

國立臺灣大學管理學院國際企業學研究所



碩士論文

Graduate Institute of International Business

College of Management

National Taiwan University

Master Thesis

虛擬貨幣之洗錢防制與打擊資恐

Virtual Currency for Anti-Money Laundering and
Combating the Financing of Terrorism

蔡佳勳

Jia-Shiun Tsai

指導教授：陳聿宏 博士

Advisor: Yu-Hung Chen, Ph.D.

中華民國 107 年 6 月

June, 2018

國立臺灣大學碩士學位論文
口試委員會審定書

虛擬貨幣之洗錢防制與打擊資恐

Virtual Currency for Anti-Money Laundering and
Combating the Financing of Terrorism

本論文係 蔡佳勳 君 (學號 R05724018) 在國立臺灣大學
國際企業學研究所 完成之碩士學位論文，於 民國 107 年 6 月
28 日 承下列考試委員審查通過及口試及格，特此證明。

口試委員：

陳幸長

(指導教授)

王建強

蔡珮玲

所長：

林俊昇

中華民國 107 年 6 月 28 日

謝 辭



在最一開始尋找指導老師之時，由於我一直迷惘於論文的方向與題目，幸好遇見我的指導教授—陳聿宏老師。陳聿宏老師也是在我的研究所生涯中，最感謝的人。老師的專業領域在於經濟學、財務金融學和會計學，但是，一直以來老師都鼓勵學生尋找自身所感興趣的議題。因此，再經過升碩二的暑期實習之後，我決定寫了洗錢防制與打擊資恐的相關議題。

在碩二的這段撰寫論文的期間，每次遇到老師，老師一定不忘關心我論文的進度。老師不但多次詢問我的研究進程，並時常在我遇到撰寫論文的瓶頸時，為我指點迷津、幫助我開拓研究思路。老師嚴謹求實的態度與踏踏實實的精神，不管是面對授課學生或是指導學生，都非常的有耐心，並對我們精心點撥、熱忱鼓勵。讓我不只在論文上，連實習、面試、求職等事情遇到挫折時，也會找老師尋求建議與解決方法。真的非常謝謝老師！！！！

除了我的指導老師之外，也謝謝在我身邊給我鼓勵、催促我論文進度、替我緊張的家人與朋友們。會向我主動討論與我論文有所相關之時事議題的爸爸新聞；在我詞窮時，給予我一排建議詞彙的妹妹字典；照顧著我的身體，並在我很累的時候，遞給我一杯咖啡的媽媽加油站；這段期間幫忙著我查詢國外文獻、分擔著我的喜怒哀樂等大大小小瑣事的朋友充電器們，也非常謝謝你們！！！！

因為有老師的教導與你們的陪伴，我原本難產的論文才得以在後來順利出生，再次謝謝你們！！！！

中文摘要



近幾年，各國都非常地重視洗錢防制與打擊資助恐怖主義（AML/CFT）這個議題。而且，隨著科技的進步與網際網路的快速擴張與廣泛應用之下，世界各國與國際間組織亦開始注意到新的洗錢形式—透過虛擬貨幣為之。

本研究藉由對虛擬貨幣與洗錢防制的基本認識，並探討台灣與其他各個國家對於虛擬貨幣的態度之後，整理出三個與虛擬貨幣洗錢相關之國際案例：

- （一）利用虛擬貨幣進行買賣交易的網路黑市—絲路；
- （二）虛擬貨幣交易平台 Mt. Gox 之比特幣消失事件；
- （三）虛擬貨幣 NEM 外流失竊案。

本文透過參考國際間組織所建議的方法，與上述之個案分析，以尋找解決之道。從上述之個案分析結果，歸納出三項可應用於任何防制虛擬貨幣洗錢案件的通則：

- （一）需急速明確界定虛擬貨幣的法律性質和業務範圍；
- （二）對虛擬貨幣交易所或交易平台進行「實名制」規範；
- （三）強化金融機構在虛擬貨幣交易所的反洗錢責任。

關鍵詞：虛擬貨幣、洗錢防制、洗錢防制與打擊資助恐怖主義、金融體系、
虛擬貨幣交易平台

Abstract



International countries put great emphasis on the issue of AML (Anti-Money Laundering) and CFT (Combating the Financing of Terrorism) in recent years. With the advances in technology and the rapid expansion of the Internet application, the new forms of the money laundering with virtual currencies began to be noticed among the international organizations and countries around the world.

Based on the understanding of virtual currencies and AML, this thesis is aimed at the AML with virtual currencies to discuss the tendency and attitude in Taiwan and other countries. It is also arranged three international cases related AML with virtual currencies, as below:

- (a) Online Trading with Virtual Currency – the black market Silk Road;
- (b) The Disappearance of Bitcoins in the Virtual Currency Trading Platform, Mt. Gox;
- (c) The Theft of Virtual Currency NEM.

By referring the recommended methods from the international agencies and analyzing the above cases, this thesis also concludes three general rules of AML with virtual currencies, as below:

- (a) Defining the legal nature and business scope of the virtual currencies clearly and rapidly;
- (b) Implementing the real-name system for virtual currency exchanges or trading platforms;
- (c) Strengthening the AML's responsibilities of the financial institutions for virtual currency exchanges.

Keywords: virtual currency, anti-money laundering, AML/CFT, financial institutions, virtual currency trading platform

目 錄



口試委員會審定書.....	I
謝辭.....	II
中文摘要.....	III
Abstract.....	IV
第一章 緒論.....	4
1.1 研究背景與動機.....	4
1.2 研究架構與方法.....	5
第二章 虛擬貨幣之定義與歷史.....	6
2.1 貨幣之基本定義.....	6
2.2 虛擬貨幣之背景與種類.....	9
2.3 虛擬貨幣之技術與運作機制.....	13
2.4 各國對於虛擬貨幣之態度.....	16
2.4.1 臺灣.....	16
2.4.2 美國.....	17
2.4.3 日本.....	18
2.4.4 中國.....	18
2.4.5 歐洲.....	19
2.4.6 俄羅斯.....	20
第三章 國際之虛擬貨幣相關洗錢案例.....	23
3.1 利用虛擬貨幣進行買賣交易的網路黑市—絲路.....	23
3.1.1 比特幣之背景與特性.....	23
3.1.2 個案之內容.....	26

