電子投票安全嗎？

法務部調查局資通安全處

雷喻翔

資料來源：本文轉載自法務部清流雙月刊 109 年 1 月號

電子投票系統簡介

傳統投票方式所需耗費的人、物力資源，隨著選舉規模不斷擴大而逐漸攀升，為了減低資源浪費，電子投票（e-voting）在過去的十幾年受到了電腦科學家廣泛地研究，許多可行的機制也被提出討論。好的電子投票系統必須滿足以下幾點特性：

一、 全體驗證能力：所有參與投票的角色，諸如投票人或監票人等，可以驗證整個投票的過程以及最終結果。

二、 個人驗證能力：每位投票者可以確認他的選票是否已經投出、是否已經成功地被紀錄以及是否被算進最終的計票結果。

三、 可靠性：投票的過程是否可以有效偵測惡意投票行為。

四、 一致性：無論是由誰來觀看投票流程，都會得到相同的選舉結果。

五、 匿名性：只有投票者本人知道他自己選票的內容，也就是要達到無記名投票的目的。

六、 透明度：為了確保公平及有效原則，整個投票過程必須是公諸於大眾。為了達成上述的條件，從而設計出有效的 e-voting，專家學者們採用了兩項有用的工具：密碼學中的盲簽章（Blind Signature）以及區塊鏈技術。

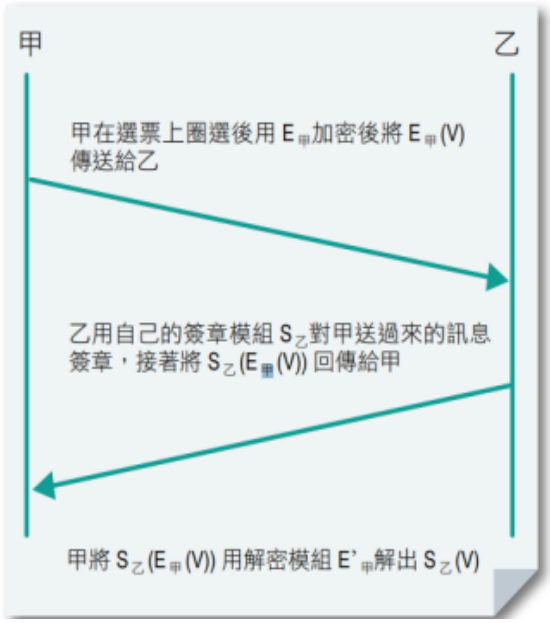
盲簽章

個人可驗證性、可靠性及匿名性可以視為投票者對於是否達成秘密投票程度的指標，盲簽章這項技術的優點可符合以上三項特性。在

講盲簽章的流程前先了解何謂數位簽章：

電子世界中要如何證明某一個文件的內容沒有被竄改過呢？這時候便可以用數位簽章來確保此事，首先將文件內容透過 MD5（一種雜湊函數）計算後得到一組值，接著同時傳送文件內容以及計算後的值，這時候任何人都可以針對該文件藉由 MD5 的演算法算出另一組值，當這兩組值的內容相等時，我們便可以放心地說所收到的文件內容與原始的內容是相同的。

這種可受驗證的數位簽章確實可以保證傳遞的內容不會經過修改，但是若放到 e-voting 中，那將會違反無記名投票原則，因為如果必須一併送出原始內容方可驗證，那麼自己的投票意向不就暴露於第三人了嗎？因此盲簽章的精神便是：驗證方不需要對原始內容簽章，驗證方所簽章的內容可以是傳送方加密過的內容，只要這個加密的內容使用者可以復原即可。



我們用以下一個簡單的例子來描述盲簽章的過程：甲是一位擁有投票權的合格選民，乙是選委會，甲如何獲得具有選委會簽章的合格選票呢？甲有自己的加密模組 E 甲及解密模組 E'甲，還有一張選票 V，乙則有 S 乙簽章模組。流程如下所示（參考左圖）：

