

# 區塊鏈運用於跨境警務合作之研究

蔡馥璟<sup>1</sup>、張躍瀚<sup>2</sup>

## 目次

|                 |                     |
|-----------------|---------------------|
| 壹、前言            | 二、數位證據之傳統與區塊鏈監管鏈之比較 |
| 貳、文獻探討          | 肆、區塊鏈與跨境警務合作之應用     |
| 一、數位證據監管鏈       | 一、區塊鏈種類介紹           |
| 二、區塊鏈演進、運作與應用趨勢 | 二、跨境警務合作導入區塊鏈科技之決策  |
| 參、數位證據監管區塊鏈     | 伍、結語                |
| 一、運作模型          |                     |

## 摘要

跨境警務合作是未來打擊犯罪的新趨勢。現代犯罪集團往往由跨境的組織所主導，藉由不同地區司法管轄的衝突，躲避執法機關的查緝。加上現今科技一日千里，數位設備與日常生活的連結日趨緊密，因此伴隨而來的，就是科技設備所產生的犯罪數位證據。該如何於跨境警務合作的框架下，維持其完整性及不可竄改性，並順利執行證物轉交作業，將是兩岸四地執法機關的重大挑戰。本研究針對區塊鏈技術應用於數位證據監管鏈的可行性進行探討，利用區塊鏈確保資料歷史性、完整性、一致性的特點，另可彈性設定使用者權限及角色的優勢，提出數位證據監管區塊鏈的架構。執法人員在接觸犯罪現場的第一時間，即可針對犯罪案件建立數位證據監管區塊鏈，有效保存及管理數位證據。另鑑於區塊鏈特性，可有效支援跨境協作的特點，本研究針對公有鏈、私有鏈及聯盟鏈運用於跨境警務合作的情境進行探討。研究成果可提供兩岸四地，建構跨境警務合作機制之參考。

**關鍵詞：**區塊鏈、數位證據監管鏈，跨境犯罪

<sup>1</sup> 蔡馥璟(Tsai, Fu-Ching): 中央警察大學刑事警察學系，助理教授。通訊地址：33304 桃園市龜山區大崗里樹人路 56 號。Email: fctsai@mail.cpu.edu.tw

<sup>2</sup> 張躍瀚(Zhang, Yue-Han): 內政部警政署刑事警察局，隊長。通訊地址：11072 臺北市信義區 忠孝東路四段 553 巷 5 號。Email: hans@email.cib.gov.tw

## Abstract

Cross-boundary police cooperation is a new trend for law enforcement agencies to fight against crimes in the future. Modern organized crimes are often dominated by illegal cross-border organizations in order to evade law enforcement agencies through conflicts of jurisdictions in different regions. With the rapid development of technology, digital devices are wildly used in daily life, so cross-border crimes are often accompanied by digital evidence, which is used to build the connections between criminal groups. Under the current framework of cross-border police cooperation, how to maintain the integrity and immutability of digital evidence and transfer it to the corresponding agencies is a major challenge. This research discusses the feasibility of applying blockchain technology to the chain of custody of digital evidence and using blockchain to maintain data history, integrity, and consistency. The proposed blockchain-oriented architecture can support flexible roles and permissions settings by smart contracts. With the advantages of blockchain, law enforcement officers can establish the chain of custody of digital evidence at the crime scene and effectively store, transfer and manage digital evidence to build trust and transparency between multiple agencies in different regions. In addition, this research focuses on the application of public chains, private chains and alliance chains in the context of cross-border police cooperation. The research results can provide a reference for the construction of cross-border police cooperation mechanisms among four districts of Cross-Straits.

**Keywords: Blockchain, Digital Chain of Custody, Cross Boundary Crime**

## 壹、緒言

隨著時代的演進，犯罪活動由以往的單一區域模式，轉換成不同地區緊密結合的產業鏈上下游關係。以目前最常見的詐騙集團犯罪模式為例，集團中主要金流及電信流集團，不僅成員不同，且分布於不同地區，所以執法機關在向上溯源的過程中，因不同犯罪地點的法律及文化認知相異，形成查緝斷點，也因此難以對跨境犯罪進行全方面的查緝。再加上目前資通訊產品的普及，犯罪者使用最新資通訊匯流技術，配合加密技術進行溝通，經常造成公民損害、人證及物證位於不同地點，更使執法機關對於整體案情研判及定罪面臨強大的挑戰。因此跨境警務合作勢必成為未來的趨勢。然而跨境警務合作需要多方建立穩固的平臺及合作