3.2 現代版的龐氏騙局？虛擬貨幣交易平台 Mt. GOX 之比特幣消失事件.....	31
3.2.1 世界第一大的比特幣交易平台 Mt. Gox.....	31
3.2.2 個案之內容.....	33
3.3 虛擬貨幣 NEM 外流失竊案.....	36
3.3.1 NEM 之背景與特性.....	36
3.3.2 個案之內容.....	37
第四章 虛擬貨幣相關之洗錢風險.....	42
4.1 洗錢的故事與定義.....	42
4.2 洗錢之方法.....	44
4.3 虛擬貨幣之洗錢風險.....	46
4.4 各國對於虛擬貨幣之洗錢防制.....	47
4.4.1 FATF.....	48
4.4.2 臺灣.....	48
4.4.3 美國.....	49
4.4.4 日本.....	50
4.4.5 中國.....	50
4.4.6 歐洲.....	51
4.4.7 俄羅斯.....	51
第五章 虛擬貨幣相關之洗錢防制.....	53
5.1 針對本文個案之洗錢防範提案.....	53
5.1.1 利用虛擬貨幣進行買賣交易的網路黑市—絲路.....	53
5.1.2 現代版的龐氏騙局？虛擬貨幣交易平台 Mt. Gox 之比特幣消失事件.....	54
5.1.3 虛擬貨幣 NEM 外流失竊案.....	55
5.2 防範虛擬貨幣洗錢行動之提案.....	56
5.3 國際已擬定之可行方案.....	60

5.4 國際新科技.....	62
第六章 結論.....	63
參考文獻.....	65



圖目錄

圖 1、研究架構圖.....	5
圖 2、虛擬貨幣之三種類型.....	12
圖 3、中心化運作架構圖與去中心化運作架構圖.....	14
圖 4、傳統隱私模式與新隱私模式.....	25
圖 5、Mt. Gox 簡要事件時間線.....	32
圖 6、Coincheck 之 NEM 虛擬貨幣被盜的紀錄.....	38
圖 7、CDD 客戶審查之流程圖.....	61

表目錄

表 1、前五大虛擬貨幣之相關統計資料.....	15
表 2、國際間對於虛擬貨幣屬性之看法.....	21
表 3、國際間對虛擬貨幣交易平台之監管情形.....	52



第一章 緒論

1.1 研究背景與動機

近幾年各國非常地重視洗錢防制與打擊資助恐怖主義 (AML/CFT) 這個議題。且目前各與國際組織間，也尚還在調整關於此議題之法律規範與監管措施。然而，科技的進步與隨著虛擬貨幣的快速擴張與廣泛應用，世界各國與國際間組織開始注意到新的洗錢形式—透過虛擬貨幣為之。

台灣即將在 2018 年下半年接受亞太防制洗錢組織 (Asia/Pacific Group on Money Laundering, 簡稱 APG) 的洗錢防制成效相互評鑑。¹而未來在 APG 評鑑時，非常有可能將金融科技和虛擬貨幣產業列入洗錢風險評估之範圍，如果台灣未能提出有效抵減相關風險的規範及措施，將未能順利通過評鑑，而被列為洗錢高風險國家，在國際金融及貿易上也將可能會面臨到國際制裁或抵制等類似的不利處境【46】。

目前世界各國與國際的法律規範中，尚未有針對虛擬貨幣的管制標準，亦尚未有一套得以防範虛擬貨幣洗錢的正式措施與方法。因此，本研究希望可以透過國際間組織所建議的可行辦法，與虛擬貨幣洗錢相關之個案分析來提出解決方案，並試著從其相同之處，找出可應用於任何防制虛擬貨幣洗錢案件的通則。

¹ 「亞太防制洗錢組織」(Asia/Pacific Group on Money Laundering, APG) 成立於 1997 年 2 月，為亞太地區防制洗錢犯罪之多邊機制，目前有 41 個會員，秘書處設於澳大利亞雪梨。1997 年 2 月在泰國曼谷召開之 APG 第 4 次籌備會議，決議以「法律管轄區」(jurisdiction) 為會員單位。台灣自 1998 年 APG 第 1 屆年會加入成為會員，並於 2011 年起開始參與提升其太平洋島國會員及觀察員在防制洗錢及打擊資助恐怖份子能力之計畫。APG 主要功能在於：評估其成員遵守反洗錢／打擊資助恐怖主義標準的程度；給予技術援助和培訓；對洗錢和恐怖主義融資的方法和趨勢進行研究和分析；為國際 AML / CFT 政策制定做出貢獻等全球參與。(資料引用來源：apgml.org -APG HISTORY & BACKGROUND)



1.2 研究架構與方法

本研究透過對虛擬貨幣的基本了解、並討論台灣與其他各個國家對於虛擬貨幣的態度之後，直接先帶出三個國際上與虛擬貨幣相關之洗錢個案：利用虛擬貨幣進行買賣交易的網路黑市—絲路；現代版的龐氏騙局？虛擬貨幣交易平台 Mt. Gox 之比特幣消失事件；虛擬貨幣 NEM 外流失竊案，以勾勒出虛擬貨幣與洗錢行為的關連性。

接著，再透過對洗錢犯罪的基本認識，與探討台灣與國際間對於虛擬貨幣之洗錢的防制狀況後，採用比較與分析的方法，進而針對個案提出其各自適合的洗錢防制提案，並歸納出有助於虛擬貨幣之洗錢防制與打擊資助恐怖主義的通則。

