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.

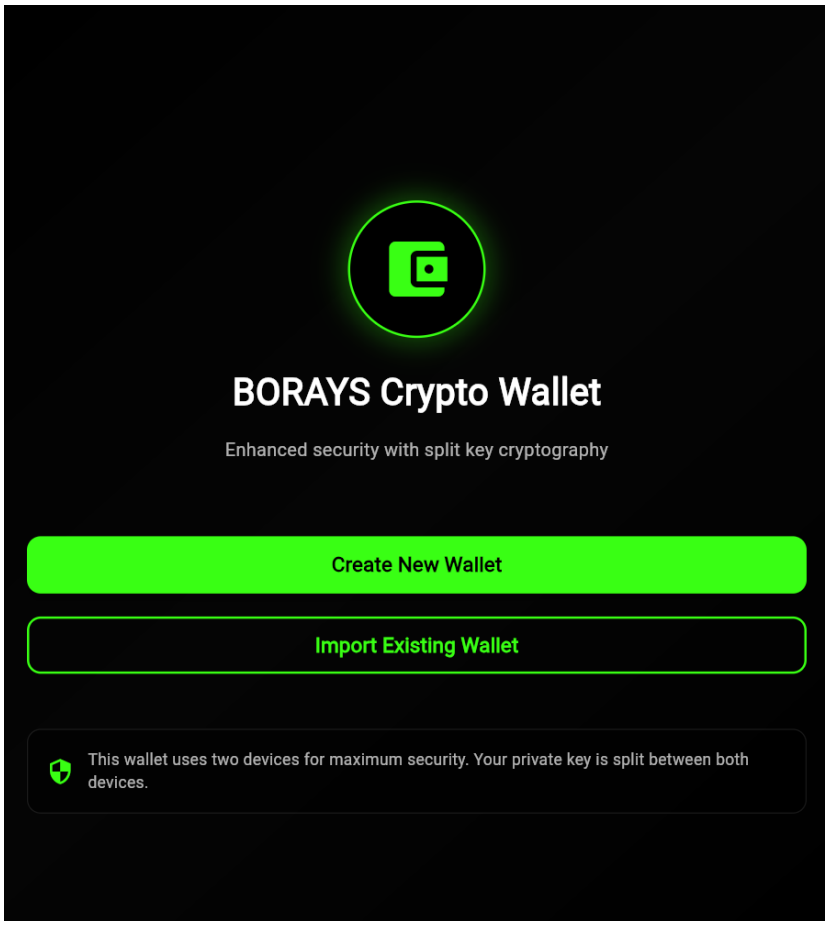

Figure 1 Home page

Step-1: Creating a Wallet

This is the initial screen users see upon launching the Borays application. It offers two primary actions:

- **Create Wallet**: For first-time users to generate a new dual-device wallet.

- **Import Wallet**: For users who wish to recover an existing wallet using mnemonic phrases.

The minimalist layout ensures ease of navigation and reduces onboarding friction for beginners.

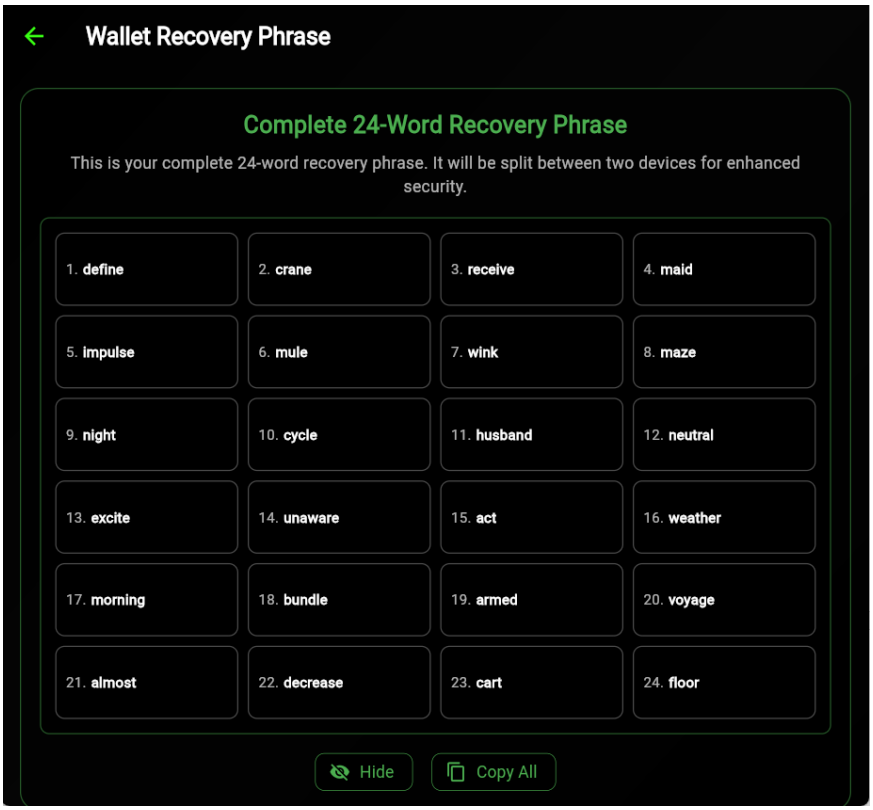

Figure 2 Complete 24-word recovery phrase

Once “Create Wallet” is selected, Borays generates a 24-word mnemonic phrase, critical for wallet recovery. This screenshot emphasizes:

- The unique phrase should be backed up immediately.
- The entire phrase is shown only once and never stored within the application. Security-conscious users should write it on paper or store it securely offline.

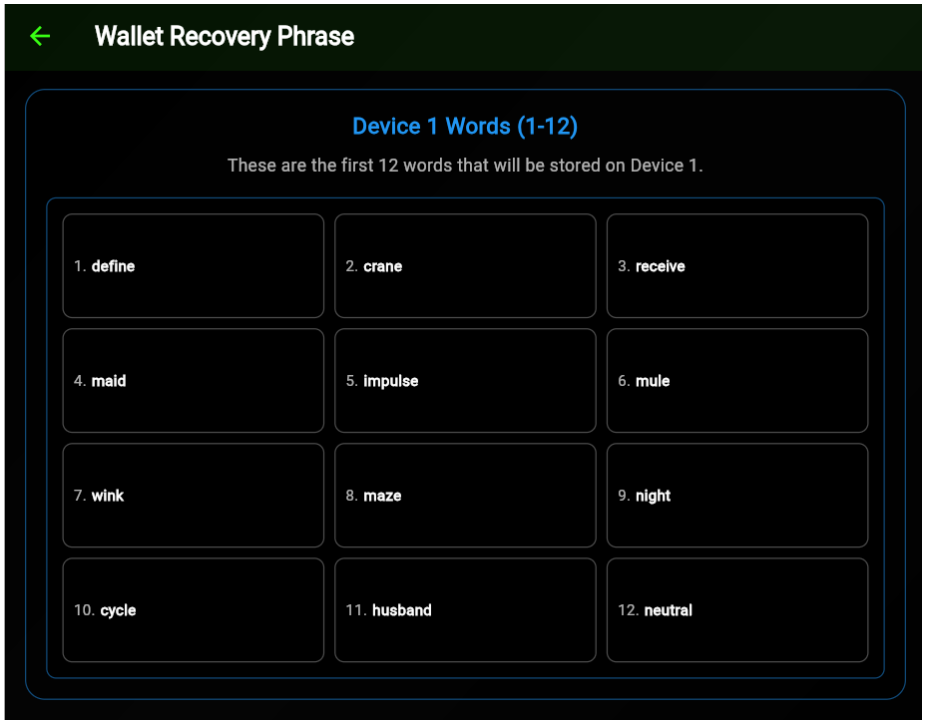

Figure 3 Device-1 recovery phrase

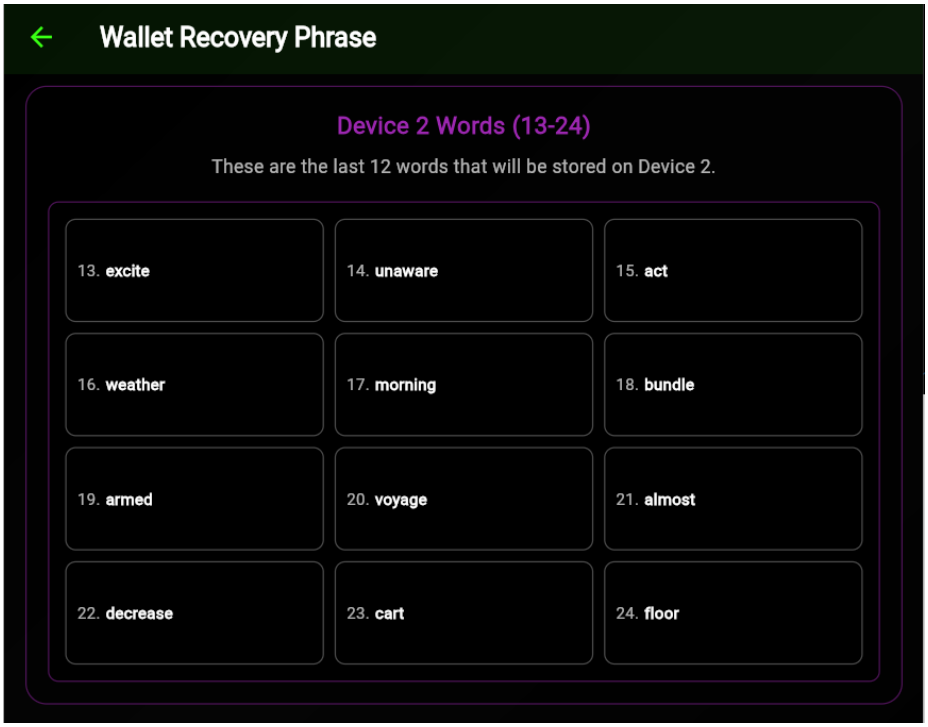

Figure 4 Device-1 recovery phrase

Borays instructs users to split the 24-word phrase:

- **Words 1–12 go on Device A**.
- **Words 13–24 go on Device B**.