共識，包含對於證據取證的標準及評價力必須力求一致，才能對案件進行整體評價。

有鑑於跨境犯罪多仰賴於先進的通訊軟硬體，故數位證據在刑事案件所扮演的角色也日益重要。數位鑑識作業從現場的蒐集採證開始，乃至在法庭上的呈現，整個流程中數位證據的妥善保存是至關重要的，不管是人為、意外、天災等，稍有不慎就有可能導致數位證據的毀損或變更，使得好不容易蒐集而來的證據付之一炬。臺灣地區的數位證據監管，主要仍使用傳統紙本的作業流程。但隨著民眾對證據品質的要求提高，人為管理的監管鏈，在法庭上的證據力經常遭受質疑[1]。究其原因多半是證據的完整性不足，且常需要耗費大半心力在驗證數位證據的證據能力。

數位證據監管鏈所需要的完整性、歷史性與一致性正好是區塊鏈所具有的優勢[2]，故本研究提出以區塊鏈實行數位證據監管鏈的作法，並加以研究分析可行性，以強化數位證據的監管紀錄與驗證性。期望提供未來數位鑑識監管區塊鏈的研究方向與參考。執法機關對於數位鑑識監管區塊鏈的研究仍屬萌芽階段，若能結合區塊鏈的技術強化其證據的完整性驗證，相信對於檢視數位證據的合法性有極大的助益。本研究先就區塊鏈的技術與特性加以介紹，再導入數位證據監管區塊鏈的模型並介紹其運作模式，然後針對跨境警務合作該導入何種類型的區塊鏈深入討論，最後，提出幾個未來研究數位證據監管區塊鏈的方向及挑戰，作為實施數位證據監管區塊鏈的參考。

## 貳、文獻探討

### 一、數位證據監管鏈

監管鏈是指在調查中依照時間順序紀錄證據狀態的程序，依照美國國家司法研究院(NIJ, National Institute of Justice)對監管鏈的定義為：「用於維護和記錄證據時間歷史的過程」[1]，在整個調查中監管鏈扮演著舉足輕重的角色，證據的完整性必須根據首次發現的情況保持下來，直到後來提交給法院，良好的監管鏈能使法院接受證據。反之，若監管的過程中受到污染，那麼辛苦取得的證據將不被採信。因此，監管鏈必須記錄證據在調查過程的任何階段，從獲取、收集、證據分析、以及處理證據的單位到實驗室，還有使用證據的人員、時間、地點、原因與方式等相關的訊息[3]。

在當今數位化的時代，網路犯罪活動的數量與日俱增，日新月異的數位證據類型，使維護可靠的監管鏈變得更加困難。且數位證據易於修改及難以保存其原始狀態之特性，突顯了傳統鑑識程序與現今數位鑑識之間的巨大差別[1]。數位鑑識是利用科學方法來發現、收集、保存、分析、解釋和呈現與案件相關的數位證據，以利於案件重建以及司法審判。為了使每個證據都能有助於司法程序，數位證據必須符合可接受、真實、完整、可靠、可信等 5 個標

準。與實體的證據相較之下數位證據具有許多特徵，例如易於複製和傳輸、非常容易被修改和刪除、容易因保存不當被新數據污染，以及對時間很敏感。此外由於容易傳輸的特性，也使得數位證據非常容易跨越國家和法律管轄區[3]。

與傳統物理或化學相關的鑑識內容相比，數位證據監管鏈發展歷程較短，且因數位原始內容無法以實體方式判別，所以經常無意間遭到污染，進而影響證據能力。另外數位證據易於複製與傳輸，使數位鑑識人員在處理數位證據時，必須非常的小心謹慎。數位證據監管鏈要求的是數據的完整性，也就是指未經授權進行任何更改的一方，不能對數位證據進行任何變更，數位證據的變更和取得僅能由有具權限的人員完成。因此數位證據的完整性保證所提供的數據是完整的，並且從最初發現證據到最後在法庭上使用時保持不變[1]。因此，證據的完整性和專家解釋證據的能力將影響數位證據在法庭上的效果。

