黃建勛、蕭舜文(2022),「以區塊鏈技術、流程安全與選民隱私設計之去中心化投票架構」,*資訊管理學報*,第二十九卷,第二期,頁 133-159。

以區塊鏈技術、流程安全與選民隱私設計之去中心化投票架構

黃建勛
國立政治大學科技管理與智慧財產研究所

蕭舜文*
國立政治大學資訊管理學系

摘要

利用網路取代實體投票的倡議已經被提出,同時也有數個國家與地區 (如愛沙尼亞與挪威) 嘗試實現網路投票,但由於資安與隱私的疑慮,導致網路投票至今仍沒有大規模地採用。而區塊鏈技術的公開、不可否認、可追溯性等特性,正適合用於網路投票。本研究分析過去網路投票案例與導入區塊鏈之網路投票文獻,認為當下的區塊鏈投票機制,面臨安全性、匿名性與便利性的取捨難題。目前區塊鏈投票機制主要有三大問題,第一是多數文獻提出的投票機制都屬於權力中心化的架構,一旦中心化架構遭受攻擊則投票流程或結果將會出現問題。第二,多數投票機制也只在流程末端與區塊鏈互動,即便區塊鏈的資料難以竄改,但仍無法保證數位 (區塊鏈資料) 與實體 (投票行為) 之間的完整性與一致性,進而造成損害選民的匿名性、代替投票與選票竄改等問題。第三,因為區塊鏈透明與公開的特性,若直接把選務資料與投票內容上鏈則違反投票匿名的準則。

本研究參考各文獻的投票機制後,提出一個使用生物辨識與區塊鏈技術的網路投票機制。針對問題一,本研究將投票五個階段之工作交給不同角色來執行與監督。在分權結構之下,任意一方受到全然的控制都無法完全改變投票的結果,進而降低受攻擊之風險。針對問題二,本研究的區塊鏈架構包含選民註冊、選民驗證與投票、選票挖礦與加密、選票解鎖與驗證及選票結果統計與追溯,為更完善的區塊鏈設計。問題三為解決選票隱私的問題,本研究基於生物特徵資訊的雜湊值設計選票,讓選票既可追蹤驗證也可保護隱私。本研究也討論與列舉可能之受攻擊風險,並確保本架構能有效避免遭受攻擊。

關鍵詞:區塊鏈、投票、生物辨識、去中心化、隱私

* 本文通訊作者。電子郵件信箱:hsiaom@nccu.edu.tw
2021/07/19 投稿; 2021/11/09 修訂;2021/12/20 接受

Huang, C.-S. & Hsiao, S.-W. (2022). A Decentralized Voting Framework with Blockchain Technology, Voting Process Security and Voter Privacy. *Journal of Information Management*, 29(2), 133-159.

A Decentralized Voting Framework with Blockchain Technology, Voting Process Security and Voter Privacy

Chien-Shiun Huang

Graduate Institute of Technology, Innovation and Intellectual Property Management, National Chengchi University

Shun-Wen Hsiao*

Department of Information Management Systems, National Chengchi University

Abstract

In the modern era of advanced Internet technology, the initiative to use the Internet to vote has been proposed. At the same time, several countries and regions (such as Estonia and Norway) have tried to implement online voting. However, due to many information security and privacy concerns, online voting has not been massively adopted. Blockchain technology has the characteristics of openness, immutable, traceability, these features are just suitable for supporting electronic voting. This research analyzes the past online voting cases and the online voting proposal studies introduced with blockchain. The current voting mechanism establishing a credible third party or system faces difficulty choosing between security, anonymity, and convenience. The popular blockchain voting mechanisms have three major problems. First, most of the voting structures proposed in the literature belong to a centralized power administration. Once the centralized administration is attacked, the voting process and results will be inaccurate. Second, most of the voting mechanisms only interact with the blockchain at the end of the voting process. Even if the blockchain guarantees that the data on the chain is difficult to tamper with, it still cannot guarantee the virtual (blockchain data) and reality (voting behavior) integrity and consistency, causing problems of damaging voter's anonymity, voter impersonation, and ballot

* Corresponding author. Email: hsiaom@nccu.edu.tw

2021/07/19 received; 2021/11/09 revised; 2021/12/20 accepted

tampering. Third, Because of the openness and transparency of blockchain, uploading the election information and ballot on blockchain violate the anonymity of voting.

After referring to the voting mechanism of various studies, this research proposes an online voting framework using biometrics and blockchain technology. For the first problem, the five voting stages are assigned to different roles for execution and supervision. Under decentralization administration, any party cannot alter the election results, thereby reducing the attack risk. For the second problem, this research proposes a more comprehensive blockchain voting framework that includes Voter Register, Voter Verify & Vote, Ballot Mining & Encryption, Ballot Decryption & Verify, and Ballot Counting & Tracing. For the third problem to solve ballot privacy, this research introduces biometric technology and hashing ballot to solve voting privacy and vote tracing. This research also discusses the attack risk and ensures that the proposed framework could avoid being attacked.

Keywords: Blockchain, I-Voting, Bio Recognition, Decentralization, Privacy

壹、緒論

公民投票是民主國家的基礎，但傳統的紙本投票與開票方法耗費大量時間與人力，且隨著公民對政治參與度增加，政府舉辦選舉的成本 (包含人力、場地、時間) 也隨之上升。傳統紙本投票面臨的問題有四者：1) 舉辦投票的金錢與人力成本高、2) 人工計開票效率不足、3) 人工計票的準確度不足、4) 選民機會成本高。在金錢成本上，根據中選會的資料，2018 年中華民國地方公職人員選舉 (九合一大選綁公投)，包含警衛、場地租用、驗證與開票人員共 295,904 個人員之聘用費用在內，總體預算為 47 億台幣 (李欣芳 2018)。根據澳洲選舉委員會統計，2019 年的投票支出為 3.7 億美元 (Australian Electoral Commission 2019)。人力成本方面，在 2019 年的印尼總統大選中，共計 1 億 9 千萬的選民參與投票。且主辦方要求在一天之內由人力完成開票，最終導致 272 名選務人員過勞死亡 (Shams 2019)。除了投開票效率不足之外，人工開票的準確性也較低。2018 年中華民國地方公職人員選舉中，在要求重新驗票後，不僅需耗費人力重新計票，重新計算後的總投票數比開票當天的總投票數少了 769 票。選民花費的時間也是社會成本，根據 2018 年九合一選舉的抽樣調查，台灣民眾投票時間平均為 2 分 30 秒 (林銘翰 2019)。據澳洲 PwC 諮詢機構預測，澳洲人民花費在投票的時間使得選民無法從事其他經濟活動，其機會成本為 5.25 億美元 (PwC Australia 2014)。有鑑於傳統紙本投票的低效率與高成本，社會需要一種能夠減少投開票人力與金錢成本並同時具有高準確度的投票方案。

在網路與資訊科技普及的時代背景下，許多國家開始實施網路投票。第一個大規模採用網路投票的國家是愛沙尼亞，透過國民身分證內配有加密、認證與簽署的功能，愛沙尼亞的國民可不受地域限制進行網路投票。在 2005 正式採用網路投票之後，愛沙尼亞一直採行「網路－實體並行」的投票方式，推行至 2019 年使用網路投票的選民約占總體投票人數的 44% (黃彥鈞 2019)。但在分析此投票的流程安全性時，愛沙尼亞發現部分線下流程的缺失與風險。舉例而言，外部攻擊者可以在選民裝置端植入惡意軟體，取得選民之資料或更動選民投票的選擇 (Danchev 2010)。外部攻擊者也可以透過 DDoS 阻斷主辦方的網路，使投票服務中斷。此外，內部攻擊者可以藉由比對選民的登入訊息與選民簽章來知曉選民的選票內容 (Springall et al. 2014)。另外，挪威在 2011 年導入國會選舉的遠端網路投票系統，雖然當時約有 70,000 名挪威公民使用遠端投票，但是考慮到資訊安全、隱私權與選民信任問題，國會宣布在 2013 年終止使用電子投票系統 (Segaard et al. 2014)。綜觀上述，為解決傳統紙本投票的問題，推行網路投票固然有其必要性與方便性，但同時也衍伸出資安與隱私的疑慮。一個適合現代社會使用的網路投票機制應考慮保有網路投票優點且降低資安疑慮，並且此創新的投票方法要具備下列條件：電子化 (便利、成本低、計票速度快與投票準確度高)、匿名性、真確性 (確保選民與選票之資訊為真且不可否認)、可追蹤性 (選民可驗證自身選票)、具安全性 (具備抵禦攻擊、擴容與備援能力)。

本研究認為區塊鏈技術是具有潛力成為網路投票機制的基礎，比特幣帳本從 2009 年 1 月運行至今，在沒有中央管理機構的情況下，比特幣網路仍能有效地紀錄帳本資料，任何上鏈的資料都可以被參與者追溯與驗證，達到抵擋資料竄改的目的。而區塊鏈公開、不可否認與可追溯的特性，目前已被數個國家運用在網路投票上。韓國在 2018 年宣布將進行區塊鏈投票方案的小規模測試 (Cho 2018)。2018 年底，西維吉尼亞州的投票採用含有區塊鏈技術的 APP 做為投票管道，讓身在海外的選民經過身分驗證後進行投票，並成功獲 150 位選民採用。然而，這些導入成果卻未盡完善，2020 年麻省理工大學團隊解析 2018 年西維吉尼亞州選舉供應商 Votatz 提供的應用程式發現，該應用程式有數個脆弱的資安漏洞可能致使選票內容被監控、阻擋或修改，而這些風險都發生於投票資料傳輸流程 (Specter, Koppel, & Weitzner 2020)。

區塊鏈技術可確保鏈上資料無法竄改，但實務上資料上鏈有兩個重大的問題。首先是實體與數位一致性的問題，投票行為與最終的數位投票資料其中間有許多數位流程，尤其再加上軟硬體可能的設計缺陷與攻擊者攻擊造成難以確保兩者的一致性。再者，即便導入區塊鏈技術，仍無法完全解決數位化投票的執行疑慮，例如：數位資訊難以確認選民的真確性、數位足跡難以消弭、數位選票的製造相較於紙本選票有資料損壞、偽造、儲存與竄改的安全疑慮。倘若無法確保選票資料與投票者的真確性，即使可透過區塊鏈確保鏈上資料無法竄改也將不具意義。

綜上所述，導入區塊鏈的儲存技術只解決終端資料的篡改問題，但是資料於終端上鏈前，資料傳遞、驗證選民身分、投票流程、保護選民隱私等機制若不完善，皆可能成為攻擊的缺口。因此，投票架構設計不僅是將選票資料傳至鏈上，還必須確保投票資訊傳輸過程安全且整體投票執行為安全的。

