國立政治大學法律科際整合研究所
碩士學位論文

區塊鏈技術於電子簽章法之相容性研究

Research on the Compatibility of Blockchain Technology in Electronic Signature Law

指導教授：臧正運 博士

研究生：翁杰廷 撰

中 華 民 國 一 百 零 八 年 七 月

DOI:10.6814/NCCU201901043

摘要

2000 年互聯網的興起讓商業關係進入數位化時代，電子簽章法的制定賦予數位環境中使用數位方法進行商業法律關係之基礎依據，使得電子商務關係得以開展；2016 年區塊鏈技術的去中心化設計翻轉以中心化管理模式為主的當代思維，但能否成功發展並落地商轉仍須先釐清其是否符合現行電子簽章法所承認之數位方法而有法律上之效力，建立在此基礎所開展之法律關係方有法源依據。

國際電子簽章法採技術中立原則，彈性的架構是為因應資訊科技日異月新的特性，而區塊鏈與現行電子簽章技術有所重疊，因此本文從檢視區塊鏈技術出發，並以兩者使用的共同技術-公開金鑰加密演算法作為主軸，探討美國和歐盟的電子簽章法規範下之電子簽章定義、中心憑證機構運作模式與責任規範、時間戳等三個核心概念，以探討區塊鏈技術是否相容於現行電子簽章法下之規範模式，並提出相關修法建議，以盡速釐清區塊鏈技術於法律上效力之爭議，以利日後金融科技之發展。

關鍵字：電子簽章法、區塊鏈、公開金鑰加密演算法、憑證機構、時間戳

DOI:10.6814/NCCU201901043

目錄

DOI:10.6814/NCCU201901043

DOI:10.6814/NCCU201901043

DOI:10.6814/NCCU201901043

圖目錄

表目錄

DOI:10.6814/NCCU201901043

第一章 緒論

第一節 研究動機

2016 年區塊鏈迅速崛起，立刻成為眾所矚目的焦點，去中心化的特色代表的是現今治理模式的重新塑造，其影響的範圍遍及各個需要以中心(Hub)為管理中樞而進行資訊交換的產業。

「世界經濟論壇」(WEF)創辦人 Klaus Schwab 指出，區塊鏈將會帶來繼蒸汽機、電能、電腦之後的第四次工業革命，俄羅斯聯邦儲蓄銀行副主席 Andrey Sharov 更預言，區塊鏈技術會讓銀行在 10 年內消失。以區塊鏈為首所建構的金融科技世代，將形塑前所未有的全球金融生態，並根本性解構現有的產業生態和服務模式，包含資訊技術管理、產品服務、交易模式和監理思維，這股破壞性創新的力量將翻轉以中心管理模式為主的現代世界。此外，根據管理顧問公司 Accenture 的研究指出，2018 年全球金融科技投資金額已高達 553 億美元，相較於 2010 年的 18 億美元，成長近 3000 倍[1]，對各國而言，區塊鏈為驅動因子的金融科技是各國新的競爭起點，更是提升國家競爭力的關鍵，因此各國亦在立法上尋求相應的管制和配套措施，期待能賦予區塊鏈相關應用法律上之效力與標準，避免其顛覆性的影響造成政府、經濟社會失序，更重要的是提供兼容並蓄的法規環境作為後盾，以蓄積金融科技創新的能量，並提升國家世界的競爭力。

區塊鏈是一個集合名詞，其代表的是四種主要技術的總稱，分別是共識機制、公開金鑰加密演算法、默克爾樹和時間戳，而其中公開金鑰加密演算法的

[1]Accenture,Global Fintech Financing, available at：https://newsroom.accenture.com/news/global-fintech-investments-surged-in-2018-with-investments-in-china-taking-the-lead-accenture-analysis-finds-uk-gains-sharply-despite-brexit-doubts.htm(Last visited on 2019/07/01)

DOI:10.6814/NCCU201901043

數位簽章功能即是我們得以辨識資料來源、擔保文件真正和數位意思表示的重要技術，而數位簽章是電子簽章技術的一種實作方法，建立了數位環境中交易雙方的信賴關係，當確認數位簽章有與書面簽章相同之法律效力，電子商務行為如買賣等法律行為方得以開展。而後續發生糾紛時節點的責任、時間戳的證據能力則是建構完整法律救濟途徑的重要議題，

此外，目前賦予區塊鏈技術應用效力的立法模式如美國亞利桑那州、田納西州、內華達州或德拉瓦州，將區塊鏈應用相關規範直接置於電子簽章法之下，此係鑑於區塊鏈技術與電子簽章使用的技術部分重疊，但細究區塊鏈技術的本質仍有許多地方與電子簽章運行的特性和邏輯相異，因此有需要將區塊鏈技術的本質作一釐清之後，再行檢視區塊鏈是否相容於現行的法規範體系，否則將兩者不同運行邏輯的技術規範硬行置於同一法規範體系，不僅造成法規範適用上的困難和疑義，更不利以區塊鏈為驅動的金融科技商業模式之發展，因此本文從區塊鏈技術特性出發，檢視區塊鏈於現行國際電子簽章法和我國電子簽章法之相容性，再提出對我國電子簽章法修訂之建議，以作為日後立法者對於區塊鏈法制建制上的參考，讓台灣能在瞬息萬變的金融科技浪潮中無法律之掣肘，取得競爭的先機。

第二節 研究目的

區塊鏈如同第三次工業革命的電腦與互聯網，作為資訊革命的核心技術，基於此所建立的平台、商業應用將是無遠弗屆，如何賦予此技術應用於法律上之效力是一大難題，本文首先分析區塊鏈的技術本質和國際監管趨勢，以建立區塊鏈監理思維和議題分析框架，以期未來區塊鏈應用所產生的新興法律議題能有一宏觀的體系作為思考主軸，並找出相應的監理方法。

此外，另以區塊鏈主要的三項技術特性-區塊鏈簽章、分散式節點、時間

DOI:10.6814/NCCU201901043

戳，並對照現行國際電子簽章法之規定，找出區塊鏈與現行電子簽章規範的相容性，在此基礎下，檢視同樣採納技術中立原則的我國電子簽章法是否能作為區塊鏈基礎規範的可能性，並提供相關修法的建議和方向。

依此，本文的研究目歸納如下：

1、分析區塊鏈技術與電子簽章技術之異同

2、區塊鏈技術於現行國際電子簽章法之相容性

3、區塊鏈技術於我國電子簽章法之相容性和相關立法缺漏

4、電子簽章法之修法建議

第三節 研究範圍

本文將以區塊鏈技術和應用的探討作為出發點，並以美國、歐盟電子簽章法作為討論範疇以分析區塊鏈於電子簽章法架構下之相容性，並於最後探討區塊鏈於我國電子簽章法之相容性和相關立法建議。

第四節 研究方法

本文以文獻蒐集及資料分析為主要研究方法，並利用相關專書著作、期刊、論文和網路發表之文章，整理區塊鏈的技術和特性，並分析現行電子簽章法的立法目的和運作模式，以探討區塊鏈是否相容於現行法制。

第五節 預期結果

本文整理歸納區塊鏈技術的本質和特性，並以此作為基礎與美國、歐盟兩國電子簽章法進行分析和比較，以期找出區塊鏈與電子簽章運行方式的異同和法規相容性，進而提出未來修法之建議。

DOI:10.6814/NCCU201901043

第二章 區塊鏈及其技術來源

第一節 區塊鏈之起源-比特幣之應用

比特幣是區塊鏈最早的應用，而區塊鏈則是實現比特幣之核心底層技術，其源自於 Satoshi Nakamoto 於 2008 年 10 月 31 日向「metzdowd.com」[2]網站的密碼學郵寄清單中發表之一篇論文《Bitcoin: A Peer-to-Peer Electronic Cash System》，這也是世界上第一個分散式匿名數位貨幣。隨著此篇論文的誕生，大家對於區塊鏈技術所能應用之領域感到興奮，世界經濟論壇創辦人 Klaus Schwab 甚至認為區塊鏈是帶動全世界第四次工業革命的關鍵技術。

因此對於比特幣核心概念的認識有助於我們對於抽象之區塊鏈技術的理解和對於區塊鏈未來應用領域之想像。

Satoshi Nakamoto 在論文中提出了比特幣主要的四項特色[3]：去中心化、防止偽造交易、防止惡意攻擊、匿名交易。

一、去中心化

傳統交易仰賴銀行作為雙方交易之中間人，並作為公正第三方以驗證、調解糾紛、賠償和風險管控，因此銀行相當重視 KYC(Know your customer)的落實，預先蒐集交易雙方的基本資料，以建立信任基礎網路，銀行亦收取交易手續費作為承擔信任風險之對價。但比特幣無須仰賴中介機構作為驗證交易之機構，改由電腦加密演算法進行精確且嚴謹之驗證，不僅大幅降低交易成本，亦讓小額支付成為可能。

[2] 網站網址請參照：https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System(2008), p1, available at：https://bitcoin.org/bitcoin.pdf

DOI:10.6814/NCCU201901043

二、防止偽造交易

傳統實體交易銀貨兩訖，雙方可清楚看到彼此長相和欲交易的契約標的。數位交易中雙方透過虛擬網際網路進行磋商締約，數位資料容易複製和偽造的特性，造成數位貨幣可能會有一筆錢被作兩次使用花費的風險(double-spending)，因此如何保障網路世界交易的安全性即是重要的課題。Satoshi Nakamoto 於是設計數位簽章(digital signature)和時間戳(timestamp server)技術以防止雙重支付(double-spending)的發生。

三、防止惡意攻擊-不可竄改性

傳統之數位交易架構，駭客只需攻擊儲存資料的中心伺服器即可癱瘓整個交易網路，但比特幣透過工作量證明機制(proof of work)，俗稱挖礦，可以想像每個節點競爭解答一個相當困難的數學題目，率先解答的節點可以將此答案資料廣播予其他網路上的節點一起驗證，若確定無誤則能將此答案資料永久記錄在一個有效區塊上且無法被更改，也因為此機制是透過嚴謹的演算法運行，外界若想惡意竄改區塊上的資料，必須獲得網路上 51%以上的算力[4]才可能實現，故整個網路資料的安全性得以確保。

四、匿名交易[5]

傳統交易中銀行作為中介機構，並掌握了雙方交易者的身分、時間、金額

[4]區塊鏈網絡如比特幣係由節點競逐解題之方式以取得記帳之權利和驗證交易，若某節點或團體掌握超過 51%以上之計算能力，則能以此優勢優先解出答案而取得記帳之權利，進而讓偽造之交易區塊加入主鏈中。

[5] 事實上有學者認為使用者於比特幣區塊鏈網絡中並非真的「匿名」(Anonymous)，而只是「假名」(Pseudonymity)而已，如同在網路論壇中使用的暱稱一樣，最後仍可追蹤 IP 位址，並映射對應之網路卡號和使用此網路卡之電腦，進而找出電腦使用者，此外任使用者的比特幣收款地址、交易明細必須是公開的，以利礦工在交易前針對雙方使用者進行查核，確認地址裡的餘額是足夠進行交易的，等於我們知道某人的銀行帳戶號碼即可公開查詢其帳戶裡的餘額有多少，

DOI:10.6814/NCCU201901043

等個人敏感的資訊，因此每筆交易與當事人真實身分是相互連結的。但於比特幣的交易中，交易雙方並不清楚各自的身分，如同股票市場上只顯示股票交易量和時間，但成交的雙方對於是何人出賣或買受股票無從知悉，而比特幣即是透過公鑰匿名的方式以達成此項特性[6]。

第二節 區塊鏈之運作原理

第一節介紹區塊鏈技術最早的應用-比特幣之特色，此節則要針對比特幣所運用之核心與基礎架構-區塊鏈作解析。

區塊鏈最重要的核心價值在於去中心化的特色，若將抽象的技術概念具體為現實事物，區塊鏈其實就是一個去中心的帳本資料庫系統，這個帳本並非僅指狹義上有金流記載的交易資訊，而是廣義地包含實務上任何有價值的資料記載，只是因為區塊鏈最早應用於比特幣等商業上的運行，僅因外界將其類比為帳本，而帳本上記載的可能是銀行業客戶的交易資訊、證券業的股票交割資訊或地政機關關於不動產買賣登記的資訊，任何需要進行資料交換、溝通的產業，都有機會透過區塊鏈進行實作。

第一項 區塊鏈之區塊

傳統網際網路進行傳輸的最小資料單位稱為「封包」，區塊鏈中記錄資料的最小單位則稱為「區塊」，每一個區塊記錄著許多資訊，包含區塊的容量大小

另外 Google 工程師 Michele Spagnuolo 甚至開發出應用軟體 BitIodine 以解析區塊鏈中的資訊以追查使用者的來源，因此使用者於區塊鏈中並非無法追蹤，而是追蹤難度增加。因此如何兼顧使用者隱私與礦工之查核需求即是區塊鏈面臨的發展困境，而零知識證明即是解決此困境的突破性技術，礦工無須知道交易上的細節如匯款者、收款者和金額即可驗證交易，惟目前運算時間、運送量龐大，因此使用尚未普及。

[6] Satoshi Nakamoto, *supra* note 3, at 1.

DOI:10.6814/NCCU201901043

(Block Size)、區塊頭(Block Header)、該區塊包含的交易總數(Transaction Counter)及這個區塊在這個區塊中的交易資訊(Transactions)。

Block Size (4 bytes) 區塊的容量大小	
Block Header(80 bytes)	Version (4 bytes)
	Previous Block Hash (32 bytes)
	Merkle Root (32 bytes)
	Time Stamp (4 bytes)
	Difficulty (4 bytes)
	Nounce (4 bytes)
Transaction Counter (1-9bytes)	
Transactions	記錄此區塊中的每筆交易之資訊 Hash 值 Tx1：Hash Tx2：Hash Tx3：Hash ……

圖 1：區塊鏈之區塊結構

(資料來源：https://ppt.cc/fRdW3x 工研院資訊與通訊研究所)

Block Size：區塊的容量大小。

Block Header：區塊頭的資料主要作為工作量證明的輸入資料。

Version：主要用來追蹤區塊鏈協議升級的版本號碼。

Previous Block Hash：從前一個區塊的區塊頭資料計算而得到的 Hash 值，也因為每個區塊有前一個區塊的區塊頭資料，使得每個區塊產生連結，藉以確保了區塊序列的正確性和連動性。

Merkle Tree Root：區塊中所有交易資料透過 Merkle Tree 演算法所得的根節點 Hash 值。

Time Stamp：該區塊的時間戳記。

Difficulty：該區塊工作量證明演算法的困難程度。

Nounce：表示已進行的工作量證明演算法的次數。

DOI:10.6814/NCCU201901043

Transaction Counter：該區塊包含的數量。

Transactions：該區塊所記錄的交易資料，以 Hash 值記錄在區塊中。

第二項　區塊鏈之技術

區塊鏈結合了多種演算法技術，這些技術並非 Satoshi Nakamoto 首創[7]，但 Satoshi Nakamoto 卻是第一個將它們巧妙地結合並應用在實際案例-比特幣的先鋒者。這些技術分別為共識機制、公開金鑰加密演算法、Merkle Tree、時間戳，以下是上述四種區塊鏈關鍵核心技術的介紹：

一、共識機制

資訊科技的時代，商業交易能透過網際網路隨時隨地進行，交易記錄透過中間機構的資料庫統一管理和記錄，以維持帳本內容的唯一性和正確性，但若中間機構出現問題，如駭客入侵、內部人疏失，使得資料被篡改、竊取甚至整個資料庫系統被癱瘓時，此種中心化管理的模式，容易造成「單點淪陷、全部淪陷」(Single Point of Failure, SPOF)的弊病，亦容易使中間機構的損害擴散至網路上的每個節點，因此區塊鏈最大的特色即是建構一個不需要第三方介入，即可驗證數據資訊之正確性的分散式帳本系統，成功解決互聯網最讓人擔憂之安全信任問題。

區塊鏈分散式帳本系統中，並無一個中心機構處理資訊之記錄和交換，因此每個節點都是中心，各自都擁有一本完整帳本且帳本上記載的資訊都是相同

[7] 「工作量證明共識機制」概念最早由 Cynthia Dwork 和 Moni Naor 於 1993 年提出，並由 Markus Jakobsson 與 Ari Juels 於 1999 年發表；「公開金鑰加密演算法」概念最早由 Ralph C. Merkle 於 1974 年提出，Whitfield Diffie 與 Martin Hellman 以此基礎於 1976 年發展出公開金鑰加密系統，兩人並於 2005 年獲得有電腦界諾貝爾獎之稱的圖靈獎(Turing Award)，以表彰其對現代密碼學之貢獻；』「Merkle Tree」由 Ralph C. Merkle 於 1976 年提出，提升巨量資料驗證的效率。

DOI:10.6814/NCCU201901043

的，但交易發生後，帳本的資訊勢必需要進行變更，為了確保各帳本的資訊能同步更新且達到內容一致性，每個節點不能同時進行記帳的動作，因交易隨時都在發生，網路上的延遲會導致各節點接受資訊的時間並不相同，若同時記帳必然會造成帳本的不一致[8]，因此由一個節點取得記帳的權力才不會導致帳本資訊更新的混亂。至於該由誰取得記帳的權力，即是區塊鏈共識機制所欲解決的，目前區塊鏈共識機制之主要設計有以下四種：

(一)、POW (Proof-of-work) 工作量證明機制

POW 機制所使用是雜湊現金函數演算法(Hashcash algorithm)，透過單向雜湊函數概念，使得給予一個任意大小的 X 值時，能得到一固定大小且相應的 Hash 值：H(X)，但外界難以由此 Hash 值回推得到 X 值。

將上述單向雜湊函數難以回推之特性包裝成一個數學難題，考驗各節點所欲付出的努力程度和誠意，每個節點透過本身的計算能力競逐解題[9]，並由最先解出題目之節點將答案和交易內容廣播給其他節點進行驗證，若驗證成功，則大家形成共識，由這個最先解出題目的節點取得將資訊儲存在區塊中之記帳權。

然而，競逐解題而取得記帳權的過程需要付出大量的運算資源和成本，因此 Satoshi Nakamoto 設計了一套激勵機制，給予解出題目的節點比特幣獎勵，提供誘因以鼓勵爭取記帳的權利，並為每一筆資料進行驗證。這也是第一個區塊鏈應用-比特幣設計的巧妙之處，除透過此種方法達成共識外，亦讓不願付出工作量擔保的節點無法參與分散式帳本的維護，以截堵詐欺行為的產生[10]。

---

[8] 張健，揭秘比特幣和區塊鏈：什麼是區塊鏈？，參考網址：https://read01.com/zh-tw/a00e7m.html#.Wrny-cOuzIV (最後瀏覽日：2019 年 7 月 1 日)

[9] 比特幣區塊鏈稱此過程為「挖礦」。

[10] Satoshi Nakamoto, *supra* note 3, at 3.

DOI:10.6814/NCCU201901043

(二)、POS(Proof-of-stake)

POW 依照「運算能力」取得共識，各個節點憑藉本身的運算資源競逐解題以決定誰能取得記帳權之共識；POS 則是依照「權益」取得共識，當一個節點，願意投注越多代幣於此系統中，則越有機會獲得記帳的權利[11]，但若被發現有偽造交易資訊的駭客行為，則其投注的代幣將被沒收，此設計也是與 POW 最大不同之處，讓駭客的詐欺行為付出代價，進而保障系統的安全，目前以太坊所建構之區塊鏈應用即是採取此種共識機制[12]。

(三)、DPOS(Delegated Proof-of- stake)

DPOS 與 POS 原理相似，皆依照權益多寡決定記帳之權利，但 DPOS 規定每個節點須投票選出代理人，類似股東投票選出董事會成員，獲得票數前幾位的超級節點將代理眾多節點行使記帳和驗證之權利，此舉將能大幅縮減參與記帳或驗證節點之數量，以增加共識驗證的效率[13]。

(四)、PBFT（Practical Byzantine Fault Tolerance）

上述三種共識機制適用於公有鏈上，優點是有較佳的驗證安全性缺點是處理速度慢，效率較差。在聯盟鏈(許可鏈)的情形，各個節點互相認識或已經過事先身分的認證，因此推定各個節點是可信的，則使用 PBFT 將能提升區塊鏈驗證的效率。

PBFT 又稱為拜占庭容錯，每個收到訊息的節點都會廣播予其他節點，並不斷進行訊息的交換和交互的驗證，透過嚴格的證明演算法，將能確保其餘可

---

[11] 許明恩，礦工失業倒數：以太坊轉型權益證明機制，參考網址：https://reurl.cc/pDdA8 (最後瀏覽日：2019 年 7 月 1 日)

[12] Vitalik Buterin ,A Proof of Stake Design Philosophy, available at：https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51 (Last visited on 2019/07/01)

[13] Weusecoins, Delegated Proof-of-Stake Consensus, p2, available at：https://www.weusecoins.com/assets/pdf/library/Delegated%20Proof-of-Stake%20Consensus.pdf

DOI:10.6814/NCCU201901043

信的節點最後達成一致的共識，並識別出有問題的節點，惟此機制適用的前提是有問題的結點不能超過 1/3，因此只能適用於聯盟鏈(許可鏈)此等已事先經過節點身分審核的類型[14]。

(五)、零知識證明

區塊鏈發展目前遇到的最大瓶頸是隱私和驗證查核無法兼顧，雖然區塊鏈號稱安全、匿名，但如比特幣和以太坊的區塊鏈設計，交易者的地址和交易紀錄皆設定為公開，方便礦工在每筆交易前進行查核以確認每個地址的餘額，雖然沒有直接連結個人的身分，但透過目前大數據技術仍可間接推知使用者之個人背景資料，因此有論者認為比特幣只有假名交易的安全性而沒有達到真正匿名交易的安全強度，為了兼顧使用者對於交易內容隱私的需求和區塊鏈礦工的查核需求，零知識證明的技術於焉而生[15]。

零知識證明是一種能將上述交易資料隱藏的情況下，礦工亦能進行查核的技術，麻省理工學院多媒體實驗室(MIT Media Lab)舉了一個有趣的例子解釋這個不可思議的概念[16]，Alice 手上有兩顆撞球，分別是綠色和紅色，除了顏色這兩顆撞球不管是球半徑、重量、觸感皆一模一樣。假設 Bob 是紅綠色盲，在 Bob 眼中 Alice 手上拿的是兩顆一模一樣的撞球，Alice 為了說服 Bob 兩顆撞球是不一樣的，則提議 Bob 可以背對著她並隨意交換兩顆球後，讓她識別原本拿在 Bob 左手的球是哪一顆，由於 Alice 不是色盲，所以不管 Bob 將兩顆球如何快速混淆，Alice 皆能快速分辨，重複幾次後，Bob 就越能相信這兩顆球一定有

---

[14] Miguel Castro & Barbara Liskov(1999), Practical Byzantine Fault Tolerance, MIT's Computer Science Lab, p3-6, available at：http://pmg.csail.mit.edu/papers/osdi99.pdf

[15] Malte Möser(2013), Anonymity of Bitcoin Transactions, p1, available at：https://pdfs.semanticscholar.org/e1ae/d9296c3af9139f48d15e043e2e8beab55409.pdf

[16] Google 的共同創辦人 Sergey Brin 曾在 Bitfury Group 舉辦之 2018 年摩洛哥塊鏈高峰會(2018 Blockchain Summit in Morocco)稱讚此項技術非常神奇和不可思議，參考網址：https://www.facebook.com/watch/?v=833730016827103 (最後瀏覽日：2019 年 7 月 1 日)

DOI:10.6814/NCCU201901043

什麼地方不同[17]。而於區塊鏈的應用中，用戶使用零知識證明技術說服礦工他們的帳戶有足夠的金額，只是他們看不到而已，藉此兼顧用戶隱私和礦工驗證的需求。

目前虛擬貨幣 Zcash 即是採用此種技術，但運算成本高且交易速度慢，尚未普及，不過當今使用者對於隱私的需求性高，此技術未來的發展指日可待[18]。

二、公開金鑰加密演算法

公開金鑰加密演算法又稱為非對稱式加密，係指加密和解密並非使用同一把金鑰。使用者擁有一把公開金鑰和一把私密金鑰，僅公開金鑰公開放置於網路上傳送，私密金鑰則是各自擁有而不進行交換，因此僅公開金鑰被竊取之風險較高[19]，縱使公開金鑰不幸被竊取，竊取者仍無法使用該公開金鑰而推知私密金鑰，故資料傳輸的安全性高。

金鑰的長度越長，再輔以因式分解函式、橢圓曲線函數等加密技術越不易被破解，常見的公開金鑰加密演算法如 RSA 和 ECC(Elliptic Curve Cryptography，橢圓曲線加密演算法)，而區塊鏈使用的即是 ECC 中的 ECDSA(Elliptic Curve Digital Signature Algorithm，橢圓曲線數位簽章演算法)，ECDSA 能提供較短之金鑰長度而達到如同 RSA 一樣的安全強度[20]。

---

[17] Neha Narula,Willy Vasquez,Madars Virza(2018),zkLedger: Privacy-Preserving Auditing for Distributed Ledgers, available at：https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/5aa1b35ce4966bd538d3f1d2/1520546653653/zkledger.pdf (Last visited on 2019/07/01)

[18] Zcash, What are zk-SNARKs?, available at：https://z.cash/technology/zksnarks/ (Last visited on 2019/07/01)

[19] 私鑰由各自的電腦儲存，不藉由網路傳送，失竊風險較低，但並非全然無風險，尤其個人電腦插上網路線即有可能受到駭客入侵，因此有建議使用離線儲存(又稱冷儲存)之方法以確保私鑰之安全性。

[20] 量子電腦的興起被認為會帶給密碼學威脅，Penta 區塊鏈實驗室奠基人 Steve Melnikoff 教授

DOI:10.6814/NCCU201901043

三、Merkle Tree

Merkle Tree 是一種節省儲存空間和資料交換的二元樹資料結構，根節點的 Hash 值由兩個中間節點的 Hash 值組合而成，每個中間節點的 Hash 值亦由它的兩個子節點的 Hash 值組合而成，因此底層資料有任何變動，即會從葉節點傳遞至根節點，以此方式歸納海量資料成為一個簡短的 Hash 值，不僅能縮減資料儲存的空間，亦能提升資料傳輸的效率。

上述機制應用於區塊鏈之大量交易當中，每組交易資料都是一個節點，藉由兩兩一組形成新的 Hash 值方式，重複進行，直到產生最終一組的 Hash 值，此 Hash 值即是 Merkle Tree 的根，此值亦會被記錄於區塊頭(Block Header)中的 Merkle Root 欄位，並作為每一筆交易資料的代表數值且僅佔 256 位元(32Byte)的儲存空間，當進行資料驗證時，僅須針對此 Hash 值進行檢查和運算，不僅減少運算資源的消耗，亦提升了區塊鏈交易的速度[21]。

甚至預言最快於 2027 年 POW 共識採用的橢圓曲線數位簽章演算法就會被量子電腦破解。屆時，量子電腦於十分鐘內即可從公鑰推導出私鑰。不過目前仍有科學家如 Daniel Bernstein 抱持樂觀態度認為現今密碼體系未來經過優化後仍可抵抗量子電腦；知名密碼學家 Bruce Schneier 亦認為量子電腦在技術上和實用性仍有許多挑戰且加密和解密技術的發展是相運而生，當量子電腦興起，勢必會有新的技術被發明出來對抗它。

[21] 駱建功、吳大智、周師文、呂有勇，數位貨幣與區塊鏈，駱建功出版社，2017 年 9 月 28 日，頁 45。

DOI:10.6814/NCCU201901043

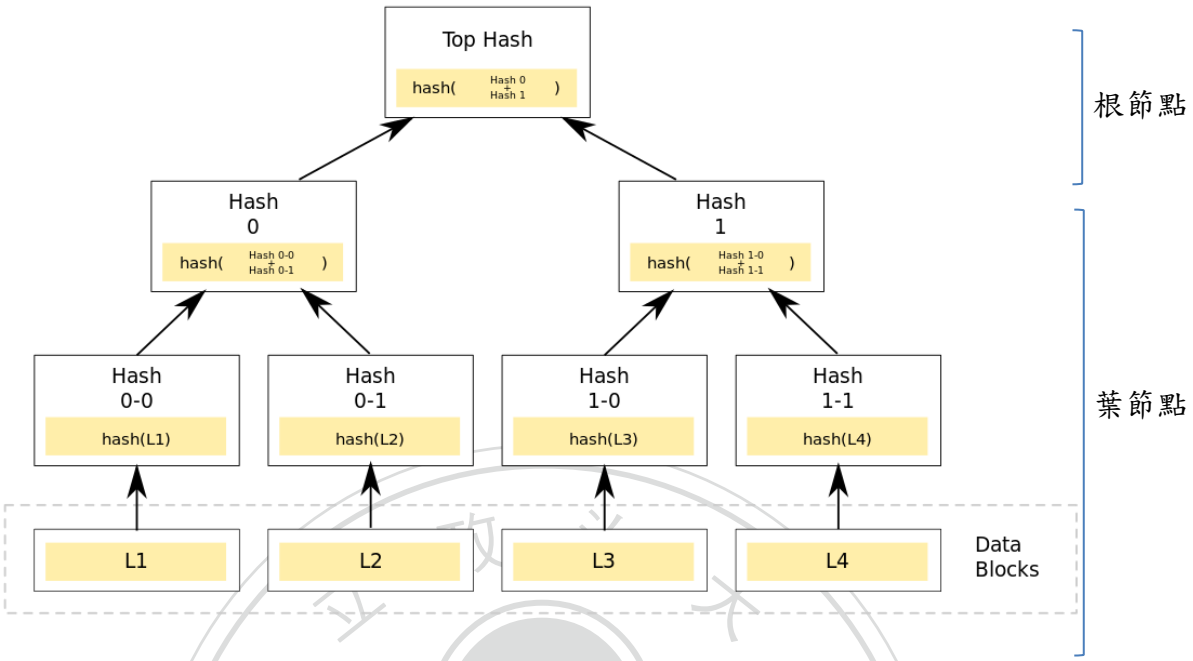

圖 2： Merkle Tree 資料結構示意圖

(資料來源：https://goo.gl/DEr4Mn)

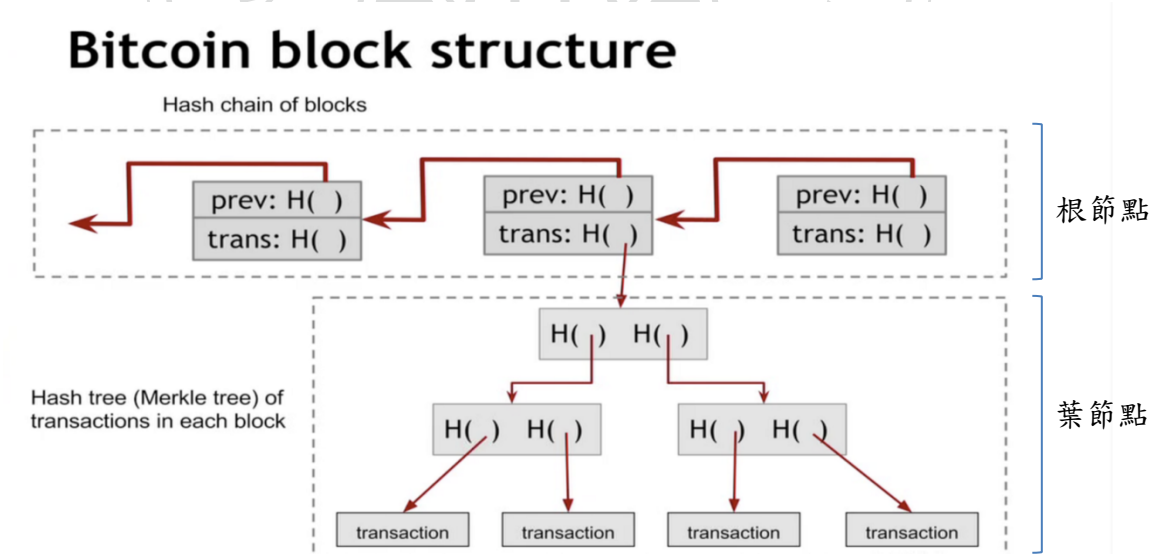

圖 3：Bitcoin 中的 Merkle Tree 資料結構示意圖

(資料來源：https://ppt.cc/fFgyWx)

DOI:10.6814/NCCU201901043

四、Timestamp Server(時間戳)

Timestamp 代表著該區塊產生的時間，有如現實世界的郵戳，使用時間標記以證明區塊資料在特定時間之有效性，並保證區塊鏈上每個區塊依序相連。此外，Timestamp 亦是區塊頭的一個欄位，透過與區塊頭(Block Header)的資料進行雜湊函數 Hash 運算後，成為下一區塊 Previous Block Hash 欄位中的數值，形成彼此相互牽連的一個資料區塊鏈序列，牽一髮動全身，任一區塊的資料遭到變動，皆會連動影響其他區塊，因此形成了一個不可篡改、不可偽造的資料庫。

第三節 區塊鏈之類型

目前區塊鏈類型可區分為開放式區塊鏈(Permissionlesss Blockchain)和認許制區塊鏈(Permissioned Blockchain)，兩者最大差別在於區塊鏈網絡是否處於隨時得自由加入新節點的狀態。

第一項 開放式區塊鏈 (Permissionlesss Blockchain)

又可稱為公有鏈(Public blockchain)，對全世界所有人開放，任何人皆可查閱帳本、發起交易且驗證交易的區塊鏈。

公有鏈常見的共識機制有工作量證明機制(POW)和權益證明機制(POS)，完全的去中心化且每個人可透過競逐記帳權和驗證交易的方式獲得一定的經濟獎勵，以維持分散式帳本的永續經營，屬於此類型的區塊鏈如比特幣或以太幣。

第二項 認許制區塊鏈 (Permissioned Blockchain)

又可稱為私有鏈、須授權之區塊鏈或聯盟鏈，非對全世界所有人開放，每

DOI:10.6814/NCCU201901043

個節點須通過審核並獲得授權後方能加入，並被賦予不同的角色和權限[22]，因此並非每個節點都有查閱帳本、發起交易、驗證等權限。此外，由於私有區塊鏈網路的節點是經過嚴密篩選，有些甚至為實名制，因此不需如比特幣等公有鏈使用 POW 共識機制透過所有節點競逐記帳權並共同驗證的方式確保信任和交易安全的問題，而是預先指定某個節點進行交易的驗證，類似傳統透過可信任之中心機構處理和驗證資訊的方式，以改善公有鏈因 POW 共識機制所耗費的大量資源和時間，提升私有鏈運作之效率[23]，屬於此類型的區塊鏈如銀行 Ripple 聯盟、超級帳本(Hyperledger)[24] 等。

第四節 區塊鏈之主要應用

區塊鏈作為一種資訊交換的協定，有別於傳統中心化的資料交換模式，去中心化的本質能解決許多產業的最大痛點-信任和透明，以下六個應用場景被認為是抽象區塊鏈技術具體作為真實可行的商業模式熱門案例。

第一項 金融領域應用

金融業從傳統銀行負責資金供需，保險業設計保險商品，證券業有價證券

[22] Zetzsche, Dirk A. and Buckley, Ross P. and Arner, Douglas W., The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain (August 13, 2017), p11, available at：https://ssrn.com/abstract=3018214

[23] Nolan Bauerle, What is the Difference Between Public and Permissioned Blockchains?, available at：https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains (Last visited on 2019/07/01)

[24] Ripple 是由 Ripple Labs Inc.透過區塊鏈所建立的認許制私有鏈-跨境即時總結算系統(Real-time gross settlement system)，能在幾秒內完成跨境交易並即時結算，目前全球約有 70 間銀行加入，包括渣打銀行(Standard Chartered)、三菱日聯金融集團(MUFG)、加拿大皇家銀行(RBC)、澳大利亞國民銀行(NAB)等；超級帳本(Hyperledger)是由 Linux 基金會發起之區塊鏈跨行業開源項目，旨在打造企業用之認許制區塊鏈底層標準，成員包括日立（Hitachi）、IBM、英特爾（Intel）、荷蘭銀行(ABN AMRO Bank)、三星(Samsung)、FedEx 等

DOI:10.6814/NCCU201901043

交割、清算等，涉及多方的清算流程、複雜的數據分析和風險控管，因此區塊鏈去中心化、不可竄改、高安全性等特徵正可為金融領域處理複雜的資訊交換、清算流程和風險分析，並使金流、資訊流透明化，改善以往由系統後台的中央管理者全權掌握此等交易資訊並造成顧客對於資料是否外洩之疑慮，因此金融產業被認為是區塊鏈影響甚鉅的領域之一。

一、 銀行徵信

銀行作為資金供需之中介角色，深深影響一國商業活動和經濟發展，而貸款客戶違約所導致銀行損失的信用風險，長久以來一直是銀行所欲解決的問題，其來自於銀行選擇客戶不當，因此發展出徵信制度，意即對於人事物進行信用調查的方法。

應用情境：客戶徵信資料共享

傳統銀行徵信的最大問題在於徵信機構間的對於客戶徵信資訊缺乏共享機制，重複對於單一客戶進行徵信，不僅造成銀行徵信成本提高，且於銀行與客戶間資訊不對等的情況，亦讓銀行無法針對不同客戶提供不同的金融服務需求。究其原因有二[25]，一、銀行同業間競爭激烈，深怕因資訊共享而導致商業機密之洩漏；二、各國都有個人資料隱私保護的規定，但資訊傳輸技術尚未能安全的傳輸資料，因此各機構間的共享將使得客戶資訊外洩疑慮增加，恐造成客戶之信任危機。