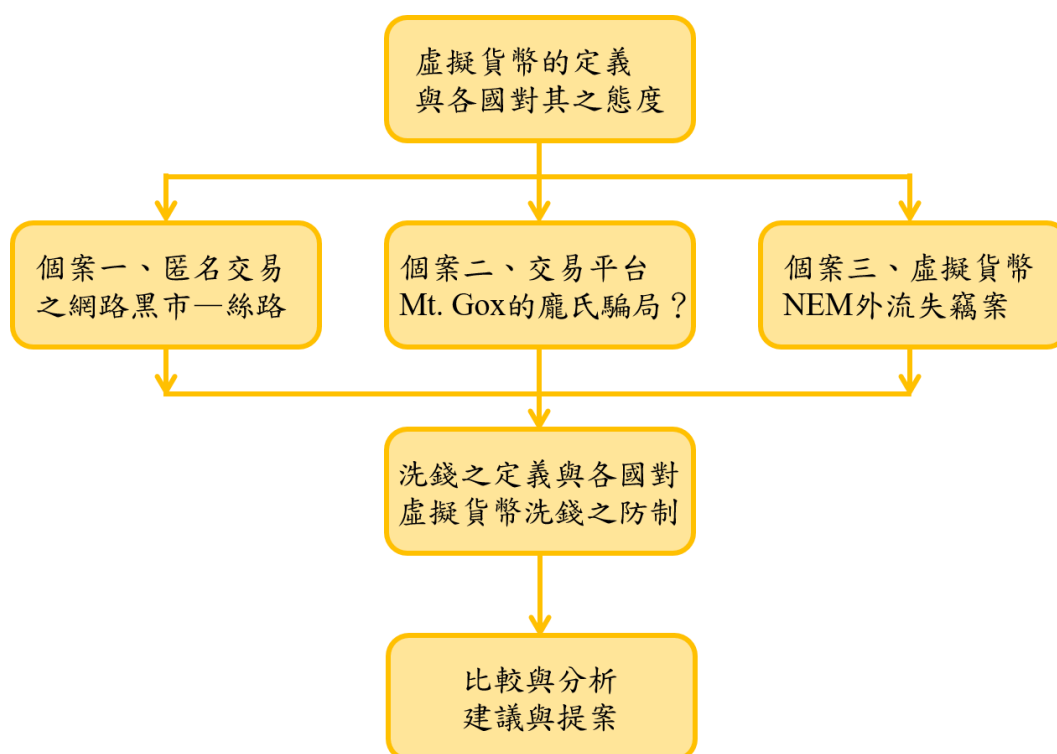


圖 1、研究架構圖



第二章 虛擬貨幣之定義與歷史

2.1 貨幣之基本定義

根據貨幣銀行學對於貨幣之基礎概念，它是有助於提升了人與人之間商品交易效率的工具。其中，「通貨」是指一個國家的中央銀行機構所發行的紙鈔及硬幣，為一般民眾最為熟悉且最普遍的貨幣型態之一。但是，根據統計，使用通貨來完成的商品交易的額度僅占所有交易總額的極小比例，現今一般日常的小額付款等交易，已一改以往用現金的消費方式，而多半使用信用卡等塑膠貨幣、甚至是像 Apple Pay、Android Pay、WeChat Pay、支付寶等移動支付的新型電子貨幣來替代；而金額龐大的財貨交易或金融工具交易則會選擇如匯款等使用安全且迅速的方式來完成。因此，以通貨來代表貨幣並不是一種完整的說法，且經濟學上亦不會單單以通貨或現金等來簡單描述貨幣的實質內涵【32】。

「貨幣」這一詞目前尚未有一個公認且統一的定義，當人們論及貨幣時，通常隱含有多種不同的意義，可能是上一段文字中所闡述到的通貨或是現金，也可能是支票、金融卡等不同形式的貨幣。一般來說，貨幣必須具備四大特性及三種功能【25】。

貨幣的四大特性：

一、普遍的接受性 (General Acceptability)

此為貨幣很重要的基本特性之一，越能被大眾所接受，其貨幣性 (money-ness) 也越好。在以前尚未有貨幣的社會，因此牛、羊、稻米等物品便可能在某個時期為一般民眾可接受做為交易的工具；曾在十九世紀及二十世紀盛行的金本位制度，黃金鑄造成的金幣、將金幣溶成的金屬塊、甚至是銀幣，在當



時便為一般民眾可接受的交易工具。²從以上兩個例子，我們也可以看出其所指的交易工具，已具備交易媒介之貨幣功能。

二、易於辨識

為了達到普遍的接受性，能簡易明確的辨識即是讓一般民眾所能接受之特性之一，能夠分辨貨幣其真偽，以避免使用上混淆之困擾。但至今，私人或犯罪組織偽造紙幣的事件已屢屢發生，為了維持這項特性、避免偽造，紙幣採用了許多防偽措施，像是使用專用的特殊紙張、應用膠版凸印、防偽水印、磁性油墨、金屬安全線、紫外線螢光記號等技術。

三、低分割成本 (Division Cost) 且品質統一

為了要成就貨幣之計價單位和交易媒介的功能，能廣泛地成為衡量各種價值不同財物貨品的單位並用其當作交換工具，貨幣應要可於分割為不同單位，常見的方式是將每個基本貨幣單位再分成更小的「輔助貨幣」，用以輔助貨幣面額較大的流通，供日常小額交易或找零之用，輔幣為主幣的 1/100 是最常用的比例，舉例來說，在美國 100 分等於 1 元。另外，不管基本貨幣或是輔助貨幣，其品質應為一致，以避免一般大眾儲存較佳品質貨幣，導致產生劣幣驅逐良幣之現象。³

四、低攜帶成本 (Carrying Cost)

貨幣應易於攜帶、保存及轉移，才能廣泛地被用於交易等的經濟活動。

² **金本位 (Gold Standard)** 是於 19 世紀中期開始盛行的一種以黃金為本位幣的貨幣制度，每單位的貨幣價值等同於若干含重量的黃金（即貨幣含金量）。在歷史上，曾有過三種形式的金本位制：金幣本位制、金塊本位制、金匯兌本位制，其中金幣本位制是最典型的形式，就狹義來說，金本位制即指該種貨幣制度。（資料參考來源：wiki.mbalib.com -金本位制）

³ **劣幣驅逐良幣 (Bad money drives out good)** 是一個經濟學定律。消費者保留儲存成色高，也就是貴金屬含量高的貨幣 (undebased money)，在市面使用成色低的貨幣 (debased money) 進行市場交易，而使得在民間流通的大多為劣幣，良幣則較少見於世。此定理後來也被廣泛用於非經濟學的層面，人們用這一法則來泛指價值不高的東西會把價值較高的東西擠出流通領域，主要指假冒劣質產品在多種渠道向正牌商品挑戰。例如說，在軟體市場上的經濟秩序和法規約束尚不完善時，或者不能很好協調工作時，盜版軟體影響正版軟體的製作、銷售等，從而危害軟體業健康發展的趨勢。這種趨勢雷同於「劣幣驅逐良幣」，可稱為「盜版驅逐正版」，是一種非正常的市場狀態。（資料參考來源：wikipedia.org -劣幣驅逐良幣）



貨幣的三大功能：

一、計價單位（Unit of Account，亦可稱為價值標準）

貨幣作為衡量價值的標準成立後，貨幣本身就可以以自己為標準，與其他商品進行量的比較，藉此將商品的價值轉化為貨幣所衡量出來的價格，財物商品便能以明確簡單的價格來標識。就經濟學角度而言，此計價單位的概念便可以用來做為物品生產以及交換的比率，生產者得以明確計算生產之成本；消費者可以衡量效用及成本，便形成經濟學上的供需機制，進一步藉由貨幣價值的訊息形成、改變經濟行為等。