These images guide Device A users through securely storing their share. Visual consistency ensures clarity during this crucial step.

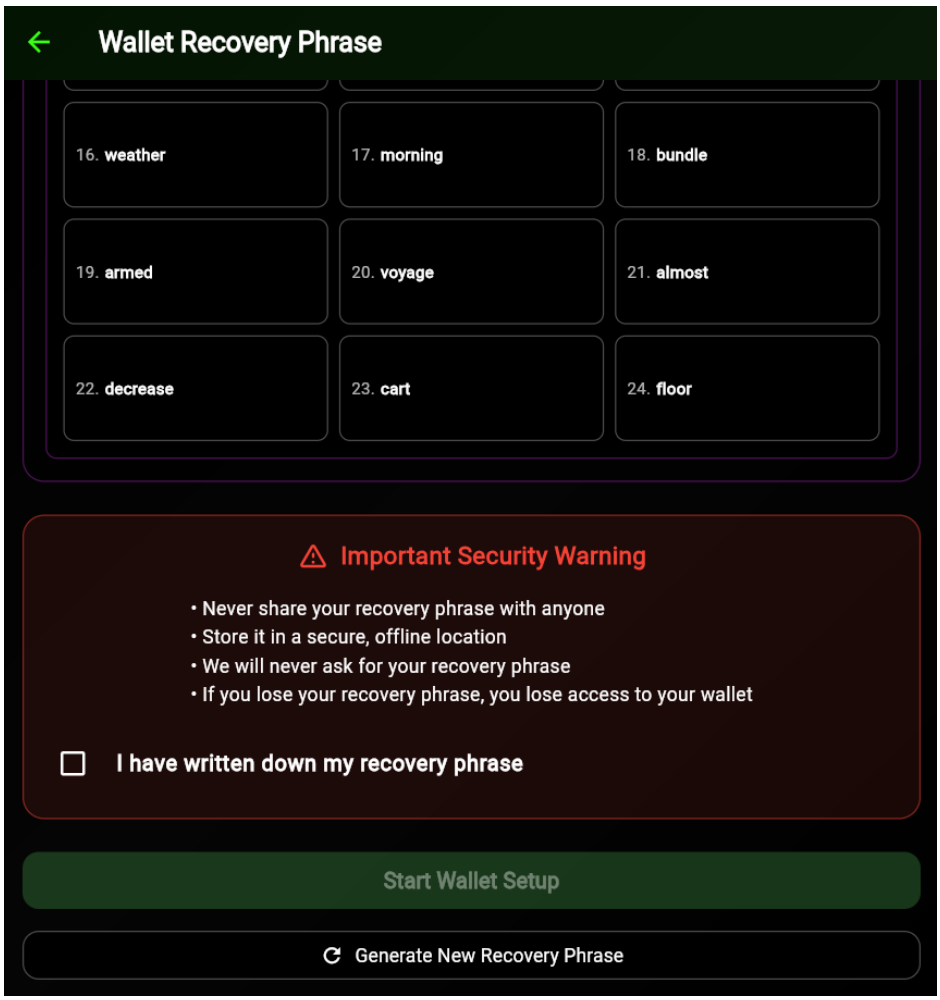

Figure 5 Setup wallet phase

This stage shows a transitional phase between mnemonic generation and password creation. The interface prompts users to proceed cautiously and reminds them of the wallet's dual-structure requirements.

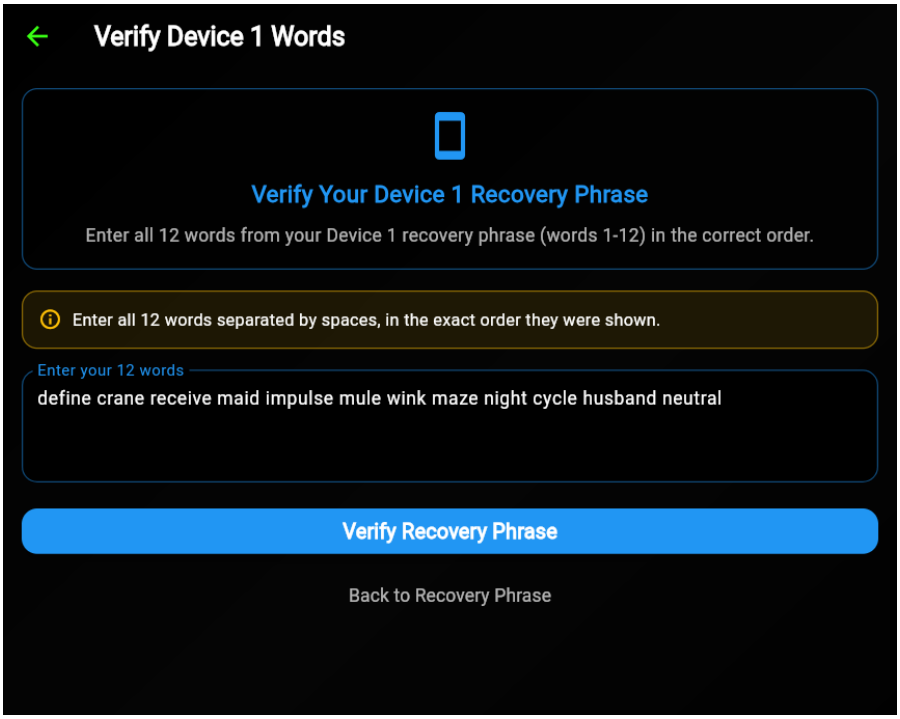

Figure 6 Device-1 Setup phase

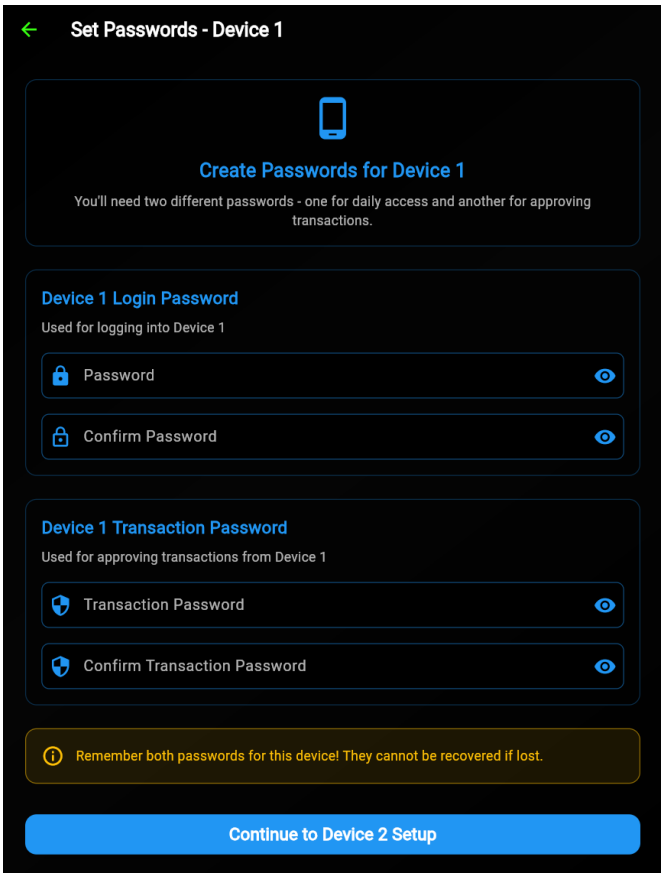

Figure 7 Device-1 Password setup phase

Step-2: Setting up devices

These figures depict password creation on Device A.

Users are asked to:

- Set a secure password for local access.
- Use strong entropy—combining symbols, numbers, and upper/lowercase characters. This local password acts as an additional line of defence beyond the device's native OS security.

