比特幣相關犯罪類型與因應作為之探討

A Study on Bitcoin-related Crime and Countermeasures

施志鴻
中央警察大學刑事警察學系
桃園市龜山區大崗村樹人路 56 號
una171@mail.cpu.edu.tw

摘要

2015 年 9 月 20 日一名香港商人在遭到綁架，綁匪透過境外 IP 電子郵件要求贖金，並以人力往返香港、傳遞訊息等手段規避查緝，最後要求家屬在香港以七仟萬港幣購買比特幣以支付贖金，警方雖在取得贖金前鎖定嫌犯，順利攻堅救出被害人，但以比特幣此種「密碼貨幣」作為犯罪工具的手法，已逐漸成為犯罪者所利用，亦對警方偵查犯罪形成新的挑戰。本文介紹比特幣之特性，並歸納出「比特幣詐騙」、「比特幣竊盜」、「被害支付」、「買賣非法物品交易」、「洗錢」等五種與比特幣相關的犯罪類型，並針對國內已偵破之比特幣三則犯罪案件進行案例分析，提出比特幣相關犯罪之整體因應架構，作為我國政應與執法機關因應相關虛擬貨幣之參考。

關鍵詞：比特幣、網路犯罪、虛擬貨幣

Abstract

On September 20, 2005, a Hong Kong businessman was abducted. The kidnappers requested for bitcoin ransom (70 million HK dollars) through email from Taiwan IP address. The police had arrested the suspects and rescued the victim before the victim's family paid the ransom. Cryptocurrency, such as bitcoin, has gradually adopted by criminals, and it has posed a challenge to the process of criminal investigation. This paper introduced the characteristics of bitcoin and concluded the following five types of bitcoin-related crime: bitcoin scams, bitcoin theft, bitcoin as ransom payment, bitcoin for illegal service, and money laundering. This paper further analyzed three bitcoin-related crimes and proposed some strategies to fight against bitcoin-related crime for law enforcement agencies.

Keywords: Bitcoin, Internet Crime, Virtual Currency

壹、 前言

2015 年 9 月 20 日一名香港商人在國內遭到綁架，該犯罪集團分工精細，犯案前事前策劃、勘查，行動時確認目標，綁架後轉換押解人質車輛，多次更換藏匿人質地點，作案期間刻意躲避監視器攝錄並關閉行動電話，僅透過境外 IP 電子郵件要求贖金，同時經由人力往返香港及傳遞訊息等手段規避查緝，最後要求家屬在香港以 7 仟萬港幣購買比特幣以支付贖金。警方雖在取得贖金前鎖定嫌犯，順利攻堅救出被害人，將犯罪成員緝捕到案，但以「比特幣」此種密碼貨幣（Crypto-Currency）作為犯罪工具之手法，已對警方偵查犯罪形成新的挑戰。

比特幣是近幾年所發展出來的一種新興虛擬貨幣，使用者基於各種不同理由使用比特幣。Yelowitz 及 Wilson 分析四種比特幣使用者類型及理由 (Yelowitz and Wilson 2015)：（1）對電腦程式人員而言，著重在比特幣挖礦與獎勵回饋；（2）對投資客而言，可由比特幣市價節節高昇獲取利益；（3）對自由主義者而言，比特幣適可擺脫中央監管，達成自由經濟之理想；（4）對犯罪者而言，則可利用其匿名性（Anonymity）從事犯罪或洗錢等非法行為。

近年來世界各地陸續爆發與比特幣相關之犯罪事件，各國政府意識到須強化其管制規範與作為，並強化執法機關之偵查技術與能力。例如英國政府於 2013 年 3 月投入約 1 仟萬英磅經費，針對虛擬貨幣發展反洗錢技術與規範。2015 年德國和奧地利政府亦投入超過 1 仟五百萬歐元，就利用虛擬貨幣在有組織犯罪的應用，合作進行一項為期 2 年命名為”BitCrime”研究計畫。該計畫包含兩項子計畫，德國子計畫關注於發展技術性及組織性之方法，確保犯罪偵查效能，同時探索管理規範以預防犯罪並且保障合法使用者。奧地利子計畫則聚焦於分析犯罪金融交易型態（Patterns），並進一步透過其他網絡進行連結，以推論出社群媒體及暗網（Dark Net）的帳戶及位址，以強化數位金融交易中犯罪者的去匿名化（De-Anonymization）與身分辯識的偵查能力[1]。為強化執法人員因應比特幣等以「區塊鏈」（Blockchain）技術為基礎之虛擬貨幣相關犯罪之能力，國際刑警組織（INTERPOL）亦在 2017 年發展一套分析系統與流程，即時追蹤與觀察比特幣轉移資料與過程，並視覺化其交易相關關係、釐清特定位址的交易路徑與群組相關位址等(Kuzuno & Karam, 2017)。顯見即便比特幣是否會繼續存續並成為貨幣主流尚為未知之數，其衍生出之各種犯罪已為未來可能趨勢，極需發展新的規範與偵查技術思維加以因應。

目前我國就比特幣相關犯罪之研究尚屬起步階段，為提供未來研究及因應作為之參考，本文先就比特幣特徵加以介紹，再歸納出目前常見比特幣相關犯罪類型，並簡介國內偵破比特幣相關犯罪案例，最後，本文提出由法規與技術層面等因應模式，以達到監管效果並確保警方偵辦比特幣相關犯罪之效能。

[1] 資料來源：https://www.bitcrime.de/en/Flyer_BITCRIME_EN.pdf，流覽日期：2016 年 6 月 22 日。

貳、 文獻探討

一、 比特幣簡介

2008 年爆發金融海嘯，各國央行透過印製法定貨幣鈔票以營救經濟，導致全球資金氾濫，幣值貶跌，大眾對政府控管貨幣失去信心，「比特幣」(Bitcoin)就在此時因應而生。比特幣是 2009 年一名自稱「中本聰」(Satoshi Nakamoto)所開發的自由開放源碼支付系統，利用網際網路的運作連結能力，以及網路運算和加密技術，創造出無須擔保、匿名、無阻力流通、保存容易及交易公開透明、無人為干預等，更自由與開放的「去中心化點對點虛擬貨幣」(Decentralized Peer-to-Peer Virtual Currency)。比特幣是一種具有數位性質之貨幣，目前主要有兩種類型的數位貨幣：第一種是經由政府貨幣所主導如 PayPal 等電子支付平台或信用卡（如 Visa, Master Card）等數位金錢（E-Money），其交易受第三方監管，並依附在法定貨幣架構當中；第二種是與政府貨幣無涉的虛擬貨幣，包含 Bitcoin、Litecoin、 Namecoin、Auroracoin、Peercoin、 Dogecoin、ETH/ETC 等(Ponsford 2015)，其中比特幣已被視為現今最成功但最具爭議性的虛擬貨幣代表（兩者比較如表 1）。