區塊鏈分散式儲存、共識機制和數位簽章加密演算法的特點，將個人資訊主權下放給客戶，由其決定是否授權給徵信機構或銀行進行資料之取用(Information access)，且讓機構-客戶間和機構-機構間之資訊交換安全獲得保障，不僅降低銀行重複徵信之成本，更讓客戶之個人資訊由傳統中心機構把持

[25] 騰訊研究院，區塊鏈在徵信業應用的探討：優勢與特點及場景分析，參考網址：https://read01.com/nNQ2Qn.html#.WsGcGi6uzIV (最後瀏覽日：2019 年 7 月 1 日)

DOI:10.6814/NCCU201901043

的情形轉變為客戶擁有對個人敏感資訊的自主權，消弭對於銀行的不信任，進而讓更多人進入金融服務網絡，使得普惠金融的理想有實現可能。

二、 保險業務

保險係指面臨同類型危險之人，透過組成共同團體的方式，匯聚成員間資金，藉以滿足個別成員損失的補償需要，而達成分散風險之制度。然保險商品的訂價取決於風險的精算，因此當一項風險難以估計或不敷成本，保險公司將選擇不予承保，因此造成某些生活上的未來不確定性風險無法獲得轉移和保障。

應用情境：班機遲誤保險

傳統保險公司決定是否承保時，須蒐集和了解客戶個人資訊，以防止詐欺情事發生。保險事故發生後，客戶亦須提供相關佐證資料以讓保險公司進行審核，因此冗長的核保至理賠過程所製造的成本，讓許多客戶買了保險卻不去申請理賠。

根據英國民航局數據顯示[26]，2014 年 6 月至 2015 年 5 月間，在 9000 班次航班中，約有 90 萬人達到申請班機延誤保險之標準，但只有不到 558000 人向保險公司申請理賠。

以區塊鏈技術建構之智能合約將能解決這個問題，讓核保至理賠過程中之資料傳輸更為安全便利，並結合物聯網(IOT)蒐集班機延誤資訊，因此當智能合約中班機延誤之條件成就，觸發合約，旅客將能自動獲得理賠，讓理賠過程程式化、透明化、自動化，不僅客戶能有效獲得保險服務保障，亦重建客戶對於保險公司之信任，對於保險公司商譽的增加不言而喻。

[26] Dan Hyde, Half a million missing out on flight delay compensation, available at https://www.telegraph.co.uk/news/shopping-and-consumer-news/11790143/Half-a-million-missing-out-on-flight-delay-compensation.html (Last visited on 2019/07/01)

DOI:10.6814/NCCU201901043

三、 資產證券化

金融產品證券化係指銀行將共同特徵或流動性低的資產，透過信用評等機制之搭配，將其重新包裝成單位化證券型式予以出售[27]，使金融機構籌資成本降低並藉此轉移違約風險、流動性風險、及利率風險等諸多風險。

應用情境：不動產證券化

不動產證券化係指將不動產所有權人持有不動產之抽象物權法律關係，轉變為持有表彰經濟效益之有價證券，由原本僵固之固定資產型態轉化為可供轉讓之證券型態，藉由證券發行之方式出售於交易市場以獲取融資，大為增加其流動性和價值[28]。但傳統上因資產價值的評估、資產運營狀況皆仰賴信評機構、第三方估價者、受託機構等中介機構的訊息發布，投資人難以去查證訊息之真實性和正確性，因而產生了信任的鴻溝，降低市場交易之活絡性。

未來透過區塊鏈技術去中心化、不可篡改之特性記錄資產運營狀況、分紅狀況，讓投資人信賴市場呈現的資訊是真實且非偽造的，不僅可提高投資人交易的意願，亦能有效促成資金的流動以活絡融資市場。

四、跨境支付[29]

傳統跨境支付交易速度和效率低落，究其原因有三，一、涉及不同國家之金融機構、貨幣；二、每個國家結算和清算程序不盡相同；三、結算和清算程

---

[27] 金融監督管理委員會銀行局，關於金融資產證券化，參考網址：https://www.banking.gov.tw/ch/home.jsp?id=116&parentpath=0,8,115 (最後瀏覽日：2019 年 7 月 1 日)

[28] 金融監督管理委員會，關於不動產證券化，參考網址：https://www.banking.gov.tw/ch/home.jsp?id=279&parentpath=0,8,119&mcustomize=onemessages_view.jsp&dataserno=21786&aplistdn=ou=data,ou=business,ou=one,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=Business (最後瀏覽日：2019 年 7 月 1 日)；中華民國信託業商業公會，不動產證券化，參考網址：http://www.trust.org.tw/content/index.asp?pno=187 (最後瀏覽日：2019 年 7 月 1 日)

[29] 麥肯錫大中華諮詢業務，區塊鏈—銀行業遊戲規則的顛覆者，2016 年 5 月，頁 10。

DOI:10.6814/NCCU201901043

序仰賴人工對帳，導致每一筆匯款資料需要 2-3 天才能到帳，並須支付高額的手續費。

區塊鏈去中心化和點對點之資料傳輸方式，將使跨境支付系統無需中介金融機構處理結算和清算業務，因此可達到交易即清算(Real-time settlement)、全天候 24 小時不間斷服務，除了提升交易速度和效率[30]之外，流程也更加透明。因此，根據麥肯錫大中華業務報告《區塊鏈—銀行業遊戲規則的顛覆者》，若區塊鏈應用在 B2B 跨境支付交易中，將可使每筆交易成本從 26 美元降至 15 美元[31]，大幅降低跨境交易之成本和摩擦力。

第二項　供應鏈領域應用

供應鏈係指產品由最初的原料至銷售商品給消費者間所有活動之環節，亦即包含原料、設備、生產、庫存、銷售、售後服務等事項[32]，上游原料供應商至中下游的製造商、零售商藉由訊息的傳遞以制定良好的生產策略以滿足顧客的需求，但因供應鏈涉及物流、資訊流、資金流多方層面的管理，訊息容易產生偏差[33]，以至於風險成本相當高且難以預測，進而影響金融機構對其徵信的準確性。

[30] 全球第一筆基於區塊鏈的銀行間跨境匯款在傳統支付模式中需要 2 到 6 個工作日，但使用了 Ripple 的技術，8 秒之內即完成了交易。
原文網址：https://kknews.cc/zh-tw/finance/ommne4m.html

[31] 麥肯錫大中華諮詢業務，同註 22，頁 10。

[32] 經濟部標準檢驗局，ISO 28000 供應鏈安全管理系統標準簡介，參考網址：www.bsmi.gov.tw/wSite/public/Data/f1388125037366.pdf (最後瀏覽日：2019 年 7 月 1 日)

[33] 此為供應鏈管理中著名的長鞭效應，係指供應鏈廠商所得的需求訊息與真實市場的顧客需求產生偏差，以至成本加重、風險倍增。

DOI:10.6814/NCCU201901043

應用情境：中小供應商融資

傳統供應鏈上的中小企業融資困難，究其原因有二[34]，一、金融機構對於非核心供應商之下游中小企業須透過進出貨資料、發票憑證或其他營業資料進行交叉比對分析後，才能驗證其是否為供應鏈上之夥伴並評估其還款能力，故徵信成本高；二、中小企業之借貸多為短期周轉資金，金額小，但金融機構稽核之成本高，放貸意願低；三、金融機構融資流程效率低，驗證流程加上後續的撥放款可能須費時數周，不敷中小企業短期資金供應的需求，導致中小企業多轉向與影子銀行[35]進行融資。

透過聯盟區塊鏈之設立，將銀行和供應鏈上之廠商一起加入到區塊鏈技術構築的資訊交換平台，基於區塊鏈資料不可篡改特性，供應鏈上中下游廠商交易資訊的真實度和透明度將能獲得保障，銀行對於借方之徵信成本不僅大為降低，亦能精確評估風險，有利於對中小供應商融資服務的設計，並解決現行供應鏈金融雙方資訊不對等和交易資訊不透明之痛點。根據研究指出[36]，傳統供應鏈金融僅能為 15%供應鏈上的中小供應商提供融資服務，但使用區塊鏈技術後，將有 85%之中小供應商能獲得金融機構提供之資金挹注，促進產業之活絡發展。

---

[34] 王妍文，當供應鏈金融遇上區塊鏈，誰能吃下新商機？，參考網址：http://www.ftrc.nccu.edu.tw/wordpresseng/?p=3439 (最後瀏覽日：2019 年 7 月 1 日)；黃嶠濛，區塊鏈+供應鏈金融：旨在打造供應鏈金融資產的交易所，參考網址：https://zhuanlan.zhihu.com/p/31216243 (最後瀏覽日：2019 年 7 月 1 日)

[35] 影子銀行 (shadow banking) 係指功能與傳統銀行相似，但卻不受法規、監理主關機關監管的金融中介機構，類似我國所謂的當鋪、地下錢莊、民間借貸或高利貸等。

[36] 林建甫，供應鏈金融 促進新南向金融版圖擴張，參考網址：https://m.ctee.com.tw/album/4c8c65b0-5bd2-4ec7-8a6c-9447a11812bc/828080 (最後瀏覽日：2019 年 7 月 1 日)

DOI:10.6814/NCCU201901043

第三項　數位版權領域應用

1990 年個人電腦和物聯網的興起，讓傳統以錄音帶、錄影帶、CD、DVD 的娛樂產業產生重大的變化，MP3、AVI、WMV 等數位檔案格式的發展更讓大眾從原本至實體店面買專輯、租影片的消費習慣轉而直接於雲端網路上下載，雖然取得產品變得方便，但也讓著作的保護變得不易，盜版、版權侵權充斥，連帶影響到著作人的權益和創作的意願。

應用情境：音樂版權

著作財產權的權利內容豐富，可分為重製權、改作權、編輯權、出租權、散布權、公開播送權、公開傳輸權、公開口述權（語文著作）、公開上映權（視聽著作）、公開演出權（語文、音樂或戲劇、舞蹈著作、現場表演）、公開展示權（未發行之美術著作或攝影著作）等[37]。

現今著作人多透過授權的方式讓被授權人得以在一定的授權時間、地區、範圍內對於著作財產權利用收益，並向被授權人收取使用報酬，增加著作之經濟價值和使用範圍，而授權方式又可分為專屬授權和非專屬授權，尤其「專屬授權」的方式讓被授權人雖未取得著作財產權，但得以「著作財產權人之地位」行使權利，因此被授權人擁有授權他人利用著作之權利[38]。

實務上，流行音樂（詞、曲）的著作財產權人多將音樂著作之「重製權」交由詞曲經紀公司處理重製權授權事宜；音樂著作之「公開播送、公開演出、公開傳輸」等著作財產權則交由著作權集管團體進行管理、授權。

---

[37] 經濟部智慧財產局，著作權基本概念篇，參考網址：https://www.tipo.gov.tw/ct.asp?xItem=219595&ctNode=7561&mp=1 (最後瀏覽日：2019 年 7 月 1 日)

[38] 章忠信，著作利用與授權之疑義解析，參考網址：http://www.copyrightnote.org/ArticleContent.aspx?ID=9&aid=2540

DOI:10.6814/NCCU201901043

著作財產權與民法一般財產權相比，擁有多元之權利內容已如上述，且授權方式除了基於法規明定之專屬授權和非專屬授權外，實務上私人以契約自由訂定授權方式亦為常見，牽涉的權利主體廣泛，加上近年來數位平台興起，更讓音樂版權之授權錯綜複雜，整體合法授權之過程相當繁瑣與費時[39]。

但透過區塊鏈分散式帳本技術，將數位內容和行使權利分配的相關資料，例如：著作人資訊、歷年作品、著作財產權利用人、權利人分配、授權的時間、範圍及地區等[40]記錄在區塊鏈上，基於區塊鏈資料不可篡改之特性，權利金流向、授權歷史等皆資訊能公開透明，方便大眾進行後續的追蹤調查，以解決傳統音樂版權晦暗不明之亂象。

第四項　身分識別領域應用

傳統上使用者為了使用政府或商業所提供的服務以進行經濟活動時，皆被要求須詳實填寫個人資料並提供相關身分證明，以利真實身分的勾稽，例如：政府自然人憑證、數位貨幣交易所註冊之身分證明、網購網站個人資料和信用卡資料等。現今多元的網路平台，讓個人經濟活動得以延伸至世界各個角落，但也造成每當我們使用一項新的網路平台所提供的服務時，須重複登錄個人資料且這些資料分散儲存於各大平台資料庫中，使用者無法真正擁有和控制自己的身分和隱私。

應用情景：分散式識別系統

「身分」對於一個人來說，是在社會行使各項權利的憑藉，例如獲得教育、醫療照護、金融服務、就業等，在高度發展國家中，公民身分是由一個健

[39] 余至浩，【臺灣區塊鏈應用實例】克服音樂版權難題第一步，靠區塊鏈解決授權分散痛點，參考網址：https://www.ithome.com.tw/news/119249 (最後瀏覽日：2019 年 7 月 1 日)

[40] 余至浩，同註 21。

DOI:10.6814/NCCU201901043

全政府所認可，但對於第三世界長期處於內亂、外患、天災以致於流離失所的國際難民而言，其所處區域政權更迭頻繁且多未經和平、合法轉移，使得他們的身分常隨著另一政權的殞落而消失，造成他們連合乎人性尊嚴的人權都無法獲得。

區塊鏈技術建構的分散式識別系統(Decentralized Identifiers，DIDs)，去中心化、資料不可篡改和不可否認等特色，讓使用者真正擁有「數位身分自主權」[41]，無須再依賴政府授與身分，只須掌握身分專屬的私鑰即能在任何地方擁有自我證明的權利；此外，在高度發展國家，原本散落在多個平台的數位身分因而得到整合且能進行同步更新，並在使用者主動授權下，將資訊透露給各類服務商使用[42]，使用者從服務商取回對個人資料的自主權利，解決目前因網路攻擊而導致個人資料外洩或服務商利用使用者個人資料進行不法獲利之情事。

第五項　教育領域應用

教育是一個國家興盛的關鍵，透過初等、高等教育體系的建置和證書的核發，證明個人於本科專業上的能力，並作為政府、公司行號舉才的基準，方得適才適所地妥善運用人力資源以促進經濟發展。但證書目前仍多以紙本的形式核發，易於毀損和偽造，不利於作為永久公示外觀的憑藉。

應用情景：學歷證明

傳統上學歷證明都以紙本形式蓋上戳章作為表徵，但此方式在現今數位科技發達的今日極易被偽造，且對許多公司行號和應徵者來說，驗證應徵人學歷

[41] Christopher Allen, The Path to Self-Sovereign Identity, available at https://www.coindesk.com/path-self-sovereign-identity/ (Last visited on 2019/07/01)

[42] 胡一天，數位身分與區塊鏈記憶體，參考網址：http://www.storm.mg/article/116734 (最後瀏覽日：2019 年 7 月 1 日)

DOI:10.6814/NCCU201901043

是否真實的過程相當費時，不僅應徵人須帶畢業證書影本至原學校進行檢核、認證、蓋印證明，公司行號的人資亦須花費時間進行核實和比對，當求職者為數眾多且來自不同國家，這樣的核實過程將更為複雜和繁瑣。

但未來將考試成績、學習課程記錄在教育體系區塊鏈上，不可篡改特性讓學歷證明偽造的機會大為降低且省去人工核實的時間成本，將能促進徵才效率和減少偽造學歷和詐欺的情形發生。

第六項　慈善領域應用

慈善是一種道德關懷，對於有需要的人給予幫助並不求回報，因此許多私人團體藉由組織形式集結人力、物力、財力，並進行統籌分配，補足政府福利制度所未能關懷的族群，由於事涉大眾的捐款和善心，因此組織和財務的透明化程度關係著眾人的愛心是否被濫用和社會福利制度能否延續，倘若信任瓦解，社會大眾不願意捐款，將對於弱勢族群的扶助有著重大的衝擊。

應用情景：慈善捐款

傳統上慈善捐款背後代表著可能是一種宗教信仰和對機構主事者的仰望，當民眾將捐款至捐款箱後，對於金流的流向是較不關注的，因為他們信任這個機構或機構領導人的德望。但公民意識抬頭的今日，這樣的方式受到挑戰，尤其多數慈善機構並不會主動公開財務報告和年度決算書，捐款金流的流向備受質疑，造成大眾對於慈善捐款是否真正用在需要幫助的弱勢團體有所疑慮[43]。

以區塊鏈記錄每筆捐款資訊，不可篡改、不可偽造和可追溯特性，讓捐款的流向和用途公開透明地呈現在大眾面前，不僅能消弭疑慮亦能提升大眾對於

[43] 2015 年慈濟慈善事業基金會因財務不透明受到各界抨擊，衛福部當時並無法源依據(財團法人法甫於 2018 年 6 月 27 日三讀通過)，因此衛福部未曾委託會計師進行財務查核，引起大眾對於慈善事業財務透明的關注。

DOI:10.6814/NCCU201901043

慈善機構的信任，讓慈善捐款率獲得成長以形成一個正面之社會循環[44]。

[44] 翁書婷，我們要呼籲慈濟用區塊鏈處理大眾的捐款嗎？，參考網址：https://www.bnext.com.tw/article/44124/should-tzuchi-start-to-consider-adopting-blockchain-technology-for-the-transparency-of-the-charity-donation (最後瀏覽日：2019 年 7 月 1 日)

DOI:10.6814/NCCU201901043

第三章 區塊鏈應用之監理

區塊鏈為資訊交換的協定，是基於多項資訊科技演算法之綜合運用，其擔保著數位環境中資訊交換的真實性和正確性，在商業應用中尤其重要，而第二章第四節所舉的案例皆是得以區塊鏈實作的可能商業應用場景，讓雙方在看不到彼此的情形下仍可藉由區塊鏈技術中的數位簽章確認發送資料的來源和資料的真實、正確性，而這也正是區塊鏈技術的核心，因若無法證實雙方在虛擬的數位環境中確有意思表示的存在或無法證實其真實性，則後續的法律行為和法律關係皆無法開展。

此外，區塊鏈有著去中心化、不可竄改和安全性高的特色，其核心價值在於「信任」，傳統中心化的治理模式過度信賴中心節點，這個中心節點可能是一個資料庫、一台路由器或是一台主機等終端裝置，但背後維護管理的皆是由「人」負責進行，人易受外界環境影響，但演算法不會，區塊鏈使用者信任的是「演算法」，沒有感情、沒有情緒，有的只是嚴謹的規則，區塊鏈將「人」這個不確定因素所生之影響降到最低，亦顛覆傳統中心管理模式的概念，其引領的第四次工業革命所帶動的商業模式創新週期相較於以往的工業革命更是縮短許多，應以何種新的監理思維和分析框架去看待區塊鏈技術所開展的法律關係是本文所欲先建立的前提，在此前提再去分析區塊鏈與現行電子簽章法之相容性，方得以正確的思維和態度看待該問題，以避免失焦與紊亂。

第一節 區塊鏈應用所生之風險

區塊鏈去中心化防止中心機構的腐敗所帶來的損害；資料不可竄改性確保資料的完整性；可驗證之匿名讓電子交易安全得以安全無虞。但水能載舟亦能覆舟，其衍生的風險亦是制定監理戰略思維時應納入考量的範圍。

DOI:10.6814/NCCU201901043

一、個人隱私保護

開放式區塊鏈中，一筆資料由區塊鏈全體節點共同驗證通過後，每個節點會同步更新各自的帳本，以維持帳本的一致性，但這也表示每個節點對於交易資料皆有訪問權，縱使上面的主要資料如交易當事人、位址皆以 Hash 值表現，經過多次交易後，透過大數據的分析，亦能建構擁有此地址的交易當事人的行為模式；在認許制區塊鏈中，節點的加入需經過組織認可，並須與真實身分進行連結，因此個人於網絡上的行為足跡將清晰可見。此外，兩種類型區塊鏈維持帳本的方式是各節點皆擁有一本完整帳本，帳本需要更新時，再以共識機制確認同步更新的步調和標的，因此帳本資訊各個節點都能掌握，使得區塊鏈仍有侵害個人隱私之虞[45]。

二、網路攻擊

區塊鏈本身的機制能確保交易的安全和資料交換的完整性，但區塊鏈的應用非僅指底層的區塊鏈技術，還包含以此底層技術構建的應用系統和終端使用者[46]。

(一)暴力攻擊法(brute force attack)

在開放式區塊鏈中多數使用 POW 共識機制，由各節點藉由本身的運算能力競逐解題，由最先解出題目之節點將答案和交易內容廣播給其他節點進行驗證，因此當某節點掌握 51%算力時，即能比其他人先行算出答案，並將偽造的交易資料廣播給其他節點進行確認，而其他節點就只能依照其所廣播的偽造資料進行再一次的比對，而無法發現原始的交易資料其實已遭竄改。

51%攻擊的主要目的是為了讓一筆錢能進行兩次花費(double-spending)，如

[45] Zetzsche, Dirk A. and Buckley, Ross P. and Arner, Douglas W., *supra* note 21, at 14-15.

[46] 杜宏毅，如何建置一個實用的區塊鏈平台，財金資訊季刊，第 90 期，2017 年 10 月，頁 45，參考網址：https://www.fisc.com.tw/Upload/b0499306-1905-4531-888a-2bc4c1ddb391/TC/9006.pdf

DOI:10.6814/NCCU201901043

同手中僅擁有 50 元卻可以連續至兩個商店以此 50 元購得商品，換言之，你可以得到總價值 100 元的商品卻僅須付出一半(50 元)的成本。

而此攻擊方式是利用區塊鏈中最長鏈合併規則(longest chain rule）所達成的。區塊鏈中並非只靜態地存在一條鏈，當有兩個礦工同時對於同筆交易解出答案而獲得記帳權，則會產生分叉而出現兩條鏈，但為避免分叉無限產生並破壞帳本的一致性，因此以最長鏈合併規則比較兩條鏈的長度，最長者始被認為是合法且正確的區塊鏈帳本，也因為這個規則的採行讓攻擊者有機可乘。

攻擊者(本身也是礦工)會先發起一筆移轉所有權或給付之交易(100BTC)，這筆交易會先進入待確認交易區，當經過其他礦工驗證後，即會寫上目前大家已有共識的區塊鏈版本(簡稱 A 鏈)，但同時攻擊者擁有強大算力，所以總能先解出答案而獲得記帳權以製作區塊，但因攻擊者未將答案廣播，因此其他礦工並不知道攻擊者私自維護著一條自己的鏈(簡稱 B 鏈)，且刻意不將這筆 100BTC 交易寫上 B 鏈，當攻擊者靠著強大算力快速累積區塊於自己維護的鏈上，且長度長於 A 鏈，則攻擊者的 B 鏈依照最長鏈規則即會成為大家主要依循的區塊鏈版本，而此鏈上攻擊者並未將自己原本花費 100BTC 之交易上鏈，所以這筆 100BTC 看似未曾被使用過，攻擊者即能再次使用此 100BTC 進行消費[47]。

三、人為操作風險

(一)上鏈資料的正確性

以區塊鏈網絡保存資料，須先透過終端使用者利用 API(Application Programming Interface，以下簡稱 API)或 AP(Access Point，以下簡稱 AP)閘道登入區塊鏈系統，並輸入資料。

因此區塊鏈雖然能保障資料的完整並且不被竄改，但前提是輸入的資料是

[47] Jimi S. ,Blockchain: how a 51% attack works (double spend attack), available at：https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474 (Last visited on 2019/07/01)

DOI:10.6814/NCCU201901043

正確且無缺陷的，但鏈下資訊上鏈前所經由的 API 或 AP 閘道本身並無法提供像區塊鏈技術一樣的安全性，因此容易成為駭客攻擊之目標，例如 Mt.GOX 交易所遭受駭客攻擊而損失價值約 875 萬美元的比特幣即是交易所建構的錢包和系統平台安全性有所缺陷，而無關區塊鏈帳本本身[48]。

(二)人為疏失

根據 2018 年企業資安報告，資安風險有 56%來自人為疏失[49]，區塊鏈由程式開發人員建立與維護，開發人員若未盡注意義務，造成程式碼或演算法有所缺陷，亦連帶影響區塊鏈的安全性，因此人員的專業、管理亦是維持區塊鏈安全的重要因子之一。

此外，使用者藉著外部應用系統連結區塊鏈系統，由於區塊鏈系統本身使用區塊鏈技術，具備高度安全性；但外部應用系統未使用區塊鏈技術，因此當其資訊安全防護措施未能達到區塊鏈技術所能達到的標準時，而使用者又無資訊安全的意識時[50]，即會成為駭客之目標，而形成區塊鏈平台架構中的弱環節(weak link)。

第二節 區塊鏈應用之國際監管趨勢

區塊鏈應用從 2008 年中本聰發表的分散式電子支付現金系統開始，比特幣此等虛擬貨幣因具有類似貨幣之功能，其定性成為了各國遇到的第一個區塊鏈應用之法律問題；隨即 2014 年以太坊首次代幣發行(Initial Coin Offering，以下

---

[48] Zetzsche, Dirk A. and Buckley, Ross P. and Arner, Douglas W., supra note 21, at 16.

[49] iThome, 2018 企業資安調查，參考網址：https://www.ithome.com.tw/article/122191 (最後瀏覽日：2019 年 7 月 1 日)

[50] 賽門鐵克調查報告顯示，資料外洩約有 5 成比例是人為疏失造成。參考網址：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7108 (最後瀏覽日：2019 年 7 月 1 日)

DOI:10.6814/NCCU201901043

簡稱 ICO)募集了 31,591 個比特幣（當時市值 1,840 萬美元），是當時第二成功的 ICO 專案[51]，並於 2015 年中推出區塊鏈平台－以太坊 (Ethereum)，讓使用者可以透過簡單的應用程式發佈智能合約，其白皮書中更將此平台命名為「新一代智能合約與分散式應用平台」(A Next-Generation Smart Contract and Decentralized Application Platform)，並強調智能合約為其平台的特色[52]，因此虛擬貨幣、ICO、智能合約可以說是區塊鏈技術早期的應用，而這三項元素建立起區塊鏈商業關係中所需要的基本三元素：貨幣、募資和契約，因此本文選擇這三個領域作為國際監管趨勢探討的標的，觀察美國、歐盟和其他國家對於區塊鏈應用的監理措施，以歸納目前國際對於區塊鏈應用可能的監理思維和態度。

一、 虛擬貨幣的定性

(一) 美國

1、FinCEN (Financial Crimes Enforcement Network)

FinCEN 是第一個對虛擬貨幣發表意見的聯邦政府單位，於 2013 年發佈 FIN-2013-G001 號指引(Guidance)，認為虛擬貨幣如同通貨[53](currency)一樣可以作為交換之媒介，但缺少通貨的某些功能，特別是無法作為法償貨幣(Legal tender)而有法律上清償債務之效力。

但因為虛擬貨幣如比特幣，可與法償貨幣互相進行轉換，是具有價值的「可轉換虛擬貨幣」[54]，因此須受到美國銀行保密法(Bank Secrecy Act)[55]的拘束

---

[51] Coinnounce, 15 insights on how Ethereum conducted its ICO in 2014, available at：https://coinnounce.com/ethereum-ico-2014/ (Last visited on 2019/07/01)

[52] 陳恭，智能合約的發展與應用，財金資訊季刊第 90 期，2017 年 10 月，頁 33。

[53] 專指由國家發行之貨幣，貨幣則是較為廣義之概念。

[54] 可轉換虛擬貨幣(convertible virtual currencies)又稱為開放式虛擬貨幣(open virtual currencies)

[55] 美國銀行保密法(Bank Secrecy Act,簡稱 BSA)，有時亦被稱為 AML(anti-money laundering law)或聯合稱為 BSA/AML。

DOI:10.6814/NCCU201901043

而負有提供相關交易報告的義務以防止洗錢之情形發生[56]。

2019 年 FinCEN 發佈了首次針對未註冊的比特幣交易所的行政罰鍰，其原因在於其未依銀行保密法(Bank Secrecy Act)向主管機關申請核准進行貨幣服務業務(money services business (MSB))，亦未建立有效之反洗錢計畫、可疑活動報告和貨幣交易報告[57]。

2、IRS(US federal fiscal agency Internal Revenue Service)

IRS 認為虛擬貨幣是一種「資產」(Property)，當出售或交易虛擬貨幣時，即應被課予資本利得稅[58]。此舉可能造成比特幣囤積而不利流通，但相較於美國聯邦所得稅率最高上限為 39.6%，長期資本利得稅最高上限為 20%，因此比特幣視為一種資產而非收入反而利於比特幣之持有者[59]。

3、CFTC(the Commodity Futures Trading Commission)

2015 年 CFTC 認為虛擬貨幣是一種「商品」(commodities)[60]，並受商品交易法(Commodity Exchange Act ,CEA)之監管，為具有交換之媒介(a medium of exchange)、帳戶單位(a unit of account)和價值儲存(a store of value)等類似通貨之

---

[56] US Department of the Treasury, Guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies(March 18, 2013), available at：https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering

[57] FinCEN，FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws(April 18, 2019), available at：https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money

[58] Internal Revenue Service, Notice 2014-21(March 21, 2014), p2, available at：https://www.irs.gov/pub/irs-drop/n-14-21.pdf

[59] The Guardian, Bitcoin to be treated as property instead of currency by IRS, available at：https://www.theguardian.com/technology/2014/mar/25/bitcoin-property-currency-irs-rules(Last visited on 2019/07/01)

[60] U.S Commodity Futures Trading Commission, In the Matter of Coinflip, Inc d/b/a Derivabit and Francisco Riordan, CFTC Docket No. 15-29 (September 17, 2015), available at：https://www.cftc.gov/PressRoom/PressReleases/pr7231-15

DOI:10.6814/NCCU201901043

功能，惟仍無法償性[61](Legal tender)。

2018 年 9 月美國 Massachusetts 地方法院認為 My Big coin(MBC) 被控挪用販賣虛擬貨幣所獲得之資金購買古董、美術品、珠寶等奢侈品一案中，認為 CFTC 有權調查和起訴關於虛擬貨幣市場詐欺之行為。此外，依據商品交易法「商品」係指有形商品如黃金、棉、油或無形的服務、權利和利益[62]，而 MBC 所發行的虛擬貨幣亦符合商品之定義[63]，因此其買賣受到商品交易法之監管，不得有詐欺消費者之行為。

4、SEC (Securities and Exchange Commission)

2017 年 SEC 將虛擬貨幣定義為一種數位價值之表徵，並具有交換之媒介(a medium of exchange)、帳戶單位(a unit of account)和價值儲存的功能，但不具法償之性質。迄今為止，此為美國聯邦層級監管者中最具實質性之定義[64]。

5、Digital assets-existing law (State of Wyoming)

懷俄明州於 2019 年 3 月通過數位資產法案，將數位資產分為三類：數位消費資產（Digital Consumer Assets）、數位證券（Digital Securities）和虛擬貨幣（Virtual Currencies），並承認虛擬貨幣的法償貨幣地位[65]，為美國第一個承認虛

---

[61] U.S Commodity Futures Trading Commission, Customer Advisory: Understand the Risks of Virtual Currency Trading(December 15, 2017) , available at：https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory_urvct121517.pdf

[62] U.S Commodity Exchange Act §1a(9), 'The term "commodity" means wheat, cotton, rice, corn, oats, barley, rye, flaxseed, grain sorghums, mill feeds, butter, eggs, Solanum tuberosum (Irish potatoes), wool, wool tops, fats and oils…and all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in.'

[63] U.S Commodity, Futures Trading Commission Federal Court Finds that Virtual Currencies Are Commodities, available at：https://www.cftc.gov/PressRoom/PressReleases/7820-18

[64] Securities and Exchange Commission, Report of Investigation under 21(a) of the Securities Exchange Act of 1934: The DAO(25 July 2017), p3, available at：https://www.sec.gov/litigation/investreport/34-81207.pdf

[65] Digital assets-existing law§101(a)(i)(ii)(iii).

DOI:10.6814/NCCU201901043

擬貨幣為金錢(Money)的州政府[66]。

(二)歐盟

1、ECB(European Central Bank)

認為虛擬貨幣非法定貨幣，而是一種以數位形式代表某種價值的貨幣替代物且未受主管機關之監管，主要由該幣之發行者或社群所控制或發行[67]。

2、EBA(European Banking Authority)

EBA 認為虛擬貨幣是一種價值的數位形式表徵，不須由中央銀行或政府發行，亦不須依附於法償貨幣，即可作為電子支付、交易或價值交換或儲存的方式，並為法人或自然人所接受。

EBA 對虛擬貨幣採取保守態度，不鼓勵虛擬貨幣的持有或交易之行為，並提出四點建議[68]：

(1) 應為每種虛擬貨幣規劃一個計畫治理機構(scheme governance authority)，此治理機構是一個非政府組織，負責管理，並同時對監管者負責。

(2) 虛擬貨幣業者應遵循客戶盡職調查(Customer due diligence)[69]、資本要求與市場濫用之相關規範。

(3)歐盟每個國家應授權計畫治理機構進行虛擬貨幣之管理。

(4)應建立虛擬貨幣交易之保證和退款機制。

---

[66] Esther Kim, Wyoming becomes first to give Bitcoin owners full property rights, available at：https://bitcoinist.com/wyoming-bitcoin-full-property-rights/ (Last visited on 2019/07/01)

[67] European Bank Authority, Virtual currency schemes – a further analysis (2015), p13,25, available at：https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[68] European Bank Authority, EBA Opinion on 'virtual currencies(4 July 2014), p39-44, available at：https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+ Opinion+on +Virtual+ Currencies.pdf

[69] 客戶盡職調查(Customer due diligence)與了解客戶(Know your costomer)政策是國際防範洗錢之兩大基石。

DOI:10.6814/NCCU201901043

2015 年 EBA 建議將虛擬貨幣納入洗錢防制指令(Anti-Money Laundering Directive,AMLD)的監管範圍[70]。

2017 年 EBA、歐洲證券及市場管理局(European Securities and Markets Authority, ESMA)和歐洲保險和職業養老金管理局(European Insurance and Occupational Pensions Authority, EIOPA)更聯合發表聲明表示虛擬貨幣因無中央銀行或任何公共機構(Public authority)作為擔保，不具有法定貨幣之地位，此外虛擬貨幣目前不受歐盟法律的監管，消費者無法得到法律之保護，因此具有高風險性[71]

3、EC(European Commission)

EC 贊成 EBA 所提出的上述四點建議，並對虛擬貨幣之定義採取與 EBA 相同之立場[72]。

4、EP(European Parliament)

EP 於 2016 年 5 月通過一份決議(resolution)，建議應對虛擬貨幣採取合比例的監管手段，不宜過度，以避免對於新技術的成長造成阻礙或增加額外之法遵成本[73]。

---

[70] European Bank Authority, Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849, available at：https://eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD

[71] ESMA, EBA and EIOPA , ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies, available at：https://eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf

[72] European Commission, Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC COM/2016/0450 final - 2016/0208 (COD), available at：https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0450

[73] European Parliament resolution of 26 May 2016 on virtual currencies (2016/2007(INI)) §14, available at：http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-

DOI:10.6814/NCCU201901043

5、CJUE(The Court of Justice of EU)

CJUE 在 2015 年 10 月 22 日 Skatteverket v. David Hedqvist 一案中裁定，根據增值稅(VAT) 歐盟增值稅指令第 135 條第 1 項對於關於法償貨幣、紙鈔、硬幣交易之豁免條款規定[74]，比特幣不需繳納增值稅。這表示比特幣被視為一種貨幣而非商品[75]。

另判決指出，虛擬貨幣是一種支付工具且具有雙向流通之性質，傳統貨幣與虛擬貨幣之間的轉換是不同支付方式之間的交換，但與以傳統記帳單位表示如歐元的電子金錢不同，虛擬貨幣使用的是虛擬的記帳單位。

挪威、德國也相繼於 2017 年、2018 年遵循歐洲法院之裁定取消對比特幣課徵增值稅[76]。

二、 首次代幣發行(Initial Coin Offering, 以下簡稱 ICO)

ICO 係指業者透過區塊鏈技術發行自己的代幣以募集投資者的比特幣、以太幣等具有市場價值的虛擬貨幣，而未來投資者可使用此業者發行的代幣換取業者研發之商品、服務或表彰一定之權利[77]。

0228+0+DOC+XML+V0//EN

[74] Article 135 (1)(e) of the EU Directive 2006/112/EC of 28 November 2006：EU member states shall provide a VAT exemption for “transactions, including negotiation, concern-ing currency, bank notes and coins used as legal tender, with the exception of collectors’ items, that is to say, gold, silver or other metal coins or bank notes which are not normally used as legal tender or coins of numismatic in-terest.”

[75] Stéphane Blemus, Law and Blockchain：a legal perspective on current regulatory trends worldwide(January 17, 2018), p3, available at：https://ssrn.com/abstract=3080639

[76] Kevin Helms , Bitcoin Transactions Declared VAT-Exempt in Norway, available at：https://news.bitcoin.com/bitcoin-transactions-declared-vat-exempt-in-norway/ (Last visited on 2019/07/01)； Nikhilesh De, Germany Won't Tax You for Buying Coffee With Bitcoin, available at：https://www.coindesk.com/germany-considers-crypto-legal-equivalent-to-fiat-for-tax-purposes/ (Last visited on 2019/07/01)

[77] 臧正運、曾宛如、方嘉麟，從區塊鏈融資論眾募規範趨勢，月旦法學雜誌，第 273 期，2018

DOI:10.6814/NCCU201901043

此種新型募資方式與傳統金融市場募資方式-首次公開募股(Initial Public Offering，以下簡稱 IPO)類似，具有資訊不對稱或詐欺之風險，因此是否須受證券法規之監管各國莫衷一是。

(一)美國

美國 SEC 於 2017 年發表一份針對 2016 年 DAO 遭駭事件的官方報告，截至這份報告出爐之前，國際間對於這種新興科技所帶來的新型募資型態如何監管仍處於不知所措的觀望狀態，因此美國這份調查報告所持的 ICO 監管態度對於各國政府至關重要。

美國 SEC 認為，根據 1933 年證券法和 1934 年證券交易法，DAO 所發行之代幣(DAO tokens)應被認為是一種投資契約(Investment contract)而視為廣義之證券[78]。

根據美國 1933 年證券法第 2(a)(1)規定：「證券係指票據、股票、庫藏股、期貨、債券、債權證明、任何利潤分享之協議、擔保品信託證書，認股證明、可轉讓之股份、投資契約、表決權信託證書證券存款證明、石油部分未分割之權利、或任何通認為證券之權益或工具。」1934 年證券交易法第 3(a)(10)與 1933 年證券法對於證券之定義大致相同，惟衍生性金融商品眾多，上述兩個法案對於證券之例示性定義已不敷使用，因此美國聯邦最高法院於 1946 年 Securities and Exchange Commission v. W.J. Howey Co.一案中發展出 Howey Test 對投資契約作最廣義之概括性規範，以合理適切地將新興募資工具納入證券交易法之監管範圍[79]。2017 年美國 SEC 針對 DAO 事件之報告亦以 Howey Test 作為判斷 DAO 發行代幣的募資手段是否符合投資契約的構成要

年 2 月，頁 89。

[78] Securities and Exchange Commission, *supra* note 63 , at 1.