## 二、區塊鏈演進、運作與應用趨勢

### (一) 區塊鏈的演進

區塊鏈的概念源於 2008 年中本聰所發表的一篇論文，名為《比特幣：一種對等式的電子現金系統》[4]，並在隔年發布第一個比特幣軟體，成為最著名的區塊鏈應用程式。中本聰所提出的區塊鏈是一種分散式帳冊的概念，主要是用在虛擬貨幣與支付系統，透過密碼學雜湊值演算法取代受信賴的第三方角色，因其難以被竄改，故能保持區塊上資料的安全性與完整性，使各節點在每一份帳冊上維持著一致性，這個階段我們也稱為區塊鏈 1.0 [2]。

區塊鏈 2.0 的代表便是以太坊，他的底層技術也是比特幣的區塊鏈技術，最重要的是附加了能自動執行的智能合約，雖然稱為合約，但是與實體的紙本契約在法律上的效力有所不同[5]，它更適合被視為提前設定好的程式，當新的交易和事件的請求發生時，只有符合已編寫好的邏輯條件才能進行下一步的交易和事件[6]。這項新的技術與概念使得區塊鏈的應用領域擴展至金融科技業、產權的移轉、資產的註冊登記、合約交易行為等更為多元。

而最新的區塊鏈 3.0 也有人稱為超級帳本，它是區塊鏈與智能合約功能的延伸，再進一步引進權限控制和安全保障，使得細部運作更為精密，目的在創建實現分布式帳冊的跨行業開放標準平台來推進區塊鏈技術[7]，除了在經濟領域有巨大的貢獻外，更開發出許多新的設計與應用，像是電子政務、身分驗證、電子投票、醫療服務等 [2]。

### (二) 區塊鏈運作原理

區塊鏈的誕生，不僅顛覆了傳統的交易模式，更在不同的產業有了新的應用。不論是第幾代的區塊鏈，其運作方式與一開始中本聰所設計的比特幣區塊鏈設計原理大同小異。其核心原則為：

1、**點對點架構**：區塊鏈本身是一個分布式的數據庫，在這個系統中各個節點的參與者都

能透過P2P的網絡來交易數位資產並儲存交易紀錄。

- 2、**時間戳記儲存訊息**：區塊鏈以時間戳和交易驗證的方式來儲存訊息(如圖1)。區塊鏈鏈結方式及內容。交易紀錄是以「塊」的方式來儲存，每一個塊包含了雜湊值、時間戳和交易訊息，其中每個塊包含了不同的隨機數用以重新計算雜湊值。後面新產生的塊透過交易驗證的方式將添加到前一個區塊鏈上，透過此方式形成一條包含許多區塊的長鏈。
- 3、**共識機制**：具備規則和安全性的共識機制。在節點上交易的雙方透過使用公私鑰加密和數位簽章演算法來達到安全性。而每一個參與的節點可以共同驗證每個事件。其工作原理如下：每當交易進入P2P網絡時，節點首先驗證交易是否合法。如果節點就其合法性達成一致，他們會確認交易並將此決定放在一個區塊中。這個新的區塊會被添加到前一個區塊鏈中結合成更長的鏈。透過這種方式，最新的區塊保持了整條鏈最新狀態的共享[8]。

