Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893
p-ISSN: 2089-3787

System Design of QR Code-Based Deterministic Cryptocurrency Wallet

Muhammad Ihsan[1*], Youvandra Febrial[2]
GathLabs, Indonesia
*Email *Corresponding Author*: emhihsan@gmail.com

Abstract

This study addresses a critical challenge in cryptocurrency adoption: managing complex seed phrases for wallet access. Traditional methods require users to store seed phrases securely, leading to potential asset loss due to human error or improper storage. This study develops a QR code-based deterministic wallet solution to replace the reliance on conventional seed phrases, with the aim of simplifying authentication and improving security. The development method integrates React with Next.js framework, and Solidity for smart contract development. Key features include authentication via QR code scan/upload, deterministic wallet generation from a combination of QR code and password, and interoperability with external wallets (MetaMask/Phantom). The results demonstrate successful NFT verification on Etherscan and seed phrase compatibility when imported to third-party platforms. This study offers a practical and innovative solution to improve user experience and security in crypto wallet management, potentially driving wider adoption.

Keywords: *QR code; blockchain; NFT; Crypto Wallet*

Abstrak

Penelitian ini membahas tantangan penting dalam adopsi mata uang kripto: pengelolaan frase awal yang kompleks untuk akses dompet. Metode tradisional mengharuskan pengguna untuk menyimpan frase awal dengan aman, yang menyebabkan potensi kerugian aset akibat kesalahan manusia atau penyimpanan yang tidak tepat. Penelitian ini mengembangkan solusi dompet deterministik berbasis kode QR untuk menggantikan ketergantungan pada seed phrase konvensional, dengan tujuan menyederhanakan autentikasi dan meningkatkan keamanan. Metode pengembangan mengintegrasikan *React* dengan *framework Next.js*, dan *Solidity* untuk pengembangan kontrak pintar. Fitur utama meliputi autentikasi via pemindaian/unggahan kode QR, pembuatan dompet deterministik dari kombinasi kode QR dan kata sandi, serta interoperabilitas dengan dompet eksternal (MetaMask/Phantom). Hasil pengujian membuktikan keberhasilan verifikasi NFT di *Etherscan* dan kompatibilitas seed phrase saat diimpor ke platform pihak ketiga. Penelitian ini menawarkan solusi praktis dan inovatif untuk meningkatkan pengalaman pengguna serta keamanan dalam manajemen dompet kripto, berpotensi mendorong adopsi lebih luas.

Kata kunci: *QR code; blockchain; NFT; Wallet Crypto*

1. Introduction

The development of blockchain technology has become a hot topic in the international world today, especially its application in financial innovation. This technology, which is able to offer security, transparency, and efficiency in transactions [1], seems to be a solution to the global economic uncertainty that has hit the world. With its decentralized principle and the use of cryptography to ensure security, blockchain technology has the potential to revolutionize various sectors, such as banking, logistics, and public services, making it a very crucial component in digital transformation [2][3]. This trend is getting hotter, especially after the massive adoption by large companies and many countries such as the United States, China, Germany, and El Salvador, this phenomenon further emphasizes its important role in the current global financial system [4]. Cryptocurrency, as the main application of blockchain, has grown rapidly since the launch of Bitcoin in 2009 by Satoshi Nakamoto, with thousands of other variants emerging in a decade [5][6][7]. With the rapid adoption as it is today, the development of secure and easy-to-use crypto wallet technology to support wider adoption is essential.

Access to digital assets can be done using a special wallet to store cryptocurrency. Unfortunately, managing seed phrases, which are the access keys to these wallets, is a challenge in itself. Seed phrases are often complex, difficult to remember, and prone to being stored in an insecure manner, increasing the risk of users losing their digital assets [8][9]. Ideally, users can access their wallets in a simple and secure manner without worrying about losing access. However, in reality, many users, especially those who are not from a technical background, have difficulty managing seed phrases, negligence in managing seed phrases can cause significant financial losses to individual users and potentially hinder the adoption of cryptocurrency on a larger scale [9][10]. The gap between ideal and current conditions indicates an urgent problem to be addressed through innovation in crypto wallet design.

To address these issues, this study proposes a deterministic cryptocurrency wallet creation application based on QR codes. This solution allows users to access their wallets by scanning a QR code, eliminating the need to remember complicated seed phrases. QR codes can store wallet access information securely, thereby reducing the risk of human error and increasing user convenience. The use of QR codes itself has been proven effective in facilitating payment and authentication systems [11]. QR code security can also be improved by adding encryption to the metadata in it. In addition, the form of the QR-Code can also be stored in the blockchain as an NFT so that its uniqueness and access can be protected. With this, QR code-based solutions are considered appropriate to simplify wallet access while maintaining security.

The main objective of this research in designing and implementing a QR code-based deterministic wallet is to increase ease of access for users, especially those who do not have high textual knowledge, while maintaining a good level of security. This research also aims to reduce the risk of asset loss due to poor seed phrase management. The benefit is that this solution is expected to encourage wider adoption of cryptocurrency by simplifying the user experience. In addition, this research contributes to the development of an inclusive and sustainable cryptocurrency ecosystem, while opening up opportunities for further innovation in digital wallet design and cybersecurity.

2. Literature Review

The development of information and communication technology has had a significant impact on various aspects of life, including in the management of digital assets such as cryptocurrency. This literature review will discuss several studies related to cryptocurrency wallets and proposed solutions to improve user experience.

Research by Negara [12] successfully designed a mobile application for an electronic wallet that operates on the Ethereum blockchain network. This study highlights the use of the web3.js library to enable interaction between the wallet application and the Ethereum node, and implements the SDLC software development method to ensure an organized structure. The advantage of this study is its focus on developing mobile applications that can be accessed by smartphone users, which is a growing market segment. In addition, this study also provides suggestions for further development, such as adding security features and integrating notification services, which can improve user experience and transaction security.

Research by Richard et al. [13] explores the challenges faced by users in using cryptocurrency wallet applications, focusing on usability, security, and trust aspects. This study identified four main themes from the analysis of user reviews, namely domain-specific challenges, security and privacy, misunderstandings, and trust issues. The strength of this study lies in its comprehensive approach in analyzing user experience, but this study has not considered innovative solutions to improve accessibility and security, which are the main focus of our study through the development of a QR code-based deterministic wallet.

Research by Zaidenberg and Kiperberg [14] introduced VirtSecIO, a hypervisor-based platform designed to execute secure modules, including HyperWallet, which functions as a cryptocurrency wallet without the need for special hardware. This study emphasizes VirtSecIO's ability to provide a secure path for input and output, while minimizing performance overhead and attack surface. The strength of this study lies in its innovative approach that combines high security with efficiency, making it an attractive alternative to traditional hardware wallet solutions that are often more expensive and complex.

Research by Almanfaluti et al. [15] developed a mobile application for a cryptocurrency digital wallet integrated with QRIS (Quick Response Indonesia Standard). This study emphasizes the use of a Webservice to ensure smooth implementation and utilizes Android Studio as a framework for application development. The advantage of this study is its ability to allow cryptocurrency owners to convert their virtual assets into Rupiah, thus facilitating payment transactions for various daily needs, such as purchasing credit and travel tickets. This study also opens up opportunities for further development in cryptocurrency-based payment systems in Indonesia.