表 1：數位金錢與比特幣比較表[2]

	數位金錢（E-Money）	比特幣（Bitcoin）
格式	數位	數位
客戶認證	依金融相關法規進行客戶身分認證	無須身分認證
發行方式	由法定法幣之央行認定數位發行	由電腦程式挖礦（Mined）產生
發行者	依法設置數位貨金融機構	民眾或礦工（Miners）

比特幣是經由所謂挖礦（Mining）產出，挖礦具有經由電腦運算程式產生比特幣，以及確保去中心化點對點分佈記帳系統（Public Ledger）正確性的雙重功能。任何人皆可至網路下載挖礦程式，該程式會連結至比特幣網絡（Bitcoin Network）建立節點（Node），每次進行比特幣交易時，該交易便會廣播至整個比特幣網絡，此時節點便會將有效的交易置入某個區塊（Block），在經由驗證工作（Proof-of-Work）解決複雜的數學問題後，該節點再將區塊廣播至比特幣網絡，待網絡確認該區塊有效後，則會將其編寫至區塊鏈（Blockchain），即記載所有交易記錄的點對點分佈記帳系統。比特幣網絡並會生成一定量比特幣給礦工，作為正確解決數學問題的獎勵回饋(Penrose 2013)。比特幣創立之初的產生量為每 10 分鐘 25 顆速度生成，在總量達到一仟五百七十五萬顆時，每次產出量即減半為 12.5 顆，直到其總量上限二仟一百萬顆為止。

[2] 資料來源：European Central Bank, Virtual Currency Schemes, 2012, http://www.cgap.org/sites/default/files/Brief-Bitcoin-versus-Electronic-Money-Jan-2014.pdf，流覽日期：2017 年 6 月 29 日。

不同於數位貨幣仍受政府管控並依附於法定貨幣，比特幣可謂為獨立一套貨幣系統，其主要特徵簡述如下(Maftei 2014; Reid and Harrigan 2013)：

（一） 低通膨風險：由於比特幣總量受二仟一百萬顆限制，再加上並無對貨幣價值的擔保者，其價值交由自由市場機制決定，因此任何人為造成的貶值是不可能發生，具較低通貨膨脹風險。

（二） 低交易風險：比特幣是採用整個 P2P 點對點網路節點（Nodes）的分散式資料庫記錄交易，運用密碼學確保各環節之運作，杜絕假幣產生，建構其安全穩定性；又因網路交易紀錄是全面保存、公開透明且無法竄改，受詐欺機會亦相對低。

（三） 交易程序迅速：比特幣透過網路創建「比特幣錢包地址」間轉移進行交易，比特幣錢包可自行生產公鑰 (Public-Keys) 收款及私鑰 (Private-Keys)[3] 付款，不若國際匯款工作天數為 2 至 5 天，付款方只要有收款方公鑰，最快在幾十分鐘內即可完成比特幣過帳，並無交易範圍等問題，可謂為世界通暢的交換媒介。

（四） 手續費低廉：比特幣交易是採取網路傳輸且無監管第三方，僅需向礦工支付少量的手續費，不必支付傳統跨國交易手續費或轉帳費用。即使透過如 Bitpay、BitoEX 等交易所買賣或兌換法定貨幣，其手續費亦較銀行低廉。

（五） 無需身分驗證：不若傳統金融交易具身分驗證機制，在比特幣網路交易者僅以公鑰被加以辯識，任何人都可透過相關軟體建立電子錢包取得公鑰，使用者無須登錄身分並經驗證程序。

根據比特幣資訊服務網站 CoinDesk 統計，截至 2018 年 10 月 10 日 1 顆比特幣的價格為 6,500.39 美元，較五年前漲幅達 5071.35%[4]。包括微軟、PayPal、戴爾電腦、日本樂天購物網站等愈來愈多企業和網站接受比特幣付款，世界各地亦有許多國家設置比特幣 ATM。顯見比特幣已逐漸成為被普遍接受的虛擬貨幣及支付系統，而其核心的「區塊鏈」（Blockchain）技術，更被譽為網路（Internet）問世以來最具破壞力之發明（解聰文，2016），未來可能會被廣泛運用到金融外各個領域，包含物聯網、不動產行業、食品安全等，帶給人類生活型態巨大改變與顛覆。

二、 比特幣相關犯罪類型

前述比特幣特徵亦對傳統經濟與社會秩序帶來諸多衝擊，其中第一個衝擊為稅賦之議題，因比特幣缺乏中央監管機制，又加上全球性流通及不具身份認證等，使得政府難以進行課稅，造成賦稅制度不公等問題。第二個衝擊乃是衍生之犯罪問題，亦為本文探討重點。比特幣目前在國際間被當作支付貨幣，也被視為投資商品，其身兼「貨幣」和「商品」之兩種特質，使其被利用在各種不同犯罪形態。綜合比特幣近年價值飆漲成為投資客追逐對象，輕易隱匿使用者身分與交易過程、交易迅速以及範圍廣泛等特性，本文歸整下列與比特幣相涉的犯罪型態：

[3] 比特幣地址是由比特幣公開金鑰進行雜湊運算得出的，公鑰是通過私鑰推算出，故可由私鑰推算出對應的公鑰位址（不可逆），參考自維基百科網站，https://zh.wikipedia.org/。

[4] 資料來源：https://stock-ai.com/dly-6-CoinDeskBPI.php#，流覽日期：107 年 11 月 11 日。

（一） 比特幣詐騙（Bitcoin Scams）

比特幣是一種新興貨幣概念與技術，其運作架構對許多人而言仍是謎團，近年比特幣價值飆漲，成為新興投資標的，許多犯罪者利用投資者無知或追求高利潤心態，進行比特幣詐騙。例如 Vasek & Moore 分析 192 件比特幣詐騙案件，依詐騙階段將其分為比特幣投資（Investment）、探勘（Mining）、錢包（Wallet）、交易（Exchange）詐騙等四種類型(Vasek and Moore 2015)，與傳統詐騙案件相似，其手法主要是宣稱可獲得較高的投資報酬率，吸引大眾買賣比特幣，待吸收達到相當金額後，即捲款潛逃。