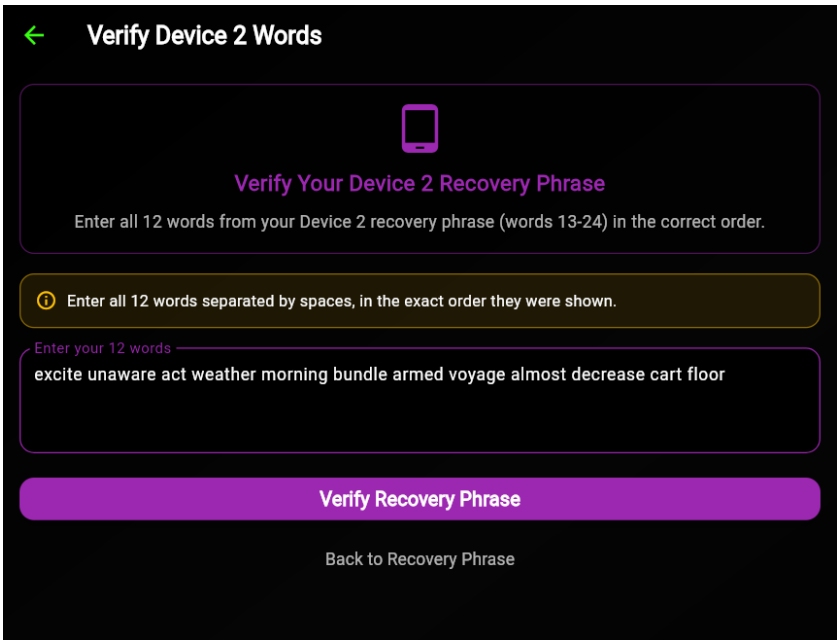

Figure 8 Device-2 Setup phase

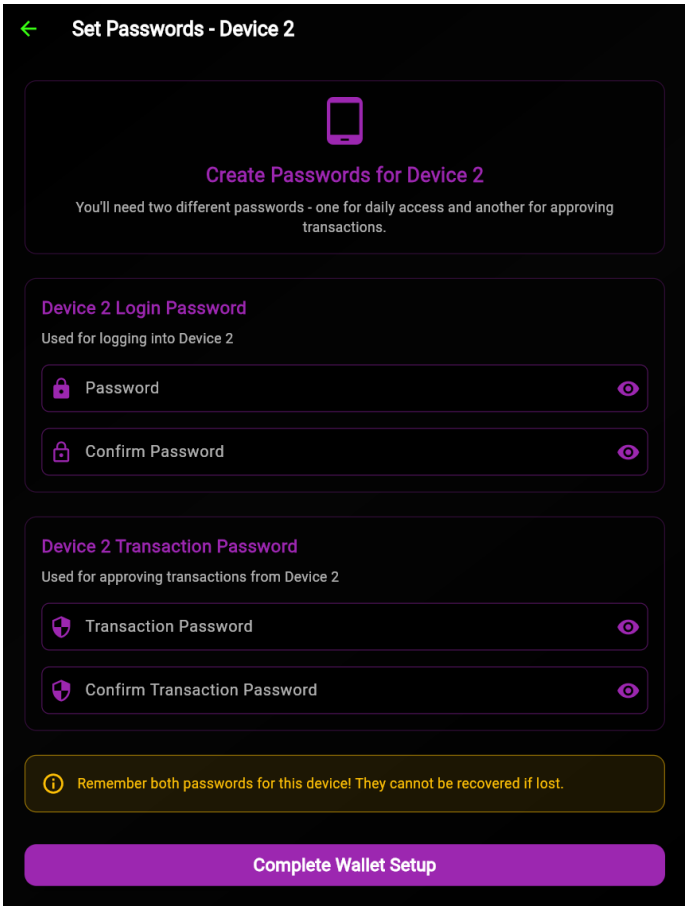

Figure 9 Device-2 Password setup phase

Mirroring Device A, Device B now:

- Confirms its own 12-word mnemonic (Words 13–24).
- Sets a unique password.

Each device functions independently and securely, with no knowledge of the other's credentials or mnemonic half.

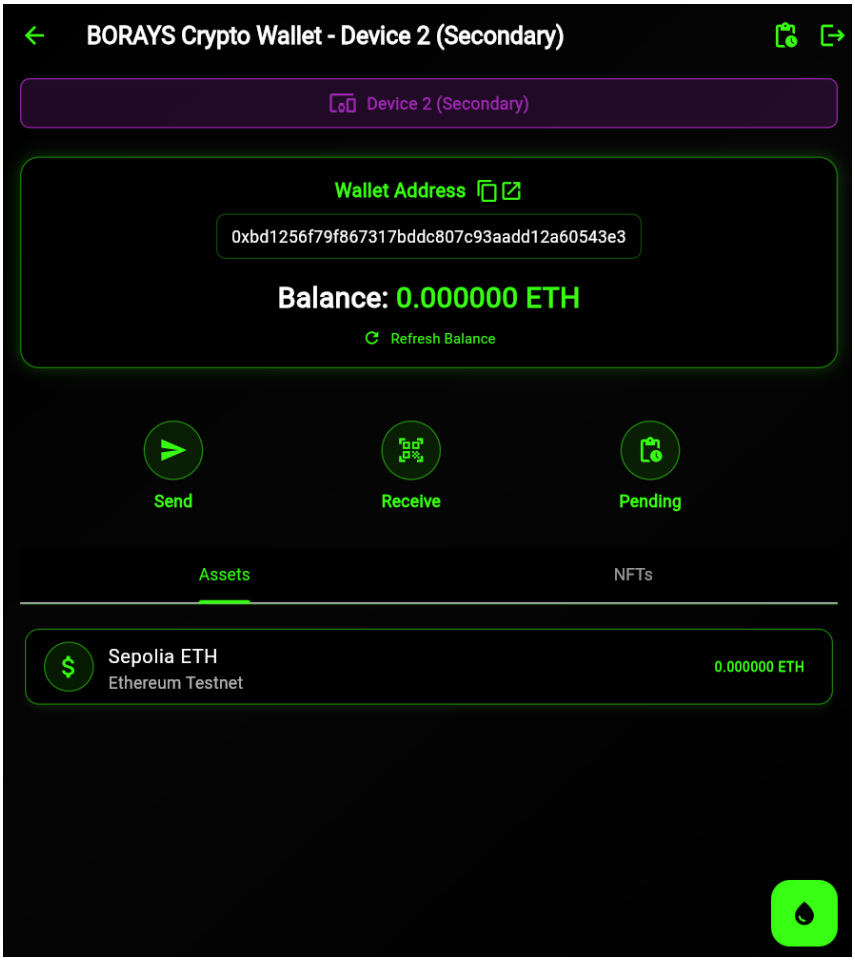

Figure 10 Device-2 Dashboard

Step-3: Go through the application

Once setup is complete, users are directed to their dashboard.

This screen provides a snapshot of:

- Token balances
- Transaction history
- “Send” and “Receive” options

Both devices will have similar dashboards but require each other to complete any critical operations.

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.

Figure 11 Device import page

For users restoring a wallet, this screen is the entry point. It includes an “Import from Seed” button to launch the recovery workflow. No private key is stored—only your 12 mnemonic words are needed.

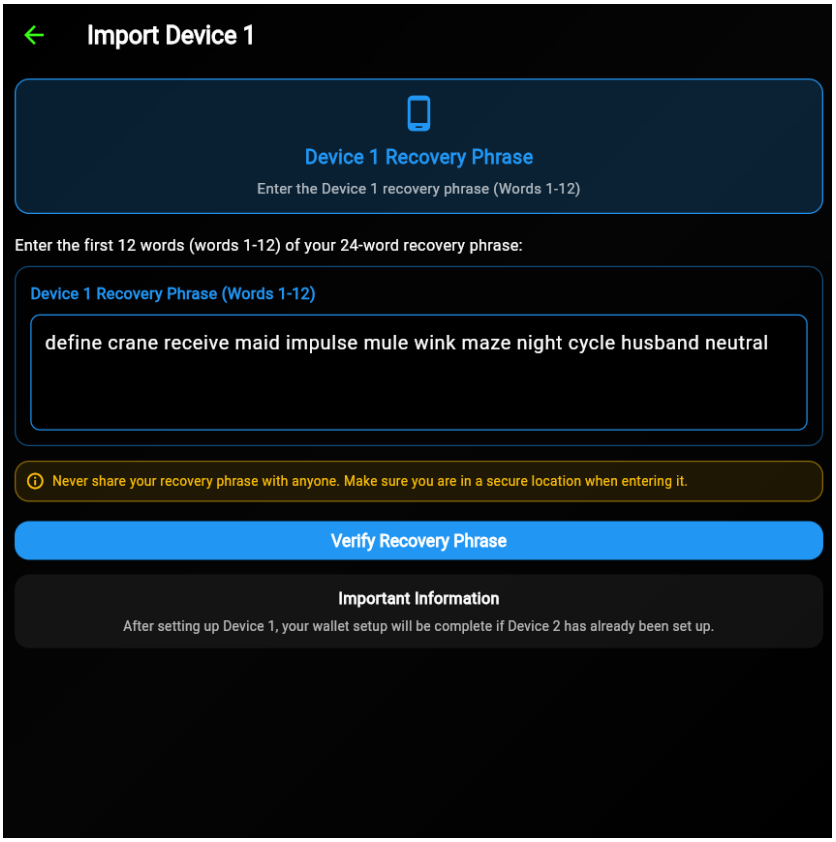

Figure 12 Device-1 Import page

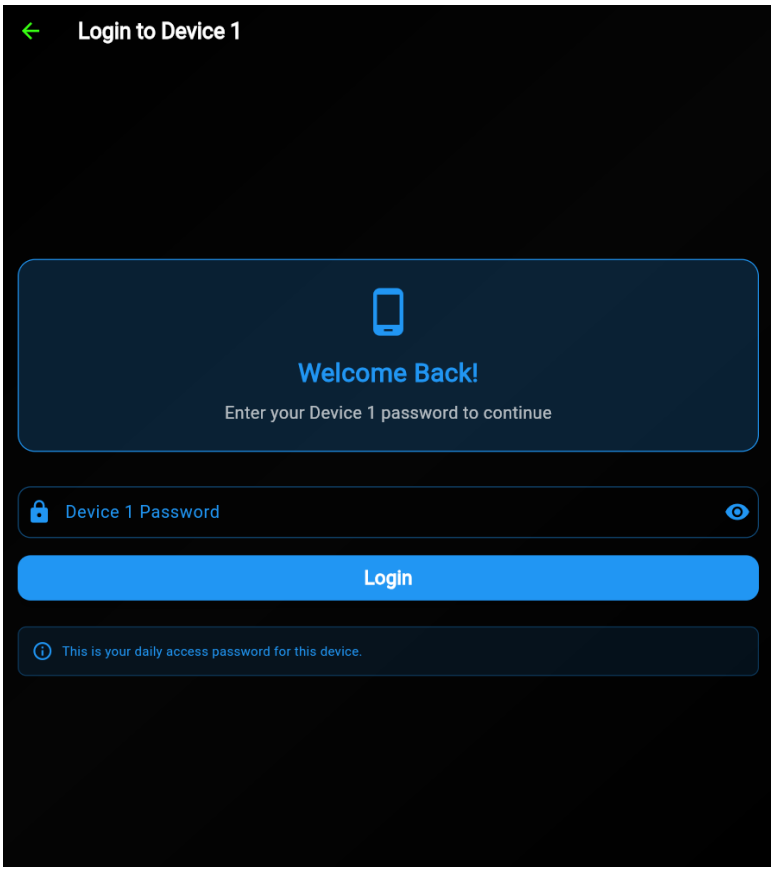

Figure 13 Device-1 password page

Device A users are asked to enter Words 1–12. Upon correct entry, they're prompted to reset or confirm their password. This flow maintains strict isolation—Device A cannot function without its specific phrase and password.