Research by Zulmy et al. [16] examines the development of an e-wallet for Rupiah Digital, which is an initiative of the Central Bank Digital Currency (CBDC) in Indonesia. This study highlights the use of blockchain technology, specifically Hyperledger Fabric, to create a secure and efficient distribution system. The advantage of this study is the methodological approach involving focus group discussions (FGDs) with experts from various fields, including economics, law, and technology, to obtain comprehensive input on the proposed e-wallet design. This study not only provides technical recommendations, but also considers regulatory and security aspects, making it a significant contribution to the development of a digital payment system in Indonesia.

Previous studies have shown progress in the development of cryptocurrency wallets, but key challenges such as seed phrase management and accessibility for non-technical users remain unaddressed. Most previous studies have focused on technical aspects such as blockchain integration [12][16], user experience analysis [13], or enhancing security through complex infrastructure [14]. The use of QR codes in the cryptocurrency context is also generally limited to transaction functions or sharing wallet addresses [15], rather than the process of creating or managing wallets themselves.

This study proposes a novel approach that integrates QR codes as the primary method for deterministic wallet creation and access. Unlike traditional approaches that rely on seed phrases, this solution allows users to generate and access their wallets simply by scanning a QR code, which is combined with a password to create unique entropy. This approach significantly simplifies the access process and eliminates the need to remember or store complex seed phrases, thereby reducing the risk of asset loss due to human error.

3. Methodology

In this study, we used the Waterfall software development method to design and implement a QR code-based cryptocurrency wallet. The Waterfall method was chosen because of its structured and sequential approach, allowing each stage to be completed before moving on to the next stage.

3.1 Requirements Analysis

In the requirements analysis stage, we identify the technical specifications and functional features required for the QR code-based cryptocurrency wallet application to operate optimally and meet user needs. This system is developed with the following functional features to achieve the research objectives of improving the accessibility and security of crypto wallets:

1) QR Code Generation as Authentication Key, Users can generate a unique QR code that can be used to login to their application. This feature simplifies access without having to memorize complex word sequences.
2) QR Code Authentication Mechanism, the system provides two methods, namely Direct scanning using the device camera and uploading an Image to process the QR code from a file. Both options provide flexibility according to user conditions.
3) Deterministic Wallet Generation, Wallet addresses and seed phrases are generated consistently based on the combination of QR code data and user passwords. The same input will produce identical outputs, ensuring reproducibility.
4) QR Code Minting as NFT, QR Codes can be converted into Non-Fungible Tokens (NFTs) on the Ethereum blockchain (ERC-721 standard), adding a layer of security through decentralized ownership verification.

5) Integrated Wallet Management, the system interface allows access to key information (wallet address, private key, seed phrase) for backup purposes.
6) Compatibility with External Wallets, the generated seed phrase is compatible with popular wallets (MetaMask, Phantom), allowing users to import/export assets between platforms without restrictions.

The above features are designed to overcome the complexity of conventional seed phrase management while enhancing security and usability. System validation will be conducted through experimental testing in Chapter IV. This specification is the basis for implementing a system that prioritizes a balance between technical reliability and practical utility.

3.2 System Design

In this stage, we design the QR code-based cryptocurrency wallet application system by defining the workflow and user interaction. The flowchart in Figure 1 shows how users interact with the application, starting from the login process to the management of the cryptocurrency wallet.

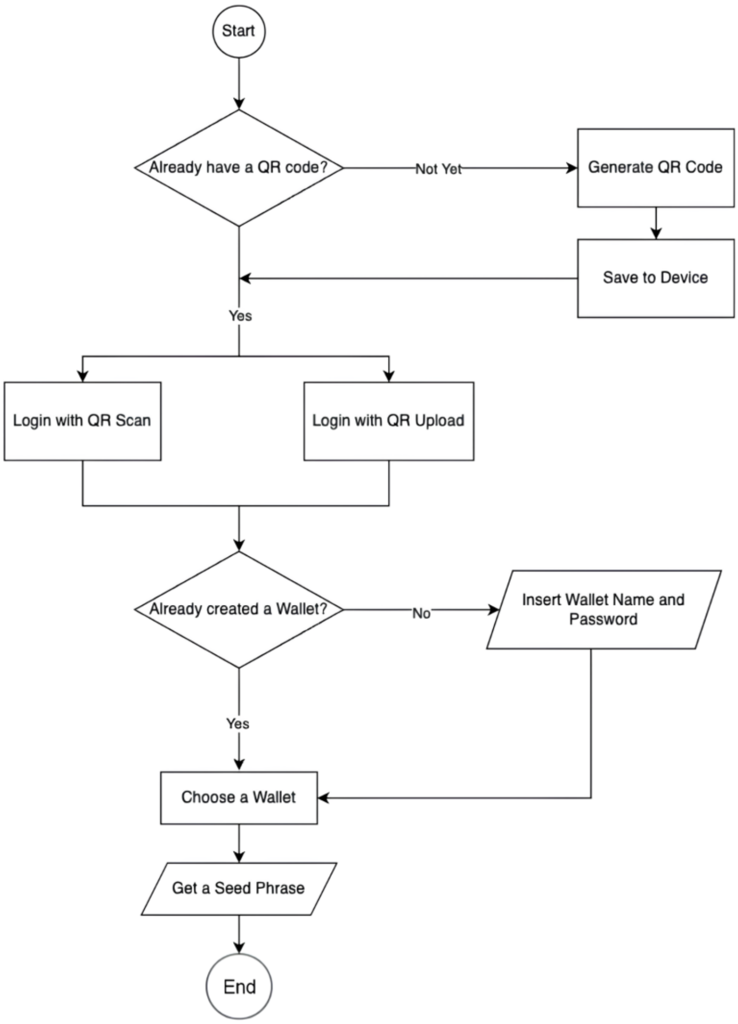


Figure 1. Application Flowchart

The authentication workflow initiates application launch, beginning with the verification of existing QR code credentials. Users who do not have a QR are guided through a QR code generation process, with explicit instructions to securely archive the generated code on their local device. Established users may authenticate through either real-time QR scanning or file upload functionalities.

Following successful authentication, the system performs wallet configuration verification. First-time users are required to complete wallet initialization by providing both a designated alias and a passphrase. Post-initialization, users select from available wallet profiles and are subsequently issued a cryptographically-generated seed phrase. This recovery mechanism serves as a critical fail-safe for wallet restoration scenarios, with strict user advisories regarding its secure offline storage.

Through this dual-phase architecture combining QR-based authentication and hierarchical wallet management, the system achieves compliance with core security protocols while maintaining operational efficiency in cryptocurrency handling.