[79] 王聖雯，ICO 市場的法律問題與監管研究，元照出版社，2018 年 9 月，頁 39-40。

DOI:10.6814/NCCU201901043

件；2019 年 4 月 FCA 更進一步發布關於數位資產的投資契約分析架構(Framework for 'Investment Contract' Analysis of Digital Assets)，臚列下述四項以說明 Howey Test 於數位資產的分析架構和考量因素：

1、 金錢之投資(an investment of money)

投資可採現金或其他非現金方式為之，如提供貨物、服務等。而數位資產藉由販售或交換而獲取對價，對價之形式可為真實法定貨幣或其他數位資產，不管是何種形式，皆屬投資行為的一種[80]。購買 DAO 代幣以換取以太幣之行為可視為一種價值之投資(contribution of value)，係以數位資產換取其他數位資產，因此構成金錢投資的要件[81]。

2、 資金必須投資於一個共同事業(in a common enterprise)

共同事業係指事業發起人和投資者間具有水平關係和垂直關係。水平關係強調各個投資者將資產匯集於一事業上而彼此命運共同，並按比例分配利潤；垂直關係則強調事業發起人和投資者間的財富依存關係，發起人之成功與投資人之獲利有直接關聯性，投資人亦承擔了發起人經營事業之風險[82]。

DAO 是一個營利組織，發行者發起募資專案並發行 DAO 代幣以換取以太幣，而投資者以持有的以太幣換取 DAO 代幣，當專案成功，投資者能藉由手中的 DAO 代幣表彰的所有權或投票權之價值的升高，而獲取利潤，DAO 投資者間因共同投資此專案而有水平關係，DAO 發起人之成敗因與投資者有直接關聯性，均符合投資一共同事業之定義。

3、 投資人有獲益之期望(with an expectation of profits)且利潤之有無全然來自於他人之努力(solely from the efforts of others)

---

[80] Securities and Exchange Commission, Framework for "Investment Contract" Analysis of Digital Assets (April 3, 2019), p2, available at：https://www.sec.gov/files/dlt-framework.pdf

[81] Securities and Exchange Commission, *supra* note 63, at 11.

[82] Securities and Exchange Commission, *supra* note 63, at 2.

DOI:10.6814/NCCU201901043

SEC 認為此項是影響數位資產是否為投資契約的主要因素，又可分為兩項進行探討[83]：

(1)仰賴他人之努力(Reliance on the Efforts of Others)

a.投資者是否期望倚賴發起人之努力而獲利。

b.投資人所倚賴的發起人之努力事項是否為重要事項，而非僅為內部重要性不高的事項。

另有以下輔助因素：

a. 重要的事項如開發、維護、管理是否由發起人所負責，而非委由分散式社區的使用者共同為之。

b. 發起人是否握有發行或消滅數位資產之權利以對其於市場價格有決定性影響。

c. 發起人是否主導數位資產發展，例如決定數位資產社區的治理模式、程式碼更新、第三方如何參與交易驗證等。

(2)合理獲益之期望(Reasonable Expectation of Profits)

在 Howey Test 中所謂利潤(Profits)並非僅指藉由外部市場力量造成供需升降而使得價格有所升跌而產生的利益。而應考量下列因素，當具有下列情形則越可能視為有合理獲益之期望：

a. 數位資產是否賦予投資人分享企業獲利之權利。

b. 數位資產是否能在次級市場轉讓或交易。

c. 投資者合理期待數位資產會因發起人之努力而增值。

d. 發起人發行數位資產是否超過市場實際所需求的數目，而提供潛在購買者作為投資之目的。

e. 數位資產的價格升跌與能轉換為此數位資產的一般商品或服務的市價

[83] Securities and Exchange Commission, *supra* note 63,at 2-4.

DOI:10.6814/NCCU201901043

並無關聯性。

投資人獲益與否仰賴 DAO 代幣發行者的專案執行、行銷和專業能力，投資人買入代幣皆以匿名為之，投資人間無法集中投票權於某一標的，此外 DAO 代幣擁有者的投票權和所有權受到限制，綜合上述，因此專案能否獲利實際上仰賴 DAO 發行者之意願和執行能力；又關於獲利之期望，DAO 代幣能自由轉讓，其手中代幣的價值亦取決於 DAO 發起人專案執行成功與否，此外 DAO 發起人亦透過宣傳管道告知投資者 DAO 是一營利事業，其目標是為專案提供資金以支持相關服務和商品之發展，投資者日後能以購買之代幣優先享有業者開發成功之服務、商品或資本利得。

(二)歐盟

目前尚無歐盟機構針對 ICO 採行任何措施，僅有 ESMA 於 2017 年強調 ICO 公司應遵循以下四項法規[84]：

1、招股說明書指令 (Prospectus Directive)

2、金融市場指令 (the Markets in Financial Instruments Directive)

3、替代投資基金經理指令(the Alternative Investment Fund Managers Directive (AIFMD))

4、第四次反洗錢指令(the Fourth Anti-Money Laundering Directive)

ESMA 於 2019 年提出的建議指出，加密資產[85]市場的規模目前尚不會影響金融體系的穩定，但對加密資產投資者的保護感到擔憂[86]，建議加密資產和加

[84] European Securities and Market Authority, ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements (November 13, 2017), available at：https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf

[85] 加密資產根據 ESMA 定義，係指由區塊鏈技術發展而出的一種私有資產，類型包含比特幣或透過 ICO 方式所發行的虛擬貨幣。

[86] European Securities and Market Authority, ESMA's Advice On Initial Coin Offering And Crypto-Assets, p39, available at：https://www.esma.europa.eu/sites/default/files/library/esma50-157-

DOI:10.6814/NCCU201901043

密資產之間的交換服務提供商與 ICO 提供商等金融服務應列入洗錢防制指令的範圍[87]。此外，ESMA 建議對於不符 MiFID II(Markets in Financial Instruments Directive 2004/39/EC)定義下之金融商品(Financial instruments)[88]而不受監管之特定類型加密資產，不應放任不管，而應制訂特別規則以控管風險[89]。

(三)中國

中國央行、中央網信辦、工業和信息化部、工商總局、銀監會、證監會和保監會於 2017 年 9 月 4 日的聯合公告中指出，依據《中華人民共和國人民銀行法》、《中華人民共和國商業銀行法》、《中華人民共和國證券法》、《中華人民共和國網絡安全法》、《中華人民共和國電信條例》、《非法金融機構和非法金融業務活動取締辦法》等法律法規，ICO 本質是一種未經批准且非法公開的融資行為，其涉嫌非法發售代幣票券、非法發行證券以及非法集資、金融詐騙、傳銷等違法犯罪活動，並自此公告日起所有 ICO 融資均應停止進行[90]。

三、 智能合約

智能合約一詞由學者 Nick Szabo 於 1996 年提出，並定義為一個可執行的電腦化交易協議，Nick Szabo 也以自動販賣機作為例子說明智能合約係指依照內建之條款或條件，透過電腦軟硬體自動化執行，而無須藉由第三人之協助[91]，如同自動販賣機透過內建程式與消費者進行互動，當消費者投入 10 元並按下按鈕，將觸發機器內建程式並依照對應的按鈕和投入之金額而打開特定商品閘門讓商品自動滑落至取物口。

1391_crypto_advice.pdf

[87] *Id.* at 36.

[88] MiFID II 列舉之金融商品共計 11 種，例如可轉讓證券(Transferable securities)等。

[89] *Id.* at 40

[90] 中華人民共和國工業和信息化部，七部門關於防範代幣發行融資風險的公告，參考網址：http://www.miit.gov.cn/n1146290/n4388791/c5781140/content.html (最後瀏覽日：2019 年 7 月 1 日)

[91] 陳恭，同註 49，頁 33-34。

DOI:10.6814/NCCU201901043

智能合約是一種電子化契約，雙方並無書面或口頭上之要約與承諾，因此是否為具備法律上拘束力之契約即有爭論。

(一)美國

1、the Arizona House Bill 2417

2017 年 3 月通過法案，是美國第一個承認智能合約合法性的州，於電子交易法章節增訂第 44-7061 條，明定智能合約可用於商業交易，並承認其法律上效力、合法性、可執行性[92]。

2、the Tennessee Senate Bill 1662

2018 年 3 月通過法案，於電子交易法章節增訂第 47-10-202 條，與 the Arizona House Bill 2417 相似，明定智能合約可用於商業交易，不能僅因契約是透過智能合約執行而否認其法律上效力、合法性、可執行性[93]。

3、the Nevada Senate Bill 398

2017 年 6 月通過法案，於電子交易法章節增訂第 719 條，明定區塊鏈係指電子紀錄藉由分散式節點共同進行資料驗證，並以密碼學方式進行加密儲存。而智能合約即屬由區塊鏈技術所加密和儲存的一種電子紀錄，具有法律上效力[94]。此外區塊鏈的使用不須取得州政府的許可執照亦不須課予稅收[95]。

---

[92] Arizona Revised Statutes§ 44-7061(c), 'Smart contract" means an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger.'

[93] Tennessee Code §47-10-202(c), 'Smart contracts may exist in commerce. No contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract contains a smart contract term.'

[94] Nevada Senate §719, ' "Blockchain" means an electronic record of transactions or other data which is: 1.Uniformly ordered;

2.Redundantly maintained or processed by one or more computers or machines to guarantee the consistency or nonrepudiation of the recorded transactions or other data; and

3.Validated by the use of cryptography.'

[95] Nevada Senate §244(1),' A board of county commissioners shall not:

DOI:10.6814/NCCU201901043

(二)歐盟

歐盟尚未針對智能合約有相關立法，但 2016 年 EP 通過對於虛擬貨幣之決議[96]後，EC(European Commission)緊接著於同年 11 月成立金融科技內部工作小組[97]，並增加相關預算以支持和促進區塊鏈相關研究和計畫[98]；2018 年 10 月 EP(European Parliament)通過非立法性決議案(non-legislative resolution)[99]強調智能合約是區塊鏈重要的應用之一，呼籲 EC 應對其法律效力和未來可能產生的法遵問題進行評估，並向國際技術標準的相關組織如 ISO,、ITU、 CEN-CELENEC 合作，建立智能合約之技術標準[100]。

(三)中國

中國最高人民法院審判委員會於 2018 年 9 月通過「最高人民法院關於互聯網法院審理案件若干問題的規定」，肯認電子數據透過區塊鏈、電子簽名、可信

(a) Impose any tax or fee on the use of a blockchain by any person or entity;
(b) Require any person or entity to obtain from the board of county commissioners any certificate, license or permit to use a blockchain; or
(c) Impose any other requirement relating to the use of a blockchain by any person or entity.

[96] 請參照註 40

[97] R. Viola and O. Guersent, European Commission sets up an internal Task Force on Financial Technology, available at：https://ec.europa.eu/digital-single-market/en/blog/european-commission-sets-internal-task-force-financial-technology (Last visited on 2019/07/01)

[98] European Parliament, "Answer given by Vice-President Ansip on behalf of the Commission", Parliamentary questions(2017), available at：http://www.europarl.europa.eu/doceo/document/E-8-2016-009012-ASW_EN.html

[99] European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation, available at：http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0373&language=EN&ring=B8-2018-0397

[100] European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)), available at ：http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0373&language=EN&ring=B8-2018-0397

DOI:10.6814/NCCU201901043

時間戳、Hash 值等方法的蒐集，具有證據能力[101]。

此外，中國國家互聯網信息辦公室更於 2019 年 1 月 10 日公布「區塊鏈信息服務管理規定」，詳列區塊鏈服務提供者未來應遵守的營運規定，其中影響層面最大的是區塊鏈服務使用者須以身分證字號或手機號碼進行註冊認證，方能使用相關服務，不願進行身分認證之使用者，區塊鏈業者不得提供服務。

上述兩項規定並未明文肯認智能合約於法律上之效力，僅承認電子數據的蒐集能以區塊鏈等數位科技方式為之且區塊鏈相關服務納入政府監管範圍，至於電子數據或區塊鏈的定義和範圍未見於規定中，後續最高人民法院發表之「最高人民法院關於互聯網法院審理案件若干問題的規定的理解與適用」[102]中亦未對此作出解釋，因此智能合約在中國是否具有法律上之效力，仍有待中國政府進一步釋疑。

第三節 區塊鏈應用應有之監理思維

從第二節區塊鏈應用之國際監管趨勢得知，各國目前仍傾向針對各種區塊鏈應用事件作各別規範，如比特幣是通貨(Currency)、資產(Property)、商品(Commodities)或是證券的認定而適用稅法、證券交易法等；智能合約是否具有法律上之拘束力等。但此以個案事件的發生而作個案性的行政解釋或立法，乃如同俗諺所說頭痛醫頭，腳痛醫腳，卻忽略根本性的共通問題，即區塊鏈技術本身所使用的交換協定方式或數位簽章，能否作為無法看到對方情形下一種擔

[101] 最高人民法院關於互聯網法院審理案件若干問題的規定第 11 條：「當事人提交的電子數據，通過電子簽名、可信時間戳、哈希值校驗、區塊鍊等證據收集、固定和防篡改的技術手段或者通過電子取證存證平台認證，能夠證明其真實性的，互聯網法院應當確認。」

[102] 中國最高人民法院，《最高人民法院關於互聯網法院審理案件若干問題的規定》的理解與適用，參考網址：https://www.chinacourt.org/article/detail/2018/09/id/3489797.shtml (最後瀏覽日：2019 年 7 月 1 日)

DOI:10.6814/NCCU201901043

保契約當事人意思表示合致的方式，否則植基於此技術上的所有商業應用法律關係將都失所附麗，因此本文嘗試建立區塊鏈監理議題的中心思維和分析框架，以避免如同現今針對技術應用之法律關係或法律行為進行規範，卻忽略基礎法律規範是否賦予此技術應用於虛擬環境中作為代表意思表示合致而具有法律上效力的問題。

第一項 監理中心思維-差異化監理

金融科技係指以電腦程式技術去實現一個金融業的商業模式[103]，而區塊鏈是驅動金融科技關鍵的底層技術，雖然區塊鏈最早的應用是以金融支付為出發點，但其可應用的情境相當廣泛，任何需要資料交換的產業皆可使用區塊鏈而達到公開透明和安全，因此區塊鏈所帶來的商業模式的改變和風險內容的變動，將促使監理的複雜程度大為提高。而面對區塊鏈所驅動的金融科技浪潮，不應將既有的監管規則直接適用於區塊鏈新創產業，而應隨著產業特性不同而做出差異化監理。

而因產業特性不同而為不同之監理措施是否會造成歧視或不平等，著名的法律經濟分析學家亦為美國聯邦上訴法院的法官 Richard Posner 在 illinois transportation trade association v. city of chicago thetimes 一案中指出，芝加哥政府並無沒收現有傳統計程車的執照，僅是讓傳統計程車公司受到像 Uber 等新興商業模式之挑戰，雖然新興科技或商業方法的崛起會使得舊有的商業模式衰退甚至消失，但憲法應保障新的商業模式加入市場競爭的機會，否則現代社會可能

[103] 金融科技一詞尚無明確之定義，但根據多數業者所申請之金融科技專利多數落在國際專利分類(International Patent Classification)G06 之分類，而 G06 係指使用科技技術如電腦、系統等設備運算、處理而達管理、促進或實施商業活動之目的之專利，因此本文以此作為金融科技之定義。

DOI:10.6814/NCCU201901043

就沒有計程車而只有馬車；沒有電話而只有電報[104]。

此外，傳統計程車和 Uber 存在差異性，例如傳統計程車讓乘客路邊揮手示意而隨機載客；Uber 乘客則須事前與 Uber 業者註冊，並簽訂關於收費、保險、司機素質和特殊需求等契約條款，Uber 擔負司機篩選、揭露相關資訊的責任，如司機姓名、搭乘路線、車子外觀且 Uber 僱用兼職的司機，其車輛平均里程數低於傳統計程車，此些差異讓芝加哥政府對於兩種不同商業模式採取不同監管措施有了正當化的理由[105]。

因此，若不同的商業方法或技術確實存在差異性，課予不同的監管措施不僅不違反平等原則，反而能促進產業創新而帶給人們更便利的生活。

第一款 監理原則-酌情應用原則[106](Proportionate Regulation)

監理的目的是為控管風險、維護公共利益，因此應根據風險的種類、大小並衡量監理所能帶來的公共利益和社會成本而賦予不同程度之監理框架。此監理框架應能確保相似的風險以相似的方式對待，並具備科技中立的彈性，以涵蓋未來和既存的服務提供者所提供之不同創新金融科技產品與服務[107]。

第二款 監理原則-賦能致動原則(Enabling Regulation)

傳統由上至下的靜態規範式監理模式(Rules-based Regulation)係指主管機關

---

[104] illinois transportation trade association v. city of chicago thetimes, No. 16-2009 (7th Cir. 2016), p4, available at：http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2016%2FD10-07%2FC%3A16-2009%3AJ%3APosner%3Aaut%3AT%3AfnOp%3AN%3A1842508%3AS%3A0

[105] *Id.* at 8-9.

[106] 簡言之，酌情應用原則即為比例原則，監理手段須有助於控管風險目的的達成且對於欲管控的風險並不會施加過重或不符比例之措施。

[107] 臧正運，臧正運觀點：形塑全球金融科技監理標準的關鍵語彙，參考網址：http://www.storm.mg/article/165779 (最後瀏覽日：2019 年 7 月 1 日)

DOI:10.6814/NCCU201901043

訂立各種具體詳盡的法令或授權各業別監理機關訂定細瑣的準則或辦法，作為商品審查與業務監理的標準[108]。但如此僵化的方式已無法因應變遷快速且複雜的金融科技世代。

賦能致動原則強調溝通、合作、互動的動態彈性監理架構，主管機關營造一個開放場域，讓所有競爭者得以公平競爭，並規劃試點計畫(pilot program)[109]和試驗性方法讓創新產品得以測試其商品、服務的市場接受度、商業模式的可行性與法規遵循的能力，主管機關亦可藉此了解創新科技的發展及對金融體系所帶來的風險，促使監管者制定相應的監理標準，並改進現有法規的缺失，進而健全市場整體的發展[110]。

第三款 監理原則-數據驅動原則(Data-driven Regulation)

數據(data)是們認知的起點，亦是現代政府和非政府組織決策的基礎[111]。區塊鏈所帶動的金融科技革命對許多產業產生裂解且涉及金流、物流、資訊流等多方領域，不僅增加監理的複雜性，更增加監管的難度。

數據驅動原則係指廣泛使用不同的監管科技，例如：人工智慧(Artificial intelligence)、雲端計算(Cloud computing)、大數據(Big Data)蒐集、分析大量的資料(data) 並轉換成有價值的資訊，以輔助監理機關判情勢並制定高品質的決策和事前風險管理計畫，防止系統性風險化成實害，戕害市場整體發展[112]。

---

[108] 中華民國證券投資信託暨顧問商業同業公會，國際動態，2009 年 4 月，參考網址：https://members.sitca.org.tw/OPF/K0000/files/CWeb/9804 國際動態.pdf

[109] 英國、新加坡和我國所推動的監理沙盒即是一試點計畫例子。

[110] G20 Principles forInnovative Financial Inclusion, Global Partnership for Financial Inclusion, p4, available at：https://www.gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20-%20AFI%20brochure.pdf

[111] Ranchordas, Sofia and Klop, Abram, Data-Driven Regulation and Governance in Smart Cities (February 19, 2018), available at : https://ssrn.com/abstract=3126221

[112] *Id* at 4

DOI:10.6814/NCCU201901043

第四款 監理原則-不予傷害(Do no harm Principle)

1950 年代電腦、互聯網帶動第三次工業革命，顛覆人類資訊交換的方式，當時美國前總統 Bill Clinton 曾於 1997 年提出互聯網監管政策-全球電子商務框架(The Framework for Global Electronic Commerce)，確立了不傷害準則(Do no harm approach) ，並在此概念下提出了五項原則[113]：

1. 由私人企業領導互聯網科技之發展，鼓勵自律。
2. 政府應避免過度干預。
3. 需要政府負責秩序維持的領域，管制手段應為可預測、具有一致性、侵害最小的簡單法規範環境。
4. 政府應認識到互聯網的獨特之處。
5. 互聯網之電子商務發展應以全球視角為基礎。

當時美國政府認為，資訊科技技術日異月新，立法的速度難以企及，因此應以彈性監管的政策框架及逐案審查(Case-by-Case)的方式，以避免僵硬的法規範阻礙創新的發展[114]。

時至今日，這項全球電子商務框架所確立的準則也適用於現今的區塊鏈應用上，區塊鏈是一種資訊交換之協定和方法，只要有資訊交換的需要，皆可能有區塊鏈應用的場域，世界經濟論壇(WEF)創辦人 Klaus Schwab 指出區塊鏈將會是繼蒸汽機、電能、電腦之後的第四次工業革命，更顯現出其影響無遠弗屆，此外與 1950 年代的互聯網興起相同，其技術逐年創新、進步，適用的產業範圍越來越廣，呈現典型資訊科技技術動態發展的特色，不宜以高度監管和缺乏彈性之法規範進行監理，不僅扼殺創新，更無法達到監理之目標。

---

[113] A Framework for Global Electronic Commerce Executive Summary, available at：https://clintonwhitehouse4.archives.gov/WH/New/Commerce/summary.html (Last visited on 2019/07/01)

[114] *Id.*

DOI:10.6814/NCCU201901043

第二項 金融科技監理議題之分析框架

第一款 監理議題分析框架

國際標準化組織(International Organization for Standardization，以下簡稱ISO)為了讓網路通訊更為普及，曾於 1984 年制定 OSI 模型(Open System Interconnection/Reference Model，以下簡稱 OSI)，將電腦網路體系架構分為 7 層，分別為第一層 實體層、第二層 資料連結層、第三層 網路層、第四層 傳輸層、第五層 會議層、第六層 表達層、第七層應用層，將網路協定功能拆解為七個部分，並定義各層的功能，第一層實體層的功能規範硬體的相關功能，如資料傳輸的電壓值、纜線規格等，階層越往上遞增，其規範越接近使用者所使用的服務功能，例如第七層應用層即規範使用者網路應用服務相關協定的功能如 HTTP（HyperText Transfer Protocol）、FTP（File Transfer Protocol），因此其階層安排的核心邏輯即是由規範硬體功能開始，隨著階層遞增會越接近使用者端的相關功能。ISO 藉由發布此功能架構，方便各國電腦工程師於開發相關服務時，能有一清晰概念與共同標準得以遵循，以利網路服務的發展[115]。

而這樣的概念架構值得援引於金融科技崛起而對於法規範頻繁衝撞的世代，先制定監理模型和劃分各層的定義和功能，再剖析法律關係屬於何階層所欲探討的問題，並對應各階層之目的，如此一來方能有一清晰和聚焦的討論重點。

因此本文援引 OSI 模型中的實體層和應用層之概念，本文實體層即指接近硬體或技術相關的法律規範，例如電子簽章法著重的是電子簽章技術產生的電子簽章於電子商務環境是否能與傳統實體簽章或意思表示具有相等之基礎法律效力，此著重於硬體技術的意思表示方法能否賦予法律上效力，因此歸類為實

[115] 陳祥輝，TCP/IP 網路通訊協定，二版，博碩文化出版社，2011 年 12 月，頁 33。

DOI:10.6814/NCCU201901043

體層；應用層則是建立在電子簽章此種以數位方法表達意思表示所開展的各項法律關係，例如網路買賣等。而本文未援引 OSI 第二層至第六層的原因是此些階層規範的是偏硬體內部傳達資訊方法如封包格式應包含何種項目、資料格式轉換等細節規定，此等非法律層次之規範，而是創新技術為了方便或統一所作之標準程序(Standard Operating Procedures)，因此本文即無納入新提出的監理議題分析框架中，以免徒增複雜和繁瑣。

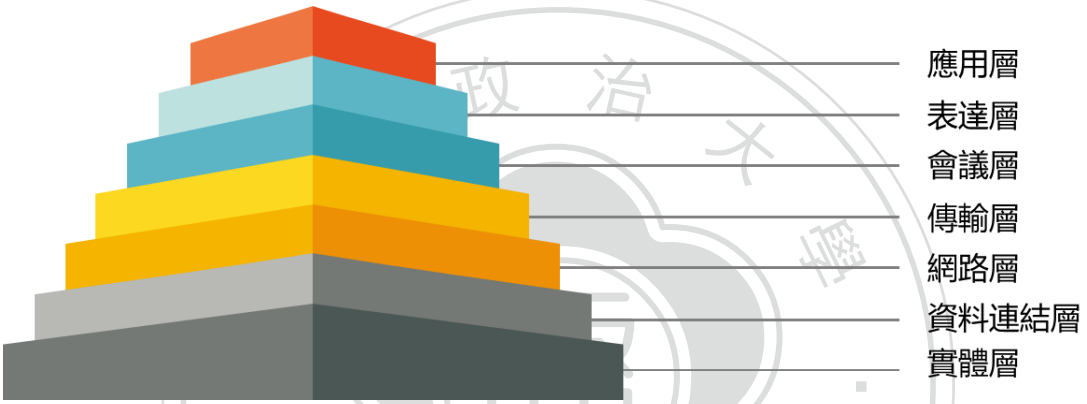

圖 4：OSI 七層模型示意圖(作者自製)

一、第一層-實體層

從本章第二節和第三節可看出，目前國際監管皆聚焦於區塊鏈技術所建構的應用方面，例如虛擬貨幣、ICO 和智能合約，透過立法的方式將區塊鏈應用納入監管的射程範圍或以行政機關函釋融入現有的法律框架進行價值判斷，如美國 SEC 以 Howey Test 判斷 ICO 是否符合美國現行證券交易法證券之定義，但卻未有針對區塊鏈技術本身或其相關行政管理之配套措施進行規範的例子。

區塊鏈技術的本質就是一種資訊系統資料交換的協定，因此如何以區塊鏈技術本質為出發點制定相關管理規範和配套措施以維護區塊鏈系統的「資訊安全」是監理者的首要課題。

而影響資訊安全的因素包含內部人員管理、教育訓練、系統硬體損害與外部網路攻擊，應可參照目前 ISO27000 資訊管理安全系統標準系列，制定相關人

DOI:10.6814/NCCU201901043

員、組織管理規範和風險管控計畫，以利未來以區塊鏈技術所建構的應用能有穩定的基礎和發展。

二、第二層-應用層

以區塊鏈技術建構的應用，涉及多種領域如金融、供應鏈、身分識別、教育、慈善等，每個領域當事人的法律關係皆有主要對應之法規，如金融對應公司法、保險法、證券交易法；供應鏈金融對應民法(私人契約)；身分識別對應個人資料保護法；教育對應私立學校法、大學法；慈善對應人民團體法、所得稅法，區塊鏈作為一個底層技術或是手段，改變的是產業運行的方式和流程，但基礎法律關係不變，例如區塊鏈應用於 ICO，以代幣取代股票發行募集資金，代幣擁有者未來可使用代幣兌換服務或賣出享受資本利得，與傳統發行股票欲募集資金的目的並無不同，只是募集的方式改變，因此實務將 ICO 視為證券而課予證券交易法中的資訊揭露義務以保護投資人；區塊鏈應用於班機遲誤保險，保險人與被保險人之間的保險契約賠償請求的權利義務關係並無改變，只是核保過程被區塊鏈取代，因此當保險事故一發生，理賠將自動匯入申請人的帳戶；區塊鏈應用於教育畢業證書發放，發放的過程原由人工核實改由區塊鏈記錄，形成不可偽造之記錄，但任何人是否皆有訪問權限，如私人企業、當事人僱用公司、學校則是個人資料保護法所欲探討之議題，但學校與學生之間最基礎的公法關係並無改變。

因此應用層的監理可回歸至原有的基礎法律關係找尋相對應之規範，區塊鏈只是驅動的因子，但本質並無不同，如 ICO 本質即是募集資金，在保護投資人和維持金融市場穩定的衡量下，給予適當監理，但不宜過度，以維持市場創新的能量。

第二款 區塊鏈應用之監理手段

區塊鏈引領的金融科技世代，除了是技術上的創新亦是管理模式的創新，

DOI:10.6814/NCCU201901043

建立在區塊鏈的基礎而開展的商業模式的創新週期相較於 18 世紀第一次工業革命已大幅縮短，舉例來說，1879 年 Karl Benz 發明內燃機並取得專利，並於 1880 年後開始生產，但未立即對當時以馬車為主要交通工具的生活模式造成擾亂和影響，一直到了 1908 年後 Henry Ford 將生產線概念應用於工廠，汽車方開始大量生產，並逐漸取代馬車成為人們日常生活交通往來工具，而這樣的過程長達約莫 30 年，緩慢的創新過程讓監管者有足夠時間提出令人信服的監管方法，但現代破壞式創新的週期相當短，其所造成不確定性風險大幅侵蝕人民對監理機關的信任[116]，因此在釐清監理議題於前述的分析框架中處在哪一個法規範階層後，再來才是思考以何種監理手段取得創新進步和消費者保護兩者之間的平衡點以達監理之規範目的。

第一目 監理沙盒

監理沙盒係指監理機關提供適格之新創事業一安全空間，測試其產品、服務和商業模式，並暫時豁免於金融監理法規之責任[117]。其目的在於創造彈性的監理環境，以鼓勵創新並促進金融市場合理之競爭。

監理沙盒的概念最早是由英國所提出，為因應金融科技世代之來臨，英國政府自 2014 年 10 月啟動創新計劃，首先成立創新中心(Innovation Hub)作為金融科技政策和法規相關的制定和研究中心，並提供創新者相關法令遵循的協助，並於 2015 年 11 月由英國金融行為監理局(Financial Conduct Authority, FCA)提出監理沙盒制度，允許助符合特定條件之金融科技新創事業於特定時間測試其商品、服務、商業模式、通路之可行性，並享有法規的豁免與指導，打破以望僅金融業者能從事金融服務之現象，同時監理者亦可從與業者的互動過程中

116 Rebecca M. Bratspiess, Regulatory Trust, 51 ARIZONA L. REV. 575, 576-575 (2009)

117 張冠群，自金融監理原則與金融消費者保護觀點論金融科技監理沙盒制度——兼評行政院版「金融科技創新實驗條例草案」，月旦法學教室，第 266 期，2017 年 7 月，頁 5-6。

DOI:10.6814/NCCU201901043

更加了解科技，並取得反饋意見以作為法規調整和消費者保護機制建立的參考，因而建立的一種協作式(Collaborative)、實驗式(Experimental)、迭代式(Iterative)精神的創新監理模式[118]，以鼓勵創新並促進金融市場公平競爭之目的。

FCA 認為監理沙盒可帶來的潛在效益有三項[119]：

(1)減低創新事業進入市場的時間與成本

監管和法規的不確定(regulatory uncertainty)將使創新的先驅者(first-movers)進入市場時間增加 1/3 倍，並讓產品之生命週期成本增加 8%[120]。

(2)增加融資管道

目前新創事業多半依賴股權融資的方法，但監管和法規不確定性將使得投資人有所疑慮而躊躇不前，造成新創事業在關鍵的起步階段即因資金不足而無法讓具有前瞻性的創意想法落地成為實際運轉的商業模式。根據研究顯示監管和法規的不確定性將使得公司的估值(company valuation)減少 15%，因此為數眾多的新創業者無法達到它們所欲達到的募資目標金額[121]。

(3)促進創新產品或服務進入市場

監管和法規不確定性使得許多新創事業的創意思想在種子期(Seed Stage)就因為無風險資本的投入，甚至無經過市場測試即胎死腹中，監理沙盒提供一個監理機關和創新業者之合作場域，確保新產品或服務進入市場前，能謹慎評估其可能造成的消費者風險，並制定適當的消費者保護措施，並妥善管理法規和監管風險，以順利將產品推入市場帶給消費者不同以往的使用

---

[118] 侯乃真，金融科技創新監理之新途徑-以監理沙盒為中心，台灣大學法律學研究所碩士班論文，2017 年，頁 58。

[119] Financial Conduct Authority, Regulatory sandbox (2015), p5, available at：https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf

[120] *Id*. at 5.

[121] *Id*. at 5.

DOI:10.6814/NCCU201901043

者體驗和服務，落實普惠金融的目標。[122]

區塊鏈所驅動的破壞式創新如虛擬貨幣、募資工具(Initial Coin Offering 首次貨幣發行、Security Token Offering 證券型代幣)、跨境支付，甚至新的治理模式如分散式自治組織至新的金融體系的建立如去中心化的分佈式金融，皆對既有之法規範產生莫大之衝擊，而監理機關對於創新業者技術、商業模式的不熟悉所造成的不確定性常是造成其不願鬆綁法規的主因[123]，但區塊鏈此種新科技所帶來的顛覆性影響，遍及各產業，若監理機關仍固守僵化的規範式監管(Rules-based)方式，將使國家創新力量和經濟成長陷入停滯，監理沙盒在公私協力合作和促進有責創新(Responsible Innovation)的精神下[124]，提供業者一個低監理密度的環境，但又可進行產品或服務測試的開放場域，在這過程中完善風險管理和建立消費者保護機制，並有效促進創新和消費者利益。此外，監理機關亦能透過雙向交流溝通之過程熟悉新的科技技術和商業模式類型，並提前預判其所可能產生的風險和法令遵循的疑義，透過監理沙盒的實踐也幫助監理機關強化了本身的監管能力(Regulatory Capacity)[125]。

第二目 監管科技

監管科技(RegTech)係指利用資訊科技促進法律遵循和監督的技術解決方案(technological solutions)[126]。2008 年金融危機後，各國莫不引以為鑑，相繼制定

---

[122] *Id.* at 5.

[123] 侯乃真，同註 104，頁 96-98。

[124] Office of the Comptroller of the Currency, Supporting Responsible Innovation in the Federal Banking System:An OCC Perspective, p5, available at：http://consumerbankers.com/sites/default/files/OCC%20whitepaper%20fin%20inno%282%29.pdf

[125] 彭金隆、臧正運，我國金融科技創新實驗落地機制之檢視與構建，月旦法學教室，第 266 期，2017 年 7 月，頁 49。

[126] IIF, RegTech in Financial Services:Technology Solutions for Compliance and Reporting(2016), p2, available at：https://www.iif.com/Portals/0/Files/private/iif-regtech_in_financial_services_-_solutions_for_compliance_and_reporting.pdf?ver=2019-01-04-142943-690

DOI:10.6814/NCCU201901043

許多金融法規以對金融產業進行管制，不僅造成業者的法遵成本提高，金融科技的興起和監理破碎化(Regulatory fragmentation)亦讓監理機關的監理複雜度提升[127]，需要的資料粒度(data granularity)[128]、資料聚合(data aggregation)[129]和資料精確度(data precision)都比以往來得高，因此迫切需要監管科技的數位化和自動化以因應日趨複雜的監理標準和需求[130]。

監管科技運用區塊鏈、人工智慧、大數據、雲端計算蒐集海量資料並轉換成有用的資訊和解決方案(insight)，以供監理機關形成良好決策和監管，以改善傳統僵化的規範式監管(Rules-based)或充滿法律不確定性的原則式監管(Principle-based)，而以數據導向(data- driven)所形成的優良評估或分析報告作為監理的依據，形成一個具有遠見和洞察力的監管模式(insight-based)[131]，以適應快速變動的金融科技社會。

監管科技讓監管者得以因應金融科技所帶來的快速變動，以下是分析監管科技的特性所能帶給監管者的優勢：

1、 建立壓力測試和風險管理模型

壓力測試和風險管理模型所需的資料、情境分析和變量越來越複雜和多元，監管科技將能幫助其進行運算並提供相關報表以進行高品質決策[132]。

---

[127] Douglas W. Arner &Jànos Barberis & Ross P. Buckley, FinTech, RegTech and the Reconceptualization of Financial Regulation(2016), p23, available at：https://ssrn.com/abstract=2847806

[128] 資料粒度係指資料的詳細程度。

[129] 資料聚合係指收集原始資料並以摘要形式彙整以進行統計分析之。

[130] Douglas W. Arner &Jànos Barberis & Ross P. Buckley, supra note 126, at 22.

[131] Accenture, REGTECH FOR REGULATORS(2018), p3, available at：https://www.worldgovernmentsummit.org/api/publications/document?id=5ccf8ac4-e97c-6578-b2f8-ff0000a7ddb6 (Last visited on 2019/07/01)

[132] IIF, *supra note* 125, at 6-8.

