G516135417 — System Security —

Project Final Exam Submission

Student Name: 李則霖

Student Number: 511172176

1. Report Structure and Components

1.1 Project Title

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

1.2Introduction

- Research context:

  隨著區塊鏈技術的迅速發展，去中心化應用（DApp）和智能合約在金融、供應鏈等多個領域得到了廣泛應用。ERC20 代幣作為以太坊生態系統中最常用的代幣標準之一，在去中心化金融（DeFi）中扮演著核心角色。第二層解決方案如 Arbitrum 的出現，進一步提升了區塊鏈的交易效率和可擴展性。然而這些新興平台上的 ERC20 代幣部署及其安全管理尚缺乏系統性的研究與實踐指南。

- Problem statement

  當前許多區塊鏈開發者在 ERC20 代幣的部署、整合和安全管理方面缺乏系統性的方法和實踐經驗。特別是在將智能合約與前後端應用結合，以及確保整個系統安全性方面，存在明顯的知識和技能缺口。

這不僅影響了區塊鏈應用的開發效率，也可能導致嚴重的安全隱患。此外，現有研究對於 Layer 2 解決方案如 Arbitrum Sepolia 上的 ERC20 代幣部署缺乏深入探討，Metamask 錢包的安全性與用戶體驗整合研究亦不充分。

- Significance of research

本研究將填補在 Layer 2 解決方案上部署 ERC20 代幣的研究空白，並提供實踐指南，提升開發者在安全性和用戶體驗方面的能力。通過整合 Metamask 錢包，將促進用戶對區塊鏈應用的接受度和使用便利性，進而推動去中心化應用的普及和發展。

- Preliminary research questions

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？
3. 在開發過程中，如何有效地結合前端、後端和區塊鏈技術，同時保障系統的整體安全性？
4. 最新的 Layer 2 解決方案和錢包安全性研究對本項目有何啟示？

1.3 Comprehensive Literature Review

- Systematic review of existing research

現有研究提出了以太坊作為去中心化應用平台的概念，闡述智能合約的基本原理，介紹以太坊虛擬機（EVM）的概念。[1]並且探討了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，並討論了數字現金和微支付系統的可能性。[2]也分析了工作量證明（PoW）和拜占庭容錯（BFT）兩種共識機制在可擴展性、性能和安全性方面的優缺點，並探討了分片和側鏈等提高區塊鏈可擴展性的潛在方法。[3] 現有研究對以太坊和智能合約的基礎知識有深入探討。

- Critical analysis of current knowledge

明顯缺乏探討 Arbitrum 等第二層解決方案在提升交易速度和降低成本方面的優勢及挑戰。例如，研究詳細分析 Arbitrum 在實現高效交

易和降低 Gas 費用方面的技術細節和實際應用案例。也缺乏分析 Metamask 在用戶認證和代幣管理中的安全機制及潛在風險。例如，評估 Metamask 在防範常見攻擊（如釣魚攻擊和惡意合約）的效果，並提出改進建議。對於新興的 Layer 2 解決方案如 Arbitrum Sepolia 上的 ERC20 代幣部署缺乏系統性的研究。此外，Metamask 錢包的安全性與用戶體驗整合研究亦不充分，尤其是在全棧應用開發中的具體實踐和協同機制方面。

- Identification of research gaps

1. 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。
2. 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。
3. 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。

- Theoretical frameworks

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。

1.4 Proposed Methodology

- Detailed research design

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：** 使用 Solidity 語言開發 ERC20 代幣智能合約，並在 Arbitrum Sepolia 測試網上部署。
- **自動化測試與性能評估：** 使用 Slither 進行智能合約的安全審計，並通過模擬不同交易場景（如高頻交易、大量交易量）評估合約的執行效率。
- **數據收集與分析：** 收集合約互動數據（如交易量、交易速度、Gas 消耗），並進行統計分析以評估性能指標。

定性方法：

- **現有最佳實踐分析：** 通過文獻分析和案例研究，總結現有 ERC20 代幣項目的最佳實踐。
- **用戶體驗評估：** 通過用戶訪談和問卷調查，評估 Metamask 錢包整合對用戶體驗的影響，並收集用戶反饋以優化應用設計。
- **安全性考量探討：** 通過專家訪談，識別全棧應用開發過程中的主要安全風險點，並探討相應的防護措施。

