

初探區塊鏈之不可竄改特性、 匿名性所衍生的法律問題

呂嘉穎^{*}

摘 要

科技的日新月異對於人類的生活帶來了創新的改變，舉例來說，奠基於區塊鏈技術的數位貨幣，對於傳統交易而言，帶來了不同的思維方式。現今區塊鏈之運用，在規劃、運用上已不限於數位貨幣，而是以更為全面的方式進入人類的生活之中。也由於這種對於未來社會所可能帶來的觀念衝擊，本文試圖從區塊鏈本質及其與現行法規間的矛盾、衝突為分析主軸，亦即以區塊鏈技術層面可能帶來的爭議，做提前性的法律制定及修正建議。

關鍵詞：區塊鏈、不可竄改、匿名性、被遺忘權

^{*} 國立中山大學中國與亞太區域研究所法律組博士候選人；逢甲大學財經法律碩士。本文部分內容發表於國立交通大學科技法律研究所舉辦之「2018 年第二十二屆全國科技法律研討會」，臺北：張榮發基金會，在此特別感謝資策會科技法律研究所顧振豪副所長、東吳大學法學院章忠信教授對本文所提供的意見與指教。另對本文提供修正建議的評審委員們，致上最崇高的謝意，然相關文責仍由作者自負。

投稿日：2018 年 11 月 26 日；採用日：2019 年 5 月 17 日

Cite as: 6 NCTU L. REV., March 2020, at 41.

On Law Problems from Immutability and Anonymity of Blockchain

Jia-Ying Lyu ^{*}

Abstract

Ever-changing technologies bring innovative changes in our life. For example, digital currency based on Blockchain provides a brand new way of transaction. Blockchain now is going to be applied not only on digital currency, but on most aspects of our life. However, it may bring impact on existing norms. The study focuses on analyzing the contradiction between Blockchain and existing laws. That is, the author provides early advices of enactment and amendment of laws to respond possible controversies caused by Blockchain.

Keywords: Blockchain, Incorruptible, Anonymous, Right to Be Forgotten

^{*} Ph.D. Candidate, Institute of China and Asia-Pacific Studies, National Sun Yat-Sen University, Taiwan; LL.M., Graduate Institute of Financial and Economic Law, Feng Chia University, Taiwan.

1. 前言

現今各界對區塊鏈（Blockchain）技術有著極大的興趣，認為該技術之應用必然對於人類的生活型態產生改變，也因為如此，當區塊鏈被嘗試於運用在不同領域的情況下，對其所可能帶來的衝擊，亦須回到其所具有的特性加以思考，並從其可能在實然面上所產生的爭議，以現有法規進行反思，從中探究法律修正及制定新法之可能。

一般民眾對於區塊鏈的瞭解，多半仍將其視為數位貨幣在交易上的一種「工具」，但論其本質卻仍能發現，所謂的數位貨幣之產生，就中本聰（Satoshi Nakamoto）提出的概念而言¹，應將其視為區塊鏈的其中一種應用方式。也就是說，在思考上數位貨幣是藉由區塊鏈之不可竄改（incorruptible）、匿名性（anonymous）、去中心化（decentralize）等特徵，為了降低交易成本及提供使用上的便捷性，所利用的一種增進效能的技術²。

由此可知，前文所提之區塊鏈特性，事實上有著不同的運用可能，如以食品履歷追蹤困難作為前提，利用區塊鏈技術將相關資訊予以整合並提供產銷、購買者等對象一種資料溯源的系統建立³。又或者是將區塊鏈結合公司治理⁴、物聯網等⁵，形成一種「被信任」的資料記錄模式。

申言之，前文所提之應用可能，多半皆以區塊鏈特性作為主要考量，透

¹ 文中所述之「中本聰」，迄今並未被確認為真實存在的人物或團隊，然揆諸相關文獻、報導，都將其視為該技術概念的「提出者」，故本文仍以該名稱論之。

² 宋俊賢、林安邦、董澤平，「虛擬貨幣於電子商務之發展及其法律上之衝擊：以比特幣為討論中心」，電子商務研究，第12卷第2期，頁239-240（2014）。

³ 陳立群，「區塊鏈在食品履歷追溯追蹤的應用」，電工通訊季刊，2018年第2季，頁5-7（2018）。

⁴ 葉銀華，「治理科技：區塊鏈與公司治理」，會計研究月刊，第379期，頁20-22（2017）。

⁵ 蕭宇程，「IOTA：為物聯網量身打造的新一代區塊鏈技術」，電工通訊季刊，2018年第2季，頁17-20（2018）。

過技術的應用，使人們的生活能夠呈現更加便捷、安全的資料儲存態樣。現今學界多數針對區塊鏈的研究，是以數位貨幣在法律上的性質作為主要論述基礎，在數位數據與實體價值之間進行分析與研究。本文並不以此作為後續爭點探微，而是從區塊鏈的特性著手，論此「被信任」的資料記錄模式，在技術使用上所可能產生的爭議進行分析，思考現行法規對區塊鏈所生問題無法解決之處為何，並試圖提出對策及相關因應措施。囿於篇幅限制，本文僅針對區塊鏈技術層面下的不可竄改特性及匿名性所可能衍生的法律問題做出闡述，雖仍受限區塊鏈迄今的運用普及性，而僅能以數位貨幣作為比較思考的對象，但並不以其作為論述的主軸，僅從技術與規範的交相配合進行討論。同時由於該技術在運用上雖有前景規劃，但實際應用所生之案例仍為少數，故本文亦儘量以現有之案例或可能產生之爭議，加以分析討論，並將區塊鏈技術於其中所可能造成的衝擊進行法律層面的判斷。

當科技發展的速度越來越快，影響人們生活的層面也越來越廣，在此情況下，法律規範的修正與對人們權利的保護，確實應該與時俱進並不斷思考。故本文首段針對區塊鏈技術層面簡單論述，試圖對其以一種概念性的技術闡述方式提供讀者相關資訊。次段則以區塊鏈的不可竄改特性、匿名性，所可能帶來的爭議提出問題做引子，參段則從我國現行法規在適用上所面臨到的難處分析之，末段則提出個人建議及結語。

期能藉由此文之淺論，對未來科技與法律跨領域思考上有著微小的貢獻，並在區塊鏈技術於應用上，能提供一種「提前性」預防可能，無論是針對法律在規範上的正當性、比例原則思考，或是從科學技術方面藉此思考相關爭議產生的可能原因，都留待更多的學者專家從不同角度彼此配合、研究，並思考如何對於人類生活有著更有效率卻不造成更多限制上的爭議之可能性。

2. 簡述區塊鏈技術

在現今科技發展極為迅速的現代化社會中，常可看到科學技術的創新與

舊有法律及生活習慣間，所產生「既可能有所衝突，又囿於促進便利性之衝突而無法放棄」的情況產生⁶，也因為如此，法規範的修訂若仍受限於立法程序時程的遲延，對於人們來說，不僅是所擁有的權利可能受到科技的創新而侵害，更甚者則對科技的發展，可能產生重大的阻礙結果。

因為這種情況迄今仍屢見不鮮，且在法律學界越來越重視跨領域思考的同時，加上現今研究者對於數位貨幣之研究顯有成效，故本文試圖將研究範圍延伸至區塊鏈的本質面進行剖析，一方面試圖從技術上推測可能產生的法律問題，二方面希冀就此文提出未來區域鏈在生活各層面應用所可能產生的問題，並加以提出概略性規範加以解決。然避免本文流於技術報告之模式，故在區塊鏈技術層面的介紹上，僅以較為簡潔、明確的方式，以圖表搭配文字簡介之，詳細的技術思考則留待更多學者專家跨領域的配合、研究。

區塊鏈的生成是為了解決如圖 1 所示的中心化（centralization）所帶來的可操控性，便如圖 2 般讓每個區塊都能夠脫離中心機制而獨立運作，且使得各個區塊的共享性增加，並藉由不同節點運作的方式，使其節點自我運算、驗證真偽，並將資訊傳遞而共同管理，而這也是區塊鏈「去中心化」（decentralization）的特點⁷。同時由於各節點運作的時間、資源有所不同，當其中一項資訊受到不同節點運算並獲得認證下，該交易訊息便能夠被認可。也就是說在運算時間不一的情況下，若能以較少的時間運算並獲得認可，以達成多方共同維護的目標，便能成立該筆交易，而這種運算方式則稱為工作量證明（Proof of Work, POW）^{8、9}。

⁶ 例如共享經濟下是否所有的「物」都能予以共享？又或者是人臉辨識系統是否侵犯了個人隱私權？以及涉及更多層面爭議情況，如基因資料庫、複製物種等，都使得法規範面臨了對於科技開放與否的矛盾。更遑論 AI 人工智慧的誕生，對於未來人類生活及法律規範所產生的衝擊及影響。

⁷ Michael Crosby et al., *Blockchain Technology: Beyond Bitcoin*, 2 APPLIED INNOVATION 6, 8-9 (2016).

⁸ Iuon-Chang Lin & Tzu-Chun Liao, *A Survey of Blockchain Security Issues and Challenges*, 19(5) INT'L J. NETWORK SEC. 653, 654 (2017).

