區塊鏈存證應用於司法數位證據之芻議

陳宏志
淡江大學產業經濟學系 兼任教師
hongzhi.mcu@gmail.com

鄒宗萱
資策會科技法律研究所創意智財中心 副主任
thtsou@iii.org.tw

前言

區塊鏈科技興起後，不限於加密貨幣，因其去中心化、可追蹤追溯、不易竄改等特性，應用在存證上，有助於提升農產品或相關生產履歷之信心。除了有形商品之存證，隨著科技的進步，因在司法訴訟中，越來越多的數位數據需要與紙本證據不同之作法。透過區塊鏈存證應用，不僅可協助檢核紙本轉數位之真偽，處理信任之議題，更可考量將日常業務或重要資訊直接存證於鏈上，節省成本及提升效率等。為解決此一需求，本文除簡介區塊鏈存證基本流程、以及應用於司法數位證據時可能遭遇之議題，如證據法則，更以美國、中國大陸法規及案例出發，希冀說明區塊鏈存證應用於司法數位證據將成為未來的趨勢，及企業可能因應與建議。

一、區塊鏈存證之基本流程

要達成區塊鏈存證應用，除分散式帳本、點對點傳輸、共識決等共通基礎技術一定必備外，相關系統至少還要能提供身分識別、資料加密、智能合約、資料查詢跟驗證等功能，以確保資料不被竄改、可供多方溝通或運用，甚至未來供對接司法機關等用途。基此，區塊鏈存證基本流程示意如下：

Step 1 檔案雜湊處理→	Step 2 存證上鏈→	Step 3 事後查證（取證）
（身分識別 / 資料加密）	（智能合約）	（資料查詢跟驗證）

在相關流程進行中，資料加密涉及演算法（Hash 值），可協助解決與原件相符之需求；而身分識別、資料查詢及驗證則係透過智能合約及公私鑰管理等，協助解決軟硬體與管理環境（用以生成、存儲、傳輸…）之可靠性，因上鏈後即可發揮區塊鏈不易竄改、可追蹤追溯之特色。具體說明如後[1]：

（一）檔案雜湊處理

1. 陳宏志（2020），〈企業營運資安難保萬一　區塊鏈存證有備無患〉，《網管人雜誌》，第 172 期，http://www.netadmin.com.tw/netadmin/zh-tw/magazine/-Viewpoint/78582583FE1744DDAA6034FFD1010359（最後瀏覽日：2020 年 7 月 22 日）。

1. 若將原始檔案完整上傳至區塊鏈備份，不僅耗費作業時間，也會造成區塊鏈資料庫與區塊鏈節點擁有者的龐大負荷。因此，可先規劃將鏈上存證的文件進行雜湊處理，而常見雜湊演算法有MD 5、SHA 256 等。
2. 雜湊處理用意在於幫檔案生成一串獨有的雜湊值，雜湊值可作為檔案的指紋，若檔案內容更動，雜湊值也會更動，不僅能作為檔案正確性的證明，也大幅降低檔案存證的空間與時間成本。

（二）存證上鏈

1. 為了將存證所需資訊統整，並保存於區塊鏈之中，企業或組織會需設計一份存證用智能合約（Smart Contract，又稱智慧合約），智能合約中會儲存相關資訊，如：存證說明、檔案雜湊值及存證時間戳。
2. 透過智能合約將上述資料備齊後，連同資料呼叫存證上鏈API，系統後台會依照智能合約範本，將資料填入範本中，完成合約上鏈所需的基本設定，最後將合約原始資料（Raw Data）傳送回存證端的裝置上。
3. 每個裝置會存有一份僅此一把的私鑰，該私鑰可用來證明裝置或裝置使用者在區塊鏈上的身份。以此一私鑰做簽章並在區塊鏈上完成的交易，可利用該私鑰來證明交易者的身份。
4. 此一系統在接到合約原始資料後，裝置使用私鑰對合約原始資料做交易簽章，並透過交易上鏈API 將交易上傳至區塊鏈上，等待交易被寫入區塊鏈。
5. 前述交易完成後，持續監聽交易紀錄的後台將捕捉到存證交易完成的紀錄，該監聽模組會負責將交易紀錄寫入資料庫中，記錄下交易地址，至此即完成存證上鏈部分。