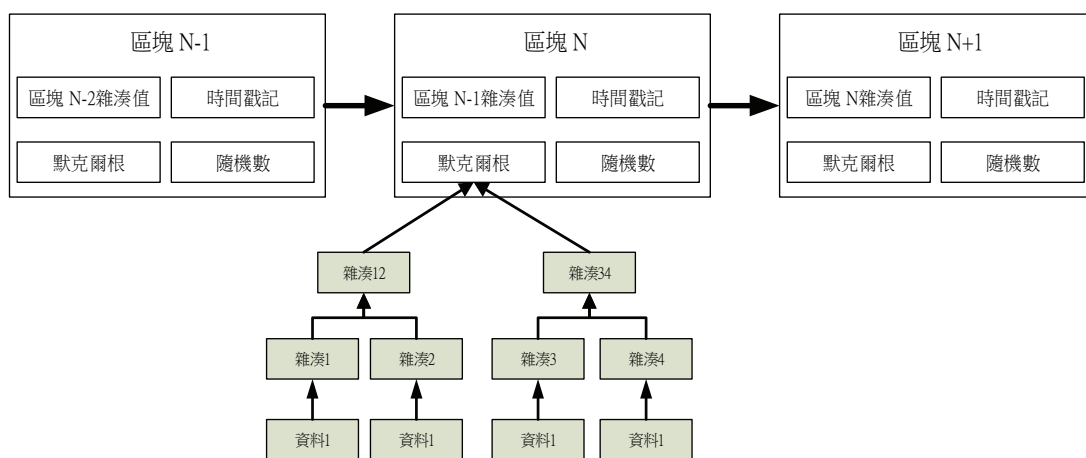


圖 1 區塊鏈運作原理

在區塊鏈中，所有交易都儲存在一個分布式的帳冊中，所有涉及的節點都持有一份副本，該副本與其他副本持續同步。因此，即使某個節點遭遇駭客攻擊，也不會影響整條鏈的運作。這種典型的 P2P 結構有助於安全性以及區塊鏈中記錄的事件不變性，另外，分布式共識協議也確保了交易的數據完整性。但這並不意味著它是完全不可改變的。有時在添加塊的過程中出現差異(比如說時間差)，或是有人偽造區塊，導致區塊鏈出現分岔的情形，那麼新的區塊會選擇添加到網絡中最長的鏈來解決這個問題，因為更長的鏈擁有更多的資源且更能被信任[4]。

而在以太坊中所使用的智能合約包含了有關交易的信息，它可以儲存參與者對條件的協議，並且一旦滿足條件，就會自動進行合約內容所涉及的變更。智能合約可以定義為「涉及數位資產和兩方或多方的機制」，其中部分或全部方將資產投入，透過網絡中的節點驗證合約

內容來重新分配資產[9]。

### (三) 區塊鏈的應用

目前在許多領域都能見到區塊鏈相關的應用，根據 Casino [10]進行區塊鏈應用的相關文獻研究發現，從 2017 年開始區塊鏈的研究數量大幅增加，尤其又以工商業最為明顯。Casino 將區塊鏈的應用分為工商業、隱私與安全性、教育、醫療、物聯網、政務、驗證、金融業、資料管理與雜項申請等 10 種。表 1 彙整各國家/地區之區塊鏈應用領域。

表 1 全球政府機關運用區塊鏈領域

| 國家/地區 | 應用領域                                                                           |
|-------|--------------------------------------------------------------------------------|
| 加拿大   | 將 NRC(國家研究委員會)預算資金儲存於區塊鏈中，民眾何隨時查看即時資訊，以增加政府資金透明度。                              |
| 美國    | 海關人員使用區塊鏈技術結合行動載具，來取代傳統使用紙本申報的進口貨物。                                            |
| 英國    | 使用區塊鏈技術進行法院數位證物保全                                                              |
| 愛沙尼亞  | 使用區塊鏈證証國民所有的金融、簽署文件等活動，以防止官員貪腐行為。                                              |
| 俄羅斯   | 莫斯科市政府使用區塊鏈認證市民，針對重大議題的投票及後續進度追綜，以改革貪腐情形。                                      |
| 杜拜    | 規劃於 2020 年之前，以區塊鏈記錄所有政府交易記錄，以減少紙張浪費。                                           |
| 澳洲    | 使用區塊鏈保存護照及出生證明資料，以確保資料的完整及安全性。                                                 |
| 西班牙   | 西班牙的主要銀行集團創建區塊鏈平臺，使銀行能夠在首次開立賬戶時識別客戶，以降低歐盟的金融犯罪。                                |
| 大陸地區  | 區塊鏈（天平鏈）技術，確保訴訟全流程記錄、全鏈路可信、全節點見證。                                              |
| 台灣地區  | 數位證據鑑定結果電子檔連同證物雜湊值記載於乙太坊區塊鏈上，院、檢及辯護人皆可便利地使用手機 APP 掃描查詢，驗證鑑定報告、來源證物及結果電子檔均未經竄改。 |

## 參、數位證據監管區塊鏈

### 一、運作模型

數位證據監管區塊鏈的主要功能便是檢視數位證據的完整性，在法庭上能以更簡便的方式證明數位證據的證據力。數位證據的取得可來自各類 3C 產品，例如：手機、電腦、行車紀錄器等電磁紀錄，由各個設備所取得的數據資料透過演算法轉成雜湊值加入區塊鏈中，透過數位證據監管區塊鏈記錄與驗證資料的完整性，它能確保資料不被竄改，並且可以隨時查看