3.3 Implementation

This system implementation seeks to establish a deterministic cryptocurrency wallet framework integrated with QR code authentication. The core technical component involves an ERC-721 compliant smart contract that manages QR code generation through Non-Fungible Token (NFT) minting processes. Below is the primary contract implementation:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.27;

import {ERC721URIStorage, ERC721} from
"@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";

contract QRNFT is ERC721URIStorage {
   uint256 private _nextTokenId;

   // Mapping untuk menyimpan pesan terenkripsi
   mapping(uint256 => string) private _encryptedMessages;

   constructor() ERC721("QR NFT", "QRNFT") {}

   function mintQR(
      address to,
      string memory tokenURI,
      string memory encryptedMessage
   ) public returns (uint256) {
      uint256 tokenId = _nextTokenId++;
      _mint(to, tokenId);
      _setTokenURI(tokenId, tokenURI);
      _encryptedMessages[tokenId] = encryptedMessage;
      return tokenId;
   }

   function getEncryptedMessage(
      uint256 tokenId
   ) public view returns (string memory) {
      require(ownerOf(tokenId) != address(0), "Token does not exist");
      require(ownerOf(tokenId) == msg.sender, "Not owner of token");
      return _encryptedMessages[tokenId];
   }

   function burn(uint256 tokenId) public {
      require(ownerOf(tokenId) == msg.sender, "Not owner of token");
      _burn(tokenId);
```

```
        delete _encryptedMessages[tokenId];
    }
}
```

The QRNFT smart contract functions to mint NFTs representing QR Codes with metadata stored using ERC721URIStorage. Each NFT created has an encrypted message that can be accessed by its owner. This contract also provides a feature to burn NFTs which will delete related data from the blockchain.

After the QR Code is created, the next step is to implement QR Code reading using the jsQR library. This library works by accepting raw image data as input, then detecting, extracting, and parsing the QR code in the image. This process includes:

1) **QR Code Localization:** jsQR detects the presence and location of the QR code in the image.
2) **Data Extraction:** Once detected, jsQR extracts the encrypted data in the code.
3) **Data Parsing:** The extracted raw data is then processed so that it can be read.

The jsQR library was chosen because of its ease of use and its ability to directly operate on raw image data without the need for complex image pre-processing. This increases the efficiency and speed of QR Code reading in the application.

Once the QR Code is successfully read, the system allows them to create a crypto wallet deterministically. This process uses a combination of the QR Code and the user's password to generate unique entropy that is used in wallet creation. Here is the pseudocode for this process:

