區塊鏈智能合約與跨境

摘要

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，就是日新月異的新型態科技犯罪，而科技設備所產生的犯罪數位證據，警方該如何維持其證據力，並做為定罪的依據，是目前犯罪偵查所面臨的挑戰。加上現代犯罪集團往往由跨國的組織所主導，藉由不同國家司法管轄的衝突，躲避執法機關的查緝。因此在跨境犯罪的框架下，維持數位證據的完整性及不可竄改性，並順利執行跨境證物轉交作業，將是全球警務合作的新趨勢。本文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，另藉由智能合約公開透明的優勢，在去中心化的概念下，進行司法文書情資交換。本研究所提出之跨境數位證據監管區塊鏈的架構，可讓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，確保在資料跨境移轉的過程中，不論在安全性、去中心化及整合度3方向，均可有效保存及管理數位證據。

數位證據監管鏈之應用

蔡馥瑔／中央警察大學刑事警察學系助理教授

關鍵詞 區塊鏈、智能合約、跨境犯罪、監管鏈

一、前言

近年來，隨著網路的普及與便利，對於傳統犯罪模式而言，產生很大的影響。資訊科技發展所帶來革命性的變革，使犯罪者透過網路科技打破了國界的限制。導致犯罪地點與型態趨向多元與多變，造成跨境犯罪的興起，諸如跨境詐欺、洗錢、毒品交易與人口販運等問題。跨境犯罪嚴重破壞了社會秩序與經濟穩定，也使得偵查工作不再侷限於單一國家。如何透過國際間的合作，共同打擊犯罪成為一大挑戰。

跨境犯罪中高度使用數位設備是非常明顯的趨勢。跨境犯罪者因分屬不同國家，在實體距離難以到達的情境下，犯罪者必須善用各項通訊科技才聯繫境外犯罪成員，因此許多跨國犯罪證據都存在於電子設備中。然而數位證據因易於修改的特性，造成保存不易，而且不同國家對於數位證據的要求不一，若不提升數位證據的取證、保存、移交的品質，即使國家之間已完成司法合作以取得案件相關的資料與證據，在法院審理時，該證據是仍難以具有足夠的證據力。

然而數位證物並非如傳統證物（文書、印章等）具有穩固性，相反的，數位證物具有脆弱性及揮發性，在調查過程中容易因處理不當或意外造成資料的變更、毀損[1]。所以數位證物如果要具證據能力，作為法院認定事實之基礎，需要經過嚴謹檢視是否遵守相關規範，檢驗標準依不同的司法權有所改變，通常需符合當地法令且具真實性、信賴性及關連性，其中真實性最重要的檢驗標的就是證物監管鏈[1-3]。

有鑒於現今新型態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。國內的數位證據監管，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[3]。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。

對於跨境犯罪而言，數位證據監管鏈更是重要。因各國對於數位證據的採證要求不同，因此，在案發地所管轄之犯罪現場，執法人員於當下所進行的證據蒐集流程，更會左右證據移交後，在另一受審國家所具有的證據力。目前針對數位證據真實性的認定，多仰賴於取證現場針對數位證物所產生的雜湊值（Hash Value），故在犯罪現場如何有效率的針對有關證據產生完整的雜湊值，是在面臨不同司法管轄權的制度下，維持數位證據力的方法之一。區塊鏈技術因其分散式帳本架構，具有去中心化、難以竄改、可追溯性等特性，確保資訊上鏈後之正確性。目前已有許多區塊鏈技術被運用在整體性的證物監管鏈上[4-8]，用來解釋雲端取證資料驗證[9]及物聯網犯罪跡證保存等問題[10]。

除了區塊鏈具有完整性、歷史性與一致性的功能，正好是監管鏈的重要特性之外，智能合約的應用更擴展了監管鏈的用途。透過智能合約在區塊鏈上公開的特性，監管鏈中數位證物的遞交及收取方，皆可藉由公開的合約內容，確保合約執行結果的公正性，進而達到雙方互信的目的。因此智能合約可藉由高度透明性且不可更改的特點，在監管鏈生態中，扮演公正且被信任的角色，數位證物跨國交付的過程中，提升雙方對數位證物的互信，確保物證的可信度。故本文提出以區塊鏈結合智能合約的架構，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。

