杜絕爭議-區塊鏈民調系統

第六組 : B09901153胡凱翔 B09901081施伯儒 B08901183喻怡鳳

動機

近年每逢選舉，選前的民調爭議總是層出不窮。雖然無法解決3%或6%的問題，然而利用區塊鏈透明和不可更改的特性，我們可以杜絕民調資料的篡改，並最大程度保證其公正性。

此外，區塊鏈去中心化技術確保交易的接受過程在多個節點之間進行，消除了中心化伺服器管理和中央數據的需求，達到保護選民隱私和個資的效果。

專題特點

- **實作GUI使用者友善介面**
- **設計一個完整公正的數位投票系統**
- **透過區塊鍊統計達成不可竄改性**
- **在以太坊上部署投開票智能合約**
- **生產出RSA公私鑰對來加解密**
- **透過TPM與R-Pi來實作FIDO驗證**
- **將私鑰儲存在TPM中**
- **透過TPM實作RSA的非對稱式溝通**
- **自行架設FIDO伺服器**

使用技術

- **Ethereum**
- **Solidity**
- **tpm2-tools**
- **web3**
- **WxPython**
- **tpm2-tss-engine**
- **flask**
- **cryptography**

流程圖