⁹ 現今技術除 POW 之外，亦有其他的運算方式（或稱為共識機制），如 POS（Proof

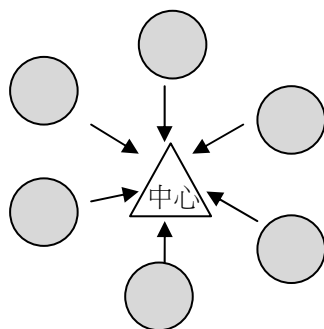


圖 1 中心化示意圖

資料來源：作者自繪。

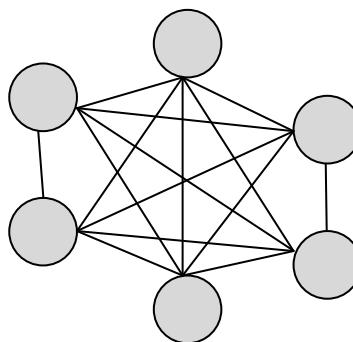


圖 2 去中心化示意圖

資料來源：作者自繪。

然而，這種運算機制常會受到質疑，認為在公開、透明且人人都能更改的機制下，所謂的安全性、私密性是否亦不見於其中？區塊鏈中的數據是透明的，但較為隱私的交易內容則相對性的被加密，也就是說任何人都能透過區塊鏈技術匿名「寫入」區塊，但卻無法恣意竄改之，因其區塊的產生是受到不同節點運算並認證且存入的結果¹⁰。

如果將區塊鏈中的各個獨立區塊解構如圖 3 所示，可以發現每個交易所

of stake，權益證明）、DPOS（Delegated Proof of Stake，股權授權證明）、POOL（驗證池）等，然此較屬技術方面之探究，囿於篇幅限制僅以最初的運算方式作為代表。

¹⁰ 如果從技術角度論之，由於區塊鏈的密碼機制為單向不可逆，也就是我們僅能將資料寫入區塊中，並無法隨意的將其回推至原本寫入的資料，而此項技術較偏向科學的運算過程，亦即默克爾（Merkle）樹結構與雜湊值的關係。於此簡述所謂的默克爾樹結構與雜湊值，簡單來說，所謂雜湊值便是以演算法針對內容進行特徵化，也就是透過其單向輸出不可逆的特性，將同一內容的資料做重複性輸出藉以檢核是否受到竄改，而此一技術並非如同加密（Encryption）般，能夠反向逆推回原本之內容，兩者有著甚大的不同。至於默克爾樹結構，則可將其視為存儲雜湊值的一個具分岔的結構，從其多層級特性與雜湊值配合，形成一種保證資訊不被竄改的方式。然而，兩者與本文撰寫之重點偏離較遠，故於此不多做詳述。

形成的區塊中，各有各的時間戳¹¹，代表了不同時間訊息所建立的資訊，同時由於雜湊值（Hash Value）的形成，加強了各區塊不被竄改的強度，並藉此與下一個區塊產生連結。

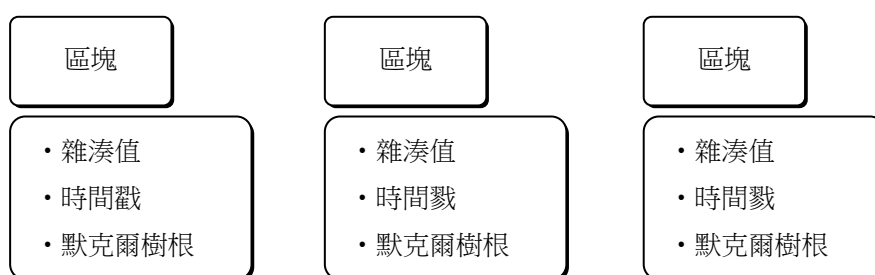


圖 3 區塊鏈的形成

資料來源：作者自繪。

若以現行比特幣交易模式論之，則可以發現區塊鏈在交易的穩定上，由於去中心化及不可竄改兩大特性的加持，導致其數位貨幣的價值性逐漸受到重視。但從技術上來看，因價值性的考量及寫入的必然性，必須有一定的機制使其能呈現所謂的能夠「寫入」但「不被竄改」，而這也是區塊鏈中公鑰與私鑰運用的機制，如圖 4 所示。

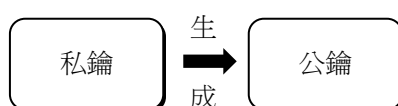


圖 4 公鑰的生成方式

資料來源：作者自繪。

¹¹ Scott J. Shackelford & Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*, 19 YALE J.L. & TECH. 334, 336-42 (2017).

所謂的公鑰與私鑰，其實就是不對稱加密方式。個人所屬的私鑰具有一定的隱私性，是用來寫入（加密）或驗證的鑰匙，每個人所擁有的私鑰都不相同，並能藉由私鑰的產生而生成一組能夠讓所有人知悉的「公鑰」（位址），而比特幣的交易便是基於此項技術獲得交易驗證。舉例來說，吾輩可將公鑰視為現實世界的帳戶，私鑰則為個人簽名。當買方欲進行一筆交易時，透過私鑰對交易進行簽名，並發送給賣方，賣方則透過帳戶與簽名進行匹配，匹配成功則代表該交易為本人所確認的。若完成此項交易，則便會形成如圖 5 的區塊，也就是一筆交易形成一個特定的區塊並使其眾所周知，若區塊逐漸形成連結，區塊鏈便因此而產生。

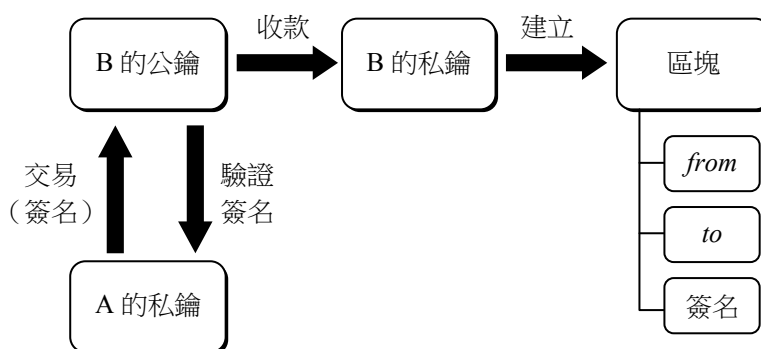


圖 5 公鑰與私鑰生成區塊的方式

資料來源：作者自繪。

當然區塊鏈的應用絕不僅限於此，至今限於技術發展的考量，仍著重在數位貨幣身上，且區塊鏈的形式仍有公有鏈、私有鏈、聯盟鏈等不同類型。綜上所述，現今研究仍以區塊鏈 1.0（數位貨幣）為主。但若將其技術特性宏觀論之，則可以發現區塊鏈所可能造成社會、生活的影響¹²，則是在其帳本

¹² Jong-Hyouk Lee & Marc Pilkington, *How the Blockchain Revolution Will Reshape the Consumer Electronics Industry*, 6(3) IEEE CONSUMER ELEC. MAG. 19, 19 (2017).

式的記憶功能，也就是後續區塊鏈 2.0（智能合約，Smart Contract）¹³、3.0（產業應用）¹⁴所衍生的資料儲存問題與現行生活產生的可能性影響。

另一種區塊鏈的特性則是所謂的匿名性，此處所稱之「匿名」並非是完全的匿名（anonymous），而是以一種防止個人資料與紀錄內容互相掛勾（pseudonymous）的方式，讓其他使用者在資料紀錄公開的框架下，卻無法從中明確瞭解到資訊寫錄者的相關資訊。亦即在技術層面上，各個區塊的節點在訊息傳輸上，可以匿名方式進行而不需要公開，但寫錄內容卻仍得查詢。舉例而言，當每個使用者藉由自己的私鑰與公鑰運算般配，得以將資料寫入並形成區塊，對外界而言會呈現出有這項資料（區塊）存在，但因系統僅能追溯回其公鑰、私鑰般配之結果，而無法針對寫錄者在現實世界中的資訊予以追查¹⁵。

也因為區塊鏈技術在應用上，仍有極大的差異及可能受到未來科技演進產生的歧異之處，為求論述有所本，故後段僅以現行法規範在面對到區塊鏈

¹³ 現行智能合約在區塊鏈上的應用仍屬規劃階段，在思考仍多以現有存在的系統，加上區塊鏈技術的初期實踐為主，舉例來說像金融衍伸方面的應用，如那斯達克的私募證券的交易平台（Pre-IPO）。陳恭、蕭婕，「運用區塊鏈打造公共治理新局面」，國土及公共治理季刊，第 6 卷第 4 期，頁 56-58（2018）；Brett Scott, *Blockchain Technology for Reputation Scoring of Financial Actors*, FINANCE & BIEN COMMUN / COMMON GOOD N 42&43 – ETHICS IN FINANCE, SENSE OF URGENCY / LE SENS DE L'URGENCE – NOMINATED ESSAYS, THE ROBIN COSGROVE PRIZE 2014/2015 – 2015 128, 128-139 (2015).

¹⁴ 其特性效用確實能夠帶給現有產業一種改變式的思考，如綠能、碳交易或藝術、人文、政府治理等。周濟群，「改變世界的未來科技——『區塊鏈』的創新應用領域」，會計研究月刊，第 373 期，頁 42-47（2016）；Alessandra Pieroni et al., *Smarter City: Smart Energy Grid Based on Blockchain Technology*, 8(1) IJASEIT 298, 301-03 (2018).

