論比特幣交易履行之保障
——以民事強制執行為核心

文／李怡諄、謝宗翰

上

壹 前言

今年之前在這一波新冠肺炎疫情滋擾下，各國央行先前紛紛祭出調降利率作為刺激市場之手段，進而影響其國內金融機構調降存款利率，投資大眾為避免現有資金遭通貨膨脹侵蝕，各種看似保本、避險，甚至價值不斷攀升之新興（金融）商品討論也日趨熱烈。其中又以近年因區塊鏈相關技術的發展與觀念之啟迪，所帶來之虛擬通貨[1]此類嶄新非典型金融商品（例如：利用分散式帳簿技術下所創造之比特幣[2]，或與智能合約結合之以太幣[3]等）最引人矚目。國際間目前除中國大陸明令禁止虛擬通貨之交易外，其餘諸如美國、日本、菲律賓及泰國等國家，則是透過證照之發給來管制平台業者之經營資格，並要求其遵循洗錢防制相關規範。在虛擬通貨於我國審判實務已不乏肯認其得作為交易客體之前提下[4]，我國現行法制對於虛擬通貨之規範，不論行政監督管理與司法制度（包含審判及強制執行層次），現今尚無一套系統性之規範。面對此大幅超越原有金融市場之廣度、深度與複雜程度之新興交易標的，伴隨頻繁交易紛沓而至的糾紛，以我國現有之法規似不足以應付此類非典型金融商品爭議，更遑論在耗盡巨量勞力、時間、費用等訴訟成本後，所獲得之裁判又該如何獲得落實，也成了前所未見之新課題。為此引起本文擬自虛擬通貨之設計原理與交易模式，檢視其法律上合理之定性，再從其定性討論在強制執行程序可能面對之困境，最後嘗試提供可能的修正建議。又虛擬通貨如前所述，其數量與種類浩繁，為集中討論之焦點，本文先以最廣為人知且交易最為活絡之比特幣作為研討之標的。

貳 比特幣之源起、技術原理及基本交易模式

一、比特幣之源起

以往資金之往來除直接透過金融機構辦理匯兌，縱使循所謂「電子第三方支付」，亦因該第三方機構之介入而使交易存在額外成本支出、金流無法完全匿蹤及被詐欺風險[5]，署名「中本聰（Satoshi Nakamoto）」者，遂於西元 2008 年 11 月 1 日提出建構一套虛擬通貨帳務管理系統的論文「Bitcoin: A Peer-to-Peer Electronic Cash System」[6]，該系統建立在區塊鏈（詳後述）概念之基礎上，使所欲交易之電子記帳單位（即日後俗稱之比特幣）直接透過點對點之方式一步到位，無須透過任何金融機構或第三方支付平台辦理結算，過程中，只會在網路上留下交易時間戳記（timestamps），而這種「分散式記帳技術」可以將每一枚比特幣在歷史上交易的每個細節予以透明、省錢又安全的記錄下來[7]。有趣的是，中本聰的前揭論文內除文章名稱與出處網址一度提及「Bitcoin」字樣外，其餘全文並未再出現「Bitcoin」之名稱，論者遂有認所謂「Bitcoin」所指實乃是一種「系統」[8]，故針對市場上作為交易媒介或計數單位之比特幣（bitcoin）應為日後使用該系統者相約成俗所給予之慣稱，而其亦確實符合我國「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」第 2 條第 1 項第 2 款所賦予虛擬通貨的定義，為方便行文以下仍以「比特幣」代稱坊間交易之標的，至於中本聰所建構之「Bitcoin」電子平台，則以 B 系統代稱之。

二、比特幣暨B系統之運作技術原理

無論作為交易之工具、標的，抑或是單純作為記帳系統，比特幣與 B 系統均須立基在具有公信力之認證機制上，而數位簽章的加密系統與區塊鏈等技術即提供了絕佳的助力。茲先針對此等比特幣運作之基礎技術原理及若干專有名詞說明如下：