DOI:10.6814/NCCU201901043

2、 即時監控

交易資料屬性不同常使監理機關進行即時監控的困難度和複雜度增加[133]，監管科技如大數據(Big Data)技術能有效蒐集、分析非結構性交易資料[134]並自動建立風險模型以輔助監理者進行評估和研擬監理對策。

3、 改善監督品質和成本

金融監理越趨複雜，增加人力無助達到監理之合規標準，監理科技能幫助監理機關達成複雜之監管需求和人力成本之降低[135]。

有別於傳統企業資訊系統所使用的的輻射式網絡(Hub and Spoke model)架構是由一個或數個數據處理中心(Hub)連結數個子節點(分公司)，並由 Hub 作為中心樞紐處理各方節點的資訊交換和維護[136]。區塊鏈是由各節點共同維護一帳本資料庫系統，因此以往將監理資源集中於超級風險傳遞者(super-spreaders)[137]如中間機構的方式將不適用於區塊鏈此種分佈式網絡，所有節點都可能是系統風險的來源[138]，而在監理資源有限情形下，不可能將資源投注於所有節點，因此監理機關如何有效使用科技管控區塊鏈所帶來的風險會是未來關注的焦點；此外區塊鏈應用本身是風險來源卻也是監理的解答，區塊鏈不可竄改特性提供監理機關明確的審計和追蹤途徑，每個資料永久被記錄於區塊中，尤其當監理機

---

133 *Id*. at 9-10.

134 非結構性資料如電子文件、圖片、電子郵件等未經過整理之無規則性資料，若未經處理難以進行蒐集和應用。

135 Lawrence G. Baxter, Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failures, 66 Duke Law Journal 567, 598-600 (2016)

136 Yu An, Yu Zhang and Bo Zeng ,The Reliable Hub-and-spoke Design Problem: Models and Algorithms(2011), p1, available at：http://www.optimization-online.org/DB_FILE/2011/05/3043.pdf

137 Andrew G Haldane, Rethinking the financial network(2009), BIS Review, p2, available at：https://www.bis.org/review/r090505e.pdf

138 Zetzsche, Dirk A. and Buckley, Ross P. and Arner, Douglas W., supra note 21, at 8.

DOI:10.6814/NCCU201901043

關加入成為區塊鏈網絡節點[139]，還能定義和部署先決條件(pre-defined conditions)如資本和流動性(Liquidity limits)限制，讓監理機關不再僅能等待風險實現後再以人工方式蒐集證據後再施以裁罰之被動監管方式，而能提前監控可疑金流和事件活動並採取預防措施，以提升監管效率和降低蒐集證據的成本[140]。

第三目 孵化器、加速器、創新中心

加速器、孵化器、創新中心的目的皆是為扶植新創企業於技術、通路、資金、人脈上提供必要之資源，以幫助企業度過艱苦的草創期，並降低失敗的機率，使得創意想法得以落地為成熟的商業模式。

此外，此些中介平台亦能作為新創業者和監管主管機關之交流平台，藉由雙向溝通落實賦能致動的監理原則-達成溝通、合作、互動的動態彈性監理架構，除了彌補監理機關和新創業者之間對於法規上的認知落差，監理機關亦可透過平台蒐集業者對於法規的意見，以作為未來修訂之參考，以免阻礙創新發展的契機。

一、 孵化器（Incubator）**和加速器**（Accelerator）

孵化器主要由非營利機構或政府建立，扶植剛起步的新創企業，篩選標準較低，並提供空間與法律、財務、商業行銷等廣泛領域的指導，為期約 1-5 年[141]。

加速器主要由營利組織所建立，扶植已度過孵化期並期望邁入高

---

[139] U.S. Commodity Futures Trading Commission ,An Assessment of the Current Implementation of Reform and Proposals for Next Steps, p34, available at：https://www.cftc.gov/sites/default/files/2018-04/oce_chairman_swapregversion2whitepaper_042618.pdf

[140] Josh Stark, Applications of Distributed Ledger Technology to Regulatory &Compliance Processes (2018), p4-8, available at：https://www.r3.com/wp-content/uploads/2018/04/Reg_Compliance_R3.pdf

[141] Susan Cohen, What Do Accelerators Do?Insights from Incubators and Angels,8 Innovations19, 19-21(2014)

DOI:10.6814/NCCU201901043

速成長的新創企業，透過研討會的方式進行密集且高效率的商業模式和流程檢視，並提供價值主張等高階的策略擬定以建立長期的品牌價值，此外亦媒合專業的投資人以幫助新創事業獲得最需要的資金挹注，為期約 3 個月[142]。

孵化器和加速器主要區別在於計畫實行期間和是否擁有新創事業股份，多數孵化器實行期間約為一年以上，加速器則約為三個月；而加速器創辦者通常會持有新創事業股份，如全球知名的 Y Combinator 規定新創事業須以 7%股份作為 Y Combinator 提供資金之對價，而孵化器多為非營利組織，因此少以股權方式參與新創公司發展[143]。

多數加速器亦含有孵化器之前期輔導功能，完整規劃新創企業前、中、後期資金和其他必要資源協助，有些更與當地監管者合作，提供法規諮詢和建議，透過雙方交流讓業者創新同時亦能兼顧法規上的規範；監管者則透過此平台第一線及時接觸新創業者並立即獲得反饋，以作為往後修法之參考，讓法規範能與時俱進，避免扼殺金融科技發展的契機。

	孵化器	**加速器**
時程	1-5 年	3 個月
夥伴關係	租賃關係(提供空間、相關服務)	投資關係(加速器擁有新創事業之股權)
參與階段	新創事業種子期	新創事業種子期
教育資源	提供特定諮詢資源如律師、會計師	提供多元形式教育資源如研討會、演講、一對一指導等
導師制度	少量的導師資源	密集且緊密關係的導師提供輔導

表格 1：孵化器和加速器比較

[142] *Id* at 20.

[143] *Id*. at 21-22.

DOI:10.6814/NCCU201901043

(資料來源：Susan Cohen, What Do Accelerators Do?Insights from Incubators and Angels,8 Innovations19, 20(2014))

下列為知名金融科技孵化器或加速器：

1.新加坡 Startupbootcamp FinTech

2010 年於丹麥哥本哈根成立，2014 年成為歐洲最大創業加速器，並於 2015 年成立新加坡分部。

其不僅提供導師、營運空間和全球投資人之媒合介紹，更與新加坡金管會(MAS)合作，提供一個月兩次的機會讓新創業者能與監管主管機關進行法規上的交流和溝通，並提出對於法規上的疑慮和建議，新加坡金管會官員蒐集意見後再進行後續的調整以利新加坡的金融科技新創能不受法規限制而蓬勃發展[144]。

2. 紐約 FinTech Innovation Lab

2012 年顧問公司埃森哲（Accenture）和紐約市合作基金合作成立 FinTech Innovation Lab 加速器，在金融科技領域的輔導經驗享譽全球，其提供新創業者與金融高階管理人員合作並收到產品使用反饋的機會、媒合全球投資者，並指派紐約州金融服務部（New York State Department of Financial Services, DFS）的監理主管人員駐點，並提供新創業者戰略諮詢和指導，幫助新創業者適應既有的法規框架，亦作為紐約州官方蒐集修法意見的平台[145]。

---

[144] 翁書婷，台灣需要什麼樣的 FinTech 加速器？也許可以參考新加坡，2016 年 4 月 8 日，參考網址：https://www.bnext.com.tw/article/39160/BN-2016-04-08-183106-40 (最後瀏覽日：2019 年 7 月 1 日)

[145] FinTech Innovation Lab New York,Former New York regulatory chief Maria Vyllo joins FinTech Innovation Lab New York, available at：https://www.finextra.com/pressarticle/78032/former-new-york-regulatory-chief-maria-vyllo-joins-fintech-innovation-lab-new-york (Last visited on

DOI:10.6814/NCCU201901043

二、 創新中心 (Innovation hub)

主要由政府建立，搭建監理者和業者的溝通橋樑，幫助業者了解監管框架，以減少監管和法律適用的不確定性，縮短上市的時間，政府亦能從業者回饋之意見，檢視監管框架與產業創新的扞格。

鑑於金融科技的興起和快速變動，各國紛紛建立創新中心以協助業者減少法律遵循之成本，以下為各國建立創新中心之整理：

(一) 英國(Innovation hub)

由英國金融行為監管局(FCA)所建立。

1、目的：協助已受監管和未受監管的企業能藉由創新中心推出新的金融商品和服務。

2、進入資格[146]：

(1)商品或服務為真的創新(genuine innovation)

(2)商品或服務有益消費者

(3)企業對於其新商品和服務的合規性投入適當的研究

(4)企業確實需要協助

3、提供的協助[147]：

(1)提供專業團隊的協助和專屬聯繫人作為反映意見和諮詢的橋樑

(2)幫助企業了解監管架構與法律遵循

2019/07/01)

[146] Financial Conduct Authority, Eligibility for Innovation Hub, available at：https://www.fca.org.uk/firms/project-innovate-innovation-hub/eligibility

[147] Financial Conduct Authority, Innovate events, available at：https://www.fca.org.uk/firms/innovate-innovation-hub/events

DOI:10.6814/NCCU201901043

(3)舉辦圓桌會議、專題研討會以促進創新和外部參與

(4)提供專屬監管手術課程(Regulatory surgeries)，企業可針對法律遵循適用上的細部問題進行詢答

(4)與海外監理機構簽署合作協議以幫助企業了解其他國際市場監理法規，並協助進入市場之必要協助

(二)澳洲 (Stone & Chalk)

由澳洲政府財政部(Dept. of the Treasury)、澳洲證券交易所(ASX)、金融機構(含 AMP, ANZ, HSBC, Macquarie, Suncorp, Westpac)、資訊業(Finzsoft, Thomson Reuters)、科技業(Finzsoft , IBM, Oracle)及其他企業(含零售業的 Woolworths、律師事務所 Allens、通訊業的 Optus)等共同投資創立。

1、目的：協助金融科技的新創公司於亞太區發展具破壞性創新的金融業務，主要包含區塊鏈技術的應用、支付金融、網路平臺投融資、機器人理財顧問及數位貨幣等[148]。

2、進入資格[149]：

(1)與金融服務業相關

(2)業務成熟度

(3)企業價值主張(Value proposition)

(4)團隊審視

3、提供的協助[150]：

(1)提供專業導師指導

(2)媒合潛在投資人

(3)與大專院校成立合作夥伴關係提供專業研究意見

[148] Stone&Chalk, Stone&Chalk programs, available at：https://www.stoneandchalk.com.au/programs

[149] *Id.*

[150] *Id.*

DOI:10.6814/NCCU201901043

(4)媒合相關業者進行商業化合作

(5)建立金融科技社區以讓加入的新創公司和跨國合作夥伴交流連結，並提供企業管理、投資、業務培訓等課程

第四節 區塊鏈監理建議

區塊鏈以科技技術奠基並驅動以金融為主要的商業模式，涉及金流、物流、資訊流多個層面，不僅包含金融市場動態(dynamic)且易變(volatile)的性質，且加上資訊科技的快速遞進，使得區塊鏈生態系形成一個複雜調適系統(Complex adaptive system)[151]，系統的運作與發展是從微觀的個體彼此互動影響而產生巨觀的動態系統面貌，因此監管者應有別於傳統監管思維而對之有一宏觀的差異化監理思維，輔以酌情應用原則(比例原則)、賦能制動原則(動態互動)、不予傷害原則與數據驅動原則(科技手段)的應用，當確立中心思維，再以區塊鏈監理模型審視不同層面所應關注的焦點，區塊鏈實體層(底層技術)著重的是技術、系統安全規範的建立；區塊鏈應用層(商業應用)則著重商業應用的法律關係和雙方的權利義務，分層剖析才能建立監管標準和規範。

區塊鏈實體層規範如電子簽章法，處理基本之法律上效力和證據能力問題，惟區塊鏈並無憑證機構此等中間機構對於資訊安全風險進行管理，因此法律規範對象應由中心機構轉變為網絡中各個節點，課予相關資訊安全維持之義務，方能健全以區塊鏈技術為基礎的各種商業應用。而區塊鏈應用層之各種區塊鏈商業應用的法律關係，則對應至各項原有的法律規範作相關調整即可，如ICO 本質就是募集資金行為，就應落實公開原則、投資者保護，不因使用的技術為區塊鏈而有所不同。

[151] Klara Palmberg, Complex adaptive systems Properties and approaches (2009), p3, available at：http://www.mementor.se/wp-content/palmberg-complex-adaptive-systems-research-report.pdf

DOI:10.6814/NCCU201901043

此外，除了以法律規定作為監理手段，在活潑的區塊鏈生態體系中，應以動態和共同協作的平行式監管，取代傳統父權思維的上對下規範模式，如此才能促成雙向溝通和成長，而手段的選擇更應以下述五點作為是否符合比例原則的衡量標準：法制體系、監理成本、預防系統性風險、促進競爭與創新、消費者保護[152]。

近年來國際討論最多的監理手段莫過於監理沙盒，英國、澳洲、新加坡、香港接相繼建立監理沙盒以期望在金融科技取得領先地位，而台灣於區塊鏈所驅動之金融科技應採取單一或多種監理手段交互運用，皆應以上述五點作為衡量標準方能符合我國之情狀。

台灣屬於大陸法系國家，原則上採取規範式監理模式，制定成文法並以正面表列的方式規定業者所能進行的業務種類，不若英美法系國家屬於原則式監理模式，僅訂定原則性事項、監理目標與預期監理結果，因此行政機關能以行政命令作補充解釋，以符合產業發展現況，但大陸法系國家修訂法律須經歷一定的立法程序，無法快速因應科技所帶來之法制變動，因此在僵化之大陸法體系下，監理沙盒給了一個法規彈性適用的實驗空間。

但實驗完成後能否將創新落地成為真實可行之商業模式，並持續與監理機關保持雙向溝通，是產業和法規得以維持動態平衡之關鍵，因此以監理沙盒作為創新產業進入市場的前哨，輔以加速器、孵化器、創新中心於不同階段提供諮詢和資金挹注，才是能否建立區塊鏈生態系的關鍵。因此監理手段的選擇並非排他互斥，而是相輔相成以兼顧公共利益之追求和產業發展週期。

此外考量監理沙盒所需之人力成本，對於台灣現況來說將難以負荷，以英國為例，其建立的創新計劃(Project Innovate)包含監理沙盒與創新中心

[152] Global Partnership for Financial Inclusion ,G20 High-Level Principles for Digital Financial Inclusion, p11-12, available at：http://www.g20.utoronto.ca/2016/high-level-principles-for-digital-financial-inclusion.pdf

DOI:10.6814/NCCU201901043

(Innovation hub)，雙管齊下且緊密連結，並設有專業團隊和專業聯繫人輔導；而台灣僅以金管會作為主管機關，雖在 2018 年設立金融科技發展與創新中心，下設創新發展組和園區發展組，創新發展組負責研擬金融科技相關子法及監理沙盒案件之審查；園區發展組則設立園區讓金融科技業者進駐以進行相關輔導，但所需人員仍從各業務局處派員支援或兼任[153]，其是否有足夠跨領域的專業諮詢人才分配給每個申請之創新公司有所疑義，此外亦引領出區塊鏈產業多樣化的面貌和跨領域科際人才的重要性，台灣目前監理分工相當細，金管會掌管銀行、電子支付、電子票證；中央銀行掌管外匯；經濟部則掌管第三方支付、電子簽章，彼此無法干涉，使得跨部會監理和制訂國家戰略式的金融科技政策困難重重；相對地，新加坡的金融監督管理局(Monetary Authority of Singapore, 簡稱 MAS)兼具我國金管會、經濟部和中央銀行的職權[154]，整合金融、經濟、金融創新資源，於 2015 年 8 月設立金融科技與創新團隊(FinTech and Innovation Group, FTIG)，此團隊與原本 MAS 中的貨幣政策與投資部門、國際發展部門、金融監督部門、企業發展部門為平行位階，由三個部門所組成：支付及科技解決方案辦公室(Payments & Technology Solutions Office)、技術基礎建設辦公室(Technology Infrastructure Office)以及金融科技創新實驗室(Technology Innovation Lab)，大為提升整合的力量和制定金融科技創新發展策略的高度，我國應可以此作為借鏡，調整組織法規將相關職權劃歸於一個部門，否則多頭馬車的結果，只會讓高速變動的區塊鏈生態系監理越形困難和複雜。

153 金融監督管理委員會金融科技辦公室設置要點第七點。

154 MAS 下設有貨幣政策與投資部門(Monetary Policy & Investment)，職掌國際經濟分析和預測，並建構宏觀經濟模型以提供新加坡作為經濟政策之基礎。MAS 相關組織圖和業務職掌說明請參考：http://www.mas.gov.sg/About-MAS/Overview/Organisation-Chart.aspx ；http://www.mas.gov.sg/About-MAS/Overview/Groups-and-Departments.aspx

DOI:10.6814/NCCU201901043

區塊鏈監理無法再以傳統垂直監管思維進行設計，從規範式監理走向原則式監理，從組織分化走向專一權責機關，從上對下父權規範走向共同協作，單一監管手段走向多元並進，甚至由產業由下而上主動發起自律組織，先藉由相關業者釐清從概念性驗證至實際商轉的運作模式，協助監理機關了解風險因素後再共同協作畫出監管底線，訂定可供業者共同遵循的最低行為準則，以強化資訊透明、防止詐欺洗錢、建立信任機制，透過監管者和被監管者戮力同心，才能實行有效的區塊鏈監理並健全區塊鏈發展環境。

在確立區塊鏈監理中心思維並構築區塊鏈監理議題分析框架，本文後續即聚焦區塊鏈監理議題分析框架中的實體層規範-電子簽章法作為論述重點，探討此作為區塊鏈基礎效力規範之可能性，方有利後續商業應用之開展。

DOI:10.6814/NCCU201901043

第四章 區塊鏈與現行電子簽章法之相容性檢視

1950 年電腦、互聯網等資訊科技術帶動第三次工業革命的發生；2015 年區塊鏈則將舊有資訊科技的技術重新組合並注入新的思維，帶動傳統由上而下中心治理模式的改變，區塊鏈平均賦權予網絡中的各個節點，由下而上將決策結果傳遞至平台，平台不再是一權獨大的中心節點，而僅作為調和各方的溝通平台。

承第二章、第三章所述，區塊鏈以科技技術驅動以金融為主的各種商業模式，包含金流、物流、資訊流，由於涉及產業面廣，並隨著資訊科技的進步形成一個複雜調適系統(Complex adaptive system)[155]，微觀下的個體彼此互動影響進而產生巨觀的動態系統面貌，本文從巨觀面的監理中心思維和分析框架出發再聚焦至微觀的底層規範，而建立區塊鏈於實體層的法律規範和依據應是目前首要的課題，以利各種區塊鏈的商業應用法律關係能以此作為基礎而順利開展。

國際上針對區塊鏈立法的立法例以美國各州為首，如亞利桑那州、田納西州、內華達州，不約而同將區塊鏈法律納入該國電子簽章法中，究其原因有三點：

1、區塊鏈技術與電子簽章主流技術-數位簽章相似，皆使用數位簽章確認電子資料為簽署者所發送且其電子資料未遭竄改，以達到不可否認性。

2、各國立法者在制定電子簽章法時即預見資訊科技日新月異，因此電子簽章法皆採技術中立原則以維持立法的彈性和安定，避免資訊科技技

[155] Klara Palmberg, *supra* note 150, at 3.

DOI:10.6814/NCCU201901043

術的快速變遷而使得法律須反覆歷經耗時的修法程序。

4、 區塊鏈與電子簽章技術旨在改善資訊交換的安全和便利，並促進電子商務發展。

綜合上述三點，選擇將區塊鏈關於法律效力的規範置於電子簽章法此等富有彈性的立法框架下是為恰當的作法，尤其電子簽章和區塊鏈所欲達成的目標相同，技術上承先啟後且有所重疊，但區塊鏈更能確保資料交換的正確性和不可否認性，似無須另設一部專法另作規範，免得疊床架屋，徒增立法成本。

而區塊鏈技術是否能相容於現行電子簽章法中有三個重點，亦為區塊鏈與電子簽章技術交錯的地方與最可能發生衝突之處：

1. 電子簽章法下之電子簽章定義

2. 中心化憑證機構之主體責任與區塊鏈分散式節點責任

3. 數位簽章時間戳與區塊鏈時間戳之法律效力

此三項重點亦是建構完整法律救濟途徑所需的三個主要議題，從區塊鏈能否該當電子簽章定義而受到電子簽章法規範；再探討使用者使用該項技術而發生損害時應向何人主張損害賠償責任，電子簽章下設有憑證機構作為責任主體，但區塊鏈分散式節點和去中心化的設計，如何建構其契約關係和侵權責任會是一大挑戰；最後時間戳作為數位環境時間序列的證明，其證據能力應如何予以規範，使之可能成為訴訟上裁判的依據更是訴訟程序中的重要議題。

因此本章特以電子簽章和區塊鏈之共同技術-公開金鑰加密演算法(又稱為非對稱式加密演算法或數位簽章)作為主軸，探討美國和歐盟的電子簽章法規範下之電子簽章定義、中心憑證機構運作模式、責任規範和時間戳等三個核心概念是否與區塊鏈技術有所差異，進而分析區塊鏈運行模式是否相容於現行電子簽章法下此種規範的模式，最後再予以分析我國電子簽章法有何需要改進之處，並提供相關修法的建議。

DOI:10.6814/NCCU201901043

第一節 美國電子交易法 UETA 介紹

第一項 立法歷程

一、背景

1983 年全球第一台圖形使用者介面(Graphic User Interface)個人電腦-蘋果麗莎誕生，縮短人與資訊科技產品的距離；1980 年美國國防部開發標準化的 TCP/IP 通訊協定，1989 年日內瓦歐洲核子研究中心（European Organization for Nuclear Research）提出 WWW(World Wide Web)的概念[156]，讓地理疆界的隔閡不再是阻礙彼此交流的因素，網際網路所帶來的資訊科技傳播革命被認為是第三次工業革命，徹底改變了人類的生活面貌。

隨著網路科技基礎建設的成熟，各種商業應用也相運而生，2000 年電子商務發展進入蓬勃期，網路電子交易的快速發展，雖然降低交易成本並提升交易效率，卻也衍生諸多法律問題，傳統的法律架構已無法滿足網際網路時代嶄新多元的交易型態。

二、UETA 誕生

有鑑於此，聯合國國際貿易委員會(United Nations Commission on International Trade Law)於 1996 年率先通過電子交易模範法，更於 2000 年完成電子簽章模範規則的制定，此模範法之中對於電子契約、電子文件的效力、書面性簽名及仲裁等問題提出規範標準，以供各國參考。

美國身為資訊科技和電子商務發展的領頭羊，1995 年猶他州即通過電子簽章法(Utah Digital Signature Act)，各州陸續跟進制定個別之電子簽章法，以滿足

[156] Terry Chen，台灣網路編年史(一)：1968 年至 2008 年，參考網址：http://tesa.today/article/700 (最後瀏覽日：2019 年 7 月 1 日)

DOI:10.6814/NCCU201901043

電子商務發展需求及保護消費者之利益，但不同州的法規範存有差異，法律矛盾使得跨州電子商務交易窒礙難行，為統一各州的電子商務規範，美國統一州法委員會於 1999 年 7 月 29 日通過「美國統一電子交易法」(Uniform Electronic Transactions Act,以下簡稱 UETA)」，為各州電子簽名法律提供了參考標準[157]。

目前，美國 50 個州中除了伊利諾斯州(State of Illinois)、紐約州(State of New York)、華盛頓州(State of Washington)之外，共計 47 個州通過以 UETA 為標準之電子簽章法[158]。

三、UETA 與 E-SIGN 之適用優先性

雖然 UETA 於 1999 年頒布，但當時的聯邦政府認為各州並不會積極採行僅具模範法性質之 UETA[159]，所以透過聯邦立法方式希望加速各州採行 UETA 的速度，以確保州際貿易不會因各州電子簽章法的不同而受到阻礙，因此美國國會於 1999 年 11 月即開始彙整當時相關電子簽章議案，包含參議院議案 761 號和眾議院法案 1714 號[160]，最後於 2000 年 6 月 30 日通過「全球暨跨州商務電子簽章法」(the Electronic Signatures in Global and National Commerce Act，以下簡稱 E-SIGN)。

E-SIGN 在立法原則、電子紀錄、電子簽章部分與 UETA 規範並無差異，

---

[157] 美國統一州法委員會(Uniform Law Commission)乃一非營利、非法人之團體，旨在促進各州法律的一致性，委員會成員有法官、律師、立法者和各州代表，但因是非官方組織，其起草之模範法(Model act)或統一法(Uniform act)僅具建議性質，而不像國家立法機關制定之法律具有實質上拘束力。

[158] 美國各州採用 UETA 之統計，參考網址：http://www.uniformlaws.org/Act.aspx?title=Electronic%20Transactions%20Act (最後瀏覽日：2019 年 7 月 1 日)

[159] Stephanie Curry, Washington's electronic signature act: An anachronism in the new millennium ,88 Wash.L.Rev 559, 560-561(2013)

[160] Summary of Bills Pertaining to Electronic Signatures and Authentication in the 106th Congress, available at：http://techlawjournal.com/cong106/digsig/Default.htm (Last visited on 2019/07/01)

DOI:10.6814/NCCU201901043

其功用是為避免各州在制定電子簽章法時排除 UETA 規範或制定有違 UETA 立法原則、精神或更不利電子簽章發展之規範，因而制訂更高位階之聯邦立法以供各州遵循，此立法目的可由 E-SIGN 第 7002[161]條中看出。而關於 UETA 與 E-SIGN 的競合問題，E-SIG 規定在以下兩種情形州政府所制定的 UETA 規範可優先於聯邦位階的 E-SIGN 而適用：

(1)州政府直接採納 UETA 規定作為州法。

(2)州政府另行制定法規範，但不違反 E-SIGN 之規定且對於各種電子簽章技術保持中立態度且賦予相同之法律效力(技術中立原則)

在兩部法律的立法原則、電子紀錄、電子簽章等規範皆無差異情形下且截至 2018 年為止美國 51 個州當中，已有 49 個州直接採行 UETA 而未另行制定法規範，因此本文以 UETA 作為主要介紹對象，並不另行針對 E-SIGN 作解析。

第二項 UETA 立法目的及立法原則

UETA 之制定是為了因應當時 2000 年資訊科技技術成熟所帶動電子商務發展之浪潮，期望提供電子交易一個堅實的法律基礎，其遵循的原則如下[162]：

(一) 消除電子商務在法律上遇到的障礙。若不以書面作為法律行為之要件，則無法達成法規範所欲達成的目的時，才例外允許限制電子簽章和電

[161] 15 U.S.C. § 7002(a)(1) 'In generalA State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of section 7001 of this title with respect to State law only if such statute, regulation, or rule of law—

(1) constitutes an enactment or adoption of the Uniform ElectronicTransactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999, except that any exception to the scope of such Act enacted by a State under section 3(b)(4) of such Act shall be preempted to the extent such exception is inconsistent with this subchapter or subchapter II, or would not be permitted under paragraph (2)(A)(ii) of this subsection;'

[162] Patricia Brumfield Fry, Introduction to the Uniform Electronic Transactions Act: Principles, Policies and Provisions, 37 Idaho L.Rev. 237, 249-50(2001)

DOI:10.6814/NCCU201901043

子記錄之法律效力。

(二) 不因當事人選擇不同之交易方式而異其法律上效力。不管是以電子方式或書面方式進行交易，應適用相同之法律原則。

(三) 法律須保持中立。法律不應限制或獨厚某種交易方式或技術，電子技術應與傳統以紙作為媒介的交易方式同等視之，不應有差別待遇；此外，更不應以法律去決定市場應採行何種交易模式。

(四) 應確保未來縱使科技和商業實踐有所轉變，現今法規範之制定都不會成為電子商務發展之阻礙。

(五) 電子簽章法屬程序法性質，其規範應避免影響現行實體法有關於交易之規定。

(六) 電子交易和電子記錄管理應與傳統書面以相同法律規定規範之，不應分割立法或另立新法。

(七) 法規範應給予電子交易法律上之確定性，並肯認電子交易之執行力。

第三項 UETA 立法規範

第一款 電子簽章類型

一、定義

依據 UETA 第 2 條第 8 項，「電子簽章」係指以電子的聲音、標記(symbol)或過程(process)附加於或邏輯上[163]關聯於一份記錄，且由具有簽章意圖之某人執行或接受[164]，但 UETA 並未進一步區分電子簽章之類型。

[163] 根據美國統一州法委員會發行的 Uniform electronic transactions act(1999) with prefatory note and comments 指出，由於電子簽章不像紙本簽章有一實體介質如紙、文書供其附著(attached)而有一有形的表現形式，因此使用邏輯地關聯(logically associated with)一詞代表電子簽章其乃經演算法而使電子數據或文件可辨認其簽署來源的無實體表現形式。

[164] UETA§2.8(1999), 'Electronic signature" means an electronic sound, symbol, or process attached to

DOI:10.6814/NCCU201901043

二、法律效力

依據 UETA 第 7 條，不能僅因紀錄、簽章是電子形式或契約以電子紀錄形成，而否認其法律上效力或執行力。法律上若以書面紀錄或簽章為要件，則電子紀錄和電子簽章亦符合要求[165]。

此條呼應了前述 UETA 之立法原則，不能因紀錄、簽章和契約之製作或發表所使用的媒介(medium)的不同而影響其法律上效力與執行力[166]。

第二款 中心化憑證機構主體責任

目前美國大部分的州雖已採用 UETA，但仍有少數如伊利諾斯州(State of Illinois)、紐約州(State of New York)、華盛頓州(State of Washington)未直接採用 UETA，而採行 UETA 的州僅少數針對憑證機構制定相關規範，下面以有明文規範憑證機構責任的明尼蘇達州電子認證法作為探討範例。

一、憑證機構之運作方式

數位簽章技術係以非對稱加密方式，產生公鑰和私鑰，簽章人(寄件人)以私鑰加密自己的文件，收件人則由簽章人所發布的公鑰對文件解密以取得文件內容。私鑰由簽章人自己保存，公鑰則發布於網路上，但收件人無從得知公鑰

---

or logically associated with a record and executed or adopted by a person with the intent to sign the record.' (參照馮震宇老師於從政大法學評論《美國電子交易法制論我國電子簽章法》頁 201 中之翻譯。)

[165] UETA §7(1999) , '

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law.'

[166] UETA §7 comment1, p26, available at http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf (Last visited on 2019/07/01)

DOI:10.6814/NCCU201901043

是否確實由簽章人(寄件人)所發布，故設計第三方憑證機構(Certificate Authority)以簽發憑證的方式，認證此公鑰確實屬於簽章人(寄件人)所有，數位憑證連結使用者身分與公開金鑰，如同網路世界中的身分證具有識別功能；而憑證機構角色則如同戶政事務所，負責個人身分證明之審核、簽發、註銷和管理。

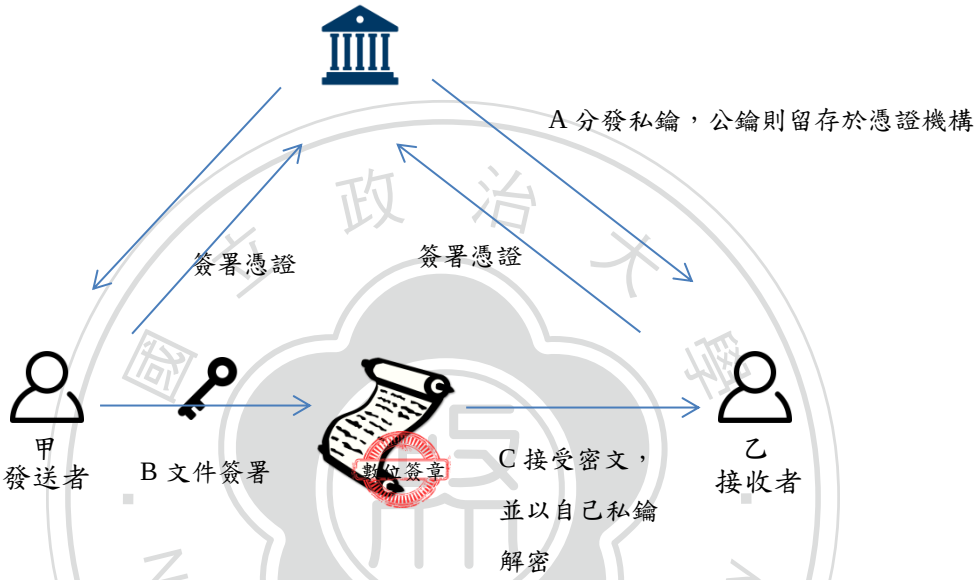

圖 5：憑證機構運作示意圖 (作者自製)

圖 5 憑證機構運作說明：

A 憑證機構負責發行公鑰和私鑰，公鑰會留存在憑證機構，私鑰則會分配予個人。

B 甲欲發送文件給乙，甲至憑證機構查詢乙的數位憑證，若確認乙數位憑證無誤，則甲即可使用對應乙數位憑證的公鑰將文件加密，形成數位簽章。

C 乙收到密文，以自己私密金鑰解密後得到文件訊息。

二、憑證機構之定義

依據明尼蘇達州電子認證法(Electronic Authentication Law) 325K.01 第 5 條、325K.01 第 22 條，「憑證機構」係指發行憑證之人或組織，而依據第

DOI:10.6814/NCCU201901043

325K.01 第 4 條「憑證」係指以下四種電腦紀錄：(1)用以識別憑證發行機構的紀錄；(2)用以命名或識別申請者之紀錄：(3)含有申請者之公鑰；(4)作為憑證機構數位簽署之紀錄[167]。

因此，憑證機構係指發行第 325K.01 第 4 條所指的四種電腦紀錄之自然人或組織，並須向州政府取得許可證照(License)。依據第 325K.05 第 1 條，憑證機構取得許可證照須符合以下八個條件[168]：(1)須向明尼蘇達州州務卿(Secretary of state)[169]取得許可且其儲存憑證之資料庫須獲得認證。(2)所屬員工對於此領域

---

[167] Minnesota Statutes 325K.01§5 (2017), 'Electronic Authentication 'Certification authority" means a person who issues a certificate.' ;

Minnesota Statutes 325K.01§22 (2017), 'Person means a human being or an organization capable of signing a document, either legally or as a matter of fact.';

Minnesota Statutes 325K.05§4 (2017), 'Certificate means a computer-based record that:

(1) identifies the certification authority issuing it

(2) names or identifies its subscriber

(3) contains the subscriber's public key; and

(4) is digitally signed by the certification authority issuing it.'

[168] Minnesota Statutes 325K.05§1 (2017), 'To obtain or retain a license, a certification authority must:

(1) be the subscriber of a certificate issued by the secretary and published in a recognized repository;

(2) employ as operative personnel only persons who have not been convicted within the past 15 years of a felony or a crime involving fraud, false statement, or deception;

(3) employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of this chapter;

(4) file with the secretary a suitable guaranty, unless the certification authority is a department, office, or official of a federal, state, city, or county governmental entity that is self-insured;

(5) use a trustworthy system, including a secure means for limiting access to its private key;

(6) present proof to the secretary of having working capital reasonably sufficient, according to rules adopted by the secretary, to enable the applicant to conduct business as a certification authority;

(7) register its business organization with the secretary, unless the applicant is a governmental entity or is otherwise prohibited from registering;

(8) require a potential subscriber to appear in person before the certification authority, or an agent of the certification authority, to prove the subscriber's identity before a certificate is issued to the subscriber.'

[169] 各州州務卿的職能各有不同，但主要負責事項多為各州之選舉事務，類似我國負責選舉工作之中選會，但明尼蘇達州州務卿除了負責選舉事務外，亦負責憑證機構之認證和許可。(參照

DOI:10.6814/NCCU201901043

有專業知識且不曾犯下欺騙、虛偽陳述、詐欺罪行或 15 年以上之重罪。(3)向明尼蘇達州國務院提交適當之擔保。(4)使用值得信賴之系統，包含對其私鑰限制訪問(Limiting access)之方法。(5)向明尼蘇達州國務院提出營運資金之證明。(6)向明尼蘇達州國務院登記組織。(7)要求憑證用戶(Subscriber)親自至憑證機構或憑證機構之代理人作身分證明(8)遵守明尼蘇達州國務院進一步之許可要求。

三、憑證機構之責任

依據第 325K.11，取得許可之憑證機構對於其憑證用戶(Subscriber)[170]所發行之憑證分為三種擔保責任[171]：1.絕對之擔保責任(Absolute warranties)。2.相對之擔保責任(Negotiable warranties)。3.信賴擔保責任(Warranties to those who reasonably rely)。前兩種擔保責任主要規範憑證機構與憑證用戶(Subscriber)之間的法律關係，絕對擔保責任不能以特約免責，相對擔保責任則允許以特約免責；最後一種擔保責任-信賴擔保責任之主體則是規範憑證機構與信賴憑證機構所核發憑證之第三人的法律關係。

1. 絕對之擔保責任(Absolute warranties)[172]：

係指取得許可之憑證機構對於憑證用戶(Subscriber)針對以下事項負絕對擔

Minnesota Statutes 325K.01§18(2017))

[170] 憑證用戶係指向憑證機構申請憑證之申請者，申請者須提交個人相關資料如出生年月日、身分證字號、電話等，以利憑證機構確認申請者之身分。

[171] Minnesota Statutes 325K.11(2017), 'By issuing a certificate, a licensed certification authority warrants to the subscriber named in the certificate that:
(1) the certificate contains no information known to the certification authority to be false;
(2) the certificate satisfies all material requirements of this chapter; and
(3) the certification authority has not exceeded any limits of its license in issuing the certificate.'

[172] Minnesota Statutes 325K.11§1(2017), 'Absolute warranties to subscribers.By issuing a certificate, a licensed certification authority warrants to the subscriber named in the certificate that:
(1) the certificate contains no information known to the certification authority to be false;
(2) the certificate satisfies all material requirements of this chapter; and
(3) the certification authority has not exceeded any limits of its license in issuing the certificate.'