（二） 比特幣竊盜（Bitcoin Theft）

該類型主要是透過駭客手法，取得被害人比特幣位址私鑰或侵入其線上錢包，再將比特幣竊取移轉。除個人受害外，近年來大型企業遭受竊盜的案例亦層出不窮，例如 2013 年 10 月澳洲比特幣錢包公司 Inputs.io 被駭客入侵兩次，損失超過一百萬美元之比特幣(Hern 2013)。2014 年 2 月全球最大的虛擬貨幣交易中心 Mt. Gox 宣稱價值四億二仟五百萬美元的比特幣遭到竊取，並宣告破產[5]。大陸地區 Bitcoin 交易所 Bter 在 2015 年遭到駭客 2 次攻擊竊取比特幣，損失金額分別達五佰萬與壹百柒拾伍萬美元[6]。2016 年 5 月總部在香港地區虛擬貨幣交易公司 Gatecoin 遭到竊取二百五十顆比特幣，損失高達二百萬美元(Cappella 2016)。2018 年 9 月，日本加密貨幣交易所 Zaif 被駭客入侵，竊取價值六十七億日圓比特幣（Bitcoin）等[7]。

（三） 被害支付（Bitcoin as Ransom Payment）

比特幣具即時性及匿名性特徵，被許多犯罪者用來要求被害人付贖的方式，以避免取款與被追查之風險。最常見的手法是利用綁架軟體（Ransomwares）對被害人電腦資料控制或加密，再要求支付比特幣作為贖金，以換取回復原來狀態。根據防毒軟體大廠趨勢科技指出，2016 年綁架軟體贖金大約在 0.5 至 5 顆比特幣左右(OConnell, 2015)，因該手法技術門檻較低而且下手範圍廣泛，已為犯罪集團帶來豐厚之犯罪所得。此外，本文先前介紹 2015 年香港商人擄人案件，歹徒提出用比特幣支付贖金，亦見運用到傳統暴力犯罪之趨勢。

（四） 買賣非法物品交易（Bitcoin for Illegal Drugs and Service）

許多非法網站會進行武器、毒品與兒童色情圖影買賣，買賣雙方透過比特幣支付進行交易。比特幣不似其他受監管的第三方支付數位貨幣（如 Paypal）須經身分驗證，亦可透過其他方式強化其匿名性，導致難以追蹤到

---

[5] 〈比特幣交易平台 Mt.Gox 申請破產保護〉，《BBC 中文網》，2014 年 2 月 18 日，http://www.bbc.com/zhongwen/trad/business/2014/02/140228_bitcoin，流覽日期：2016 年 7 月 15 日。

[6] 〈中國 Bitcoin 交易所 Bter 被攻擊，損失約 175 萬美元〉，《企業趨勢》，2015 年 2 月 17 日，http://unwire.pro/2015/02/17/bitcoin-bter-has-been-hacked/news/，流覽日期：2016 年 7 月 15 日。

[7] 〈日本虛擬貨幣交易所 Zaif 遭駭客入侵，損失 6,000 萬美元比特幣〉，《財訊快報》，2018 年 9 月 20 日，https://tw.stock.yahoo.com/news/，流覽日期：2018 年 9 月 25 日。

支付方之真實身分，故已廣泛被運用到非法物品交易。最典型案例為美國「絲綢之路」（Silk Road）黑市購物網站案例，該網站透過 Tor 架構的暗網（Dark Net）進行毒品與槍枝等非法物品買賣，2012 年絲路每月銷售額估計略超過一百二十萬美元，且販售物品多為毒品，被謔稱為「線上藥局」（Online Pharmacies）或毒品界的亞馬遜等(Chen 2012)。除 Tor 本身具隱匿追查功能外，加上使用者使用比特幣付款，形成雙重匿名功能及效果，增加偵辦之困難度(Christin 2013; Raeesi 2015)。2011 年，紐約州參議員 Charles Schumer 等要求對絲綢之路和比特幣展開調查，2013 年 10 月 2 日美國聯邦調查局以打擊犯罪活動爲理由進行查禁，2014 年 10 月 6 日再次被查封關閉其 2.0 版本，目前以 3.1 版恢復上線。

（五） 洗錢（Money Laundering）

洗錢是將犯罪不法所得（俗稱髒錢），漂白為看似合法之所得。一般而言，洗錢會經過下列三個程序：（1）置入（Placement）：將髒錢置入某個經濟系統、（2）層析分離（Layering）：將髒錢與其非法來源脫勾、（3）混和（Integration）：將已漂白之金錢以看似合法狀態重新置入經濟系統(Bryans 2014)。比特幣無須身分認證、輕易匿名、交易快速、無範圍限制等特性，近年來已成為犯罪集團新興洗錢管道。例如 2014 年 1 月美國比特幣交易站運營者 Robert Faiella 被指控在前述絲綢之路案件，協助毒販將一百萬美元兌換為比特幣，涉及洗錢犯罪，於 2015 年遭到判刑 4 年。此外，亦有證據顯示非法比特幣已被用來支持 ISIS 等恐怖組織運作 (Home Office 2016)。

即使比特幣與前述非法行為具有關聯，亦有具體案件發生，但其涉及程度與廣度為何，則未有定論。加拿大民主國家防禦基金會制裁和非法融資中心（Center on Sanctions & Illicit Finance memorandum）分析 2013 至 2016 年間進入加密貨幣交易所與交易平台之資金，與非法活動相關者只佔 0.61%。此外，與洗錢相關之比特幣交易比例則逐年下降，由 2013 年 1.07%下降到 2016 年 0.12%，部分原因可能為如 Monero 等更以保護隱私為中心的加密貨幣，在某程度上取代比特幣，成為暗網市場之首選貨幣(Fanusie & Robinson, 2018)。Paquet-Clouston, Haslhofer, & Dupont(2018)經由比特幣公開區塊鏈（公鑰）分析發現 2013 至 2017 年間被害人交付綁架軟體（Ransomwares）贖款僅 12,768,536 美元，結論指出此問題並未若外界想像如此嚴重。但另一方面，Foley, Karlsen, & Putniņš(2018) 分析過去破獲之比特幣犯罪案例（含 Silk Road 案），歸納非法與合法交易之特徵差異；再進一步利用「控制偵測法」（Detection Controlled Estimation Model, DCE）檢視比特幣交易情形，其發現約有四分之一使用者（25%）以及近半數交易（44%）與非法行為相關，該研究亦發現運用在非法用途的比特幣比例逐年降低，推論其原因是近年來合法使用比特幣的比例增加；另一個原因亦因其他具更不透明性與隱私化的虛擬貨幣（例如 Dash, Monero, ZCash 等）可供選擇；即使如此，該研究仍證實比特幣與非法行為高度相關。