各階段的數位證據狀態資料。而智能合約的加入，可以設定使用者的權限與功能來存取數位證據監管區塊鏈上的資料[11]。

如圖 2 所示，由各個電子設備所取得的雜湊值，將會儲存至區塊中，而使用者像是處理員警、鑑識人員、調查人員、律師、檢察官及法官等，透過智能合約所賦予的權限及功能來存取區塊鏈上的資料，利用區塊鏈中的雜湊值來比對數位證據是否有遭到竄改，而在區塊鏈上所做的行為都會被記錄並儲存下來，這保障了證據資料不會遭到竄改而保有其完整性。

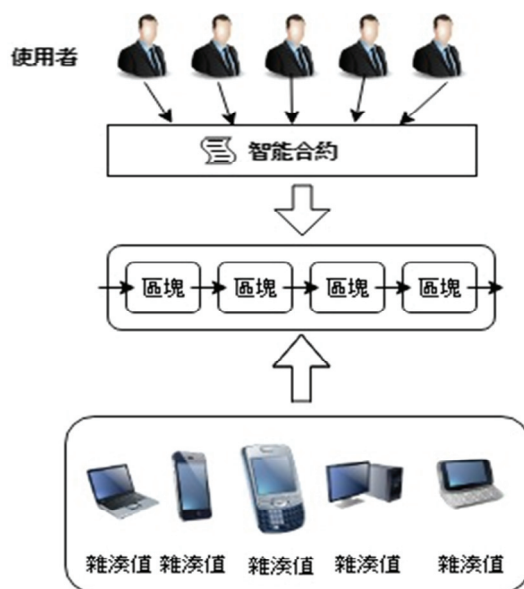


圖 2 數位證據監管區塊鏈

## 二、數位證據之傳統與區塊鏈監管鏈之比較

傳統的數位證據監管鏈主要係填寫紙本或電子表單為主，包括鑑識人員姓名，對所檢查證據的簡單描述以及檔案的雜湊值[1]。從刑案現場取得的數位證物需要進一步的送鑑分析，依照臺灣地區數位證物鑑識程，證物送鑑機關需要派員將證物及現場數位證據蒐證報告送至刑事警察局，經雙方確認證物無誤後完成交接，並由刑事警察局登記受理。受理後證物會逐一登錄並拍照，然後移至證物室保存，經過鑑識分析後歸還送鑑證物並檢附書面鑑識報告。在鑑識報告中會記載鑑識人員、送鑑單位、送鑑時間、鑑識項目、鑑識方法、證物資訊、鑑識工具及版本、鑑識結果、報告出具時間、附件等。送鑑單位需要派員送交待鑑證物外，鑑識機關同時需要派員接收、點交證物，而不管最後鑑識完成與否，還要將證物及鑑識報告一併交還送鑑機關，過程中人員的來回奔波造成雙方都會耗費一定的人力與時間，另外數位證物在移交、保存、鑑識分析的過程中，儘管鑑識機關花費時間逐一檢視證物，然而實際上數位證物的內容是否遭到毀損或竄改極難察覺。

相較之下，利用數位證物監管區塊鏈可以大幅減少所需要的人力與時間並保障數位證物的完整性。透過數位證物監管區塊鏈，從一開始取得數位證物即製作雜湊值，並上傳至區塊鏈上。送鑑機關將資料備份後送至鑑識機關，而不需要送交整個證物，鑑識完後自然也能省去再返還證物的流程，將證物送至鑑識機關後，鑑識機關能立即透過區塊鏈上的資料比對數位證物雜湊值來確定資料是否正確。透過智能合約的設定，使有權限的人登入存取數位證據監管區塊鏈上的資料，任何對區塊上的資料所採取的動作都會被記錄下來，包括時間、單位、人員以及採取的行為等，這比事後鑑識報告所記載的項目將更具說服力。最後，製成的鑑識報告，也能上傳至區塊上，減少紙本報告傳遞的作業流程，以及便於在法庭上的呈現。