（三）事後查證

1. 若事後有查證需求，需要查驗檔案，即可至資料庫中查詢該檔案的存證交易地址，利用交易地址可存取該存證合約中的內容，並確認當初對存證合約簽章的私鑰是誰所有，是否符合權限。
2. 存證步驟可依序參考如後：（a）首先確認簽署存證合約之人的身份；（b）取出該合約中所儲存的檔案雜湊值、存證描述與存證時間戳；（c）使用以上資訊與被查驗檔案做比較，確認檔案雜湊值與修改時間是否符合以上資訊。
3. 被查驗的檔案是否遭受過竄改，即可利用存證合約來進行確認，藉此達成存證需求。

二、區塊鏈存證應用在司法數位證據之議題

除了透過區塊鏈應用協助存證，如欲推展至司法領域，需符合電子簽章法或相

關法令外，能否落實此一應用的關鍵在於司法機關的認可。以我國民事訴訟為例，因常是私權糾紛，法諺有云：「舉證之所在、敗訴之所在」，故證據是訴訟程序內非常重要的關鍵。如依民事訴訟法第 222 條第 1 項前段，法院為判決時，應斟酌全辯論意旨及調查證據之結果，依自由心證判斷事實之真偽。法官要形成心證，多以證據協助判斷事實真偽之關鍵。爰規劃以區塊鏈應用協助存證等，不僅需符合技術或規格需求，更先要符合司法實務對數位證據之相關見解。

在刑事訴訟領域，採用監視錄影器、錄音檔案等數位證據更是常見。以最高法院 107 年台上字第 3724 號刑事判決為例，判決書內提及：... 一般而言，數位證據具無限複製性、複製具無差異性、增刪修改具無痕跡性、製作人具不易確定性、內容非屬人類感官可直接理解（即須透過電腦設備呈現內容）。因有上開特性，數位證據之複製品與原件具真實性及同一性，有相同之效果，惟複製過程仍屬人為操作，且因複製之無差異性與無痕跡性，不能免於作偽、變造，原則上欲以之證明某待證事項，須提出原件供調查，或雖提出複製品，當事人不爭執或經與原件核對證明相符者，得作為證據。

然如原件滅失或提出困難，當事人對複製品之真實性有爭執時，非當然排除其證據能力。此時法院應審查證據取得之過程是否合法（即通過「證據使用禁止」之要求），及勘驗或鑑定複製品，苟未經過人為作偽、變造，該複製品即係原件內容之重現，並未摻雜任何人之作用，致影響內容所顯現之真實性，如經合法調查，自有證據能力。至於能否藉由該複製品，證明確有與其具備同一性之原件存在，並作為被告有無犯罪事實之判斷依據，則屬證據證明力之問題。

三、司法數位證據應符合訴訟之證據法則：中美案例分析

區塊鏈存證如欲運用於司法領域，關鍵在於應符合既有法令暨需求，如證據法則，再來才會討論技術實質內容，如時戳、簽章或憑證。因數位證據（泛指非紙本文件之內容）在存證之應用，其主要目的如同紙本文件希望透過公證取得一定之效力。除依我國司法實務之見解外，數位證據能否作為法院在訴訟案件內所採認之證據，及需要具備那些要件…（包含但不限於區塊鏈之應用），先以美國及中國大陸之實踐為例，說明如下：

（一）美國佛蒙特州

該州就區塊鏈科技應用作為法院程序（Title 12：Court Procedure）之證據訂有相關規範[2]。其在審判進行（Chapter 081：Conduct Of Trial）的規定內，認為區塊鏈之應用作為證據時，除有已宣誓之適格證人外，還需要有下列 4 要件，始能符合該州證據法則（Vermont Rule of Evidence 902）：

1. 存證時間（the date and time the record entered the blockchain），係指如於鏈上完成

2. 美國佛蒙特州法規查詢（The Vermont Statutes Online）https://legislature.vermont.gov/statutes/section/12/081/01913（最後瀏覽日：2020 年 7 月 22 日）。