二、交易媒介（Medium of Exchange）

如前段貨幣的四大特性與計價單位功能所述，不論以何種形式存在，貨幣若具備普遍接受性、可以被分割和轉移等特性，且具有衡量價值標準的功能，即可當作財物商品交換之工具。貨幣若具有計價單位及交易媒介功能，生產者除了可明確計算生產之成本，也得以進而以促進專業化及分工化的生產模式，增加生產之效率；而消費者除了得以衡量效用及成本，也可以以貨幣支付完成財貨物品之交換需求。過去在以物易物制度之下，由於並沒有一個大眾能夠普遍接受的交易媒介，因此交換物品時，有一方很有可能得到自己並不是很想要的物品（此為單方的欲望重合），貨幣具備交換媒介功能的重大意義在於可以達成雙方的欲望重合，不僅使同等同效益的價值雙向流動，也得以降低以往以物易物制度所衍生的搜尋、驗證等交易成本，進而發揮生產消費的效率，促進了經濟社會的發展。

三、延期支付的標準（Standard for deferred payment）

又稱為債務的標準。過去以物易物制度的社會因須透過實物借貸方式，債權債務關係難以計算也不易形成。然而，有了得以做為計價單位貨幣的出現，使債務的本金與利息所產生的計價單位問題有了共同的標準，以助於現代債務制度的建立與信用經濟的發展。此延期支付功能需要另外分拆出來提及，是因為當債務是以貨幣來計算時，其價值會因為通貨膨脹和貨幣貶值而減低。



在舊的定義當中，貨幣還有一項價值的儲藏（Store of Value）的功能，這項功能是為了使消費者可將其一部分的個人所得儲藏供作為未來消費之用，無須在獲得通貨時全數使用完畢。貨幣僅為眾多價值儲藏工具之一，許多金融投資資產及實質資產亦具備價值儲藏之功能，一般來說，貨幣為一般民眾所傾向選擇的價值儲藏工具，做為價值儲藏的風險也是最低的。但是，貨幣的實質價值可能會因為通貨膨脹、物價高低而受到影響，長期下來，價值儲存功能並不及其他三項功能重要且恆定【25】。

貨幣的形式從過去貝殼、糧食等自然物的商品貨幣，金屬加工後的紙張與硬幣，到現在各種的貨幣種類，包括通貨、各類儲蓄存款、信用卡以及移動支付的塑膠、電子貨幣等。而本篇論文主要探討的正是現在網際網路時代與電子交易普及的經濟中，所衍生出一種漸漸取代實體貨幣的貨幣形式—虛擬貨幣。

2.2 虛擬貨幣之背景與種類

由於網際網路、電腦通信技術、資料庫技術等的發展，造就了基於網路空間的虛擬市場。虛擬貨幣（virtual currency、virtual money）指非真實的貨幣，是在連接現實的虛擬空間中，可以進行購買商品和服務、投資等將近可以與現實貨幣達到同等目的的貨幣。因此，具有貨幣銀行學定義的交易媒介和記帳單位之貨幣功能。

起初，銀行所發行如信用卡等的電子貨幣，即是一種「偽虛擬貨幣」。這一類的電子貨幣具有虛擬貨幣的數字化、符號化之形式，也突破了原本法定通貨貨幣的特性，像是電子貨幣可以不需透過政府的中央銀行，僅透過一般私人機構銀行也可發行，且就流動性而言，銀行的電子貨幣遠遠超越一般的通貨【25】。



再來，我們非常熟悉的股票、衍生性金融工具等市場，其本質是虛擬的。一般貨幣市場的流通速度，如利率是由各國的中央銀行所直接決定的，而股票市場和衍生性金融工具市場最大的不同之處在於，它們建立在國際的景氣狀況、國家的經濟發展和公司的信用與營利收入等廣泛的訊息與人們對於市場的信心之上，並且透過實體業務的操作，形成了規模龐大、為大眾所認同且受到政府法律規範的一個虛擬市場，因此，它也可以被當做是一個最為以現實為基礎的「前虛擬貨幣經濟市場」【25】。

參考歐盟央行（European Central Bank，簡稱 ECB）於 2012 年 10 月 29 日所提出的「虛擬貨幣架構報告（Virtual Currency Schemes）」，該報告將虛擬貨幣分為三種類型：封閉性虛擬貨幣架構、單向流通性虛擬貨幣架構和、雙向流通性虛擬貨幣架構【10】。⁴

一、封閉性虛擬貨幣架構（Closed virtual currency schemes）

所謂封閉性虛擬貨幣架構是指設計上與真實世界、實體經濟幾乎無連結，也被稱作為「遊戲內」架構（“in-game only” schemes）。使用者於支付預定費用後，依據在該虛擬社會中角色的表現可以賺取虛擬貨幣。而這些虛擬貨幣僅能夠用於購買該虛擬社會中之虛擬商品與服務。理論上，這類型的虛擬貨幣不能在虛擬社會之外進行交易，意即無法兌換成為真實世界中之貨幣、商品或服務。

網路線上遊戲，例如著名的網路角色扮演遊戲 World of Warcraft 魔獸世界的 WoW Gold，是此款遊戲使用的虛擬貨幣。玩家有非常多的機會可以在遊戲中賺取到更多的 WoW Gold，而這些 WoW Gold 作為在遊戲中交易買賣遊戲的

⁴ 資料引用來源：European Central Bank (2012), Virtual currency schemes OCTOBER 2012, pp. 13-15.

裝備與道具，主要是為了讓玩家去裝備自己遊戲中的角色以達到更高的等級。且設計此遊戲的公司 Blizzard Entertainment 也明確制定了條款，嚴禁在現實世界中購買和出售 WoW Gold。



二、單向流通性虛擬貨幣架構 (Virtual currency schemes with unidirectional flow)

單向流通性虛擬貨幣架構指得以特定匯率，透過現實世界的貨幣直接購買兌換，但經兌換後不得再轉換回原始的實際貨幣。而兌換的規則條件則是由該單向流通性虛擬貨幣架構之創造者所建立。此架構的虛擬貨幣除了可以用於購買虛擬社會中的商品或服務之外，有些也得以購買現實社會中之商品和服務。

此種架構為現今大多數網路相關產業之經營者所廣泛使用。例如 Facebook 於 2009 年所推出的虛擬貨幣 Facebook Credits (FB)，其可以使用戶購買在 Facebook 平台上任何應用程式中的虛擬商品。以 FB 1 = 0.10 美元的匯率兌換 Facebook Credits，若為其他國家的貨幣，則使用每日匯率轉換為美元、透過信用卡、PayPal 帳戶等各種其他支付方式來購買此貨幣；Nintendo 任天堂的虛擬貨幣 Nintendo Points 也為這一類的架構，Nintendo Points 可以在任天堂遊戲中的商店獲得，也可以透過實體零售店購買 Nintendo Points Card，且這些 Nintendo Points 都不能轉換回實體貨幣。