表 2 顯示數位證據的紙本監管鏈與透過監管區塊鏈的方式做比較，在紙本監管鏈中數位證物需要送至鑑識機關來鑑識分析，才能確保數位證物的內容未受到汙染，這也使得證物的傳遞流程較單一化無法變通，另外還需要花費額外的人力與時間來傳遞與檢查數位證物，因此較遠的送鑑機關也顯得相對不便；相較之下，數位證據監管區塊鏈因為在第一時間即提取原始檔案製成雜湊值上傳至區塊鏈，因此可以確保此雜湊值不會被改變，送鑑機關可以透過更多元的方式，比如說 透過雲端、電子郵件、檔案傳輸等方式來傳遞數位證據的備份檔案，再透過區塊鏈上的雜湊值來核對數位證據的完整性，而無須擔心數位證據在傳送的過程中遭到毀損或竄改而無法察覺。這不僅能讓原本需要送鑑證物、送鑑與鑑識雙方檢視證物以及歸還證物的流程更為簡便，還能減少所耗費的人力與時間，另外由於區塊鏈儲存在網路中的各個節點，故只要使用網路及相應程式便能存取區塊鏈中的資料，讓整個數位證據監管區塊鏈能不受地域上的限制，即使在國外或跨境犯罪，也能透過網路查看數位證據監管區塊鏈的內容。

表 2 數位證據之傳統與區塊鏈監管鏈機制比較

|        | 傳統監管鏈     | 區塊鏈監管鏈     |
|--------|-----------|------------|
| 形式     | 紙本        | 區塊鏈        |
| 證物保管方式 | 證物須送至鑑識機關 | 證物無須送至鑑識機關 |
| 證物傳遞   | 較單一       | 多元性        |
| 作業流程   | 繁複        | 簡便         |
| 所需人力   | 多         | 少          |
| 耗費時間   | 多         | 少          |
| 地域性    | 狹隘受限      | 廣泛不受限      |

## 肆、區塊鏈與跨境警務合作之應用

### 一、區塊鏈種類介紹

因應科技的進步，許多新型態犯罪為了逃避司法機關的查緝，而將犯罪流程分散於不同區域，造成警方偵查困難。其中利用各地區訴訟或司法程序的不同，製造偵查斷點，更成為不法集團的慣用手法。近期兩岸四地間，不斷出現跨境大型詐騙集團，造成人民財物巨大損失，所以掃蕩跨境詐騙集團一直是各級政府的重點工作。然而為了進行刑事案件訴追，避免罪犯者逍遙法外，相關證據的順利移交，成為後續刑事訴訟成功與否的重要關鍵因素。鑑於新興科技犯罪所查扣的證物中，數位證據的比例亦逐年升高。考量數位證據容易變造或偽造的特性，如何在移交過程中，使雙方均能確保移交證據的完整性、一致性，成為兩岸四地執法機關的重要議題。

考量區塊鏈具有去中心化、歷史性、一致性及完整性等特點，且區塊鏈之雜湊資料亦為全世界通用，故導入區塊鏈協助數位證據移交，是個值得努力的方向。本研究以現有區塊鏈之種類，探討跨境犯罪證據移交的可能模式，區塊鏈的應用相當多元，依據其存取範圍、設計結構及功能，主要可分為以下 3 種：

- （一）**公有鏈**：公有鏈的主要使用範圍為全世界的節點，所有的使用者皆可過節點都能存取區塊鏈上的資料，每筆交易行為都是公開的，資料分散式儲存在各個節點上，因此不需要信賴的中介者來管理，所以公有鏈被視為完全去中心化的平臺。也因為公有鏈不屬於任何一個機構或團體，故區塊中計算資料的一致性、完整性，是由代幣機制獎勵的礦工來完成工作。公有鏈的代表者為目前常見的虛擬貨幣，例如比特幣或以太幣等。
- （二）**私有鏈**：私有鏈是由特定的組織或個人所擁有及管理，由創建區塊鏈的管理者來制定使用者的權限，決定哪些人能訪問區塊鏈上的內容，資料集中儲存在有權限的參與者中，因此仍由中心來管理參與者所能存取區塊上的資料 [9]。也因為特定組織可擁有私有鏈，故其形態無法維持完全去中心化，而轉變為部分去中心化。此類區塊連因可控制結點的參與程度，故交易速度較公有鏈快速，亦可維持較佳的隱私性。
- （三）**聯盟鏈**：聯盟鏈的性質介乎於公有鏈及私有鏈，其發展原因係為了達成多個性質相關的產業資料交易，雖然無法達到公開鏈完全透明的交易公開及便利性，但聯盟鏈可維持私有鏈的高隱私度。其中資料區塊的上鏈及驗證是由經過許可的節點才能執行，所以相較於公有鏈及私有鏈，聯盟鏈具有更彈性的權限設計。

