系統安全

軟創三乙 511172176 李則霖 2024/10/31

1. 引言與研究問題

2. 文獻綜述、研究差距和方法

3. 研究架構設計

4. 意義和結論

引言

利用在系統安全課程所學，瞭解區塊鍊系統的安全性機制與防禦機制。並且嘗試在乙太區塊鍊二層Abitrum鏈seoplia測試網部屬智能合約發行ERC20標準代幣，搭配前端、後端、資料庫及Matemask錢包增加使用體驗，並且提供智能合約安全性檢測。

研究問題

1. 如何在 Arbitrum Sepolia 測試網上有效地部署 ERC20 代幣，並確保智能合約的安全性？
2. 如何最佳地整合 Metamask 錢包與全棧應用，以提供無縫的用戶體驗和安全的代幣管理？

現有研究的主要發現

現有研究提出了以太坊作為一個去中心化的應用平台的概念。 闡述智能合約的基本原理，介紹以太坊虛擬機（EVM）的概念。[1] 提出智能合約的早期概念，探討了如何在公共網絡上形式化和保護關係，討論了數字現金和微支付系統的可能性。[2]分析工作量證明（PoW）和拜占庭容錯（BFT）兩種機制在可擴展性、性能和安全性方面的優缺點。提高區塊鏈可擴展性的潛在方法包括分片和側鏈等技術。[3]

[1] Buterin, V. (2014). Ethereum White Paper.

[2] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

[3] Vukolić, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In: Camenisch, J., Kesdoğan, D. (eds) Open Problems in Network Security. iNetSec 2015. Lecture Notes in Computer Science(), vol 9591. Springer, Cham. https://doi.org/10.1007/978-3-319-39028-4_9

確定當前知識的差距

現有缺乏針對Arbitrum Sepolia等新興第二層解決方案上ERC20代幣部署的系統性研究。而且全棧區塊鏈應用開發中，前端（如Metamask整合）、後端和智能合約之間的協同機制研究不足。對於非技術用戶而言，現有的ERC20代幣管理界面仍然存在易用性和安全性的平衡問題。

擬議的研究設計和方法

- 智能合約開發測試與佈署
- 全棧應用開發與區塊鏈協同
- 安全性評估與整合WEB3

全棧區塊鏈整合架構設計

前端應用 (React.js)

後端服務 (Node.js/Express)

資料庫 (MongoDB)

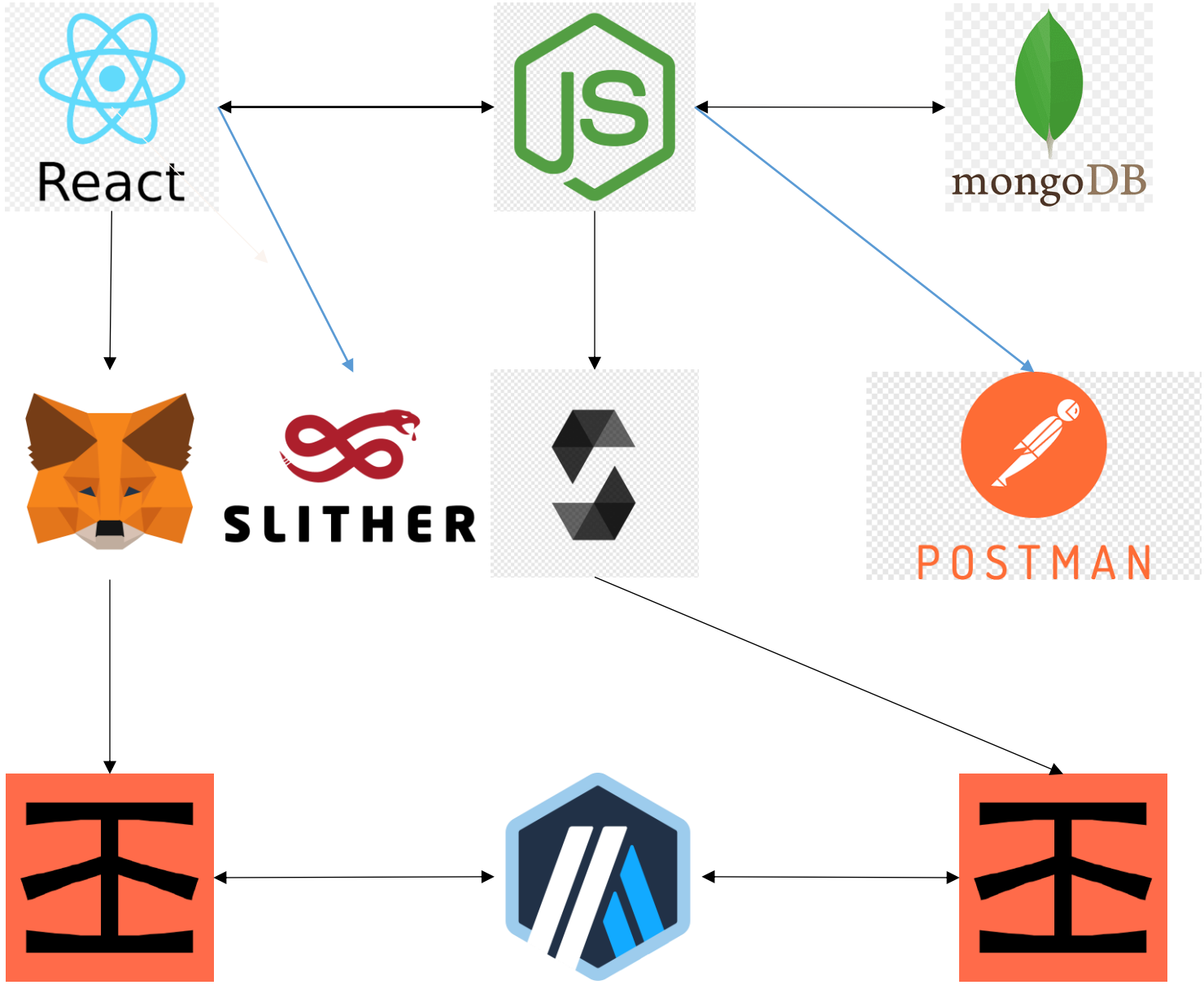
使用者錢包 (MetaMask)

區塊鏈測試網(Abitrum Seoplia)

區塊鏈節點服務 (Infura)

智能合約檢測(Slither)

API檢測(Postman)



預期結果

- 開發一個功能完整、安全可靠的 ERC20 代幣智能合約，並成功部署在 Arbitrum Sepolia 測試網上。
- 構建一個整合 Metamask 錢包的全棧應用，實現代幣的交易和管理功能。
- 分析並總結全棧區塊鏈應用開發過程中的主要挑戰和解決方案，為未來類似項目提供參考。

對系統安全的重要性

如何保護資產的安全無論在什麼年代都是重要的議題，在去中心化金融(DEFI)越來越盛行的年代，提供一個能夠在區塊鏈安全交易的資產，與容易操作的工具與便捷的方式對於整個系統發展至關重要。

報告結束，感謝聆聽。