交易之日期與時間。

2. 上鏈時間（the date and time the record was received from the blockchain），係指該交易紀錄達成共識後出塊之日期與時間。
3. 紀錄保存（the record was maintained in the blockchain as a regular conducted activity），係指該紀錄被保存在區塊鏈上，且因不斷出塊之設計，而具不易竄改、可追蹤追溯等特色。
4. 持續運作（the record was made by the regularly conducted activity as a regular practice），係指區塊鏈依原本設計之架構，持續於一定期間內達成共識並出塊的機制運作無礙。

而符合上開要件之證據，可用以推定以下事項：

1. 透過有效之區塊鏈應用，其驗證的事實或紀錄為真。
2. 透過區塊鏈應用建立事實或紀錄之日期和時間，即為該事實或紀錄上鏈之日期和時間。
3. 透過區塊鏈應用而取得紀錄者，即為本人。
4. 若法院或對照之當事人同意驗證區塊鏈紀錄之格式或方式等，則應以該特定格式或方式向法院證明符合本條規定之區塊鏈紀錄，且已獲得他方同意。

（二）中國大陸

中國大陸民間投入區塊鏈甚早，如ICO在2016至2017年間蔚為風潮，但也因此產生許多詐騙等不法情事。其主管機關意識到區塊鏈之重要性後，除2017年9月間由人民銀行等七單位聯名發布公告禁止不法ICO[3]外，也正視其影響力並透過官方的能量，投入區塊鏈應用等，如工信部於2018年5月發布「2018中國區塊鏈產業白皮書」[4]，內容除金融領域外，還包含徵信、大數據分析、資料市集、著作權存證等應用。

其中在司法領域部分，存證應用等也有初步成果，如民間在2019年4月發布「區塊鏈法規合規白皮書」[5]外，同年6月中國大陸最高人民法院資訊中心也發布「區塊鏈司法存證應用白皮書」[6]。因相關應用更涉及到電子證據相關，主要以最高人民法院於2019年10月14日公布修正之「最高人民法院關於民事訴訟證據的若干規定」為主，並自2020年5月

3. 陳宏志（2017），〈中國大陸、香港陸續發布對首次代幣發行（ICO）之相關規範〉，《科技法律透析》，29卷11期，頁9-10。
4. 中國大陸工業和信息化部（2018），《2018年中國區塊鏈產業白皮書》，http://www.miit.gov.cn/n1146290/n1146402/n1146445/c6180238/part/6180297.pdf（最後瀏覽日：2020年7月22日）。
5. 深圳壹帳通智能科技有限公司（2019），《區塊鏈法律合規白皮書》，https://www.ocft.com/pdf/01.pdf（最後瀏覽日：2020年7月22日）。
6. 中國信息通信研究院（2019），《區塊鏈司法存證應用白皮書》，http://www.caict.ac.cn/kxyj/qwfb/bps/201906/P020190614499397999292.pdf（最後瀏覽日：2020年7月22日）。

1 日起施行[7]，調整許多涉及電子證據之規範，如第 14 條例示電子證據的規定、第 15 及 23 條提出及保全電子證據原件之要求、第 93 條採認電子證據考量因素等。

更重要的是，杭州互聯網法院已於 2018 年做出號稱是第一個區塊鏈存證的相關判決[8]：2018 浙 0192 民初 81 號民事判決（案件編號 055078），案由為杭州華泰一媒文化傳媒有限公司訴深圳市道同科技發展有限公司侵害作品資訊網路傳播權糾紛。

本案最後判決為被告賠償原告人民幣 4,000 元定讞，就杭州互聯網法院裁判觀之，關鍵在於華泰公司（原告）將網頁截圖、源碼資訊轉成 Hash 值後，並上傳至 Factom 區塊鏈，有助於確保真實性。綜合觀之，中國大陸因電子證據在科技應用上並不一定限於區塊鏈，參照「最高人民法院關於民事訴訟證據的若干規定」之精神，只要能證明該證據之生成、存儲、傳輸等所依據的軟硬體完整、可靠，可供監測、核查，以及能完整地被保存、傳輸等（該規定第 93 條參照），都可協助判斷其真實性。