¹⁵ 特別是在每項資料寫入，都是為公鑰與私鑰彼此匹配的一個「行為」時，對區塊鏈使用者而言，有大的可能同時擁有多個公、私鑰，在一個「行為」結束後所形成的區塊，對外界而言僅能瞭解這個行為所產生的區塊確實存在，但在多個區塊並存的情況下，現實世界的個人資訊被追查的可能性相較為低，也就是說僅能查知公私鑰的行為產生，卻無法明白知道私鑰持有者是誰。

不可竄改、匿名性所可能產生的爭議，做出預先的思考及分析，期許能就衍生的法律問題做規範性的論述。然因目前科技發展並未有相關案例可供證明此項爭議是否會發生，因此仍須藉由部分邏輯性的思考作為輔佐，藉此思考法律該如何加以因應。

3. 論不可竄改、匿名性所可能產生的爭議

在此段敘述開始之前，首先須就其所可能產生的「爭議」區分，通念上所謂的違「法」，多以其行為違反現行法律規範，而所依其生之懲處與限制，也就是說當在行為所造成他人的權利、利益受損，法律則於其後介入令行為人予以補償¹⁶。另從圖 6 中可知，區塊鏈所可能產生的爭議（或論其是否成罪），事實上亦非單一行為能夠論述，而是必須將其行為拆分，而分論在不同過程中所產生的罪責，亦如行政罰法第 25 條中，針對不同行為所違反之法律義務分別處罰的態樣，從行為本身做出探討¹⁷。

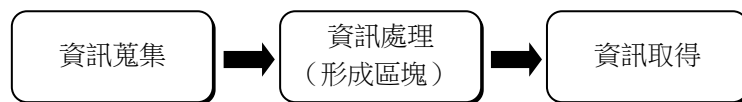


圖 6 資訊形成區塊及利用的過程

資料來源：作者自繪。

¹⁶ 亦如刑法三階論（Dreistufentheorie）中，從構成要件該當、違法性、罪責做出是否成立犯罪的判斷，也就是說在犯罪判斷的基礎上，是具有層次性的邏輯思考，對於該行為是否成立犯罪，仍需以一種較為審慎的態樣，從不同角度加以探討，而非單純的認為論斷該行為是否成罪。

¹⁷ 對於行為數的判斷，學界與實務上都有其論證方式，對於判斷依據多以行為人的意思為主要考量，類似情況亦見於刑法之中，本文亦採此類觀點，認為取得、處理、發送應屬三行為，而不能以單一行為視之。該行為數的判斷與本文主旨關連較遠，故以註腳解釋。相關論述請參：羅天綱，「行政罰上行為數的判斷——兼評最高行政法院 100 年 5 月份第 2 次庭長法官聯席會議決議」，法令月刊，第 63 卷第 12 期，頁 50-59（2012）。

也就是說，圖 6 所示在資訊傳遞過程中，違法行為與區塊鏈所產生的連帶性影響，其實是能夠分成「前段」（資訊蒐集）、「中段」（資訊處理）、「後段」（資訊取得）三個不同的行為。在此必須強調之處在於，此處名詞之使用，是從其技術層面加以描寫，而非於不同應用階段所衍伸的名詞差異性。舉例來說，對於區塊鏈於數位貨幣的運用上，資訊蒐集的部分為以現實資產購買（轉換）為數位貨幣（或以礦工挖礦方式消耗電力、時間），而資訊處理則是形成區塊鏈之中的過程（運算機制），而資訊取得則為將數位貨幣再次轉換回法定貨幣（或貨品）的型態。

再現行法律對本文所述之「前段」、「後段」行為，如生違法可能，仍有其相關法律規範可適用，例如於「前段」資訊蒐集上，若資訊蒐集手段違法，本就屬於法律所不許之行為，故其違法性應無以置喙，如證人保護法第 16 條中，針對公務員洩漏或交付相關保密證人之資訊即為例證。又或者是「後段」資訊取得後所生之行為，如透過網路論壇取得相關性交易資訊及性行為所衍生的違法事由，所觸犯的刑法第 231 條、社會維護法第 80 條等犯責。若從數位貨幣的角度觀之，後段所生之爭議，政府仍有相關的介入（因應）方式¹⁸，故本文並不對前、後段行為予以討論，而是將重點論述放在「中段」上，亦即以技術層面所可能與我國現行法規衝突的情況，試圖探討並分析之。

3.1 不可竄改特性

對區塊鏈而言，由於雜湊演算法的特性，對資料的正確度來說，有著必然的影響力，也因為這種資料紀錄具有極高正確程度，所以被視為區塊鏈在應用上能夠被肯定的其中一項原因。然而，為了維持這種正確度，不可竄改的特性亦為其中所必須存在的要件之一，原因在於當資料被驗證並寫入區塊後¹⁹，所形成的區塊會與下一個區塊鏈結起來，亦即將此資料內含至下一個

¹⁸ 如洗錢防制法之於區塊鏈。宋俊賢、林安邦、董澤平，前揭註 2，頁 244-245。

¹⁹ 透過 Hashcash 演算法以一對一的函數確保資料不被竄改，但從其中卻能發現資料寫

區塊之中，因此在區塊鏈系統中，便能發現此類可供驗證的區塊，事實上是經過非常多次的區塊疊加所形成的區塊鏈。

然而，這種區塊鏈的不可竄改特性仍可能產生不少爭議，舉例如下：

3.1.1 被遺忘權（right to be forgotten）難以行使

被遺忘權為歐洲法院認為當事人具有網路個人資料的刪除請求權，認為搜尋引擎業者（Google）有其義務對當事人之要求，而刪除相關結果呈現於搜尋引擎的情況²⁰，亦被媒體簡稱為「被遺忘權」。由於該判決所延伸的法學思考實屬廣泛，且理應另開他文做較完整的陳述，為避免在論述上有所疏漏，故本文僅以判決之中心意旨，亦即為「人們具有就特定資訊要求資料儲存者刪除的權利」談起²¹。

前幾年全球反對性侵暴力的「我也是」（#Metoo）運動從歐美拓展至全世界，當時北京大學學生在網路上以一篇文章，控訴時任南京大學（控訴時於北京大學任教）教授，以權勢威逼女學生性侵並造成該生自殺身亡的憾事，該消息一傳出，北大校方便試圖壓制這種聲浪，並以屏蔽的方式讓這項消息被封鎖。然而，當時的網路使用者為了跨越這種「限制」，透過區塊鏈的不可竄改特性，藉由儲存於以太坊（Ethereum）之中，避免了中國大陸政府（或學校）對該消息的封鎖，進而散布到世界各個角落²²。

入的軌跡。因此項技術過於偏數學演算概念，故於此處忽略僅以文字做表示。

²⁰ Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 49 U.C. DAVIS L. REV. 1017, 1030-42 (2015).

²¹ 相關文獻可參：張志偉，「記憶或遺忘，抑或相忘於網路——從歐洲法院被遺忘權判決，檢視資訊時代下的個人資料保護」，政大法學評論，第 148 期，頁 11-17（2017）；楊柏宏、陳鈺雄，「被遺忘權之研析——以歐盟法院 Google Spain SL 案及歐盟個資保護規章為中心」，萬國法律，第 208 期，頁 99-104（2016）。

²² 陳瑞霖，突破封鎖，以太坊交易紀錄傳播中國高校#MeToo 異議事件，2018 年 4 月 24 日，科技新報：<https://technews.tw/2018/04/24/break-censorship-someone-use-ethereum-transaction-recording-me-too-event-in-china-university/>（最後點閱時間：2020 年 2 月 25 日）。

另一方面，臺灣臺北地方法院 104 年度訴更一字第 31 號民事判決中，原告亦對 Google 主張被遺忘權之行使，要求 Google 刪除有關原告更名以前，相關可能侵害其權益之搜尋結果，雖後續法院判決仍不予採納其意見，但亦能從中看出此種資料存續所造成之影響。

綜上所述，區塊鏈的不可竄改特性，事實上是與被遺忘權有所衝突的，雖這種資料存續的概念，由上述兩例可知，並不見得有著絕對性的好壞，但不可諱言的是，當區塊鏈以此特性將資料寫錄形成區塊後，似乎儼然形成了另一種不可避免的保存資訊卻不可刪除的型態。

如再將所可能儲存的資料內容，以較不受社會公序良俗所接受的情況，但事實上卻存在於生活之中的角度思考，這種不可竄改性所造成的影響，似乎較上述兩例來的更為直接卻也更不可被接受。

舉例來說，現今世界各國對於兒童性虐、性交相關的圖片，皆採最嚴格審查、追蹤的方式，進行相關的限制及規範。但若有心人士將其儲存於區塊之中，並藉此加以散布、轉傳²³，在無中心化的管理之下，該檔案並無法刪除及銷毀之。再者，若以現今臉書社團或不倒翁（Tumbler）為例，當使用者上傳了有關於不特定第三人的自拍裸照、恐怖主義宣傳影片等資訊，仍可藉由中心化的方式試圖屏蔽或刪除該項訊息，但在區塊鏈中，由於其不可竄改、去中心化的特性，所導致的訊息存續，可能對於不雅照被上傳者、不特定第三人產生永續性的影響。

因此，所謂的被遺忘權在未來區塊鏈被大量運用的社會中，似乎已有適用上的困難，然於此必須再次強調，此種情況雖可能藉由前文所提之「前段」、「後段」等方式加以預防或要求資料上傳者受法律制裁，但本文仍以資料儲存的不可竄改為重點，其餘部分並不多做涉入。

申言之，針對於資料寫錄而言，確實無法輕易的界定這種不可竄改特性

²³ 黃彥鈞，比特幣區塊鏈存有虐童內容，害礦工也被當變態？，2018 年 3 月 26 日，科技新報：<http://technews.tw/2018/03/26/child-abuse-image-in-bitcoin-blockchain/>（最後點閱時間：2020 年 2 月 25 日）。

的好或是壞，但對於區塊鏈來說，也是因為不可竄改性，使其在紀錄上相較於可被竄改的其他系統而言，有著更被人所信任的價值存在。然而，當被遺忘權是可取捨的時候，這種所謂的「信任」是否可能被有心人士利用，進而造成特定情況下，信譽、名聲之受損，又或者如後文所討論的，在無法判斷訊息正確性為前提，所謂的「虛假訊息」將產生人們權益上的受損？

3.1.2 訊息正確性

除前述所言，資料可能在區塊鏈之中發生欲刪除但不得刪除的窘境，另一種思考模式則是針對不可竄改特性下，提供之訊息是否可能產生影響展開相關論述。同圖 6 所示，對於區塊鏈形成而言，除「中段」進入「後段」期間，所可能產生的資料不可竄改（不可刪除）所衍發之爭議外，另一個面向則是從「前段」進入「中段」，對於訊息提供可能發生之爭議。

理論上來說，前文所述之訊息審查亦可視為監管態樣的一種，也就是透過事前對於訊息的形式，加以預防性的不使其進入系統當中。當然這種模式也並非百分百的預防措施，但在可於事後修改、刪除的情形底下，此類訊息仍可藉後續的機制予以刪除相關資訊。

然回歸訊息正確性論之，區塊鏈僅能就資訊處理的期間（亦即寫入過程中）擔保其不受第三方竄改之影響可能降至最低²⁴，但卻無法針對訊息的來源加以驗證、審核。再者，這種不受第三方竄改的可能機率，卻同時也無法避免有心人士加以修改，如 51%攻擊²⁵。雖然這種攻擊需耗費代價極高，但

²⁴ Zibin Zheng et al., *Blockchain Challenges and Opportunities: A Survey*, 14(4) INT. J. WEB AND GRID SERVICES 352, 367-69 (2018).