二、區塊鏈

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》[11]，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[12]。

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[13]，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[14]。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[15]，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[16]。

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（peer-to-peer）的網絡來交易數位資產並儲存交易紀錄，P2P網路是利用每個使用者作為節點而形成的資料交換網路，其優點可減少中心型網路節點的依賴程度，並增加可靠度。

2、時間戳記驗證訊息：區塊鏈以時間戳記驗證及記錄交易發生的時間，並將訊息儲存在區塊中（如圖1）。區塊鏈鏈結方式及內容是以「區塊」的方式來儲存，每一個區塊包含了雜湊值、時間戳和交易訊息，其中每個區塊包含了不同的隨機數用以重新計算雜湊值。後面新產

生的區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[16]。

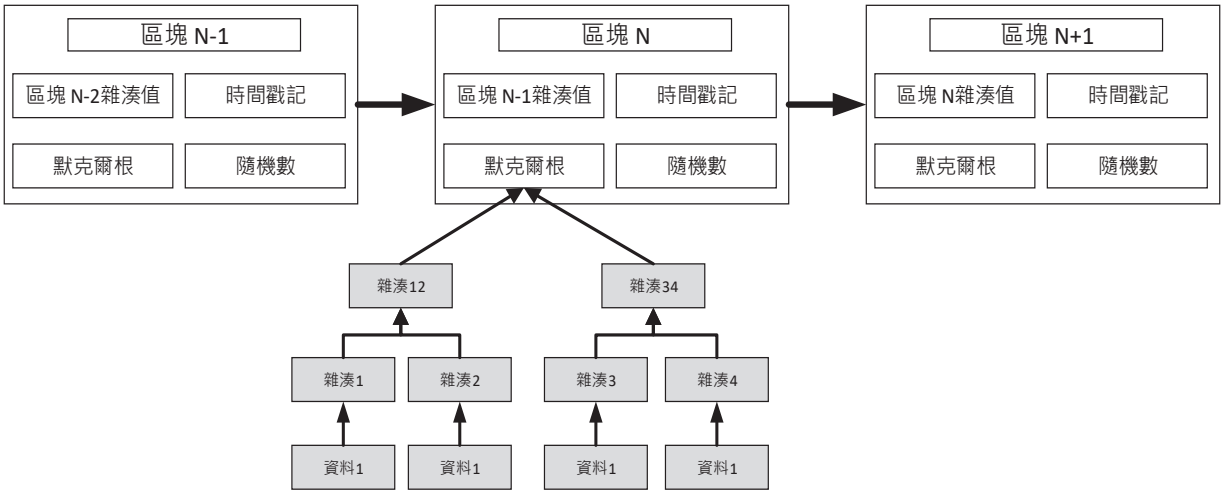

圖1、區塊鏈運作原理

區塊鏈雖具有高度透明的優點，但在不同商業應用上，可能產生商業機密外洩的風險。另一方面，區塊鏈因具有去中心化的特點，相對造成資料過於分散，無法使用強大的中央機構，進行多邊資料交換，意味著資料傳遞速度較慢。且共識機制需仰賴較多節點共同驗證，無法如現行星狀架構，以單一中央機構進行驗證，也造成交易效率不佳。故在不同的應用領域，學者提出不同版本的區塊鏈機制，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及完整性，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。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。

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，則以許可制的聯盟鏈較符合現行運作機制，藉由參與聯盟鏈的成員皆需經過核可，管控聯盟鏈的成員，而成員在聯盟鏈內的讀取及參與交易的權限，可透智能合約加以規範，同時兼顧資料隱私及權限公開的優點。

除了較常見的金融領域，許多企業及政府機關也開始運用區塊鏈提升資料的安全性及透明度。例如供應鏈管理、電子身份證、電子化醫療記錄管理[17]等。區塊鏈使用的情境適用於許多單位共同創造及維護交易記錄，因為其高度透明性及資料不可更改的特性，對區塊鏈上的內容提供非常好的稽核機制[18]，所以可以取得各單位的信任。所以區塊鏈在政府機關內已有許多的應用，但利用區塊鏈科技於數位證物管理是較少研究探討的[17-19]。表1彙整了各項區塊鏈應用領域及國家。