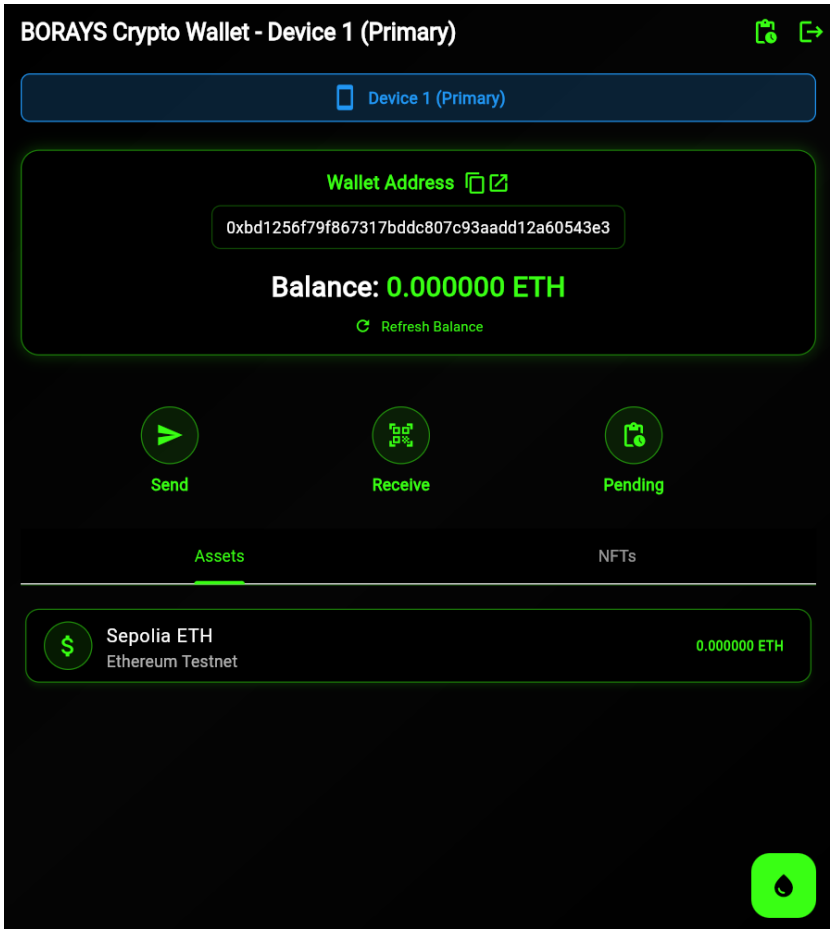

Figure 14 Device-1 Dashboard imported successfully

Confirms that Device A has been successfully restored. The dashboard loads with the expected wallet address and balance synced from the blockchain.

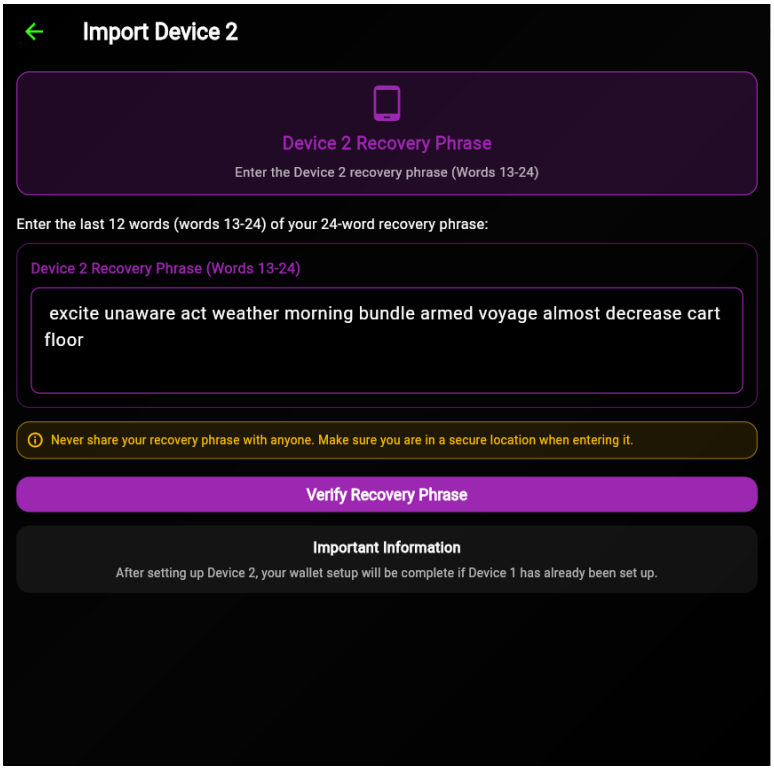

Figure 15 Device-2 Import page

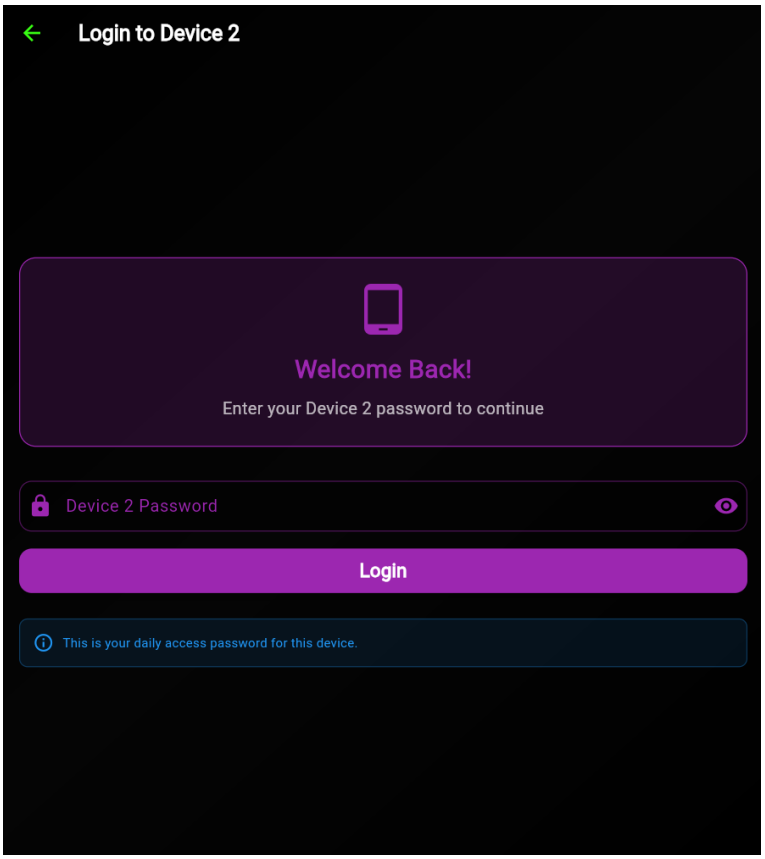

Figure 16 Device-2 password page

Similarly, Device B must enter Words 13–24 and reconfigure its password. This ensures both sides of the wallet are validated independently before functioning in tandem.

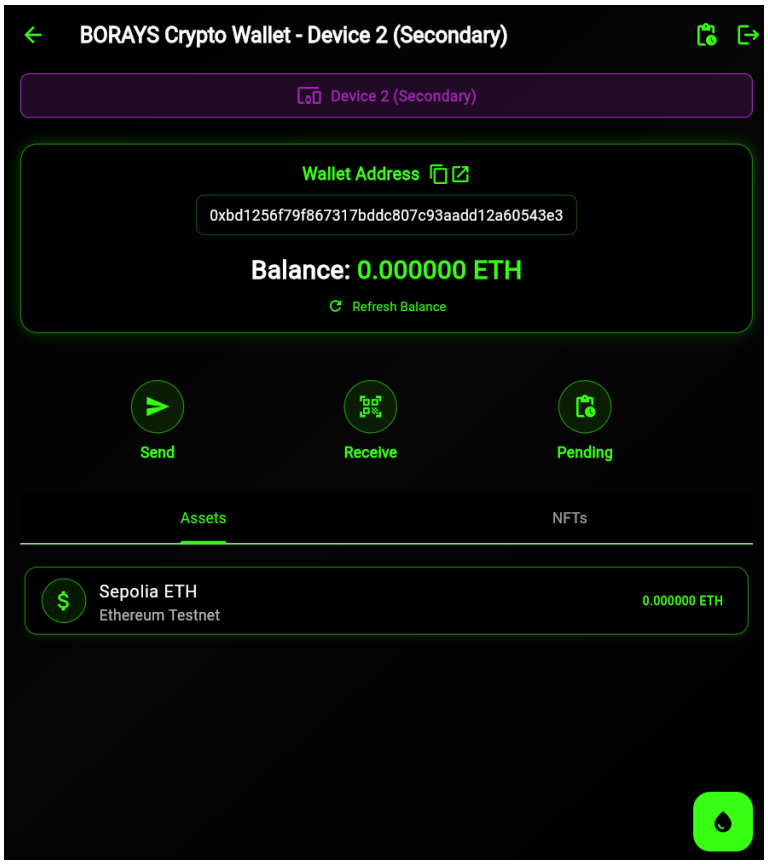

Figure 17 Device-2 Imported successfully

Device B is fully recovered. It's now ready to authenticate and approve transactions when Device A initiates them.