參、 國內比特幣相關犯罪案例簡介

實際上，前述所列之犯罪類型並非因為比特幣所造成，而是因為比特幣特性故助長犯罪發生並且導致偵查困難度，成為犯罪份子利用工具。其中最關鍵特性在於比特幣使用者與交易「匿名性」，事實上匿名性並非比特幣本身所要表徵的特徵，在比特幣交易中，使用者 IP 位址皆能與其公鑰產生聯結，若是使用者未隱匿其 IP 位址，理論上可經由公鑰再聯結到其社會網絡與實體位置等資料，得知其真實身分。換句話說，比特幣隱匿性來自於缺乏中央監管與身分認證機制，再加上使用者刻意隱匿之結果。美國聯邦調查局曾指出比特幣使用者可透過下列方式增強其匿名性：（1）針對每次交易建立或使用新的比特幣錢包位址；（2）透過某些匿名性軟體（Anonymizer）隱匿其 IP 位址；（3）在建立新的支付時，將原有比特幣錢包位址結合至新建立的比特幣錢包位址；（4）透過特定洗錢機構；（5）使用第三方數位錢包（E-Wallet）服務合併多個比特幣錢包地址，讓其得以在任何設備儲存及取得比特幣；（6）某些客制化軟體讓使用者得以輕易挑選任其所有之比特幣錢包位址進行交易，使不具技術背景的使用者亦能輕易匿名進行比特幣交易(Federal Bureau of Investigation 2012)。整體而言，比特幣僅具有偽匿名性（Pseudo-Anonymity）之特性。

目前我國認定比特幣並非貨幣，不具真正通貨（Real Currency）特性。2013 年 12 月 30 日中央銀行會同金融監督管理委員會（下稱金管會）發佈新聞稿告知比特幣屬高度投機之數位「虛擬商品」，缺乏專屬法規之交易保障機制，故民眾應自行承擔有關收受、交易或持有比特幣所衍生的相關風險[8]。金管會又於 2014 年 1 月 6 日發布新聞稿，要求銀行等金融機構不得收受、兌換比特幣，亦不得於銀行 ATM 提供比特幣相關服務[9]。銀行被禁止辦理比特幣相關業務，且禁止比特幣於第三方支付的交易流程中使用。後因出現許多以招攬投資虛擬貨幣的活動，包括首次代幣發行(Initial Coin Offering，簡稱 ICO)的募資行為，2017 年 12 月 19 日金管會再度提醒社會大眾投資比特幣等虛擬商品的風險，並重申金融機構不得參與或提供虛擬貨幣相關服務或交易[10]。目前我國尚無虛擬貨幣交易所，僅有二家平台代理商辦理比特幣買賣事宜，其中一家 BitoEX 平台代理商與全家便利商店合作，自 2015 年 9 月起提供購買比特幣的服務，並可將比特幣直接兌換該公司現金券，即可在其店家進行折抵購買商品金額。近年陸續發生比特幣相關犯罪

---

[8] 中央銀行、金融監督管理委員會，〈比特幣並非貨幣，接受者務請注意風險承擔問題〉新聞稿，2013 年 12 月 30 日，http://www.cbc.gov.tw/ct.asp?xItem=43531&ctNode=302，流覽日期：2017 年 7 月 24 日。

[9] 金融監督管理委員會，〈金融機構 ATM 不得提供比特幣相關服務〉新聞稿，103 年 1 月 6 日，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201401060003&toolsflag=Y&dtable=News，流覽日期：2017 年 7 月 24 日。

[10] 金融監督管理委員會，〈金管會再次提醒社會大眾投資比特幣等虛擬商品的風險〉新聞稿，106 年 12 月 19 日，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201712190002&ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News，流覽日期：2018 年 9 月 24 日。

案件，因此犯罪方式為新興模式且無集中監管機制，故目前警方在偵辦上採取與比特幣廠商合作，提供資料與技術協助偵查。本文透過訪談相關比特幣業者與偵查人員，簡要介紹國內三則偵破案例介紹如下：

一、案例 1：花輪互助會吸金案

2016 年 3 月起施○○等人於臉書頁面設立「花輪比特幣國際互助社區」，宣傳某高投資報酬率之比特幣互助會網路平台，投資者只要投資 1 顆比特幣，下層再有 3 人以同金額投資加入遊戲，上層投資人即可獲得 2.5 顆比特幣。該集團利用暗樁偽裝投資人，以真、假混摻方式發放紅利，再由暗樁發送讚揚訊息，並利用名人宣傳不實訊息，以取信其他投資人，不到一個月期間即吸引三百多名投資人參與。犯罪集團將被害人投資比特幣，分批轉至其他帳戶，再以現金提領，獲利達兩千多顆比特幣。本案因犯罪集團分贓不均，內部成員將其對話截圖發至群組內，因而啟動本案之偵查。

為蒐集相關事證，專案小組加入該互助會網路平台之 Line 討論群組，進行相關犯罪事證蒐證，並掌握集團幕後主嫌身分。另一方面，投資民眾亦陸續發現犯罪集團未依約發放紅利，驚覺遭到詐騙，查詢得知本案相關錢包屬某平台代理商所有，故被害民眾撥打電話至該公司要求凍結或發還已投資之比特幣。該平台代理商透過金流大數據分析相關錢包比特幣出入行為，發現其在短時間由多個不同錢包轉入 1 顆面額之比特幣，集結一定數額後轉至其他錢包賣出之異常情形，故要求被害者前往警察單位報案取得報案三聯單證明，再依該報案證明為依據凍結此被害人投資比特幣流向。因該交易所針對其電子錢包建置交易資料庫（Transaction Pool），分析其「比特幣交易網絡」（Bitcoin Network）；又加上該公司在開戶時設有嚴格的身分驗證機制，客戶將比特幣變換法定貨幣時，尚需經過身分證件及銀行匯款帳戶之驗證，故迅速分析出比特幣流向以及實體帳戶關聯性，即時提供相關資訊作為偵辦參考。本案經蒐證完竣，於 2016 年 3 月 23 日發動搜索並拘提犯嫌林○○等 3 人，查扣電腦主機、手機、銀行存摺、金融卡、現金新臺幣七百餘萬等證物。

