分散式投票系統

專題編號：114-1-CSIE-S013
執行期間：113 年第 1 學期至 114 年第 1 學期
指導教授：陳香君
專題參與人員：111590003 謝品寬
111590022 丁勇智
111590450 陶冠丞

一、 摘要

本研究開發一套「分散式投票系統」，透過 P2P 網路架構實現無伺服器運作，並移除傳統區塊鏈中的代幣及挖礦機制。系統採事件驅動式投票協定，投票者在本地端使用 AES-256-CBC 加密選票後，將不含身分資訊的密文廣播至所有節點。投票截止時，各節點交換解密金鑰進行去中心化計票，確保匿名性與結果不可竄改。系統具備圖形化介面，發起者只需輸入投票主題即可建立投票。投票結束後，所有結果將加密封存在各節點，形成可驗證的永久紀錄。本系統可應用於校園、社群及 NGO，提供低成本、高安全性且易於部署的去中心化投票方案。

關鍵詞：分散式投票、無記名投票、P2P 網路、節點發現

二、 緣由與目的

現今電子投票系統主要面臨兩種極端架構的挑戰：中心化伺服器系統與公有鏈投票系統 [1]。 中心化架構雖具備易於管理與部署的優點，但其單點結構使系統成為 DDoS 攻擊的主要目標，且投票資料的公正性高度依賴管理者誠信，缺乏獨立外部審計機制 [2]。 相對地，以太坊 (Ethereum)等公有鏈投票方案 [3] 雖提供高度透明與不可竄改的機制，但其交易手續費（Gas Fee）昂貴、交易確認時間長，且缺乏原生實名機制，使其在小規模、一次性或短期投票場景中顯得成本過高且操作不便。為兼顧去中心化的信任性與低成本的實用性，本研究從 P2P 網路架構出發，建構一個「任務完成即結束」的臨時性分散式投票網路。本專案實作了一個輕量級節點架構，可透過 UDP 廣播進行區域網路內節點自動發現（Peer Discovery），並在投票結束後自動封存所有紀錄。

三、 研究範圍

本次概念性驗證（PoC）聚焦於小型自治組織的線上投票需求，目標網路拓撲為 3 至 10 個對等節點。 這些節點可部署於同一區域網路（LAN），或透過 VPN 組成一個安全的私有網路。本系統提供了一個前端介面，讓使用者能輕易地新增節點並加入 P2P 網路。而節點是系統的核心，一個獨立的 Node.js 應用程式。每個節點都運行一個 WebSocket 伺服器來與其他節點通訊。節點之間會自動交換彼此的 peer 列表，並透過 UDP 廣播來發現區域網路中的新節點，形成一個動態的 P2P 網路。 隱私層方面，本系統採用 AES-256-CBC 對稱加密。選民在 GUI 介面投票時，選票內容與一個匿名的投票 ID 會被一同加密。加密後的密文廣播至全網，而解密金鑰則由投票者節點本地保存。直到投票階段結束、進入計票階段時，各節點才會交換金鑰來解密所有選票，確保了投票的匿名性。

四、 使用技術方法

本投票系統基於以下技術實作：

- P2P 網路通訊: 使用 ws (WebSocket) 套件建立節點間的即時雙向通訊。每個 voting-node.js 實例既是伺服器也是客戶端，能主動連接已知節點，也能接收新節點的連入請求。
- 節點自動發現: 透過 Node.js 內建的 dgram 模組實現 UDP 廣播。節點會定期向區域網路廣播自己的存在，並監聽其他節點的廣播，藉此自動發現並連接到新加入的 peer，大幅簡化了網路設定的複雜度。

- 投票加密: 使用 Node.js 的 crypto 模組進行 AES-256-CBC 加密。 選票在本地 GUI 加密後，僅有密文在網路中傳輸。在計票階段，各節點廣播自己持有的金鑰，集齊所有金鑰後才能解密完整的票箱，防止任何單一節點在投票期間窺探票面內容。
- 本地驗證: 投票結束後， 拿本地的 Private token 比對投票結果的 list 確認是否有成功投票。

五、 架構流程

本系統節點間用 WebSocket 與 UDP 廣播進行節點發現並連線， 並且能自動防止重複節點 ID。投票分兩階段：投票階段（將加密投票匿名廣播智其他節點）與共識階段（節點間交換解密金鑰並解密投票達成結果共識），系統流程如圖 1。

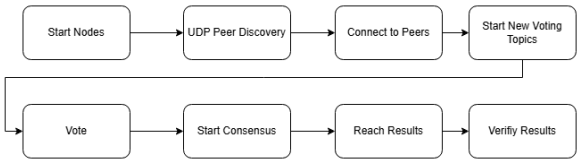

圖 1　系統流程圖

六、 實驗結果

本次實驗結果完成了投票系統以及前端介面，用戶可以透過前端介面查看已連線的節點、啟動投票、 投票。

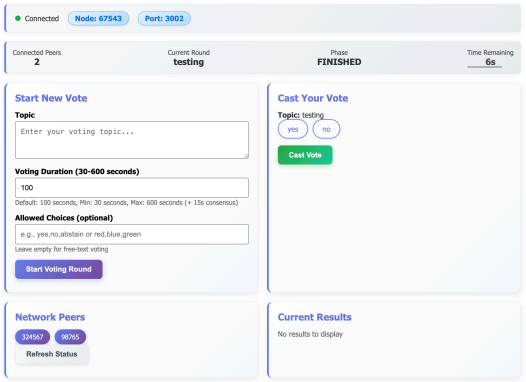

圖 2　前端用戶界面

待投票結束後，系統會自動比對票卷是否有被計入， 並顯示。

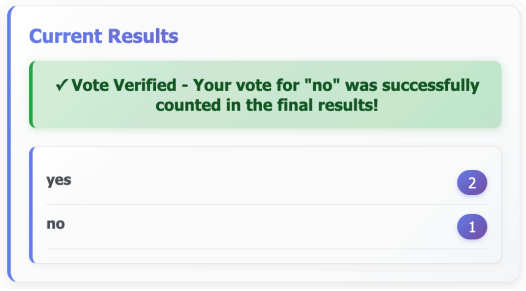

圖 3　投票後自驗票

本次實驗採用 Docker 容器化技術，讓系統在本地環境中能夠快速且便利地完成測試與部署。透過統一介面建立多個容器化節點（node），以檢驗系統的可用性與穩定性，有效縮短測試時間並降低設備成本。

七、 結論

實驗結果顯示， 該系統在 3 至 10 個節點 的小型區域網路環境中能穩定運行。透過 AES-256-CBC 對稱加密 於投票階段保護選票內容， 並僅在計票階段進行金鑰交換，有效確保投票過程的隱私性與完整性。此外，系統以「一節點一票」作為基本身份識別機制，有效防止雙重投票攻擊，驗證了此輕量級去中心化架構的可行性。

綜上所述，本研究成功驗證了一個無伺服器、可快速部署的分散式投票系統概念。未來若能進一步整合共識演算法與強化身份驗證機制，該系統可由概念性驗證（PoC）邁向實際應用，成為校園、社群與非政府組織（NGO）間可信且具成本效益的去中心化投票解決方案。

八、 參考文獻

[1] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, 和 G. Hjálmtýsson, 《Blockchain-Based E-Voting System》, 收入 *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018.

[2] M. Sharp, 《Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal》, *Network*, 2024.

[3] A. A. H. Othman, E. A. A. Muhammed, H. K. M. Mujahid, H. A. A. Muhammed, 和 M. A. A. Mosleh, 《Online Voting System Based on IoT and Ethereum Blockchain》, *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.1234567.