本研究的第一個挑戰是設計一個完善的網路投票機制，對此，我們將採取五階段的投票流程，基於區塊鏈導入加解密金鑰的機制和投票設計的部份 (準備流程、選民檢驗…等等)，我們將投票分為選民註冊、選民驗證與投票、選票挖礦與加密、選票驗證上鏈及選票結果統計與追溯的流程設計，且每個階段都需要與區塊鏈互動 (在鏈上留下相應之可驗證資料)，以確保每個階段的資料皆須受到驗證且無法被竄改。第二個挑戰是設計去中心化的投票架構。針對文獻中的所觀察到的安全問題，本研究提出將權力分散的機制來減少被攻擊風險，設計各角色 (例如，主辦方、投票裝置與區塊鏈驗證節點) 特有的工作與權限，同時加入區塊鏈作為防止資料被竄改的技術。第三個挑戰是確保如何設計一個安全的區塊鏈網路投票機制能防範資安的風險 (選民隱私的揭露)。本研究透過結合生物辨識機制解決網路投票的代理投票與選民隱私等問題，並以雜湊技術代表選民與選票，使得選民隱私得以保護且攻擊者難以回推其身分。

本研究並探討此架構的設計是否能有效解決網路投票的流程安全性、選民與選票匿名性等問題。透過區塊鏈特性與本架構角色分權的設計進行計算與評估來驗證此架構即使各角色受到攻擊皆不會造成投票流程安全的危害及選民與選票資訊的暴露。

貳、文獻探討

一、加密技術與區塊鏈

(一) 雜湊演算法

雜湊演算法又稱哈希函數，是一種單向不可回推的演算法，雜湊能接受任意輸入值，並輸出固定長度且不重複的值，因演算法特性，此一值可以視為輸入值的「指紋」(Feistel 1973)。比特幣中挖礦時所使用的雜湊函數為 SHA-256，此函數由美國國土安全局設計，並於 2001 年發布 (Gilbert & Handschuh 2003)，其輸出為 256 位元。此雜湊函數之值域相當大，所有可能的排列組合共有 2^{256} 個，約等於 1.1579×10^{77}，以現今的電腦計算能力，難以使用窮舉法破解，因此相當安全。

(二) 對稱式加密

在對稱式加密中，加解密僅使用一組金鑰來加密及解密訊息，此金鑰則稱為密鑰 (Secret Key)，只有擁有密鑰的使用者才能解密訊息。由於對稱式加密演算法大部分是公開的，因此密鑰在對稱式加密中非常重要不可外洩，因為對稱式加密的安全性是倚賴密鑰的性質 (例如：密鑰的長度)，常見的對稱式加密為 AES、ChaCha20、3DES、Salsa20、DES、Blowfish (Agrawal & Mishra 2012)。

(三) 非對稱加密

非對稱加密也稱為公鑰交換加密系統，最早由 Diffie 與 Hellman 提出，並首次將非對稱加密作為實務運用(Diffie & Hellman 1976)。相較於傳統的對稱加密解密使用同一把金鑰，非對稱加密使用的加密與解密金鑰是不同的，因此在沒有安全傳輸管道的環境中，資料傳輸者不用事先將自己的金鑰傳輸給接收者，雙方只需要公開自己的公鑰，理論上即可達成保密的資訊傳輸 (Edgar & Manz 2017)。

各種非對稱加密除了加解密與金鑰產生之演算法 (質數運算、橢圓曲線) 不同外，其目的都在於建立一個基於公鑰交換的資訊傳輸環境。以下圖 1 為例，訊息傳送者與訊息接收者 A 與 B 會先使用隨機數產生一組私鑰 (Private Key)，並以私鑰計算出各自的公鑰 (Public Key)，並將公鑰傳遞給對方。當雙方都同具備公私鑰後，訊息傳送者 A 會依序使用自身的私鑰與 B 的公鑰進行加密，訊息接收者 B 則是會使用自身私鑰和 A 的公鑰依序解鎖來獲得訊息傳輸者的原始訊息。

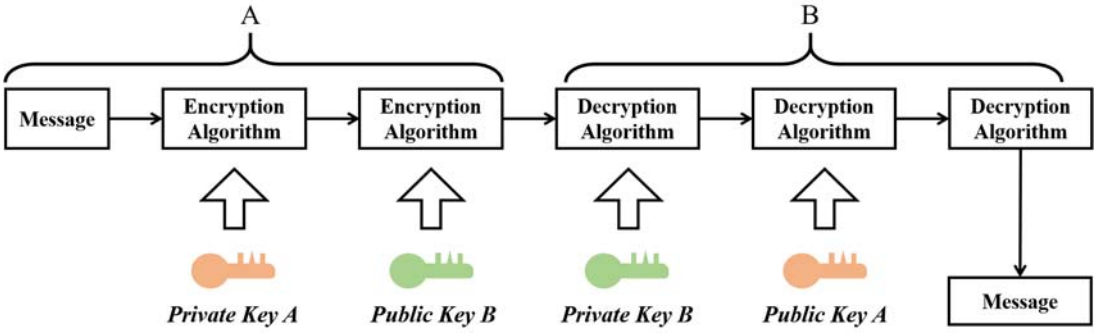

圖 1：基於公鑰交換之訊息交換示意圖

（四）數位簽章

DSA (Digital Signature Algorithm) 在 1991 年由 David W. Kravitz 提出(Kravitz 1991)，數位簽章是一種用於確保訊息正確並能驗證的方法 (US Patent No. 5231668A 1991)，基礎技術使用的是以雜湊與非對稱加密作為基礎，利用私鑰加密可以用公鑰解密的特性來驗證訊息的來源者是否正確，並對比解密後文本與解密前文本的雜湊值是否相同來確認內容真確性。數位簽章可以確定此特定訊息的發送者，且內文被沒有被更動過 (Pornin 2013)。以圖 2 說明，A 欲傳輸一文本給 B，為確保文本的正確性與發送者為 A 本人。第一步是將欲傳輸之文本以 A 的私鑰加密為加密文本，第二步是將文本計算其雜湊值並再加密成數位簽章。A 再將加密文本與數位簽章傳給 B，B 會利用 A 已公布的公鑰對加密文本與數位簽章進行解密 (圖 3：數位簽章與訊息驗證)，最後 B 計算文本的雜湊值，並比對是否與 A 傳過來的數位簽章是否相同，進而確認此一訊息來自 A 且文本並無更動。

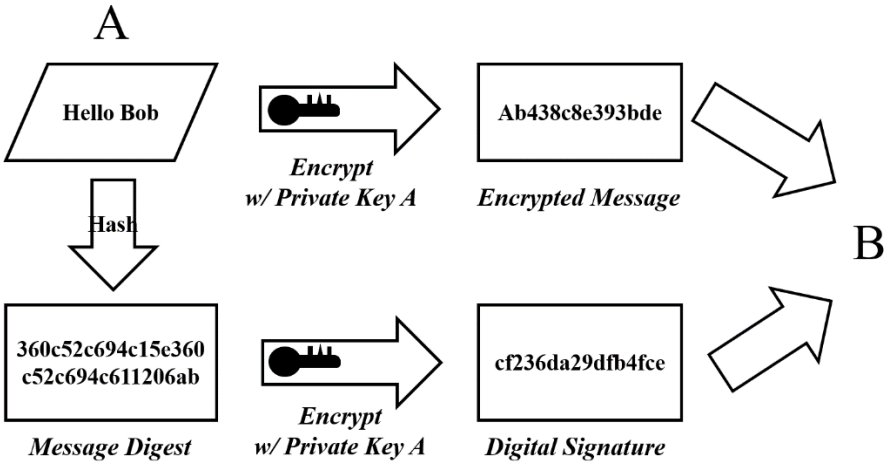

圖 2：數位簽章之製作

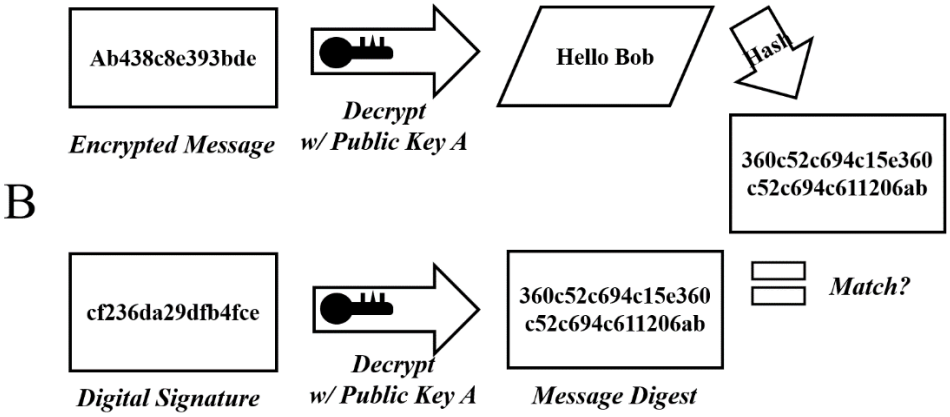

圖 3：數位簽章與訊息驗證

（五）區塊鏈技術

綜合上述之知識與技術，Nakamoto (2008) 提出的點對點交易系統中提出了區塊鏈的概念。區塊鏈可視為一種資料的儲存結構，區塊與區塊之間會透過與前者的雜湊值，加上特定的隨機值 (又稱之為工作量證明) 形成在固定目標值之內的雜湊值，並將此資訊 (前塊雜湊、塊中資料、隨機值) 進行雜湊運算，成為下

一個區塊的前塊雜湊，因此所有鏈上的區塊都是連動的。任意區塊中的資料更動都會造成區塊本身的雜湊值改變，進而造成後續所以有的區塊雜湊值改變。區塊之架構如下，圖 4 區塊鏈資料架構所示：

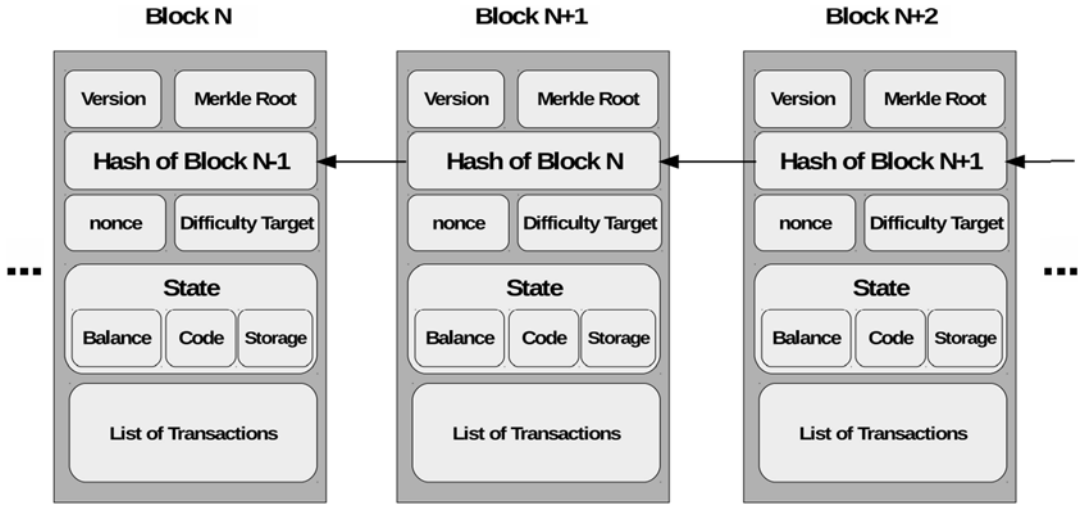

圖 4：區塊鏈資料架構
(來源 Khan & Salah 2018)