²⁵ 由於51%攻擊較屬技術層面的思考，本文於此簡單敘述其工作原理。區塊生成的情形為公私鑰間的配合，當一項資訊被寫錄時，公鑰與私鑰生成的區塊將會等待其他使用者（如數位貨幣的礦工）確認。最初確認的使用者，便將其運算完的區塊告知其餘使用者，並等待驗證與檢核，此亦為使用者間的共識（consensus）。然而，若寫錄的私鑰持有者在他人運算時，試圖以另一支的區塊鏈進行運算，當該區塊鏈未如實廣播的情況下，與另一有共識的區塊鏈便產生了分支。也就是說，同一筆資料寫錄在不同區塊鏈之中，很可能會產生了雙重認證（或雙花攻擊，double-spend at-

卻也說明了如果耗費的代價小於所可能得到的利益時，確實有其使用的機率存在²⁶。

因此，當區塊鏈有著前段所述之不可竄改特性時，訊息的正確性可能影響了相關利害關係人的權利。舉例來說，如近年來政府部門不斷強調假新聞所造成社會動盪的影響²⁷，在訊息來源廣而雜亂的現代化社會中，不時可見媒體在發布新聞之後，經後續相關驗證發現該消息與現實有所出入，而第一時間將該新聞「下架」。但在區塊鏈中，這種下架的可能性受限於前文所述之不可竄改特性，如此類消息透過其他使用者在不清楚狀況的情形之下，皆對該區塊有所共識並且上鏈。那麼對當事人所形塑出的不實報導（資訊），卻可能造成一輩子的負擔。

另一方面，區塊鏈運用的其他形式也可能產生相同的問題，如農產品產銷履歷在區塊鏈適用上，透過其形塑的不可竄改性，確實能夠提供消費者在

tack) 的情況。接下來該使用者只要盡力的將所塑造的區塊鏈長度，超越原本正常寫錄的區塊鏈，並在第一時間予以廣播，使其符合區塊鏈的規則性，在驗證並無問題的情況下，該筆資料便產生了處理的空間，也就是原本資料寫錄與所塑造區塊鏈之間的重複性，當塑造的區塊鏈被驗證後，原先區塊鏈的資料寫錄便不存在。該使用者只要試圖將資料在其他使用者上鏈之前，再次以其他方式寫錄其他區塊鏈之中，便能有著51%攻擊的效果存在。若以更簡略的方式說明，則可視為單一使用者在區塊鏈之中的運算能力大於總和的一半，則其便能以一己之力決定資料寫錄的成功與否，甚至變更內容。Dmitry Efanov & Pavel Roschin, *The All-Pervasiveness of the Blockchain Technology*, 123 *PROCEDIA COMPUTER SCI.* 116, 119 (2018); Jin Ho Park & Jong Hyuk Park, *Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions*, 9(8) *SYMMETRY* 164, 171-75 (2017).

²⁶ Zhiyong Li, *Will Blockchain Change the Audit*, 16(6) *CHINA-USA BUS. REV.* 294, 296 (2017); Richard Dennis & Gareth Owen, *Rep on the Block: A Next Generation Reputation System Based on the Blockchain*, in 10TH INTERNATIONAL CONFERENCE FOR INTERNET TECHNOLOGY AND SECURED TRANSACTIONS 131, 133 (2015).

²⁷ Hunt Allcott & Matthew Gentzkow, *Social Media and Fake News in the 2016 Election*, 31(2) *J. ECON. PERSP.* 211, 219 (2017).

食用上有著更佳的保障措施²⁸。然而，如提供農產履歷的供給者、訊息輸入機關惡意以假資訊魚目混珠，試圖蒙騙消費者，又或者是輸入資訊者一時不察，將相關資訊輸入錯誤。在區塊鏈僅能就輸入資訊予以形成區塊，並且上鏈的情況底下，所衍生之錯誤又該如何歸（究）責？

同樣的從儲存的資料寫錄來看，如發生錯誤所造成的影響可能令其人格及相關權益受損論起。例如，於區塊鏈與醫療數據平臺之間，訊息的正確性對於病患、醫師而言極為重要，當然所儲存的資料同樣的亦不希望其外流。區塊鏈技術對於醫療數據平臺而言，有著極大的安全性、保護性²⁹，但在這種情況底下，區塊鏈的原生不可竄改特性，事實上也讓醫療系統的資料輸入者必須抱持著更為戒慎恐懼的態度。試想，原先系統對於患者病歷資料儲存，有著能夠修正的可能性存在，但當這種資訊儲存在區塊鏈之中，如原先並未罹患特殊隱疾的患者，因醫生或相關資料處理人員之疏失，將其輸入資訊錯誤，而使該患者成為了罹患特殊隱疾的病患，當該筆資料被驗證且上鏈後，此項訊息對於患者及其家屬又會造成多大的影響？特別是部分迄今仍受社會誤解的疾病，當上鏈後如生外流可能，縱然後續試圖修正，但在不可竄改特性底下，證明該項資訊之謬誤可能，便顯得極為困難與不受民眾信任。

3.2 匿名性

除在公有鏈上，每個使用者都屬於匿名的，在此情況下，因區塊鏈的匿名性特點，極難追查到各個使用者與現實身分之間的連結，也因為如此，目前世界各國政府在甚難以技術層面突破該限制的情況下，所採取的方式則為透過前文所述的對「前段」、「後段」的進出加以控管，如比特幣轉出或轉入法定貨幣時，透過與現實銀行的合作，從中杜絕欲透過此項技術進行非法

²⁸ Jing Hua et al., *Blockchain Based Provenance for Agricultural Products: A Distributed Platform with Duplicated and Shared Bookkeeping*, in 2018 IEEE INTELLIGENT VEHICLES SYMPOSIUM (IV) 97, 98-100 (2018).

²⁹ Huawei Zhao et al., *Efficient Key Management Scheme for Health Blockchain*, 3(2) CAAI TRANSACTIONS ON INTELLIGENCE TECH. 114, 115-16 (2018).

活動的用戶。雖然如此，所謂的匿名性並不代表所有的寫錄內容都是被隱藏的³⁰，在區塊鏈之中，資料寫錄過程與來源都會被記載區塊之中，亦可供任何人查詢。但此種狀況，卻能藉由同時掌握不同的私鑰加以避免，也就是當某一人士以不同的私鑰寫錄資料於區塊之中，對於資料來源與現實身分之連結，有著更具效率的匿名效果。

但這種匿名性的特點，卻也使其產生了爭議，如將其運用於須身分驗證的現實情況之中，如投票³¹、各種資訊寫錄等，都可能受到不特定人士以金錢、權勢等方式，迫使實際具有使用權（私鑰）的使用者，提供所擁有之私鑰寫錄於區塊之中³²。在這種情況下，所謂的資料寫錄亦產生了如前所述，並無法確認其真實性的結果，或可能產生與原先私鑰擁有者，於寫錄上有著不同意欲的情況³³。雖然這屬於前文對「前段」介入的預防，但從「中段」

³⁰ 亦有論者將其視為匿名公開（Public Anonymous）或論其為假名（Pseudonymity），然本文為求前後文連貫，亦將其視為匿名性。Harry Halpin & Marta Piekarska, *Introduction to Security & Privacy on the Blockchain*, in 2017 IEEE EUROPEAN SYMPOSIUM ON SECURITY & PRIVACY WORKSHOPS 1, 1-3 (2017).

³¹ Patrick McCorry, Siamak F. Shahandashti & Feng Ho, *A Smart Contract for Boardroom Voting with Maximum Voter Privacy*, in FINANCIAL CRYPTOGRAPHY & DATA SECURITY 357, 363-64 (Aggelos Kiayias ed., 2017).

³² Simon Dyson, William J. Buchanan & Liam Bell, *The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime*, 1(2) JBBA 5997, 5997-6000 (2018).