DOI:10.6814/NCCU201901043

保之責任：(1)憑證中關於憑證機構之資訊[173]皆正確無誤。(2)憑證之發行是符合本法之要求的。(3)憑證機構在合乎條件[174]下發行憑證。

2. 相對之擔保責任(Negotiable warranties)[175]：

除憑證機構與憑證用戶(Subscriber)有特別約定，憑證機構對以下事項負有相對之擔保責任：

(1)暫停或撤銷憑證之義務

當有第 325K.14 條和第 325K.15 條之情形，憑證機構須立即暫停或撤銷其所發行之憑證。

第 325K.14 第 1 條規定兩項非交易用途憑證之絕對暫停憑證事由[176]：

a. 憑證中所記載之憑證用戶(Subscriber)或可能知道私鑰安全之憑證用戶(Subscriber)代理人、商業夥伴、僱員或直系親屬提出暫停憑證之聲請。

b. 根據第 325K.10 條，當憑證之發行未遵守本法規定且對於合理信賴憑證之人造成重大的損害時，由國務院下令暫停憑證。

當有上述所列絕對暫停憑證事由，並已給予憑證機構關於行政程序法所給

---

173 憑證機構資訊如是否為獲得政府認證之憑證機構、憑證機構所使用的數位簽章演算法等。

174 發放憑證前應先確認憑證資訊無誤、是否收到用戶之請求等。

175 Minnesota Statutes 325K.11§2(2017), 'Negotiable warranties to subscribers. Unless the subscriber and certification authority otherwise agree, a certification authority, by issuing a certificate, promises to the subscriber:
(1) to act promptly to suspend or revoke a certificate in accordance with section 325K.14 or 325K.15;and
(2) to notify the subscriber within a reasonable time of any facts known to the certification authority that significantly affect the validity or reliability of the certificate once it is issued.'

176 Minnesota Statutes 325K.14§1(2017), '(1) upon request by a person identifying himself or herself as the subscriber named in the certificate, or as a person in a position likely to know of a compromise of the security of a subscriber's private key, such as an agent, business associate, employee, or member of the immediate family of the subscriber; or
(2) by order of the secretary under section 325K.10.'

DOI:10.6814/NCCU201901043

予之程序保障後，國務院應發布暫停憑證之命令，但暫停期間不得超過 96 小時。

第 325K.14 第 2 條規定相對暫停憑證事由[177]：

a. 憑證中所記載之憑證用戶(Subscriber)或憑證用戶(Subscriber)代理人、商業夥伴、僱員或直系親屬提出暫停憑證之聲請。

b.請求者指出憑證機構已無法提供服務(unavailable)。

當有上述相對暫停憑證事由，國務院得向請求憑證暫停者要求其提供證據，並得決定是否暫停憑證。因此當國務院有暫停事由而下令暫停憑證時，憑證機構須遵守國務院之命令立即暫停或撤銷憑證之發行。

(2)通知義務

當憑證機構知悉任何影響憑證的有效性和信賴性的事實，應在合理時間內通知憑證用戶(Subscriber)。

3. 信賴擔保責任(Warranties to those who reasonably rely)[178]

取得許可之憑證機構對於信賴其所發行憑證之人負有以下信賴擔保責任：

---

[177] Minnesota Statutes 325K.14§2(2017), 'Suspension for 96 hours; other causes. (a) The secretary may suspend a certificate issued by a licensed certification authority for a period of 96 hours, if:

(1) a person identifying himself or herself as the subscriber named in the certificate or as an agent, business associate, employee, or member of the immediate family of the subscriber requests suspension; and

(2) the requester represents that the certification authority that issued the certificate is unavailable.'

[178] Minnesota Statutes 325K.11§3(2017), ' Warranties to those who reasonably rely. By issuing a certificate, a licensed certification authority certifies to all who reasonably rely on the information contained in the certificate that:

(1) the information in the certificate and listed as confirmed by the certification authority is accurate;

(2) all information foreseeably material to the reliability of the certificate is stated or incorporated by reference within the certificate;

(3) the subscriber has accepted the certificate; and

(4) the licensed certification authority has complied with all applicable laws of this state governing issuance of the certificate.'

DOI:10.6814/NCCU201901043

a.憑證上所記載的資訊是正確的。

b.可預見之關於信賴的重要資訊皆在憑證中被陳述或做為參考。

c. 憑證用戶(Subscriber)已接受憑證。

d.憑證機構已遵循州內關於發行憑證之相關法律。

四、憑證機構之罰則

違反本法規定之取得許可之憑證機構，依據第 325K.07 條，有以下之罰則[179]：

1.接受調查

國務院得發布命令並行使調查權以確保憑證機構遵守本法。

2.暫停或撤銷

若憑證機構未遵守國務院之命令，國務院得暫停或撤銷憑證機構之許可證。

3.民事懲罰(Civil penalty)

若憑證機構違反本法規定，國務院得向其徵收罰款，每次違規事件所徵收之金額不能超過 5000 美元。

---

[179] Minnesota Statutes 325K.7(2017), '

1. Investigation. The secretary may investigate the activities of a licensed certification authority material to its compliance with this chapter and issue orders to a certification authority to further its investigation and secure compliance with this chapter.
2. Suspension or revocation. The secretary may summarily suspend or revoke the license of a certification authority for its failure to comply with an order of the secretary.
3. Civil penalty. The secretary may by order impose and collect a civil monetary penalty against a licensed certification authority for a violation of this chapter in an amount not to exceed $5,000 per incident. In case of a violation continuing for more than one day, each day is considered a separate incident. The secretary may adopt rules setting the standards governing the determination of the penalty amounts.
4. Payment of costs. The secretary may order a certification authority, which it has found to be in violation of this chapter, to pay the costs incurred by the secretary in prosecuting and adjudicating proceedings relative to the order, and enforcing it.'

DOI:10.6814/NCCU201901043

4.支付費用

若憑證機構違反本法規定，國務院得要求其支付國務院起訴或裁定之相關程序費用。

第三款 時間戳

UETA 並未對時間戳有所定義，但採用 UETA 之明尼蘇達州另設電子認證法以對時間戳作相關之規範。

一、明尼蘇達州電子認證法(Electronic Authentication Law)

(一)時間戳之定義

依據第 325K.01 第 37 條，時間戳係指附加於訊息、數位簽章以確認數位簽署之標記，並至少指名日期、時間和註記時間戳之人的身分[180]。

(二)時間戳之法律效力

第 325K.24 第 1(d)條規定，若遇電子簽章之爭議，推定數位簽章是由公正第三方使用可值得信賴系統加蓋時間戳前所創立的[181]。第 325K.24 第 2 條更進一步指出法院應參酌此章規定作出合理之責任分配判決[182]。因此，條文雖未明確指出時間戳於法律上之效力，但由第 325K.24 第 1(d)條、第 2 條可知，若時間戳係由公正第三方利用可值得信賴之系統所加註且對其有所爭執之一方無法舉反證推翻，則可推定簽署數位簽章之時間點一定在時間戳所指名之時間之後，法院應以此事實作為責任分配判決的衡量依據，由此可知，時機戳提供時

[180] Minnesota Statutes 325K.01§37(2017), '"Time stamp" means either:
(1) to append or attach to a message, digital signature, or certificate a digitally signed notation indicating at least the date, time, and identity of the person appending or attaching the notation; or
(2) the notation thus appended or attached.'

[181] Minnesota Statutes 325K.24§1(d)(2017), 'A digital signature was created before it was time stamped by a disinterested person utilizing a trustworthy system.'

[182] Minnesota Statutes 325K.24§2(2017), 'A court of this state shall give effect to liability allocations between the parties provided by contract to the extent not inconsistent with the requirements of this chapter.'

DOI:10.6814/NCCU201901043

間序列上的證明，並由對方負擔舉證責任。

第二節 歐盟電子身分認證與信賴服務規章 eIDAS 介紹

第一項 立法歷程

一、背景

美國各州於 1995 年陸續制定電子簽章法，刺激與美國競逐全球電子商務發展龍頭的歐盟亦開始著手規劃相關法制框架，以促進跨國電子商務發展。1997 年德國即率先制定通過「聯邦資訊與電信服務架構條件法」[183]，其中的第三章即是關於數位簽章之規定，開啟歐盟電子簽章法立法之先河。

二、 1999/93/EC 指令誕生

1997 年 4 月 18 日歐盟執委會(下稱「執委會」)提出了一份電子商務倡議(European initiative on electronic commerce)，基於於電信自由化使得電信服務之總體價格下降，進而帶動互聯網使用率之增加和電子商務之多元應用[184]，執委會建議應建立統一監管框架，以加強跨國電子商務的信任和信心。1997 年 10 月 8 日執委會[185]提出《確保電子通訊安全和信任-邁向歐洲數位簽章和加密之整體架構》(Ensuring Security and Trust in Electronic Communication-Towards a

[183]原文 Gesetz des Bundes zur Regelung der Rahmenbedingungen fuer Informations- und Kommunikationsdienste--IuKDG)，簡稱「多元媒體法」（das Multimedia-Gesetz）

[184] European initiative on electronic commerce, available at： https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al32101 (Last visited on 2019/07/01)

[185] Amended proposal for a European Parliament and Council Directive on a common framework for electronic signatures, available at： http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1523186153809&uri=CELEX:51999PC0195 (Last visited on 2019/07/01)

DOI:10.6814/NCCU201901043

European framework for Digital Signatures and Encryption)，1997 年 12 月 1 日歐盟理事會回應表示歡迎，並請執委會盡快提交關於數位簽章指令的提案。歐洲議會亦於 1998 年 7 月 17 日的決議（A4-0189 / 98）中強調歐洲須建立一個法律框架，以確保數位簽章之信任以促進電子商務和電子通訊之發展。1998 年 5 月 13 日執委會正式提出《關於電子簽名之共同架構》草案(a proposal for a European Parliament and Council Directive on a common framework for electronic signatures)，最終於 1999 年 12 月 13 日通過《1999/93/EC 歐洲議會及理事會關於電子簽章整體架構指令(Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures，簡稱 1999/93/EC)，並於 2000 年 1 月 19 日生效。

三、eIDAS 承先啟後

1999/93/EC 是指令(Directives)之性質，最初旨在提供一個法律框架來鼓勵和促進歐盟地區使用電子簽名，並促進電子商務跨境之發展，但因為只是一個立法框架，歐盟會員國只須依照指令規劃之目標框架制定國內法即可，以致會員國間立法歧異，造成市場破碎化，不利區域整合與歐盟委員會於 2005 年所提之「數位單一市場策略」(Digital Single Market strategy)之達成[186]。因此歐盟於 2014 年 9 月 17 制定「電子身分認證與信賴服務規章」(The Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market ,簡稱 eIDAS)，並廢除 1999/93/EC 指令。

eIDAS 是規章(Regulation)，為具有強制力性質之法律，直接適用於所有會員國，除了消弭 1999/93/EC 指令所造成各會員國間之立法歧異，並確保整個歐

[186] Adobe(2016), Compliance with European electronic signatures legislation, p2, available at：https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-sign-eidas-compliance-uk.pdf (Last visited on 2019/07/01)

DOI:10.6814/NCCU201901043

盟和非歐盟會員國對電子簽名和證書的跨境認證[187]。

第二項 立法目的及立法原則

1999/93/EC 指令旨在提供電子簽章一個適當法律框架和標準，並承認其法律上效力，以回應資訊科技基礎設施快速革新所帶動之全球電子商務發展。eIDAS 亦延續此宗旨，並透過規章(Regulation)的規範方式，提供更為安全、可靠和易於使用的跨境(Cross-border)和跨部門(Cross-sector)電子交易之法律框架，並加強和擴展 1999/93/EC 所欲達成之目標[188]。

其立法遵循的立法原則如下：

(一) 技術中立原則。電子簽章技術只要能滿足本規章之要求，應賦予法律上效力，而不應給予差別待遇[189]。

(二) 一般流通性原則。承認高度安全保證之電子簽章以確保相互承認，但為了實現單點聯繫(points of single contact)與促進電子簽章跨界使用的目標[190]，也應接受安全保證度較低之電子簽章。

---

187 eSignature in the EU, available at：http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l24118 (Last visited on 2019/07/01)

188 eIDAS preface(3), available at：http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (Last visited on 2019/07/01)

189 eIDAS preface(27), available at：http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG#ntr10-L_2014257EN.01007301-E0010 (Last visited on 2019/07/01)

190 eIDAS preface (48), available at：http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2009.274.01.0036.01.ENG&toc=OJ:L:2009:274:TOC (Last visited on 2019/07/01)

DOI:10.6814/NCCU201901043

第三項 電子簽章立法規範

第一款 電子簽章類型

eIDAS 中定義了三種類型的電子簽章，基本電子簽章、進階電子簽章、合格電子簽章。

一、基本電子簽章(Standard electronic signatures)

(一)定義

依照第 3.10 條「基本電子簽章」係指一電子形式的數據，附加於或邏輯地[191]與其他電子形式數據相關聯，並提供簽名人用於簽署之目的[192]。

由條文可知形成基本電子簽章有三個要件：

1. 存在一電子形式的數據。
2. 與其他電子形式數據有附加或邏輯上之關聯。
3. 簽名人用於簽署之目的。

這些要件在 eIDAS 中並未有更詳盡的定義或解釋，因此存有相當大的解釋空間。

另根據前言(26)、(27)亦指出隨著資訊技術的進步，本法應採取開放創新的方法，並保持技術中立原則，只要滿足本法之要件，任何電子簽章技術都應賦予法律上之效力[193]。

---

[191] eIDAS 並未針對何謂邏輯地與其他電子數據相關聯作出解釋，但對照美國統一州法委員會提出的 UETA 註釋本中指出由於電子簽章不像紙本簽章有一實體介質如紙、文書供其有形附著(attached)，因此使用邏輯地關聯(logically associated with)一詞描述電子簽章與其他電子數據透過演算法而無形附著的表現形式。另可參照註 114。

[192] eIDAS §3.10(2014) , ‘electronic signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.’

[193] eIDAS Preamble(26)，‘Because of the pace of technological change, this Regulation should adopt an approach which is open to innovation.’ ;
eIDAS Preamble(27), ‘This Regulation should be technology-neutral. The legal effects it grants should

DOI:10.6814/NCCU201901043

綜合上述，只要能取得簽署人之簽署意願並驗證傳輸文件之真偽之電子工具皆能稱為基本電子簽章，如 PIN code、對稱式或非對稱式加密技術、人類生理外貌辨識、指紋辨識、瞳孔虹膜辨識、聲紋辨識、ＤＮＡ比對辨識等皆符合基本電子簽章之定義。

(二)法律效力

依照第 25.1 條，基本電子簽章不得僅因其是電子的形式或不符合格電子簽章的要求而否定其法律上效力或作為法律上證據之能力[194]。

因此，會員國得自由規定基本電子簽章在法律上效力或證據上之能力，但不能因其是電子的形式或不符合格電子簽章要件等理由，而拒絕使用或否定其法律上效力和法律上證據之能力。惟須注意的是，這不代表基本電子簽章具有與傳統手寫簽名相同之法律效力或待遇。

二、進階電子簽章(Advanced electronic signatures)

(一)定義

依照第 3.11 條，「進階電子簽章」係指符合第 26 條四個要件之電子簽章[195]：

1. 與簽署人有唯一之聯繫。

---

be achievable by any technical means provided that the requirements of this Regulation are met.'

[194] eIDAS §25.1(2014) , 'An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.'

[195] eIDAS §3.11(2014) , 'advanced electronic signature means an electronic signature which meets the requirements set out in Article 26.';

eIDAS §26(2014), 'An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.'

DOI:10.6814/NCCU201901043

2. 能識別簽署人身分。

3. 簽署人可高度信賴並單獨控制。

4. 與簽署之數據相關聯，故能偵測到數據之任何更改。

(二)法律效力

eIDAS 中並未就進階電子簽章之法律效力進行特別規範，因此其法律上效力仍應回歸適用基本電子簽章之規範。但若進階簽章滿足特定之法律要件，則稱為合格電子簽章，而合格電子簽章之法律效力 eIDAS 即有明文規定，因此可將進階電子簽章看作合格電子簽章製作之基礎要件。

三、合格電子簽章(Qualified electronic signatures)

(一)定義

依照第 3.12 條，「合格電子簽章」係指進階電子簽章依據合格憑證和合格的電子簽名產製設備所製作[196]。因此可知合格電子簽章要件有三：

1.須滿足進階電子簽章之要件

2.依據一份有效的合格憑證[197]所簽署

3.由合格的電子簽名產製設備所製作。

(二)法律效力

依照第 25.2 條，合格的電子簽章與手寫簽名具有同等法律上效力[198]。第 25.3 條更進一步規定，歐盟會員國依據 eIDAS 合格電子簽章之要件所簽署之合格電子簽章，其他歐盟會員國亦應承認之[199]。此條規定消弭了 1999/93 / EC 指

[196] eIDAS §3.12(2014), 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures'

[197] 依據第 2.14 條合格憑證係指由合格信任服務提供者所發行並滿足附件 I 之要求。

[198] eIDAS §25.2(2014),' A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.'

[199] eIDAS §25.3(2014),' A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.'

DOI:10.6814/NCCU201901043

令造成會員國間對於電子簽章定義和法律效力立法歧異之情形，並透過法律上之互相承認來實現安全和跨境之電子交易。

第二款 中心化憑證機構主體責任

一、信任服務提供者[200]之定義

依照第 3.16 條「信任服務」係指以下三種服務：1.有關電子簽名、電子印章或電子時間戳之製作、驗證和確認等相關服務。2.網路憑證之製作、驗證和確認。3.保存與電子簽名、電子印章或憑證等相關之服務[201]。

依照第 3.19 條，「信任服務提供者」係指提供一項或多項信任服務的自然人或法人，而此信任服務提供者可為合格信任服務提供者，亦可為非合格的信任服務提供者[202]。

二、信任服務提供者之責任

依照第 13.1 和 13.2 條規定，信任服務提供者因故意或過失而未遵守本法之義務並造成自然人或法人之損害，須負擔損害賠償責任。但若信任服務提供者事前已告知客戶信任服務之使用限制且此使用限制可由第三方機構進行確認，則信任服務提供者不須為客戶超過使用限制之行為負責[203]。

---

[200] eIDAS 中係以 trust service provider 指稱提供電子簽章身分認證的機構；而 UETA 中則以 Certification authority 一詞，中文多譯成憑證機構，也是國內較常看到的名稱。兩者名詞雖有不同，但其功能和內涵皆相同。

[201] eIDAS §3.16(2014),' trust service' means an electronic service normally provided for remuneration which consists of:
(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
(b) the creation, verification and validation of certificates for website authentication; or
(c) the preservation of electronic signatures, seals or certificates related to those services;

[202] eIDAS §3.19(2014) , 'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider'

[203] eIDAS §13.1(2014), 'Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply

DOI:10.6814/NCCU201901043

而關於舉證責任部分，依非合格信任服務提供者和合格信任服務提供者區別其規定。若是「非合格信任服務提供者」之服務，當有損害發生，須由客戶對其損害和因果關係負擔舉證之責；若是「合格信任服務提供者」[204]之服務，當有損害發生，則推定其有故意或過失，除非合格信任服務提供者能舉證無過失，否則應負損害賠償責任。

綜合上述，非合格信任服務提供者原則上負擔過失責任，並由客戶負擔舉證責任；合格信任服務提供者的部分，因其已通過本法規定之認證，相較於非合格信任服務提供者，本法課予較為嚴格之推定過失之責任，且將舉證責任倒置由合格信任服務提供者自己舉證無故意或過失。此外，兩者若事前已告知客戶相關之使用範圍限制，則不負損害賠償責任。

第三款 電子時間戳

一、定義

依照第 3.33 條，「電子時間戳」係指電子形式的數據，以電子形式將其他電子形式數據綁定至特定時間[205]。

另依照第 3.34 條，「合格電子時間戳」係指滿足第 42 條規定之要件之電子時間

with the obligations under this Regulation.

The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.

The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.';

eIDAS §13.2(2014), 'Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.'

[204] 依據 eIDAS§3.20(2014)合格信任服務提供者係指監理機關授予合格資格的信任服務提供者。

[205] eIDAS §3.33(2014), 'electronic time stamp means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.'

DOI:10.6814/NCCU201901043

戳。而第 42 條指出合格電子時間戳應符合以下三個要件[206]：

1.使其以日期、時間綁定之資料無法在不被偵測之情況下任意更改。

2.以世界協調時間(Coordinated Universal Time)作為標準時間。

3.以合格信任服務提供者提供之進階電子簽章或其他等效之方法進行簽署。

二、法律效力

第 41.1 條係電子時間戳之一般性效力，其規定不能僅因時間戳為電子形式或不符合本法合格電子時間戳之要件，而否認其作為法律上證據之能力[207]。

而第 41.2 條則針對合格電子時間戳之法律效力有進一步之規定，若被認定為合格電子時間戳，則推定具有日期和時間上之準確性且其所綁定之資料亦具有完整性[208]。

此外，歐盟會員國所發行之合格電子時間戳，亦應被其他會員國所承認。

[206] eIDAS §42(2014), 'A qualified electronic time stamp shall meet the following requirements:
(a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
(b) it is based on an accurate time source linked to Coordinated Universal Time; and
(c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.'

[207] eIDAS §41.1(2014), 'An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.'

[208] eIDAS §41.2(2014), 'A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.'

DOI:10.6814/NCCU201901043

第三節 區塊鏈技術與國際電子簽章法之相容性

第一項 區塊鏈簽章與電子簽章定義

第一款 傳統簽章之目的及功能

從部落至工商社會，為了讓雙方不會因為口頭約定而造成誤解或爭執，確保雙方交易安全，因此多以契約書面將約定事項記載於紙本，並於契約上簽章，以作為雙方不可否認之證據，傳統上簽章的目的及功能如下[209]：

(1)識別簽署人的來源(識別功能)

(2)確保文件的完整性(認證功能)

(3)簽署人身分的真實性證明(不可否認功能)

(4)簽署人意向之表達(表達意向功能)

(5)證明契約的存在(證據功能)

第二款 電子簽章之定義及法律效力

一、電子簽章定義

美國 UETA 第 2(8)條將「電子簽章」定義為附屬於紀錄或邏輯上有關聯的電子聲音、象徵，由某人執行或接受，並有於該紀錄簽章之意圖[210]。

歐盟 eIDAS 則區分三種不同類型之電子簽章，並定有不同法律要件和效力。最為基礎類型之「基本電子簽章」規範於第 3.10 條，係指一電子形式的數據，附加於或邏輯地與其他電子形式數據相關聯，並提供簽名人用於簽署之目

[209] Charlotte Salemans , An analysis of the legal effect of an electronic signature used to sign an agreement in a blockchain application under Dutch law(October 31, 2017), p6, available at：http://www.ubvu.vu.nl/pub/fulltext/scripties/14_2604465_0.pdf

[210] UETA§2(8)(1999), 'Electronic signature" means an electronic sound, symbol, or processattached to or logically associated with a record and executed or adopted by aperson with the intent to sign the record.'

DOI:10.6814/NCCU201901043

的[211]。

兩者皆採技術中立原則，只要電子技術所形成的電子簽章能達到法規要求，法律不應差別待遇或獨厚某種技術，甚至應隨著科技發展而將「電子」一詞作廣義解釋。因此電子簽章技術例如數位簽章、生物辨識、指紋辨識、瞳孔虹膜辨識、聲紋辨識、DNA 比對鑑識等，皆為廣義之電子簽章。

二、電子簽章法律效力

美國 UETA 第 7(a)條[212]與歐盟 eIDAS 第 25.1 條[213]皆規定，不能僅因簽章是電子形式而否認其法律上效力或執行力。但歐盟 eIDAS 另區分三種不同類型之電子簽章：基本電子簽章、進階電子簽章、合格電子簽章，並異其法律效力，符合合格電子簽章之要件者，始與手寫簽名有同等之法律效力，基本電子簽章和進階電子簽章則須再進一步檢驗其電子簽章之可靠性，例如電子簽章生成之技術標準或流程是否安全可靠，以作為法律上效力判斷之依據。

第三款 區塊鏈簽章與現行法之相容性

一、區塊鏈簽章定義

傳統簽章透過人類筆墨字跡的不可偽造、不可否認等特性，使簽署的文件具有法律上效力和商業上之意義，但隨著科技技術進步，偽造人類筆墨字跡已非難事，此外，電子商務蓬勃發展，電子交易逐漸取代傳統面對面的交易，如何確認雙方交易當事人和交易效力成為重要課題，遂發展出電子簽章，以密碼學技術、生物辨識技術，希望杜絕簽名仿造之情事，以維護交易安全。

---

211 eIDAS §3.10(2014) , ‘electronic signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.’

212 UETA§7(a)(1999), ‘A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.’

213 eIDAS §25.1(2014) , ‘An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.’

DOI:10.6814/NCCU201901043

而區塊鏈簽章係指透過區塊鏈技術所保護的簽章，並視為電子簽章的一種[214]。用以證明電子文件是由發送方簽署且傳送的，並確保電子文件的完整性。

二、區塊鏈簽章運行方式

區塊鏈中每一筆交易皆透過數位簽章之簽署，而每一筆交易的標的可以是所有權轉換、版權移轉等，並將交易的軌跡安全記錄在帳本，且不受中間機構的控制，例如比特幣交易系統即是屬於數位貨幣的所有權轉換。

以比特幣為例，寄件者須先確認收件者之位址，以方便進行數位貨幣之所有權轉換，收件者利用 SHA-256 雜湊函數產生私鑰，再利用私鑰進行橢圓曲線加密運算產生相對應之公鑰，算出公鑰後再以 SHA-256 雜湊函數和 RIPEMD-160 雜湊函數得到公鑰之哈希值，此亦為比特幣之位址。

寄件者收到收件者之位址後，亦以 SHA-256 雜湊函數產生私鑰，並進行橢圓曲線加密運算產生對應之公鑰，以私鑰對收件者的位址、交易資料的哈希值進行加密，形成一個數位簽章，並將交易資料、數位簽章和寄件者之公開金鑰一同打包廣播給區塊鏈網絡進行後續驗證。

寄件者是否有效的將比特幣轉移給收件者，並非由收件者進行確認，而是由區塊鏈中的節點進行 POW 競逐取得記帳權，之後取得記帳權之節點須將答案和該筆交易廣播至整個區塊鏈網絡，由全體節點共同進行驗證，驗證節點會以寄件者之公開金鑰對此交易之數位簽章進行解密，解密後會得到一哈希值，此外會再以此筆交易資料、收件者之位址進行單向雜湊函數得到另一個哈希值，將兩個哈希值進行比對，若兩者一致，表示交易資料未遭到竄改，當多數節點利用上述方法驗證交易資料確認無誤，有效交易即成立。

---

[214] 請參照亞利桑那州電子交易法第 44-7061 條(A), 參考網址：https://codes.findlaw.com/az/title-44-trade-and-commerce/az-rev-st-sect-44-7061.html；

、田納西州電子交易法第 47-10-201 條(1)，參考網址：https://publications.tnsosfiles.com/acts/110/pub/pc0591.pdf

DOI:10.6814/NCCU201901043

上述過程讓驗證者得以確認電子資料是由簽署者所發送且其電子資料未遭竄改，以達到不可否認性，至於是否為簽署者本人為之，則非所問，但目前在認許制區塊鏈為方便管理和落實消費者保護，亦設計有中心機構事先進行身分資格的查核，通過後方得加入區塊鏈的管理機制，但開放式區塊鏈為達到匿名性的功能，通常不會進行身分勾稽。

三、區塊鏈簽章與國際現行法之相容性

美國 UETA 和歐盟 eIDAS 為了達成促進電子交易安全與全球電子商務發展之立法目的，並因應資訊科技快速發展，對於電子簽章之定義皆採取抽象、廣義之解釋，不限定電子簽章須由某種特定技術作成。

區塊鏈簽章係以雜湊函數、數位簽章技術確保了所簽署之數據之真實性、完整性，並以時間戳作為特定時間之存在證明，而美國 UETA 和歐盟 eIDAS 對於電子簽章之最基本定義係指，有簽署之意圖並以電子形式的數據附加或邏輯性的關聯於另一電子數據。

因此在美國 UETA 和歐盟 eIDAS 的規範體系下，電子簽章簡單來說就是一電子形式的數據，並附加於所欲簽署之文件[215]或具有邏輯上之關聯，這意味著文件和電子簽章可以作為單獨的電子數據存在，不需要包含在相同的電子數據或資料夾中，只要邏輯上相關聯即可[216]，而區塊鏈簽章亦使用數位簽章技術將區塊鏈簽章附加於交易資料或電子文件並一同打包寄送給收件者，符合兩國電子簽章之定義，惟歐盟 eIDAS 將電子簽章進一步細分為三種類型：基本電子簽章、進階電子簽章、合格電子簽章。基本電子簽章的要件與美國 UETA 電子簽章之定義相同，惟「進階電子簽章」另設有四個要件：

(1)與簽署者有著唯一的聯繫。

[215] 此處的文件是有別於電子簽章的電子數據。

[216] Charlotte Salemans , *supra* note 208, at 10.

DOI:10.6814/NCCU201901043

(2)能夠識別簽署者。

(3)電子簽章係以電子數據資料(electronic creation data)產生，簽署者可高度信賴並擁有獨立的控制權。

(4)與簽署的資料具有連動性，任何資料的變動皆可檢測。

進階電子簽章之規範目的在於加強簽署者和簽署的數據之間的關聯性，可增強簽署人之識別，但與基本電子簽章一樣，仍無法對於簽署人的身分作出真實性的證明。因此，第三種類型之「合格電子簽章」要求須由合格的電子簽章產生設備根據合格憑證以產生簽章，透過合格的第三方 TSP(Trust Service Provider)頒發憑證以認證簽署人身分的真實性，以達到不可否認之功能使簽署人無法否認電子簽章之效力。

綜上所述，區塊鏈簽章符合現行美國 UETA 電子簽章之定義，但在歐盟 eIDAS 將電子簽章區分為三種類型的法律架構下，區塊鏈簽章僅符合 eIDAS 基本電子簽章與進階電子簽章之定義，惟不符合「合格電子簽章」對於簽署人身分真實性證明的要求，區塊鏈技術下之交易並無如電子簽章有所謂的憑證機構此等中間機構針對簽署人(使用者)身分進行查核，因此無法知悉簽署人(使用者)的姓名、信用等個人資料以與其簽章進行連結，故不該當合格電子簽章之要件，亦無法被賦予與手寫簽名相同之法律效力。但若在認許制區塊鏈中，節點加入前多須經過身分查核，因此可能符合合格電子簽章之要求。

第二項 中心化憑證機構之主體責任與區塊鏈分散式節點責任

區塊鏈技術，又可稱為分布式帳本技術(Distributed Ledger Technology)，讓以往中心化的資源分配和風險管理的模式轉變為分布式(Distributed)，換言之，節點與節點之間無需有一中心節點主導資訊交換、風險管理或身分認證，因

DOI:10.6814/NCCU201901043

此，這樣去中心化而有多重主體參與的區塊鏈網絡，其法律關係和責任是否應有所不同即有討論的空間，因此以下先探討現行電子簽章法對於憑證機構此中心主體的法律責任，再分析區塊鏈分散式節點的特性，並建構可能的法律關係，以得出現行電子簽章以中心主體作為規範主軸的法律關係是否能適切反映區塊鏈分散式節點運作的特性。

第一款 中心化憑證機構之主體責任

美國 UETA 並未對憑證機構作出相關規範，各州中亦僅有明尼蘇達州以電子認證法明文規範憑證機構的三種責任，這應與美國前總統 Bill Clinton 於 1997 年提出之互聯網監管政策-全球電子商務框架(The Framework for Global Electronic Commerce)[217]有關，其確立所謂不傷害準則(Do no harm approach)[218]，並認為資訊科技時代應多藉由私人協議或市場機制來解決問題，而非採行由上而下之傳統監管框架[219]，因此對比歐盟明文規範憑證機構之責任，美國傾向以主導國際標準訂定的方式如 PKI 架構(Public Key Infrastructure) [220]，讓業者自主遵守，並透過市場競爭和監督的力量淘汰不適任之業者，政府只須採取最低度、可預測性之干預措施，避免扼殺資訊科技指數式的發展能量[221]。

---

[217] A Framework for Global Electronic Commerce Executive Summary, *supra* note 112.

[218] 源自於 Hippocratic Oath，原為西方行醫者作為警惕自我的誓詞，認為醫生的首要考慮是切勿傷害到病人。

[219] Adam Thierer, 15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm, available at： https://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm/#69bebc471703 (Last visited on 2019/07/01)

[220] PKI (Public Key Infrastructure)，又稱為公開金鑰基礎架構，是一個具有中心管理者、參與者、硬體、軟體、管理流程規範的基礎架構，目的是為了將使用者的個人身分和公開金鑰進行連結，進行使用者的憑證申請、管理，以確保使用者身分驗證(Authentication)和電子訊息交換的完整性(Integrity)、不可否認性(Non-repudiation)和信賴(Confidentiality)。

[221] Marco Dell'Erba, Demystifying technology. Do smart contracts require a new legal framework? Regulatory fragmentation, self-regulation,public regulation(May 17, 2018), p29-30, available at：

DOI:10.6814/NCCU201901043

歐盟 eIDAS 從憑證機構的定義、注意義務、損害賠償責任、舉證責任皆有清楚之規定，有別於美國傾向最低管制態度，歐盟對於憑證機構的責任採取明文規範方式，對於業者有強制力，使用者保障也較為周全。

惟須注意的是，美國和歐盟皆未對電子簽章是否須設立憑證機構作一明確規範，美國無，歐盟則以是否為合格憑證機構所簽署之電子簽章區分為基本電子簽章、進階電子簽章、合格電子簽章，而異其法律上之效力；換言之，電子簽章於美國、歐盟法律上之生效並非以能否識別電子簽章使用者的身分真實性為必要，也不必然需有中心化憑證機構之存在。

第二款 區塊鏈分散式節點責任

區塊鏈是一去中心化之帳本資料庫系統，在資訊科技中每個節點代表著一台計算機，並共同維護著帳本上資料之完整性和正確性。

而各國法律通常規範的是人對物基於所有權的使用、收益和控制關係，因此計算機本身(節點)並不會是責任主體，對於計算機(節點)行使控制和操縱的自然人或法人才可能是法律上之主體，並基於契約責任或侵權責任對受損害之另一方當事人負法律上之責任，但由於計算機被人所使用，猶如人之手足延伸，因此本文直接以節點稱之，不再作名詞上之區分，合先敘明。

欲釐清區塊鏈網絡節點上之法律上之責任，須先確認區塊鏈之類型，並識別網絡上節點之角色和任務後才能對於每個節點進行定性，並賦予相應之法律上權利義務關係。

目前區塊鏈類型可區分為開放式區塊鏈(Permissionlesss Blockchain)和認許制區塊鏈(Permissioned Blockchain)，兩者最大差別在於節點之加入是否隨時處於自由開放之狀態，因此節點責任亦可能有所不同。

一、開放式區塊鏈

https://ssrn.com/abstract=3228445

DOI:10.6814/NCCU201901043

(一)簡介

又稱為公有鏈(Public blockchain)。對全世界所有人開放，完全的去中心化，每個加入之節點皆可查閱帳本、發起交易與驗證交易，節點透過競逐記帳權和驗證交易獲得一定之經濟獎勵，以維持各節點共同維護帳本之誘因。

(二)責任主體

公有鏈對於所有人開放之特色，讓其節點之數量和屬性處於一個浮動之狀態，但仍可歸類為以下三種主體[222]：

1. 核心開發者：建立區塊鏈之程式設計者，具有資訊技術能力和話語權之核心開發者。

2.驗證節點：運行於區塊鏈之節點，並利用本身運算資源對交易進行驗證。

3.區塊鏈應用系統使用者：使用服務提供者提供之區塊鏈相關服務，例如利用交易所服務取得比特幣之擁有者。

開放式區塊鏈網絡服務中可區分上述三種利害關係人，而欲討探節點之責任，則應聚焦於第一和第二種類型之利害關係人，係因驗證者必為區塊鏈中之節點，其適用區塊鏈之運行規則，並投入本身運算資源為新增之交易進行驗證，而核心開發者則是建構區塊鏈的核心人物，兩者皆參與分散式帳本的實際運作，因此是本文欲探討之責任主體。

(三)責任內容

1. 與傳統輻射式網絡比較

(1)傳統輻射式網絡特性

傳統企業資訊系統架構常使用輻射式網絡(Hub and Spoke model)處理數據的交換和維護，建立一個或數個數據處理中心(Hub)，再將每個 Hub 連結數個子節點(分公司)，由 Hub 作為樞紐處理各方節點的資訊，不僅在設計上較為便利，

[222] Zetzsche, Dirk A. and Buckley, Ross P. and Arner, Douglas W., *supra* note 21, at 21-22.