（六）區塊鏈類型

區塊鏈根據其存取與參與權限大致可以分為兩種，公有鏈、私有鏈。而公有鏈是指所有人都可以成為這個網路中的節點驗證者或是使用者，自由地發起交易，且鏈上的所有資訊都是公開的，而數據的認可則需要使用共識機制來協調，如工作量證明、權益證明等等，來維護公有鏈帳本的資料正確性。而私有鏈是由私人或是某個機構所控制的區塊鏈，不同於公有鏈，私有鏈的資訊存取權限是可控制的，由於不需要在陌生的開放環境中取的共識。私有鏈也可以由不同的機構一同組成聯盟鏈 (Consortium blockchain) 的部分去中心化架構。私有鏈可以設計成沒有貨幣 (token) 的形式，不像公有鏈需要設計某種獎勵機制來促成帳本的正確性。

（七）工作量證明

區塊鏈上資料的安全性來自於工作量證明的難度堆疊，工作量證明源於 Adam 在 1997 年提出之雜湊現金 (Hash Cash) 的構想 (Back, 1997)，該方法是對欲傳輸之訊息 (Msg) 加上一個隨機值 (nonce)，透過不斷變換隨機值並進行雜湊運算，最終會得到一個位於目標值 (Target) 域內的雜湊值 (H)。

$$Hash(Msg + nonce) = H < Target$$

此一行為被稱之為挖礦 (Mining)，在區塊鏈網路中負責挖礦並產生工作量證明的節點稱之為礦工節點。由於雜湊函數所產生的值域相當廣大，並且無法回推，只能以窮舉法嘗試，透過計算力的堆疊，攻擊者想要更動過去的資料會需要對後續的所有區塊進行從新挖礦。而區塊鏈中的共識，除非攻擊者擁有能瞬間挖完所有區塊的計算力，或是掌握超過半數的計算力。若要試圖以計算力竄改帳本中的資料，需要極為龐大且不合理的計算能力。隨著時間成長的挖礦難度、越來越多的節點加入，都會使對帳本之攻擊成本將隨時間不斷提高。

(八) 共識演算法

區塊鏈作為一種分散式資料庫，為確保在各個資料庫之間的資料都同步，也為了確保在鏈尾上被新加入的區塊內資訊是正確的，區塊鏈網路需要透過共識機制，來使各個節點確認目前新加入資料的正確性。即便沒有中心化的機構，各節點也可確保各地的帳本資料是正確且一致的。

共識演算法的設計有許多種，如比特幣採用的共識演算法屬於工量證明 (PoW)，以太坊的測試用區塊鏈 Rinkeby 採用權責證明 (PoA)，由少數較大的節點具有最高權限來處理交易。在共識機制下，帳本的資訊也會分散在區塊鏈的各個全節點 (Full Node)中，不會因為單一節點遭受攻擊而導致資料缺失或被竄改，且資料一旦被認可後便無法更改，越多全節點能更有效的分散被攻擊的成本。

(1) PoW (Proof of work): 比特幣中使用工作量證明 (PoW) 來增加每個區塊發送之成本，大幅提高散播虛假區塊的成本。在工作量證明的機制下，只有第一個解出正確答案 (工作量證明) 之節點能獲得來自 Coinbase 的獎勵，礦工節點在計算出正確的隨機值之後會將此區塊推播之各節點。各個節點會將接收到的新區塊使用雜湊函數進行驗證，如果區塊附上的工作量證明無法使區塊之雜湊小於目標值，礦工會否決此區塊。而在比特幣中，當有兩個礦工同時算出合法的工作量證明時則會產生分岔，等到下一個礦工搶先算出下個區塊的工作量證明，各節點則會取得共識，認可最長的鏈，因其包含了最大數量之計算力投入。此外，由於只有第一個達成正確值的礦工能獲得獎勵，其他礦工所付出之計算能力就會作廢，帳本使用工作量證明的方式作為誘因來鼓勵各個礦工互相競爭，可以有效控制各個節點保持誠實，卻也消耗了大量的能量。

(2) PoA (Proof of authority): PoA 作為共識機制的區塊鏈網路中會由聲譽良好之節點作為帳本的驗證者，並不是任意點都能加入成為驗證者或是礦工。不同於 PoS 或 PoW 之節點匿名性，驗證者以身分或是名譽作為類似押金的標的物，以換取簽署並且驗證他人交易之獎勵。為了避免權力濫用，一個系統中允許多個驗證者以多重簽署的方式認可交易。PoA 相比 PoW 有更高的交易處理量，但也大大的減少網路節點的分散性，能應用在供應鏈或是測試網路這種有大量資料、著重較快交易速度且不需要去中心化的私有環境。

二、網路投票與區塊鏈網路投票

(一) 網路投票案例與區塊鏈網路投票文獻整理

下表 1 為導入區塊鏈技術之投票架構文獻與兩個網路投票案例的各項投票環節手段之整理。

(二) 網路與區塊鏈投票文獻討論

(1) 投票權力中心化：從文獻回顧得知，目前的投票機制仍舊採取中心化的機制來處理信任問題，投票的流程、選票的印製、計票的系統全部由中心化的機構負責，選民只能被動地接受投票結果，並進行有限的監督。因此過去的研究企圖導入區塊鏈機制將投票結果上鏈，企圖解決中心化機制的信任與監督問題。在

投票資料儲存上，多數的研究是由主辦方來進行區塊鏈資料更新，但此投票的流程仍舊是由中心化機構負責，無法進行更嚴格的監督與驗證。Hanifatunnisa & Rahardjo (2017) 提出的投票方案資料則是採分散式上鏈，雖然分散式上鏈較符合去中心化的概念，但僅將投票結果上鏈 (亦即資料儲存的去中心化以及有限的公開化)，仍無法完全解決中心化機構的信任問題，投票的流程仍舊是由中心化機構負責無法進行更嚴格的監督與驗證，例如：2020 美國總統大選的多米寧 (Dominion) 投票機遭候選人川普指控不安全 (Giles & Horton 2020)；位於密西根州安特里姆郡（Antrim County）的計票軟體也遭指控將原屬共和黨的票數計入民主黨 (張如嫻 2020)。在引入區塊鏈的情況之下，無論指控是否屬實選舉人與被選舉人均可監督與驗證投票，消弭不信任與不實指控的問題。

表 1：各網路與區塊鏈投票文獻綜合評比

文獻	投票環境	需求裝置	選民註冊手段	選舉驗證手段
Ayed (2017)	定點註冊遠端投票	電腦或行動裝置	資料庫	檢查選民資料庫
Hjálmarsson et al. (2018)	遠端	能與智能合約互動裝置	資料庫	檢查選民資料庫
Liu & Wang (2017)	遠端	電腦或行動裝置	驗證子	檢查驗證子簽章
Hanifatunnisa & Rahardjo (2017)	遠端	能與智能合約互動裝置	資料庫	對比資料庫
Wei & Wen (2018)	遠端	行動裝置	Ballot ID 生成	Ballot ID 與個資配對
愛沙尼亞案例 Estonia (2020)	遠端	電腦	無	註冊資料登入
新南威爾斯案例 Brightwell et al. (2015)	網頁或電話	電腦或電話	Voter ID 與 PIN 碼	註冊資料登入
文獻	選票辨別	區塊鏈共識	選票追溯手段	匿名性手段
Ayed (2017)	個資雜湊	PoW	重現選票資訊	資料雜湊化
Hjálmarsson et al. (2018)	無提及	PoA	透過 TX ID	透過智能合約的互動
Liu & Wang (2017)	盲簽之選票	無提及	無提及	選民使用第二組公私鑰投票
Hanifatunnisa & Rahardjo (2017)	無提及	依預訂節點順序驗證	無提及	透過預先設定之節點投票
Wei & Wen (2018)	選民指紋	無提及	重現選民指紋	選民指紋
愛沙尼亞案例 Estonia (2020)	選民簽章	X	追蹤選民簽章	簽章剝離
新南威爾斯案例 Brightwell et al. (2015)	選民簽章	X	追蹤選民簽章	簽章剝離

中心化的機構除了信任問題外，在網路投票的情境下面臨更高的資安風險，包含攻擊威脅與選民隱私。攻擊威脅可分內部與外部，內部威脅考慮到單一機構可能產生的濫權行為，因此應設計更完善而開放的監督與驗證機制。外部威脅考慮投票軟硬體系統可能遭受到攻擊，導致投票的過程或結果有誤，因此利用去中心化的投票架構或可降低資安風險。區塊鏈投票架構因得利於分散式結構，可以避免單一系統遭到攻擊。因此，本研究在引入網路投票機制時，同時考量整體的投票流程上鏈以及分散式的投票架構，以確保網路投票的信任與避免安全問題。

(2) 裝置安全性疑慮：文獻皆希望選民可以進行遠端網路投票，但此設計須考量到選民的裝置是否皆能達到一定的資安水準。在實行層面，管控選民不同的裝置將相當困難。此外，遠端投票將無法確保操作裝置的人是否為選民或受到脅迫。無論是現行案例或是文獻都無法去除冒充他人投票的可能性。只要攻擊者取得其帳號密碼，即可假冒成選民進行投票，選票追蹤也使買票方更容易監控選民的選票 (Estonia 2020)。因此，本研究認為現階段使用具有專用裝置 (生物辨識) 的投開票所有其必要性，於投開票所投票可以確保投票人在一個公開卻隱密的環境投票，可以避免投票遭到監控或脅迫。並可確保註冊與投票均為本人之動作，確保網路投票無作弊之可能，因此現階段設計為線上與線下混合型。未來若個人智慧裝置具有安全性驗證裝置 (例如：TPM (Trusted Platform Module)、NFC 及指紋、人臉辨識裝置等) 則可使用非專用裝置投票，也無需特別設立投開票所。

(3) 選票辨別資訊與選民之連結：從過去的文獻中得知網路投票的方式需要驗證選票為選民本人，因此選票將會與選民連結，進而使選民資訊容易因為選票而洩漏，造成選民的隱私權與投票匿名性之損害。因此，Hanifatunnisa & Rahardjo (2017) 提出讓選民透過預先設定好之節點來投票，並消除選票與選民資料的連結，透過合法節點來送出選票，可以保障選民的隱私權。但因為選票沒有選民資訊導致選票缺少可驗證性，若其他流程中被攻擊而加入虛假的選票則會無法驗證。因此，Ayed (2017) 與 Wei & Wen (2018) 提出的選票上存有識別選民的資訊，主辦方利用選民資料製作出 Ballot ID，讓選民可以透過選票上的資訊或 Ballot ID 追蹤驗證選票。但若攻擊者可破譯選票資訊或 Ballot ID，則可曝光該選民的資訊與選票 (Hanifatunnisa & Rahardjo 2017; Ayed 2017; Wei & Wen 2018) 。因此，本研究設計選民身分資訊加密、選舉辨識碼以及生物辨識資料雜湊。此三樣資訊可以唯一辨識選民身分、選舉與選民生物辨識資料，攻擊者無法變造或還原任意資訊。將生物辨識資料雜湊資料庫儲存於區塊鏈上也可以保證生物辨識資料庫不會被攻擊與變造，而生物辨識資料以雜湊的方式儲存可以保證其選民隱私安全。