表1、區塊鏈科技於全球政府機關的應用領域

應用領域	國家
驗證以區塊鏈記錄政府土地註冊及交易資料	印尼、越南
使用區塊鏈技術結合行動載具，記錄所有政府交易記錄，以減少紙張浪費。例如:海關以區塊鏈來取代傳統使用紙本申報的進口貨物。	美國、杜拜
使用區塊鏈技術進行法院數位證物保全	英國、中國、中華民國
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，及政府資金的透明度。	愛沙尼亞、俄羅斯、加拿大
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。	澳洲
銀行集團創建區塊鏈平臺，使銀行能夠識別客戶，以降低歐盟的金融犯罪。	西班牙

三、智能合約

對於數位證物而言，因涉及許多隱私性資料，所以設定存取權限是必要的。區塊鏈在最初的設計上，是一種去中心化的交易機制。強調公開、透明的運作方式，使每個參與的節點都能見到交易的內容。因此並未涉及到權限管理的功能。目前比特幣所使用區塊鏈1.0架構，即是以公開帳本為主的運作機制，強調交易的高度透明性，以取得所有比特幣交易者的信賴。但當運用區塊鏈記錄數位證物時，對於犯罪資料的存取與查詢，因涉及民眾的個人隱私，所以應該導入權限控管制[18]，可強化隱私權的保護及提升證物管理的安全性。本研究中由於涉及了多國的偵查主體，系統內的資料還涉及了個人隱私，所以必須考量開放資料存取的權限。

智能合約是一種區塊鏈上的協議機制，可用於規範區塊鏈的交易行為，目前已有許多應用的研究。智能合約可在區塊鏈上執行運算邏輯。智能合約是在1994年提出，他是一種以信息化傳播，其可驗證及執行的合約，智能合約是以太坊區塊鏈上執行邏輯運算最主要的應用。智能合約的內容位於區塊鏈上，所有參與的節點都能看到其程式碼設計。此外，智能合約可以執行計算、儲存訊息以及公開屬性狀態，並在符合條件時自動執行。在多方參與者中可以解決由誰主導控制權的問題，作為可信賴的第三方。整體而言，使用智能合約能夠提供可證明的數據和透明度，從而增強信任度。透過自動化執行，減少傳統業務與應用程序中存在的驗證成本以及時間。另外智能合約必須公開於區塊鏈上，在區塊鏈上的用戶都有權檢視合約內容，所以可同時兼顧透明與隱私的需求，亦可用於數位證據在區塊鏈的權限控管問題，據我們所知，目前暫無研究對於此議題有較深入的探討。

目前智能合約最主要的應用平臺為以太坊，其最主要的功能在於與區塊鏈結合，因為區塊鏈具有不可竄改的特性，所以智能合約也可確保一旦儲存於區塊鏈中，合約內容即無法更改，所以合約的任一方無法片面更動合約，而造成另一方的損失。以太坊的智能合約開發標準為ERC協定，ERC的全名為Ethereum Request for Comments。ERC協定中描述了各種智能合約的開發原則，以下介紹較常見的3種協定，分別為ERC20、ERC223和ERC721。

ERC20於2015年提出，是以太坊最常見的智能合約，因為ERC20功能簡單且具備代幣（Token）轉換的功能，所以可以實現帳戶中代幣的餘額、轉帳、接收轉帳等功能，所以也能在以太坊中進行代幣的轉換。在ERC20中的每個代幣都是同等且可互換的，例如:甲帳戶中的1塊以太幣跟乙帳戶中的1塊以太幣是相等的。此外ERC20的同質化代幣還有可分割的特性，例如1塊乙太幣可被分為2個0.5塊的乙太幣，ERC20的同質化及可分割性的概念與目前實體貨幣概念相近，故被廣泛使用於虛擬貨幣的發行標準。ERC223主要是用來修正ERC20執行智能合約時，若傳送方及接收方未進行確認（Approve），以致傳送（Transfer）位址錯誤時，所傳送的代幣會遺失的問題。另一個ERC223的優點在於可使用較少步驟完成代幣的傳送，意謂著較少的步驟將