（一）作為加密系統的數位簽章機制

所謂數位簽章，依我國電子簽章法第 2 條第 3 款之規定，乃係指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。若加密與解密使用之金鑰同一，則稱為對稱性密碼系統，因使用對稱性密碼或加密系統，僅能提供單獨一組加密與解密之運作，除無法確保自己能排他掌握該資料的獨占性外，也無法達到雙方交互驗證之效果[9]，故而比特幣及 B 系統所採用者，為非對稱式金鑰加密系統（Asymmetric Encryption），亦即其用以加密與解密所使用之金鑰並不同一，在此種非對稱式加密系統中，每一個用戶都會擁有一對金鑰，包含著：①可以對外公開的公開金鑰（public key，下簡稱公鑰）及②只能私自收藏的私密金鑰（private key，下簡稱私鑰）。其中，公鑰在使用者之間（例如比特幣交易之轉讓人與受讓人）是可以相互揭示的（可以想像成將該公鑰展示給對方查看表徵身分的信物），功用在於使對方可以驗證與自己往來者之身分。

（二）防免一物二賣的區塊鏈概念

正因為 B 系統創設之理念乃是去中心化的點對點交易，在摒除第三方交割、結算之情況下，確實存在一物二賣的風險，而區塊鏈概念的運用，即是為了杜絕此弊端而來。其核心思想是將所有已經完成且符合公認條件的交易紀錄區塊，根據時間戳記的時序鍊接起來，並在非單一的機制下保留紀錄（也就是不存在唯一、單獨的紀錄保存機構）。前揭過程中，對各個交易紀錄進行公認驗證程序者，便是俗稱礦工的 B 系統參與者及節點[10]（運作上尚可細分全節點 Full node、修剪節點 Pruning node 與輕量節點 Lightweight node，至於其驗證之方式，因非本文介紹之重點且不影響文章之脈絡開展，恕暫略之）。以比特幣之交易為例，當轉讓人欲移轉其持有之比特幣（最小之交易單位稱為「聰（Satoshi）」，是一枚比特幣的一億分之一）時，該筆交易之內容，包括：①比特幣協議版本；②交易的比特幣出自何處；③該支出處持有的比特幣數量；④轉讓人的數位簽章；⑤交易的比特幣轉入何處；⑥受讓人的比特幣數量等訊息，會由轉讓人在 B 系統上廣播公告，等待 B 系統上的各個礦工依據系統預設的共識機制競相驗證，最先完成驗證手續的礦工，就取得將交易紀錄的區塊在 B 系統上記帳的權利，並且可因該記帳權而獲得獎勵（也就是俗稱挖礦取得的比特幣）。其獎勵之來源有二，一是來自 B 系統之原始設定，依據 B 系統的設計，直接源自系統所提供挖礦的獎勵會日趨減少，終至趨近於零產出，故而坊間才會預估 B 系統將來全部產出之比特幣存在 2,100 萬枚之數量上限，其二則是來自交易的轉讓人為儘早使該次交易獲得礦工們優先協助驗證所懸賞之手續費，手續費同樣是比特幣，數額由轉讓方自己決定，高額能產生使礦工盡快處理之誘因，一毛不拔則廣播的交易資料可能就沒有礦工願意處理[11]。

三、基本交易模式

在初步瞭解比特幣運作之基礎技術原理後，本文嘗試綜合解析比特幣之交易模式如下：

當比特幣交易在買賣雙方達成契約意思表示合致後，轉讓人欲將某一枚比特幣移轉給受讓人時，運作上會先由轉讓人利用受讓人所提供的公鑰 A（配對之私鑰則為受讓人私自保管之 a）來進行加密，將交易的訊息內容 H（即所轉讓之該枚比特幣交易細節，例如前文所述之協議版本等內容）透過演算法變成密文 h 後，轉讓人也會同時將 H 的內容使用雜湊演算法（Hashing Algorithms）計算出一個雜湊值[12]H'，接著由轉讓人將 H' 以自己的私鑰 b（該私鑰 b 乃係與公鑰 B 配對一組，作為加密與解密的工具）加密做成數位簽章，再將該數位簽章（內含 H'）與密文 h 傳送給受讓人，而受讓人收到密文 h 與數位簽章後，會先以轉讓人提供的公鑰 B 將數位簽章解密還原出 H'，爾後再使用自己的私鑰 a 將密文 h 解密還原成 H，繼而將 H 使用相同的雜湊演算法，看能否得出相同的 H'。由此可知，數位簽