二、案例 2：Yes-BTC「數位比特股份有限公司」背信詐騙案

有國內三大平台代理商之稱的 Yes-BTC「數位比特股份有限公司」比特幣平台董事長何○○，涉嫌在 2015 年 1 月間，對外謊稱該公司有 VIP 客戶高價收購比特幣，調高公司比特幣收購價格約 1、2 成，吸引民眾至其他比特幣交易平台購買比特幣後，轉至該公司變賣。之後對外宣稱公司上線第 1 天就遭駭客攻擊，被盜走 435 顆、市值三百多萬元的比特幣，為彌補該缺口，故以公司名義向地下錢莊借貸三百萬元，最後因資金周轉不靈而宣告倒閉，被害人及股東求助無門向檢方提告。

本案經清查何嫌背景，發現何嫌個人積欠地下錢莊債務，急需大量資金週轉，具有犯案動機。另外，因比特幣區塊鏈特性，自挖礦開採出來後之交易流程均是公開、透明以及被加以保存的，故警方分析投資者轉賣之比特幣流向後，發現該批比特幣皆轉往大陸地區某比特幣交易所兌換法定貨幣，經商請該交易所協助取

得該帳戶相關資料，發現係為何嫌設立帳戶。警方聲請搜索票後查扣電腦等相關證物，發現何嫌係透過變更公司伺服器後台設定，將客戶比特幣轉入自己私人比特幣錢包，再變賣為現金，短短一個月有 49 人受害，騙走一仟六百多顆比特幣轉賣，證明係何嫌一人自導自演之背信詐騙案。

三、案例 3：全家超商盜買比特幣案

2014 年全家便利商店即與 BitoEX 比特幣交易所合作，民眾至 BitoEX 平台代理商開戶，經驗證完成取得該公司電子錢包，即可在便利商店設置之 FamiPort 機臺取得二維條碼，印出交易單據，至門市付款購買比特幣，購買之比特幣將自動匯入事先申請之電子錢包。2015 年 9 月起，消費者並可進一步透過 Famiport 機臺將錢包內比特幣，轉換成一百元及二百元現金券，購買全家門市內的任何商品。但因並不承認比特幣為貨幣，故此交易視為「以物易物」的虛擬商品，故商店並不提供找零服務。

2016 年 3 月，犯罪集團為不法獲取比特幣牟利，事先安排成員擔任全家超商大夜班店員，之後再由數名車手至鄰近數家全家超商 FamiPort 機臺，點選及列印比特幣購買條碼，因每間全家超商每日購買比特幣交易金額上限為新臺幣二十萬元，故車手分別將當日該店可購買之比特幣數額全數印出，再拿至事先安排之店員處掃描條碼完成購買交易，但實際上並無付款，取得比特幣後再轉賣牟利。

為確保交易安全性，BitoEX 平台代理商設有線上交易風險監控機制，利用大數據資料分析異常的交易型態，在案發當日其監控某家全家超商短時間出現大筆結帳交易紀錄，經追查發現其購買之交易條碼均出自結帳店鄰近之全家超商門市（如圖 1），故立即此這些異常交易封鎖，並通知全家超商進行調查，即時破獲此不法集團，並防止被害擴大。

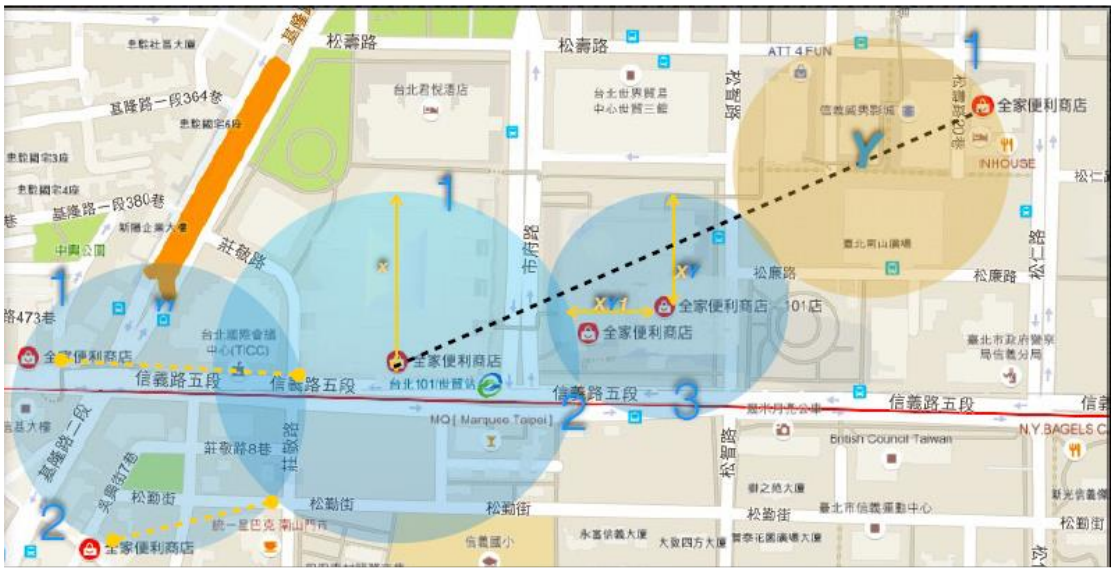

圖 1：全家超商盜買比特幣案案發時序地點分析示意圖

四、案例綜評

前述國內偵破之比特幣案例案情尚屬單純，犯罪集團亦未使用匿名等技術規避偵查，然由偵辦過程或可勾勒出未來比特幣規範方向與偵查技術初略圖像，供

後續建議參考。綜合案例探討，本文歸納出下列思考面向：第一、即便比特幣缺乏中央監管機制，但一般民眾可能會透過平台代理商建立電子錢包，進行比特幣購買、交易與變賣為法定貨幣等，因此平台代理商管理機制完善與否，或可間接補足未具身分驗證與匿名性之缺漏，並可提供及時追蹤、凍結可疑帳戶等作為，協助偵查並避免被害擴大（如案例 1、2、3）。第二、比特幣核心技術區塊鏈特性，使得任何比特幣交易過程皆能追蹤，建立交易網絡進行追蹤，以瞭解相關流向（如案例 1、2）。第三、同上特點，這些公開交易過程可讓執法人員取得交易行為資訊，透過大數據分析分析出異常行為樣態，形成具有意義之偵查情資（Intelligent）協助偵查（如案例 3）。然而，受訪平台代理商在訪談過程中亦強調，比特幣管理機制並非法律規定，其涉及所需人力、設備等成本考量，故取決於各公司之營運政策，長久而言將導致管理完善公司無法負荷而改變其政策方向；且若僅有部分平台代理商建置管理制度，非法者亦可有可能尋求管理較為鬆散之交易架構規避，亦易形成犯罪者尋求之漏洞，故應建置統一的規範與制度。