三、雙向流通性虛擬貨幣架構 (Virtual currency schemes with bidirectional flow)

使用者得以根據匯率真實世界貨幣之買賣虛擬貨幣。按其與真實世界的互通性，此架構的虛擬貨幣與其他任何的可轉換貨幣雷同，且該類型允許使用者購買包含虛擬和真實世界兩者的商品或服務。

舉例言之，Second Life 虛擬世界中使用者可以透過虛擬貨幣 Linden Dollars (L\$) 創建「頭像」(“avatars”)。用戶可以在 Second Life 中以 Linden Dollars 互相買賣商品和服務，以創造出有個人特色的角色。根據與現實世界

的匯兌比率，Linden Dollars 可用美元與其他國家的貨幣、透過信用卡、PayPal 帳戶等支付方式來購買此貨幣，用戶也可以出售其多餘的 Linden Dollars 以換取美元；除了 2013 年來，最為人所知的比特幣（Bitcoin）之外，尚有新經幣（NEM）、小蟻股（neo）、以太幣（eth）等虛擬貨幣，在眾多交易撮合的第三方平台上，得以法幣兌換，也得以將之兌換回法幣。

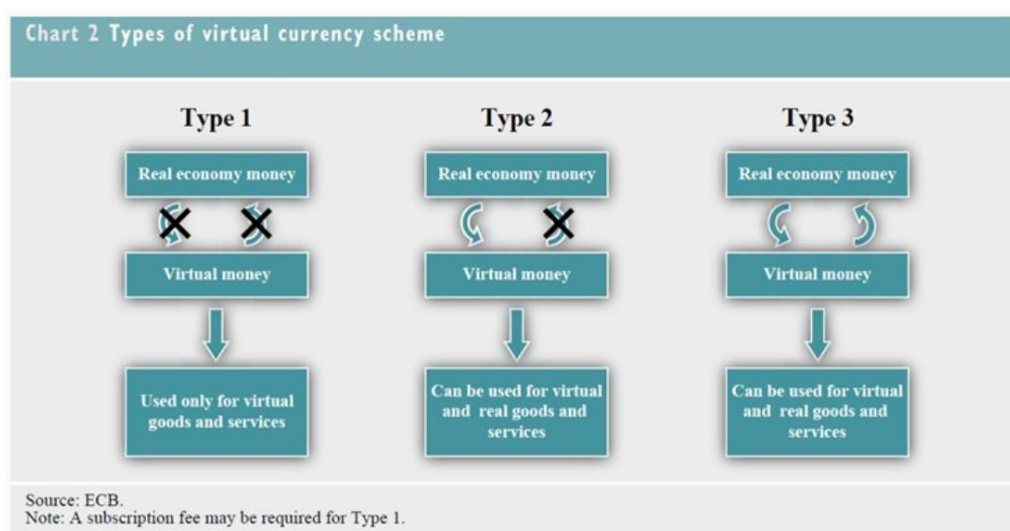


圖 2、虛擬貨幣之三種類型

圖片來源：ECB, Virtual Currency Schemes OCTOBER 2012, pp. 15.



2.3 虛擬貨幣之技術與運作機制

透過與電子貨幣的些微比較，來了解虛擬貨幣的運作機制：虛擬貨幣與電子貨幣的價值同樣以數位的形式來儲存，惟絕大部分的電子貨幣是法定貨幣的數位儲存形式；虛擬貨幣則為非法定貨幣的數位儲存形式，須透過兌換程序才能取得法定貨幣。電子貨幣均為中心化機制，例如卡片形式的悠遊卡，網路形式的電子支付機構儲值帳戶；虛擬貨幣可以中心化或去中心化機制運作，去中心化機制的典型代表就是比特幣，比特幣等虛擬貨幣使用加密技術，因此又稱做加密貨幣 (Cryptocurrency)【30】。

虛擬貨幣的交易設計乃採用 P2P 技術，可降低交易成本，並具匿名性。⁵為了避免偽造，虛擬貨幣的產生與消費等每筆交易，都會透過 P2P 分散到全球的網路中，可避免傳統電子貨幣將資料和程式儲存在中央伺服器，而易受外來駭客攻擊之風險。不同於現行買賣雙方需要透過結算所 (clearing house) 等中央機構或中介機構來集中處理的金融交易架構，意即「一對一」的作業模式，虛擬貨幣沒有中介機構或中央機構來負責維護帳簿，其採行的是分散式帳本技術，由每一個節點(Node)負責帳簿的維護，並保有一份所有交易資料的帳本，因而稱為去中介化 (disintermediated) 或去中心化 (decentralized) 的貨幣系統【30】。⁶

⁵ **P2P 技術**：Peer-to-Peer 的意思是「點對點」、「對等連接」、「對等網路」，是無中心伺服器。對等網路的每個用戶端既是一個節點 (Node)，也具有伺服器 (Server) 的功能，任何一個節點無法直接找到其他節點，必須依靠用戶群 (peers) 進行資訊交流。此技術的作用在於，得以降低資料遺失的風險。(資料參考來源：wikipedia.org -對等網路)

⁶ **分散式帳本技術 (Distributed Ledger Technology, DLT)** 是運用 P2P 技術，在多部電腦和多個地點共享和同步處理的交易資料庫，不需集中控管。每一方都擁有同一份記錄，這份記錄會在有新增資料時立即自動更新。(資料參考來源：SAP Leonardo -區塊鏈與分散式帳本技術)