(4) 區塊鏈設計：區塊鏈導入的投票系統文獻皆是私有鏈或許可鏈而非公有鏈，即使公有鏈的去中心化程度與攻擊成本都較私有鏈高，但公有鏈的交易處理量較慢，無法應付大量投票的需求。再者，採用私有鏈可以有效管控帳本的驗證者或節點，並能省去比特幣或是以太坊中巨額的交易手續費用與燃料費用 (Hjálmarsson et al. 2018)。因此，本研究採取私有鏈的方式進行區塊鏈導入，此方式可以處理大量的投票資訊、嚴格控管投票的節點與省去公開鏈的交易手續費用。

(5) 投票資訊與鏈之互動：Ayed (2017) 和 Brightwell et al. (2015) 的案例都是使用資料庫做為選民驗證依據，將選民資料與資料庫的註冊資料進行比對。但只要主辦方伺服器遭到攻破，攻擊者就能添加虛假的選民資料進而偽造選票。因此，其他網路投票設法導入了區塊鏈，以解決單一資料庫被攻擊的問題。但除了 Hjálmarsson et al. (2018) 提出的智能合約投票外，其餘的區塊鏈投票方案都是在確認選票資訊無誤後，再由主辦方的節點將最後的選票新增上鏈。然而，選民的註冊與驗證都沒有與區塊鏈互動。若攻擊者竄改選民註冊或驗證資料，主辦方將無法驗證，攻擊者只要照原有的流程執行，依然可以將虛假的選票上鏈，此區塊鏈導入方式無法解決選民驗證遭受攻擊的缺點。

綜上所述，此研究提出將所有註冊、領票、投票與驗證流程都與區塊鏈互動，將各階段之資料都上鏈，使各個階段皆無被攻擊造假之風險。

(三) 小結

從各個文獻選民驗證手段、選票加解密與選票訊息來看，在投票機制的設計上，將面臨匿名性、安全性與便利性三者之間的互相取捨，如下圖 5 所示：

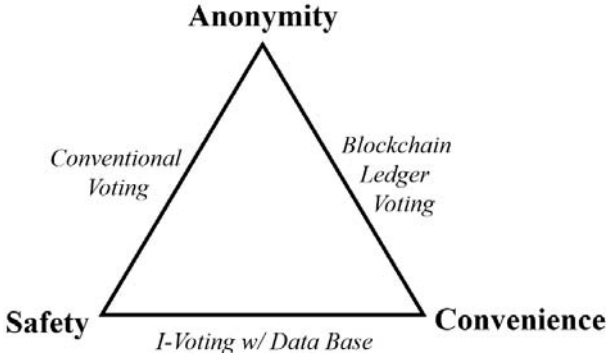

圖 5：網路投票之三角圖

在網路投票的三難中，直接使用加密貨幣進行投票，可以最大程度的滿足匿名性與便利性，任何能與區塊鏈互動之裝置都可以是投票裝置，帳戶本身也沒有與選民連結，但也容易造成買票、選票灌水、代替投票等問題；而傳統紙本投票犧牲了最大程度的便利性，來達成匿名性與安全性；選擇有主辦方的網路選票雖然能確保安全性，但為了確保選民的合法性，主辦方採用金鑰簽署或是資料庫對比的方式，會一定程度的犧牲選民的隱私。延續上述的三難抉擇，在安全層面上，個人裝置難以確保其軟體與硬體上沒有被惡意控制或是監視，而公開於大眾的網頁投票容易遭受 DDoS 攻擊。由於遠端投票的部分只要掌握選民的資料或是密碼即可控制其金鑰來進行投票，因此較建議以可控管之裝置進行投票。關於便利性的指標有兩者，一是選民註冊與投票的方便程度，使用行動裝置或是到主辦方規定之場地進行投票，二是選民查詢選票的難易度，過於簡易的選票追蹤功能可能導致買票者更容易確認，因此也需要有限度的限縮選民任意查詢的權利。

總結來說，區塊鏈只能解決末端資料被竄改的問題，但仍面臨網路投票的問題。因此針對區塊鏈作為基礎的網路投票，主要問題有三：投票權利過於集中而導致的高風險、選票買賣可能性與選民隱私、投票環節與區塊鏈互動過少。

參、文獻探討

一、情境假設與區塊鏈設計

(一) 資料傳輸與基礎建置假設

本研究之情境會有一個公正且安全的權威性機構 (Central Authority，以下簡稱 CA，例如：內政部憑證管理中心) 作為公鑰交換與加解密的基礎設施。每個裝置都配有預先註冊在 CA 的公鑰 (Public Key)。因此，在 CA 是具有權威且可信賴的情況之下，裝置資料進行傳輸會具有機密性 (Confidentiality)、一致性 (Integrity)。在此假設之下，即便傳輸之訊息被攻擊者中途攔截也無法解密得知訊息，因為攻擊者必須取得接收者的私鑰 (Private Key) 才有對訊息解讀之能力。此外，為了確保選民的真確性，本架構使用生物辨識技術將雜湊化的生物特徵資訊結合至選票中，只有本人才能進行投票且非本人無法追溯選民資訊。此機制需配合生物特徵資訊、具有身分證資料之 IC 卡 (身份證字號、選民密鑰 (Secret Key))。因此假定所有選民皆配有此類 IC 卡，同時所有有效選民的生物特徵資訊會註冊於政府控管的生物特徵資訊資料庫中 (通常可於選民註冊時蒐集)。

(二) 區塊鏈設計

以太坊的創辦人 Vitalik Buterin 在 2017 年會議中 (Buterin 2017) 以不可能的三角形來描述區塊鏈網路的設計瓶頸，敘述在一個分散式帳本中，其效能 (P)、去中心化 (D) 與安全性 (S) 三者無法同時並存的，在同樣的安全性程度下，去中心化程度將與效能成反比 (Gomez 2017)。

$$P = \frac{\alpha}{D \times S}$$

由於本設計的安全性是不可妥協之特性，因此在設計上對效能與去中心化進行取捨。由於投票的環境中，短時間內會有大量的選票須被處理，因此區塊鏈必須具備處理高交易資料量 (Transaction Per Second, TPS) 的能力。且因為投票主辦方的存在，因此完全地去中心化並不是最主要的訴求，所以能夠適當的保留去中心化機制用以抵禦攻擊即可。因此本研究為了保證安全性與極大化區塊鏈效能，本研究架構採用 PoA (Proof of Authority) 共識機制的許可鏈，不會開放未經許可的節點加入區塊鏈，且由少數的驗證節點來處理交易。

二、提案主架構

本文所提出之投票架構屬於線上與線下混合型，選民仍需進入配有特殊投票裝置的投票場所 (流程圖中稱投票裝置) ，並且本架構配有生物特徵資訊資料庫 (Bio DB) 和公鑰資料庫 (Public key Database, PKey DB) 與數個選舉舉辦方控管之節點 (PoA Node)。本研究之主架構共分以下階段：(1) 選民註冊 (Voter Register)、(2) 選民驗證與投票 (Voter Verify & Vote)、(3) 選票挖礦與加密 (Ballot Mining & Encryption)、(4) 選票解鎖與驗證 (Ballot Decryption & Verify)與

(5) 選票結果統計與追溯 (Ballot Counting and Tracing) 選票結果統計。圖 6 為階段 1-4 之示意圖。表 2 為主架構所使用的元件名稱與說明。

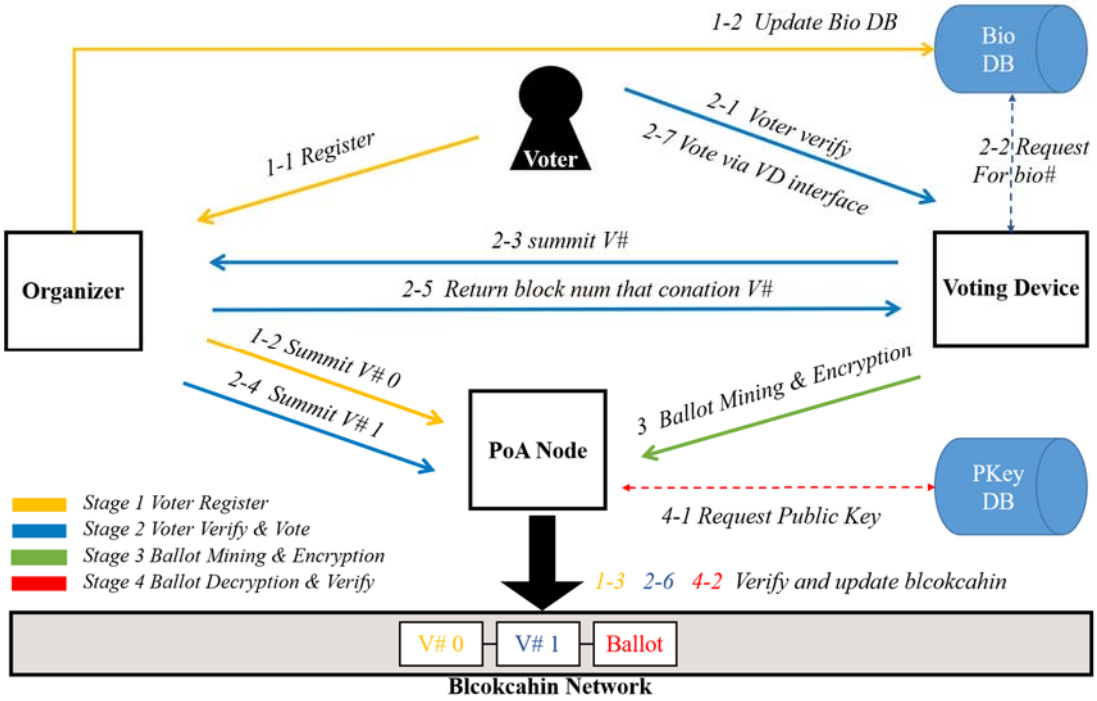

圖 6：主架構流程 (依照參與方)

表 2：主架構元件名稱與說明

名稱	說明	簡寫
生物特徵資訊資料庫	儲存選民之生物特徵資訊 (Bio Data) 與生物特徵資訊雜湊 (Bio Hash)。	Bio DB
主辦方機構	主辦方機構可以是選務機構或是外部廠商，配有生物辨識與身分證讀取裝置，並負責發送選民的註冊與驗證紀錄給區塊鏈驗證節點。	Organizer (Org)
投票裝置	投票裝置需要在投票之前部署，具生物辨識與身分證讀取，並具有產出選票的能力。	Voting Device
公鑰資料庫	配有各投票裝置代碼 (Did) 與對應之公鑰。	Pkey DB
區塊鏈網路驗證節點	將來自主辦機構的選民註冊與驗證紀錄上鏈，對投票裝置傳輸之選票進行驗證再上鏈。	PoA Node
區塊鏈	區塊鏈的主鏈，儲存三種不同類型的資料。	Main Chain