DOI:10.6814/NCCU201901043

當網絡中任一節點出現系統故障，也能迅速隔離有問題之節點，易於管理和維護，但此種模型最大缺陷在於若數據處理中心(Hub)受到攻擊，則整個網絡將陷於停擺，容易造成「單點淪陷、全部淪陷」(Single Point of Failure, SPOF)的弊病，系統可靠度因而受到影響[223]。

(2)傳統輻射式網絡法律關係

傳統輻射式網絡應用於企業資訊架構代表著物理上硬體設備連接和邏輯上資訊交換之模型和架構，但亦可抽象地描述商業上的利益關係或法律關係。

幅射式網絡中各方節點皆代表著一個法律上責任主體，雖追求著共同之商業利益，但每個節點僅與中心(Hub)有著雙邊契約關係，與其他節點間並無任何法律上關係，因此當某個節點的不正當行為侵害整個網絡之商業利益，只有中心(Hub)能透過契約向此節點主張損害賠償責任，其他節點雖然亦受到商業上之損害，但基於債之相對性，無法向此節點主張任何契約責任；而關於侵權責任，則會落入有無任何權利受到侵害和經濟上損失是否能請求的討論[224]。

2. 區塊鏈分散式網絡

(1)特性

區塊鏈最重要的設計在於以分散的方式將記錄資訊之帳本分別儲存在各個節點上，透過共識機制進行溝通以確保帳本上資訊更新的一致性和正確性，讓每個節點處於平等之地位共同參與帳本之維護，與傳統輻射式網絡由中心機構(Hub)單一維護一個帳本，並與其他節點僅有抽象之商業利益連結關係而無物理技術上之連結有很大之不同。

---

[223] C. W. Von Bergen, Martin S. Bressler, Never Underestimate the Power of a Backhoe: Integrating Single Points of Failure into Strategic Planning (2014), p4-6, available at：http://homepages.se.edu/cvonbergen/files/2015/03/Never-Estimate-the-Power-of-a-Backhoe_Integrating-Single-Points-of-Failure-into-Strategic-Planning.pdf

[224] *Id*. at 26-27.

DOI:10.6814/NCCU201901043

(2)法律關係

區塊鏈去中心化、分散式的設計，讓資料的存取、處理和管理都不是由單一節點獨自為之，由傳統中央權力機構掌握資源分配之話語權的模式轉變為平均分權(Shared control)的模式，權力下放至各個節點，每個節點都掌握著維護帳本的權利，與傳統以中心機構維護帳本，並由其擔負帳本正確性和完整性的全部責任有別，在開放式區塊鏈中，法律關係已非單純中心和節點之雙邊契約關係，共同目標和利益之追求與分散式共同維護帳本的運作模式，形成了多邊契約(Multi-party contract)或合資(joint venture)、合夥(partnership)的法律關係[225]；而侵權責任則會落入有無任何權利受到侵害和經濟上損失是否能請求的討論。

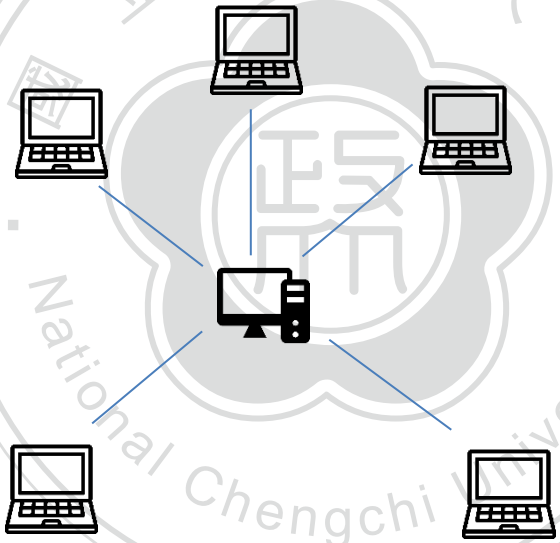

圖 6：輻射式網絡(作者自製)

[225] Zetzsche, Dirk A. and Buckley, Ross P. and Arner, Douglas W., supra note 21, at 28.

DOI:10.6814/NCCU201901043

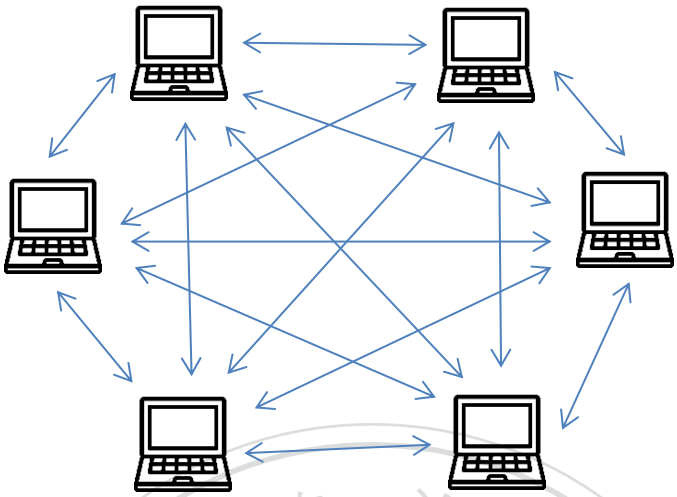

圖 7：區塊鏈分散式網絡(作者自製)

A.契約關係

(A)普通法系

a. 開放式區塊鏈

根據美國法律整編契約法第二版第 17 條(1)、第 21 條和第 22 條(1)可知英美法中契約具備四個要件要約(Offer)、承諾(Acceptance)、約因(Consideration)、受法律約束的意圖(Intention of create legal relationship)[226]。據此，契約的成立即是兩人以上為特定目的且有受法律約束的意圖，而互為合致之締約的意思表示，而意思表示多屬明示，然而亦有雙方並無明示的言詞，但從當事人行為、

[226] Restatement of The Law(Second) Contracts §17 Requirement Of A Bargain (1), 'Except as stated in Subsection (2), the formation of a contract requires a bargain in which there is a manifestation of mutual assent to the exchange and a consideration.';
Restatement of The Law(Second) Contracts §21 Intention to Be Legally Bound , 'Neither real nor apparent intention that a promise be legally binding is essential to the formation of a contract, but a manifestation of intention that a promise shall not affect legal relations may prevent the formation of a contract.'
Restatement of The Law(Second) Contracts §22 Mode of Assent: Offer and Acceptance (1), 'The manifestation of mutual assent to an exchange ordinarily takes the form of an offer or proposal by one party followed by an acceptance by the other party or parties.

DOI:10.6814/NCCU201901043

客觀環境或雙方的關係等事實推斷雙方有承諾之意思表示者，亦成立所謂事實上契約[227](Contract implied in Fact)。

開放式區塊鏈中，以比特幣為例，各參與之節點或比特幣開發者間並無明示或事先透過簽訂協議之方式而有法律上之契約關係，任何想加入比特幣區塊鏈參與挖礦，只須下載並運行挖礦程式，即可以開始挖礦成為區塊鏈之節點，關閉程式即可退出，因此挖礦程式與現行美國法院所承認的線上電腦軟體按鍵契約(Clickwrap agreement)有所不同，線上電腦軟體按鍵契約是美國法院於 2000 年為因應電子商務之興起而發展的概念，係指使用者在使用網站或相關服務前，網路服務提供者會在網頁呈現一個彈出式屏幕(Pop-up window)，並列出服務條款，使用者須按下「我同意」按鍵方能繼續使用網站服務。其突破傳統契約法要約(Offer)或承諾(Acceptance)等意思表示須以言語或書寫的方式為之，當使用者按下同意鍵時，雙方即成立契約，至於使用者是否確實閱讀彈出視窗上之條款、當事人對於契約條款是否協商過程皆在所不問，只要雙方當事人清楚知悉彈出視窗上之契約條款的存在或網路服務提供者有盡到通知使用者有此條款之義務即可[228]，但在如比特幣的開放式區塊鏈中，無預先設定此類彈出視窗的同意按鍵，如何確定區塊鏈之節點或開發者是否有明確意思表示願意受到契約上之拘束並負有契約上責任容有疑慮。

但根據美國最高法院承認事實上契約理論，縱無明示的意思表示，為了公平與衡平之法理，仍可依照當事人行為、關係或環境等客觀事實而成立契約關

---

[227] 在 USC, in re Baltimore & Ohio R. Co. v. United States(1923)案件中，美國最高法院承認事實上契約的存在亦指出事實上契約之定義：an agreement ‘implied in fact,’ founded upon a meeting of minds, which, although not embodied in an express contract, is inferred, as a fact, from conduct of the parties showing, in the light of the surrounding circumstances, their tacit understanding.

[228] R3 and Norton Rose,Can smart contracts be legally binding contracts?, p27-29, available at：http://www.nortonrosefulbright.com/files/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf

DOI:10.6814/NCCU201901043

係[229]；此外美國 UETA 中亦加入「電子代理人」的概念，其係指計算機程式或電子或其他自動化手段，用於獨立發起行動或回應全部或部分之電子紀錄和執行，並未經自然人干預或審查[230]。因此，契約行為意思表示合致行為，亦能透過電子代理人進行，簡言之，雙方可不經由當面口頭或書面的方式即能成立意思表示合致之契約行為，例如自動販賣機販售飲料，消費者透過投幣與電子代理人互動，意即販賣機嵌入式系統中的一連串事先經過安裝的程式和指令進行進行買賣契約之意思表示，仍可成立契約行為而受到拘束。

區塊鏈之開發者和驗證者共同參與分散式帳本之運作，縱無明示而成立契約關係，仍可能因為共同開發、維護，並基於同一利益的行動等客觀事實，而被認定具有契約上的關係。

而此契約上關係類型近於合夥關係(Partnership)，依據美國統一合夥法(Uniform Partnership Act)第 102(11)、202 條，合夥係指兩人或兩人以上之商業組織(business organization)，以獲取利益為目的並以共同經營方式實行相關活動[231]，而成為合夥人的方式不限以金錢出資，亦能以提供勞務或其他利益為之[232]，因此合夥財產的組成不限於金錢，亦可包含有體、無體財產或任何利益

---

[229] Lumhoo v.Home Depot USA，Inc.，229 F.Supp。2d 121,160（EDNY 2002）法院認為原告提供了足夠的客觀證據支持當事人與雇主曾訂立只要超過 8 小時的工作時間即以加班費率計算加班費之「口頭合同」的推論。

[230] UETA§2(6) ‘ “Electronic agent” means a computer program or an electronic or otherautomated means used independently to initiate an action or respond to electronicrecords or performances in whole or in part, without review or action by anindividual.’

[231] Uniform Partnership Act (1997)(Last Amended 2013)§102(11), ‘ Partnership means an association of two or more persons to carry on as co-owners a business for profit formed under this [act] or that becomes subject to this [act] under [Article] 11 or Section 110. The term includes a limited liability partnership.’

[232] Uniform Partnership Act (1997)(Last Amended 2013) §403,‘A contribution may consist of property transferred to, services performed for, or another benefit provided to the partnership or an agreement to transfer property to, perform services for, or provide another benefit to the partnership.’;

DOI:10.6814/NCCU201901043

[233]；主觀上是否有意成立合夥關係在所不問，並強調合夥的核心概念在於以協議進行控制權的共享和利潤的分配[234]。

此外，第 102(12)條亦指出合夥協議(Partnership agreement)可以口頭或默示(implied)方式為之[235]。

區塊鏈之開發者對區塊鏈帳本進行初始的設計和建立；驗證者則是維持區塊鏈帳本正確性和完整性的要角，藉由提供自身運算資源幫助資料進行驗證，因此兩者皆為區塊鏈正常運作不可或缺之角色，又區塊鏈常伴有經濟獎勵的設計，如比特幣、代幣(token)，這也是驗證者願意參與區塊鏈帳本資料驗證的最大誘因；至於開發者雖秉持開源的精神(Opensource)，開放程式碼自由散佈，但以比特幣為例，其核心開發者受到 Blockstream 區塊鏈公司贊助，甚至有部分核心開發者就是此家公司之創辦人[236]，致力於比特幣維護、擴容和側鏈技術發展，因此帳本之維護對其所設立公司之利益息息相關。

開發者無中生有地創造區塊鏈、驗證者提供自身運算資源以實現區塊鏈分散式帳本核心功能-去中心化，兩者皆以經濟利益作為動機，符合合夥「兩人以上共同經營並以獲取利益為目的而實行相關活動」之定義，且區塊鏈去中心

Uniform Partnership Act (1997)(Last Amended 2013) §102(2) , ‘ Contribution, except in the phrase right of contribution, means property or a benefit described in Section 403 which is provided by a person to a partnership to become a partner or in the person’s capacity as a partner.’

[233] Uniform Partnership Act (1997)(Last Amended 2013) §101(11), ‘Property means all property, real, personal, or mixed, tangible or intangible, or any interest therein.’

[234] Uniform Partnership Act (1997)(Last Amended 2013) SECTION 102 comment, p62, available at：https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=d4bd53b5-0e2a-d71e-6d84-66a26e296324&forceDialog=0

[235] Uniform Partnership Act (1997)(Last Amended 2013) §102(12), ‘Partnership agreement means the agreement, whether or not referred to as a partnership agreement and whether oral, implied, in a record, or in any combination thereof, of all the partners of a partnership concerning the matters described in Section 105(a). The term includes the agreement as amended or restated.

[236] JP Buntinx, What is Blockstream, available at：https://themerkle.com/what-is-blockstream/ (Last visited on 2019/07/01)

DOI:10.6814/NCCU201901043

化、分權的特色，權力和利益非由中心機構所掌握，而是藉由程式碼決定記帳的權利和經濟獎勵分配的順序，開發者和驗證者的共同參與維持了整個區塊鏈之運作，並確保相關利害關係人之利益，縱無明示意思表示，基於美國法院承認事實上契約，亦成立合夥之契約關係，而對第三人負連帶責任[237]。當對外負清償責任時，應先以合夥財產清償之，不足部分始應由全體合夥人以個人財產負連帶清償責任[238]。在開放式區塊鏈中，由於驗證者多以運算資源此等無形財產做為出資方式，因此合夥財產就是由此些看不到、摸不著的無形財產組成，但運算資源此抽象的利益有賴於電腦此等硬體設備(有形財產)的運轉與提供，且這些設備為了進行複雜運算，通常具有極高的財產價值[239]，因此亦可拍賣或變賣之以清償金錢債權。

(B) 大陸法系

根據德國民法典第 145 條，契約成立係指當事人意思表示合致，而所謂意思表示係指為以特定之法律效果為目的，將其內心意思表現於外部之行為，因無特別要式之規定，亦可以默示為之[240]。縱當事人無成立契約之合意，僅依事實上提供給付之行為或事實上利用行為，亦可能成立事實上契約關係 。

事實上契約關係為德國聯邦最高法院援引 Haupt 教授的理論，認為現代社會因工業發達、生產進步、消費日增，產生了大量交易型態，傳統契約理論要

---

[237] Uniform Partnership Act (1997)(Last Amended 2013) §306(a), 'Except as otherwise provided in subsections (b) and (c), all partners are liable jointly and severally for all obligations of the partnership unless otherwise agreed by the claimant or provided by law.'

[238] Uniform Partnership Act (1997)(Last Amended 2013) §307(d), 'A judgment creditor of a partner may not levy execution against the assets of the partner to satisfy a judgment based on a claim against the partnership unless the partner is personally liable for the claim under Section 306.'

[239] 如比特幣挖礦機需要的運算資源相當龐大，硬體設備規格極高，非一般桌上型電腦所能企及。

[240] 國立臺灣大學法律學院，德國民法（上）—總則編、債編、物權編，2016 年 10 月，頁 110。

DOI:10.6814/NCCU201901043

求契約成立須達到意思表示合致過於僵化，不足以適應現代社會交易型態。此外，若無法主張契約關係責任，而僅能依據侵權行為主張損害賠償責任，被害者除須舉證有權利受到損害，主觀要件方面還須證明加害人確有故意或過失，對於被害人相當不利[241]。因此基於誠信和公平，而承認事實上契約關係。

開放式區塊鏈各個節點自願加入區塊鏈網絡，開發者創立區塊鏈初始環境，驗證節點則執行區塊鏈最重要的功能-資料驗證，兩者有著共同利益並實行相關活動，完整論述如同 A.契約關係(A)普通法系章節所述，又在德國實務承認事實上契約關係下，應可認成立合夥之契約關係，然 Haupt 教授當初提出事實上契約理論主要是基於社會給付義務，欲調整在無契約關係下所衍生的不平等情形，並擴張保護射程範圍，但此論述撼動傳統契約理論最主要的締約自由原則，契約因當事人意思表示合致而成立，背後所蘊含乃任何人皆能自由、自信選擇締約相對人以締結任何內容之契約，因此事實上契約理論仍充滿爭議。惟有學者指出縱不承認事實上契約關係，若能由事實推知有締約意思，亦可依默示而成立契約[242]。區塊鏈中自願下載程式而加入區塊鏈網絡成為節點之行為，可解釋為有可得推知成為區塊鏈網絡節點且共同維護帳本之意思表示，且以獲取利益為目的[243]，進而應認有成立商業上夥伴關係或合夥關係之意思表示，而合夥關係責任分配原則上係依照出資比例，若無法估計出資額，則平均分擔，有別於認許制區塊鏈每個節點互相認識且有事前的責任分配協議，開放式區塊鏈中節點分散於世界各地，並無事先約定出資比例，責任分配應以平均分擔為

241 王澤鑑，德國最高法院民事判利研究(二)，國立臺灣大學法學論叢，第 2 卷第 1 期，1972 年，頁 237。

242 王澤鑑，同註 96，頁 241。

243 開放式區塊鏈節點之加入通常是為獲益之目的，但認許制區塊鏈中節點加入的目的可能不一而足，多為希望能獲取某種好處，如 Ripple 聯盟鏈成員希望達到跨境交易的方便性和安全性，但亦有因監理之需求，而希望成為監理者，以管控市場秩序如各國監理主管機關等。

DOI:10.6814/NCCU201901043

適。

(C)我國法

依據我國民法第 153 條，當事人對於必要之點、非必要之點意思表示合致時，契約即為成立，且此意思表示可以明示或默示為之[244]。至於是否能僅因事實上之行為而成立契約行為，我國實務未如德國聯邦最高法院引用 Haupt 教授的事實上契約理論而加以承認，目前只見於學說上之討論，而學說上亦有兩種立場，肯定說認為事實上契約關係能解決契約法以外之規範如無因管理、不當得利或侵權行為所未能處理之問題，如停車不付費，難以主張當事人間有何契約關係，亦難以主張無因管理、不當得利或侵權行為[245]，故得以事實上契約關係理論主張契約成立而應負債務不履行責任[246]；否定說則認為，基於特定事實可推知雙方有締約之意思，則此特定事實可視為默示之意思表示而成立契約，無須另行創造事實上契約理論而破壞現行契約法理論意思表示合致而成立契約之架構[247]。

開放式區塊鏈中，自願下載程式而加入區塊鏈網絡成為節點之行為，在我國雖無如德國事實上契約理論得以援引，但我國民法契約之成立亦能以默示之意思表示為之，尤其上述我國學說有認為，若從特定之事實行為可推知有締結契約之意思，不妨可解釋為默示之意思表示而成立契約行為。

惟此應定性為何種契約，依據我國民法第 667 條，合夥係指二人以上互約出資以經營共同事業之契約。依此，只要當事人間就互約出資和經營共同事業

---

[244] 林誠二，契約之成立約推定成立，月旦法學教室，第 82 期，2009 年 8 月，頁 10。

[245] 在停車不付費之案例，係為非給付型不當得利中之權益侵害之不當得利，被告無法律上原因而受有利益，原告主請求被告返還無法律上原因而增加之利益，則此利益數額如何計算即有困難。

[246] 邱聰智，新訂民法債編通則(上)，新訂一版，2000 年，48 頁。

[247] 王澤鑑，同註 96，頁 246。

DOI:10.6814/NCCU201901043

達成意思表示合致合夥契約即成立，不以合夥人已實行出資為成立要件[248]，又出資得以金錢或其他財產權，或以勞務、信用或其他利益代之；另共同事業亦不以營利事業為必要[249]。

開放式區塊鏈中，用戶自願下載程式加入區塊鏈網絡成為節點並貢獻其CPU 運算能力之行為，應可認有以 CPU 運算能力作為利益出資並經營和維護區塊鏈分散式帳本此共同事業之默示意思表示，又共同事業不以營利事業為必要，故若有公益開放式區塊鏈未以經濟獎勵回饋給節點，仍可成立合夥契約。對外責任方面，當各節點因維護區塊鏈帳本此共同事業而造成他人損害，而對第三人負擔債務，若合夥財產不足清償合夥之債，則依據我國民法第 681 條，須由合夥人就其個人責任財產負連帶清償之。

B. 侵權責任

(A)普通法系

英美學者將侵權行為定義為：「除違約之外之民事不法行為，法院就此不法行為提供損害賠償之請求以作為救濟方式。」[250]並旨在保護人身或所有權不受侵害[251]，但侵權責任的保護範圍為何，是否僅及於權利受侵害而遭受之損害或侵權行為所致的純粹上經濟損失亦是保障範圍，尤其數位資料當事人是否擁有所有權，國際未有定論[252]，因此侵權行為保障範圍是否能擴及至純粹上經濟損失會是一討論重點，而美國就此發展出一系列的實務判決。

---

[248] 22 年台上字 2894 號判例

[249] 李淑明，債法各論，八版，元照出版社，2017 年 1 月，頁 492。

[250] 黃心怡，英美侵權行為概論，月旦法學雜誌，第 189 期，2011 年 2 月，頁 154。

[251] Seely v. White Motor Co. , 63 Cal.2d 9 (1965)

[252] 區塊鏈的去中心化特色有論者認為可以使當事人真正用有資訊自主權，由當事人決定資料如何使用和授權，而非由中心機構掌控。但中心化的網路時代，數位資料如使用者網路瀏覽紀錄、註冊資料等儲存在中心機構的資料，使用者能否依所有權進而對中心機構主張使用、收益、處分之權目前仍是莫衷一是。

DOI:10.6814/NCCU201901043

「純粹上經濟損失」係指非原告的人身或財產受到損害而引起之損失[253]，而在英美侵權法發展的過程中，對於純粹上經濟損失請求持保留的態度，原因在於擔憂課予被告過重之責任，例如電力公司進行管線維護工程，因過失導致線路短路，使得民生住戶停電，導致冰箱裡的食物腐壞，則各家住戶是否能本於受有經濟上損失而向電力公司請求損害賠償容有疑慮。目前實務純粹經濟上損失案例可分為三種類型[254]：1、故意引起的純粹經濟上損失；2、違反法定義務之純粹經濟上損失；3、過失侵權導致的純粹上經濟上損失。

故意侵權行為所引起的純粹上經濟損失，如詐欺、侵占、對於契約履行妨礙且當事人有預期之利益等[255]可請求損害賠償；違反法律上所設定之義務而造成的純粹上經濟損失亦可請求損害賠償[256]，惟較多爭論的是第三種類型因過失導致的純粹經濟上損失的情形。

1927 年美國聯邦最高法院於 Robins Dry Dock & Repair Co. v. Flint [257]一案中確立過失侵權責任以財產權受損害為賠償原則，案例事實如下：Flint 向船公司承租某船舶，並用以運送貨物。而該船舶每半年需進廠保養維修一次，並由 Flint 將船交付予負責保養維修之公司 Robins Dry Dock & Repair Co.，但保養公司在保養維修過程中因過失致船舶螺旋槳受損而延遲返還船舶的時程，Flint 因而無法如期使用船舶運送貨物而受有收入上之損失。法院認為 Flint 雖為船舶之租賃人，但非船舶所有權人，船舶所有權人仍為船公司，因此未有任何財產權受有損害；另 Flint 與船公司之間雖有船舶租賃契約之存在，但未課予第三人任

[253] Vincent R. Johnson,The boundary-line function of the economic loss rule, 66 Wash. & Lee L. Rev. 523, 524 (2009)

[254] 李昊，論英美侵權法中過失引起的純經濟上損失的賠償規則，比較法研究，第 5 期，2005 年 9 月，頁 64。

[255] Vincent R. Johnson, *supra* note 247, at 533.

[256] Vincent R. Johnson, *supra* note 247, at 532.

[257] Robins Dry Dock & Repair Co. v. Flint, 275 U.S. 303 (1927)

DOI:10.6814/NCCU201901043

何義務，船公司與保養公司之保養契約中 Flint 亦非第三方受益人。因此保養公司因過失致延遲返還船舶而導致 Flint 受有損失之行為，並未違反契約義務，亦未有任何財產權受有損害，僅有純粹上經濟損失，而法院尚未承認純粹上經濟損失得以請求損害賠償[258]，此一確立美國實務上對於過失侵權行為致純粹上經濟損失原則上不能請求損害賠償之態度。

而在後續 Seely v. White Motor Co.[259]和 East River S.S. Corp. v. Transamerica[260]亦重申侵權責任旨在保護人身或所有權不受侵害，買受人就商品不符其經濟上期待而受的不利益，不得依侵權行為規定向製造者請求損害賠償之立場。因此，英美法原則上以人身或所有權等權利受有侵害方能請求損害賠償為原則，至於「純粹上經濟損失」之案例類型是否即全然否定請求損害賠償之可能，於某些州法院開始出現雜音。

Kinsman transit company v. City of Buffalo 一案中，Kinsman 運輸公司因過失撞上紐約州的水牛河的一座活動橋[261]，因而封閉兩個月，致某一穀物出賣人無法通行水牛河，因此無法履行交付穀物予買受人之買賣契約義務，因而向 Kinsman 運輸公司請求損害賠償。聯邦第二巡迴上訴法院雖依循向來實務見解，認為運輸公司侵害的是民眾的債權，但未有絕對權受侵害的情形，進而駁回兩位受害人之損害賠償請求，但在判決理由中對美國聯邦最高法院於 1927 年 Robins Dry Dock & Repair Co. v. Flint 所樹立之過失侵權行為不能請求純粹經濟上損失之損害賠償提出質疑，認為此一原則未有一令人信服之理由[262]。

---

258 Victor P. Goldberg,Recovery for Pure Economic Loss in Tort: Another Look at "Robins Dry Dock V. Flint", 20(2) The Journal of Legal Studies 249,255-257(1991)

259 Seely v. White Motor Co. , 63 Cal.2d 9 (1965)

260 East River S.S. Corp. v. Transamerica, 476 U.S. 858 (1986)

261 又稱為 Moveable bridge，為通航需要，橋身能進行開合。

262 338 F.2d 708 (2d Cir. 1964) and 388 F.2d 821 (2d Cir. 1968).

DOI:10.6814/NCCU201901043

加州最高法院更於 Biakanja v. Irving[263]一案中打破長久以來由美國聯邦法院認為純粹上經濟損失不能請求損害賠償之原則。本案中公證人因過失而未將遺囑人作成之遺囑交由兩位證人見證，使得繼承人最後僅能繼承部分遺產，法官認為此行為人因過失致無契約關係之第三人(繼承人)受有純粹上經濟上損失，而第三人得否據以請求損害賠償是一法律政策問題，應考量該契約影響被害人(第三人)之程度、行為人對被害人(第三人)遭受之損害是否有可預見性、行為人之行為對於損害之因果關聯性、行為人之行為於道德上之可非難性及行為人對於此純粹上經濟損失負擔損害賠償責任是否有助於預防未來再生同類損害等因素，本案件法官認為公證人與遺囑人契約關係之最終契約目的是為了讓遺囑人死後之遺產得依照其所作之遺囑上的分配適切地移轉予繼承人，因此認定本案之繼承人(第三人)得向有過失之公證人請求因其過失行為而造成繼承人未能獲得應得遺產之純粹上經濟損失。

因此，以往一概否定純粹上經濟損失得以請求損害賠償的原則已有例外情形，加入不同之考量因素進行權衡已漸為其他各級法院
所接受，紐澤西州最高法院在 People Express Airlines, Inc. v. Consolidated Rail Corp.[264]一案中亦表示過失侵權行為所致之純粹
經濟損失不予賠償的原則在實務上已有許多例外情形發生，因此無須墨守成規，重點在於被告之行為對於原告造成損害的事實是否得以預見和行為人之行為與結果之發生之因果關聯性，據此即能避免被害人承擔過多不合理之損害賠償責任。

開放式區塊鏈分散式帳本中記載著交易資料，若出現運行或驗證上的錯誤，導致資料交換發生遺漏、外洩等情形，此時可能構成隱私權侵害、數位資

[263] Biakanja v. Irving , 49 Cal.2d 647(1958).

[264] People Express Airlines, Inc. v. Consolidated Rail Corp., 495 A.2d 107 (N.J. 1985)

DOI:10.6814/NCCU201901043

料所有權的侵害或純粹經濟上損失。

區塊鏈帳本所公開之交易資料如比特幣地址，其實是經過雜湊函數運算所得的寄件者或收件者之公鑰，作用就如同電子郵件地址一般，因此在開放式區塊鏈中的交易被認為具有匿名特性，即使交易資料外洩但在難以藉由這些雜湊函數資料拼湊交易雙方當事人身分並進而推敲其行為模式，難謂有造成當事人之損害而構成隱私權侵害；而對於數位資料，當事人是否擁有所有權或控制權(ownership)國際未有定論[265]，因此討論仍會聚焦在違反注意行為構成純粹經濟上損失時是否得以請求損害賠償，區塊鏈由開發者創造初始環境，並由每個節點共同維護帳本，若無盡一個理性之開發者或節點之注意義務[266]，而對第三人造成經濟上損失，且開發者和節點對於其過失的行為所可能侵害之主體、損害是可得確認和預見的，在未對商業自由有過多限制下，法院應課予損害賠償責任。而理性之開發者或節點應盡之注意義務可能包含，如程式碼維護、安全性漏洞修補與更新、組織資安教育訓練、風險管理等，或以是否達到國際上資訊安全管理標準 ISO/IEC 27000、ISO/IEC 27001 所列舉的相關指標作為法院進行審理之注意義務之標準，皆是實務可進行參酌的方向。

(B) 大陸法系

德國侵權行為架構係由德國民法第 823 條和 826 條所構築，德國民法第 823 條第 1 項規定，因故意或過失不法侵害他人生命、身體、健康、自由、所有權或其他權利者，負損害賠償責任；第 2 項，違反以保護他人為目的之法律者負擔損害賠償責任[267]。同法第 826 規定，因故意違反善良風俗之方式加損害

[265] 區塊鏈的去中心化特色有論者認為可以使當事人真正擁有資訊自主權，由當事人決定其資料如何使用和授權，而非由中心機構掌控。

[266] 英美法係以合理謹慎之人作為是否違反注意義務之標準。

[267] BGB§823, ‘

(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des

DOI:10.6814/NCCU201901043

於他人者，對該他人負損害賠償責任。[268]

第 1 項係屬權利侵害類型，保護客體限於絕對權；第 2 項則將保護客體擴大至利益，亦包含純粹經濟上損失。第 826 條則屬利益侵害類型，亦包含純粹經濟上損失，但主觀要件限縮於故意且違背善良風俗才能請求[269]。德國聯邦法院發現侵權行為之主張若只限於因故意或違反保護他人之法律所造成之純粹經濟上損失有害於當事人正義和經濟發展，遂以實務判決逐漸擴張解釋第 823 條保護客體及於營業權，第 826 條之「故意」包含未必故意[270]及重大過失[271]。

區塊鏈由每個節點共同維護帳本，當帳本上的資料因節點故意或過失遺漏、外洩，能否依照侵權行為主張即面臨與英美法系相同之討論，即此侵害行為究屬隱私權侵害、數位資料所有權的侵害或是純粹經濟上損失，現行德國實務雖擴張侵權行為之保護範圍，但對於「權利」之解釋多年來處於保守態度，目前僅擴及至營業權，此外是否承認個人對其數位個人資料有所有權仍晦暗不明，因此寄望以德國民法架構下之侵權行為作為請求損害賠償責任之基礎較有難度。

另一個較為可行之侵權行為請求權基礎係為甫於 2018 年生效之歐盟隱私權法律-一般資料保護規定(General Data Protection Regulation，簡稱 GDPR)，取代

---

daraus entstehenden Schadens verpflichtet.

(2) Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.'

[268] BGB§826,'Wer in einer gegen die guten Sitten verstoßenden Weise einem anderen vorsätzlich Schaden zufügt, ist dem anderen zum Ersatz des Schadens verpflichtet.'

[269] 葉啟洲，純粹經濟上損失在台灣侵權行為法上的保護-以最高法院相關裁判為中心，月旦法學雜誌，第 241 期，2015 年 6 月，頁 49。

[270] 未必故意係指加害人對於其行為可能造成損害之事實有所預見，而該結果之發生亦不違背其本意。

[271] 邱琦，純粹經濟上損失之研究，台灣大學法律研究所碩士班論文，2002 年，頁 108。

DOI:10.6814/NCCU201901043

數據保護指令 95/46/EC(Data Protection Directive 95/46/EC)，旨在保護所有歐盟公民之個人資料隱私，因此任何政府機構、企業或非營利組織只要有經手處理歐盟公民之個人資料，皆會受 GDPR 之規範[272]。而「個人資料」之定義係指任何能識別或可識別的自然人資訊，而所謂可識別是指能直接或間接透過如姓名、號碼、地理位置資料或網路上識別符號(online identifier)[273]，並使用這些識別符號(identifier)進行個人身分、心理、精神、文化、經濟、社會認同的剖析，以建構個人的身分。

區塊鏈運行中所產生的公開資料如比特幣交易當事人之地址，係經過雜湊函數運算所得的哈希值，本身屬中性的資料，不具有識別一個人身分之真實性證明功能，因此能否符合 GDPR 的個人資料定義而納入其保護範圍亦有疑義。

(C)我國法

依據我國民法第 184 條第 1 項前段，因故意或過失不法侵害他人之權利者，負損害賠償責任。保護客體限於權利，而不及其他法律上之利益；第 184 條第 1 項後段保護客體則包含權利、利益但主觀要件上限於故意且背於善良風俗；第 184 第 2 項保護客體亦包含權利、利益，違反保護他人之法律即推定有過失，惟能證明無過失時始可免責。

如同上述英美法系和大陸法系之討論，若區塊鏈帳本上的資料因節點故意或過失遺漏、外洩，此行為究屬隱私權侵害、數位資料所有權的侵害或是純粹經濟上損失則有疑義，由於區塊鏈上的交易資料或交易地址僅為一經過加密運算之符號，即使外洩亦難以拼湊交易雙方之身分，因此難以主張個人資料之隱私權侵害，另我國亦尚未承認數位資料之所有權，因此，僅可能透過第 184 條

[272] 參照 GDPR §4(7)(8)。

[273] 根據 GDPR recital(30) Online identifier 係指任何透過設備、工具或協議(protocols)所提供的網物上識別符號，例如 cookie、IP 位置、無線電頻率等。

DOI:10.6814/NCCU201901043

第 1 項後段主張加害者有故意背於善良風俗之情事而主張侵權行為損害賠償責任，惟舉證責任由被害人負擔，且限於「故意」以背於善良風俗之方法，過失背於善良風俗而生之侵權行為則無所從主張；另一可能是以第 184 條第 2 項主張違反保護他人之法律而該當侵權責任，此處之「法律」應係個人資料保護法，個人資料保護法所稱「個人資料」係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料，個人資料保護法第 2 條定有明文，因此若能證明此外洩之資料能直接或間接識別個人，則可能違反個人資料保護法而該當個人資料保護法之侵權責任[274]和民法之一般侵權責任。

此外，若能證明多數節點有違反善良管理人之注意義務而構成侵權行為，依據民法第 185 條共同侵權行為，則構成侵權行為之多數節點間需負連帶責任，被害人得以向任一節點請求侵權行為之損害賠償，有利被害人求償。

二、認許制區塊鏈

(一)簡介

又稱為私有鏈。僅對特定團體成員開放，因此須通過審核並獲得授權才能加入成為節點，並分工合作賦予不同角色和權限，因此並非每個節點都有查閱帳本、發起交易、驗證等權限，且為了商業上之身分勾稽需求和區塊鏈運作效率，多採實名制。

(二)責任主體

由於認許制區塊鏈成員的加入須經過審核與授權，其責任主體與開放式區

[274] 個人資料保護法第 29 條第 1 項「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」

DOI:10.6814/NCCU201901043

塊鏈相較起來較為單純和容易識別，責任主體可分為以下三種：

1、核心開發者：建立區塊鏈之程式設計者，具有資訊技術能力和話語權之核心開發者。

2、驗證者：運行於區塊鏈之節點，並利用本身運算資源對交易進行驗證。在認許制區塊鏈中，驗證者是事先被指定。

(三)責任內容

A. 契約關係

認許制區塊鏈中的節點通常是商業關係中的夥伴或策略聯盟的盟友，為了處理鏈下(off-chain)的資產交易例如證券、貨幣、所有權等商業交易紀錄，而以實名制方式構建區塊鏈網絡，與開放式區塊鏈處理鏈上(on-chain)資產例如：比特幣、代幣(tokens)有別[275]。

因此認許制區塊鏈中，節點間派出代表彼此經過面對面磋商、談判，最後訂立契約以釐清區塊鏈網絡上的權利義務關係，例如是否有訪問資料權限、是否為驗證節點等，並依照契約中的責任條款負擔債務不履行之責任。

此外，2000 年美國法院因應電子商務興起而發展出的線上電腦軟體按鍵契約(Clickwrap agreement)之概念，雖然無法適用於各個節點得以自由加入的開放式區塊鏈情境，但在認許制區塊鏈的應用中如智能合約應得以援引此概念處理相關法律紛爭。

線上電腦軟體按鍵契約(Clickwrap agreement)係指電子商務網站會預先擬定定型化契約條款，並於會員註冊或使用網站服務前，將彈出視窗(Pop-up window)呈現於會員的螢幕前，當會員閱讀後並按下「我已閱讀並同意會員約定條款說明」的同意鍵後，即代表雙方協議成立並願意受契約條款之拘束。

---

[275] Gareth W. Peters, Efstathios Panayi.(2015),Understanding Modern Banking Ledgers through BlockchainTechnologies: Future of Transaction Processing and SmartContracts on the Internet of Money (2015), p6, available at：https://arxiv.org/pdf/1511.05740.pdf