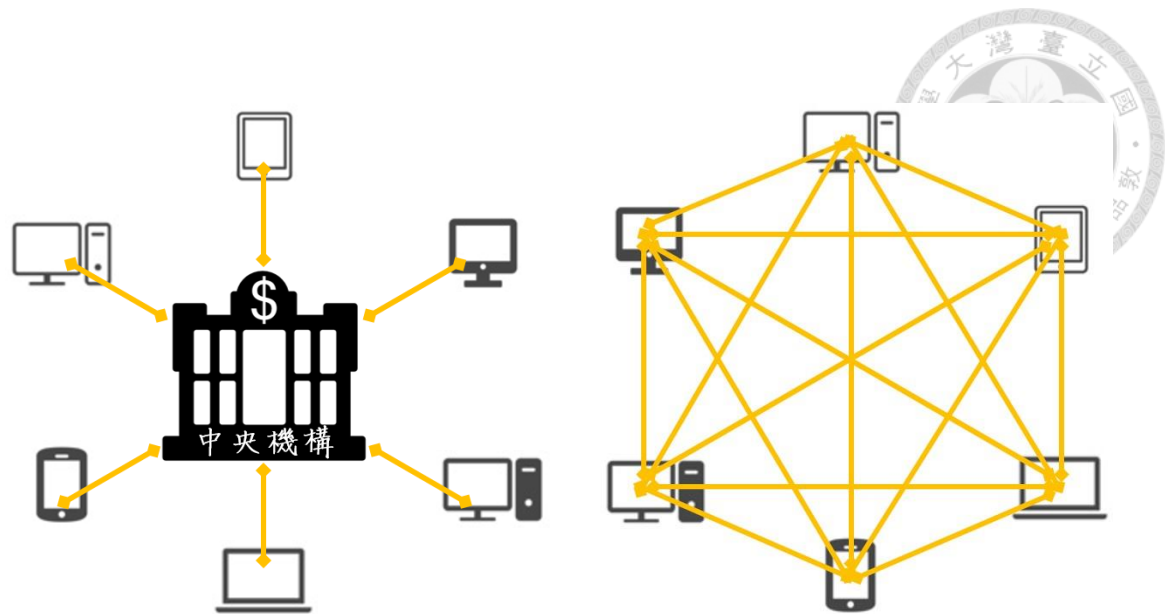







圖 3、中心化運作架構圖與去中心化運作架構圖

截至 2018 年 3 月 1 日止的統計，目前全球虛擬貨幣的總市值約 4,413 億美元。雖然，全球的虛擬貨幣多達 1,500 種，但首宗問世的虛擬貨幣——比特幣，市值約占所有種類之虛擬貨幣四成，以約 1,761 億美元的市值，及約 1,689 萬單位的流通量居首。因此，由於虛擬貨幣的總價值多仰賴比特幣支撐，虛擬貨幣總價格的波動亦與比特幣的價格波動緊緊相扣，市場參與者也大都以比特幣，作為對虛擬貨幣發展的指標。下表為統計截至 2018 年 3 月的前五大虛擬貨幣之相關統計資料【47】：



表 1、前五大虛擬貨幣之相關統計資料

虛擬貨幣種類	市值 (美元)	價格 (美元)	流通量	市值占比
 Bitcoin (比特幣, BTC)	\$1,761 億	\$11,280	1,689 萬	約 40%
 Ethereum (以太幣, ETH)	\$840 億	\$849.38	9,797 萬	約 19%
 Ripple (瑞坡幣, XRP)	\$354 億	\$0.9034	390 億	約 8%
 Bitcoin Cash (比特幣現金, BCH)	\$205 億	\$1,246.5	1,699 萬	約 5%
 Litecoin (萊特幣, LTC)	\$205 億	\$208.22	5,547 萬	約 2%

資料來源：coinmarketcap.com

虛擬貨幣的產生多數藉由挖礦(Mining)而來,有些則是由科技公司自己發行。比特幣並不依靠特定的貨幣機構發行,而是 P2P 技術中的用戶端電腦以一套編碼系統為基礎,在完成複雜的特定數學問題計算後而產生的,任何人只需要運行特定的軟體即可以參與比特幣的製造,上述的方式即稱之為「挖礦」,而因為電腦程式控制它的最終總發行量為 2,100 萬個,因此不會有發行量增加導致通貨膨脹的問題。在上表中所提及的瑞坡幣,則是 2013 年 Ripple 公司發行 1,000 億單位(後續不再增發),逐步售予市場參與者。另外,無總量上限、第二大虛擬貨幣—以太幣是以部分公司自己發行,部分挖礦之方式產生,且由礦工挖礦所取得的新虛擬貨幣,每年不得超過 2014 年公開銷售量 7,200 萬單位之 25%【47】。



2.4 各國對於虛擬貨幣之態度

虛擬貨幣可以在虛擬空間中，進行購買商品和服務、投資等行為，表面上具有交易媒介和記帳單位的貨幣功能。但是，將虛擬貨幣與法定貨幣及一些主要的金融商品做比較，大部分虛擬貨幣和比特幣的價格波動皆非常大，並不適合充當計價單位，且其風險、交易投機性很高，只有僅少數虛擬貨幣用來當做交易媒介。因此，虛擬貨幣很難成為貨幣替代品，迄今多數國家亦認定其非為貨幣【32】。

2.4.1 臺灣

2015 年發生香港富商在台被綁架，且綁匪要求以比特幣交付贖金之事件時，台灣金融監督管理委員會（以下簡稱金管會）表現強硬的態度，強調比特幣在台是不合法的支付工具；而中央銀行則認為比特幣的價值不穩定，並不具記帳單位及價值儲存等功能，缺乏真正通貨的特性，也不具法償效力，因此將比特幣視為虛擬商品【5】。

台灣目前尚未針對虛擬貨幣制定任何的專法，而金管會於 2017 年 12 月 19 日發出的新聞稿中，強調虛擬貨幣為高風險、高投機性的商品，且由於近來的價格波動極大，提醒社會大眾務必要審慎評估投資風險。此外，該新聞稿亦特別重申要求銀行等金融機構應配合「金融機構不得參與或提供虛擬貨幣相關服務或交易」的落實辦理【37】。由此可知，台灣對於虛擬貨幣交易的態度仍趨於保守【28】。

虛擬貨幣之法律規範雖尚未發展成熟，但在金管會及中央銀行將其視為「虛擬商品」的考量之下，主管機關仍可以以其他現有的法規來管制虛擬貨幣的交易活動。例如，使用者若有糾紛的產生時，乃可適用消費者保護法；若遇有人利用虛擬貨幣洗錢則是以洗錢防制法處理【28】。



2.4.2 美國

美國對虛擬貨幣一直維持非常謹慎，甚至有些抵制的態度【1】。在比特幣誕生初期，美國相關部門的一份文件中，認為比特幣是一種典型的虛擬貨幣，不具備實際貨幣的全部屬性和法定貨幣地位。於美國時間的 2018 年 2 月 6 日上午，美國參議院舉行對於加密貨幣監管之聽證會。這場聽證會值得注意的是，整體看來美國證券交易委員會（SEC）主席 Jay Clayton 和美國商品期貨交易委員會（CFTC）主席 J. Christopher Giancarlo，兩位主席對於加密貨幣的態度並未一味地否認，而是表示需要尋求更多立法且合理地監管【13】。