（文轉三版）

註釋

1 關於此類金融商品究應以加密貨幣、虛擬貨幣或虛擬通貨稱之，不一而足，由經濟部公告之網路連線遊戲服務定型化契約應記載及不得記載事項、網路連線遊戲服務定型化契約範本，使用之用語為虛擬貨幣，然於 2018 年 11 月 7 日我國洗錢防制法第 5 條第 2 項增訂「辦理虛擬通貨平台及交易業務之事業」爾後，諸如證券集中保管事業管理規則、證券商管理規則、虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法等新法規均已統一使用虛擬通貨稱之，故本文亦從之。

2 參閱宋俊賢、林安邦、董澤平（2014），〈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，第 244 頁。

3 參閱林玫君（2019），〈區塊鏈智能合約的契約法問題〉，《國立中正大學法學集刊》，第 63 期，第 130 頁。

4 例如臺灣臺中地方法院 108 年訴字第 3798 號民事事件審理中，即曾明確認定虛擬通貨並非法所不容許交易之違禁商品。

5 例如：提供不可逆服務之賣方，無法要求買方提供不可逆之支付，來確保其能獲得交易之對價，參閱廖崇崴（2019），〈初探比特幣之民事強制執行〉，《華岡法粹》，67 期，第 151 頁。

6 網址：https://bitcoin.org/bitcoin.pdf（最後瀏覽：2022 年 8 月 8 日）

7 參閱陳榮傳（2019），〈論比特幣與比特幣之債〉，《軍法專刊》，65 卷 6 期，第 5 頁。

8 參閱陳丁章、范建得、黎昱萱，自比特幣技術的特徵論虛擬貨幣的法律特性及其相關議題，第 13 頁，初版，2021 年 4 月。

9 當交易的兩造都是使用同樣一組金鑰來進行加密與解密時，形同與他人分享對簽章內容的修正權限，則所有共享該加密與解密之金鑰者眾，將有礙於特定交易對象。至於非對稱式金鑰加密系統之交互驗證模式，詳本文後述。

10 B 系統的節點（node）可以理解為共同維護 B 系統的參與者，約略來說，除了個別礦工外，尚包含其他參與打包區塊的伺服器，同前註 8，第 18 頁。

11 見前揭註 8，第 17 頁、第 19 頁及第 26 頁。

12 所謂雜湊演算法，可以將任何長度的資料轉換成一組由數字和英文字母（大小寫）所組成之一定長度、不可逆推且唯一的雜湊值，原始資料內容改變，雜湊值就會改變，見前註 8，第 16 頁。

13 見前揭註 8，第 14 頁、第 15 頁。

14 見前揭註 8，第 16 頁、第 17 頁。

JUDICIAL 司法 徵稿啓事
三、文稿內容應符合學術倫理規範，請勿違反學術社群共同接受的行為準則；並請適當遮掩個資及其他法定限制公開事項。
六、文稿一律不退件，請自留底稿。稿件如經採用，文責自負。
七、刊出文稿除紙本刊登外，亦置司法院網站；並酌計稿酬，寄贈該期刊物。

憲法法庭 111 年憲判字第 15 號判決

照舊供作農田水利使用之土地 如無權源應予補償 3年內擬定計畫

【本刊訊】憲法法庭 8 月 12 日作成 111 年憲判字第 15 號判決。

案由

（1）聲請人雲林地院民事庭真股法官為審理案件，認農田水利會組織通則第 11 條第 2 項前段規定有違憲疑義，聲請解釋。（2）7 位聲請人有關補償事件受敗訴判決，經用盡審級救濟，認確定終局判決所適用之同一規定有違憲疑義，聲請解釋。

判決主文

中華民國 59 年 2 月 9 日修正公布之農田水利會組織通則第 11 條第 2 項前段規定：「原提供為水利使用之土地，應照舊使用」（109 年 7 月 22 日制定公布之農田水利法第 11 條第 1 項規定：「本法施行前提供農田水利會水利使用之土地，應照舊使用。」意旨相同）。其應照舊使用之土地，如屬人民所有，而未以租用、價購或其他方式取得權源，因其已形成個人之特別犧牲，即應依法徵收，給予相當之補償，並於 3 年內擬定徵收補償相關計畫，籌措財源，俾於合理期限內逐步完成徵收補償，始符憲法第 15 條保障人民財產權之意旨。