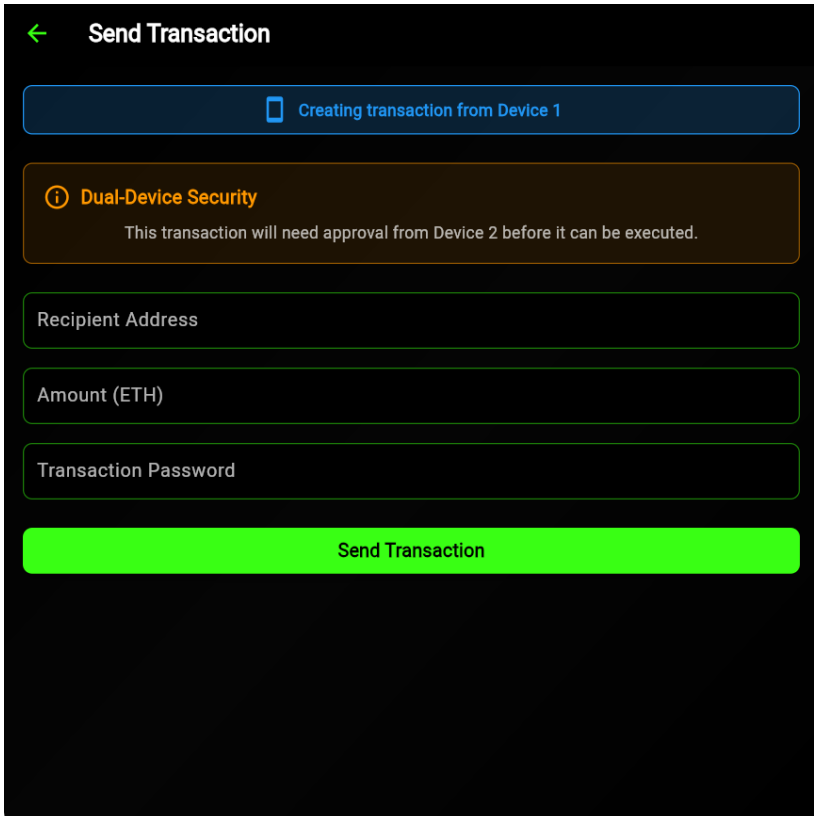

Figure 18 Device-1 Transaction page

The transaction interface allows users to:

- Enter a recipient address
- Specify token amount
- Enter their local password

This triggers the co-signing request, not an immediate transaction broadcast.

Figure 19 Device-1 Receive page

This screen displays the user's public wallet address and QR code for receiving assets.

- It is read-only—safe to share.
- This address never reveals or exposes any private information.

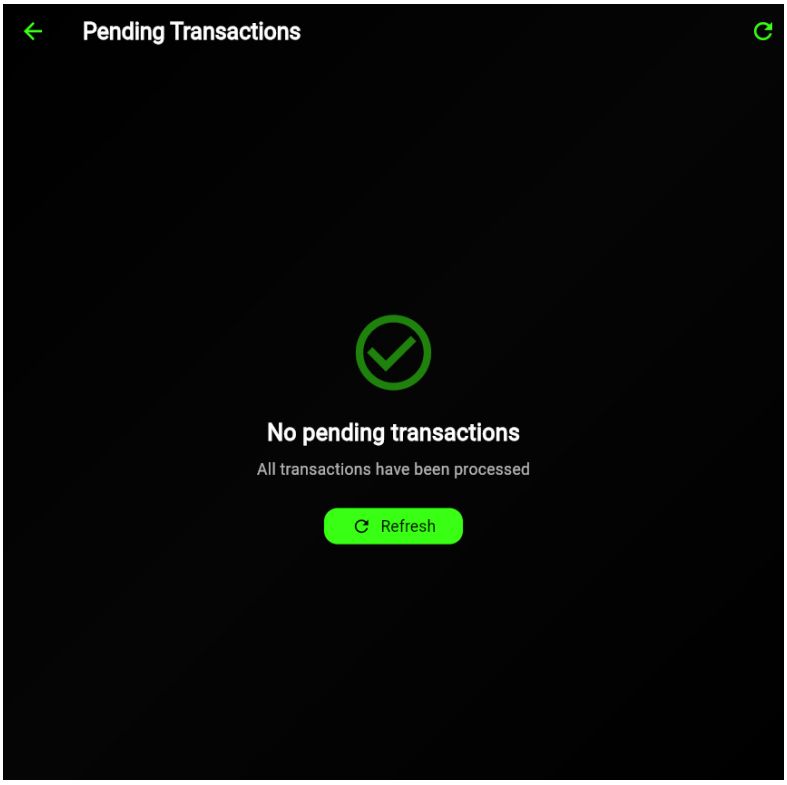

Figure 20 Device-1 pending transaction page

Pending transactions appear here until Device B confirms. Users can track unapproved actions and ensure Device B completes the second half of the signature.

Receiving Cryptocurrency

Receiving cryptocurrency using Borays is both intuitive and secure, thanks to its dual-device architecture and seamless integration with blockchain protocols. This section outlines the detailed process of receiving Ethereum (or compatible ERC-20 tokens) using the Borays wallet. It also explains the underlying mechanics that ensure safety, reliability, and transparency for both novice and advanced users.

After setting up the Borays wallet on both devices and completing the pairing process, you can begin receiving cryptocurrency. To do this:

On either Device A or Device B:

1. Open the **Borays app**.
2. Navigate to the **Dashboard** tab.
3. Locate the **"Receive"** button—usually next to the balance display.
4. Tap on it to view your Ethereum public wallet address.
5. You'll see:
    - A string of alphanumeric characters (your wallet address).

- A corresponding QR code that can be scanned for easy sharing.

For testing purposes or if you're setting up the wallet in a sandbox environment, you can use the Ethereum Sepolia faucet to request free test tokens.

1. Visit: https://cloud.google.com/application/web3/faucet/ethereum/sepolia
2. Paste your Borays wallet address.
3. Submit the request and wait for confirmation.
4. After a few seconds to minutes, you will receive the test tokens in your wallet.

You can confirm the receipt of tokens on the Dashboard screen, where the balance will automatically update once the transaction is recorded on the blockchain.

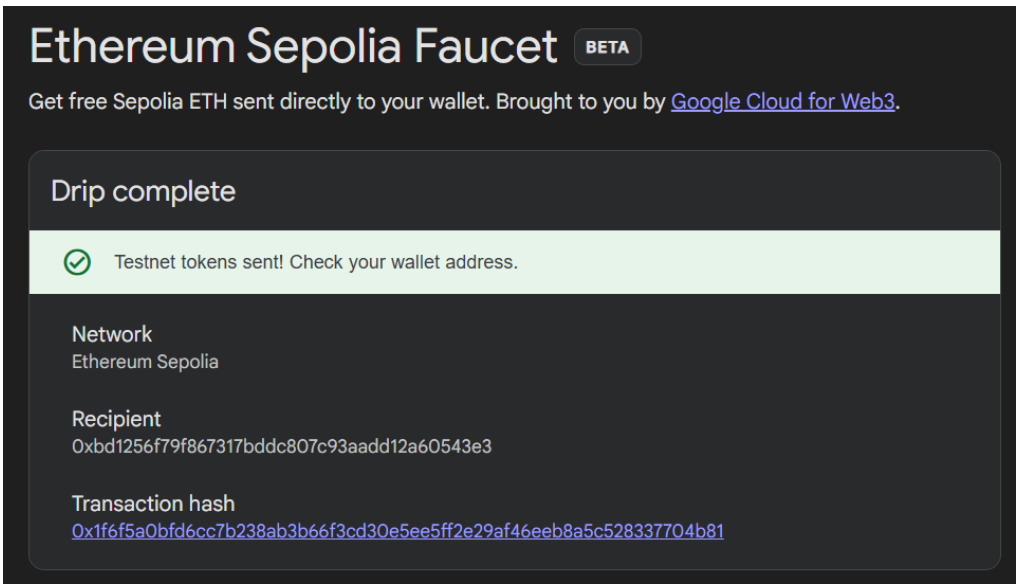

Figure 21 Ethereum test tokens

This screenshot shows the Sepolia faucet interface, where users paste their Ethereum address and request free test ETH. It simulates how mainnet transactions will function.