三、投票流程分析

本研究所使用的區塊鏈 (以下稱 Main chain) 會是以許可鏈的形式，只有驗證節點 (以下簡稱 PoA Node) 才能將投票資料驗證與上鏈，而主辦單位 (Org) 與一般民眾皆可以讀取鏈上資料。Main chain 中的資料會根據不同投票階段會有三種不同功用的資料依序為：

(1) 選民註冊紀錄 (以下簡稱 V#0)

(2) 選民驗證紀錄 (以下簡稱 V#1)

(3) 選票 (以下簡稱 Ballot)

Main Chain 有三種不同格式的資料，其關係如 (圖 7) 所示。在註冊階段時 (Voter Register Stage) 鏈上資料皆是選民註冊紀錄 (V#0)，選民註冊階段結束後，不允許再有選民資料上鏈。投票階段時 (Voting Stage) 則有選民驗證紀錄 (V#1) 與選票 (Ballot) 紀錄交錯儲存於鏈上。當選民於投票裝置經投票機驗證選民 ID 卡與生物辨識資訊時，選民驗證紀錄會由投票裝置生成，並關聯至選民註冊紀錄後再經由 PoA Node 驗證上鏈。由於註冊、驗證與選票皆紀錄於鏈上，Org 與 PoA Node 可進行資料比對來確保資料的正確性。選民也可透過自身 ID 卡中對稱式加密的密鑰 (Secret Key) 與生物特徵資訊雜湊驗證該選票是否確實上鏈。

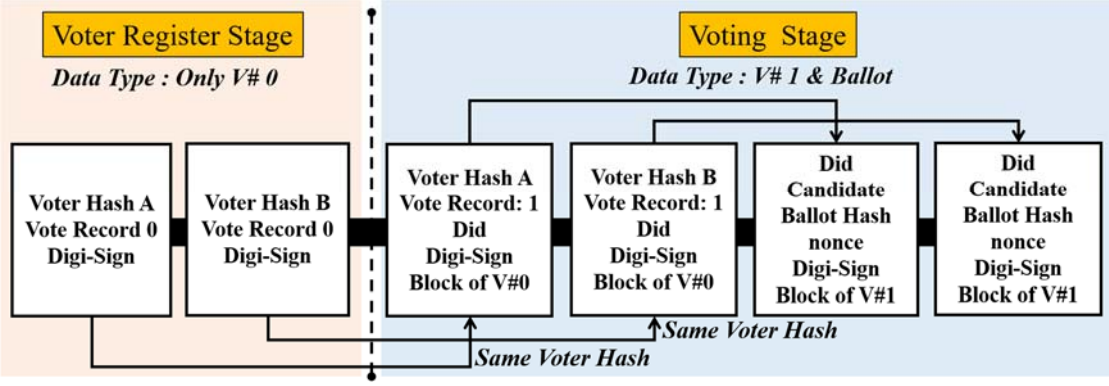

圖 7：本研究區塊鏈資料示意圖

(一) 選民註冊 (Stage 1: Voter Register)

如圖 8，此階段對應主架構 (圖 6) 中的步驟 1-1 至 1-3：選民需要在投票開始之前進行註冊，流程依序如下：

(1) 選民須到主辦方 (Org) 進行身分資料與生物特徵的驗證與註冊，確保該選民、ID 卡上身份資料及生物特徵吻合為同一人。

(2) 為保證選票資料上並無明碼之 ID 資料 (例如：身分證號碼)，選民身份將由 ID Encryption 表示，其產生方式為 ID 卡內之電路直接將身分證資料利用 ID 卡內的密鑰 (或其變形，例如 Salted Key) 進行對稱式加密後輸出於讀卡機。此加密身份資料僅能由此選民之 ID 卡產生，除選民本人外皆無法回推 ID 資料，可確保投票之匿名性。將選民加密之身份資料 (ID Encryption)、生物特徵資訊雜湊 (Bio Hash) 與選舉辨識碼 (Election Code) 三者綜合之雜湊結果紀錄為選民雜湊 (Voter Hash)。

(3) 主辦方 (Org) 在完成選民註冊後，主辦方將 Voter Hash 與投票紀錄等資訊進行簽章，此紀錄 (V#0) 會被當成 transaction (TX) 傳送給區塊鏈網路的節點，以作為後續投票的驗證依據。

在註冊階段，所產生之 TX 是位於選民註冊紀錄 (V#0)，此 TX 會將下列資訊傳送至區塊鏈驗證節點 (PoA Node) 進一步進行驗證：

(1) 選民雜湊 (Voter Hash)

(2) 投票紀錄 (Vote Record)

(3) 本筆資料之數位簽章 (Digital signature form Org)

只有當擁有本人的身分證資料加密 (ID Encryption) 與生物特徵資訊雜湊 (Bio Hash) 時才能產出正確的選民雜湊 (Voter Hash)。因此，每個選民雜湊都代表一名合法的選民。選舉辨識碼為每次選舉中獨特的識別碼，用以確保選民在不同的選舉活動中有不同的選民雜湊 (Voter Hash)。

V#0 資料中的數位簽章可由主辦方之私鑰進行簽章，以確保註冊資訊的完整性與來源，其私鑰為主辦方保管，公鑰則事先公開。另外，在投票前也需分別建置兩個不同的資料庫：生物特徵資訊資料庫 (Bio DB) 與公鑰資料庫 (Pkey DB)，分別記錄選民之生物特徵資訊雜湊 (Bio Hash) 和各投票裝置之公鑰。

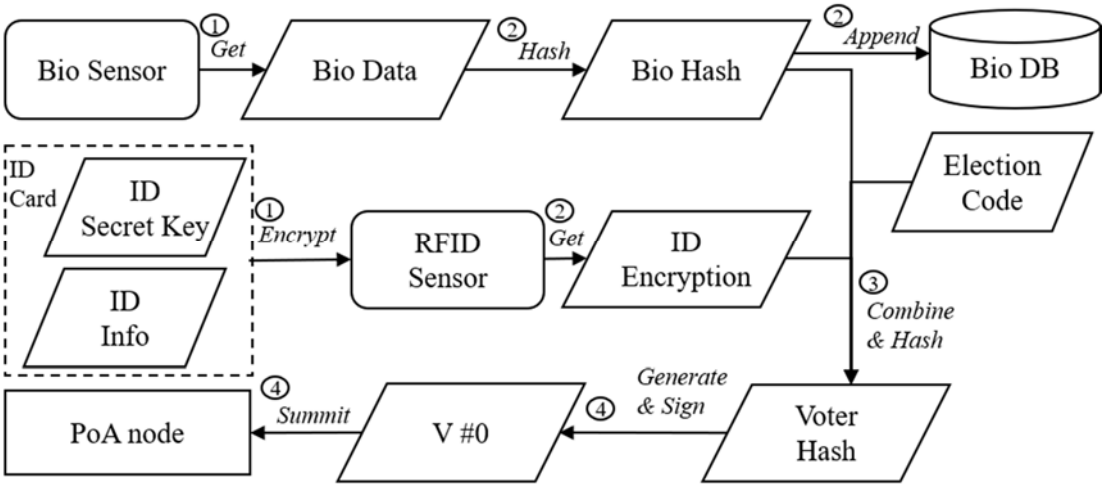

圖 8：選民註冊流程圖

(二) 選民驗證與投票 (Stage 2: Voter Verify and Vote)

此階段如圖 9 對應主架構 (圖 6) 中的步驟 2-1 至 2-6 選民驗證環節。圖 9 是投票裝置與主辦方互動之流程圖：

(1) 選民進入投票場所需經兩層驗證，第一個是身分證資料驗證，第二個是生物特徵資訊驗證，透過身分證 IC 卡取得加密之身分證資料，再將生物特徵資訊雜湊送至 Bio DB 進行比對，確認為已註冊之選民。

(2) 投票裝置將 ID Encryption、Bio Hash 與 Election Code 的數據綜合並進行雜湊運算，進而得到選民雜湊 (Voter Hash)。

(3) 主辦方收到後會對鏈上之選民註冊紀錄 (V#0) 進行比對，若存有相同的選民雜湊則代表此選民為註冊選民，將回傳其區塊號碼 (Block No.)，並更新選民的投票狀態使其無法重複投票 (V#1)。此階段之 Bio DB 只允許讀取，因此可利用分散式資料庫或是離線存取方式，減少伺服器的負荷。

(4) V#1 作為選民驗證紀錄，由投票裝置簽章後發送至 PoA Node，其私鑰為投票裝置保管，公鑰則事先公開，V#1 將包含選民雜湊 (Voter Hash)、投票紀錄 (Vote Record)、投票裝置號碼 (Did)、此資料之數位簽章 (Digital Signature by Voting Device)、選民註冊記錄區塊 (V#0 Block. NO)。

下一階段如下圖 9 對應主架構 (圖 6) 中的步驟 2-7 至 2-6 選民驗證環節。圖 10 是選票資訊 (Ballot Value) 產生之流程圖：

(1) 選民在透過身分驗證取得 Voter Hash 後，本研究並不直接使用 Voter Hash 作為 Ballot 上的選民資料，而是再串接一個可控範圍的隨機值混成並進行雜湊運算得到選票雜湊 (Ballot Hash)。此設計使雜湊結果與選民雜湊不會有直接連結以增加選票的獨立性。而且在未知此隨機值的情況之下，駭客只能使用暴力破解法 (Brute Force)來獲得 Voter Hash。但選民可以在已知 Voter Hash 的情況下，利用選票追溯的機制來確認自身的投票內容 (見選票結果統計與追溯階段 Stage 5)。選民在確認其 Voter Hash 之生物辨識及 ID 身份正確的同時，可由投票裝置介面選取候選人或廢票，再由投票裝置結合 Ballot Hash 生成選票 (Ballot)。因此，選票 (Ballot) 包含選票發出之投票裝置代碼 (Did) 、投票選擇 (Candidate, C) 與選票雜湊 (Ballot Hash)。