另外，美國中央與地方各個政府與機關對於虛擬貨幣的看法與著重點也不太一樣。加州政府於 2014 年 6 月，通過了《數字貨幣合法化法案》（簡稱「AB-129 法案」），其法案之立法目的在於修改現行法律，以確保使用各種形式的替代貨幣，包括數字貨幣（digital currency）、積分（points）、優惠券（coupons）或其他有貨幣價值的東西（other objects of monetary value），購買商品和服務或匯款時不會觸犯法律。該法案的成立，不但明確地承認虛擬貨幣的合法地位【33】。之後，更在加州的金融法下新增專門規範虛擬貨幣企業的章節，為虛擬貨幣業務帶來了制度確定性；紐約州金融服務管理局也在 2015 年 9 月接受 Circle Internet Financial 公司的申請，讓它成為紐約第一家可以提供虛擬貨幣服務的合法業者；而美國中央的代表—商品期貨交易委員會則聲明，期貨交易法對於商品的定義相當廣泛，因此將比特幣與其他的虛擬貨幣定義為商品而不是貨幣，並且比照石油、黃金、小麥等商品納進政府課稅與管制範圍【47】。



2.4.3 日本

日本為比特幣與區塊鏈技術的發源國，因此日本政府對比特幣等虛擬貨幣向來持正面的態度，也對於其發展十分重視。⁷經過 2016 年日本金融監管機構(FSA)，將比特幣等虛擬加密貨幣視為與現金等價的貨幣之立法修正建議研究，日本內閣正式簽署的《支付服務法案修正案》，於 2017 年 4 月正式承認數位貨幣的經濟地位，也將比特幣視為合法的交易工具【40】。

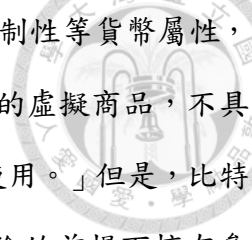
日本監管機構與交易所也起草和擬定相關的政策，以期望大力推動虛擬貨幣的發展。截至 2017 年 5 月的統計，日本比特幣的交易已經占全球交易量的 34.46%，每日交易量超過 1.2 億美元。而 2017 年 7 月開始免除比特幣交易 8% 的消費稅之法案，導致日本市場的比特幣交易量更高達到全球的 51%，正式取代美國成為最大的市場【49】。也估計原本只有約 4,500 家接受比特幣付款的商店，將可能迅速擴展到 26 萬家以上的店家採用比特幣的支付功能。而就在 2018 年年初，日本東京房地產公司 Yitanzi 以 547 枚比特幣（價值約新台幣 1.7 億元）出售一棟商業大樓，是日本首宗以數位貨幣交易的建案，且其他等待出售的建築物也皆可採用比特幣的交易【9】。

2.4.4 中國

2013 年中國人民銀行、工業和信息化部、中國銀行業監督管理委員會、中國證券監督管理委員會和中國保險監督管理委員會，中國為首的五家官方機構聯合發佈了《關於防範比特幣風險的通知》（以下簡稱《通知》）。⁸《通知》明確了比特

⁷ 區塊鏈 (blockchain、block chain) 技術起源於中本聰的比特幣，作為比特幣的底層技術。是一種不依賴第三方、通過自身分散式節點進行網路數據的存儲、驗證、傳遞和交流的一種技術方案。從金融會計的角度，可以把區塊鏈技術看成是一種分散式、開放性、去中心化的大型網路記帳簿(資料庫)，任何人都可以在任何時間採用相同的技術標準，加入自己的信息以延伸區塊鏈，而系統亦會將這段時間內所更新的內容發給系統內所有的其他人以進行備份，使得系統中的每個人都能夠有完整且相同資料的帳簿。(資料參考來源：wiki.mbalib.com-區塊鏈)

⁸ 資料參考來源：中華人民共和國中央人民政府(2013)，人民銀行等五部委發布關於防範比特幣風險的通知(銀發〔2013〕289號)。



幣的性質，認為比特幣不是由貨幣當局發行，不具有法償性與強制性等貨幣屬性，並不是真正意義的貨幣【1】。「從性質上看，比特幣是一種特定的虛擬商品，不具有與貨幣等同的法律地位，不能且不應作為貨幣在市場上流通使用。」但是，比特幣交易作為一種互聯網上的商品買賣行為，普通民眾在自擔風險的前提下擁有參與的自由。《通知》亦要求，各金融機構和支付機構不得以比特幣為產品或服務定價，不得買賣或作為中央對手買賣比特幣，不得承保與比特幣相關的保險業務或將比特幣納入保險責任範圍，不得直接或間接為客戶提供其他與比特幣相關的服務等。

但是，中國政府與企業則表現出濃厚的興趣並支持區塊鏈技術的發展。像是，廣東省佛山市禪城區推出「智信城市」計劃，是全中國首個探索區塊鏈政務應用的縣區；中國眾安科技公司宣布將推出 blockchain 生產系統，將區塊鏈技術應用到整個食品供應鏈【24】。

雖然中國也是比特幣交易量龐大的地區，但中國政府對虛擬貨幣的態度比美國更加保守、更加抵制。除了也將比特幣與其他的虛擬貨幣定義為商品而不是貨幣，甚至對虛擬貨幣持續嚴格監管。於 2017 年 9 月封鎖虛擬貨幣的交易活動，叫停所有發行虛擬貨幣的融資活動，也要求所有虛擬貨幣交易所停止在中國的所有交易活動，中國政府更多次抨擊虛擬貨幣。

2.4.5 歐洲

歐洲議會起草的一項虛擬貨幣報告強調，虛擬貨幣與區塊鏈技術可以大幅降低交易支付、資金轉移等成本，同時提高支付系統的速度和效率，也可追蹤記錄交易，不但帶給消費者眾多的福利，對於經濟發展也有著重要的貢獻，更有助於以防不法的行為【1】。



德國聯邦財政部 (GFMM) 在 2013 年 8 月就發出聲明，認為虛擬貨幣可屬於私人的金錢 (private money) 或是記帳單位，承認比特幣的貨幣與稅收地位，是世界第一個正式認可比特幣的國家。而歐盟最高法院也已於 2015 年 10 月，正式宣佈比特幣是貨幣而不是商品【47】。雖然，比特幣的貨幣地位被正式承認，但至今歐盟尚未針對虛擬貨幣進行立法，謹多次以新聞稿的形式提醒大眾虛擬貨幣的高風險以及不確定性【28】。

對於比特幣等的虛擬貨幣與區塊鏈技術之高速發展，歐洲中央銀行、各大銀行與科技公司抱持著非常開放的態度，也已計劃諸多相關技術的銀行業務並涉獵多個項目中【1】。

2.4.6 俄羅斯

俄羅斯政府與相關部門不看好比特幣等虛擬貨幣，甚至自 2014 年以來採嚴格禁止的態度，除了宣佈全面禁用以外，其財政部甚至還有傳出研擬針對進行虛擬貨幣交易最高可處 4 年有期徒刑的提案【47】。然而，俄羅斯對區塊鏈技術卻是充滿熱情。

目前，俄羅斯對於加密貨幣交易的禁止有所緩和，對於交易監管的態度也有所轉變。俄羅斯中央銀行亦聲稱，為了要分析金融市場中的先進技術和創新技術，將建立工作小組。而幾個首要之研究對象包含區塊鏈技術、移動技術、支付技術等領域【1】。⁹

⁹ 移動技術 (Mobile Technology、Mobile Action Technology) 即是行動運算技術。舉凡一切可供使用者在「移動的行為 (非長時間在定點)」中，能如常使用裝置的技術。在這個定義下，筆記型電腦、行動電話、藍芽耳機、紅外線印表機、PDA、GPS、無線基地台...等還在陸續增加中的相關系列產品，都是屬於行動運算技術所衍生的產品。(資料參考來源：answers.yahoo.com-行動運算技術是什麼??)