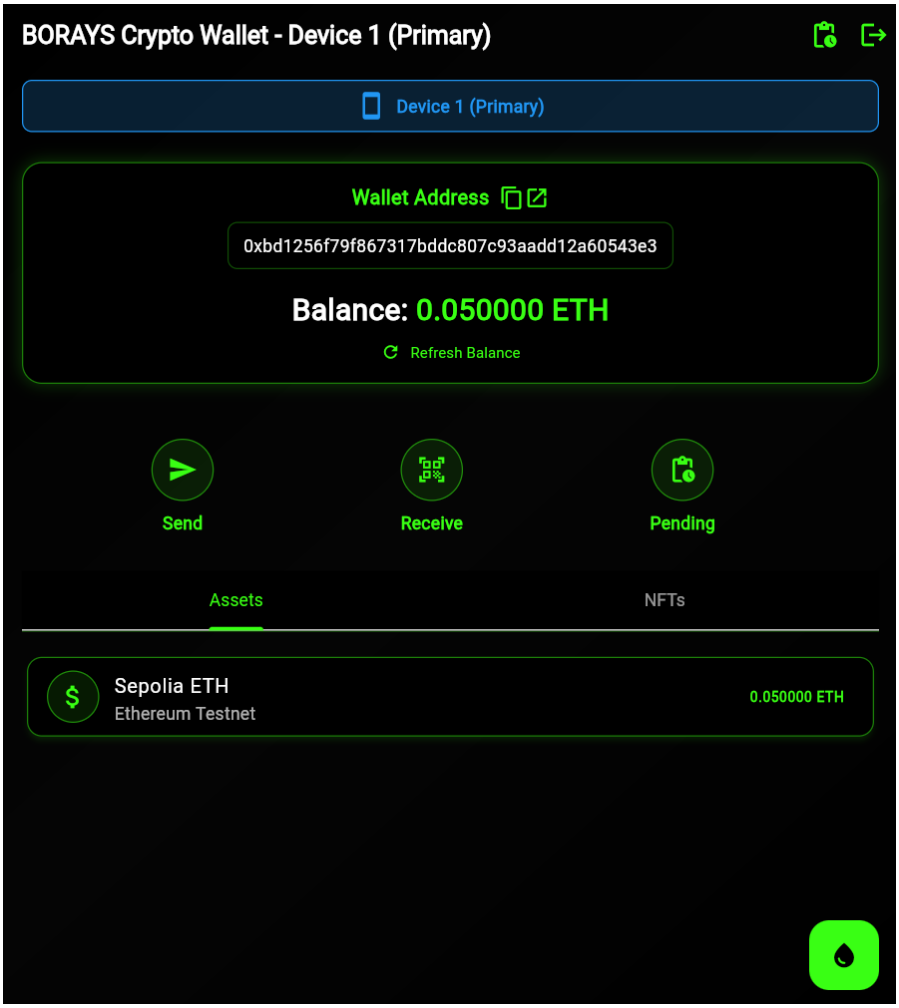

Figure 22 Ethereum received successfully

Once the faucet sends ETH to your wallet, the updated balance appears on the dashboard. This screenshot confirms successful token receipt. The background blockchain activity—block validation, mining, and syncing—is all handled automatically by the Borays backend.

Although the receiving operation is technically simpler than sending, Borays still ensures high standards of integrity and confidentiality:

Key Security Elements:

- **Read-only address**: The public address used to receive tokens cannot be used to access or spend funds.
- **Private key remains split**: No part of the private key is reconstructed or accessed during the receive operation.
- **Network verification**: Transactions are only displayed after being validated on-chain.
- **Device-agnostic access**: Both Device A and Device B can retrieve balances independently, ensuring redundancy.

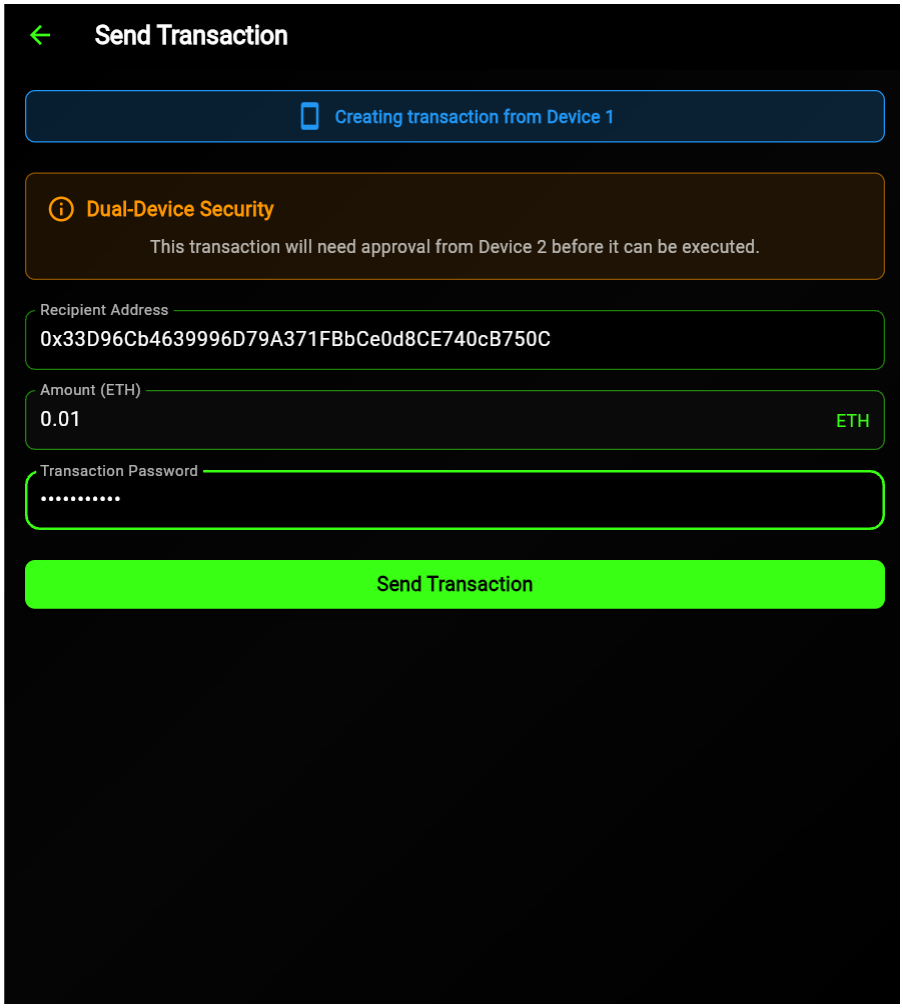

Figure 23 Sending Ethereum from device-1

In this image, the sender (Device A) is preparing to send Ethereum to another wallet:

- The recipient's wallet address is entered manually.
- The user specifies the amount to send.
- A secure password (set during wallet creation) is required to initiate the transaction.

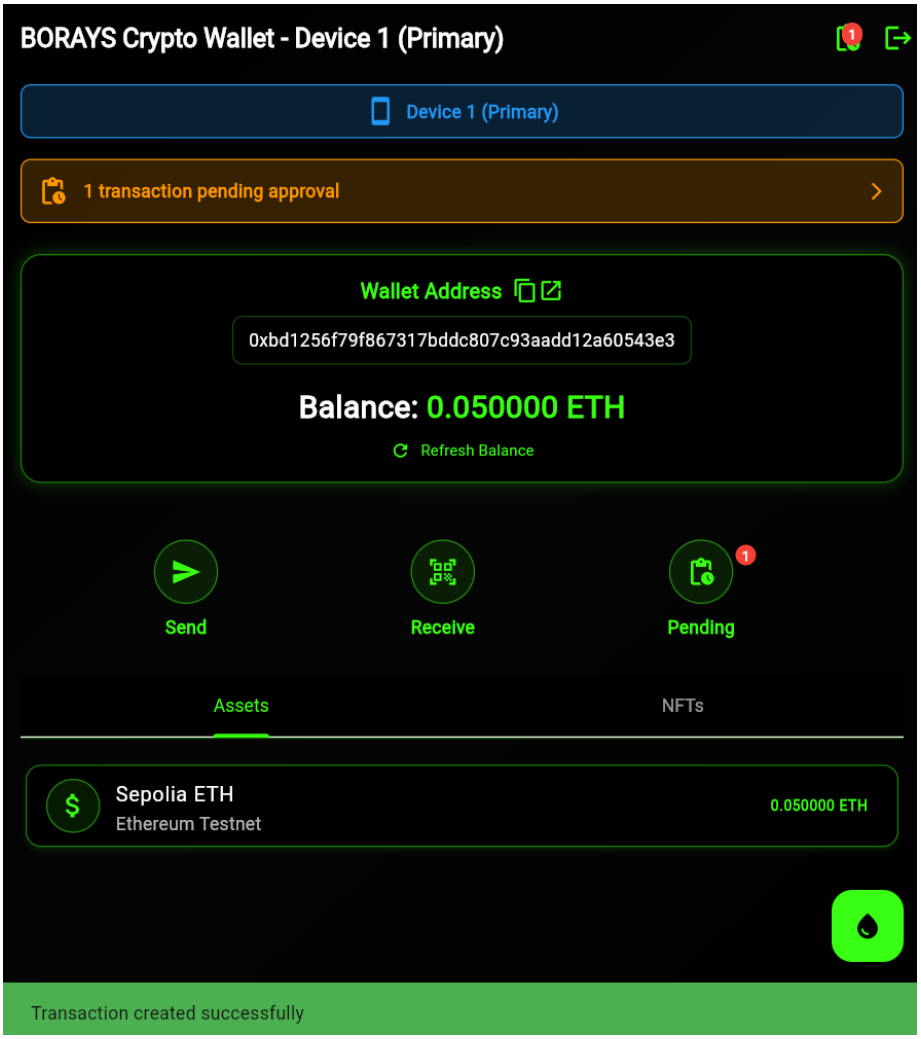

Figure 24 Transaction Initiated from device-1

This screenshot marks the crucial point at which the transaction workflow officially begins in Borays. After the user on Device A inputs the recipient's Ethereum address, selects the amount to transfer, and confirms the action by entering their local password, the application prepares the transaction payload.