- Data collection methods

安全性評估：

- 使用 Slither 工具進行智能合約的靜態分析和安全審計，識別潛在漏洞並蒐集資訊。
- 進行滲透測試，評估全棧應用的安全性，特別是 API 和數據庫的防護措施，並記錄安全日誌。

用戶體驗調查：

- 設計問卷調查，收集用戶對 Metamask 整合的使用感受和反饋，涵蓋易用性、功能性和安全性等方面。
- 進行用戶訪談，深入了解用戶在使用過程中的需求和痛點，並收集改進建議。

- Proposed analysis techniques

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。

- Justification of methodological choices

  混合研究方法能夠全面評估技術實現的可行性和效能，同時深入理解用戶體驗和安全性問題。定量方法提供了具體的性能指標和數據支持，而定性方法則補充了對用戶需求和安全挑戰的深刻理解。

- Potential implementation challenges

  - **測試網環境限制：** Arbitrum Sepolia 測試網可能無法完全模擬主網的真實環境，部分測試結果可能存在偏差。
  - **技術複雜性：** 全棧應用的開發涉及多種技術，需確保前後端與區塊鏈的無縫整合。
  - **用戶參與度：** 用戶體驗評估需要足夠的參與者，以確保結果的代表性和可靠性。

1.5 Expected Outcomes and Future Research

- Anticipated research contributions

  - 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。
  - 提出一套針對 ERC20 代幣項目的最佳實踐指南，涵蓋智能合約開發、前後端整合和用戶認證等方面。
  - 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。
  - 提供具體的性能指標（如交易吞吐量、交易確認時間）和可量化的用戶體驗評估（如用戶滿意度調查結果）。

- Potential implications for system security

  - 提升區塊鏈應用在第二層解決方案上的部署安全性，減少潛在的安全漏洞。
  - 通過整合 Metamask 錢包，增強用戶資產管理的安全性，提升整體系統的信任度。

- Proposed future research directions

- 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。

1.6 References

[1]. Buterin, V. (2014). *Ethereum white paper*. Retrieved from https://ethereum.org

[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

[4]. Erinle, Y., Kethepalli, Y., Feng, Y., & Xu, J. (2023). SoK: Design, vulnerabilities, and security measures of cryptocurrency wallets. *arXiv*. https://doi.org/10.48550/arXiv.2307.12874

[5]. Gangwal, A., Gangavalli, H. R., & Thirupathi, A. (2022). A survey of layer-two blockchain protocols. *arXiv*. https://doi.org/10.48550/arXiv.2204.08032

[6]. Huang, C., Song, R., Gao, S., Guo, Y., & Xiao, B. (2024). Data availability and decentralization: New techniques for zk-rollups in layer 2 blockchain networks. *arXiv*. https://doi.org/10.48550/arXiv.2403.10828

[7]. Homoliak, I., & Perešíni, M. (2024). SoK: Cryptocurrency wallets -- A security review and classification based on authentication factors. *arXiv*. https://doi.org/10.48550/arXiv.2402.17659

[8]. Sguanci, C., Spatafora, R., & Vergani, A. M. (2021). Layer 2 blockchain scaling: A survey. *arXiv*. https://doi.org/10.48550/arXiv.2107.10881

[9]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

[10]. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

[11]. Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020). The decentralized financial crisis. *arXiv*. https://doi.org/10.48550/arXiv.2002.08099

[12]. Eskandari, S., Moosavi, S., & Clark, J. (2019). SoK: Transparent dishonesty: Front-running attacks on blockchain. *arXiv*. https://doi.org/10.48550/arXiv.1902.05164

[13]. Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). SoK: Decentralized finance (DeFi). *arXiv*. https://doi.org/10.48550/arXiv.2101.08778

[14]. Zheng, G., Gao, L., Huang, L., & Guan, J. (2021). Operation principles of smart contract. In *Ethereum Smart Contract Development in Solidity* (pp. 159–195). https://doi.org/10.1007/978-981-15-6218-1_6

[15]. Verstappen, J. (2024). A smart contract taxonomy. *Compact*. Retrieved from https://www.compact.nl/pdf/C-2024-1-Verstappen.pdf