DOI:10.6814/NCCU201901043

智能合約中的條款係以程式碼代替原本雙方合意協商的法律文字將交由電腦自動執行，但雙方合意內容仍是先以白紙黑字，經由協商、談判而修訂而成，最終再轉換成程式碼訂入智能合約中，縱使雙方未能會面討論契約內容，而是透過網路進行通訊交流，一方預擬的契約條款仍可透過一個彈出屏幕詢問締約者是否同意智能合約條款並受其拘束，如此應能合理解釋雙方皆有受條款拘束之意思表示，並賦予智能合約於法律上之效力。

B. 侵權責任

如同開放式區塊鏈侵權責任之探討，雖然成員間有契約關係而對彼此負擔契約上責任，但如果區塊鏈網絡發生駭客攻擊致客戶資料外洩，例如銀行共組區塊鏈聯盟以達到客戶徵信資料共享，若區塊鏈網絡遭到攻擊導致銀行的客戶資料外洩，客戶與申辦銀行有契約關係，但與銀行區塊鏈聯盟並無契約關係，僅是契約關係外之第三人，則能否向區塊鏈聯盟負責驗證之節點主張侵權責任，則要檢視不同法系對於經濟上損失能否請求損害賠償的態度，此於一、開放式區塊鏈部分已有探討，於此不再贅述。

第三款 區塊鏈分散式主體責任與現行法之相容性

區塊鏈的共識機制取代了數位簽章中憑證機構的角色，公鑰的驗證無須經由中心憑證機構檢驗或核實公鑰是否為簽署者所有，區塊鏈共識機制讓網絡中所有節點分享其運算資源，共同進行驗證工作。

但當驗證工作有所錯誤而導致加密資料外洩或遭人不法使用，在數位簽章中，核發公鑰之中心化憑證機構是唯一的責任主體；但於區塊鏈中，驗證是由驗證節點共同為之，共同維護一本帳本，此外區塊鏈的初始環境是由開發者所設計，驗證節點和開發者可視為兩人以上有共同經營並以獲取利益為目的而實行相關活動，應認成立合夥關係，因此當有資料外洩之情事導致第三人損失，應由開發者和驗證節點依照合夥之契約關係共同擔負責任，並對外負連帶之

DOI:10.6814/NCCU201901043

責。

對照中心化憑證機構責任與區塊鏈分散式節點責任，責任主體由單一變為多個，責任承擔由單一承受變為共同承擔，責任內容對外皆可能成立契約責任和侵權責任，但由於區塊鏈節點可能數以萬計，法律關係比起中心化憑證機構只有單一責任主體複雜許多，尤其節點彼此之間並無亦意思表示，是否能依照傳統契約法成立契約關係如合夥容有疑慮，但若依照現行國際實務判例，承認所謂事實上契約關係，某種程度上擴充了傳統契約關係成立需要意思合致之限制，因此仍可依照傳統契約法課予契約責任；而侵權責任方面，若因節點未盡善良管理人注意義務，包含未對自我電腦系統安裝防毒軟體或未對系統防護更新導致他人偽裝本人登入區塊鏈網絡進行訪問或下載資訊，導致他人財產權損害，則應負損害賠償責任。

區塊鏈網絡雖無中心憑證機構作為責任主體，但區塊鏈的建置和運行皆仰賴開發者和驗證節點，尤其驗證節點取代傳統由中心憑證機構單獨負責身分來源的驗證工作，因此區塊鏈並不會因為去中心化而找不到責任主體，而是探查網絡中的節點是否有盡善良管理人之注意義務以維護本身設備，若違反注意義務，自應由單一節點負擔侵權責任或由多數節點成立共同侵權行責任[276]，現行國際立法例課予憑證機構責任雖與區塊鏈運行機制相左，但差別只在於責任主體的不同，由中心憑證機構轉變由節點負責，注意義務和責任內容則無太大差異，惟須注意的是，若開發者與各節點成立的是合夥關係，單一節點對外之侵權責任，開發者和其他節點亦可能須連帶負責。

[276] 區塊鏈資訊安全可分為區塊鏈系統本身的安全防護機制和區塊鏈系統上之應用服務安全防護機制，尤其以區塊鏈系統上所架設之應用服務裝置最易被駭客入侵突破，透過節點如伺服器、電腦等裝置查看節點日誌檔(Log)而找出駭客登入資訊、IP 位置、網路卡號碼 MAC address 以釐清各節點之責任歸屬，並探求節點之資訊安全防護是否盡到應有之注意義務。

DOI:10.6814/NCCU201901043

第三項 數位簽章時間戳與區塊鏈時間戳之法律效力

第一款 數位簽章時間戳

一、意義

現實社會中，為避免寄件人和收件人對於資料寄送的時間人各執一詞，因此以公正的第三方-郵局的郵戳作為實體世界的時間證明；電子社會中，電子交易和電子文件的交換不再以傳統書面契約簽名並押上日期作為契約成立生效的時間點或以郵局的郵戳證明寄送時間的方式為之，而改以數位簽章技術將電子文件與當事人連結，並設計時間戳以確保雙方對於文件存在、交換和契約成立生效的時點有一可信賴的證明，對於維持法律關係的穩定和促進電子交易之信賴有相當大的幫助。

二、運行方式

數位簽章技術係以非對稱加密方式，產生公鑰和私鑰，簽章人(寄件人)以私鑰加密自己的文件，收件人則由簽章人發布之公鑰對文件解密以取得文件內容。私鑰由簽章人自己保存，公鑰則發布於網路上，但收件人無從得知公鑰是否確實由簽章人(寄件人)所發布，故設計第三方憑證機構(Certificate Authority)以簽發憑證的方式，認證此公鑰確實屬於簽章人(寄件人)所有，但當憑證因過期而失效或撤銷，時間戳能作為簽章在某一特定時間前即已存在的證據，證明文件的數位簽章確實是在憑證有效期間內所簽署的。

時間戳係由第三方時間戳機構(Time Stamp Authority，TSA)根據國際電子時戳標準規範 RFC 3161[277]所提供，先由簽章人將已由私鑰加密過的文件利用單向雜湊函數(One-Way Hash Function)產生文件的訊息摘要 (Message Digest,，

[277] RFC 3161 的標準中規定了時間戳的請求和回應的格式，並建立時間戳機構操作的相關安全需求，及關於處理請求和產生回應的過程。

DOI:10.6814/NCCU201901043

MD)，再將訊息摘要送往時間戳機構，時間戳機構會在訊息摘要附加時間資訊後再做一次數位簽章得到時間戳，再將時間戳傳送給使用者，如此一來簽章人即可得到擁有時間證明的時間戳，來做為不可否認的時間存在證明[278]。

三、法律上證據能力

(一)美國

1. 時間戳-電子紀錄

依據 UETA 第 2 條第 5 項「電子」係指電氣、數位、磁性、無線、光學、電磁或類似的技術而言，因此「電子紀錄」[279]係指透過上述方式或類似技術創造、產生、傳送、傳播或儲存的紀錄，例如資訊處理系統、電腦設備和程式、電子資料交換、電子郵件、語音郵件、傳真、掃描或其他相似之技術所產生或儲存的資料皆屬之[280]。惟「電子」一詞應作廣義解釋，並不侷限於現有技術，而應隨著新技術的發展而賦予不同內涵，只要此技術所產生的資料能以可感知、可察覺的方式取得，即是 UETA 所指稱的電子紀錄[281]，以達到 UETA 期望使任何非以傳統書面或口頭方式成立之電子商業交易不會僅因使用之媒介(medium)的不同而否認其法律上效力之立法目的。

時間戳係由公正第三方時間戳機構將經過數位簽章技術加密之文件，附加

---

[278] 楊中皇、葉志青、蘇聖雄、張家瀚，時戳服務，資通安全政策分析專論，財團法人國家實驗研究院科技政策研究與資訊中心，2006 年，參考網址：http://security.nknu.edu.tw/psnl/publications/2007/10_CHANG,KU-HAN/%AC%E3%A8s%A5%CD%A4w%B5o%AA%ED%A4%CE%A4w%B1%B5%A8%FC%A4%A7%A4%E5%B3%B9.pdf

[279] UETA §2(7), 'Electronic record means a record created, generated, sent,communicated, received, or stored by electronic means.'。

[280] UETA §2(5), comment 6, p9, avaialb at ：http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf

[281] UETA §2(5)comment 4, p8, avaialb at ：http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf

DOI:10.6814/NCCU201901043

時間資訊後再做一次數位簽章之加密而得到的電子標記，因此亦符合 UETA 電子紀錄之定義，且不能因其電子之形式而否認其法律上效力。

UETA 僅模糊規定電子紀錄不能因其電子之形式而否認其法律上效力，但未指明電子紀錄於證據法上之意義。參照明尼蘇達州電子認證法關於時間戳之規定，時間戳若是由無利害關係之第三方機構利用可值得信賴之系統所加註且當事人無法舉反證推翻，則可推定簽署數位簽章之時間點確實在時間戳所指名的時間之後，法院應以此事實作為責任分配判決的衡量依據[282]，既然能作為責任分配之依據，應以肯認其證據能力作為前提。

2. 證據能力

傳統上證據是否具有可採性，亦即是否具有證據能力，須通過四大證據排除法則之檢驗：違法證據排除法則、驗真法則[283]、傳聞法則、最佳證據法則。前兩項法則對於電子證據之適用較無問題，但傳聞法則、最佳證據法對於電子證據之適用則有爭議。

依照傳聞法則，傳聞證據不具證據能力。而傳聞係指證人於審判(Trial)外或聽證會(Hearing)外所為之陳述，而以該陳述證明待證事實為真實[284]。又所謂陳述(Statement)，依聯邦證據法第 801 條(a)規定，係指言詞或書面之主張或行為人非言語之動作，而有意以之作為其主張之表示。因此，傳統上信用卡刷卡紀錄、銀行存款或帳目明細或 ATM 提款紀錄亦被認為是行為人有意作為的一種主張表示，只是透過電子化或數位化的方式記錄和表現，因此屬於傳聞證據[285]。

---

[282] Minnesota electronic authentication law §325K.01(37) , avilable at ：https://www.revisor.mn.gov/statutes/cite/325K.01

[283] 亦有學者譯為「真實性之證明」、「真正證明」，段重民、崔汴生譯，司法院司法行政廳編，美國聯邦證據法，2003 年 1 月，頁 121；亦有學者將之譯為「驗真」，Arthur Best 著，蔡秩明、蔡兆誠、郭乃嘉譯，證據法入門：美國證據法評釋及實例解說，2002 年 12 月，頁 278。

[284] Federal Rules of Evidence §801(c)。

[285] 朱帥俊，刑事證據法則對於電子證據適用之研究，交通大學管理學院碩士在職專班科技法律

DOI:10.6814/NCCU201901043

但是否所有電子證據皆有傳聞法則之適用，美國司法實務上將其分為三種類型討論：電腦生成紀錄(Computer-generated Records)、電腦存儲紀錄(Computer-stored Records)以及兼具上述兩種之混和形式(both Computer-generated and Computer-stored Records)。「電腦生成紀錄」係指非經人為而全由電腦自動生成之紀錄，不包含人類之主張(Assertion)或陳述，例如：電話繳費紀錄、行動電話通聯紀錄、電子郵件標頭資料、全球定位系統資料、網路服務提供者(ISP)的登入資料等[286]，儘管上述記錄有些是經由人為輸入資料進行觸發而取得，但此為對電腦系統所發出的指令，非人類之主張或陳述，因此無傳聞法則之適用，但是否具有證據能力仍須進一步視舉證者能否證明電腦系統處於正常運作狀態並確保其產生正確之結果[287]，以作為是否排除其作為證據資格的標準；「電腦儲存紀錄」則是以數位方式記錄並儲存人為的陳述於電腦或類似之儲存設備，例如：個人信件、便條紙、日記或商業交易紀錄藉由人輸入並儲存於電腦設備等[288]，與人為的陳述並無二異，因此有傳聞法則之適用；「兼具電腦生成記錄與儲存記錄」除了有傳聞法則適用，亦需檢驗電腦系統及程式是否正常運作。

時間戳是第三方時間戳機構經由數位簽章加密技術所產生，經由人輸入指令而啟動程序，後續則依靠加密演算法運行而得出時間戳，並無表彰人的想法，因此並非屬於以數位方式紀錄人類之陳述或主張的電腦儲存紀錄，而較接近於實務上所稱的電腦生成紀錄[289]，故應以第三方時間戳機構產生時間戳的系

組，2007 年，頁 162。

[286] United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, p192, available at：https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

[287] *Id.*at 200。

[288] *Id.*at 192。

[289] George Cornell ,The evidentiary value of automatically transcribed voicemail messages, 17 Journal

DOI:10.6814/NCCU201901043

統和程式的運行是否正常運作或演算法有無明顯錯誤來判斷時間戳有無作為證據上的能力，而非僅以電子形式的紀錄即認具有傳聞法則的適用而否定其證據能力。

最佳證據法則係指除非原始證據因不可抗力之理由而無法取得，否則所有在法庭提出的證據必須是原始證據。此法則源自於英國司法程序文書審制度，要求起訴之原告必須提供原始文書予法院，以防詐欺或錯誤，並讓法院有足夠之依據進行公平判決。

傳統上此法則僅適用於文書證據，且必須提供原始文書，而不能提供複本，但現今亦適用於錄音、照片和以電腦輸出列印之紙本文件[290]。時間戳此等電子紀錄、電子證據是否符合最佳證據法則之「原本」容有疑慮，美國司法實務上有認為電磁紀錄是透過電腦顯示且視覺可讀，亦是數據的準確反映，因此亦屬於最佳證據法則所指稱的原始文書[291]。

電子證據於傳聞法則和最佳證據法則的適用上雖有隔閡，但隨著實務上判決解釋的調整，亦建立電子證據是否具證據能力之判斷標準。

時間戳係為一經過數位簽章嚴謹的加密技術所得之電子紀錄，其透過參數設定和演算法設計自動運行，並經由嚴謹加密技術進行資料完整性和真實性之保全，不包含人類之陳述，故無傳聞法則適用；時間戳能透過視覺上於電子設備顯示而辨其意義，且加密技術讓時間戳難以偽造，符合最佳證據原則要求當事人提出原始證據以防止詐欺和錯誤的精神，因此時間戳若由第三方時間戳機構以正常安全之設備運行且根據國際電子時戳標準規範 RFC 3161 所產生，則應肯認其具有法律上之證據的能力。

---

of Science & Technology Law 259,276-278(2011)

[290] Federal Rules of Evidence §1001(a)(b)(c)(d)。

[291] 朱帥俊，同註 273，頁 186。

DOI:10.6814/NCCU201901043

(二)歐盟

1. 時間戳-電子形式數據

依據 eIDAS 第 3.33 條，「電子時間戳」係指將電子數據綁定至特定時間的電子形式(Electronic form)數據。雖無對「電子」一詞作定義，但依循技術中立之原則，不應對於不同技術予以差別待遇，因此對「電子」一詞應作廣義解釋，而泛指一切關於電子控制之相關技術[292]。

2.證據能力

eIDAS 第 41.1 條規範「合格電子時間戳」之要件，但電子時間戳之證據能力(admissibility)並不會因其電子的形式或不符合「合格電子時間戳」之要件而否定其法律上之效力與作為法律上證據之能力(admissibility)。惟合格電子時間戳享有日期、時間為正確之推定且其所綁定的資料亦推定具有完整性，因此生舉證責任倒置情形，提出合格時間戳之當事人不負舉證責任，改由他方承擔時間戳上時間準確性和資料完整性之事實不存在的舉證責任。

第二款 區塊鏈時間戳

一、意義

區塊鏈時間戳亦為一種時間證明，使每一筆數據資料上都有時間標記，以確保每個區塊依序相連且無法竄改，有如現實中的公證人角色，確保交易資料的安全性、真實性和時間序列，以作為未來爭執時不可否認之證據。

二、運行方式

區塊鏈時間戳係由每個區塊抓取系統時間後取得，時間戳會與區塊頭(Block Header)的資料一同經過雜湊函數 Hash 運算後，成為下一區塊的 Hash

[292] Cambriage English 對於電子一詞的解釋：using, based on, or used in a system of operation that involves the control of electric current by various devices.

DOI:10.6814/NCCU201901043

值，因此每個區塊互相鏈結和牽動，任一區塊的資料遭到竄改，Hash 值即會改變，亦連動影響他區塊的 Hash 值，因此雜湊函數保障了資料的完整性、不可否認性、不可竄改性，亦讓時間戳上的日期時間成為可信賴之證明。

三、法律上效力

區塊鏈時間戳係由雜湊函數確保時間戳無法被竄改，數位簽章之時間戳則由公正第三方時間戳機構產生且透過數位簽章方式確保時間戳的安全和信賴。

國際尚無明文規範區塊鏈時間戳之法律效力，然從數位簽章之時間戳的相關立法規範和實務案例觀之，法院就電子時間戳效力所關注的重點在於產生電子時間戳的系統設備和程式運行是否具有可靠性和安全性，例如美國實務區分電腦生成紀錄和電腦儲存紀錄，其中不包含人類陳述之電腦自動生成之紀錄，舉證者應證明電腦系統處於正常運作狀態並確保其產生正確之結果，以此做為是否具有證據能力之判斷；歐盟亦在 eIDAS 規範合格時間戳才享有日期、時間為正確之推定，而合格時間戳須由合格信任服務提供者所提供，合格信任服務提供者須符合僱用專業人員、系統技術安全性和可靠性、承擔風險能力等多項指標。

區塊鏈時間戳利用雜湊函數保證其安全性，而數位簽章時間戳將時間資訊附加在已經過數位簽章技術加密過的文件後再次透過數位簽章加密而取得的方式，等於是雙重數位簽章的方式來確保時間戳之安全和唯一性。兩者的加密方式雖有所不同，但目的皆為讓時間戳成為不可否認之證明，且就區塊鏈時間戳使用之雜湊函數，例如比特幣使用的 SHA-256 雜湊函數，有 2 的 256 次方的組合約等於 10 的 77 次方，比全世界原子數量總和 10 的 49 次方還多，安全性高，且經過全體節點驗證，因此於法律上之效力或證據能力至少應比照數位簽章時間戳之規定予以肯認。

DOI:10.6814/NCCU201901043

第三款 區塊鏈時間戳與國際現行法之相容性

區塊鏈時間戳係由雜湊函數和鏈狀的資料結構(每個區塊之哈希值皆是以前一個區塊資料和時間戳經雜湊函數運算後所得)，且透過網絡中每個節點之共同驗證，安全性比數位簽章時間戳更值得信賴，只是產生方式略有不同；此外，亦符合美國或歐盟關於電子時間戳之定義，係為一種帶有時間資訊之電子數據用以證明所欲綁定的特定資料於特定時間存在的證據，因此以國際現行法賦予區塊鏈時間戳法律上效力和證據能力應無疑義。

DOI:10.6814/NCCU201901043

茲以下表列出區塊鏈與電子簽章之異同：

<table>
<tr><th></th><th colspan="3">電子簽章</th><th>區塊鏈</th></tr>
<tr><td rowspan="4">定義</td><td>美國 UETA</td><td colspan="2">以電子的聲音、標記(symbol)或過程(process)附加於或邏輯上關聯於一份記錄，且由具有簽章意圖之某人執行或接受。</td><td rowspan="4">寄件者先以 SHA-256 雜湊函數產生私鑰，並進行橢圓曲線加密運算產生對應之公鑰。收到收件者之位址後，以私鑰對收件者的位址、交易資料的哈希值進行加密，形成一個數位簽章，並將交易資料、數位簽章和寄件者之公開金鑰一同打包廣播給區塊鏈網絡進行後續驗證。</td></tr>
<tr><td rowspan="3">歐盟 eIDAS</td><td>基本型</td><td>一電子形式的數據，邏輯地附加於其他電子形式數據相關聯，並提供簽名人用於簽署之目的。</td></tr>
<tr><td>進階型</td><td>符合基本電子簽章要件之外另符合以下四點：
1. 與簽署人有唯一之聯繫。
2. 能識別簽署人身分。
3. 簽署人可高度信賴並單獨控制。
4. 與簽署之數據相關聯，故能偵測到數據之任何更改。</td></tr>
<tr><td>合格型</td><td>符合進階電子簽章要件之外，另符合以下兩點：
1. 依據一份有效的合格憑證所簽署之電子簽章。</td></tr>
</table>

DOI:10.6814/NCCU201901043

			2.由合格的電子簽名產製設備所製作。	
節點責任	美國 UETA	大部分州並無規定，僅明尼蘇達州訂有下列規定： 三種類型之擔保責任： 1.絕對之擔保責任 2.相對之擔保責任 3.信賴擔保責任 責任內容： 1.接受調查 2.暫停或撤銷憑證機構之許可證 3.民事懲罰 4.支付裁罰程序之費用		開放式區塊鏈 平均分權(Shared control)的模式，權力下放至各個節點，由每個節點共同進行資料的存取、處理和管理。 形成的法律關係可能為： 1.多邊契約(Multi-party contract) 2.合資(joint venture) 3.合夥(partnership) 認許制區塊鏈 非完全平均分權，會因其所組成的區塊鏈網絡之需求和目的，而賦予每個節點不同之權限。此外由於事先成員皆須經審核，法律關係會依照其所簽訂之契約而定。
	歐盟 eIDAS	損害賠償責任	故意、過失而違反義務並造成他人損害者，負擔損害賠償責任。	
		舉證責任	**非合格信任服務提供者：** 由客戶負擔「損害」和「因果關係」之舉證責任。 **合格信任服務提供者：** 推定過失責任，由	

DOI:10.6814/NCCU201901043

			和格信任服務提供者舉證非故意或過失。	
時間戳	美國 UETA	大部分州並無規定，僅明尼蘇達州有明文之定義： 時間戳係指附加於訊息、數位簽章以確認數位簽署之標記，並至少指名日期、時間和註記時間戳之人的身分。		由每個區塊抓取系統時間後取得，並與區塊頭(Block Header)的資料一同經過雜湊函數 Hash 運算後，成為下一區塊的 Hash 值，因此每個區塊呈現連動狀態，任一區塊鏈資料有所變動皆會被發現，保障了資料的完整性、不可否認性、不可竄改性，亦讓時間戳上的日期時間成為可信賴之證明。
	歐盟 eIDAS	係指以電子形式將其他電子形式數據綁定至特定時間。		

表格 2：電子簽章和區塊鏈比較 (作者自製)

DOI:10.6814/NCCU201901043

第五章 區塊鏈與台灣電子簽章法之相容性

承接上一章解析區塊鏈於美國、歐盟電子簽章法之相容性，本章則探討我國電子簽章法作為區塊鏈基礎規範的可能性，並以美國 UETA、歐盟 eIDAS 作為比較對象，以檢討我國現行法與區塊鏈之相容性和相關立法漏洞。

第一節 台灣電子簽章法立法背景

鑑於電子商務之蓬勃發展，世界各國從 1996 年起開始即陸續推動電子簽章之立法工作，聯合國國際貿易委員會(UCITRAL)首開先河於 1996 年 3 月通過電子交易模範法，後續更有如德國（1997 年）馬來西亞（1997 年）、義大利（1997 年）、新加坡（1998 年）、韓國（1998 年）、香港（2000 年）、日本（2000 年）、美國聯邦（2000 年）先後完成立法。

台灣為推動電子政府和電子商務的普及化，並建立安全及可信賴之網路交易環境，由經濟部委託資策會科技法律中心進行數位簽章之研究，並參酌聯合國及歐盟等國際組織訂定電子簽章法之相關立法原則，於 2001 年 10 月 31 日三讀通過電子簽章法，2002 年 4 月 1 日正式施行。

第二節 台灣電子簽章法立法原則

台灣電子簽章法(下稱本法)係參照外國立法例，訂立以下三項立法原則[293]：

(一) 技術中立原則：係參照聯合國及歐盟等國際組織倡議的「電子簽章」（electronic signature）為立法基礎，不以「數位簽章」(digital signature)

[293] 行政院函請審議「電子簽章法」草案文書，參考網址：https://lis.ly.gov.tw/lgcgi/lgmeetimage?cfcbcfcdcecbcfcfc5cac8c8d2cac7c7

DOI:10.6814/NCCU201901043

之技術為限，以因應未來生物科技等電子鑑別技術之創新發展。因此，利用任何電子技術製作之電子簽章及電子文件，只要功能與書面文件及簽名、蓋章相當，皆可使用。

(二) 契約自由原則：交易雙方得自行約定應採行何種適當之安全技術、程序及方法作成之電子簽章或電子文件，以作為雙方共同信賴及遵守之依據，立法者不以強行規定規範技術標準。另憑證機構與使用者之間亦可自行約定雙方之權利義務關係。

(三) 市場導向原則：政府對於憑證機構之管理及電子認證市場之發展，宜以最低必要之規範為限。今後電子認證機制之建立及電子認證市場之發展，宜由民間主導發展各項電子交易所需之電子認證服務及相關標準。

第三節 區塊鏈簽名與現行法相容性

根據本法第 2 條，「電子簽章」 指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。而「電子文件」則指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。

本法對於電子簽章之定義如同美國和歐盟等立法例以抽象的方式描述電子簽章之內涵，但我國條文文字卻更加不明確，僅稱電子簽章係指與電子文件有關聯性並具依附性關係，與美國或歐盟將規範主體限定於電子數據或電子的聲音、標記或過程不同，我國雖然在定義上放寬但卻在功能上進行限縮，必須得以辨識簽署人身分、資格及電子文件真偽方屬本法的電子簽章。

區塊鏈共識機制取代了數位簽章中憑證機構的角色，以往需要憑證機構發給申請人私鑰並簽發公鑰憑證，以供第三人驗證公鑰和私鑰之配對關係，確保公鑰確實為數位簽章簽署者(申請人)所有，如同數位環境的戶政事務所，負責

DOI:10.6814/NCCU201901043

個人身分審核與證明，但區塊鏈中只利用共識機制和雜湊函數技術確保資料不被竄改，並確認是由寄件者(數位簽章簽署者)所加密和簽署的資料，最後由區塊鏈中的節點共同進行驗證，並無憑證機構進行個人身分審核與證明，因此只能確保簽署者身分來源的正確性，但卻無法證明確實由簽署者本人為之。

因此區塊鏈簽章非本法所稱之電子簽章，而無法納入本法之保護範圍，應可參照美國 UETA 或歐盟 eIDAS 之作法，將電子簽章定義放寬，即電子簽章不須與真實身分勾稽為必要，以符合電子簽章技術中立之原則，至於真實身分勾稽之需求，實務上由憑證機構為之，但美國、歐盟皆未要求憑證機構之設置為電子簽章成立之要件，換言之，憑證機構對於真實身分之審核只是增強使用者的信任和法律上之效力，歐盟即以是否為合格憑證機構所簽署之電子簽章區分為基本電子簽章、進階電子簽章、合格電子簽章，而異其法律上之效力。我國以數位簽章技術作為設計電子簽章法的基礎[294]，而數位簽章技術設有憑證機構作為簽章簽署者身分查核的角色，因此，每個數位簽章都與個人身分進行連結，但數位簽章技術僅是實現電子簽章的一種方式，電子簽章與真實身分連結此一行政管理上之需求與電子簽章本身之技術、安全性無關，不應以此限制電子簽章法所能保護之射程範圍，否則將與電子簽章法技術中立的立法原則有所違背，並箝制了其他技術的發展與應用。

第四節 區塊鏈分散式節點責任與現行法相容性

本法係採技術中立原則，電子簽章可泛指數位簽章、生物辨識、指紋辨識、瞳孔虹膜辨識、聲紋辨識、DNA 比對鑑識等技術，但數位簽章技術發展最

[294] 立法院公報第 90 卷第 47 期第 51 頁時任經濟部政務次長林義夫先生指出政府設計電子簽章法確實是以數位簽章技術作為藍圖和想像，乃因數位簽章技術是當時世界發展最快和最為成熟的電子簽章技術。

DOI:10.6814/NCCU201901043

早且成熟度最高，因此本法以數位簽章技術為中心而制定憑證機構的相關規範。

本法第 11 條至第 15 條皆為憑證機構相關規範，憑證機構對因其經營或提供認證服務之相關作業程序，致當事人或善意第三人因信賴該憑證而受有損害者，皆應負賠償責任，但若能證明無過失或對憑證之使用範圍設有明確限制時，對逾越該使用範圍所生之損害，皆不負賠償責任，第 14 條第 1 項、第 2 項定有明文。

第 14 條乃推定過失責任之立法方式，只要憑證機構因經營或提供認證服務有致當事人或善意第三人受有損害之事實，即推定有過失，憑證機構就其無過失負舉證責任，對於受損害之當事人或第三人較為有利。

區塊鏈以共識機制取代憑證機構的概念，共識機制的開發係開發者所建立，共識機制的運作則有賴區塊鏈網絡中的節點共同為之，兩者是區塊鏈網絡中的要角，共同維護著區塊鏈的運行，自應課予理性節點和開發者所應用有的善良管理人之注意義務，並如同現行法對於憑證機構之規定，亦應以推定過失責任為原則，由節點和開發者舉證自己無過失，例如舉證節點和開發者的系統設備或開發環境符合國際資訊安全管理標準等，由傳統憑證機構一人做為責任主體轉變為開發者和網絡中的節點共同承擔責任，而彼此的法律關係，雖未能如大陸法系以事實上契約作為成立契約關係的依據，但依照民法第 153 條，意思表示亦可以默示為之，而所謂默示之意思表示係指表意人之舉動或其他情事，足以間接推知其效果意思者而言[295]，因此若表意人以獲利為目的，並自願加入區塊鏈網絡成為節點，應可認為有成立合夥關係之合意。

依據我國民法第 667 條，合夥係指二人以上互約出資以經營共同事業之契約，而出資得為金錢或其他財產權，或以勞務、信用或其他利益代之。若合夥

[295] 最高法院 29 年上字第 762 號判例。

DOI:10.6814/NCCU201901043

人因執行合夥事務，侵害他人權利而成立侵權行為者，與法人之有代表權人，因執行職務加損害於他人之情形相類，其所生之法效應等量齊觀，被害人自可類推適用民法第 28 條之規定，請求合夥與該合夥人連帶負賠償責任[296]。惟節點若為公司，依據我國公司法第 13 條則不能成為他合夥事業之合夥人，因此在本國法之規範下，僅於開放式區塊鏈方能以合夥定性區塊鏈各節點之法律關係；若於聯盟鏈中，通常節點為社團法人中的公司，則不能成立合夥關係，但因聯盟鏈成員資格採事前審查，且締結契約以明確規範彼此權利義務關係，因此不若開放式區塊鏈各節點因無明確意思表示而造成疑義。

區塊鏈中各個節點提供運算資源以驗證每一筆交易資料以獲取潛在利益如比特幣、代幣，縱使運算資源非此條文所指稱的財產權出資，應可認為是一種利益的出資，尤其區塊鏈的去中心化，傳統由中心機構擔負的資料驗證和維護帳本的責任，轉由各個節點共同承擔之，因此各節點的運算資源對於區塊鏈網絡的順利運行是不可或缺的重要利益，藉由下載程式成為區塊鏈的節點，可推知其有為區塊鏈網絡的共同利益作出貢獻之默示意思表示，因而成立合夥關係，而對外負連帶責任，若任一節點違反理性節點之注意義務而成立侵權責任，例如：未定期進行安全性漏洞修補與更新，因而侵害他人權利而成立侵權行為者，有如法人之代表權人對外成立侵權行為，被害人可類推適用民法第 28 條請求區塊鏈網絡和該節點連帶負賠償責任。

綜上所述，區塊鏈運行機制和數位簽章中心化憑證機構的運行機制有本質上的不同，本法憑證機構相關行政管理規範難以適用於現行區塊鏈機制，但責任的設計則應可與憑證機構推定過失責任相同，將舉證責任由節點承擔，方符合電子網路世界使用者較難舉證服務提供者是否有故意過失之現狀。

[296] 最高法院 101 年度台上第 1695 號民事判決。

DOI:10.6814/NCCU201901043

第五節 數位簽章時間戳之規範漏洞與區塊鏈時間戳之規範架構

美國 UETA 並無時間戳的相關規範，但與本法同屬大陸法系的歐盟 eIDAS 不僅給予時間戳明確定義，並根據符合不同要件之時間戳賦予不同之證據能力，探求原因係因兩個不同法系的國家對網路科技的規範有著截然不同的態度。

美國自始以來對於網路科技偏向放任態度，歐盟則是規範導向之監理，明確於法規範中制定要件並要求業者遵守。因此，美國於憑證機構管理機構責任、時間戳之定義和第三方時間戳機構責任皆無著墨，而由業者自律和市場競爭淘汰不適任業者，藉此維持創新的能量。

本法主要參酌聯合國[297]、歐盟，但繼受方面卻出現立法體系不一致情形，關於憑證機構責任採取歐盟明確規範的立法模式，但關於時間戳卻無任何相關規範，立法者的態度於立法文件中並無紀錄，因此亦無法確定立法者欲採卻的是美國放任的態度，而委由市場機制監督和業者自律，還是採取歐盟規範式監理態度作一明確規範。若欲採取歐盟立法例，無時間戳規範即是一立法疏漏，應可參酌同屬大陸法系歐盟的立法方式，明確賦予時間戳法律上效力和證據能力，否則僅賦予電子簽章效力，卻不對電子簽章能否作為呈堂證據至關重要的時間戳作出規範，難免有臨門一腳之憾。

區塊鏈時間戳係由雜湊函數和鏈狀的資料結構(每個區塊之哈希值皆是以前一個區塊資料和時間戳經雜湊函數運算後所得)，且透過網絡中每個節點之共同驗證，安全性比數位簽章時間戳更值得信賴，因此區塊鏈本身非規範重點，而應著重於區塊鏈開發者對於程式開發的流程和風險控管，包含人員組織管理、

[297] 美國 UETA 即是參照聯合國而制定。

DOI:10.6814/NCCU201901043

程式碼維護、系統設備更新等，以確保區塊鏈之運行正確順暢，進而加強區塊鏈時間戳本身作為證據之證明力。

第六節 電子簽章法修改建議

本章第三節至第五節主要以區塊鏈簽名、區塊鏈分散式節點責任和區塊鏈時間戳三個部分分析區塊鏈與電子簽章法之異同，以下亦以此分述電子簽章法之修改建議：

第一部分，區塊鏈簽名能確保簽署者所加密和簽署的資料不被竄改，但因無憑證機構作身分勾稽，因此並無法確認簽署者的真實身分和資格，故無法該當本法第 2 條對於電子簽章可用以辨識及確認電子文件簽署人身分、資格的定義。

考量本法立法目的和國際的趨勢，皆以技術中立為原則，因此只要能識別簽署人(識別功能)、表達簽署人之意向(表達意向功能)、證明契約的存在(證據功能)的電子技術，皆應可適用電子簽章法而有法律上之效力，不讓立法的文句對技術發展造成限制或偏袒的效果，以維護自由市場競爭和創新發展。

據此應可參酌美國 UETA、歐盟 eIDAS 之電子簽章定義：

美國 UETA 第 2 條第 8 項：「「電子簽章」 係指以電子的聲音、標記(symbol)或過程(process)附加於或邏輯上關聯於一份記錄。」

歐盟 eIDAS 第 3.10 條：「「基本電子簽章」係指一電子形式的數據，附加於或邏輯地與其他電子形式數據相關聯，並提供簽名人用於簽署之目的。」

由上述可觀察出美國 UETA 和歐盟 eIDAS 皆未規範電子簽章本身須具備識別簽署者真實身分的功能[298]，僅說明其為一電子標記或數據附加於或邏輯上與

[298] 電子簽章中簽署者之身分通常另設立憑證機構進行識別和檢驗，有如現實生活中的戶政事務

DOI:10.6814/NCCU201901043

電子文件相關聯，甚至未要求電子簽章須達到與簽署者或簽署之文件有不可否認性之功能，將法規範客體放寬至最大，因此各項電子簽章技術隨著時間演進或科技技術進步，皆能納入電子簽章法規範中，至於其法律上效力或證據能力，則會因個案所使用的核心技術或標準嚴謹程度而賦予不同之法律上效力和證據能力。

我國與歐盟皆為大陸法系國家，非如美國以實務判例之累積而形成判準，故可參酌歐盟 eIDAS 區分三種不同之電子簽章類型：基本電子簽章、進階電子簽章、合格電子簽章，規定不同要件並異其法律上效力和證據能力，以維護法律上之安定性，並提供業者可供遵循之準則，亦同時保護消費者權益。

第二部分，區塊鏈分散式節點責任，各節點間與開發者之權利義務可參酌合夥關係進行規範，而我國電子簽章法中關於憑證機構規範乃以數位簽章技術為基礎建立，與區塊鏈運行機制有所不同，縱使如認許制區塊鏈，為改善公有鏈使用 POW 共識機制所耗費之大量資源和時間，因此採用類似傳統中間機構或只賦權於某些超級節點進行節點資格審核或驗證資訊以追求效率，雖有中心化之特點，但實際運行原理仍與數位簽章憑證機構不同，因此我國電子簽章法中對於憑證機構行政管理規範難以移植適用於開放式或認許制區塊鏈，但節點損害賠償責任宜與憑證機構推定過失責任作相同設計，因被害者使用區塊鏈提供之服務，對於區塊鏈使用的系統設備、演算法設計或資訊安全防護皆難以知悉，在如此雙方資訊不對等、證據偏在的情形下，應課予負有專業知識能力或對自己設備較為了解之節點負擔舉證責任，方符合公平要求。

至於注意義務之標準應以一個理性之開發者或節點應盡之注意義務作為衡

所負責個人身分審核並發給身分證明，電子簽章本身僅能證明係由正確之來源簽署，但無法證明是由真正簽署者使用電子簽章。例如甲拿著乙的印鑑和存簿至郵局領錢，郵局僅能形式審查檢驗其具備由乙帳戶領錢之必備文件：乙的印鑑和存簿，但無法確認拿著乙印鑑和存簿的甲是否確實為乙本人。