At this moment:

- The transaction is not yet broadcast to the network.
- Instead, it enters a "pending approval" state and is securely relayed to Device B for secondary authorization.
- The data is transmitted using Paillier homomorphic encryption, ensuring that Device B sees only encrypted signing components. No raw private key material or sensitive transaction metadata is exposed in plaintext across the channel.

This figure visually represents the non-repudiation guarantee—the user initiating the transaction cannot later deny its origin, and the system ensures cryptographic integrity from the very first step.

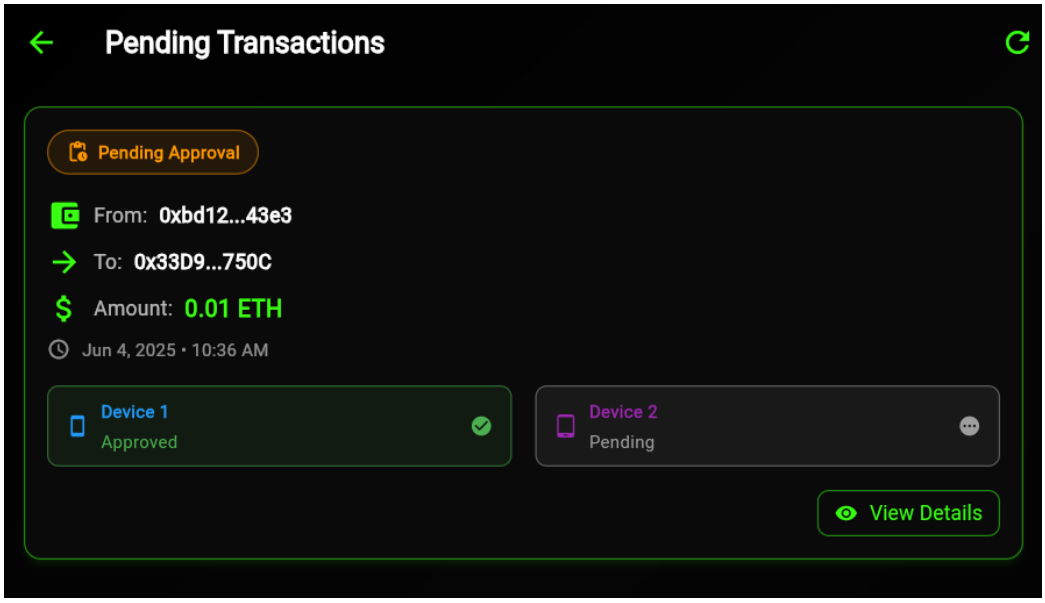

Figure 25 Pending Transaction in device-2

Once Device B is online and connected, it detects the pending transaction from Device A. Borays uses Firebase's real-time database syncing mechanism to seamlessly share the transaction metadata (like recipient address, amount, gas fee) between the two devices.

Key features visible or implied in this stage:

- Device B does not auto-approve any incoming request. It treats every transaction as a new event requiring human interaction.
- The pending screen serves as a checklist interface, allowing the user to verify that all transaction fields align with expectations.
- This form of mutual accountability ensures no single point of control, even if one device is compromised or acting maliciously.

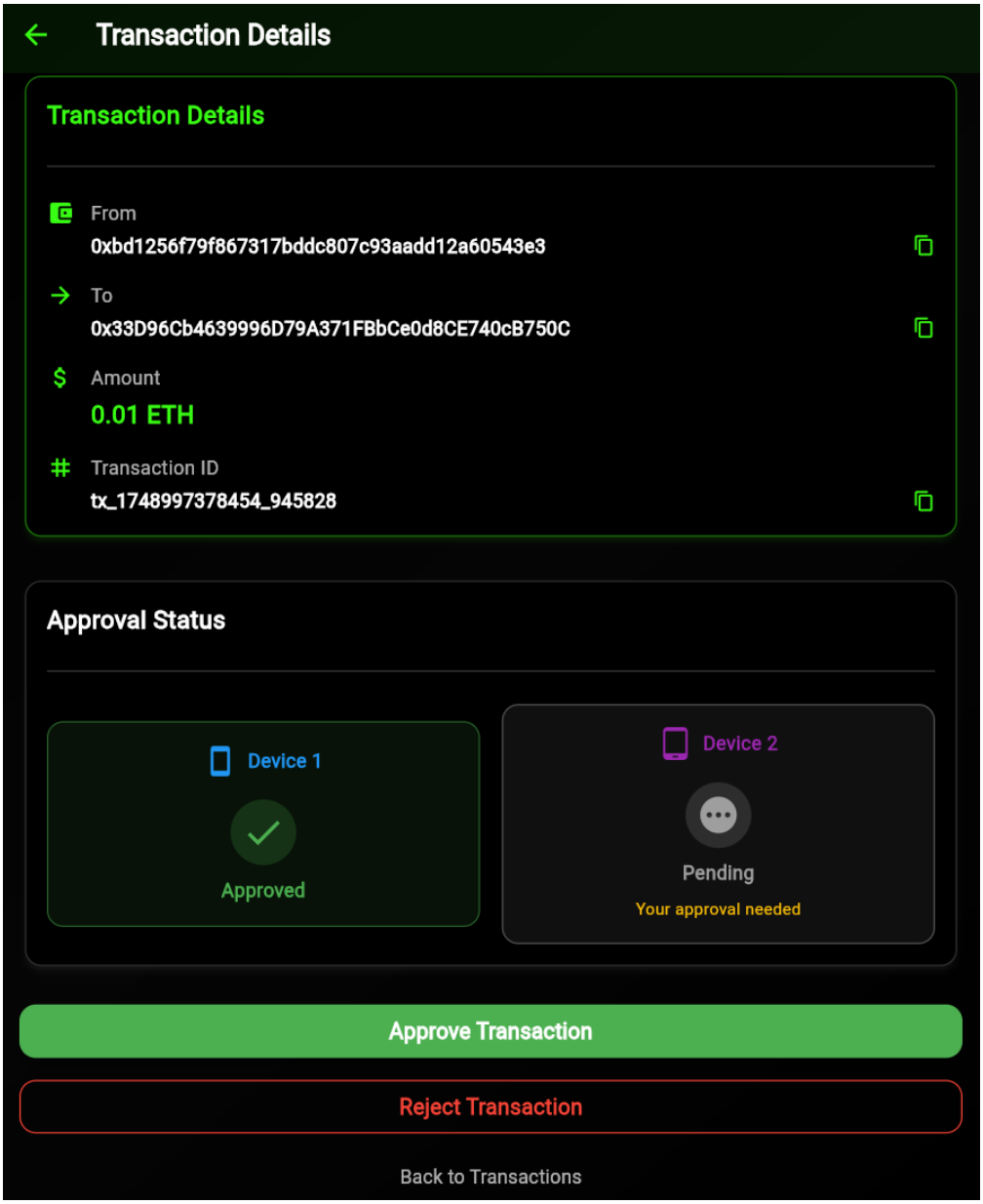

Figure 26 Device-2 Approval page

Here, the user on Device B takes an active role in the dual-approval signing mechanism. The application displays:

- The exact transaction details from Device A,
- The corresponding sender and receiver wallet addresses,
- The amount of Ethereum to be transferred,
- The timestamp and transaction ID.

Before granting final approval, the user must enter Device B's local password, which acts as a second layer of protection. Only after successful authentication will Device B complete its part of the signature using its share of the private key.

This multi-step process ensures:

- Explicit user consent for every outgoing transaction,
- Elimination of accidental or unauthorized transfers,
- Enforcement of true two-party governance over asset movement.