```
FUNCTION
generateWalletFromQRAndPassword(qrData: STRING, password: STRING) RETURNS {
wallet: Wallet, seedPhrase: STRING }:
    // Generate deterministic entropy from QR data and password
    hash = SHA256(qrData + ':' + password)
    // Extract the first 32 bytes (64 characters in hex) of the hash as entropy
    entropy = CONVERT_TO_BUFFER(hash[0:64], 'hex')
    // Generate a mnemonic seed phrase from the entropy
    mnemonic = GENERATE_MNEMONIC_FROM_ENTROPY(entropy)
    // Create a hierarchical deterministic (HD) wallet node from the mnemonic phrase
    hdNode = CREATE_WALLET_FROM_PHRASE(mnemonic.phrase)
    // Derive a standard wallet from the HD node's private key
    wallet = CREATE_WALLET_FROM_PRIVATE_KEY(hdNode.privateKey)
    // Return the wallet and the seed phrase
    RETURN { wallet, seedPhrase: mnemonic.phrase }
END FUNCTION
```

This function uses SHA-256 cryptographic hashing on the combination of the user's QR Code and password data to generate unique entropy. From the hashing result, the first 32 bytes are taken as entropy which is then used to generate a seed phrase (mnemonic) using a library such as ethers.js. Because this process is deterministic, the same combination of QR Code and password will always produce the same wallet address and mnemonic.

With this approach, the system allows users to re-access their crypto wallets using only the QR Code and password without the need to store additional information, thus increasing security and convenience of use.

3.4 Testing

The experimental validation phase assessed whether the developed system operated in accordance with design specifications. Testing protocols encompassed multiple verification vectors: QR code minting as non-fungible tokens, QR-based authentication, deterministic wallet generation, on-chain verification through blockchain explorers, and seed phrase portability testing with established hot wallets including MetaMask and Phantom.

Initial validation focused on the QR code tokenization process. Test subjects generated QR codes subsequently transformed into NFTs via the implemented smart contract. Success criteria included visibility confirmation within ERC-721 compatible cryptocurrency wallets. Additional validation required metadata accessibility verification through the contract's storage mechanisms, confirming proper on-chain representation of the access credentials.

Following successful QR code generation, secondary validation examined the minting verification process through blockchain explorer interaction. Subjects located contract addresses and minting transactions via Etherscan to confirm on-chain representation. Successful identification of the NFT with corresponding metadata within the blockchain explorer environment indicated proper tokenization of authentication credentials. Metadata examination provided empirical evidence of secure credential persistence within the distributed ledger architecture.

The next test is carried out on the QR Code reading process. After successfully logging in, the user will create a crypto wallet deterministically based on the QR Code and password entered. Testing is done by trying to create a wallet on another device using the same combination of QR Code and password. If the seed phrase and wallet address generated are identical, then the system functions according to the expected deterministic concept.

The final test is carried out by importing the generated seed phrase into a hot wallet such as MetaMask and Phantom. The user will try to enter the seed phrase into the wallet to ensure that the wallet created is compatible with industry standards. If the seed phrase can be imported successfully and the wallet can be used for transactions or storing crypto assets, this proves that the system has succeeded in producing a valid and interoperable crypto wallet with the wider blockchain ecosystem.

With this series of tests, it is hoped that every main feature in the system can run well, starting from creating a QR Code as an NFT, verifying NFT minting in the blockchain explorer, logging in using a QR Code, creating a wallet deterministically, to the interoperability of the seed phrase with popular crypto wallets.

3.5 Documentation

The entirety of the source code and system implementation resides in a GitHub repository with comprehensive documentation, ensuring both transparency and reproducibility. These documentation materials encompass detailed explanations regarding smart contract architecture, QR code generation and utilization protocols, and cryptocurrency wallet interaction mechanisms. Each code segment contains explanatory comments describing its functional purpose, thereby facilitating comprehension and extension by other developers or researchers pursuing related work.