四、結語

觀察美國或中國大陸之司法實務後，兩國對於數位或電子證據之認定，無論是否運用區塊鏈科技，核心均在於如何證明與原件相符（真實性），以及軟硬體與管理環境（用以生成、存儲、傳輸…）之可靠性等。除符合訴訟法之證據法則外，從技術面觀之，存證應用需至少提供身分識別、資料加密、智能合約、資料查詢跟驗證之功能。

以中國大陸系爭案件運用之 Factom 區塊鏈[9]為例，該公司在 2014 年成立於美國德州，以去中心化方式結合開源軟體，運用區塊鏈提供企業記錄與管理文件或資訊，並開發相關應用程式，如存證及取證、數位身分識別、公證、代幣化、監測、法令遵循及分散式資料存儲等功能。以存證為例，該公司係透過對應身分之憑證（API key），結合權限設計，以證明時間及狀態。至於公證則是發揮區塊鏈特色，越多人使用就越不容易竄改。

另在我國，如區塊科技之存證王 APP 亦提供存證相關服務。該 APP 可就數位證據（如照片、影音檔案），加上檔案產生時的時間戳與產生地點 GPS 訊息，檔案生成 Hash 值後，上傳至區塊鏈（先上傳至私鏈 Chromaway，累積 1, 000 筆交易後再上傳至以太鏈備份）中進行存證[10]。

惟需要進一步探討的是，由於區塊鏈應用的本質為去中心化之設計，利用分散式

7. 中國大陸最高人民法院（2019），《最高人民法院關於民事訴訟證據的若干規定》，http://www.court.gov.cn/fabu-xiangqing-212721.html（最後瀏覽日：2020 年 7 月 22 日）。
8. 杭州互聯網法院訴訟平台，案件查詢，https://www.netcourt.gov.cn/#lassen/search（最後瀏覽日：2020 年 7 月 22 日）。
9. Fatcom 公司網站，https://www.factom.com/（最後瀏覽日：2020 年 7 月 22 日）。
10. 區塊鏈存證王，https://app.chainsecurity.asia/blockchainwitness/web/index.html（最後瀏覽日：2020 年 7 月 22 日）。

帳本等作為提供服務的基礎。倘信任該應用所生的結果，如存證，在符合前述美國或中國大陸之證據法則下，理應符合證據能力及證明力之需求，用何種技術反而不是重點，如是否使用 Factom 或其他區塊鏈進行存證。此外，數位證據若涉及電子文件，在我國還可能有電子簽章法相關議題，如該存證屬電子簽章或數位簽章，或是否需要憑證機構、憑證實務作業基準等。基此，要落實區塊鏈之存證應用，對應之法制也會需要調整。

綜上所述，企業或組織透過區塊鏈應用如存證來保護內部資料，在技術上並非難事，系統設計只要符合前述規格，應可初步符合需求。但實務上常遭遇企業資料或營業祕密外洩的風險，對造或合作對象等會要求提供資料來源證明。更重要的是，當發生糾紛的時候，法院也會要求證明資料之真實性。在未修法或導入科技應用之情形下，目前大多只能透過提供大量書面資料等作為佐證，但常被質疑證明是否為真，花費攻防雙方極大心力。如採逐案公證，成本亦極高。

為促進信任、降低成本或提升效率，透過區塊鏈技術不易竄改、安全等特性幫助廠商存證，或許是解決方式之一，惟關鍵是讓法院認可新科技的解決方案。未來除推動研擬如美國、中國大陸之法令，在我國可能是民事或刑事訴訟法、電子簽章法等，並可提修配套法規，規範數位證據之證據法則外，區塊鏈存證系統或功能之規劃，可依法規需求與區塊鏈技術特性，將企業內部日常業務之機密或必要資訊，定期且自動存證於鏈上。發生爭議或需要訴訟時，更可讓法院等直接採認，確實發揮科技應用的效益。