

比特幣之介紹及其交易
在台灣法律環境之適用

Alex TSAI

December 2013

一、 概念及原理

比特幣(Bitcoin)是一種網路虛擬貨幣，使用者只須經由網路，通過一個自由開放原始碼的軟體即可參與，是一個點對點(Peer-to-Peer)及去中心化(Decentralized)的支付系統。比特幣與一般虛擬貨幣最大不同之處在於，它是一種雙向貨幣流的虛擬貨幣架構，可用以做為虛擬及實體商品或服務交易的支付工具[1]。

比特幣的概念是由一位化名叫 Satoshi Nakamoto(中本聰)於西元 2008 年在一個密碼學網站中發表一篇名為“Bitcoin: A Peer-to-Peer Electronic Cash System”論文中提出[2]。於 2009 年初中本聰開創了第一個比特幣 P2P 使用者節點，並發行了有史以來的 50 個比特幣。新的比特幣是由 P2P 網路節點完成特定數學演算後產生，最初的前四年內，每十分鐘將發行 50 個比特幣，在此四年內將有 10,500,000 比特幣被製造出來，以後發行速率每 4 年遞減一半，亦即在第 5 年到第 8 年間全球發行速率為每十分鐘 25 個，製造出 5,250,000 比特幣，以此速率遞減，並將於 2140 年製造出最後一枚比特幣，使其貨幣總量被限定為 2100 萬個，從而構建出了一個缺稀性的供需機制[3]。

二、 交易方式及特點

比特幣是類似電子郵件的虛擬貨幣，使用者須先在一電子設備上安裝比特幣錢包(Bitcoin Wallet)[4]，安裝後將自動產生一組比特幣地址(Address)[5]及私密金鑰(Private Key)[6]，如同電子郵件帳號和密碼之關係。比特幣的交易方式是付款方透過電子設備依據收款方地址將比特幣直接支付對方，比特幣的交易資料將被傳輸到一個「區塊」(Block)[7]，此一交易因此得到初步確認(Confirmation)[8]，此一區塊會再連結到前一個區塊，以得到更多確認，而通常的交易會得到 6 個區塊確認，使交易風險獲得最大的控制。比特幣所有的交易歷史都儲存在「區塊鏈」(Block Chain)[9]中，是對所有比特幣交易歷史的記錄[10]。

比特幣發行系統是經 P2P 對等網路技術及密碼學原理所產生，因在 P2P 網路中不存在伺服器，每個使用者端即是一個節點，故不存在如國家中央銀行一般的中央機構，確保了比特幣發行系統無法被任何政府或個人惡意介入或破壞，且因該系統已設定貨幣發行總量，不會產生通貨膨脹問題。又比特幣是以匿名方式流通於全世界，且幾乎沒有任何交易成本，因此迅速成為全球受歡迎的交易方式。

三、 比特幣之現況及法律地位

依據 BitPay 網站顯示，目前全球已有超過 12,000 家商店或組織接受比特幣做為支付工具[11]，各國政府也對比特幣展現高度關注。2013 年 8 月 19 日，德國政府正式承認比特幣是一種貨幣單位，屬私人資金性質[12]。同年 11 月 20 日美國參議院聽證會公布美國聯邦準備理事會主席柏南克(Ben Bernanke)提出之信函，柏南克於函中表示比特幣此類虛擬貨幣「或具有長期的承諾(may hold long-term promise)」性質，認為目前還沒有對虛擬貨幣進行直接干預和監管之必要[13]。中國人民銀行副行長於同年 11 月 20 日表示，該行近期不可能承認比特幣的合法性，但比特幣交易作為一種網路上的買賣行為，民眾擁有參與的自由[14]。

我國中央銀行總裁彭淮南先生於同年 11 月 23 日接受立委質詢時表示，比特幣沒有法償效力，只能用於發行者與會員間的交易，現在遊戲廠商發行的點數就如同比特幣的初級，對於比特幣的交易，中央銀行將視為貴金屬交易加以管理[15]。彭淮南於同年 11 月 27 日立法院質詢時再次強調，依據中央銀行法規定台灣交易工具還是中央銀行發行的貨幣[16]。

四、 比特幣在台灣法律環境下之適用

1. 比特幣之法律性質

從貨幣觀點分析，貨幣以發行權區分，可分為本國貨幣及外國貨幣，在台灣各有不同規範依據。按中央銀行法第 13 條規定，中華民國貨幣由中央銀行發行，對於在中華民國境內之一切支付具有法償效力(Legal tender)[17]；又依據管理