可降低手續費（Gas）。以往使用ERC20進行代幣傳送須經由2個步驟，在ERC223標準中，僅使用1個步驟，所以ERC223的手續費將只有ERC20的一半。雖然ERC223可向下相容ERC20，且相較於ERC20有許多優點，但因ERC20開發較早，故ERC223的廣泛程度及不及ERC20。

ERC721與前述ERC20及ERC223則是完全不同的設計理念。ERC721最主要的概念就是提供了非同質化（Non-fungible）的概念。例如:甲帳戶中的1塊以太幣與乙帳戶中的1塊以太幣是不相同的。既然ERC721的代幣具有非同質化的特徵，所以代幣也是不允許分割或合併的，在ERC721架構中，無法將2個0.5枚以太幣，合成1枚以太幣。而這個概念與現實世界的資產相契合，藉由每個資產特有的識別資料（Token ID），可應用於許多數位資產的管理，例如收藏品、遊戲寶物、裝備等，例如近年來的NFT交易平臺Opensea及Rarible等，其交易金額與交易次數履創新高，都顯示ERC721協定未來將有可能與實體資產結合，創造出新時代的交易模式。

四、跨境犯罪證據監管鏈的應用

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[20]。如圖2所示，A、B、C等3個國家利用聯盟區塊鏈架構，建立了以太坊數位證據監管鏈平臺，每個國家司法人員都具有一個帳號，帳戶名稱為區塊鏈中的位址表示方式，以「0x」為開頭的以太坊位址，其中智能合約亦有相對應的位址。若A國境內發生了跨國刑事案件，且該案涉及B國的管轄權，故數位證據必須由A國移轉給B國進行後續偵查。然而B國的偵查

人員收到A國移轉的數位證據後，必須先進行數位證據的驗證，確保在傳輸過程中，並未遭受到修改。在本研究提出的架構中，A國司法人員可將所取得的數位證據案件雜湊值，透過智能合約將雜湊值上傳至區塊鏈上，此時B國的偵查人員即可透過智能合約的管控，於區塊鏈上查詢該案件的雜湊值，若雜湊值與跨國司法文書記載的雜湊值一致，則代表該案件的數位證據並未受到修改，為可信任的證據。

本研究所提出的架構，主要是針對跨國案件移轉之數位證據，是否適合以區塊鏈做為實踐監管鏈功能之初探，研究結果顯示，以許可制的聯盟鏈配合智能合約，透過權限管理可賦予各國司法人員彈性的權限，可解決多邊合作長久以來存在的資料分享困擾，也能提高情資與證據交換的安全與效率。後續研究可將司法人員的身分擴增為處理員警、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相對應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。

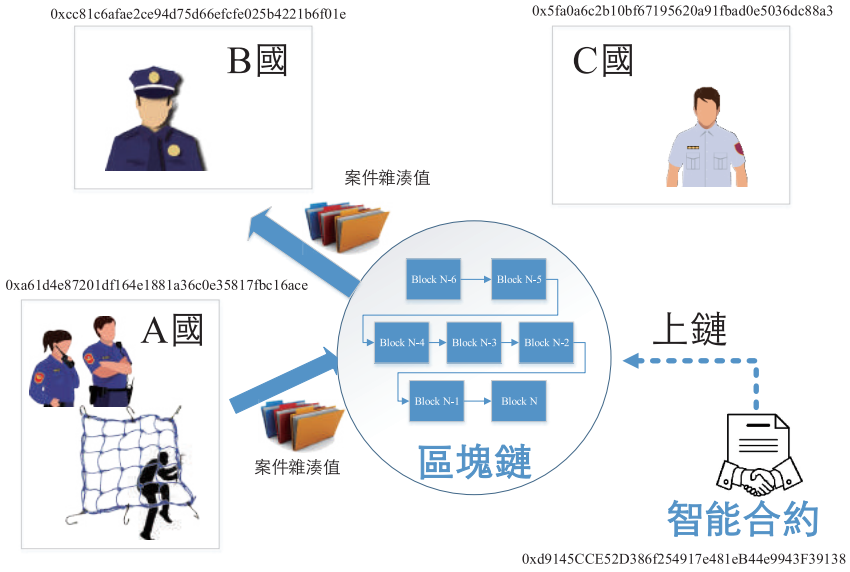

圖2、跨境犯罪之數位監管區塊鏈架構

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。本研究針對跨境刑事案件物證移轉機制，以下列3個層面討論導入之區塊鏈機制之注意事項：