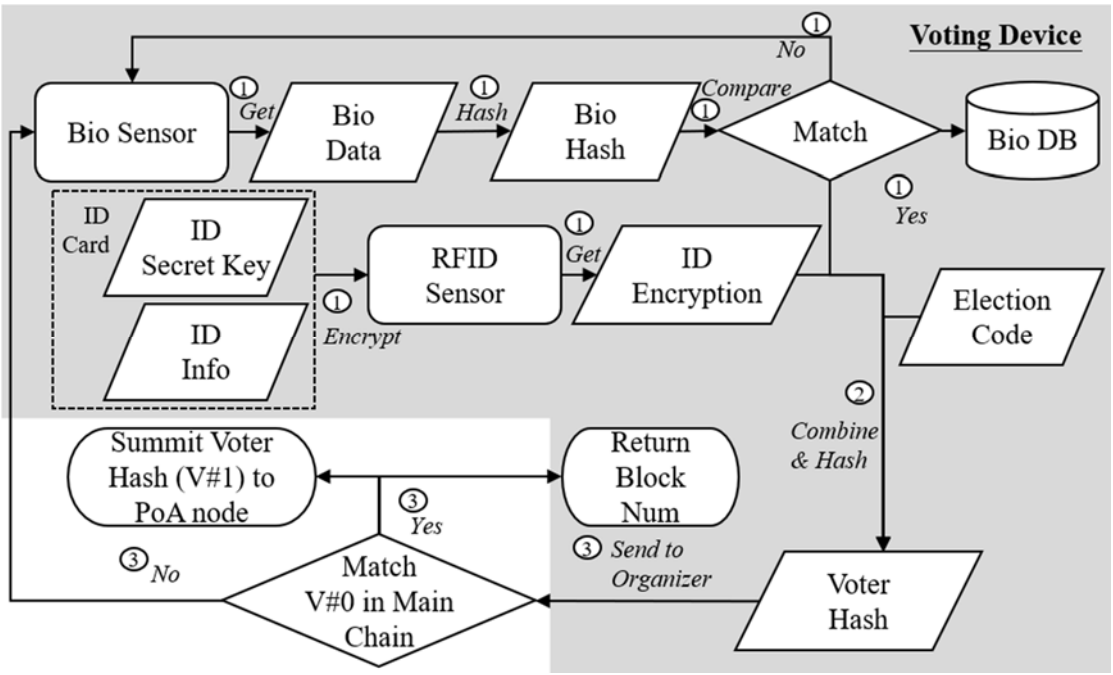

圖 9：選民驗證流程

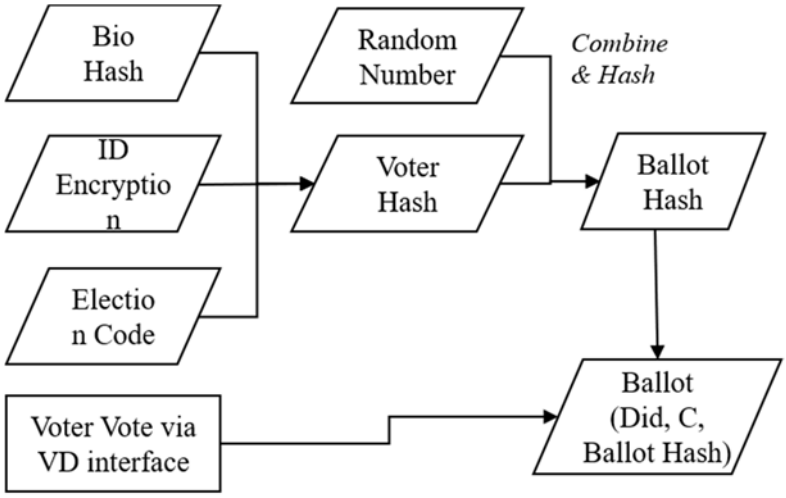

圖 10：選票產生流程圖

(三) 選票挖礦與加密 (Stage 3: Ballot Mining & Encryption)

此階段流程如圖 11，對應主架構 (圖 6) 中的 Stage 3，投票裝置將上一階段之選票加上 nonce 值，並依此進行挖礦，直到選票與 nonce 值之雜湊小於目標的數值 (Target) 為止。之後，投票裝置會將選票 (Ballot) 中的投票選擇 (C) 使用主辦方的公鑰進行加密，產生加密投票選擇 (C')，以確保投票過程中投票選擇 (C) 不會在開票前公布進而影響選舉。投票裝置再將選票 (Ballot) 經投票裝置之私鑰簽章，以確保此選票是由投票裝置所發出。投票裝置簽章後，其私鑰為投票裝置保管，公鑰則事先公開。最後選票雜湊附上投票裝置之代碼 (Did) 以及驗證紀錄區塊號碼 (V#1 Block No.)，再傳送給區塊鏈的節點驗證。

透過此挖礦的程序確保投票裝置不會大量且快速的產生選票，避免攻擊者利用投票裝置惡意大量產生選票。另外，本研究設計之工作量證明作用於此階段亦即 Nonce 值是由投票裝置所計算，此設計可以減少 PoA Node 計算工作量證明之負擔。因為投票裝置之數量與運算總能力應遠大於 PoA Node 之數量與運算總能力，因此本研究將工作量證明設置於投票裝置上而非 PoA Node 上，將工作量證明傳遞至 PoA Node 經驗證後再上鏈。

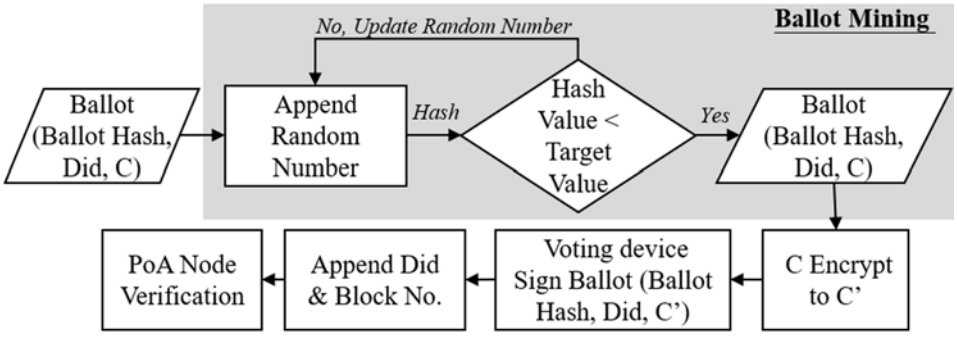

圖 11：選票挖礦與傳輸流程

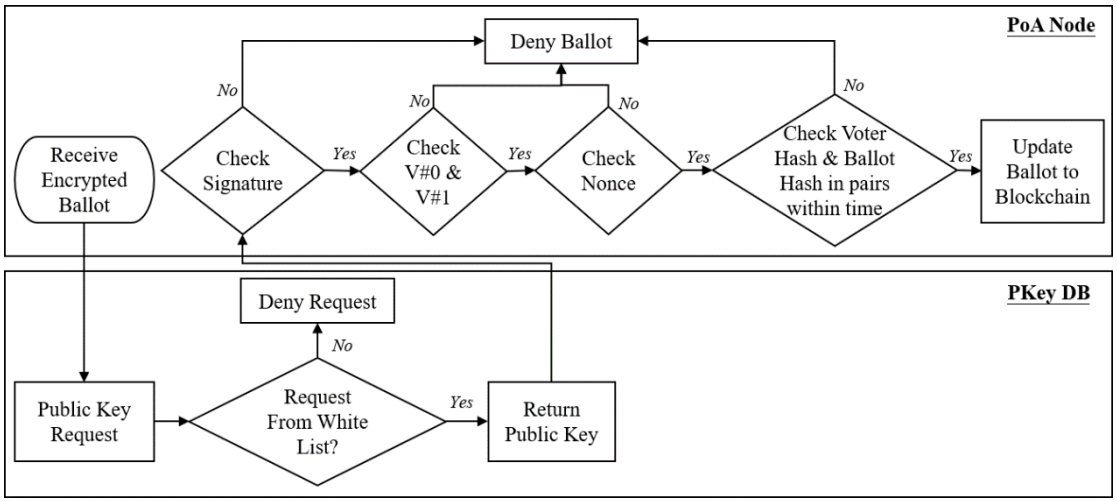

圖 12：選票解密與驗證流程圖

(四) 選票解鎖與驗證 (Stage 4: Ballot Decryption & Verify)

如圖 12，此階段對應主架構 (圖 6) 中步驟中的 Stage 4。

(1) 投票裝置將選票簽章後送出後，簽章的選票會放入 PoA Node 共用的交易池 (TX pool) 之中，各個驗證節點會從交易池中抽取交易。簽章的選票會交由 PoA Node 驗證，驗證之後把選票更新至鏈上。

(2) PoA Node 驗證選票會先向 Pkey DB 請求對應投票裝置公鑰進行簽章驗證，Pkey DB 會確認請求來自於白名單，並回傳對應投票裝置之公鑰。PoA Node 若無法使用對應投票裝置的公鑰解鎖即會否決選票。

(3) 使用收到的 V#1 區塊號碼 (Block. No)，再確定鏈上存在驗證紀錄 (V#1) 與註冊紀錄 (V#0) 且順序正確。

(4) 透過確認 Ballot 裡的 Nonce 值雜湊運算後符合目標值 (Target) 來確定投票裝置符合工作量證明，PoA Node 不需額外進行工作量證明。

(5) PoA Node 需額外進行選民與選票的驗證，由圖 12 可知，解密後之選票包含 Ballot Hash 之資料以及選民資料所處的區塊 (V#1)，但 PoA Node 無法確保該 Ballot 是該 Voter Hash 所產生，因此本研究要求 PoA Node 以挖礦的方式確認 Voter Hash 與 Ballot Hash 於圖 10 中是否為一對，也就是說是否有一 random number 可以符合該 Voter Hash 與 Ballot Hash 的生成方式。由於該 random number 有值域的限制，因此 PoA Node 能在有限的時間之挖到該 random number。若 PoA Node 無法在有限時間內找到該 random number 則該選票將會被 deny (見第四章之投票時間分析)。

(五) 選票結果統計與追溯 (Stage 5)

此階段 (圖 13) 為開票階段，主辦方透過檢驗選票上的數位簽章，確保其選票的真確性且已被節點驗證，再利用主辦方之私鑰解開加密之投票選擇 (C') 來公布統計投票的結果。另外，為了提升安全性，除公私鑰加密與雜湊值驗算的設計之外，為確保每張選票都有被計算到且沒有被添加虛假選票，本研究透過比對多項數據來保證選票數量的真確性。下列數據可以交互驗證確認投票的人數、選票數量，各項數據分別為：

(1) 投票裝置成功查詢 (V#1) 的紀錄次數

(2) 驗證節點 (PoA Node) 收到來自認可之投票裝置的選票總數

(3) Main Chain 上對應之投票裝置 (Did) 的選票 Ballot 數量

(4) 投票裝置計算之實體使用人數

若最後於投票流程結束後，統計上述四數據之值皆相同，便可證明以下四點：

(1) 每個投票的選民都有通過選民驗證 (V#0 V#1 皆存在)

(2) 每張選票都來自於認可的投票裝置

(3) 投票裝置與驗證節點之間沒有被加入虛假的選票

(4) 驗證節點沒有在上鏈過程加入虛假的選票

主辦方在開票後交叉對比這四項資料，並依此作為選票數量正確的依據。因為若有任一個參與方被攻陷或是試圖以灌水的方式來更動選票都會造成選票數量的不正確。此外，由於選票的產生中會有隨機數混入後才進行雜湊運算，同樣的選民可能會產生不同的選票。因此，會將確保每張選票 (Ballot) 都只有唯一的

