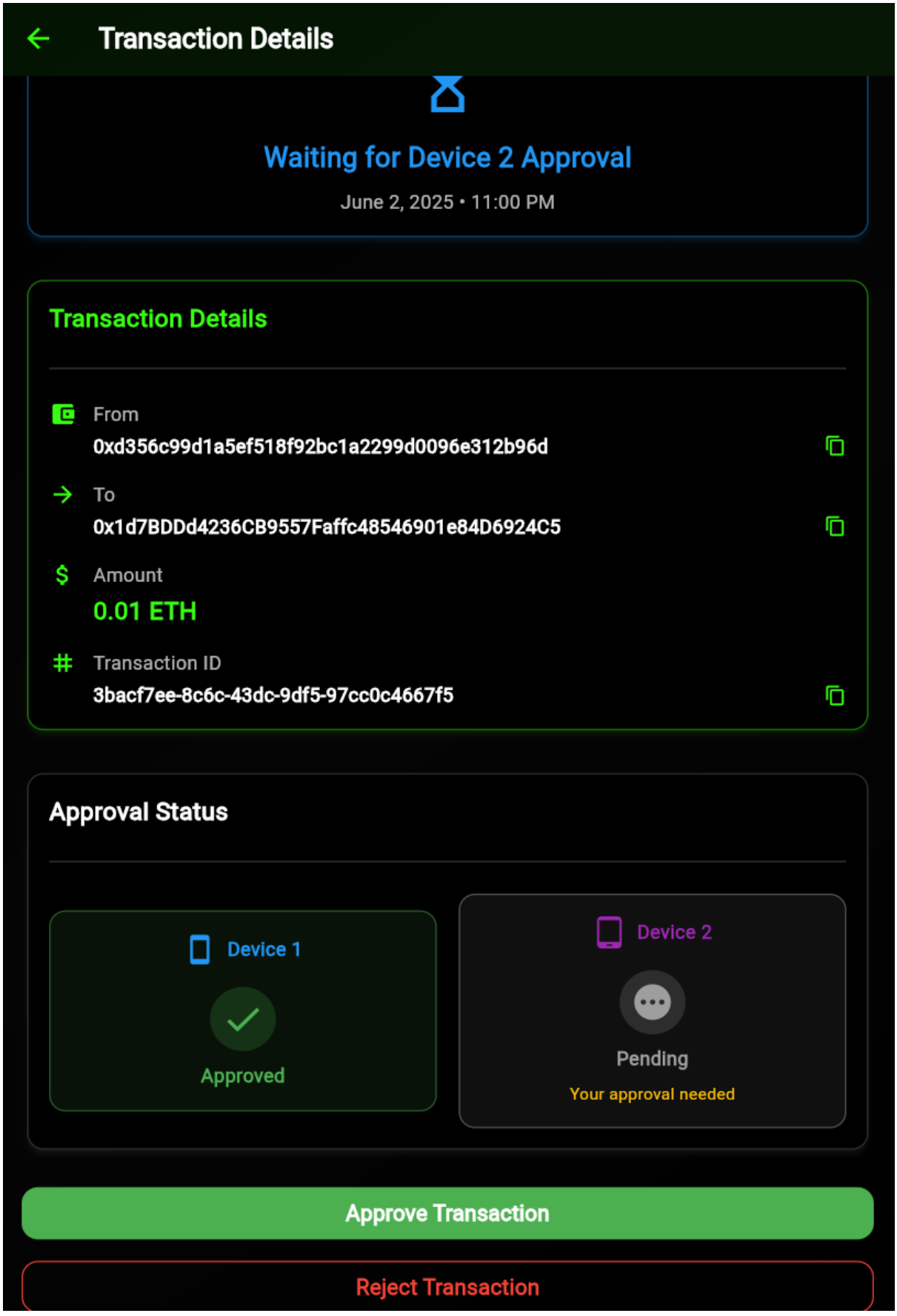

Figure 26 Device-2 Approval page

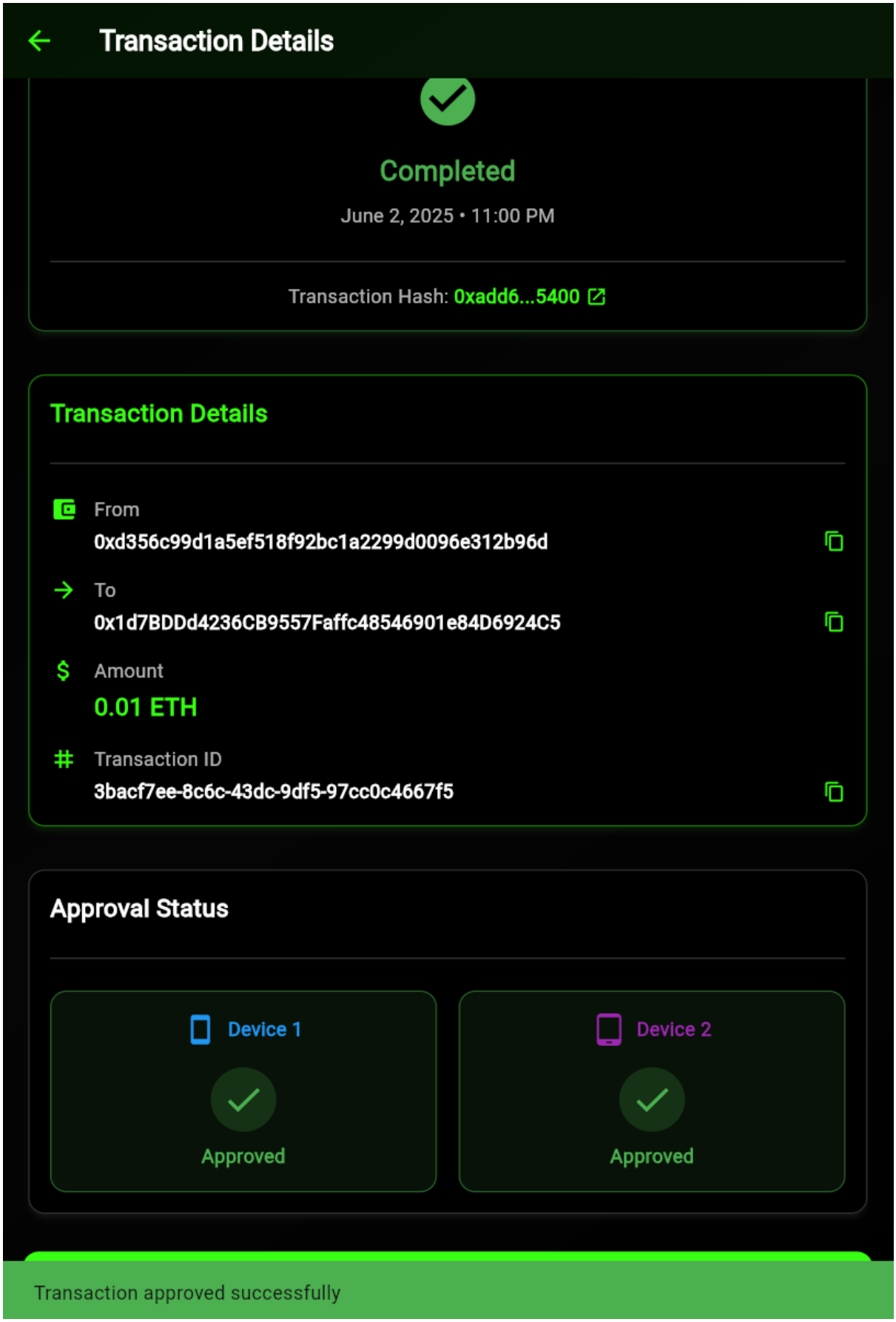

Figure 27 Transaction approved

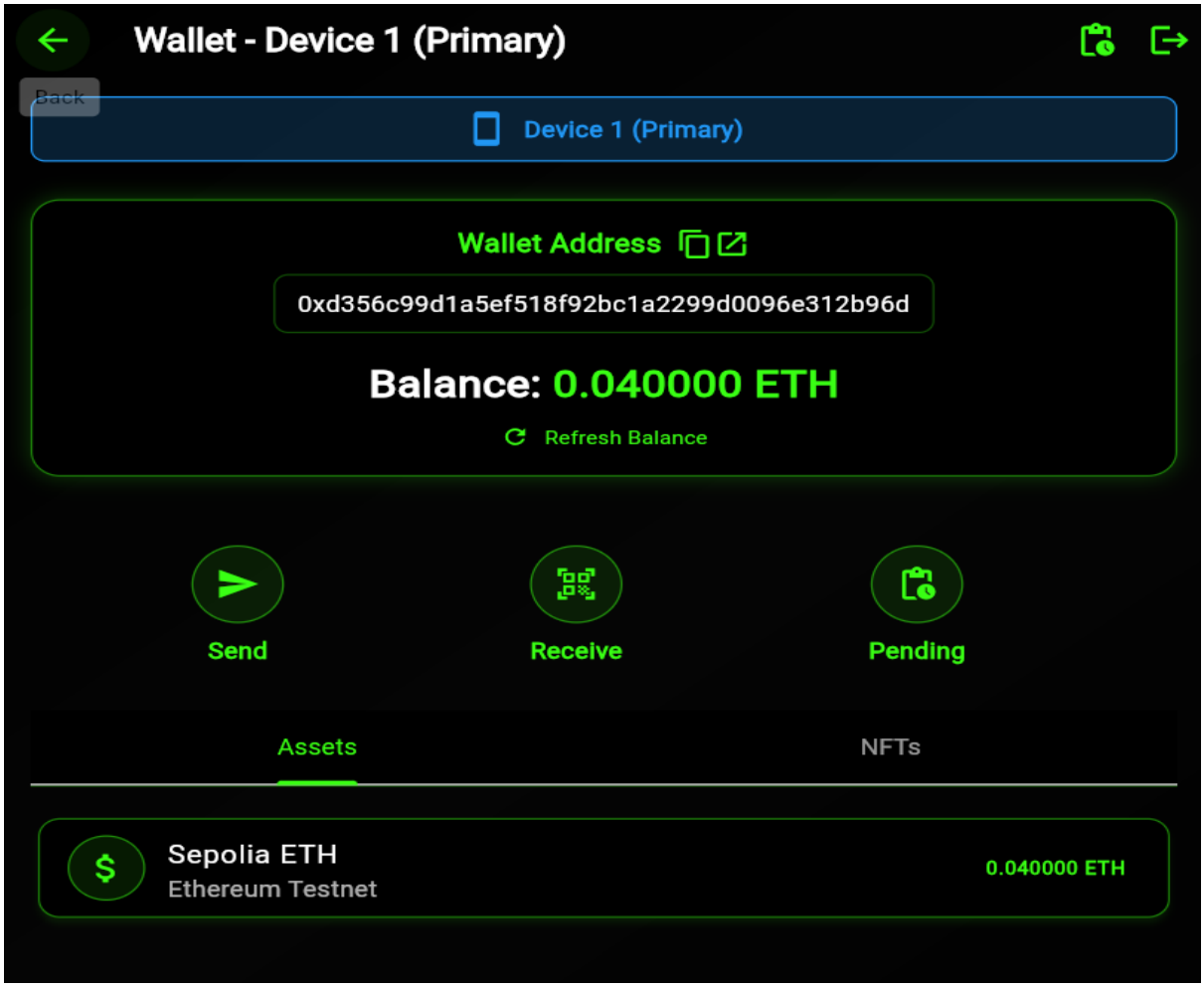

Figure 28 Updated Balance after transaction

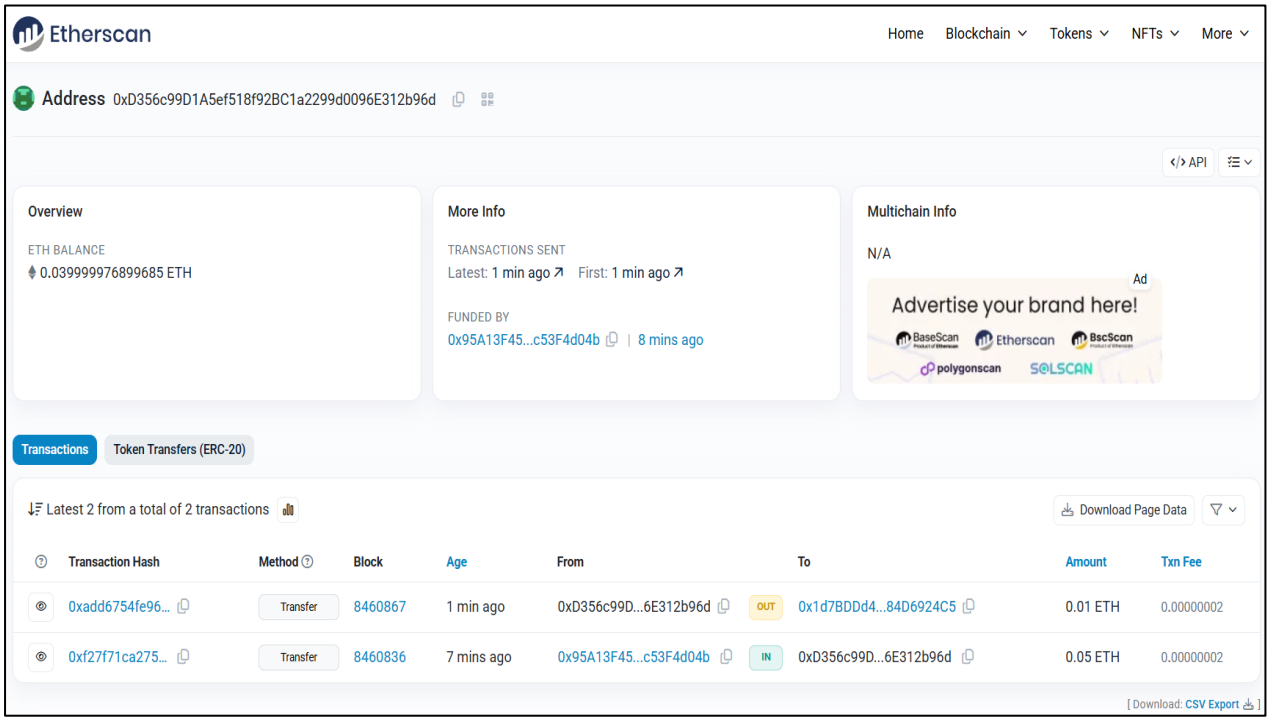

Figure 29 Verifying the authenticity of the transaction

Wallet Features and Management

The Borays wallet provides users with a secure and intuitive interface to manage tokens, view assets, and adjust important settings—all while maintaining the system's core security principles.

1. Balance

Once both devices are set up and paired, users can access real-time account information on **Device A** or **Device B**.

- **Token Balance**:
  The **Dashboard screen** shows the current Ethereum and token balances, updated directly from the blockchain.

