Scuola universitaria professionale della Svizzera italiana
Dipartimento tecnologie innovative

SUPSI

Sapphire Wallet: Blockchain Interoperability

Student

Nolli Manuele

Supervisor

Gremlich Giuliano

Co-supervisor

Guidi Roberto

Degree Course

Master of Science in Engineering: Computer Science

Year

2023 - 2024

Date

May 7, 2024

Contents

List of Figures

List of Tables

Abstract

Introduction

Chapter 1

Motivation and Context

Chapter 2

Problem

Blockchain technology lacks of *user experience*, every time a user wants to interact with a blockchain, he needs to sign a transaction, pay a fee, and wait for the transaction to be confirmed. This is a big barrier for the adoption of blockchain technology, compared to the traditional web 2.0 applications where the interaction is seamless, and the user does not need to know anything about the underlying technology.

The field is a very active research area, many solutions and chains have been proposed. In fact, millions of users and developers started to use them. [1] However, an important question arises when there are multiple chains: *which one should I use?*

Interoperability is the answer to this question, as it allows different chains to communicate with each other. In this way, the decision of which chain to use is not unrecoverable and a business can benefit from the best features of each chain without losing market share. But how can this be achieved *without experienced users?*

The goal of this Master project is to analyse the current state of the art of blockchain interoperability and account abstraction, and to propose a solution that allows users to interact with multiple chains without the need to know anything about the underlying technology.

Chapter 3

State of the Art

This chapter presents the state of the art of blockchain interoperability and account abstraction, with an emphasis on EVM-compatible blockchains.[2] In the first section, the concept of account abstraction is introduced, with a focus on the evolution of the ERC standards and the Argent wallet. The second section presents the state of the art of cross-chain communication, categorising the bridges according to the trust model, communication model, and asset transfer model. Finally, the Internet Computer Protocol (ICP) is presented, as it is a promising solution for both account abstraction and cross-chain communication.

3.1 Account Abstraction

The term *Account Abstraction* refers to the ability to extend the capabilities of an account in a blockchain. In the context of Ethereum, there are two type of accounts: [3]

- *Externally Owned Accounts (EOA)*: controlled by anyone with the private key.
- *Contract Accounts*: A deployed smart contract. Controlled by the code.

EOAs are the only account type that can initiate transactions, while contract accounts can only *react* [1] to transactions, which makes it difficult to do batches of transactions and requires users to always keep an ETH balance to cover gas. Other limitations include the lack of recovery options, the need to pay a fee for each transaction, and the risk of losing the private key. Generalising, the user experience is not as seamless as in traditional web 2.0 applications. [4]

Account abstraction is a way to solve these problems by allowing users to flexibly program more security and better user experiences into their accounts. This is achieved by *abstracting* the account model, allowing users to use contract accounts instead of EOAs. The use of

[1] A smart contract can initiate a transaction by calling another smart contract, but the transaction is still initiated by an EOA.

a new type of account named **Smart Contract Wallets** unlocks new possibilities, including: [4]

- *Flexible security models*:
- *Recovery options*:
- *Multi owner accounts*:
- *Relayed transactions*:
- *Batch/Multi transactions*:
- *Innovative User Experience*:

3.1.1 ERC standards

EIP-86, EIP-2938, EIP-3078, EIP-4337, ERC-4337

3.1.2 Argent

3.2 Cross-Chain Communication

3.2.1 Bridge classification

3.2.1.1 Trust model

3.2.1.2 Communication model

3.2.1.3 Asset transfer model

3.3 ICP: Internet Computer Protocol

Chapter 4

Problem Approach: Sapphire Wallet

4.1 Architecture

4.2 Blockchain

Smart contracts deployed on the blockchain.

4.2.1 Base Chain

4.2.2 Dest Chain(s)

4.3 Bridge

4.4 Backend

Microservices infrastructure.

4.4.1 API Gateway

4.4.2 Wallet Factory

WalletCreation.draw.io

4.4.3 Sapphire Relayer

4.4.3.1 Base Chain Relayer

TransactionExecution.draw.io

4.4.3.2 Dest Chain Relayer

All bridgeCall folder

4.4.4 Sapphire Portfolio

Problem: how to retrieve the wallet info on all the chains?

portfolio folder

4.5 Mobile Application: Sapphire Wallet

4.5.1 Wallet Creation

4.5.2 Wallet Recovery

4.5.3 Home Page

Write all the operations, balance of chains, button.

4.5.4 NFTs Page

4.5.5 Settings Page

guardian

Chapter 5

Results

Chapter 6

Conclusions

Linkografia

[1] “Essential blockchain statistics 2023.” (Dec. 2022), [Online]. Available: https://www.zippia.com/advice/blockchain-statistics/ (visited on May 6, 2024).

[2] “Ethereum virtual machine.” (), [Online]. Available: https://crypto.com/glossary/it/ethereum-virtual-machine-evm (visited on May 7, 2024).

[3] “Ethereum accounts.” (Oct. 2023), [Online]. Available: https://ethereum.org/en/developers/docs/accounts/ (visited on May 7, 2024).

[4] “Ethereum account abstraction.” (Mar. 2024), [Online]. Available: https://ethereum.org/en/roadmap/account-abstraction/ (visited on May 7, 2024).