在ARBITRUM SEPOLIA測試網上部署ERC20代幣並整合METAMASK錢包的全棧應用開發

系統安全

軟創三乙 511172176 李則霖 2024/12/12

1. 研究背景與研究問題

2. 文獻綜述 – 當前研究及研究差距

3. 方法 – 研究設計與實施

4. 預期結果、未來方向和結論

研究背景

- **網路安全形勢概述:** 區塊鏈技術成為網路安全的重要一環，其應用範圍廣泛，涵蓋金融、物流等領域。
- **當前的技術挑戰:** Layer 2 解決方案雖提升效率，但智能合約部署和整合缺乏標準化指導。
- **特定問題域:** Arbitrum Sepolia測試網上ERC20代幣的部署與安全管理。
- **研究動機:** 彌補安全性實踐的不足，提升全棧應用的開發效率與用戶體驗。

研究問題

- **研究問題:** 如何在Layer 2 測試網上實現安全且高效的ERC20代幣部署與全棧應用整合？
- **具體研究目標:**開發安全的ERC20代幣合約。改善智能合約與前後端的協作。
- **研究意義:**提供Layer 2 平台的實踐指南。改善用戶對DApp的接受度。
- **貢獻:** 首次系統化分析Arbitrum上的ERC20代幣整合。

文獻綜述 - 當前研究

現有研究:

- 提出以太坊作為去中心化應用平台的概念，介紹以太坊虛擬機（EVM）的概念。
- 探討智能合約的早期概念，如何在公共網絡上形式化和保護關係。
- 分析了工作量證明（PoW）和拜占庭容錯（BFT）兩種共識機制在可擴展性。

批判分析:

- 缺乏探討Arbitrum等第二層在提升交易速度和降低成本方面解決方案。
- 缺乏分析Metamask在用戶認證和代幣管理中的安全機制及潛在風險。
- 對於新興的Layer 2解決方案。

文獻綜述 – 研究差距

- 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。
- 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。
- 本研究將基於區塊鏈安全性理論和用戶體驗設計理論，結合系統安全最佳實踐，構建一個全面的研究框架，涵蓋智能合約開發、全棧應用整合和用戶體驗優化等方面。

方法 – 研究設計

本研究採用混合研究方法，結合定量和定性分析：

定量方法：

- 智能合約開發與部署。
- 自動化測試與性能評估。
- 數據收集與分析。

定性方法：

- 現有最佳實踐分析。
- 用戶體驗評估。
- 安全性考量探討。

方法 – 實施

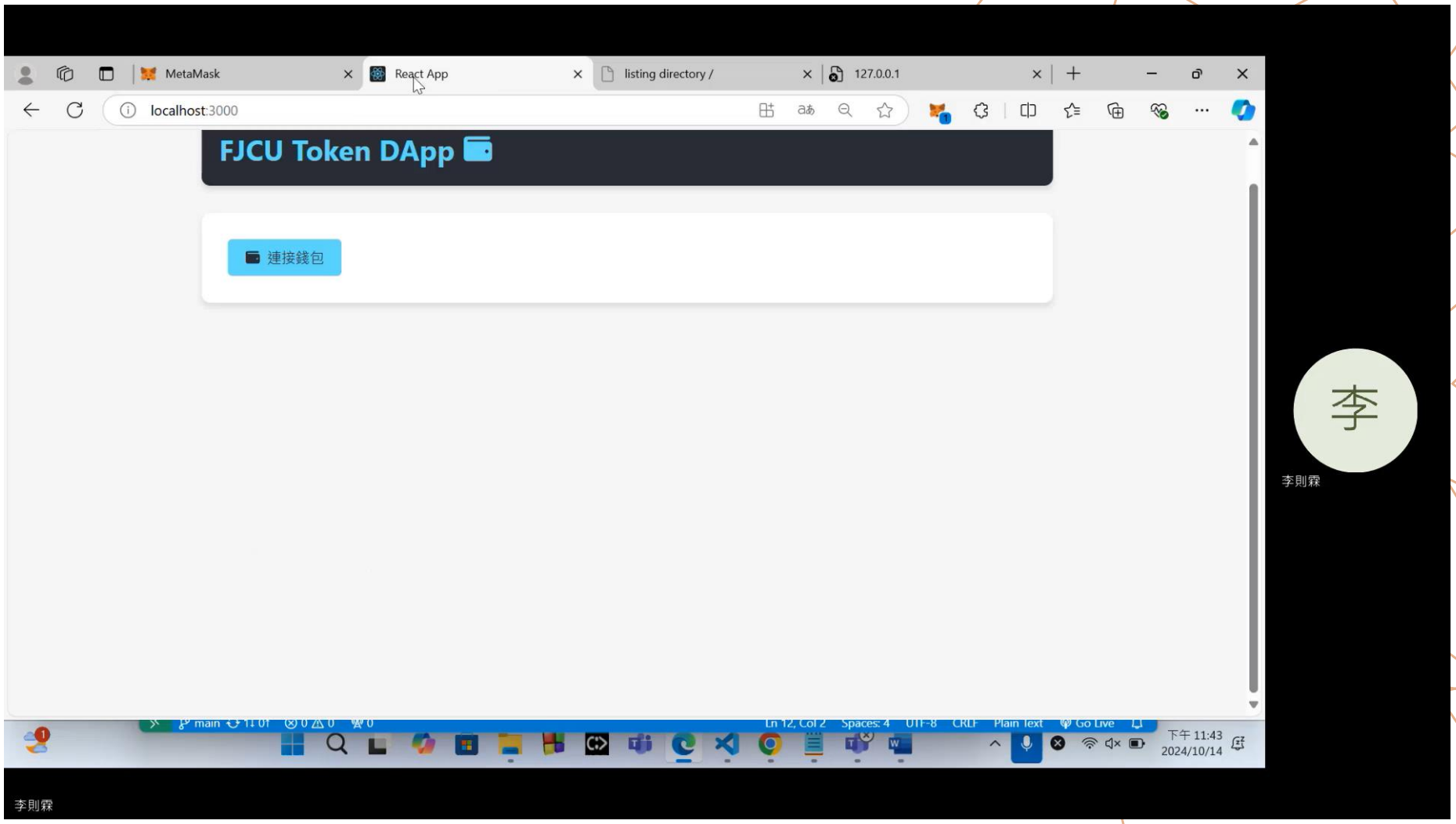
智能合約開發：

- 使用Solidity語言開發ERC20代幣智能合約。
- 在Arbitrum Sepolia測試網上部署和驗證合約功能。

全棧應用開發：

- 前端： 使用React.js開發用戶界面，整合Metamask錢包功能，並設計友好的用戶交互界面。
- 後端： 使用Node.js和Express構建服務器，處理API請求和數據管理，確保後端系統的穩定性和安全性。
- 數據庫： 使用MongoDB存儲用戶數據、交易記錄和應用配置，並實施數據加密和訪問控制以保護敏感信息。

預期成果


MetaMask
React App
listing directory /
127.0.0.1
localhost:3000
FJCU Token DApp
連接錢包
李則霖
李則霖

未來研究方向

- 擴展研究至主網環境，驗證測試網結果的有效性和可行性。
- 深入研究其他Layer 2解決方案（如Optimism）上的ERC20代幣部署及其安全性。
- 探討更多錢包整合方案，提升用戶體驗和資產管理的安全性。
- 開發更具體的測試案例和自動化測試框架，進一步提升智能合約和全棧應用的穩定性和安全性。

結論

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。

感謝聆聽 Q&A時間