肆、比特幣犯罪因應架構

比特幣是一種創新且令人驚豔的虛擬貨幣，開創出非政府數位貨幣可能性與風潮，在比特幣之後至 2018 年 7 月為止，全球已出現如 Ethereum、Dash、Zcash、Litecoin, Monero 等 1,629 種私人虛擬貨幣(Gonzalez, 2018)，比特幣在市場流通與普遍度仍居於領先地位(Irwin & Turner, 2018)[11]。但比特幣具備缺乏中央監管、不須擔保、匿名、無阻力流通等特性，已被廣泛運用在作為犯罪客體、交易貨幣與洗錢工具等非法行為，導致執法機關在偵辦時面臨相當地挑戰。綜合前述比特幣特徵與案例介紹，本文認為比特幣相關犯罪偵查涉及貨幣、金流、偵查技術等面向，故由管理規範與偵查技術兩個層面提出建議，試圖建構一個整體的初步因應架構（如圖 2）。

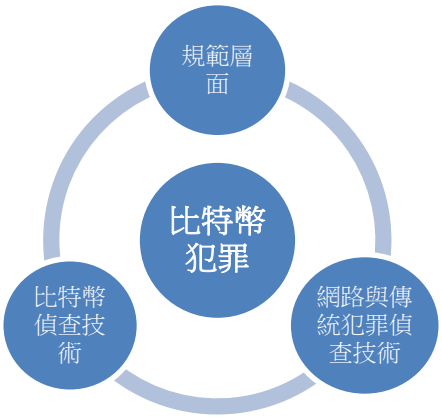

圖 2：比特幣犯罪偵查因應架構

[11] 根據統計資料顯示，2018 年最普遍使用的十種虛擬貨幣依序如下：Bitcoin、Bitcoin cash、Litecoin、Dogecoin、Ethereum、BAT、NEO、Ripple XRP、Stellar (XLM)、Cardano (ADA)，Reynard, C. 2018. “The 10 most popular cryptocurrencies in 2018” ，in: Telegraph（5. 25, 2018）, Retrieved 8.22, 2018, from https://www.telegraph.co.uk/technology/digital-money/top-10-popular-cryptocurrencies-2018/.

一、管理規範層面

因無前例可尋，比特幣管制規範面臨到相當之難題。目前各國各自有其不同的管制架構與規範，缺乏一套全球化規範可供參考。隨著比特幣經濟的快速成長，建構一套適當之管制是勢在必行的趨勢。比特幣規範涉及面向相當廣泛，包含金融、經濟、稅制、科技等議題，加上比特幣在全球流通並無範圍限制，若無跨境整合模式恐難收監管之效，因此其規範應難一步到位，恐須隨著比特幣市場發展與技術之開發，經由嘗試修正（Trial and Error），始能建構出一套合適模式。在管理規範層面，本文提出下列三個方向建議[12]：

（一） 明確界定比特幣之定位：各國政府目前尚無法具體規範比特幣的主要原因，在於未能明確定位比特幣性質，例如德國、巴西正面承認比特幣為貨幣，其他多數國家則採取觀望態度，將其視為虛擬商品者(De Filippi 2014)，導致各國規範架構莫衷一是，以致在預防及打擊犯罪的效能大打折扣。在清楚界定比特幣的定位後，始能在此基礎下進一步探討及建構跨境規範架構。目前國際規範比特幣主要有兩種取向，第一種將其比擬或視為貨幣，而納入傳統金融管理架構；第二種為針對比特幣重新建構一套全新的管理架構(Middlemas 2016)，本文建議我國政府應給予比特幣明確定位，參酌國際發展訂定共同遵循之管理規範。然而，無論比特幣定位或規範架構為何，比特幣起端於對政府央行控管貨幣的不信任，進而創造出一套自由、開放之貨幣架構，若政府過度干預其供需運作與匯率等，則與比特幣本質相悖，將有使其因人為因素而泡沫化之虞，故本文建議規範之射程應僅限於與稅賦、犯罪相關範疇，避免干涉匯率等自由開放架構。

（二） 強化消費者及比特幣交易平台之自我規範：因比特幣並無貨幣價值的擔保，其價值完全交由自由市場機制決定，故應藉由市場機制，強化消費者及比特幣交易所自我規範。除外在政經環境因素影響外，例如英國脫歐公投通過後，投資者擔心英磅或歐元貶值，故轉而購買比特幣，導致其價值攀升(Levy 2016)，比特幣價值最關鍵因素在於其是否具備可信性，其中可信性之基礎在於比特幣交易安全與穩定性。目前許多國家採取風險告知方式，提醒投資者相關風險與自行承擔責任。本文建議我國應持續關注並宣導比特幣相關犯罪問題，鼓勵民眾應尋求具完善制度之比特幣交易所或平台管理商進行交易，以降低其交易風險，並且避免因

[12] 在本文截稿前，我國中央銀行、法務部及金管會等單位已達成共識，未來相關業者必須如同金融業一般遵守防洗錢機制。依洗錢防制法第 5 條規定，其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員，也可被指定為非金融事業或人員。未來虛擬貨幣相關業者必須要採取確認客戶身分、保存交易紀錄、一定金額以上交易應向法務部調查局申報等措施，以防制洗錢，甚至金管會還要求，虛擬貨幣帳戶必須採取實名制，惟相關規範與法制作業尚在研議與推動中，黃敬哲，〈比特幣滲入犯罪行為，台灣將開始監管〉，《科技新報》，2018 年 6 月 15 日，http://technews.tw/2018/06/05/bitcoin-infiltrate-criminal-behavior-taiwan-will-begin-supervision/，流覽日期：2018 年 7 月 12 日。

比特幣來源與犯罪相涉而遭調查、甚至凍結等不利益。另一方面，各國政府應明確立法課予比特幣交易所或平台管理商相關管理義務，主動控管可疑犯罪情狀，並在符合法定程序下提供必要資訊，作為偵查犯罪參考，以強化偵查效能，因而確保比特幣安全性與可信性。