判決理由摘要

一、人民之財產被設為公物，如欠缺權源，應予徵收

國家將人民所有之特定財產設定為公物，致人民就該財產無從自由使用收益，基於法治國家之要求，自須具備設定公物關係之權源，如欠缺權源，因其已形成個人之特別犧牲，即應依法徵收，給予相當之補償，始符憲法保障人民財產權之意旨。

二、農田水利用地為公物，照舊使用係為確保公益

農田水利事業包括農田之灌溉、排水及防洪等，乃農業發展所必需，攸關國家經濟及民生。自 44 年 1 月 19 日修正公布水利法第 3 條及同年 9 月 17 日公布施行臺灣省各地農田水利會組織規程起，農田水利會即為公法人，屬國家間接行政之行政主體，設置目的係為促進農田水利事業，於農田水利事業區域內就農田之灌溉排水事項提供公共使用，其性質自屬公物。109 年制定公布農田水利法，農田水利會由公法人改制為行政機關，該法施行前原由農田水利會管理之農田水利設施及供農田水利使用之土地，回歸國家直接行政，改由行政院農業委員會管轄，其性質仍屬公物。

農田水利用地既為公物，係推行農田水利事業所不可或缺者，而與國家經濟及民生息息相關，攸關特別重要公益，且歷經久遠年代未曾中斷作為農田水利之用，除非情事變更，已無繼續作為農田水利之必要而廢止其公物關係，否則即應維持其公物之使用，以確保特別重要公益之實現，59 年之規定明定原提供水利使用之土地應照舊使用。

三、照舊使用人民所有之土地，如未取得權源，即應依法徵收

惟國家將人民所有之土地設定為公物，要求所有權人須容忍其土地供公共使用，致人民就該土地無從自由使用收益，基於法治國家之要求，應具備設定公物關係之權源，若欠缺權源，因其已形成個人之特別犧牲，即應依法徵收，並給予相當之補償，始符憲法第 15 條保障人民財產權之意旨。

為供農田水利設施照舊使用之土地如原已具備設定公物關係權源，自不生問題，否則即應以租用、協議價購或其他方式取得權源。若未能取得權源，即應依法徵收，給予補償，並於 3 年內擬定徵收補償相關計畫，俾於合理期限內徵收補償。（完整判決書請見憲法法庭網站）

司法院第 204 次院會

司法院通過憲法訴訟法修正草案

【本刊訊】司法院 8 月 11 日召開第 204 次會議，由許宗力院長主持，通過憲法訴訟法修正草案及行政院送會銜之刑法第 185 條之 3 修正草案。

憲法訴訟法本次修正，係為因應憲法法庭審判實務運作，優化調整部分條文，計修正 15 條，增訂 1 條，重點摘要如下：

一、其他法律規定得聲請司法院解釋者，其聲請仍應依其性質，分別適用憲法訴訟法所定相關案件類型及聲請要件之規定。

二、刪除有關擬制相對人之規定。

三、當事人依憲法法庭通知到庭，應委任律師為訴訟代理人為原則，不以言詞辯論期日到庭為限。

四、增訂審查庭就聲請顯無理由者，毋庸命補正，得一致決裁定不受理。

五、增訂關係人得委任訴訟代理人，其依通知到庭時，應委任訴訟代理人。

六、增訂憲法訴訟法所稱關係人之定義。

七、排除關係人再聲請憲法法庭裁定許可擔任法庭之友，並明定聲請裁定許可擔任法庭之友之期間；如係聲請裁定許可提出專業意見者，於聲請裁定許可階段，除以書面敘明與審理案件之關聯性外，並應敘明其立場及論點要旨；聲請裁定許可擔任法庭之友，以及經憲法法庭裁定許可擔任法庭之友後，提出法庭之友意見書，均應為相關之資訊揭露。

八、憲法法庭就分別提起之數宗聲請得合併審理、合併裁判；其合併審理者，得指定其中一宗或數宗聲請案件行言詞辯論。

九、增訂言詞辯論期日應通知關係人及其訴訟代理人到庭，並賦予憲法法庭裁量當事人或關係人本人是否到庭之權。

十、公開大法官就實體裁定主文之立場，並採主筆大法官顯名制。

十一、增訂憲法法庭宣告法規範違憲溯及失效者之效力規定；修正憲法法庭判決諭知法規範違憲立即失效與溯及失效宣告效力之規範體系，並刪除刑事以外確定裁判於違憲範圍內一律不得再予執行之規定。