一、 甲先用自己的加密模組將已經有圈選結果的選票加密，接著將加密結果傳給乙。

二、 乙收到甲傳來的訊息，由於乙無從得知甲的解密模組，因此無須擔心乙會知道甲秘密投票的內容。乙用自己的簽章模組對甲送過來的訊息進行簽章，然後便將這個資訊再回傳給甲。

三、 甲在得到了乙所傳遞過來的訊息後，用解密模組 E’甲解出 S 乙 (V)，這便是乙對於甲的投票內容所做的簽章。

根據上述的步驟，甲在無須揭露自己投票內容的前提之下順利地獲取了乙方對於甲方投票內容的簽章。個人可驗證性、可靠性及匿名性在這個簡單流程中都得以確保。

區塊鏈

相較於盲簽章較著重在於「秘密投票」這個目的，區塊鏈則是著重於 e-voting 在「公眾使用」上的透明度。區塊鏈是一項源自於比特幣的技術，它是一種資料結構的概念，區塊鏈中的所有資料都是以區塊（block）的方式呈現，區塊和區塊間彼此連結成串，我們可以抽象地將之想像成為鏈狀結構，這也是區塊鏈之所以會如此命名的原因。

要在區塊鏈上建立一個新的區塊節點，必須遵守區塊鏈對等（Peer-to-Peer, P2P）網路上的相關規則，任何違反建立規則的區塊將不被區塊鏈所接受。為了達到去中心化及達到共享性的目標，每一個區塊鏈上的資料都是分散地儲存在雲端上，任何人都可以存取。經由使用區塊鏈，所有的資料傳送不再是單純的點對點擁有資料，而是將資料傳至公開的 P2P 對等網路上，一切的資訊都可透明接受檢驗。

接續上個章節，投票人取得選委會簽章，投票內容也獲得選委會的確認；接下來的實際投票動作，投票人用另一組非對稱金鑰，將本身的選票以及從選委會獲得的簽章一併傳送至區塊鏈網路，由於這一組非對稱金鑰僅個人知道，因此這一動作可以實踐秘密投票的要求；最後一個步驟是投票後整理階段，選委會從區塊鏈網路上驗證每一張選票是否符合選票格式、是否具有選委會發出的簽章、是否於投票截止日前投出及該張選票是否已經計算過。

由於區塊鏈的性質，整個過程可由所有參與人以及可存取區塊鏈的第三方共同進行計票以及稽核。

相關議題

在前述所介紹的盲簽章及區塊鏈技術，的確可以建立起一套可運作的基本電子投票系統，然而在實際的運作及更嚴謹的安全性上仍有一些議題需要考量。

第一是身分識別的問題，資料透過 P2P 區塊鏈網路來溝通傳遞，有了公開透明的好處，但是也帶來了暴露投票者 IP 的風險，進而透過網路封包分析，勾稽出投票者與投票結果的關聯。為了避免暴露 IP，經由洋蔥網路（TOR）隱藏個人的 IP 成為一種可能的解決方式；

第二點是資料的保密及中立性。P2P 區塊鏈網路雖公開透明，但反面來看是在投票的過程中，投票進度也揭露於公眾，這多少也會影響選舉的最終結果。一種最直接的解決方式是不採用誰都可存取的公眾 P2P 區塊鏈網路，而是採用具一定程度權限控管且須經過授權的區塊鏈網路。然而要提高保密程度，公開透明就會遭受到質疑，這也是系統設計過程中需要取捨之處。

隨著資訊科技的進步，電子投票技術時至今日已算略具雛形，然而投票本身無論是政治性的選舉或是公投，其結果都是社會大眾矚目的焦點，只要投票過程稍有爭議，主事者難免遭受非議，因此在尚未百分之百處理潛在性風險之前，應持續提升相關的技術研究。