驗證紀錄 (V#1) 與唯一的註冊紀錄 (V#0)，以此方式來確認沒有重複計算選票。

最後本研究提出選票追溯方法，使選民可以追溯自身選票。選民若對選票的真確性有疑慮，可以透過選民 ID 卡產生的加密身分證資料 (ID Encryption)、生物特徵資訊與選舉辨識碼來重新組合並得到選民雜湊 (Voter Hash)，並再以工作量證明的方式搜索選票的隨機值，將選票雜湊 (Ballot Hash) 找出並再次確認選票資訊。因本程序包含工作量證明搜索，在已知生物特徵辨識資訊、身分證資料和選舉辨識碼配對之情況，個人進行選票追溯需耗費一定的運算能力與時間，但由於攻擊者無法知曉這些選民資訊的配對，因此無法知道特定選民的投票結果。

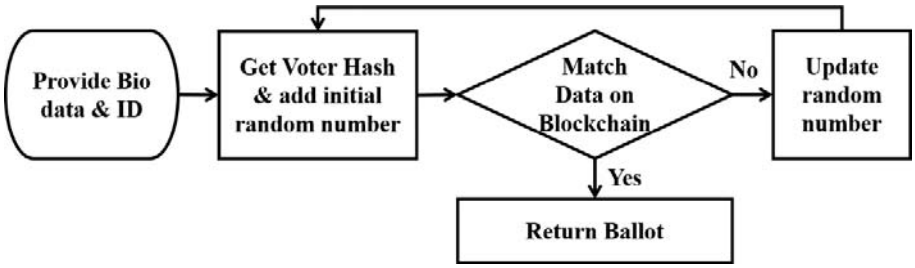

圖 13：選票追溯流程圖

肆、架構評估與安全性分析

一、投票時間分析

本研究是採用 PoA 作為共識機制的原因在於處理交易量的速度。不過由於選票中的工作量證明是由分散在各個投票裝置中的計算力來執行，架構中有設置驗證環節來確保資料的正確性。因此各角色需要彼此配合才能使整體投票與開票需要的時間可控制內，主辦方可以透過調整工作量證明的難度與隨機範圍來控制挖礦的時間，影響投票與開票時間的參數有下列幾項，如表 3：

表 3：投票參與角色對投票時間影響參數

選民	投票裝置	驗證節點
● 選民人數 (總選票數量) ● 裝置操作時間	● 投票裝置數量 ● 投票裝置挖礦時間 ● 選民驗證時間 ● 裝置計算能力 ● 工作量證明難度	● 選票驗證時間 (隨機值難度) ● 節點數量 ● 節點計算能力

選票需要經過投票裝置進行挖礦之後才會發送到驗證節點，來自各個裝置所產出的選票需要匯流至交易池 (TX pool) 中。PoA Node 將選票驗證完，並更新至 Main Chain 上的速度必須大於各投票裝置發出的量，才不會造成交易堵塞，影響開票時間。而投票裝置進行的挖礦難度可以透過設定雜湊目標值，配合裝置之硬體算力來推斷挖礦時間。在同一時間內，各個投票裝置的挖礦是同步進行的，因此產生一張選票之時間為：

$$\frac{選民人數 \times (裝置操作時間 + 選民驗證時間 + \frac{工作量證明難度}{裝置計算能力})}{投票裝置數量}$$

驗證節點驗證選票的時間是由隨機值的值域來控制，選民驗證 (V#1) 需要由選民雜湊 (Voter Hash) 挖礦產生。因此，在有選民雜湊之狀態下限定隨機數之值域即可限制驗證節點需的驗證時間。隨機數之設計用意在於控制驗證的時間，此時間可用於判定選民雜湊的真確性，隨機數的範圍等於驗證節點算力與控制時間之乘積。驗證節點會否決無法在時間之內驗證之選票，達到選票驗證之效果。

$$選票隨機值上限 = 控制時間(s) \times 節點計算能力(Hash/s)$$

投票裝置產出選票與驗證節點驗證之選票數量相等時，投票所需時間如下：

$$\frac{選民數量 \times \left(裝置操作時間 + 選民驗證時間 + \frac{工作量證明難度}{裝置計算能力}\right)}{投票裝置數量} + 選民數量 \times \left(\frac{工作量證明難度}{節點計算能力 \times 節點數量}\right) = 總投票時間$$

當主辦方確認投票時間與選民數量後，可依照計算裝置的算力推算並調整選票工作量證明之難度、隨機數範圍以及投票裝置之數量，避免出現開票延遲。

二、生物辨識方式採用考量

生物辨識有數種技術，目前指紋、面部辨識以及指靜脈辨識皆是相對成熟的技術。生物辨識作為選民驗證的基礎，是利用人體生物特徵的獨特性和與難以變動性 (長時間內不會出現重大改變)，選擇生物辨識的主要考量，如表 4 為：

- 辨識成功率 (準確率)
- 生物特徵之擷取資料特性 (資料大小)
- 感測器與其硬體成本 (建置成本)
- 生物特徵隨時間之變化性 (穩定度)
- 生物特徵擷取之難易度 (安全性)

表 4：生物辨識技術綜合比較

生物辨識	標的	準確率	資料大小	建置成本	穩定度	安全性
聲紋	聲波音色	低	小	中	低	低
指紋	指紋特徵	高	小	低	低	低
指靜脈	靜脈紋路	高	中	中	高	高
面部	面部特徵點	中	高	中	中	低
虹膜	虹膜紋路	高	小	高	高	中
掌紋	手掌紋路	高	小	中	中	中
視網膜	血管紋路	高	小	高	低	高

(資料來源：Saini & Rana 2014; Jain, Hong & Pankanti 2000)

本研究採用較為普遍且已被民眾接受之生物辨識方法：指紋及面部辨識。此兩種生物辨識方式有較高的準確性及建置成本較低，例如，機場自動通關採用此兩種辨識技術已多年，金融單位、行動支付也採用此方法來保護金融安全，政府、

民間單位與民眾皆已熟悉此兩種辨識流程，並了解其安全性及準確性（姚介修 2017）。相較於現況之選務人員人工確認選民身份，指紋及面部辨識可以十秒內快速且準確的分辨選民身份，降低選民時間成本及人為確認疏失機率。

三、投票參與方分權架構

本研究將對投票各個流程與行動都賦予對應的權力，以避免單一機構企圖濫權或是受到攻擊者的控制。本架構中在許多環節中都有去中心化的設計，類似於權責分立的概念。在 2015 年新南威爾斯州已採用類似的方式將不同的選票處理單位分開，減少舞弊風險 (Brightwell et al. 2015)。在選票產生的部分，選票的產生需要選民的生物特徵資訊與身分資料，投票裝置無法自行產生認證之選票，想要產生選票需選民本人才可以產出正確的組合。V# 0 與 V# 1 的資料則是由主辦方及投票裝置負責產生，能把資料上傳至鏈上的只有 PoA Node。而 PoA Node 的方式可以避免單一節點濫權或是被惡意控制，即便攻擊者控制驗證節點也沒有辦法產生任何具認證的選票。

表 5：本研究各角色對應之權限

	區塊鏈權限	計算(挖礦)能力	Bio DB	PKey DB	選票生成	選民身份證與生物特徵資訊	V# 0 V#1 生成
選民	X	X	X	X	X	O	X
投票裝置	X	O	讀	X	O	O	O
Org	讀	X	寫	寫	X	X	O
PoA Node	讀寫	O	X	讀	X	X	X

表 5 表示各個角色之權。在此分權的架構下，沒有單一機構或是角色可以對投票結果產生影響。後續的攻擊情境分析中會依序探討各個參與方被攻擊且控制之可能情況。

四、安全性分析

(一) 攻擊假想一：投票裝置 (Voting Device) 受到控制

若攻擊者想擾亂投票，可透過控制投票裝置而使之進行虛假投票。由於投票裝置具有產出選票的能力 (其簽章具有效力)，攻擊者可以透過投票裝置發出大量的虛假選票。此類虛假選票的生成有兩個困難點：

第一，攻擊者首先會遇到的問題是每張選票都需要附上工作量證明 (Nonce)，因此提案中使用的選票挖礦可以解決選票濫發的問題。基於裝置計算力是固定的，每個裝置在投票期間能產生的選票有限 (如下算式)，主辦方可以推算出每個裝置產出之極限票數，倘若有攻擊者將挖礦行為的資訊外包給外部的計算能力，濫發選票會使遭攻擊之投票裝置被偵測。

$$裝置最大產生票數 = \frac{裝置計算能力(Hash/s) \times 投票總時間(s)}{工作量證明難度(Hash\ Try)}$$

第二，攻擊者透過投票裝置所生成的虛假選票會被否決，因為投票裝置產生

之虛假的選民雜湊既沒有註冊紀錄 (V#0)，也沒有驗證紀錄 (V#1)，因此會被否決掉，且沒有正確區塊編號 (Block. No) 中的選民雜湊，驗證節點進行驗證時也會超過驗證的限制時間而被淘汰。

(二) 攻擊假想二：PoA 節點受到控制

PoA Node 被控制的情況之下，攻擊者擁有存取與寫入區塊鏈的權限。攻擊者若想要加入虛假的選票來影響選票結果，由於 V#0 記錄在鏈上，因此虛假的選票無法匹配 V#0 且數量不相符，所以被控制之 PoA 不可能發出虛假選票。

此外，對攻擊者而言最理想之攻擊情境是在投票開始之前就已經攻破 PoA Node，並在選民註冊階段加入虛假的 V#0。並在投票開始後，使用預先儲存的虛假選民雜湊來製作 V# 1 與可以符合上述驗證之選票。即使如此，攻擊者仍然需要面對數個困難，首先創建 V#0 與 V#1 的權限是由主辦方及投票裝置所擁有，偽裝 V# 0 與 V#1 的紀錄需要取得主辦方及投票裝置的私鑰。總結來說，即使擁有區塊鏈的存取與寫入能力，攻擊者也必須要竊取主辦方及投票裝置的私鑰，並在投票開始之前，才有辦法在投票結果之中加入虛假的選票。

再者，如果攻擊者採用分散式阻斷服務攻擊 (DDoS)，妨礙 PoA 節點驗證選票，使至於選票無法上鏈，則攻擊者必須攻擊足夠多的驗證節點才有辦法癱瘓投票，只要還有沒有被攻陷的節點存在，交易池中的選票終究會被更新到鏈上。

(三) 攻擊假想三：主辦方受到控制

PoA Node 被控制的情況之下，攻擊者擁有存取與寫入區塊鏈的權限。攻擊者若想要加入虛假的選票來影響選票結果，由於 V#0 記錄在鏈上，因此虛假的選票無法匹配 V#0 且數量會不相符，所以被控制之 PoA 節點不可能發出虛假選票數量。