表 3 各類型區塊鏈比較表

|     | 安全性 | 效率 | 去中心化 | 權限彈性 | 整合度 |
|-----|-----|----|------|------|-----|
| 公有鏈 | 高   | 低  | 高    | 低    | 易   |
| 私有鏈 | 低   | 高  | 低    | 低    | 易   |
| 聯盟鏈 | 低   | 高  | 中    | 高    | 難   |

## 二、跨境警務合作導入區塊鏈科技之決策

目前兩岸四地之跨境刑案偵辦，主要依據「海峽兩岸共同打擊犯罪及司法互助協議」內容辦理，其中並未訂定刑事訴訟移轉管轄之規定[12]。其中調查取證主要還是依據己方相關規定，故導入之證據移交機制必須保持相對彈性，減少強制性規定。若能在既有且世界通用之框架或平臺上進行協作，避免另外建置交流平臺，將可降低導入門檻，提升成功機率。

目前區塊鏈資料之完整性及一致性，已由學術及實務之多個研究機構採用，其中最有名的運用即發展出用於貨品交易之虛擬貨幣，其公開分散式帳本所要達成的目標，就是確保人、機構及物品間的相互信任關係，而跨境犯罪之數位證物移交，則必須建立在互信的觀點上。故導入區塊鏈應為實現此機制的最佳工具之一。然而區塊鏈技術隨著應用情境的不同，大致可區分為公有鏈、私有鏈及聯盟鏈 3 種，藉由表 3 可知，3 種區塊鏈形式各有其優缺點，本研究針對跨境刑事案件物證移轉機制，以下列 3 個層面討論較適合導入之區塊鏈種類：

- （一）**安全層面**：雖然各種區塊鏈之目的均為確保上鏈資料的一致性及完整性，但區塊鏈受攻擊的新聞亦不在少數，排除因資料管理不當，而遭入侵的案例，實際針對區塊鏈技術攻擊的手法中，最常被提到的就是「51%攻擊」，而造成前述攻擊的前提，必須控制足夠的運算節點數，控制運算節點的成本與整體區塊鏈節點總數成正比，換句話說區塊鏈中具有愈多運算參與者，則愈不容易遭受資料竄改。故就安全層面而言，導入公有鏈可增加數位證據的公信力。
- （二）**去中心化**：區塊鏈與現行證物鏈最大的不同在於具有去中心化的特質，傳統兩岸四地情資交換多以對口方式進行，即每個地區需推舉個人或機構擔任聯繫窗口，各地內部單位之需求均透過窗口統一進行協商，但導入區塊鏈即將面臨此機制的改變，區塊鏈內每個節點皆可獨立上傳資料，各節點均具有相同的權力。因此去中心化意謂著難以受到控制，若以政府追求穩定及可控制的思維，聯盟鏈將較符合現有體制的運作方式。
- （三）**整合度**：兩岸四地共同建置數位證據區塊鏈平臺因涉及法律與政治等因素，不同時期合作的模式將會隨之改變。故提出的整合架構，亦應能隨著不同合作模式，而呈現高度彈性的適配。因跨境警務合作將涉及多個機關，故本研究僅針對

公有鏈及聯盟鏈之整合度進行探討。首先聯盟鏈必須建立一套兩岸四地的區域網路，納入該網路的執法機關，才能將管轄的數位證物上傳。然而開放己方內部網路與其它跨境司法機關共同存取，是一道難以橫跨的難題。內部網路往往定位為資安等級較高，用於傳送內部機敏資料的途徑，若將聯盟鏈與內部網路相通，即等同於內部安全門戶大開，難以符合現今網路管理相關規定。但若另外重新規劃網路基礎建設，專用於兩岸四地司法協作區塊鏈平臺，亦有疊床架屋的缺點。再者因應不同時期的合作模式，亦可能更限縮或更寬鬆的認定聯盟鏈範圍，這些變動皆需動態新增或刪除節點，造成額外行政負擔。如採用公有鏈則無上述問題，無論兩岸四地以何種形式協作，皆可使用全世界公開的網路進行資料傳輸，較有利於提升整合的彈性。