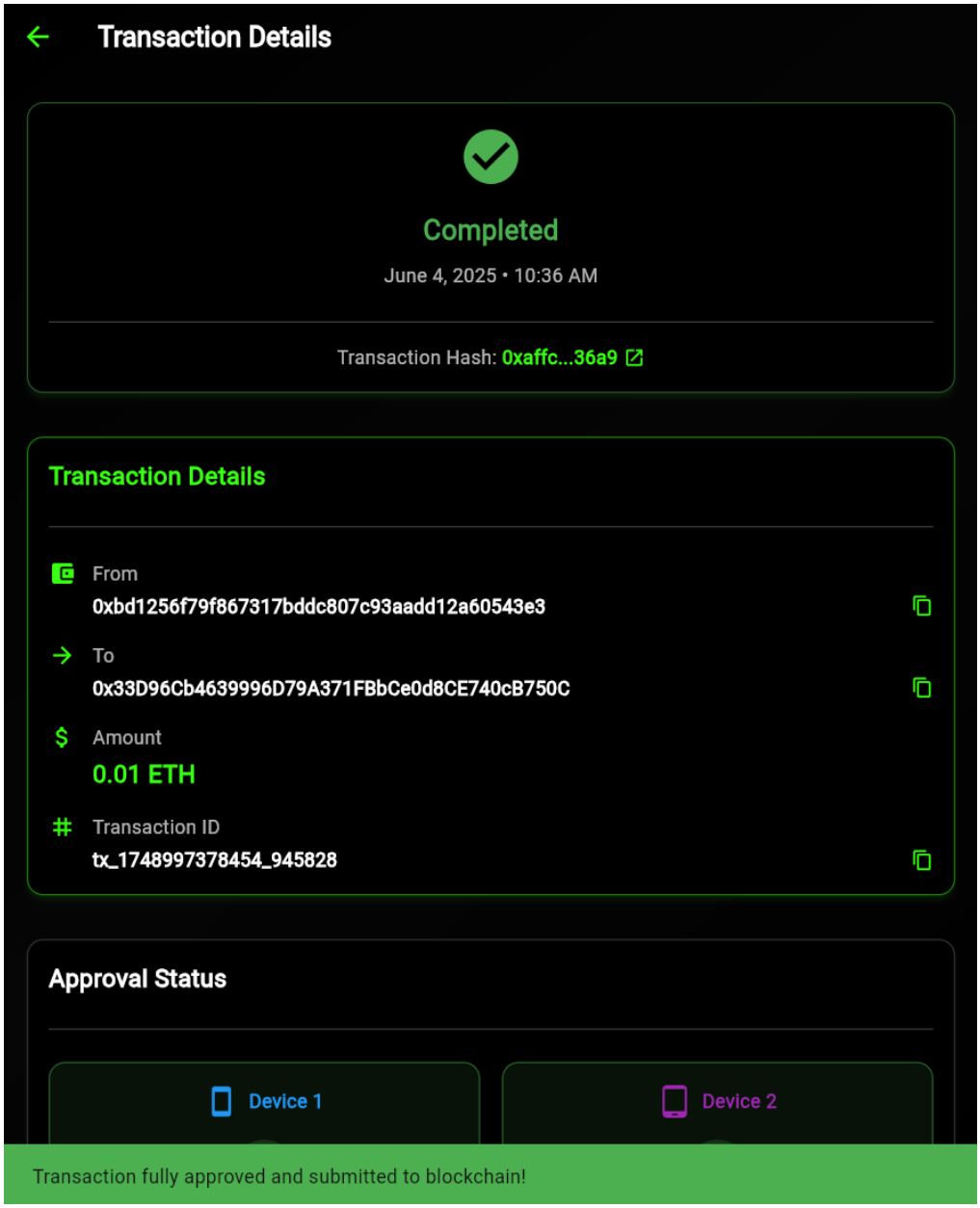

Figure 27 Transaction approved

After the approval is granted by Device B, both cryptographic shares (from Devices A and B) are combined in encrypted form to produce a valid ECDSA signature. This signature is then broadcast to the Ethereum blockchain via the wallet's integrated Web3 provider.

Behind the scenes:

- Borays uses internal APIs to package the transaction and send it to the blockchain.
- A listener confirms once the transaction hash is mined into a block.
- The transaction hash is returned to both devices as proof of success and is logged for future reference.

This step closes the transaction loop and confirms to the user that the transfer was not only approved by both parties but also successfully included in the distributed ledger.

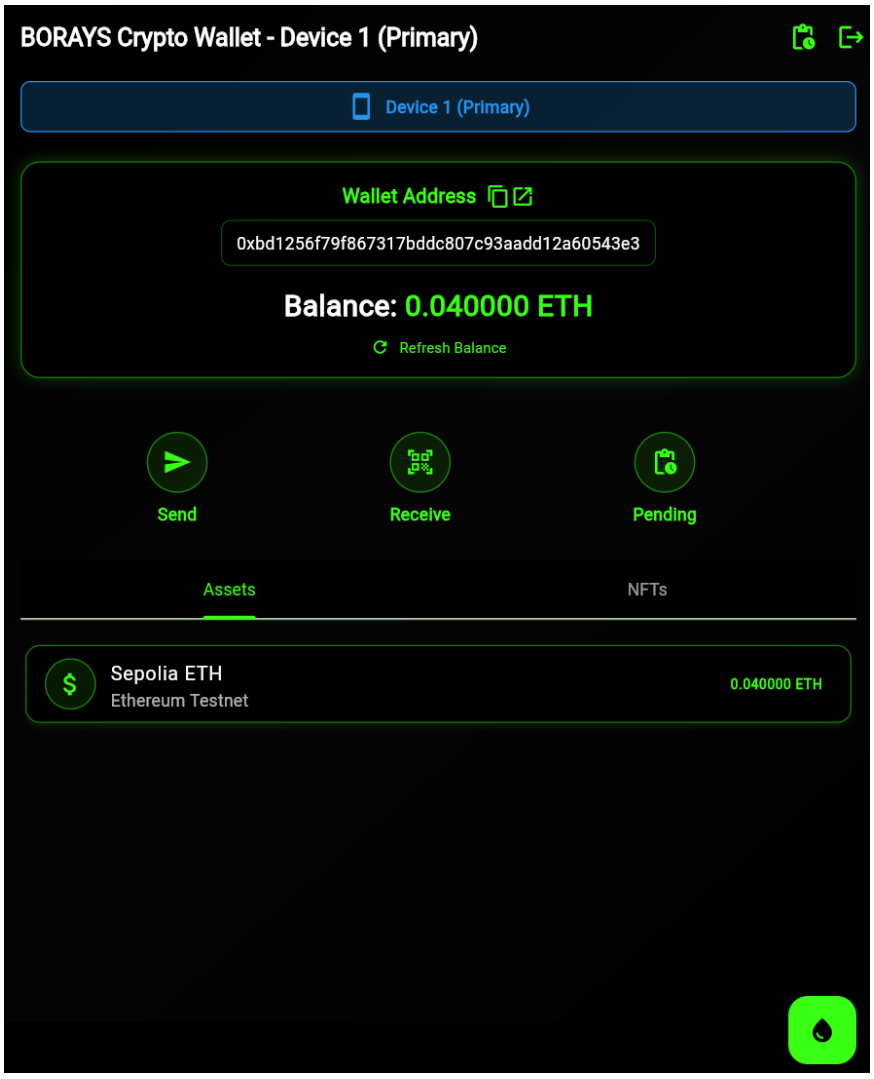

Figure 28 Updated Balance after transaction

Once the transaction is confirmed on the blockchain, Borays refreshes the balance view for the wallet. This screenshot shows the post-transaction state:

- Ethereum has been deducted from the sender's account.
- The new balance is fetched directly from the blockchain and reflected in real time.
- The user also has access to a transaction history tab to cross-reference previous operations.

This transparent feedback loop builds user trust and confirms operational accuracy. It also allows users to monitor gas fees and on-chain activity without relying on external tools.

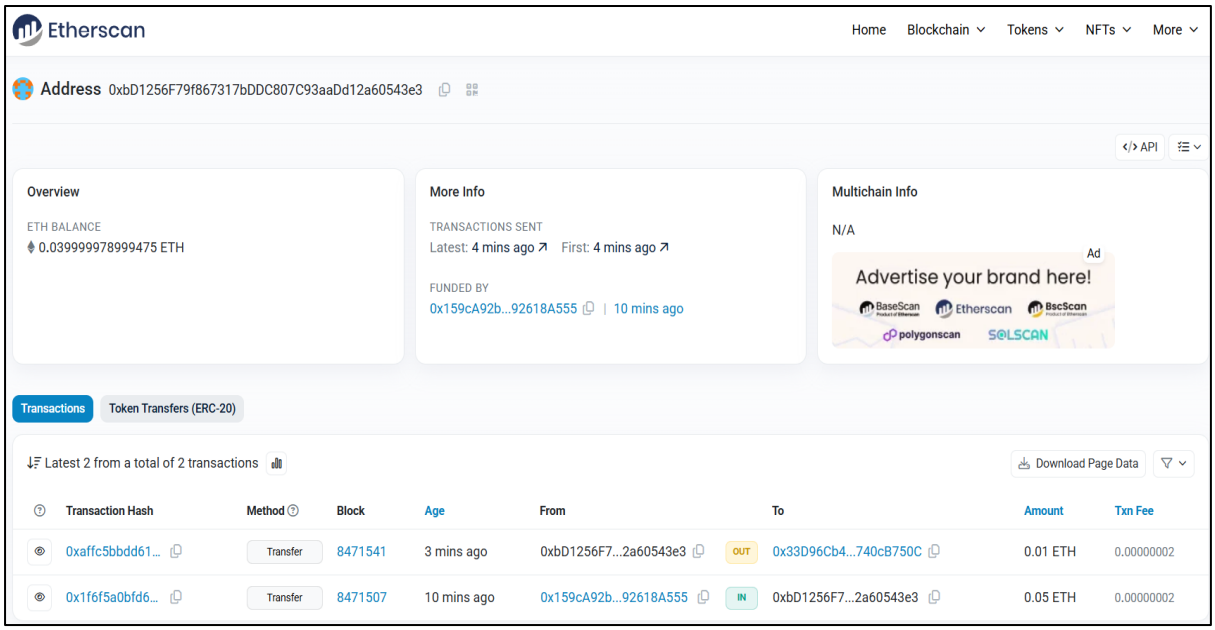

Figure 29 Verifying the authenticity of the transaction

While Borays does not currently include a built-in feature for linking directly to blockchain explorers, users can manually verify the authenticity of their transactions using platforms like Etherscan.

In this case, after completing a transaction within the Borays wallet, the transaction hash (TXID) can be retrieved and manually entered into a blockchain explorer such as:

🔗 https://etherscan.io

This external verification allows users to check:

- Transaction Status: Confirm whether the transaction has been mined and included in a block.
- Sender and Receiver Addresses: Ensure the funds were sent to the correct recipient.
- Gas Fee and Usage: Review how much was spent on transaction execution.
- Timestamp and Block Number: Confirm when the transaction was finalized.

Key Takeaways:

- **Proof of Finality:** Users can confirm that the transaction has been successfully processed and added to the blockchain ledger.
- **Transparency & User Autonomy:** Borays empowers users by supporting standard Ethereum addresses and formats, making manual validation simple and accessible.

- **Security Best Practice:** For users concerned about integrity or for high-value transfers, manual verification through Etherscan adds an extra layer of confidence.

Although this step is not automated in the current version of Borays, future releases may include direct links to block explorers' post-transaction for improved user experience.

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.

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