3. Settings and Wallet Management

The **Settings** tab includes essential options to control and maintain your wallet experience:

- **Log Out**: Securely log out of the wallet on the current device.
- **Restore Wallet**: Re-import using your mnemonic phrase in case of app reinstallation or device replacement.

4. Security Features

Borays has been architected with security-first principles:

- **Private Key Never Reconstructed**:
  Your private key is split using a two-party ECDSA scheme. No single device ever holds the full key at any point.
- **Paillier Encryption for Communication**:
  During transaction signing, the partial keys and approvals are exchanged using Paillier homomorphic encryption. This ensures:
    - All signatures are securely computed.
    - No sensitive information is leaked during communication.
- **Local Password Protection**:
  Each device enforces its own password gate, adding a second layer of protection.
- **Device Isolation**:
  Even if one device is compromised, transactions cannot be processed without the other.

Frequently Asked Questions (FAQ)

Q1: What happens if I lose one device?

Use the mnemonic phrase on a new device and re-pair.

Q2: Can I send cryptocurrency from one device only?

No. Both devices must approve each transaction.

Q3: What encryption does Borays use?

ECDSA for digital signatures, Paillier encryption for secure exchange.

Q4: How is my mnemonic stored?

It's entered manually and not stored. Keep it safe offline.

Q5: Can I use the same wallet on more than two devices?

No. Only two devices are supported per wallet setup for security.

Troubleshooting Guide

Issue	Cause	Solution
Transaction approval stuck	Device B closed or unresponsive	Reopen app and check Pending Approvals
App crashes	Compatibility or storage issues	Clear cache or reinstall latest version

Safety Recommendations

- Always store the mnemonic phrase **offline**.
- Do not share pairing codes with anyone.
- Regularly back up your data.
- Lock devices with secure PINs or biometrics.

Support & Contact

This application is developed as an academic project by **Group T – University of Wollongong**.

For queries or demo support:

Email: support@borayswallet.com

Documentation: https://github.com/kyathamvinay/Borays-Dual-wallet.git