³³ 舉例來說，LegalThings 透過私有鏈的架構，開發了 LegalFling（應用程式），並以性自主權為考量，藉由雙方都同意的情況下，將性行為的同意狀態、內容作為區塊鏈的保存內容，並試圖將其後續若雙方產生訴訟時所提供的證據。雖然這項行為牽涉層面過於廣泛，且並非所有行為都屬於本文所欲探討的內容。然以一個案例作為思考或許亦能解釋本文文中註釋之情形，若 A 與 B 藉該應用程式彼此合意發生性行為，但行為結束後卻發現是 C 使用了 B 的私鑰與 A 進行性行為，而後 C 控告 A 違反了當事人意願發生性行為，雖有合約證明但性行為雙方卻非合約簽訂的當事人，且於現實生活中並無法知悉是 C 使用 B 的私鑰時，那麼所生之法律爭議事實上是非常複雜的。黃彥鈞，LegalThings 把所有約定都搬上區塊鏈，從約炮到商業契約無所不包，2018 年 8 月 6 日，科技新報：<https://technews.tw/2018/08/06/legalthings-change-contract-by-blockchain/>（最後點閱時間：2020 年 2 月 25 日）。

所產生的影響論之，卻也能發現當交易雙方在現實層面所生之資訊不對等，很可能導致這種資料的寫錄於技術中是合法、合理的存在，但實際上操作的正確性卻是可能受到質疑的。

另一方面，前段所論之資料正確性，事實上也與匿名特性息息相關，當這種訊息的提供在區塊鏈中，個人資訊是相對「被隱藏」的，那麼對於訊息的發布而言，如以偏激、不實之言論發表相關資訊並被寫入區塊中，那麼這種資訊在不可被竄改的情況下，勢必會對個人、政府等相對人造成影響。

舉例來說，刑法第 309 條公然侮辱罪、第 310 條誹謗罪，對兩者於社會新聞版面上出現的頻率，應使民眾對其並不感到陌生。如臺灣高等法院 107 年度上易字第 2143 號刑事判決中，在臉書散布文字毀損他人名譽，在雙方皆能確定行為人與被害人之身分的時候，對於犯罪對象之逮捕亦能採較為簡單的方式，甚或於審判之中，相關犯罪事證之獲取，也得以透過特定機關之提供，在確認犯罪事實與行為人之間的關連性後，予以論罪處刑自不待言。然而，無論是公然侮辱或誹謗，在行為與受害者皆被確認的情況下，若透過區塊鏈對該言論寫錄其中，並讓其他使用者皆能得知該項訊息的情況下，應成立其罪並無疑義。然而，該如何證明該行為與行為者之間的連結，更甚者尋找到此類行為人，在其匿名性的保護之下，若如前所述並無區塊鏈私鑰與現實法定身分並無關連性，那麼是否將造成這種不實言論透過前述之不可竄改性持續存在，並且對受害者有著長遠性的影響，又無法迫使加害者進行補償或懲罰？

匿名性受重視之原因在於對於隱私的保護，但對於區塊鏈而言，這種「選擇性公開」的思考，確實對於實然面與應然面都造成了影響。雖然在科技上，已有零知識證明（zero-knowledge proofs）可供解決，但該技術的創新與監管面的衝突，卻是仍待解決的一項難題³⁴。

³⁴ 最早使用該技術的 Zcash，受限於成本過高的考量，並無法全面性的使用該技術，再加上該技術屬於晚近發展，人們對其認知並不完全，受制於此本文僅做簡單介紹。所謂零知識證明為，在雙方對於資訊的判斷有著限制性的情況下，亦能加以驗證該資訊的特徵，且不洩漏相關內容。舉例來說，在你無法接近提款機操作為前提，我

雖然從技術面看似能夠加強或解除這種匿名性所帶來的影響，但從數位貨幣中最強調隱私概念的門羅幣（Monero, XMR）來說³⁵，卻為了避免前述 51% 攻擊帶來的改變³⁶，而強行加以硬分叉（hard fork）³⁷，藉由技術層面的提升來防範因此「轉向」中心化造成的匿名性效能減損。

由於區塊鏈技術仍屬發展階段，相對性的爭議解決機制也尚待完善或發展，倘若科技發展便屬動態時，法律規範與時俱進的改變，是絕對需要以前瞻性思考作為法規修正的邏輯架構。然而，這種技術的不可預期性，事實上也帶給吾輩在思考上，必須從跨領域人才彼此配合的角度論起，但在文章敘述、撰寫上，實無力以單篇文章呈現如此包羅萬象、面面俱到的統合性概念，故本文後段試圖限縮其論述架構，從我國現行法規在面對本段所提出

該如何證明我知道地上這張提款卡屬於我呢？當然最簡單的方法，便是找一臺提款機，讓你在距離提款機非常遠的情況下，我操作提款機並輸入密碼，當畫面跳能夠領錢的那個畫面時，請你觀察這個畫面確實是需要密碼才能進入的。那麼，你在沒有得知我密碼的情況下，又能確認我具有這張提款卡的密碼，便能驗證我擁有這張提款卡的使用權。當然，如果同一張提款卡密碼本來就已經讓很多人知道便另當別論，然而此處設定的情況則是單一提款卡僅有一人知曉其密碼。林之晨，區塊鏈的「零知識證明」是什麼東西？，2018 年 11 月 5 日，天下雜誌：<https://www.cw.com.tw/article/article.action?id=5092794>（最後點閱時間：2020 年 2 月 25 日）；Charles Rackoff & Daniel R. Simon, *Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack*, in *ADVANCES IN CRYPTOLOGY-CRYPTO'91*, at 433, 434 (Joan Feigenbaum ed., 1991).

³⁵ Amrit Kumar et al., *A Traceability Analysis of Monero's Blockchain*, in *COMPUTER SECURITY-ESORICS 2017*, at 153, 155 (Simon N. Foley, Dieter Gollmann & Einar Snekkenes eds., 2017).

³⁶ 由於專業礦機的運算力相對於一般以顯示卡為運算的礦機而言，有著更高的效能。假設這種礦機被特定機關、人士大量取得，造成了 51% 的結果，則可能對於該幣種有著價值降低的可能。

³⁷ 相對性的概念則為軟分叉（soft fork），兩者最大差異處在於，硬分叉在分叉點過後所產生的區塊鏈，並不與原先分叉點之前的區塊鏈相容，而軟分叉則反之。*Bitcoin Developer Guide, Consensus Rule Changes*, BITCOIN, <https://bitcoin.org/en/developer-guide#consensus-rulechanges> (last visited Feb. 10, 2019).

的爭議，在不可竄改特性及匿名性作為前提考量之下，於未來適用上所可能面臨的難處分析，並於文末對後續法律規範之修正提出個人建議。

4. 現行法規範適用之難處

對於科技法律而言，相較傳統法學更具有跨領域整合的必要性，雖然近年來法律學界已正視該情況，亦從不同角度對法律與科技間的關連性進行剖析。雖於立法技術上有著不確定法律概念的存在，試圖藉由裁量權及判斷餘地的使用（Margin of appreciation），使其能夠補足現行法規範之不足，然受限於立法程序緩慢及相關跨領域法律人才培養時間冗長，法律對於科技演進的速度，實難以「並行」之方式予以修正³⁸。

故本段將從我國現行法規範出發，以法律對前述之爭議於思考上可能面對的爭議為本，提供個人意見及法律修正之建議。總的來說，區塊鏈在特性上與現實層面所產生的爭議，應能略分成下列幾項觀點做思考。

4.1 被遺忘權與不可竄改特性

除由於被遺忘權屬近來被重視的權利之一，但在各國法律上，卻仍可從相關判決中作為論述之佐證，如以保護人權最力的美國來說，在最高法院相關判決中，也同樣揭橥了對於被遺忘權的未全面肯認³⁹。其中最大之爭議在於被遺忘權如何在隱私權與資訊公開中間取得平衡？且若從名譽權與言論自由論之，也發生了同樣的爭議⁴⁰。

本文主旨並非探討被遺忘權，但從其中法律規範未能完善定義的情況下，區塊鏈若產生相關的矛盾，該從何論之或者是否能以被遺忘權評斷都將是

³⁸ 張智聖，「科技與法律的介面：科技性不確定法律概念『判斷餘地』之研究」，生物產業科技管理叢刊，第5卷第2期，頁87-88（2016）。

³⁹ 顏于嘉，「由美國資訊隱私法制觀察被遺忘權在美國的發展」，萬國法律，第211期，頁30-31（2017）。

⁴⁰ 蕭郁澹，「俄國修正資訊保護法明定保護被遺忘權——被遺忘權的明文化，正考驗網路資訊的文明化」，科技法律透析，第27卷第10期，頁6（2015）。

個極大的問題。也就是說，在層次判斷上應先就被遺忘權有著框架上的思考，從規範上明確定義被遺忘權的構成要件，若區塊鏈中的不可竄改特性，確實違反了此類被定義出來的構成要件，那麼才有後續論罪處刑的可能性產生。

如以我國相關判決來看，臺灣高等法院臺中分院 106 年度上易字第 729 號刑事判決中，亦肯認這種被遺忘權受限於科技日新月異的發展，在現有法律規範上的架構並不完善，如若從臺灣臺北地方法院 104 年度訴更一字第 31 號民事判決論之，則可以發現在我國民法中並沒有針對被遺忘權之規範，且該判決將其定義為「使一般人消極不記憶他人過去，而請求被告刪除網路上與其相關之檢索結果及可據以在網路上搜尋已被公開資料之關鍵字」。另臺灣臺北地方法院 105 年度訴字第 3517 號民事判決亦對法無明文規範抱持同樣看法，並將前述所謂「不記憶他人過去」等詞語，更限縮到「對自己負面、過時之身分資訊要求移除之權利」。且最高法院 106 年度台上字第 2652 號民事判決更認其歐美所述之被遺忘權，事實上是要求搜尋引擎刪除搜尋時的連結與結果，而非對於原存在之事實資料予以刪除。