十二、更明確化人民聲請法規範憲法審查及裁判憲法審查案件之要件。

十三、增訂人民聲請法規範憲法審查及裁判憲法審查案件經憲法法庭判決宣告法規範溯及失效者，亦得準用第 53 條之規定。

增進雙向溝通

司法院與律師座談 增進雙方意見交流

【本刊訊】司法院為促進與律師界的溝通與互動，於 8 月 5 日舉辦「司法相關事務座談會」，邀請全國律師聯合會陳彥希理事長、監事會林國泰召集人、副理事長、理監事、秘書長等人參加。會議由林輝煌秘書長主持，許宗力院長親臨致詞，周占春副秘書長及相關廳處主管與會。

會議先由司法院各廳處長宣導需要律師支持或配合的業務，與會律師亦提出多項建議，包括希望法官能多依職權調閱電子戶籍資料；判決主文公告宜兼顧正確性與即時性，避免公告後再變更；加大裁判書查詢系統字體，以利閱讀；儘量提供可選取文字之電子卷證檔案光碟，俾利編撰書類等。

許院長致詞時感謝律師界在憲法訴訟法、國民法官法制定過程中積極參與並提供意見，協助推動法案，並請繼續予以支持。金字塔訴訟制度的改革是未來的重要目標，期許各方能持續溝通並支持此制度。另外，也鼓勵優秀律師轉任法官，共同提供人民更好的司法服務。許院長也表示，座談中律師提出的議題及建議，司法院都將作為重要的參考意見。

陳理事長亦代表全律會感謝司法院舉辦本次座談，提供法官、律師交流機會，增進彼此的理解與互信，期盼透過良好的溝通，讓司法更好。

（文接二版）

章可以重複確認轉讓者的身分，達到無法否認的效果，而使用公私鑰的機制，則是可以確定訊息內容的完整性及未被變更[13]。

簡言之，無論是透過私人洽購，或是交易平台的媒合，只要該比特幣交易之本質為比特幣之登記轉讓，如前所述，該交易之概念即係由轉讓人將所欲交易的該枚比特幣前一次交易（轉帳）的訊息，連同這一次（當次）交易（轉帳）的訊息，以受讓人所提供之公鑰，利用雜湊演算法來進行加密後，一方面由轉讓人連同前揭密文與自己的數位簽章一併寄送予受讓人供其使用與前揭公鑰成對的私鑰進行解密，另一方面轉讓人也會將交易之訊息廣播公告，使 B 系統上廣大的礦工群競相驗證該枚比特幣是否曾經易手而另有其主，來協助將取得公認共識的交易紀錄與舊有之交易紀錄（區塊）產生鏈接。

由此可知，所謂比特幣之轉讓，實際上是由轉讓人將該枚比特幣的下一位持有人作成交易紀錄後，透過數位簽章制度確認發送訊息之人別正確及區塊鏈之制度確認歷史軌跡連貫無缺，轉讓人的私鑰存在，是為了完成廣播公告前的交易紀錄製作所必需，系統上之礦工完成區塊認證後，下次要改寫該枚比特幣的交易紀錄時，前次交易受讓人便轉客為主的化身為轉讓人繼續相同的運作模式，換言之，概念上私人所持有之比特幣只是 B 系統的某分支帳本，客觀上私人持有的比特幣的電子錢包（包含線上錢包、硬碟錢包），甚或是紙錢包（列印私鑰資訊的紙張）均不存在何「比特幣」，所以私人持有的，只是可以用來註記各枚比特幣交易紀錄的「私鑰」而已[14]，也就是可以在 B 系統完成紀錄留存的電子簽章工具。

（下期待續）

（作者李怡諄為臺灣高等法院高雄分院法官 謝宗翰為臺灣高雄地方法院法官）

WEEKLY 周刊

一、本刊歡迎兼顧理論與實務、探討司法制度、法學新知、足供讀者參考的作品；並歡迎司法人、事及法院的故事。來稿請聯繫（02）23618577 分機 844 或 845。

二、作品如以偵、審中案件，及未確定案件為主題，或作者為文稿議題之關係人士，請勿來稿。

四、文長宜在 7200 字以內，以利一次刊出。文內引用資料請加註解，以利參考。

五、本刊對來稿有權潤飾斟酌，對有疑義之內容將洽請作者再行檢視；不願接受刪改者，請加註說明。