（三） 建立比特幣與法定貨幣轉換之實名制度：雖然比特幣所有交易過程在區塊鏈皆為公開透過，然而交易者僅以公鑰呈現，無法辨識隱藏其後的真實身分。傳統金融機關已建立「知悉顧客原則」（Know-Your-Customer Principle），強化洗錢防制的功能，為追蹤比特幣相關犯罪所得以及防範洗錢，美國經濟犯罪執法網絡（Financial Crime Enforcement Network, FinCEN）即在 2013 年提出指引（Guidance），詳細建議比特幣交易公司應蒐集顧客資訊，以利於顧客能將比特幣兌換為其他貨幣時能與其真實身分聯結(Penrose 2013)。本文建議我國未來應明確立法，至少將「知悉顧客原則」運用至比特幣系統的邊界處，即在比特幣與傳統法定貨幣、物品或服務交換時點（俗稱下車點）(Möser et al. 2013)，落實實名制度與身分驗證機制，提供偵查機關得以連結犯罪相關人身分之機制，減輕其匿名之性質。

二、偵查技術層面

即使比特幣匿名、無阻力流通等特性，對於執法機關造成威脅；但另一方面，不若傳統金融系統雖建立完整身分登錄與驗證機制，但對未透過如銀行匯款等機制之金流走向卻難以掌握；比特幣根基於區塊鏈技術，其所有交易過程皆會被公開記錄保存下來，成為一種公開資訊（Open Resource），換句話說，比特幣具有「匿名但透明」之特性，所有的比特幣交易都是透明和可溯源的，它們會被永久地儲存在 Bitcoin 網路，成為偵查另個有利契機(Tziakouris 2018)。因此，本文歸納下列幾個偵辦比特幣相關犯罪之偵查技術與重點：

（一） 發展比特幣交易記錄與即時追蹤技術：比特幣是透過整個 P2P 點對點網路節點（Nodes）的分散式資料庫記錄所有的交易情形，一旦使用者在電腦或行動上安裝比特幣錢包，即根據公鑰與私鑰推算第一個比特幣位址（Address），作為發送與接收比特幣之交易（Transaction）。在一個比特幣交易，使用者通常會使用許多位址，例如交付方（Sender）可能由多個位址送出比特幣且接收新位址，但所有位址皆受使用者之私鑰所控制，因此在此交付過程所涉及之數個位址，皆屬同一位使用者所有。在確定一位使用者使用之位址後，再透過這些位址與其它交易交集比對，則可進一步確定哪些交易是屬於同一使用者(Foley et al. 2018)。亦即透過電腦演算法（Algorithm），可將交易層次之資料轉化為使用者層次之資料，作為比特幣使用者交易追蹤與記錄(Ron and Shamir 2013)。此外，目前已有商用技術服務可用來追蹤比特幣交易路徑；例如 Chainalysis 公司提供分析比特幣之交易與位址，提供瞭解整個比特幣交易生態，包含使用者交

易行為與型態等 (Gonzalez 2018)。建議我國執法單位可發展與運用相關追蹤技術，俾利掌握可疑使用者之交易流向與手法。

（二） 分析與建立非法使用者交易特徵：在掌握使用者層次之資料後，可進一步分析合法與非法使用者之交易行為與形態，並分析出後者交易特徵。Foley, Karlsen, & Putniņš(2018) 分析過去執法單位破獲之比特幣犯罪案例（含前述 Silk Road 案），歸納出非法用途之交易特徵，發現非法比特幣使用者密集進行小額比特幣交易、錢包持有非常少量比特幣、並且集中與特定帳戶重覆進行交易。非法交易使者較常將比特幣作為支付系統而非投資標的，且會使用其他強化匿名性之技術隱匿其交易行為與實際 IP 位址。當執法機關掌握非法使用者特徵後，可進一步作為偵測疑似非法交易金流與位址，過濾出潛在的比特幣使用者，讓執法人員能由過去反應式偵查模式，轉變為以情資為導向（Intellegence-led）的主動式偵查模式(Irwin & Turner 2018)。

（三） 結合網路與傳統偵查技術：在前述比特幣交易記錄與即時追蹤技術與過濾可疑非法使用者後，理論上可進而聯結到其社會網絡與實體位置等資料，得知其真實身分，但與傳統網路犯罪遭遇的挑戰相同，非法使用者可能會利用暗網（Dark Net）或電腦駭客技術等方式利用他人電腦或轉到國外主機作為跳板，以規避偵查人員發現其身分，因此偵查機關應持續強化網路偵查技術以突破該限制。此外，比特幣主要運用在如毒品買賣、槍枝買賣、性交易、戀童色情影片、恐佈主義等犯罪型態，偵查人員可利用前述主動式偵查情資，輔以時間序列及其他偵查情資，建構出犯罪人的犯罪行為與形態，再與其他偵查線索連結，追查嫌疑人之身分與所在地等(Reid and Harrigan 2013)。例如在絲路案件（Silk Road）案件中，國際刑警組織（INTERPOL）利用前述追蹤技術，鎖定一位涉案之比特幣使用者之帳戶、位址、交易以及電子郵件等資訊，再透過公開情資分析在比特幣論壇發現該使用人的相關訊息，始能追查其身分與涉案情形與事證(Gonzalez 2018)。

伍、 結語

隨著科技發展，傳統國家政府由上至下的現代治理思維，逐漸受到挑戰，比特幣可謂其中最具代表性之後現代產物。此種缺乏中央監管並且配合網路科技之虛擬貨幣，雖有自由、便捷、便宜之優點，但對犯罪問題帶來相當嚴峻之挑戰。在比特幣出現之後，陸續發展出更具實際匿名之虛擬貨幣，即便流通方式尚並如比特幣如此普及，但值得我國執法機關持續關注，本文由比特幣相關犯罪類型與遭遇問題等討論，最後提出管理規範與偵查技術兩個層面之因應架構，期可作為我國因應未來相關虛擬貨幣之參考。