綜上所述，應能得出被遺忘權要件至少包含了，具負面效果、可供他人檢索資料之連結結果兩大要件，然而，這兩大要件除負面效果在認定上應能較適當判斷之外，所謂的可供他人檢索他人資料之結果，卻可能造成適用上的困難，如在公有鏈之中，這種資料的「透明性」確實能夠符合要件，但在私有鏈之中，如親戚朋友或不特定團體所架設之私有鏈，所謂的可供他人檢索之程度為何，仍易產生爭論。

假設前述判斷都成立的情況下，那麼法規範該如何讓此類資訊「被刪除」？當這種資訊搜尋之結果如前述案例是與服務提供商有關時，司法可藉由相關手段讓這些可能觸及被遺忘權的資訊不再出現。但在區塊鏈不可竄改特性的狀態下，又該如何解決？

本文認為以目前技術層面來看，完全刪除有其困難性存在，但在思考上或許能夠以同樣的方式對此類侵犯權利之行為予以彌補。舉例來說，法規範在思考上除依其他法律就損失之利益、侵犯之權利予以實質補償之外，另可令訊息散布者或同一區塊鏈的使用者，將該判決結果或真實訊息以新區塊生

成的方式，如備註般的使其進入區塊鏈之中。也就形成了虛假事實、不當資訊的區塊會受到後來區塊的建立，而產生一種如同「被要求」刊登於報章雜誌的聲明⁴¹。

然而，這卻會面臨到一個問題，也就是該如何找到所謂的資訊散布者，這項爭議確實有其問題存在，但容本文於其後再一併說明之。假設無法找到資訊散布者，亦能以徵求該區塊鏈其他使用者之方式，藉由獎勵機制使用之方式，讓區塊鏈使用者願意出借其私鑰予以修正，此筆金額之使用並非全然政府付費，而是如果未來技術能夠追查到訊息散布者，或有其他方式證明此項資訊之散布為何人的情況下，可將其視為先行墊付之款項，而讓真正侵犯權利的行為人，於後為其行為加以負責。

4.2 資料正確性

在資料寫錄方面，除前段所敘述的對當事人所生之負面效果外，另一種需要考量的地方則是在於，若登載的資訊非為正確的情況，在其不可竄改特性的影響下，並沒有修正之機會，倘若造成他人權益上的損失，對於當事人而言，同樣有著極大的影響，雖可能以前文補修正之方式做出彌補，但對於相關資源之耗損，卻又有著極大的浪費可能性⁴²。

再者，這種登載（寫錄）誤差所發生的可能性，事實上應遠大於前段行為人針對特定使用者所形成之區塊，原因在於當區塊鏈運用到 2.0、3.0 世代時，代表了使用者從原來 1.0 中的買賣雙方（含礦工），增加到民眾與政府、政府與政府，又或者是金融機關、綠電交易等運用型態，所產生誤差的機率應隨訊息處理量增加而提高。如以醫療系統在病歷登載上所使用之區塊鏈來說，

⁴¹ 常可見被遺忘權與人格權、名譽權之間做連結，但在現行法規範的「缺少」之下，被遺忘權是否被認為是人格權、名譽權確實是受到質疑的，見文中相關判決。然若以所謂回復名譽方式觀之，文中所稱之「覆蓋」手段，亦不失為一種事後補償、修正可行處。相關回復名譽之法規範探究請參：黃茂榮，「回復名譽之適當處分及強制登報道歉的合憲性」，植根雜誌，第 26 卷第 8 期，頁 23-29（2010）。

⁴² 如運算所生之電力、效能耗損等。

假設一位病患在看病完後便會建立一個區塊，一位醫生一天能看 50 個病患，那麼單一醫生一天至少有 50 個區塊產生，當這種數量受到科別、醫生數、病患數量的改變，而有著眾數上的成長時，通念論之，確實能夠發現其登載出錯的機率，遠大於前文單一行為人「攻擊」一位（含以上）使用者之機率。

另一方面，當這種登載誤差所造成的影響，在追溯上同樣相較前段行為人來的較易找到，主要原因則是該區塊鏈使用者屬於「被限制的」，也就是在政府部門登載人員僅屬於公務員、醫院病患履歷登載人員亦有所管控。此類行為人發生了登載誤差，因其身分別、案由之不同，如屬公務員身分可依刑法第 210 條到第 220 條所述加以論罪處刑，但非公務員身分者，因部分條文屬身分犯適用，是否無以適用之？本文認為，由於區塊鏈使用具有不可竄改的特性，在登錄上確實應更加謹慎查核、輸入⁴³，如以僥倖之心態登載，在明知其所造成之影響可能對於當事人產生難以抹滅的爭議時，應得以類推適用刑法第 210 條到第 220 條，但得以於罪責之思考上予以減少其刑，或要求對相關受影響者之利益補償並回復之。

但所謂的誤差「辯證」卻又是另一種需要考量的問題，因此除了顯而易見的登載錯誤之外（如性別外表登載），其餘資料的登載誤差，必須探討之處在於，如何判斷源頭資料的正確性。若當事人所提供的訊息本就有所誤差，在登載上所生之影響是否應由資訊提供者承擔？又或者此訊息雖為資訊提供者提供之錯誤，但因區塊鏈之特性，而使區塊鏈使用者認其資訊正確，而產生後續影響，當事人間的權利義務又該如何歸屬、區分？

如以本文主旨觀之，理應將區塊鏈的資訊運算過程（區塊建立）視為電磁紀錄之一種，亦即若資訊提供者明知、故意提供不實之資訊，因其行為影響了他人之電磁紀錄，且致生他人或公眾之損害者，應能類推適用刑法第 359 條。原因在於區塊鏈若能以前述之方式「覆蓋」不實資訊，在後續修正

⁴³ 此種論述如同公務員在公文書登載時，考量到登載資料會對民眾有著極大的影響及其後果，故於登載時應負實質審查義務。黃茂榮，「2011 年刑事法發展回顧：法律說詞與說詞之外」，臺大法學論叢，第 41 卷特刊，頁 1545-1546（2012）。

（補）手段適用上，必須耗費著更大的時間、金錢（運算機器）等，故所產生的損害確實符合刑法第 359 條後段所述。

當然，此段對於資料正確性的論述，必須以行為人（含資訊提供者）之意與欲作為考量之基礎，也因為探究當事人真意之困難，且非本文所論述之重點，故於分析上僅從相關法規範及可能面臨的爭議做思考，細部探究仍待相關學者專家提供更為縝密之意見。

4.3 實名制與匿名性的衝突

對區塊鏈技術而言，匿名性確實為其特性之一，亦如前述所採取的寫錄過程公開，但不公開使用者資訊，也讓更多的使用者願意相信此項技術的公正性⁴⁴。另一方面，區塊鏈屬於去中心化的一種技術，亦即將中間人（intermediary）的角色去除之，然而，這種去中心化的情況，加上匿名性的考量，事實上仍有極大的問題需要解決。舉例來說，如個人私鑰丟失的情況下，並沒有辦法藉由傳統中心化的思考，提供一個「再獲取」的機會。另一方面，當如前所述需要追查使用者真實資訊時，以現行技術而言，在去中心化的框架下確實難以尋找，而這也加強了匿名性所可能導致犯罪行為適用的不良影響。

如以技術層面為例，現實世界亦發覺此問題並試圖解決，如國際銀行區塊鏈聯盟所發展的琴弦（Corda）平臺，透過隔離權限的方式達到隱私資料的保護，並提取部分區塊成為公證結點予以資料寫錄，除主動性的保密措施之外，另就加密性的概念思考，如公鑰基礎設施（Public Key Infrastructure, PKI）等技術對寫錄內容加密，讓擁有解密鑰的相對人可解密以保障隱私⁴⁵。

⁴⁴ Michael Nofer et al., *Blockchain*, 59(3) BUS. & INFO. SYS. ENGINEERING 183, 184 (2017).

⁴⁵ Richard G. Brown et al., *Corda: An Introduction*, R3-CEV (Aug. 2016), https://pdfs.semanticscholar.org/b100/0a6166b6e221f61f35259dbfab4f4d6df76a.pdf?_ga=2.21545428.8.653812434.1580288912-1951266822.1580288912; Mike Hearn, *Corda: A Distributed Ledger*, CORDA TECHNICAL WHITE PAPER (Nov. 29, 2016), <https://www.corda.net/content/corda-technical-whitepaper.pdf>.

若從其他國家對於區塊鏈匿名性與實名制的衝突論起，在中國大陸所提出的區塊鏈信息服務管理規則草案中，從區塊鏈提供之公司須以申請制設立、司法單位得以對區塊鏈的用戶資料予以調查，並且以實名制（真實姓名、身分）註冊等方式，實際介入並取消了匿名性的特點。此種方式確實對於區塊鏈在監管層面上有著最為直接的效果，但將此匿名性去除之後，等同於將所有資訊更為公開。舉例來說，數位貨幣的帳戶連結、交易資訊，在以往僅有中心化的機構得以檢視特定資訊，如聯徵中心對用戶信用報告之查詢等，然若將所有銀行系統以區塊鏈連結，則相關報告之生成、查詢，儼然變得更加簡單且不受用戶授權與否的限制。

再者，此種方式亦加強了政府對人民之監控，除前文所述之「前段」監管之外，對於本文主旨所討論的「中段」而言，也提供了政府部門「即時性」的犯罪防制可能，但在資料來源不見得正確的情況下，如貿然以區塊鏈生成證明犯罪事實，在比例原則適用上是否又顯得過於獨斷專行？

另一方面，相對於東方的中國大陸，西方世界的歐盟在一般資料保護規則（General Data Protection Regulation, GDPR）執行之後，透過被遺忘權的使用，能將相關資訊（Cookie、IP、生物特徵）等加以隱藏，在這種情況下，似乎區塊鏈的匿名性亦能妥善適用。但是此種作法所產生的問題，似乎可能造成不實言論在網路上可恣意傳播，但不論在技術上、法規範上都很難找到「負責」的對象。換種角度做思考，如 GDPR 強調的必須刪除連結（link）、影印（copies）、複製（replication）⁴⁶，以及資料可攜權（Right to data portability）⁴⁷，對於區塊鏈中的區塊生成而言，似乎有著無法刪除並違反 GDPR 規範的可能性。

雖然兩種模式似乎呈現出兩極化的資料處理思考，但無論從何種角度觀之，都能發現這種思考模式，對於現有科技發展、生活應用都有著無法短期

⁴⁶ Shaniqua Singleton, *Balancing a Right to Be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD*, 44 GEORGIA J. INT'L & COMP. L. 165, 177-78 (2015).