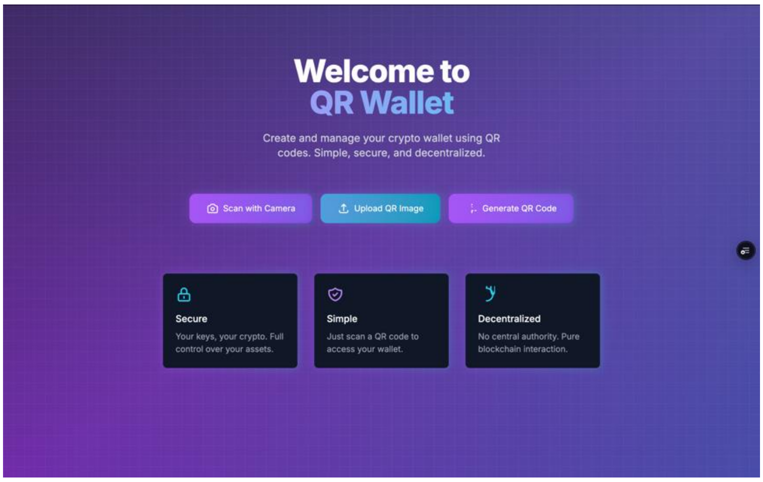
Additionally, users possess the capability to examine QR code-related transactions through blockchain explorer interfaces, enabling independent verification of proper execution sequences. The public availability of this documentation through GitHub significantly reduces barriers to entry, allowing interested parties to access, evaluate, and extend the system architecture with minimal friction. This openness not only facilitates scientific reproducibility but also encourages community-driven improvements to the authentication framework.

4. Results and Discussion

This section presents the results of the implementation of the QR Wallet application, which was developed to facilitate access and management of crypto wallets using QR codes. The results obtained include the appearance of the application interface and testing of the main features that have been developed.

1) Landing Page

The landing page presents QR Wallet, an application enabling users to manage cryptocurrency wallets through QR codes in a straightforward, secure, and decentralized manner. Three primary features appear: Scan with Camera for direct QR code scanning, Upload QR Image for importing existing QR code images, and Generate QR Code allowing users to create new authentication credentials. This introductory interface emphasizes user sovereignty over digital assets and highlights the simplicity of wallet access through QR code scanning.



Welcome to
QR Wallet

Create and manage your crypto wallet using QR codes. Simple, secure, and decentralized.

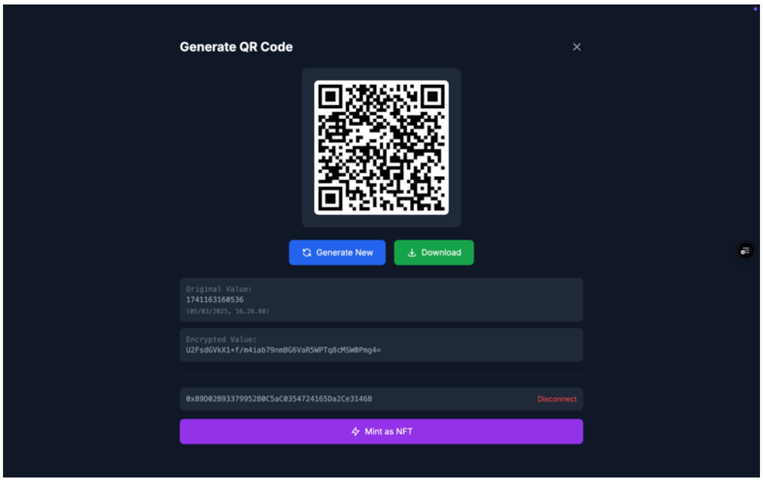
Secure
Your keys, your crypto. Full control over your assets.

Simple
Just scan a QR code to access your wallet.

Decentralized
No central authority. Pure blockchain interaction.

Figure 1. Landing Page View

2) Generate QR Code



Generate QR Code

Original Value:
1741163160536
(05/03/2025, 16.26.00)

Encrypted Value:
U2FsdGVkX1+f/m4iab79nmBG6VaR5WPTq8cMSW0Pmg4=

0x89D02B93379952B0C5aC0354724165Da2Ce3146B

Figure 2. Generate QR Code View

Pressing the Generate QR Code button from the landing page takes users to a new screen showing their freshly-created QR code. The page has this dark background that makes the QR code really stand out at the top. There are a couple of options here - a blue "Generate New" button if you want to make another code, and a green "Download" button to save it. What's interesting is the "Mint as NFT" button at the bottom - this lets users actually turn their QR code into an NFT (Non-Fungible Token) on the blockchain, which basically creates a permanent record of it that nobody can mess with.

3) Scan with Camera

When users picks "Scan with Camera" in QR Wallet, they get this screen with a popup that has a red frame showing where to point the camera. The red frame helps users know exactly where to position the QR code they're trying to scan from another device. In the example image, you can see a phone with a QR code while the app is trying to detect it. There's a "Cancel" button in the top right corner that lets you back out if needed. You can still see the main app screen behind the popup, with the "Welcome to QR Wallet" text visible, which kinda reinforces that the whole point of this app is dealing with QR codes in a secure way.

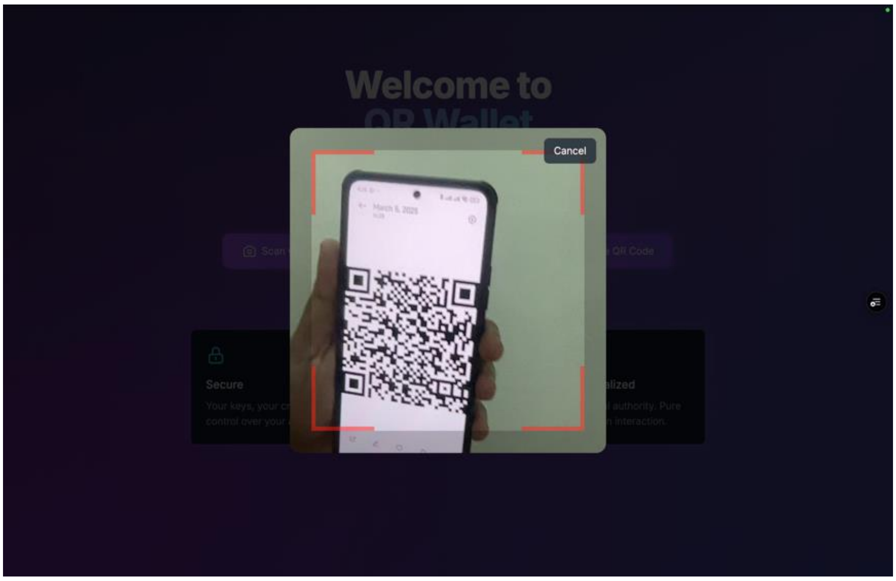
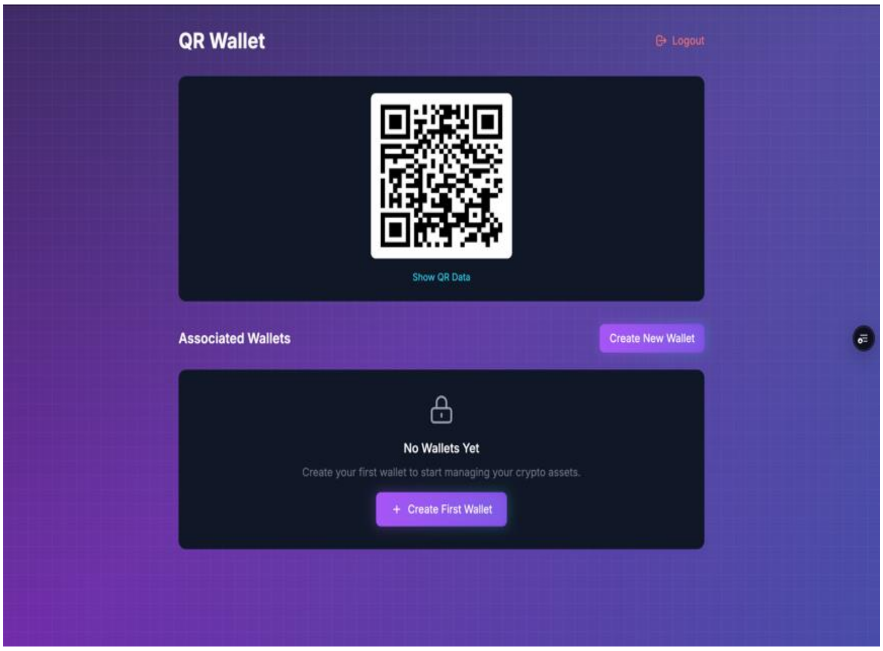


Figure 3. Scan with Camera View

4) Dashboard View

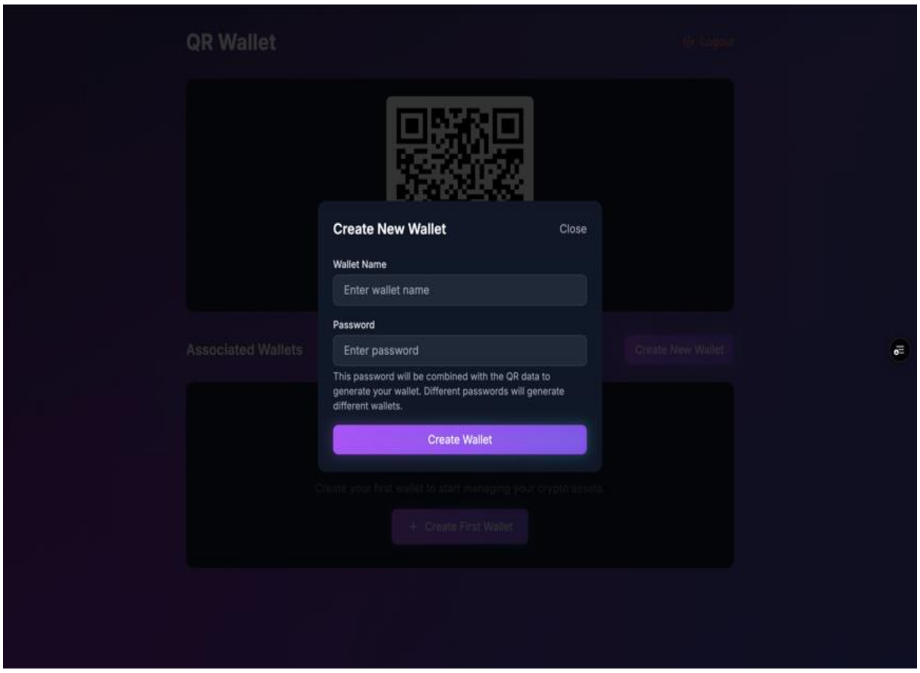
After you've scanned a QR code successfully - either by uploading an image or scanning directly with your camera - QR Wallet shows the user this management page for your crypto wallets. On this screen, the user can see the QR code that they just scanned displayed pretty clearly, which shows you that everything worked right. From here, users can manage all their wallet stuff.



Create your first wallet to start managing your crypto assets.

Figure 4. Dashboard View

The "Create New Wallet" button is used to create a new crypto wallet. If the user does not have a connected wallet, the system will display a notification "No Wallets Yet", users can create a new wallet by pressing "Create First Wallet" or "Create new wallet", here users will be asked to enter the wallet name and password. With these features, the QR Wallet application functions as a QR code-based digital wallet manager, which makes it easier for users to store, read, and manage crypto assets in a safer and more practical way.



Wallet Name: Enter wallet name

Password: Enter password

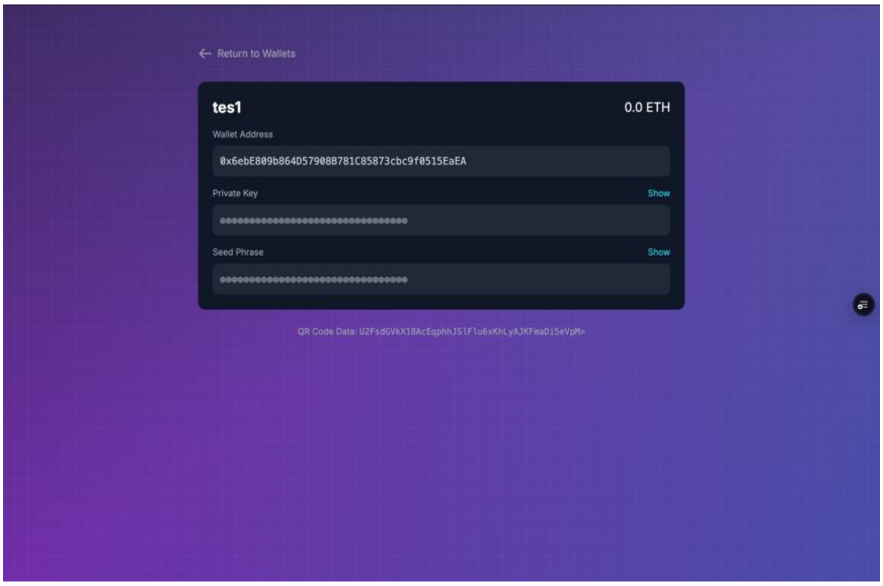
This password will be combined with the QR data to generate your wallet. Different passwords will generate different wallets.