外匯條例第2條及第5條規定，有關外國貨幣買賣之外匯業務，係由中央銀行管理[18]，而所謂外國貨幣，從文義解釋應為本國以外主權國家所發行之法定貨幣，於中華民國進行交易時，即應受我國中央銀行管理。惟比特幣並非我國中央銀行所發行之貨幣，實無可能被視為本國貨幣，又比特幣亦非任何其他主權國家所發行之法定貨幣，亦無可能被視為外國貨幣；加以彭淮南先生已明確表示比特幣不具法償效力及台灣的交易工具仍是中央銀行發行的貨幣等語，應可推認我國在短期內實無可能承認比特幣具有正式貨幣之地位。

其次，從遊戲點數性質分析，依據經濟部頒佈之線上遊戲點數(卡)定型化契約應記載及不得記載事項規定，所謂線上遊戲點數(卡)，指預付一定金額購買發行人所發行記載或圈存一定面額、遊戲物品項目或使用次數等形式之點數(卡)，並由持有人將表彰價值之序號或其他方式登錄至特定帳號中，用以兌換發行人所提供之線上遊戲服務或商品，依其定義，遊戲點數只能用於發行者與會員間的交易，發行人與會員間即存在一契約關係，而具有債之相對性。然比特幣係一支付系統，其發行目的係在做為全球性交易工具，本身不存在發行人或會員關係更無任何主體提供線上遊戲服務或商品，故比特幣之性質與遊戲點數仍有明顯不同。

再者，比特幣是由P2P對等網路技術和密碼學原理所產生的虛擬貨幣，任何持有電子設備之人均可以一定方式或對價取得及使用，現雖已有國家(德國)承認比特幣具有貨幣地位，惟從台灣法律規定分析，比特幣尚難被認定具有貨幣地位。至於比特幣之法律性質為何，可從比特幣的取得及交易方式進行分析。進言之，比特幣之取得除少數人可經由挖礦(Mining)方式取得外，其主要取得的方式仍須以現金、商品或勞務等做為交換對價，交易者間之法律關係實與買賣關係較為接近(關於比特幣交易之法律關係分析，另述於後)，亦即比特幣是由買受人以一定對價向持有人取得對比特幣之權利；買受人取得比特幣後，可再次行使對比特幣的權利，以取得對應物，亦即持有人對比特幣具有支配權、絕對權及對世權，比特幣因此具有「物」之性質，而屬無形財產。又，我國司法實務[19]均認為虛擬貨幣係屬電磁紀錄，持有人對於虛擬貨幣擁有支配權，可任意處分或移轉，於現實世界中具有一定之財產價值，可做為刑法竊盜罪(第323條及320條

第 1 項)[20]及詐欺罪(第 339 條第 2 項)[21]之客體，可見我國實務亦肯認虛擬貨幣係屬動產而具物權性質[22]，而比特幣既為電磁紀錄之虛擬物品，其性質亦應作相同解釋。

2. 比特幣交易之性質

有關比特幣之交易究應屬何種契約類型？依上揭說明，本文認定比特幣之法律性質為動產，故若買受人為取得比特幣而以現金交付出賣人，其性質應屬買賣契約，然若比特幣持有人再以比特幣做為取得物品或勞務之對價，此一法律關係應與互易契約較為接近，惟仍有待將來法院形成見解。然因民法第 398 條規定，有關互易之法律關係，準用關於買賣之規定，故無論解釋為互易契約或買賣契約，尚不致發生法律適用上的困難。

最後，彭淮南先生於同年 11 月 23 日明確表示，將來若比特幣有在台灣流動時，中央銀行將會視為貴金屬交易加以管理，似已暫時為比特幣交易之性質定下基調，亦即中央銀行認定比特幣係屬動產，而其交易類似貴金屬交易，屬物之買賣關係，應依相關法律進行規範及管理。

[1] 資策會，歐洲央行發表「虛擬貨幣架構」報告，法國比特幣交易平台取得 PSP 資格
<http://stli.iii.org.tw/ContentPage.aspx?i=5940>

[2] <http://bitcoin.org/bitcoin.pdf>

[3] <http://zh.wikipedia.org/wiki/%E6%AF%94%E7%89%B9%E5%B8%81>

[4] A Bitcoin wallet is loosely the equivalent of a physical wallet on the Bitcoin network. The wallet actually contains your private key(s) which allow you to spend the bitcoins allocated to it in the block chain. Each Bitcoin wallet can show you the total balance of all bitcoins it controls and lets you pay a specific amount to a specific person, just like a real wallet. This is different to credit cards where you are charged by the merchant. <http://bitcoin.org/en/vocabulary>

[5] A Bitcoin address is similar to a physical address or an email. It is the only information you need to provide for someone to pay you with Bitcoin. An important difference, however, is that each address should only be used for a single transaction. <http://bitcoin.org/en/vocabulary>

[6] A private key is a secret piece of data that proves your right to spend bitcoins from a specific wallet through a cryptographic signature. Your private key(s) are stored in your computer if you use a software wallet; they are stored on some remote servers if you use a web wallet. Private keys must never be revealed as they allow you to spend bitcoins for their respective Bitcoin wallet.