⁴⁷ 資訊於不同服務系統之間的轉移。

改變的問題存在。退萬步言，雖然此種思考模式仍著重在本文所論之「前段」與「後段」之中，但對於「中段」的資訊處理而言，卻帶來了極大的影響，也就是如以監管為主的方式做思考，區塊寫錄的過程中便會產生了犧牲匿名性效益的結果。而若以開放的觀點論之，則可能加強了不可竄改特性所帶來的負面影響，以及前文所述相關資訊寫錄在犯罪行為上應用的難以追查性。故本文並不於此試圖定義我國該以何種方式做政策、法規範的框架，而僅以現行法規範所面對的問題提出修正之建議。

對政府而言，資訊公開本為人民獲得相關資訊之權利，同時避免相關決策行使時，所產生的「黑箱」決策疑慮⁴⁸。相關條文亦見諸於政府資訊公開法之中，也因為如此，透過區塊鏈的使用，確實能讓此種目的有著更透明的實現可能，但細觀其中仍能發現與現行法規範衝突的情況。舉例來說，如同法第 14 條可要求修正，受限於前述之不可竄改性，又該如何接受其要求進而修正？同法第 18 條對於限制公開之資訊，於現行法規範中得依法不公開，若以此為前提，區塊鏈的使用卻是有著部分公開的特性，那麼這種不公開的情況又該如何處理。雖然該法已就前述問題於第 14 條第二項中，如本文所建議之情況，若該資訊無法修改，則以附加之方式做註記，似可作為區塊鏈資料寫錄時一種可供修正的態樣。

除公部門資訊處理、寫錄之外，另從個人資料保護法論起，亦可見其匿名性與法規範的問題。雖然個資法涵蓋了本文在「前段」、「中段」、「後段」的運用保護，但從其處理（「中段」）論之，可以發現第 6 條中所述特定資料不得處理及其但書所示，都能看出若區塊鏈將資料處理時，所可能面臨到的問題所在。如同條第一項中論其法律要求公開之項目，當法律直接要求特定資訊須公開時，如以中國大陸「實名制」區塊鏈的角度思考，將對特定資訊與個人身分呈現「常態性」的公開，而非「特例性」的公開，若從

⁴⁸ 林敬庭、董祥開、連婕妤，「政府資訊公開與個資保護之模糊與歧異：六都政府網站員工聯絡資訊公開程度之比較分析」，民主與治理，第 5 卷第 2 期，頁 5-11（2018）。

GDPR 思考之，此類的資訊公開將與其有著嚴重的衝突性存在。除此之外，亦有其他的規範條文將可能受到影響，如同法第 18 條公務機關必須指派專人辦理安全維護事項，藉此保護個人資訊滅失、竄改云云，但此種「專人」辦理之事項，似乎亦將中心化視為必要條件之一，那麼區塊鏈的適用性便有所爭議。雖然我國在 2018 年 6 月所公布的資通安全管理法，似乎對於資通安全有著更佳的保障，但從同法第 3 條第三項對資通安全的定義中，卻能發現這種所需「授權」的定義過於模糊，如以區塊鏈的使用技術來看，「授權」意指公、私鑰間的「匹配」或是使用者之間的「共識」抑或兩者兼採？當這種資通安全的「情資」，形成區塊鏈並上鏈後，對現實使用者之權益而言，屬於保護或是侵犯，亦難做出明確的論斷。

5. 結語

申言之，本文在探究上受限於技術層面於未來的不可控性及相關法規規範的缺乏，在論述過程中僅能以特殊案例作為分析的依據。當區塊鏈逐漸深入於生活之中，此種特殊案例成為常態發生的可能性則必然提高，試想在手機並未普及的時期，又如何論所謂行動支付所衍生的爭議。但當手機技術推陳出新且逐漸演進之時，似乎當初所被認為可能發生的爭議，迄今已常見於吾輩生活左右。

對於區塊鏈之研究而言，除技術層面的考量外，亦須透過法律專業人才的培養、參與，從可能面對到的問題以多重角度檢視之後，並提出解決之方案，而將此類爭議造成影響的機率性降到最低，對於我國法規與區塊鏈特性（不可竄改、匿名性）之間所產生的矛盾，作者有以下建議提出，待未來技術面完善、跨領域思考建立之後，能以本文之發想為探究之出發點，從技術、法律兩方面通盤性的思考修正之可能。

5.1 區塊鏈的定義：電磁紀錄

在性質上，理應將區塊鏈視為電磁紀錄之一種，亦即刑法第 10 條中所

謂「電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄」，如以該定義視之，應能就其價值性及相關法律規範直接適用於有關電磁紀錄之竄改、滅失之條文。理由在於，此類型資訊之處理方式，應仍建構在廣義的電腦處理型態之上，從前文所述之技術層面做例證，可知這種紀錄型態與處理方式，與電磁紀錄之定義並無出入。也因為如此，本文認為對於區塊鏈而言，應能直接適用電磁紀錄之相關規範。

5.2 區塊鏈保險：提供修正之經費

如文中所述，若區塊鏈需修改、追查，所耗費的時間、人力、經費頗為龐大，若在區塊鏈使用上能如同大專院校電腦使用費般，在建立私有鏈或公有鏈的情況下，使其繳交些許保險（或使用）費用，當創造區塊鏈時收取一次費用，且區塊鏈存續或使用者加入時亦繳交相關費用，對於未來可能發生的相關爭議時，政府部門亦能以此方式給區塊鏈「必須」關閉（修正）所提供之補償，或是提供硬分岔修正所需之經費，如此便能在不發生如中國大陸對區塊鏈實名制的情況下，又能提供一種解決之辦法。但此種方式仍須思考收取經費之法源，或以立專法、納稅收之方式做思考。

5.3 回復原狀：加註之思考

若因相關使用造成其他使用者權益受損，除行為人應面對該有之刑罰外，對於民事責任之承擔應如下做修正。民法第 213 條第一項所述，應將他方之損害回復至損害發生前之原狀。但在區塊鏈不可竄改特性，且確認行為人為前提的情況下，僅能要求行為人除刑事責任與金錢賠償之外，負擔相關修正所需之金錢，舉例來說，如以加註之方式為本，透過公權力的介入要求其餘使用者出借其私鑰（或直接購買私鑰），藉此加註原區塊鏈之行為為不法，相關費用由行為人承擔。前述之情況為影響較小的侵害權益，如行為影響被害人重大，需透過公權力之介入，以硬分岔之使用，相關費用同樣由行為人承擔。若行為人無法確認，則回到前段所述以保險經費支出。

5.4 被遺忘權：硬分叉之使用

於此同時，我國法律規範必須先將被遺忘權做統整性、妥善性的思考，無論以法律何種層次論之，都應先將其入法，才能夠做出後續之各項法規修正。當然，被遺忘權該如何入法或以何種法律視之，並非本文所探討的重點，若特殊案例符合我國未來被遺忘權之法令規範，當情節重大且必須以硬分叉之方式解決問題時，才能於法有據且於判決中亦不產生未定論的狀態。再者，然若相關法規予以建立，亦能於其中明訂相關時序上硬分叉使用的判準，也就是說，當同一時間產生了不同的被遺忘權使用要求，進而有著硬分叉的多個可能性產生，除須盱衡當時科學技術的處理可能之外，藉由法規規範的框架設立，從時間先後、利益多寡等比較衡量，交由司法權予以權衡使用其被遺忘權的先後次序，並思考權利因此受損害者，相關補償機制之建立。然若如此，此類技術與權利之問題，亦難一言以蔽之，而需權衡不同個案之產生，以不同思考模式做出判斷，也因此本文於此建議，理應優先思考被遺忘權之法制建立，再行以技術層面加以衡量及修正。

5.5 技術思考：分級權限與零知識證明

法律規範應配合技術之考量，從保密層級之不同做出區別的標準，因此在私鑰取得上，可先就相關權限之取得從身分、財力等類別做出條件限制，並以其作為進入區塊鏈的優先門檻。再者，雖現行零知識證明對於區塊鏈而言，是否適用仍屬不定論，但卻提供了一種從技術層面解決的思考模式。

退萬步言，本文所提出的問題，確實是種較為「躍進」且在法規範思考上涵蓋極為廣泛的爭議。因此區塊鏈對於現行法律所可能造成的「修正」而言，事實上僅能以提出特殊案例，或以現行判決作為論述之大方向。也因為如此，仍期許透過本文的思考，對未來科技與法律之間的「跨領域」有著些許的貢獻，特別是區塊鏈與吾輩生活之連結，如能藉此產生些不同角度的發想，確實得以為人類生活帶來更多的保障及更大的便利性。