Create your first wallet to start managing your crypto assets.

Figure 5. Create New Wallet View

4.1.5 Wallet View

This view shows the details of the wallet "tes1" that has been created. This wallet has a unique address (Wallet Address) that can be used to receive transactions. In addition, there is a Private Key, which functions as an access credential to control this wallet, and a Seed Phrase, which is a collection of random words used to recover the wallet if access is lost. We can display it with In practice, this information is very sensitive and should not be shared with anyone, because anyone who has the Private Key or Seed Phrase can fully control the wallet.



tes1 0.0 ETH

Wallet Address: 0x6ebE809b864D57908B781C85873cbc9f0515EaEA

Private Key: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Seed Phrase: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

QR Code Data: U2FsdGVkX18AcEqphhJ5lFlu6xKhLyAJKFmaDi5eVpM=

Figure 6. Create New Wallet View

4.2. Testing

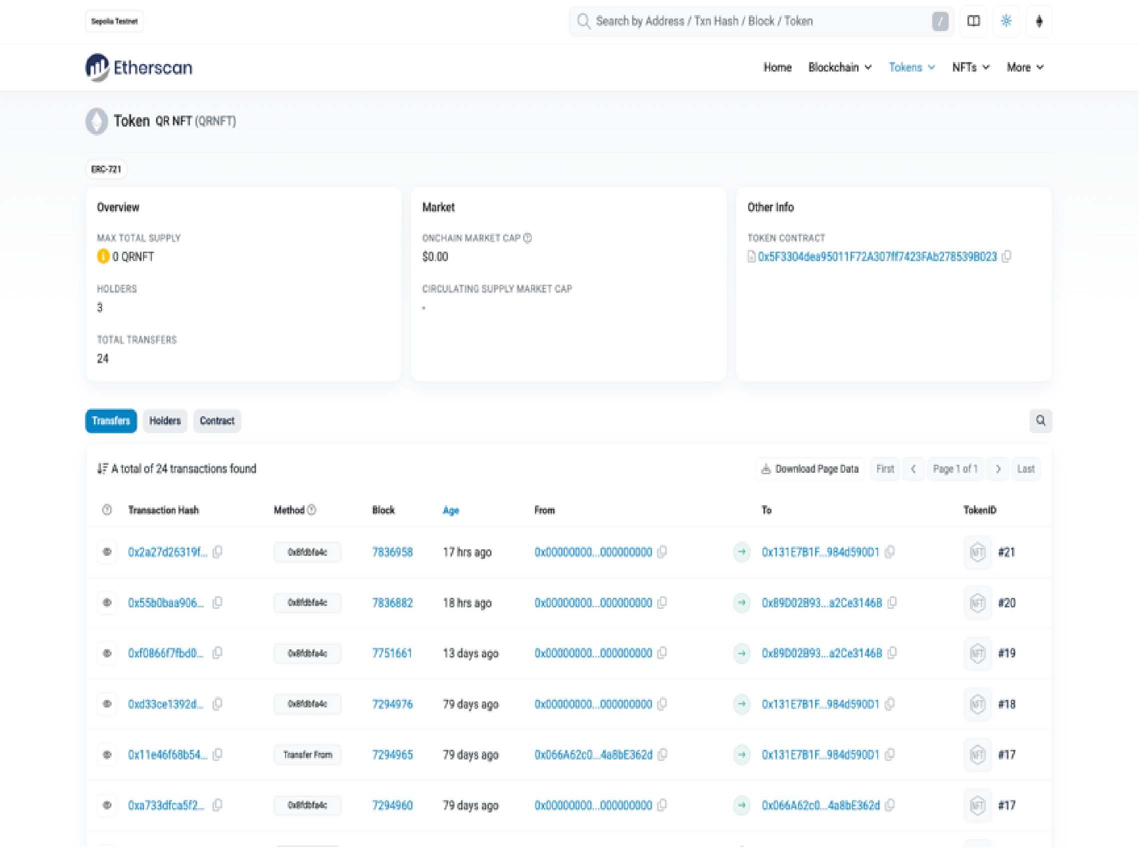
In this section, we will test the system to ensure that the developed features function as expected. Testing includes validating the creation of QR codes, the authentication process using QR codes, and testing the compatibility of seed phrases with external wallets such as MetaMask and Phantom Wallet.

1) Verifying NFT Smart Contract on Block Explorer

Our first test involved making sure the QR Code minted as an NFT was properly recorded on the blockchain and could be verified through a block explorer like Etherscan.

This verification aimed to confirm that the NFT was successfully recorded on the blockchain and remained accessible to its owner. The checking process began by looking up the NFT smart contract address used during minting. Users can simply enter this contract address in the block explorer's search field to pull up detailed contract information, including a list of all related transactions.

For this research, we deployed our NFT smart contract to the Sepolia testnet at address 0x5F3304dea95011F72A307ff7423FAb278539B023. We performed our verification checks at sepolia.etherscan.io. Checking on etherscan allows us to see more details of the smart contract itself, from the address data that deploys it, to the details of each transaction that occurs in it.



Token QR NFT (QRNFT)

ERC-721

Overview

MAX TOTAL SUPPLY
0 QRNFT

HOLDERS
3

TOTAL TRANSFERS
24

Market

ONCHAIN MARKET CAP
$0.00

CIRCULATING SUPPLY MARKET CAP
-

Other Info

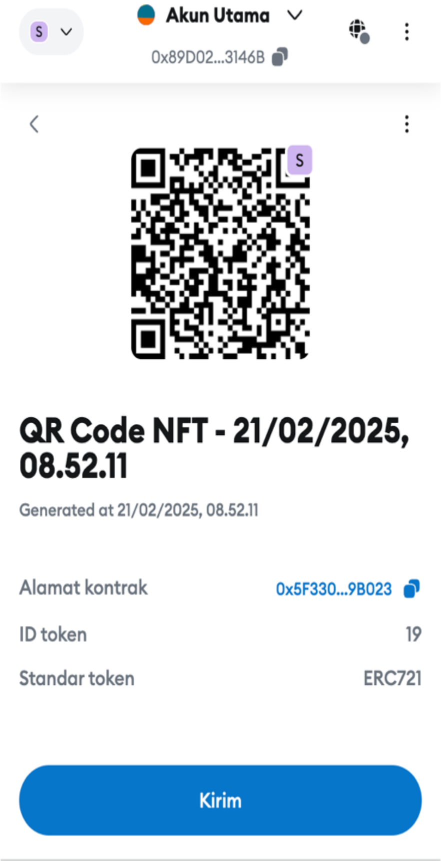
TOKEN CONTRACT
0x5F3304dea95011F72A307ff7423FAb278539B023

A total of 24 transactions found

Transaction Hash	Method	Block	Age	From	To	TokenID
0x2a27d26319f...	0x8fdbfa4c	7836958	17 hrs ago	0x00000000...000000000	0x131E7B1F...984d590D1	#21
0x55b0baa906...	0x8fdbfa4c	7836882	18 hrs ago	0x00000000...000000000	0x89D02B93...a2Ce3146B	#20
0xf0866f7fbd0...	0x8fdbfa4c	7751661	13 days ago	0x00000000...000000000	0x89D02B93...a2Ce3146B	#19
0xd33ce1392d...	0x8fdbfa4c	7294976	79 days ago	0x00000000...000000000	0x131E7B1F...984d590D1	#18
0x11e46f68b54...	Transfer From	7294965	79 days ago	0x066A62c0...4a8bE362d	0x131E7B1F...984d590D1	#17
0xa733dfca5f2...	0x8fdbfa4c	7294960	79 days ago	0x00000000...000000000	0x066A62c0...4a8bE362d	#17

Figure 7. Etherscan QRNFT

We verified NFT ownership by checking whether the asset appeared in the user's wallet. This verification can be done using any NFT-compatible wallet such as MetaMask or Phantom Wallet. When the minted NFT shows up in the user's collection list, we consider the minting process successful, and the QR Code has officially become a unique digital asset stored on the blockchain.


Akun Utama

0x89D02...3146B

QR Code NFT - 21/02/2025, 08.52.11

Generated at 21/02/2025, 08.52.11

Alamat kontrak	0x5F330...9B023
ID token	19
Standar token	ERC721

Figure 8. NFT display in Metamask

2) Check Import Seed Phrase to Metamask and Phantom

The next test is an attempt to import the wallet created to existing hot wallet providers such as metamask and phantom. As is known, cryptocurrency wallets are represented by seed phrases and private keys. Therefore, we can use and access the same wallet on different platforms.

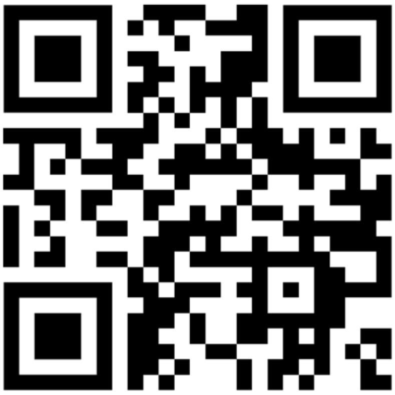
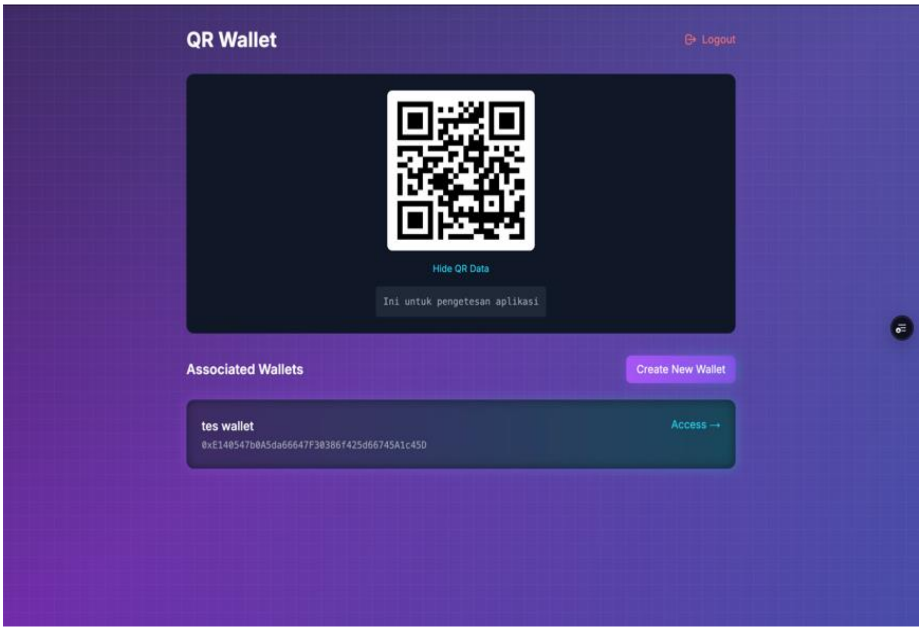


Figure 9. QR code with data "This is for application testing"

To simplify the process, here we use the qr code in figure 9 which has the data "This is for application testing". We do not use the qr generated on the generate page or the one that has been minted because it will be more difficult when readers want to test what we are doing here.

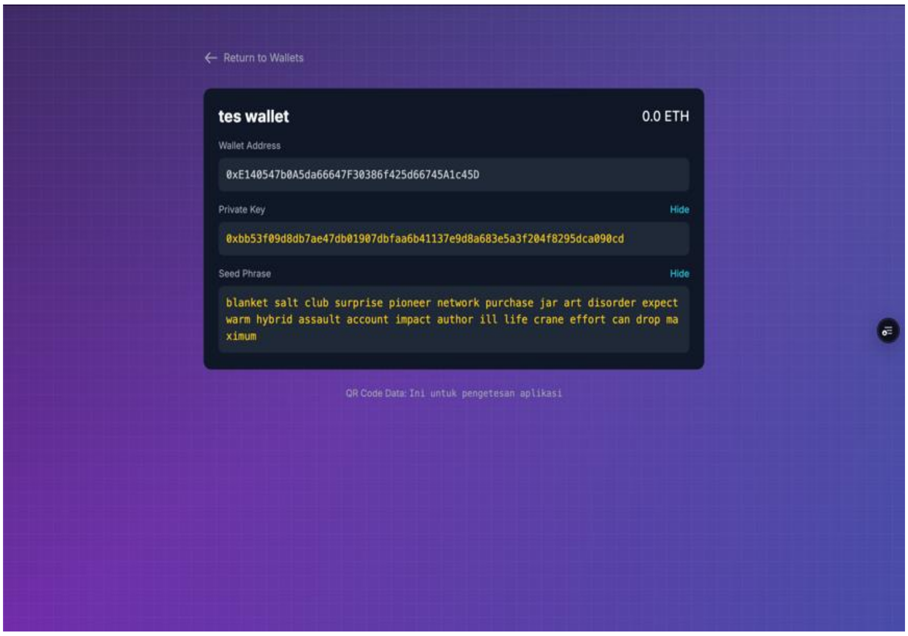


Ini untuk pengetesan aplikasi

tes wallet