（一）資料安全：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。故就資料安全層面而言，若參與的國家愈多，則區塊鏈的數位證據公信力亦相對提升。

（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，傳統國際間執法機關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，然而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。然而去中心化架構意謂著難以受到控制，若以政府追求穩定及可控制的思維，可考慮採用聯盟鏈方式，建立較符合現有體制的運作方式。

（三）整合度：因跨境警務合作將涉及多個國家，若開放己方內部網路與其它跨境司法機關共同存取，將是一道難以橫跨的難題。加上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，若將內部網路向外接通，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。此情況下可考慮採用公有鏈，讓執法機關以全世界公開的網路進行資料驗證，當然，區塊鏈上傳送的資料僅止於數位證據的雜湊值，用於證明該數位證據並未遭到修改，而非上傳敏感的犯罪資料。

五、結語

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。FACT

參考文獻

1.Montasari, R., The comprehensive digital forensic investigation process model （CDFIPM） for digital forensic practice. 2016.

2.Casey, E., Digital evidence and computer crime: Forensic science, computers, and the internet. 2011: Academic press.

3.Giova, G., Improving chain of custody in forensic investigation of electronic digital systems. International Journal of Computer Science and Network Security, 2011. 11（1）: p. 1-9.

4.Bonomi, S., M. Casini, and C. Ciccotelli, B-coc: A blockchain-based chain of custody for evidences management in digital forensics. arXiv preprint arXiv:1807.10359, 2018.

5.Chopade, M., et al. Digital Forensics: Maintaining Chain of Custody Using Blockchain. in 2019 Third International conference on I-SMAC （IoT in Social, Mobile, Analytics and Cloud）（I-SMAC）. 2019. IEEE.

6.Li, S., T. Qin, and G. Min, Blockchain-based digital forensics investigation framework in the internet of things and social systems. IEEE Transactions on Computational Social Systems, 2019. 6（6）: p. 1433-

1441.

7.Lone, A.H. and R.N. Mir, Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 2019. 28: p. 44-55.

8.Tian, Z., et al., Block-DEF: A secure digital evidence framework using blockchain. Information Sciences, 2019. 491: p. 151-165.

9.Zhang, Y., et al. A blockchain-based process provenance for cloud forensics. in 2017 3rd IEEE International Conference on Computer and Communications （ICCC）. 2017. IEEE.

10.Brotsis, S., et al. Blockchain solutions for forensic evidence preservation in IoT environments. in 2019 IEEE Conference on Network Softwarization （NetSoft）. 2019. IEEE.

11.Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system. 2008.

12.Swan, M., Blockchain: Blueprint for a new economy. 2015: O'Reilly Media, Inc.

13.Staples, M., et al., Risks and opportunities for systems using blockchain and smart contracts. Data61. 2017, CSIRO）, Sydney.

14.Buterin, V., A next-generation smart contract and decentralized application platform. white paper, 2014.

15.Cachin, C. Architecture of the hyperledger blockchain fabric. in Workshop on distributed cryptocurrencies and consensus ledgers. 2016.

16.Pilkington, M., 11 Blockchain technology: principles and applications. Research handbook on digital transformations, 2016. 225: p. 225-253.

17.Batubara, F.R., J. Ubacht, and M. Janssen. Challenges of blockchain technology adoption for e-government: a systematic literature review. in Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. 2018.

18.Xu, X., et al. A taxonomy of blockchain-based systems for architecture design. in 2017 IEEE international conference on software architecture （ICSA）. 2017. IEEE.

19.Ølnes, S., J. Ubacht, and M. Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly, 2017. 34（3）: p. 355-364.

20.Lone, A.H. and R.N. Mir, Forensic-chain: ethereum blockchain based digital forensics chain of custody. Sci. Pract. Cyber Secur. J, 2018. 1（2）: p. 21-27.