綜上所述，使用公有鏈在安全性及整合性能對於跨境合作提供較佳的解決方案，但若考量政府針對協作的可控制程度，則以聯盟鏈較符合現行運作機制。

數位化時代的來臨、網路犯罪的增加，使數位證據的數量急遽上升，成為犯罪偵查主要的情資來源。由於數位證據易於複製、傳輸的特性，傳統的監管鏈無法保證數位證據在監管的過程中未遭更改，使數位證據在法庭上的證據力常常受到質疑。比特幣的發明使區塊鏈技術逐漸受到重視與討論，其擁有的特色包含去中心化、歷史性、完整性與一致性等正好是數位證據監管鏈所需要的，因此本研究提出一個數位證據監管區塊鏈的架構來進行探討。由各個電子設備所取得的數據資料透過演算法轉成雜湊值加入區塊鏈中，經過智能合約的設定與管理來賦予使用者權限，有任何的存取行為都將會被區塊鏈記錄下來。相較於傳統的數位證據監管鏈，使用區塊鏈來監管數位證據不只在證物的保管、證物的傳遞與整個鑑識的流程都更為簡便外，相對的人力與時間的花費較少，更不受地域性的限制，提升了使用者存取數位證據的便利性並且確保資料不會被更改。

數位證據監管區塊鏈提供了數位證據的雜湊值比對，在法庭上能以更有效率及便捷的方式來驗證數位證據的完整性。考量複雜的跨境警務合作模式，本研究以 3 種區塊鏈種類，針對安全性、去中心化程度及整合性等 3 個面向進行討論。

- 公有鏈：具有高度整合性特點，可提供不同跨境合作模式的適配方案，其較高公認程度的安全性，亦符合數位證據防止竄改的需求。但現行透過窗口統一進行協商的機制，會因導入公有鏈而面臨改變。
- 私有鏈：具有較高的安全性及效率。但因兩岸四地跨境犯罪須進行多方資料交換，由單一地區所建置的私有鏈，較不符合跨境司法互助需求。
- 聯盟鏈：具有高效率及權限彈性，設計理念較符合現行建立聯繫窗口的司法協作模式。但開放內部網路的安全議題，則需以較嚴格的標準檢視。

## 參考書目

1. Giova, G. "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems", *International Journal of Computer Science and Network Security*, Vol. 11, No. 1, 2011, pp. 1-9.
2. Swan, M. *Blockchain: Blueprint for a New Economy*. " O'Reilly Media, Inc.", 2015.
3. Prayudi, Y., and Sn, A. "Digital Chain of Custody: State of the Art", *International Journal of Computer Applications*, Vol. 114, No. 5, 2015.
4. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.
5. Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A., Weber, I., Xu, X., and Zhu, J. "Risks and Opportunities for Systems Using Blockchain and Smart Contracts. Data61." CSIRO), Sydney, 2017.
6. Buterin, V. "A Next-Generation Smart Contract and Decentralized Application Platform", *white paper*, Vol., 2014.
7. Cachin, C. ", Architecture of the Hyperledger Blockchain Fabric." Paper presented at the Workshop on distributed cryptocurrencies and consensus ledgers, 2016.
8. Pilkington, M. "11 Blockchain Technology: Principles and Applications", *Research handbook on digital transformations*, Vol. 225, 2016.
9. Ølnes, S., Ubacht, J., and Janssen, M. "Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing." Elsevier, 2017.
10. Casino, F., Dasaklis, T. K., and Patsakis, C. "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues", *Telematics and Informatics*, Vol. 36, 2019, pp. 55-81.
11. Lone, A. H., and Mir, R. N. "Forensic-Chain: Ethereum Blockchain Based Digital Forensics Chain of Custody", *Sci. Pract. Cyber Secur. J*, Vol. 1, No. 2, 2018, pp. 21-27.
12. 楊雲驊. "兩岸刑事訴訟管轄權移轉之探討－以歐洲刑事訴訟移轉管轄公約為中心", *刑事政策與犯罪研究論文集*, Vol. 16, 2014, pp. 27-41.

轉載自『第十四屆海峽兩岸暨香港澳門警學研討會發言論文集』頁 125-135。