0xE140547b0A5da66647F30386f425d66745A1c45D

Figure 10. Dashboard with the created Wallet.

After the QR code is successfully read, here we create a wallet with the password "123". The result is a wallet with the address 0xE140547b0A5da66647F30386f425d66745A1c45D. To enter and see more details, we enter the password as when creating the wallet.



tes wallet 0.0 ETH

Wallet Address: 0xE140547b0A5da66647F30386f425d66745A1c45D

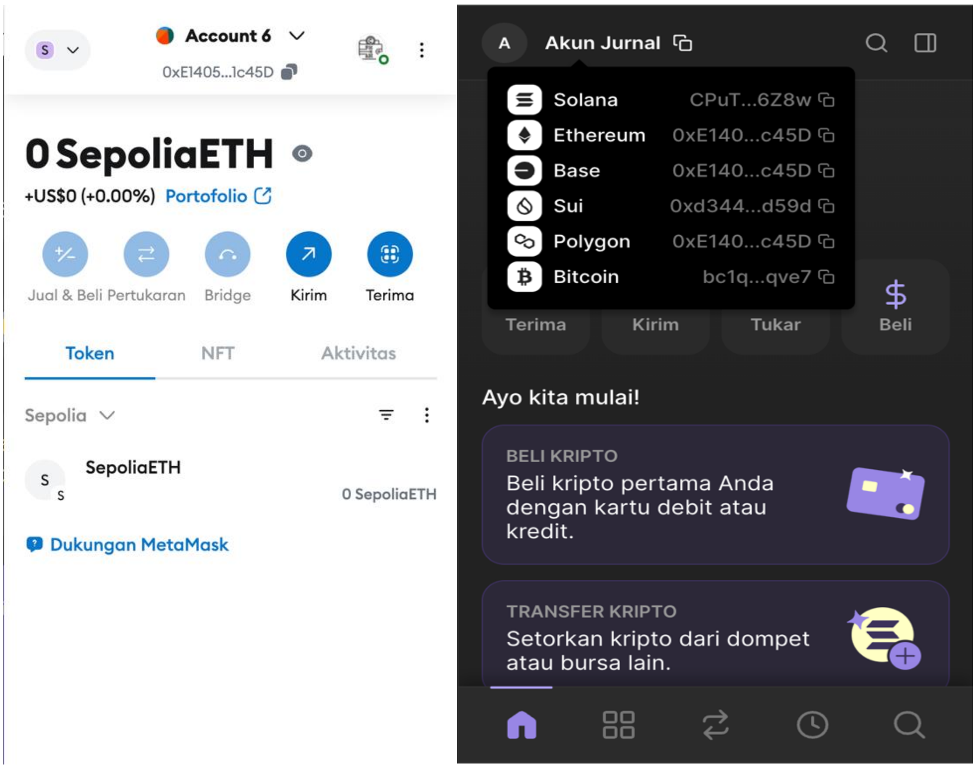
Private Key: 0xbb53f09d8db7ae47db01907dbfaa6b41137e9d8a683e5a3f204f8295dca090cd

Seed Phrase: blanket salt club surprise pioneer network purchase jar art disorder expect warm hybrid assault account impact author ill life crane effort can drop maximum

QR Code Data: Ini untuk pengetesan aplikasi

Figure 11. Private Key and Seed Phrase display.

From the QR code used plus the password "123" we get a wallet address with a private key and seed phrase that is ready to use. After getting the seed phrase, the next step is to test it by trying to import it to another wallet provider.



Solana	CPuT...6Z8w
Ethereum	0xE140...c45D
Base	0xE140...c45D
Sui	0xd344...d59d
Polygon	0xE140...c45D
Bitcoin	bc1q...qve7

Ayo kita mulai!

BELI KRIPTO
Beli kripto pertama Anda dengan kartu debit atau kredit.

TRANSFER KRIPTO
Setorkan kripto dari dompet atau bursa lain.

Figure 12, Import Results in Metamask (Left) and in Phantom (Right).

Figure 12 shows the import results in Metamask and Phantom Wallet. MetaMask is an Ethereum-based wallet that is widely used to manage digital assets and access dApps. Phantom is a wallet that supports various blockchain ecosystems, including Solana, Ethereum, Base, Sui, Polygon, and Bitcoin.

From the import results, the visible address is 0xE1405...1c45D both on metamask and Phantom. This shows that the resulting wallet is a valid wallet and can be used to make further crypto transactions later.

4.3 Discussion

This research aims to overcome the complexity and risk of seed phrases, which are often difficult to remember and potentially lost [8][9]. This system offers an alternative approach by using QR codes for the authentication process, which allows users to access their wallets simply by scanning the code they have, thus reducing the vulnerability and human error that often occurs when remembering or entering quite complicated seed phrases. This wallet is also designed deterministically, where the same combination of QR code and password will always produce identical wallet addresses and seed phrases, this is to ensure reproducibility and ease recovery without full dependence on one device. QR codes can also be minted as Non-Fungible Tokens (NFTs) on the Ethereum blockchain, this method can be an additional decentralized verification of ownership and reduce the risk of duplication or misuse. In addition, the generated seed phrases are also compatible with popular platforms such as MetaMask and Phantom, ensuring interoperability and supporting wider adoption in the crypto ecosystem, providing flexibility for users to integrate their wallets into various services.

Compared to previous research, this approach offers uniqueness. For example, Negara [12] developed an Ethereum wallet based on a mobile application, but still relies on seed phrases without alternative solutions. Richard et al. [13] analyzed the challenges of crypto wallet users, but did not provide specific solutions. Zaidenberg and Kiperberg [14] introduced a hypervisor-based HyperWallet, which although secure, is less user-friendly for non-technical users. Meanwhile, Almanfaluti et al. [15] utilized QR codes for transactions, not for wallet management.

This study integrates QR codes as an alternative solution for cryptocurrency wallet management, expanding the scope of its use to a wider field.

This approach also has the potential to be expanded by exploring the use of QR codes in other forms, such as integration on wearable devices such as smartwatches and smartbands. With the growing trend of the Internet of Things (IoT) and wearable technology, QR codes can be integrated into these devices for fast and secure authentication. For example, users can scan a QR code from a smartwatch to access a crypto wallet on their laptop and mobile phone, or the creation of a smartband that has a unique QR-Code embedded in it that can be used to create a wallet. With an easier and more user-friendly approach, the use of blockchain technology can be further expanded and adopted massively.

5. Conclusion