(四) 攻擊假想四：針對選民真確性與隱私之攻擊

根據區塊鏈的原始設計，上鏈之資料是可以供大眾以及節點驗證。但因為投票資料是有絕對的隱私需要，因此在本研究的設計中共有三項隱私資料，經過適當的設計使得投票人的身份證資料（ID Info）、生物特徵資訊（Bio data）及投票選擇（Candidate，C）不可經任何運算或關聯反推。選民註冊流程（圖 8）中，身份證資料以對稱式加密的方式表示（可使用 ID 卡上之密鑰或其變形，例如使用 Salted Key），僅有持 ID 卡之選民才能產生該資訊並且任何其他人無法回推其 ID info。因此即使持有身份證資料（ID）與生物特徵資訊（Bio Data）者亦無法透過暴力破解找出對應該投票選擇的選民。再者，若攻擊者擁有 Bio Hash、Election Code 與 Voter Hash 的公開資料，在圖 8 的設計上也只能回推至 ID Encryption，且根據雜湊設計之原理需要非常大量的暴力運算才能得到一組有效的 ID Encryption 值與 Voter Hash、Bio Hash 相對應。即使可以使用暴力破解法得到有效的 ID Encryption 值，該值仍由選民的密鑰（或 Salted Key）保護，因此無法回推 ID info。因此鏈上資料是無法回推投票選擇與選民身份之間的關係。

由於 Voter Hash 的設計已經避免個人資料遭受破解，因此本文大部分皆採用簽章的方式來確保發出紀錄或選票的真確性。反之，若使用加密的方式將使流

程顯得繁瑣且也失去本研究採用區塊鏈分散式資料庫公開透明的特性。

攻擊者若想要針對選民的隱私進行攻擊，唯一的方法就是進行加密演算法的暴力破解 (Brute Force) 進行運算後，在與鏈上之資料一一進行對比。本研究是將身分證資料進行以選民的對稱式密鑰加密，對稱式的密鑰使用可視 ID 卡之能力設計，該密鑰只能由選民擁有，不分享給其他任何人，如愛沙尼亞採用的 EsEID 卡中具有 1024 位元的金鑰 (Edgar & Manz 2017)，可使用此金鑰當作一次性的對稱式加密密鑰，供選民此次投票使用加密 ID 卡的身份資料生成 ID Encryption。根據美國國家標準局之建議 (NIST 800-57 2020)，在 2030 年之前可使用 256 位元之密鑰長度則足以保護長時間的加密資料。據計算，若高速計算器可每秒檢驗 2^{32} 個密鑰，則需 2^{224} 秒完成暴力破解 (約 2^{199} 年)，攻擊者將難以使用大量運算得到選民的選票結果。

(五) 選民未完成投票流程

選民有未按照流程之設計中途離開之可能。本研究設計選民需要在選擇候選人的同時進行 Voter Hash 的生物辨識驗證及身份驗證以確保為本人投出最後之投票選擇 (C)。若是選民未完成投票流程將不會產生 Voter Hash、Ballot Hash 及 Ballot。因此若是選民中途離開投票裝置 (例如，拔除 ID 卡、離開投票區域導致無法進行臉部或指紋偵測)，其他人也無法再產生出選民之 Voter Hash 進而代為選民進行投票。

(六) 軟硬體設計之安全

本研究認為需隱私保護之軟硬體設計與實作需經公正第三方驗證及保證，例如美國投票機需透過 U.S. Election Admission Commission 的 Voluntary Voting System Guidelines (VVSG) 驗證 (U.S. Election Admission Commission 2021)。並且本研究認為已經公正驗證之軟硬體應於執行時期受到監控與保護，而 Root of Trust (可由信賴平台模組 Trusted Platform Module 實作, ISO/IEC 11889-1:2015) 概念可以有效的於執行時期保護設備的安全，確保設備的運作依照原先設計的運行 (ISO/IEC 11889-1:2015 2015)。因此在 Root of Trust 以及第三方驗證的手續之下我們可以確保所有的軟硬體不會進行非預期或惡意的動作，由此可以限制政府或主辦方的作為並確保民主制度的運行。

伍、結論

本研究發現網路投票設計所面臨的難題：選民真確性與匿名性的兩難、主辦方權力集中帶來的高風險。針對前兩個問題，本研究透過 Voter Hash 與 Ballot 的設計，使得選民的身分與驗證不因區塊鏈的公開與透明特色而導致選民隱私暴露。此外，投票機制避免使用選民自身的金鑰簽署選票，而是透過 V#0 和 V#1 紀錄來確認合法性，此種投票機制即便收到選票的主辦方也無法得知選民的身分。相比於網路投票實例，可以大幅度的保障選民的隱私，本研究利用加解密、雜湊演算法及區塊鏈架構設計，解決了選票匿名性與真確性的兩難問題。亦即本研究可以將選票放置於公開的分散式區塊鏈中供所有人審視，且經區塊鏈節點認證之上

鏈資料即無法修改，而不需揭露其選民、選票的隱私資訊，但選民本人可以選後進行認證確認該選票是否真確且上鏈。另外，是解決主辦方權力過於集中帶來的攻擊風險，在本研究設計之下，即使有主辦方遭到完全控制也難以危害到整體投票資料的安全。如果花費大量成本來影響結果，不只將耗費大量攻擊者運算資源，且其攻擊行動也會被發現。

最後，過往研究之文獻大多都專注於「投票」流程的設計，但本研究之架構設計包含較完整的註冊、身分驗證、投票、開票與選票追溯的區塊鏈流程，專注於整體流程與資料的正確性。此區塊鏈投票架構包含以下特色：電子化(成本低、計票速度快與投票準確度高)、匿名性、真確性(確保選民與選票之資訊為真)、可追蹤性(選民可追溯自身選票)、具備抵禦攻擊的能力。本論文針對各流程中可能的安全疑慮進行討論與分析，確保適當的安全機制可維護選民隱私與投票公正性。

誌謝

本文由陳呈祐協助完成此篇著作之研究工作與編寫，謹此致謝。

參考文獻

李欣芳 (2018)，大選綁 10 公投總花費約 47 億，自由時報，https://news.ltn.com.tw/news/politics/paper/1245513。

林銘翰 (2019)，中選會辦理投票模擬演練，ETtoday，https://www.ettoday.net/news/20190921/1540340.htm。

姚介修 (2017)，機場自動通關 使用人次突破 5 千萬，自由時報，https://news.ltn.com.tw/news/life/breakingnews/2143550 (存取日期 2021/9/4)

張如嫻 (2020)，密西根州計票系統出錯 川普 6000 票誤算給拜登，Newtalk，https://newtalk.tw/news/view/2020-11-07/490778。

黃彥鈞 (2019)，愛沙尼亞線上投票比率創紀錄，科技新報，https://technews.tw/2019/03/12/nearly-half-of-voters-using-online-voting-in-estonia/。

Agrawal, M. & Mishra, P. (2012), A comparative survey on symmetric key encryption techniques, *International Journal on Computer Science and Engineering*, 4(5), 877-882.

Australian Electoral Commission (2019), Cost of elections and referendums, https://www.aec.gov.au/elections/federal_elections/cost-of-elections.htm.

Ayed, A. B. (2017), A conceptual secure blockchain-based electronic voting system, *International Journal of Network Security & Its Applications*, 9(3), 1-9.

Back, A. (1997), Hash cash postage implementation, http://www.hashcash.org.

Brightwell, I., Cucurull, J., Galindo, D. & Guasch, S. (2015), An overview of the iVote 2015 voting system. New South Wales Electoral Commission, Australia, Scytl Secure Electronic Voting, Spain, 1-25.

Buteri, V. (2017). BeyondBlock Taipei 2017. https://www.youtube.com/watch?v=9RtSod8EXn4.

Cho, M. H. (2018), South Korea to develop blockchain voting system, ZDNet, https://www.zdnet.com/article/south-korea-to-develop-blockchain-voting-system.

Danchev, D. (2010), Study finds the average price for renting a botnet, ZDNet, https://www.zdnet.com/article/study-finds-the-average-price-for-renting-a-botnet.

Diffie, W. & Hellman, M. (1976), New directions in cryptography, *IEEE transactions on Information Theory*, 22(6), 644-654.

Edgar, T. W. & Manz, D. O. (2017), Research methods for cyber security, *Syngress*.

Estonia (2020), 'i-Voting e-Estonia', https://e-estonia.com/solutions/e-governance/i-voting.

Feistel, H. (1973), Cryptography and computer privacy. *Scientific american*, 228(5), 15-23.

Gilbert, H. & Handschuh, H. (2003), Security analysis of SHA-256 and sisters, *International workshop on selected areas in cryptography*, Springer, Berlin, Heidelberg, 175-193.

Giles, C. & Horton, J. (2020), US election 2020: Is Trump right about Dominion machines?, BBC Reality Check, https://www.bbc.com/news/election-us-2020-54959962.

Gomez, M. (2017), Ethereum Co-Founder Vitalik Buterin Weighs in on Blockchain Improvement & Scaling Issues, *Cryptovest*, https://cryptovest.com/news/ethereum-cofounder-vitalik-buterin-weighs-in-on-blockchain-improvement--scaling-issues/.

Hanifatunnisa, R. & Rahardjo, B. (2017), Blockchain based e-voting recording system design, *11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, Bali, Indonesia, October 26-27, 1-6.

Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M. & Hjálmtýsson, G. (2018), Blockchain-based e-voting system, *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA, July 2-7, 983-986.

ISO/IEC 11889-1:2015 (2015), Information technology - Trusted platform module library - Part 1: Architecture, https://www.iso.org/standard/66510.html.

Jain, A., Hong, L. & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, 43(2), 90-98.

Khan, M. A. & Salah, K. (2018), IoT security: Review, blockchain solutions, and open challenges, *Future generation computer systems*, 82, 395-411.

Kravitz, D. W. (1991), Digital signature algorithm, *US Patent No. 5231668A*.

Liu, Y. & Wang, Q. (2017), An E-voting Protocol Based on Blockchain, *IACR Cryptol. ePrint Arch.*, 1043.

Nakamoto, S. (2008), Bitcoin: A peer-to-peer electronic cash system, *Decentralized Business Review*, 1-9.

NIST 800-57 (2020), Recommendation for Key Management, https://doi.org/10.6028/NIST.SP.800-57pt1r5.

Pornin, T. (2013), Deterministic usage of the digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA), *Internet Engineering Task Force RFC*, 6979, 1-79.

PwC Australia. (2014), Plebiscite could cost Australian economy $525 million, https://www.pwc.com.au/press-room/2016/cost-plebiscite-mar16.html.

Saini, R. & Rana, N. (2014). Comparison of various biometric methods, International Journal of Advances in Science and Technology, 2(1), 24-30.

Segaard, S. B., Christensen, D. A., Folkestad, B. & Saglie, J. (2014). Internettvalg: hva gjør og mener velgerne, Institutt for samfunnsforskning, Oslo, Norway

Shams, S. (2019), Indonesia: More than 270 election staff died from overwork https://www.dw.com/en/indonesia-more-than-270-election-staff-died-from-overwork/a-48517308.

Specter, M. A., Koppel, J. & Weitzner, D. (2020), The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in us federal elections, *USENIX Security Symposium*, 1535-1553.

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. & Halderman, J. A. (2014), Security analysis of the Estonian internet voting system, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,* Arizona, USA, November 3-7, 703-715.

U.S. Election Admission Commission (2021), Voluntary Voting System Guidelines VVSG, https://www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf

Wei, C. C. Z. & Wen, C. C. (2018), Blockchain-based electronic voting protocol, *JOIV: International Journal on Informatics Visualization*, 2(4-2), 336-341.