DOI:10.6814/NCCU201901043

量基準，如程式碼維護、安全性漏洞修補與更新、組織資安教育訓練、風險管理等，相關資訊安全規範亦可參照我國個人資料保護法第 19 條第 1 項第 2 款，其指出非公務機關對於個人資料之蒐集或處理應採取適當之安全措施，又所謂「適當之安全措施」依照個人資料保護法施行細則第 12 條係指防止個人資料被竊取、竄改、毀損、滅失或洩漏，而採取技術上及組織上之措施，且此措施應與所欲達成之個人資料保護目的間，具有適當比例為原則。而「措施」得包含以下事項[299]：

一、配置管理之人員及相當資源。

二、界定個人資料之範圍。

三、個人資料之風險評估及管理機制。

四、事故之預防、通報及應變機制。

五、個人資料蒐集、處理及利用之內部管理程序。

六、資料安全管理及人員管理。

七、認知宣導及教育訓練。

八、設備安全管理。

九、資料安全稽核機制。

十、使用紀錄、軌跡資料及證據保存。

十一、個人資料安全維護之整體持續改善。

以上 11 項資訊安全措施亦可作為衡量區塊鏈網絡節點是否盡到善良管理人注意義務之指標，以防相關法規所課予之資訊安全注意義務標準不一，不利業者遵循和發展。

綜上所述，現行電子簽章法關於憑證機構規範是以數位簽章技術為基礎和架構予以規範，難以適用區塊鏈之運作機制，宜另設章節作權利義務之規範方

[299] 個人資料保護法施行細則第 12 條第 2 項。

DOI:10.6814/NCCU201901043

為適宜，但對於所有電子簽章技術皆應注意的資訊安全議題，則可參照現行個人資料保護法中對於非公務機關儲存或交換個人資料之系統設備所課予之資訊安全規範[300]作相同程度的設計或以國際上資訊安全管理標準 ISO/IEC 27000、ISO/IEC 27001 作為參考指標，可於法規以列舉方式定之，但不宜直接課予作為義務，僅作為業者可資遵循的標準與法院進行損害賠償責任裁判的基準和心證依據，其它則委由業者自律和市場監督，以避免過度妨礙市場的自由競爭，並維持資訊科技技術創新發展的能量[301]。

第三部分，美國 UETA 並無時間戳的相關規範，故可參酌同屬大陸法系之歐盟 eIDAS 對於時間戳的立法模式：

歐盟 eIDAS 第 41.1 條：「電子時間戳不得僅因時間戳為電子形式或不符合本法合格電子時間戳之要件，而否認其作為法律上證據之能力。」

歐盟 eIDAS 第 41.2 條：「合格電子時間戳應享有日期和時間準確性和其所綁定資料具有完整性之推定。」

由上述可知，歐盟 eIDAS 不強行規定僅合格電子時間戳方有法律上效力，而是符合合格電子時間戳之要件下享有法律上關於時間準確和資料完整之推定，若對於合格電子戳之時間有所疑義或主張其所綁定之資料完整性有所欠缺，則應由對造負舉證責任。

此種立法模式旨在保護電子時間戳不會因其電子形式而否認法律上之效

300 例如個人資料保護法施行細則第 12 條列舉公務機關或非公務機關所應盡之「適當安全措施」義務。

301 業者若能遵循嚴格之資訊安全標準，例如具有國際公信力之準 ISO/IEC 27000、ISO/IEC 27001，將提升使用者使用相關產品之意願，至於不採用嚴格資訊安全標準之業者，則可能在市場競爭之下逐漸不受使用者信賴，因而退出市場。尤其相較於其他產品，資訊科技產品或服務之週期相當短暫，競爭激烈的情形下，眾家業者將競相推出好的產品和服務以取得顧客忠誠度，實不須以法律規範相繩，而委由市場監督機制，並制定消費者保護的損害賠償規範即可。

DOI:10.6814/NCCU201901043

力，惟個案中是否具有法律上之效力和證據能力，則應進一步探討其所產生電子時間戳的技術、設備、資訊安全防護等，因此合格電子時間戳要件之規定，其實就是關於資訊安全之規範，當電子時間戳可偵測資料是否遭到竄改、時間源準確、由合格機構所產生等中性條件，則應賦予法律上效力並享有法律上推定以減輕舉證之責任，而不規範僅某項技術所產生的電子時間戳方為合格電子時間戳，以符合國際電子簽章法一貫之「技術中立原則」，我國亦可參酌相關規定以補足時間戳漏未規範之弊病，賦予法律上效力和證據能力，尤其未來以區塊鏈為基礎之電子商務革命即將開展，電子交易和資料交換相關爭議只會更多，而電子時間戳作為權利義務關係發生時間的佐證，具有商務上和法律上之重要性，應速予規範，以利在法制上的基礎帶動區塊鏈下一波的電子商務革命。

DOI:10.6814/NCCU201901043

第六章 結論

2008 年 9 月 15 日雷曼兄弟倒閉，金融海嘯席捲全球，造成全球股市巨幅下跌，並連帶影響各國經濟發展，更重要的是對於中心化的金融運作體系產生信心危機，在雷曼兄弟破產的一個月後，2008 年 10 月 31 日 Satoshi Nakamoto 以區塊鏈技術所推出的第一項區塊鏈應用-點對點電子現金系統比特幣，該系統透過點對點進行，無須仰賴金融中介機構，即能達到貨幣移轉、交易即結算等功能，而且不可竄改之特性更加迎合網路使用者長久以來對於安全、隱私的期待，比特幣的出現等於宣告挑戰現有的中央集權式貨幣體系。

前三次世界重要的發明和變革如蒸汽機、電能、電腦和互聯網，其所提升的是工業生產的效率或生活之便利性，但區塊鏈的出現是根本治理模式層面的變革，以往建立在中心化治理模式的各種資訊交換活動，甚至是產業運行規則、商業模式和治理思想都將因區塊鏈的出現而須有不同的風貌，其不只是破壞創新，而是人類秩序的重新形塑。

區塊鏈是多項技術的集合名詞，包含共識機制、公開金鑰加密演算法、Merkle Tree、時間戳等，融合舊有技術並創造新的價值是區塊鏈發明人 Satoshi Nakamoto 的一大貢獻，但此種顛覆性的技術和相關應用如何重新塑造監理思維並建立法規範，以提供法律上之效力至為重要。

目前國際上對於區塊鏈相關應用的監理仍是採取個案審查(Case-by-Case)，頭痛醫頭腳痛醫腳的破碎式監理方式，造成法不安定性，人民無法預見其所為之行為的法律效果，無助創新的發展，因此應從區塊鏈所驅動的金融科技世代的特性作不同的監理思維的變化。

區塊鏈技術所驅動的金融科技世代，對於各產業產生顛覆性的影響，帶來的商業模式改變、監理複雜程度、風險內容都有大幅變化，難以一標準即適用

DOI:10.6814/NCCU201901043

於所有應用區塊鏈技術之各項產業，應視產業特性而訂定不同監理規範，方符合平等原則。此外，在瞬息萬變的區塊鏈世代，創新發展週期將不像以往以 10 年至 20 年作為一個週期，現在可能 10 年內就有一以區塊鏈技術為基礎的商業模式對人類生活產生深刻影響，因此應以差異化監理作為中心思想，輔以酌情應用(比例原則)、賦能致動(合作互動)、數據驅動(數據分析)、不予傷害(避免干預)等原則，考量公共利益、社會成本賦與不同監理框架，並以溝通、合作、互動的方式讓監理者和被監理者對科技技術、產品服務和其可能帶來的風險種類大小進行互信和了解，藉此監理者亦能蒐集相關資料和意見後，並輔以監管科技將這些資料(Raw data)轉換成有價值的資訊(Information)以供監理機關建立事前預測分析和事中監控計畫，以因應創新、跨境交易頻繁所帶來的監理複雜度和合規成本的提升。

巨觀的區塊鏈監理中心思想確立後，方才是微觀的法規範體制之建立，而法規範體制又能分為實體層和應用層，實體層聚焦的是科技技術的特性和相應之管理方式；應用層聚焦的則是在科技技術的基礎下所開展的各項商業應用和法律關係。

電子簽章法作為 19、20 世紀電子商務開展的關鍵法律之一，承認數位環境所為之法律行為效力，亦是本文所指稱的實體層規範，目前國際上以美國為首如美國亞利桑那州、田納西州、內華達州或德拉瓦州，將區塊鏈法律納入電子簽章法中，此係鑑於區塊鏈技術與電子簽章使用的技術部分重疊，而此重疊部分分別為電子簽章、中心憑證機構責任和分散式節點責任、時間戳。

美國、歐盟對於電子簽章之定義在技術中立原則下，只要能識別簽署人(識別功能)、表達簽署人之意向(表達意向功能)、證明契約的存在(證據功能)的電子技術皆可適用電子簽章法而有法律上之效力，區塊鏈簽章除了符合上述功能之外，更能確保所簽署之資料的完整性和不可竄改性，安全性更勝一籌，當能

DOI:10.6814/NCCU201901043

符合定義。然而我國雖然對於電子簽章亦採抽象定義，但侷限於可辨識簽署人身分、資格及電子文件真偽的電子簽章方符合我國現行法之保護範圍，本文認為太過狹隘，將行政管理上對於真實身分認定之需求用以認定技術是否應受法律保障不適當亦不合理，建議應可採取歐盟 eIDAS 將電子簽章分為三種類型：基本電子簽章、進階電子簽章和合格電子簽章而異其法律上之效力和證據能力，類型化的方式讓業者得自行選擇對其最適合的選項，並委由市場機制來監督，而非先將某些電子簽章技術排除在外，不僅扼殺創新的發展亦讓市場選擇項目減少，不利不同產業發展之需求。

現行電子簽章下中心憑證機構的建置是為驗證公鑰來源，並確保資料傳輸的安全性，但區塊鏈的共識機制取代了中心憑證機構的功能，驗證工作和帳本維護的工作由網絡上所有節點共同為之，因此傳統由中心節點單獨負責的模式不復存在，轉而由每個節點共同承擔責任，這也是電子簽章和區塊鏈最大的不同之處。

區塊鏈類型又可分為開放式區塊鏈和認許制區塊鏈，開放式區塊鏈是完全的去中心化，節點可任意加入，並共同維護一個帳本，彼此的法律關係接近於合夥或合資，縱使節點間無明示之意思表示，但在普通法系、大陸法系普遍承認事實上行為在基於誠信和公平之法理的衡量下亦可能成立契約關係下，若節點有主觀上獲取利益為目的而加入區塊鏈網絡成為節點，則彼此之間仍可成立合夥之契約關係，而平均分擔責任；我國實務雖然不承認僅憑事實行為而能成立事實上契約關係，但肯認基於特定事實可得推知雙方有締約之默示意思表示，因此在我國法下亦能成立合夥契約而平均分擔責任。

至於區塊鏈因故發生資料遺漏、外洩之侵權責任情形，由於國際尚未承認數位資料所有權的概念，因此討論重點會集中於數位資料遺漏所造成之純粹上經濟損失是否得以請求。普通法系肯認故意侵權行為得請求純粹上經濟損失，

DOI:10.6814/NCCU201901043

過失侵權行為則在行為人對於造成損害的事實得以預見且行為人之行為與結果之發生具有因果關聯性時得以請求純粹上經濟損失；大陸法系則恪守需有絕對權受有侵害方得請求損害賠償，純粹上經濟損失不管是行為人故意或過失造成，皆不得請求損害賠償；我國對於純粹上經濟損失雖然無法依照民法第 184 條第 1 項請求，但可依民法第 184 條第 1 項後段主張侵權責任，惟須舉證行為人有背於善良風俗之情事。另亦可依照民法第 184 條第 2 項主張違反保護他人之法律而該當侵權責任，而此處之「法律」應指個人資料保護法第 2 條而言。

認許制區塊鏈的法律關係相對來說較為簡單，由於成員身分皆事先經過審核，團體亦有其成立之目的和宗旨，因此多會事先簽定契約以釐清彼此在區塊鏈網絡所擔任之角色與責任，契約關係即依雙方承諾而定；至於侵權責任，則與開放式區塊鏈的討論相同，主要會聚焦於純粹上經濟損失是否能請求的部分。

時間戳在電子簽章之運行下仰賴中心憑證機構簽發憑證方式為之，關於時間戳在訴訟上之證據能力，美國未有相關規定，但根據美國實務上之分類應屬非人類之陳述的電腦生成紀錄，因此其證據能力應以產生時間戳機構的系統運行是否正常運作來斷定，且時間戳透過電腦顯示具有視覺可讀性，亦符合最佳證據法則指稱之原始文書而得為作為證據；歐盟明文規定合格時間戳之要件，其所載的日期和時間推定為正確且其所綁定之資料亦推定具有完整性；我國關於時間戳之規定，從電子簽章法 2001 年公布以來一直付之闕如，承認電子簽章效力促進電子商務發展，卻未能對於電子簽章之時間戳是否具有證據能力予以明確規範實屬可惜，最後一哩路若能完成，將能完備我國電子簽章法之法制。

區塊鏈的時間戳是由每個區塊抓取系統時間後取得，並與區塊頭(Block Header)的資料一同經過雜湊函數 Hash 運算後，成為下一區塊的 Hash 值，因此每個區塊呈現連動狀態，任一區塊鏈資料有所變動皆會被發現，保障了資料的

DOI:10.6814/NCCU201901043

完整性、不可否認性、不可竄改性，亦讓時間戳上的日期和時間成為可信賴之證明。因此區塊鏈時間戳的安全性比電子簽章時間戳更值得信賴，因此承認其在訴訟上之證據能力應無問題，現行電子簽章法關於時間戳規範亦能直接適用。

我國電子簽章法雖然採取與國際電子簽章法相同之技術中立原則，但卻於電子簽章定義加以限縮，惟有可辨識簽署人身分、資格及電子文件真偽的電子簽章方屬我國電子簽章法之保護範疇，應參照美國 UETA 和歐盟 eIDAS 將電子簽章定義放寬，以利隨著科技技術的變動而能容納不同技術特性之電子簽章技術。

區塊鏈分散式節點責任之設計，傳統中心憑證機構之管理資料、驗證功能在區塊鏈中由各個節點共同分擔之，因此課予憑證機構如程式碼維護、安全性漏洞修補與更新、組織資安教育訓練、風險管理等注意義務，應該也會是各個理性節點所應負擔之注意義務，不應有所差別待遇，而現行法上可參考個人資料保護法施行細則第 12 條或國際上資訊安全管理標準 ISO/IEC 27000、ISO/IEC 27001 制訂相關資訊管理之最低規範，但不課予作為義務，僅作為業者可資遵循的標準與法院進行損害賠償責任裁判的基準和心證依據，其它則委由業者自律和市場監督，以避免扼殺創新和市場自由競爭。

時間戳的概念於我國電子簽章制定之初，未見討論，但其在訴訟法上作為權利義務關係發生時間的佐證，具有商務上和法律上之重要性，應速予規範，並參考歐盟 eIDAS 一概承認其證據能力，但因產生電子時間戳的技術、設備、資訊安全防護等差異而異其舉證責任。

區塊鏈作為第四次工業革命的關鍵技術，其所帶來的去中心化啟示，中心權力將下放至各個節點所擁有，未來對於數位資料如何處分和使用收益，將不再由中心權力機構掌握話語權，而這樣全新的分散式治理模式將深刻影響社

DOI:10.6814/NCCU201901043

會，電子簽章法作為區塊鏈應用法律效力的根據，在本文提出的三個與區塊鏈有所競合的部分若能進行修訂和立法，將有助區塊鏈相關的商業模式和法律關係在可信賴的法治基礎上展開，並成為未來金融科技健全發展的重要觸媒。

DOI:10.6814/NCCU201901043

參考文獻

一、 中文資料

(一)專書

1. 邱聰智，新訂民法債編通則(上)，一版，2000 年。
2. 陳祥輝，TCP/IP 網路通訊協定，博碩文化出版社，二版，2011 年 12 月。
3. 駱建功、吳大智、周師文、呂有勇，數位貨幣與區塊鏈，一版，駱建功出版社，2017 年 9 月。
4. 李淑明，債法各論，八版，元照出版社，2017 年 1 月。
5. 王聖雯，ICO 市場的法律問題與監管研究，一版，元照出版社，2018 年 9 月。

(二)期刊文章

1. 王澤鑑，德國最高法院民事判利研究(二)，國立臺灣大學法學論叢，第 2 卷第 1 期，1972 年，頁 237。
2. 林誠二，契約之成立約推定成立，月旦法學教室，第 82 期，2009 年 8 月，頁 10。
3. 黃心怡，英美侵權行為概論，月旦法學雜誌，第 189 期，2011 年 2 月，頁 154。
4. 葉啟洲，純粹經濟上損失在台灣侵權行為法上的保護-以最高法院相關裁判為中心，月旦法學雜誌，第 241 期，2015 年 6 月，頁 49。
5. 麥肯錫大中華諮詢業務，區塊鏈—銀行業遊戲規則的顛覆者，2016 年 5 月，頁 10。
6. 張冠群，自金融監理原則與金融消費者保護觀點論金融科技監理沙盒制度——兼評行政院版「金融科技創新實驗條例草案」，月旦法學教室，第 266 期，2017 年，頁 5-6。
7. 彭金隆、臧正運，我國金融科技創新實驗落地機制之檢視與構，月旦法學教

DOI:10.6814/NCCU201901043

室，第 266 期，2017 年 7 月，頁 49。
8. 杜宏毅，如何建置一個實用的區塊鏈平台，財金資訊季刊，第 90 期，2017 年 10 月，頁 45。
9. 陳恭，智能合約的發展與應用，財金資訊季刊第 90 期，2017 年 10 月，頁 33。
10. 臧正運、曾宛如、方嘉麟，從區塊鏈融資論眾募規範趨勢，月旦法學雜誌，第 273 期，2018 年 2 月，頁 89。

(三)學位論文

1. 邱琦，純粹經濟上損失之研究，台灣大學法律研究所碩士班論文，2002 年，頁 108。
2. 李昊，論英美侵權法中過失引起的純經濟上損失的賠償規則，比較法研究，第 5 期，2005 年 9 月，頁 64。
3. 朱帥俊，刑事證據法則對於電子證據適用之研究，交通大學管理學院碩士在職專班科技法律組，2007 年，頁 162。
4. 侯乃真，金融科技創新監理之新途徑-以監理沙盒為中心，台灣大學法律學研究所碩士班論文，2017 年，頁 58。

(四)網際網路

1. 張健，揭秘比特幣和區塊鏈：什麼是區塊鏈？，參考網址：https://read01.com/zh-tw/a00e7m.html#.Wrny-cOuzIV (最後瀏覽日：2019 年 7 月 1 日)
2. 許明恩，礦工失業倒數：以太坊轉型權益證明機制，參考網址：https://reurl.cc/pDdA8 (最後瀏覽日：2019 年 7 月 1 日)
3. 王妍文，當供應鏈金融遇上區塊鏈，誰能吃下新商機？，參考網址：http://www.ftrc.nccu.edu.tw/wordpresseng/?p=3439 (最後瀏覽日：2019 年 7 月 1 日)
4. 黃嶠濛，區塊鏈+供應鏈金融：旨在打造供應鏈金融資產的交易所，參考網址：https://zhuanlan.zhihu.com/p/31216243 (最後瀏覽日：2019 年 7 月 1 日)
5. 林建甫，供應鏈金融 促進新南向金融版圖擴張，參考網址：

DOI:10.6814/NCCU201901043

https://m.ctee.com.tw/album/4c8c65b0-5bd2-4ec7-8a6c-9447a11812bc/828080 (最後瀏覽日：2019 年 7 月 1 日)

6. 余至浩，【臺灣區塊鏈應用實例】克服音樂版權難題第一步，靠區塊鏈解決授權分散痛點，參考網址：https://www.ithome.com.tw/news/119249 (最後瀏覽日：2019 年 7 月 1 日)
7. 章忠信，著作利用與授權之疑義解析，參考網址：http://www.copyrightnote.org/ArticleContent.aspx?ID=9&aid=2540 (最後瀏覽日：2019 年 7 月 1 日)
8. 胡一天，數位身分與區塊鏈記憶體，參考網址：http://www.storm.mg/article/116734 (最後瀏覽日：2019 年 7 月 1 日)
9. 翁書婷，我們要呼籲慈濟用區塊鏈處理大眾的捐款嗎？，參考網址：https://www.bnext.com.tw/article/44124/should-tzuchi-start-to-consider-adopting-blockchain-technology-for-the-transparency-of-the-charity-donation (最後瀏覽日：2019 年 7 月 1 日)
10. 翁書婷，台灣需要什麼樣的 FinTech 加速器？也許可以參考新加坡，參考網址：https://www.bnext.com.tw/article/39160/BN-2016-04-08-183106-40 (最後瀏覽日：2019 年 7 月 1 日)
11. 臧正運，臧正運觀點：形塑全球金融科技監理標準的關鍵語彙，風傳媒，參考網址：http://www.storm.mg/article/165779 (最後瀏覽日：2019 年 7 月 1 日)
12. Terry Chen，台灣網路編年史(一)：1968 年至 2008 年，參考網址：http://tesa.today/article/700 (最後瀏覽日：2019 年 7 月 1 日)
13. 楊中皇、葉志青、蘇聖雄、張家瀚，時戳服務，資通安全政策分析專論，財團法人國家實驗研究院科技政策研究與資訊中心，參考網址：http://security.nknu.edu.tw/psnl/publications/2007/10_CHANG,KU-HAN/%AC%E3%A8s%A5%CD%A4w%B5o%AA%ED%A4%CE%A4w%B1%B5%A8%FC%A4%A7%A4%E5%B3%B9.pdf (最後瀏覽日：2019 年 7 月 1 日)
14. IThome，2018 企業資安調查，參考網址：https://www.ithome.com.tw/article/122191 (最後瀏覽日：2019 年 7 月 1 日)
15. 金融監督管理委員會銀行局，關於金融資產證券化，參考網址：

DOI:10.6814/NCCU201901043

https://www.banking.gov.tw/ch/home.jsp?id=116&parentpath=0,8,115 (最後瀏覽日：2019 年 7 月 1 日)

16. 金融監督管理委員會，關於不動產證券化，參考網址：https://www.banking.gov.tw/ch/home.jsp?id=279&parentpath=0,8,119&mcustomize=onemessages_view.jsp&dataserno=21786&aplistdn=ou=data,ou=business,ou=one,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=Business (最後瀏覽日：2019 年 7 月 1 日)
17. 中華民國信託業商業公會，不動產證券化，參考網址：http://www.trust.org.tw/content/index.asp?pno=187 (最後瀏覽日：2019 年 7 月 1 日)
18. 中華民國證券投資信託暨顧問商業同業公會，國際動態，參考網址：https://members.sitca.org.tw/OPF/K0000/files/CWeb/9804 國際動態.pdf (最後瀏覽日：2019 年 7 月 1 日)
19. 經濟部標準檢驗局，ISO 28000 供應鏈安全管理系統標準簡介，參考網址：www.bsmi.gov.tw/wSite/public/Data/f1388125037366.pdf (最後瀏覽日：2019 年 7 月 1 日)
20. 經濟部智慧財產局，著作權基本概念篇，參考網址：https://www.tipo.gov.tw/ct.asp?xItem=219595&ctNode=7561&mp=1 (最後瀏覽日：2019 年 7 月 1 日)
21. 行政院函請審議「電子簽章法」草案文書，參考網址：https://lis.ly.gov.tw/lgcgi/lgmeetimage?cfcbcfcdcecbcfcfc5cac8c8d2cac7c7 (最後瀏覽日：2019 年 7 月 1 日)
22. 中華人民共和國工業和信息化部，七部門關於防範代幣發行融資風險的公告，參考網址：http://www.miit.gov.cn/n1146290/n4388791/c5781140/content.html (最後瀏覽日：2019 年 7 月 1 日)
23. 中國最高人民法院，《最高人民法院關於互聯網法院審理案件若干問題的規定》的理解與適用，參考網址：https://www.chinacourt.org/article/detail/2018/09/id/3489797.shtml (最後瀏覽

DOI:10.6814/NCCU201901043

日：2019 年 7 月 1 日)

24. 騰訊研究院，區塊鏈在徵信業應用的探討：優勢與特點及場景分析，參考網址：https://read01.com/nNQ2Qn.html#.WsGcGi6uzIV (最後瀏覽日：2019 年 7 月 1 日)

二、外文資料

(一)期刊文章

1. Patricia Brumfield Fry, Introduction to the Uniform Electronic Transactions Act: Principles, Policies and Provisions, 37 Idaho L.Rev. 237, 249-50(2001).
2. Rebecca M. Bratspiess, Regulatory Trust, 51 ARIZONA L. REV. 575, 576-575 (2009).
3. Vincent R. Johnson,The boundary-line function of the economic loss rule, 66 Wash. & Lee L. Rev. 523, 524 (2009).
4. George Cornell ,The evidentiary value of automatically transcribed voicemail messages, 17 Journal of Science & Technology Law 259,276-278(2011).
5. Stephanie Curry , Washington's electronic signature act: An anachronism in the new millennium ,88 Wash.L.Rev 559, 560-561(2013).
6. Susan Cohen, What Do Accelerators Do?Insights from Incubators and Angels,8 Innovations19, 19-21(2014).
7. Lawrence G. Baxter, Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failures, 66 Duke Law Journal 567, 598-600 (2016).

(二)學位論文

1. Satoshi Nakamoto,Bitcoin: A Peer-to-Peer Electronic Cash System (2008).

DOI:10.6814/NCCU201901043

2. Douglas W. Arner &Jànos Barberis & Ross P. Buckley, FinTech, RegTech and the Reconceptualization of Financial Regulation(2016).
3. Zetzsche, Dirk A. and Buckley, Ross P. and Arner, Douglas W., The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain (2017).
4. Stéphane Blemus, Law and Blockchain：a legal perspective on current regulatory trends worldwide (2018).
5. Ranchordas, Sofia and Klop, Abram, Data-Driven Regulation and Governance in Smart Cities (2018).
6. Marco Dell'Erba, Demystifying technology. Do smart contracts require a new legal framework? Regulatory fragmentation, self-regulation,public regulation (2018).

(三)網際網路

1. Weusecoins, Delegated Proof-of-Stake Consensus, available at：https://www.weusecoins.com/assets/pdf/library/Delegated%20Proof-of-Stake%20Consensus.pdf (Last visited on 2019/7/1)
2. Miguel Castro & Barbara Liskov, Practical Byzantine Fault Tolerance, MIT's Computer Science Lab, available at：http://pmg.csail.mit.edu/papers/osdi99.pdf (Last visited on 2019/7/1)
3. Neha Narula,Willy Vasquez,Madars Virza(2018),zkLedger: Privacy-Preserving Auditing for Distributed Ledgers, available at：https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/5aa1b35ce4966bd538d3f1d2/1520546653653/zkledger.pdf (Last visited on 2019/7/1)
4. Internal Revenue Service, Notice 2014-21(March 21, 2014), available at：https://www.irs.gov/pub/irs-drop/n-14-21.pdf (Last visited on 2019/7/1)

DOI:10.6814/NCCU201901043

5. U.S Commodity Futures Trading Commission, Customer Advisory: Understand the Risks of Virtual Currency Trading(December 15, 2017), available at：https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory_urvct121517.pdf (Last visited on 2019/7/1)
6. Accenture, Global Fintech Financing, available at：https://newsroom.accenture.com/news/global-fintech-investments-surged-in-2018-with-investments-in-china-taking-the-lead-accenture-analysis-finds-uk-gains-sharply-despite-brexit-doubts.htm (Last visited on 2019/7/1)
7. Vitalik Buterin, A Proof of Stake Design Philosophy, available at：https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51 (Last visited on 2019/7/1)
8. Zcash, What are zk-SNARKs?, available at：https://z.cash/technology/zksnarks/ (Last visited on 2019/7/1)
9. Nolan Bauerle, What is the Difference Between Public and Permissioned Blockchains?, available at：https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains (Last visited on 2019/7/1)
10. Dan Hyde, Half a million missing out on flight delay compensation, available at：https://www.telegraph.co.uk/news/shopping-and-consumer-news/11790143/Half-a-million-missing-out-on-flight-delay-compensation.html (Last visited on 2019/7/1)
11. Christopher Allen, The Path to Self-Sovereign Identity, available at：https://www.coindesk.com/path-self-sovereign-identity/ (Last visited on 2019/7/1)
12. Jimi S., Blockchain: how a 51% attack works (double spend attack), available at：

DOI:10.6814/NCCU201901043

https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474 (Last visited on 2019/7/1)

13. Coinnounce, 15 insights on how Ethereum conducted its ICO in 2014, available at：https://coinnounce.com/ethereum-ico-2014/ (Last visited on 2019/7/1)

14. US Department of the Treasury, Guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies(March 18, 2013), available at：https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering (Last visited on 2019/7/1)

15. FinCEN, FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws(April 18, 2019), available at：https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money (Last visited on 2019/7/1)

16. The Guardian, Bitcoin to be treated as property instead of currency by IRS, available at：https://www.theguardian.com/technology/2014/mar/25/bitcoin-property-currency-irs-rules (Last visited on 2019/7/1)

17. U.S Commodity Futures Trading Commission, In the Matter of Coinflip, Incd/b/a Derivabit and Francisco Riordan, CFTC Docket No. 15-29 (September 17, 2015), available at： https://www.cftc.gov/PressRoom/PressReleases/pr7231-15 (Last visited on 2019/7/1)

18. U.S Commodity, Futures Trading Commission Federal Court Finds that Virtual Currencies Are Commodities, available at：https://www.cftc.gov/PressRoom/PressReleases/7820-18 (Last visited on 2019/7/1)

DOI:10.6814/NCCU201901043

19. Securities and Exchange Commission, Report of Investigation under 21(a)of the Securities Exchange Act of 1934: The DAO(25 July 2017), available at：https://www.sec.gov/litigation/investreport/34-81207.pdf (Last visited on 2019/7/1)

20. Esther Kim, Wyoming becomes first to give Bitcoin owners full property rights, available at：https://bitcoinist.com/wyoming-bitcoin-full-property-rights/ (Last visited on 2019/7/1)

21. European Bank Authority, Virtual currency schemes – a further analysis (2015), available at：https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (Last visited on 2019/7/1)

22. European Bank Authority, EBA Opinion on 'virtual currencies(4 July 2014), available at：https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+ Opinion+on +Virtual+ Currencies.pdf (Last visited on 2019/7/1)

23. European Bank Authority, Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849, available at：https://eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD (Last visited on 2019/7/1)

24. ESMA, EBA and EIOPA , ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies, available at：https://eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf (Last visited on 2019/7/1)

DOI:10.6814/NCCU201901043

25. Kevin Helms , Bitcoin Transactions Declared VAT-Exempt in Norway, available at：https://news.bitcoin.com/bitcoin-transactions-declared-vat-exempt-in-norway/ (Last visited on 2019/7/1)

26. Nikhilesh De, Germany Won't Tax You for Buying Coffee With Bitcoin, available at：https://www.coindesk.com/germany-considers-crypto-legal-equivalent-to-fiat-for-tax-purposes/ (Last visited on 2019/7/1)

27. European Securities and Market Authority, ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements (November 13, 2017), available at：https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf (Last visited on 2019/7/1)

28. European Securities and Market Authority, ESMA's Advice On Initial Coin Offering And Crypto-Assets, available at：https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf (Last visited on 2019/7/1)

29. R. Viola and O. Guersent, European Commission sets up an internal Task Force on Financial Technology, available at：https://ec.europa.eu/digital-single-market/en/blog/european-commission-sets-internal-task-force-financial-technology(Last visited on 2019/7/1)

30. European Parliament, “Answer given by Vice-President Ansip on behalf of the Commission”, Parliamentary questions(2017), available at：http://www.europarl.europa.eu/doceo/document/E-8-2016-009012-ASW_EN.html (Last visited on 2019/7/1)

31. European Parliament resolution of 3 October 2018 on distributed ledger

DOI:10.6814/NCCU201901043

technologies and blockchains: building trust with disintermediation, available at：http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0373&language=EN&ring=B8-2018-0397 (Last visited on 2019/7/1)

32. European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)), available at ：http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0373&language=EN&ring=B8-2018-0397 (Last visited on 2019/7/1)

33. A Framework for Global Electronic Commerce Executive Summary, available at：https://clintonwhitehouse4.archives.gov/WH/New/Commerce/summary.html (Last visited on 2019/7/1)

34. Financial Conduct Authority, Regulatory sandbox (2015), available at：https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf (Last visited on 2019/7/1)

35. Office of the Comptroller of the Currency, Supporting Responsible Innovation in the Federal Banking System:An OCC Perspective, available at：http://consumerbankers.com/sites/default/files/OCC%20whitepaper%20fin%20inno%282%29.pdf (Last visited on 2019/7/1)

36. IIF, RegTech in Financial Services:Technology Solutions for Compliance and Reporting(2016), available at：https://www.iif.com/Portals/0/Files/private/iif-regtech_in_financial_services_-_solutions_for_compliance_and_reporting.pdf?ver=2019-01-04-142943-690 (Last visited on 2019/7/1)

37. Accenture, REGTECH FOR REGULATORS(2018), available at：

DOI:10.6814/NCCU201901043

https://www.worldgovernmentsummit.org/api/publications/document?id=5ccf8ac4-e97c-6578-b2f8-ff0000a7ddb6 (Last visited on 2019/7/1)

38. Yu An, Yu Zhang and Bo Zeng ,The Reliable Hub-and-spoke Design Problem: Models and Algorithms(2011), available at：http://www.optimization-online.org/DB_FILE/2011/05/3043.pdf (Last visited on 2019/7/1)

39. Andrew G Haldane, Rethinking the financial network(2009), BIS Review, available at：https://www.bis.org/review/r090505e.pdf (Last visited on 2019/7/1)

40. U.S. Commodity Futures Trading Commission ,An Assessment of the Current Implementation of Reform and Proposals for Next Steps, available at：https://www.cftc.gov/sites/default/files/2018-04/oce_chairman_swapregversion2whitepaper_042618.pdf (Last visited on 2019/7/1)

41. Josh Stark, Applications of Distributed Ledger Technology to Regulatory &Compliance Processes(2018), available at：https://www.r3.com/wp-content/uploads/2018/04/Reg_Compliance_R3.pdf (Last visited on 2019/7/1)

42. FinTech Innovation Lab New York,Former New York regulatory chief Maria Vyllo joins FinTech Innovation Lab New York, available at：https://www.finextra.com/pressarticle/78032/former-new-york-regulatory-chief-maria-vyllo-joins-fintech-innovation-lab-new-york (Last visited on 2019/7/1)

43. Financial Conduct Authority, Eligibility for Innovation Hub, available at：https://www.fca.org.uk/firms/project-innovate-innovation-hub/eligibility (Last visited on 2019/7/1)

44. Financial Conduct Authority, Innovate events, available at：https://www.fca.org.uk/firms/innovate-innovation-hub/events (Last visited on

DOI:10.6814/NCCU201901043

2019/7/1)

45. Stone&Chalk, Stone&Chalk programs, available at：https://www.stoneandchalk.com.au/programs (Last visited on 2019/7/1)

46. Global Partnership for Financial Inclusion ,G20 High-Level Principles for Digital Financial Inclusion, available at：http://www.g20.utoronto.ca/2016/high-level-principles-for-digital-financial-inclusion.pdf (Last visited on 2019/7/1)

47. Summary of Bills Pertaining to Electronic Signatures and Authentication in the 106th Congress, available at：http://techlawjournal.com/cong106/digsig/Default.htm (Last visited on 2019/7/1)

48. European initiative on electronic commerce, available at： https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al32101 (Last visited on 2019/7/1)

49. Amended proposal for a European Parliament and Council Directive on a common framework for electronic signatures, available at： http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1523186153809&uri=CELEX:51999PC0195 (Last visited on 2019/7/1)

50. Adobe(2016), Compliance with European electronic signatures legislation, available at：https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-sign-eidas-compliance-uk.pdf (Last visited on 2019/7/1)

51. eSignature in the EU, available at：http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l24118 (Last visited on 2019/7/1)

52. Adam Thierer, 15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm, available at：https://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-

DOI:10.6814/NCCU201901043

clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm/#69bebc471703 (Last visited on 2019/7/1)

53. C. W. Von Bergen, Martin S. Bressler, Never Underestimate the Power of a Backhoe:Integrating Single Points of Failure into Strategic Planning (2014), available at：http://homepages.se.edu/cvonbergen/files/2015/03/Never-Estimate-the-Power-of-a-Backhoe_Integrating-Single-Points-of-Failure-into-Strategic-Planning.pdf (Last visited on 2019/7/1)

54. R3 and Norton Rose,Can smart contracts be legally binding contracts?, available at：http://www.nortonrosefulbright.com/files/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf (Last visited on 2019/7/1)

55. JP Buntinx, What is Blockstream, available at：https://themerkle.com/what-is-blockstream/ (Last visited on 2019/7/1)

56. Klara Palmberg, Complex adaptive systems Properties and approaches (2009), available at：http://www.mementor.se/wp-content/palmberg-complex-adaptive-systems-research-report.pdf (Last visited on 2019/7/1)

57. Gareth W. Peters, Efstathios Panayi.(2015),Understanding Modern Banking Ledgers through BlockchainTechnologies: Future of Transaction Processing and SmartContracts on the Internet of Money (2015), available at：https://arxiv.org/pdf/1511.05740.pdf (Last visited on 2019/7/1)

58. illinois transportation trade association v. city of chicago thetimes, No. 16-2009 (7th Cir. 2016), available at：http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2016%2FD10-07%2FC%3A16-2009%3AJ%3APosner%3Aaut%3AT%3AfnOp%3AN%3A1842508%3AS%3A0 (Last visited on 2019/7/1)

DOI:10.6814/NCCU201901043