This research focuses on the development of a QR Code-based deterministic crypto wallet system that allows users to create and access wallets efficiently without having to remember complex seed phrases. The test results show that this method can generate valid wallets with appropriate private keys and seed phrases, which can be imported into external wallets such as MetaMask and Phantom Wallet. Thus, this system proves that the QR Code-based approach can be a safe and practical alternative solution in crypto wallet management, while reducing the risk of losing access due to user negligence in storing seed phrases.

The complete implementation of this system is available in our open-source GitHub repository at github.com/gathlabs/wallet-qr. This repository contains documentation on code to facilitate adoption by developers and researchers. Additionally, the repository includes scripts that described in this paper, allowing for independent verification of our findings. We encourage the academic and development communities to explore, utilize, and potentially enhance this solution through contributions to the repository, furthering the practical applications of blockchain technology in secure credential management.

References

[1] I. D. Astuti, S. Rajab, Dan D. Setiyouji, “Cryptocurrency Blockchain Technology In The Digital Revolution Era,” Aptisi Trans. Technopreneurship Att, Vol. 4, No. 1, Pp. 9–16, Jan 2022, Doi: 10.34306/Att.V4i1.216.

[2] W. Swastika, H. Wirasantosa, Dan O. H. Kelana, “Rancang Bangun Website Akademik Dengan Penyimpanan Sertifikat Digital Menggunakan Teknologi Blockchain,” J. Teknol. Inf. Dan Ilmu Komput., Vol. 9, No. 1, Pp. 33, Feb 2022, Doi: 10.25126/Jtiik.2021863645.

[3] Baihaqsani, A. Kusyanti, Dan P. H. Trisnawan, “Implementasi Teknologi Blockchain Dengan Sistem Smart Contract Pada Klaim Asuransi,” J. Teknol. Inf. Dan Ilmu Komput., Vol. 11, No. 5, Pp. 1105–1112, Oct 2024, Doi: 10.25126/Jtiik.1078016.

[4] R. Arora, M. Kapoor, N. Singh, Dan M. Z. Yaqub, “Green Cryptocurrency And Business Strategies: Framework And Insights From A Stewardship Literature Review,” Bus. Strategy Environ., Vol. 34, No. 1, Pp. 804–829, Jan 2025, Doi: 10.1002/Bse.3996.

[5] V. D. Senna Dan A. M. Souza, “Cryptocurrency And Financial System: Systematic Literature Review,” Rev. Adm. Empres., Vol. 63, No. 4, Pp. E2022-0019, 2023, Doi: 10.1590/S0034-759020230403x.

[6] H. Herman, J. Husna, M. K. Biddinika, D. Yulianto, F. Fitriah, Dan S. Suwanti, “Kerangka Sistem Aset Digital Pada Infrastruktur Blockchain Yang Sejalan Dengan Syariah Islam,” Jipi J. Ilm. Penelit. Dan Pembelajaran Inform., Vol. 9, No. 2, Pp. 768–781, May 2024, Doi: 10.29100/Jipi.V9i2.5431.

[7] A. Elbahrawy, L. Alessandretti, Dan A. Baronchelli, “Wikipedia And Cryptocurrencies: Interplay Between Collective Attention And Market Performance,” Front. Blockchain, Vol. 2, Pp. 12, Oct 2019, Doi: 10.3389/Fbloc.2019.00012.

[8] S. T. Bukhari, M. U. Janjua, Dan J. Qadir, “Secure Storage Of Crypto Wallet Seed Phrase Using Ecc And Splitting Technique,” Ieee Open J. Comput. Soc., Vol. 5, Pp. 278–289, 2024, Doi: 10.1109/Ojcs.2024.3398794.

[9] S. Houy, P. Schmid, Dan A. Bartel, “Security Aspects Of Cryptocurrency Wallets—A Systematic Literature Review,” Acm Comput. Surv., Vol. 56, No. 1, Pp. 1–31, Jan 2024, Doi: 10.1145/3596906.

[10] H. Byun, J. Kim, Y. Jeong, B. Seok, S. Gong, Dan C. Lee, “A Security Analysis Of Cryptocurrency Wallets Against Password Brute-Force Attacks,” Electronics, Vol. 13, No. 13, Pp. 2433, Jun 2024, Doi: 10.3390/Electronics13132433.

[11] F. M. Kurnia, “Pembangunan Aplikasi Transaksi Menu Di Kedai Xyz Kopi Menggunakan Qr-Code Dan One Time Password Berbasis E-Wallet,” Matrix J. Manaj. Teknol. Dan Inform., Vol. 10, No. 3, Pp. 113–122, Nov 2020, Doi: 10.31940/Matrix.V10i3.1919.

[12] I. P. K. Negara, A. A. N. M. A. Putra, Dan I. B. K. D. S. Negara, “Rancang Bangun Aplikasi E-Wallet Untuk Jaringan Blockchain Ethereum Berbasis Aplikasi Mobile,” J. Inform. Eng. Technol., Vol. 02, No. 02, Pp. 11–22, May 2021.

[13] R. Richard, M. A. Marsuki, G. A. Pamungkas, Dan F. Irwanto, “Enhancing Mobile Cryptocurrency Wallets: A Comprehensive Analysis Of User Experience, Security, And Feature Development,” Jitk J. Ilmu Pengetah. Dan Teknol. Komput., Vol. 10, No. 1, Pp. 15–22, Jul 2024, Doi: 10.33480/Jitk.V10i1.5157.

[14] N. J. Zaidenberg Dan M. Kiperberg, “Hyperwallet: Cryptocurrency Wallet As A Secure Hypervisor-Based Application,” Eurasip J. Inf. Secur., Vol. 2024, No. 1, Pp. 25, Aug 2024, Doi: 10.1186/S13635-024-00159-2.

[15] I. K. Almanfaluti, N. A. Putri, Dan M. S. Navaro, “Application Design: Integration Of Qris E-Wallet Cryptocurrency Using Prototype Method,” Indones. J. Innov. Stud., Vol. 26, No. 1, Dec 2023, Doi: 10.21070/Ijins.V26i1.997.

[16] M. F. Zulmy, M. V. Kurniawati, Dan S. Yazid, “The Conceptual Design E-Wallet For Rupiah Digital,” J. Ilmu Komput. Dan Inf., Vol. 18, No. 1, Pp. 29–45, Jun 2024, Doi: 10.21609/Jiki.V18i1.1309.