<http://bitcoin.org/en/vocabulary>

[7] A block is a record in the block chain that contains and confirms many waiting transactions. Roughly every 10 minutes, on average, a new block including transactions is appended to the block chain through mining.

<http://bitcoin.org/en/vocabulary>

[8] Confirmation means that a transaction has been processed by the network and is highly unlikely to be reversed. Transactions receive a confirmation when they are included in a block and for each subsequent block. Even a single confirmation can be considered secure for low value transactions, although for larger amounts like 1000 US\$, it makes sense to wait for 6 confirmations or more. Each confirmation *exponentially* decreases the risk of a reversed transaction.

<http://bitcoin.org/en/vocabulary>

[9] The block chain is a public record of Bitcoin transactions in chronological order. The block chain is shared between all Bitcoin users. It is used to verify the permanence of Bitcoin transactions and to prevent double spending.

<http://bitcoin.org/en/vocabulary>

[10] <http://zh.wikipedia.org/wiki/%E6%AF%94%E7%89%B9%E5%B8%81>

[11] <https://bitpay.com/directory#/>

[12] <http://finance.sina.com.hk/news/-33431-6110174/1.html>

[13] <http://qz.com/148399/ben-bernanke-bitcoin-may-hold-long-term-promise/>

[14] <http://news.cnyes.com/Content/20131122/KHBI444M9QELA.shtml>

[15] 聯合新聞網 <http://udn.com/NEWS/FINANCE/FIN4/8308072.shtml>; 東森新聞雲

<http://www.ettoday.net/news/20131120/298323.htm>; 今日新聞網

<http://www.nownews.com/n/2013/11/20/1025514> 等。

[16] 自由新聞網 <http://www.libertytimes.com.tw/2013/new/nov/28/today-e13.htm?Slots=BE>

[17] 係指國幣對於本國境內之一切支付具有合法清償效力之謂。國幣未經依法公告失其法償效力之前為法償貨幣，債務人以法償貨幣支付，債權人不得拒絕，否則應負遲延受領之責。

<http://www.cbc.gov.tw/lp.asp?CtNode=317&CtUnit=488&BaseDSD=7&mp=1&nowPage=27&pagesize=15>

[18] 依據管理外匯條例第 2 條規定，所謂外匯包括外國貨幣、票據及有價證券。

[19] 臺灣高等法院刑事判決 101 年度上易字第 494 號刑事判決、臺灣臺北地方法院 101 年度簡字第 114 號刑事判決、臺灣新北地方法院 91 年訴字第 2032 號刑事判決、法務部法檢字第 0920800696 號、(90)法檢決字第 039030 號函等。

[20] 臺灣新北地方法院 91 年訴字第 2032 號刑事判決認定被竊取之虛擬財產係屬電磁紀錄，被告破壞被害人對虛擬財產之持有支配關係，並建立自己之持有支配關係，構成刑法第 323 條及第 320 條第 1 項之竊盜罪。

[21] 臺灣高等法院刑事判決 101 年度上易字第 494 號刑事判決認定虛擬世界的財物屬刑法詐欺罪保護之法益，「惟該等虛擬財物並無人類可以感觸之實體物存在，以詐術手段為之，應認係取得財產上不法之利益」，應構成刑法第 339 條第 2 項之詐欺得利罪。

[22] 法務部法檢字第 (90) 法檢決字第 039030 號函認定電磁紀錄於竊盜罪以「動產」論，於詐欺罪亦屬「動產」，故虛擬物品得作為刑法竊盜罪及詐欺罪保護之客體。

* * * * *
* * *
*

DISCLAIMER

This publication is not intended to provide accurate information in regard to the subject matter covered. Readers entering into transaction on the basis of such information should seek additional, in-depth services of a competent professional advisor. Eiger Law, the author, consultant or general editor of this publication expressly disclaim all and any liability and responsibility to any person, whether a future client or mere reader of this publication or not, in respect of anything and of the consequences of anything, done or omitted to be done by any such person in reliance, whether wholly or partially, upon the whole or any part of the contents of this publication. This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, please visit <http://creativecommons.org/licenses/by-sa/3.0/>.

eiger