參考文獻

中文期刊

- 宋俊賢、林安邦、董澤平，〈虛擬貨幣於電子商務之發展及其法律上之衝擊：以比特幣為討論中心〉，《電子商務研究》，第 12 卷第 2 期，頁 235-253，2014 年 6 月。
- 周濟群，〈改變世界的未來科技——「區塊鏈」的創新應用領域〉，《會計研究月刊》，第 373 期，頁 42-47，2016 年 12 月。
- 林敬庭、董祥開、連婕妤，〈政府資訊公開與個資保護之模糊與歧異：六都政府網站員工聯絡資訊公開程度之比較分析〉，《民主與治理》，第 5 卷第 2 期，頁 1-35，2018 年 8 月。
- 陳立群，〈區塊鏈在食品履歷追溯追蹤的應用〉，《電工通訊季刊》，2018 年第 2 季，頁 1-7，2018 年 6 月。
- 陳恭、蕭婕，〈運用區塊鏈打造公共治理新局面〉，《國土及公共治理季刊》，第 6 卷第 4 期，頁 50-61，2018 年 12 月。
- 張志偉，〈記憶或遺忘，抑或相忘於網路——從歐洲法院被遺忘權判決，檢視資訊時代下的個人資料保護〉，《政大法學評論》，第 148 期，頁 1-68，2017 年 3 月。
- 張智聖，〈科技與法律的介面：科技性不確定法律概念「判斷餘地」之研究〉，《生物產業科技管理叢刊》，第 5 卷第 2 期，頁 85-125，2016 年 3 月。
- 黃茂榮，〈回復名譽之適當處分及強制登報道歉的合憲性〉，《植根雜誌》，第 26 卷第 8 期，頁 19-40，2010 年 8 月。
- 黃茂榮，〈2011 年刑事法發展回顧：法律說詞與說詞之外〉，《臺大法學論叢》，第 41 卷特刊，頁 1537-1574，2012 年 11 月。
- 葉銀華，〈治理科技：區塊鏈與公司治理〉，《會計研究月刊》，第 379 期，頁 19-23，2017 年 6 月。
- 楊柏宏、陳鈺雄，〈被遺忘權之研析——以歐盟法院 Google Spain SL 案及歐盟個資保護規章為中心〉，《萬國法律》，第 208 期，頁 98-120，2016 年 8 月。
- 蕭宇程，〈IOTA：為物聯網量身打造的新一代區塊鏈技術〉，《電工通訊季刊》，2018 年第 2 季，頁 14-21，2018 年 6 月。

蕭郁澹，〈俄國修正資訊保護法明定保護被遺忘權——被遺忘權的明文化，正考驗網路資訊的文明化〉，《科技法律透析》，第 27 卷第 10 期，頁 5-6，2015 年 10 月。

顏于嘉，〈由美國資訊隱私法制觀察被遺忘權在美國的發展〉，《萬國法律》，第 211 期，頁 25-33，2017 年 2 月。

羅天綱，〈行政罰上行為數的判斷——兼評最高行政法院 100 年 5 月份第 2 次庭長法官聯席會議決議〉，《法令月刊》，第 63 卷第 12 期，頁 37-62，2012 年 12 月。

其他中文參考文獻

林之晨，區塊鏈的「零知識證明」是什麼東西？，2018 年 11 月 5 日，天下雜誌：<https://www.cw.com.tw/article/article.action?id=5092794>（最後點閱時間：2020 年 2 月 25 日）。

陳瑞霖，突破封鎖，以太坊交易紀錄傳播中國高校#MeToo 異議事件，2018 年 4 月 24 日，科技新報：<https://technews.tw/2018/04/24/break-censorship-someone-use-ethereum-transaction-recording-me-too-event-in-china-university/>（最後點閱時間：2020 年 2 月 25 日）。

黃彥鈞，比特幣區塊鏈存有虐童內容，害礦工也被當變態？，2018 年 3 月 26 日，科技新報：<http://technews.tw/2018/03/26/child-abuse-image-in-bitcoin-blockchain/>（最後點閱時間：2020 年 2 月 25 日）。

黃彥鈞，LegalThings 把所有約定都搬上區塊鏈，從約炮到商業契約無所不包，2018 年 8 月 6 日，科技新報：<https://technews.tw/2018/08/06/legalthings-change-contract-by-blockchain/>（最後點閱時間：2020 年 2 月 25 日）。

英文期刊

Allcott, Hunt & Matthew Gentzkow, *Social Media and Fake News in the 2016 Election*, 31(2) J. ECON. PERSP. 211 (2017).

Crosby, Michael, Nachiappan, Pradan Pattanayak, Sanjeev Verma & Vignesh Kalyanaraman, *Blockchain Technology: Beyond Bitcoin*, 2 APPLIED INNOVATION 6 (2016).

Dyson, Simon, William J. Buchanan & Liam Bell, *The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime*, 1(2) JBBA 5997 (2018).

- Efanov, Dmitry & Pavel Roschin, *The All-Pervasiveness of the Blockchain Technology*, 123 *PROCEDIA COMPUTER SCI.* 116 (2018).
- Lee, Edward, *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 49 *U.C. DAVIS L. REV.* 1017 (2015).
- Lee, Jong-Hyoun & Marc Pilkington, *How the Blockchain Revolution Will Reshape the Consumer Electronics Industry*, 6(3) *IEEE CONSUMER ELEC. MAG.* 19 (2017).
- Lin, Iuon-Chang & Tzu-Chun Liao, *A Survey of Blockchain Security Issues and Challenges*, 19(5) *INT'L J. NETWORK SEC.* 653 (2017).
- Li, Zhiyong, *Will Blockchain Change the Audit*, 16(6) *CHINA-USA BUS. REV.* 294 (2017).
- Nofer, Michael, Peter Gomber, Oliver Hinz & Dirk Schiereck, *Blockchain*, 59(3) *BUS. & INFO. SYS. ENGINEERING* 183 (2017).
- Park, Jin Ho & Jong Hyuk Park, *Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions*, 9(8) *SYMMETRY* 164 (2017).
- Pieroni, Alessandra, Noemi Scarpato, Luca Di Nunzio, Francesca Fallucchi & Mario Raso, *Smarter City: Smart Energy Grid Based on Blockchain Technology*, 8(1) *IJASEIT* 298 (2018).
- Shackelford, Scott J. & Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*, 19 *YALE J.L. & TECH.* 334 (2017).
- Singleton, Shaniqua, *Balancing a Right to Be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD*, 44 *GEORGIA J. INT'L & COMP. L.* 165 (2015).
- Zhao, Huawei, Peidong Bai, Yun Peng & Ruzhi Xu, *Efficient Key Management Scheme for Health Blockchain*, 3(2) *CAAI TRANSACTIONS ON INTELLIGENCE TECH.* 114 (2018).
- Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen & Huaimin Wang, *Blockchain Challenges and Opportunities: A Survey*, 14(4) *INT. J. WEB AND GRID SERVICES* 352 (2018).

英文研討會論文

- Rackoff, Charles & Daniel R. Simon, *Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack*, in *ADVANCES IN CRYPTOLOGY-CRYPTO'91*, at 433

(Joan Feigenbaum ed., 1991).

Dennis, Richard & Gareth Owen, *Rep on the Block: A Next Generation Reputation System Based on the Blockchain*, in 10TH INTERNATIONAL CONFERENCE FOR INTERNET TECHNOLOGY AND SECURED TRANSACTIONS 131 (2015).

Hua, Jing, Xiujuan Wang, Mengzhen Kang, Haoyu Wang & Fei-Yue Wang, *Blockchain Based Provenance for Agricultural Products: A Distributed Platform with Duplicated and Shared Bookkeeping*, in 2018 IEEE INTELLIGENT VEHICLES SYMPOSIUM (IV) 97 (2018).

Halpin, Harry & Marta Piekarska, *Introduction to Security & Privacy on the Blockchain*, in 2017 IEEE EUROPEAN SYMPOSIUM ON SECURITY & PRIVACY WORKSHOPS 1 (2017).

Kumar, Amrit, Clément Fischer, Shruti Tople & Prateek Saxena, *A Traceability Analysis of Monero's Blockchain*, in COMPUTER SECURITY-ESORICS 2017, at 153 (Simon N. Foley, Dieter Gollmann & Einar Snekkenes eds., 2017).

McCorry, Patrick, Siamak F. Shahandashti & Feng Ho, *A Smart Contract for Boardroom Voting with Maximum Voter Privacy*, in FINANCIAL CRYPTOGRAPHY & DATA SECURITY 357 (Aggelos Kiayias ed., 2017).

Scott, Brett, *Blockchain Technology for Reputation Scoring of Financial Actors*, FINANCE & BIEN COMMUN / COMMON GOOD N 42&43 – ETHICS IN FINANCE, SENSE OF URGENCY / LE SENS DE L'URGENCE – NOMINATED ESSAYS, THE ROBIN COSGROVE PRIZE 2014/2015 – 2015 128 (2015).

其他英文參考文獻

Bitcoin Developer Guide, Consensus Rule Changes, BITCOIN, <https://bitcoin.org/en/developer-guide#consensus-rulechanges> (last visited Feb. 10, 2019).

Brown, Richard G., James Carlyle, Ian Grigg & Mike Hearn, *Corda: An Introduction*, R3-CEV (Aug., 2016), https://pdfs.semanticscholar.org/b100/0a6166b6e221f61f35259dbfab4f4d6df76a.pdf?_ga=2.215454288.653812434.1580288912-1951266822.1580288912.

Hearn, Mike, *Corda: A Distributed Ledger*, CORDA TECHNICAL WHITE PAPER (Nov. 29, 2016), <https://www.corda.net/content/corda-technical-whitepaper.pdf>.