參考文獻

1. 中央銀行、金融監督管理委員會，〈比特幣並非貨幣，接受者務請注意風險承擔問題〉，2013 年 12 月 30 日，http://www.cbc.gov.tw/ct.asp?xItem=43531&ctNode=302，流覽日期：2016 年 7 月 24 日。
2. 金融監督管理委員會，〈金管會再次提醒社會大眾投資比特幣等虛擬商品的風險〉新聞稿，2017 年 12 月 19 日，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201712190002&ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News，流覽日期：2018 年 9 月 24 日。
3. 金融監督管理委員會，〈金融機構 ATM 不得提供比特幣相關服務〉新聞稿，2014 年 1 月 6 日，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201401060003&toolsflag=Y&dtable=News，流覽日期：2017 年 7 月 24 日。
4. 黃敬哲，〈比特幣滲入犯罪行為，台灣將開始監管〉，《科技新報》，2018 年 6 月 15 日，http://technews.tw/2018/06/05/bitcoin-infiltrate-criminal-behavior-taiwan-will-begin-supervision/，流覽日期：2018 年 7 月 12 日。
5. 解聰文，〈Blockchain：Internet 問世以來最具破壞力的發明〉，《火箭科技評論》，2016 年 3 月 18 日，http://rocket.cafe/talks/58431.，流覽日期：2016 年 7 月 1 日。
6. 〈中國 Bitcoin 交易所 Bter 被攻擊，損失約 175 萬美元〉，《企業趨勢》，2015 年 2 月 17 日， http://unwire.pro/2015/02/17/bitcoin-bter-has-been-hacked/news/，流覽日期：2016 年 7 月 15 日。
7. 〈日本虛擬貨幣交易所 Zaif 遭駭客入侵，損失 6,000 萬美元比特幣〉，《財訊快報》，2018 年 9 月 20 日，https://tw.stock.yahoo.com/news/，流覽日期：2018 年 9 月 25 日。
8. 〈比特幣交易平台 Mt.Gox 申請破產保護〉，《BBC 中文網》，2014 年 2 月 18 日，http://www.bbc.com/zhongwen/trad/business/2014/02/140228_bitcoin，流覽日期：2016 年 7 月 15 日。
9. Bryans, D. 2014. "Bitcoin and Money Laundering: Mining for an Effective Solution," *Indiana Law Journal* (89:1), pp. 442-472.
10. Bureau for International Narcotics and Law Enforcement Affairs. 2014. "Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies."
11. Cappella, N. 2016. "$2 Million Lost in Bitcoin Cryptocurrency Hack," in: *The Stack*.
12. Chen, A. 2012. "The Underground Website Where You Can Buy Any Drug Imaginable." Retrieved 7.22, 2016, from http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160
13. Cherry Reynard,〈The 10 most popular cryptocurrencies in 2018〉，《Telegraph》，2018 年 5 月 25 日，https://www.telegraph.co.uk/technology/digital-money/top-10-popular-cryptocurrencies-2018/，流覽日期：2018 年 10 月 1 日。

14. Christin, N. 2013. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," *Proceedings of the 22nd international conference on World Wide Web*: ACM, pp. 213-224.
15. De Filippi, P. 2014. "Bitcoin: A Regulatory Nightmare to a Libertarian Dream," *Internet Policy Review* (3:2), pp. 1-11.
16. Fanusie, Y., & Robinson, T. (2018). *Bitcoin laundering: An analysis of illicit flows into digital currency services*: Center on Sanctions & Illicit Finance memorandum.
17. Federal Bureau of Investigation. 2012. "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity." from https://www.wired.com/images_blogs/threatlevel/.../Bitcoin-FBI.pdf
18. Foley, S., Karlsen, J., & Putniņš, T. J. 2018. "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" Retrieved from https://ssrn.com/abstract=3102645
19. Gonzalez, E. (2018). Cryptocurrencies: Threats and Investigative Opportunities for Law Enforcement. Retrieved from https://is.cuni.cz/webapps/zzp/detail/204125/
20. Hern, A. 2013. "Bitcoin Site Inputs.Io Loses £1m after Hackers Strike Twice." Retrieved 7.14, 2016, from https://www.theguardian.com/technology/2013/nov/08/hackers-steal-1m-from-bitcoin-tradefortress-site.
21. Home Office. 2016. "Action Plan for Anti-Money Laundering and Counter-Terrorist Finance." Retrieved 7.1, 2016, from https://www.gov.uk/government/publications
22. Irwin, A. S., & Turner, A. B. 2018. "Illicit Bitcoin transactions: challenges in getting to the who, what, when and where". *Journal of Money Laundering Control*(just-accepted).
23. Kuzuno, H., & Karam, C. 2017. "Blockchain explorer: An analytical process and investigation environment for bitcoin". Paper presented at the *2017 APWG Symposium on Electronic Crime Research (eCrime)*.
24. Levy, A. 2016. "Bitcoin Gains Validity as Digital Gold after Brexit Vote," in: *CNBC*.
25. Maftei, L. 2014. "Bitcoin-between Legal and Informal," *CES Working Papers* (6:3), pp. 53-59.
26. Middlemas, R. 2016. "Bitcoin Theft: Regulatory Response to an Emerging Technology," in: *Allen & Overy*.
27. Möser, M., Böhme, R., and Breuker, D. 2013. "An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem," *eCrime Researchers Summit (eCRS)*: IEEE, pp. 1-14.
28. OConnell, J. 2015. "Bitcoin Ransoms Are Becoming More Popular in Kidnappings," in: *CCNLA*.
29. Paquet-Clouston, M., Haslhofer, B., & Dupont, B. 2018. "Ransomware Payments in the Bitcoin Ecosystem." *arXiv preprint arXiv:1804.04080*.
30. Penrose, K. L. 2013. "Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws," *North Calronina Banking Institute* (18), pp. 529-551.

31. Ponsford, M. 2015. "A Comparative Analysis of Bitcoin and Other Decentralized Virtual Currencies: Legal Regulation in the People's Republic of China, Canada, and the United States," *Hong Kong Journal of Legal Studies* (9), pp. 29-50.
32. Raeesi, R. 2015. "The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can This Storm Be Weathered?," *Glendon Journal of International Studies/Revue d'études internationales de Glendon* (8:1-2), pp. 1-20.
33. Reid, F., and Harrigan, M. 2013. "An Analysis of Anonymity in the Bitcoin System," *CoRR*), pp. 197-223.
34. Reynard, C. 2018. “The 10 most popular cryptocurrencies in 2018”，in: *Telegraph*（5. 25, 2018）, Retrieved 8.22, 2018, from https://www.telegraph.co.uk/technology/digital-money/top-10-popular-cryptocurrencies-2018/.
35. Ron, D., & Shamir, A. 2013. “Quantitative analysis of the full bitcoin transaction graph” . Paper presented at *the International Conference on Financial Cryptography and Data Security*.
36. Tziakouris, G. 2018. “Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective”. *IEEE Security & Privacy, 16*(4), pp. 92-94.
37. Vasek, M., and Moore, T. 2015. "There’s No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams," *International Conference on Financial Cryptography and Data Security*: Springer, pp. 44-61.
38. Yelowitz, A., and Wilson, M. 2015. "Characteristics of Bitcoin Users: An Analysis of Google Search Data," *Applied Economics Letters* (22:13), pp. 1030-1036.