下表為統整幾個重點國家對於虛擬貨幣／比特幣的屬性之看法：

表 2、國際間對於虛擬貨幣屬性之看法

屬性	國家
法定貨幣	無
私人貨幣	德國、歐盟央行（ECB）
金融／普通商品	台灣、美國、日本、中國、法國、加拿大、英國、澳洲、印度、荷蘭、瑞典
非法商品	俄羅斯、泰國、印尼

資料來源：新時代的貨幣銀行學概要（二版），李榮謙編著

綜合上述我們可以看出，目前至今，沒有任何國家承認虛擬貨幣為法定貨幣，且世界各國對於虛擬貨幣的看法與態度皆有所不同，大致上可分為三種：第一，對比特幣等虛擬貨幣採支持態度，也推動各種政策推以促進行業發展，這類型以日本、德國、加拿大等國家為代表；第二，抱持著較為謹慎的態度，以台灣、美國、中國、英國等國家為代表，而其中每個國家的謹慎程度也存在著不小的差別；第三，以俄羅斯、泰國等國家為代表，對虛擬貨幣表示抵制的態度。

然而在區塊鏈技術方面，隨著比特幣的知名度提高，各界亦開始關注到比特幣所應用的底層技術－區塊鏈。虛擬貨幣因為價格波動幅度非常不穩定，無法成為普遍接受的交易媒介；且多半採用匿名交易，容易淪為不法洗錢工具；再加上，其高投機性的風險，若價格受到人為的操控，很可能會有泡沫化的趨勢，因此其未來發展的可能性是有所限制的。但是，區塊鏈技術所應用的分散式帳本技術，具有資訊

可分散、公開揭露、交易紀錄可追蹤及不易竄改等特性，做為一種新興技術是非常具有發展與創新應用的潛力，因此世界大部分國家都認為區塊鏈技術所帶來的影響是無法被忽略的，且表示接受並支持區塊鏈技術的發展。



第三章 國際之虛擬貨幣相關洗錢案例



3.1 利用虛擬貨幣進行買賣交易的網路黑市—絲路

3.1.1 比特幣之背景與特性

當提及虛擬／加密貨幣時，最容易讓人聯想到、最具代表性的便是**比特幣 (Bitcoin)**。比特幣的首次出現，是來自於 Satoshi Nakamoto (中本さとし，可譯為中本聰或中本哲史) 於 2008 年發表的一篇論文，題目為《Bitcoin: A Peer-to-Peer Electronic Cash System》(可譯為《比特幣：一種對等式的電子現金系統》)。為了避免通貨膨脹的問題，比特幣貨幣供給數量上限設定為 2,100 萬個【47】。

在這篇論文之介紹部分，便清楚地說明中本聰發明比特幣的動機與目的：¹⁰

「網際網路的商業應用幾乎已經完全仰賴金融機構，做為處理電子支付之被信任的第三方。雖然系統在大多數情況下都能運作良好，但這類系統仍有一項固有的缺點，那就是以信任為基礎的模式 (trust based model)。由於金融機構無法避免出面調解爭議，因此完全不可逆的交易 (non-reversible transactions) 實際上是不可能的。調解成本會增加交易成本、限制最小的實際交易規模、切斷日常小額支付的可能性，且失去不可逆之服務的支付能力會是一個更大的成本。可逆性的服務讓信任的需求增加，商人必須更加謹慎對待自己的客戶，因此會向他們提供更多不是他們所需要的信息，且一定比例的欺騙行為是可以被接受為無法避免的。而以上這些成本及支付的不確定性在使用實體貨幣時皆可避免，但尚未存在一個機制是可以

¹⁰ 資料引用來源：Satoshi Nakamoto (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, pp. 1.



在缺乏可信任方的情況下，透過通訊渠道來進行。

我們所需要的是一個以加密證明 (cryptographic proof) 取代信任的電子支付系統，藉由允許任何有意願並達成共識的雙方能夠直接交易，而不需信任的第三方參與。計算不可逆 (computationally impractical to reverse) 的交易可以保護賣家避免受騙，並且可以輕鬆地實施常規性託管機制 (routine escrow mechanisms) 來保護買家。在這篇論文中，我們透過一個點對點的分散式時間戳 (peer-to-peer distributed timestamp) 記伺服器，去產生按交易時間排序之計算證明進而解決雙重支付的問題。¹¹只要誠實的節點能夠共同合作去控制比攻擊者族群更多的 CPU 運算能力，這個系統就會是安全的【15】。」

比特幣在設計上，以個人數位簽名 (digital signature) 搭配交易時間戳記 (timestamp) 的方式來預防偽造，進而證明該次交易的唯一性。並採用工作量證明 (Proof of Work) 機制的點對點網路，來公開記錄交易的歷史資訊，而「挖礦 (Mining)」正是在執行工作量證明的運算。挖礦的即是使用電腦來執行某個運算程式，使用者電腦所付出的運算能力、電力及時間，就會有相對的機會獲得比特幣，來做為付出的獎勵。搭配上工作量證明的運作，電腦運算能力的強弱，也就決定著挖到礦的機率【39】。

比特幣還有一項值得一提的特性——匿名交易。在與上段同篇論文的隱私部分中，提及到：「為了達到一定程度的隱私，傳統的銀行業務模式 (the traditional banking model) 藉由限制交易參與者及被信任的第三方取得資訊的權限。¹²而公開發佈所有交易雖抵觸了上述的做法，但仍可藉由『保持公開金鑰匿名性』來維持隱私。」

¹¹ 在使用實體貨幣時，因為交易都是銀貨兩訖，所以沒有上述的信任問題；但數位虛擬貨幣就不一樣了。數位媒介的特色之一，就是非常容易複製，因此每當線上交易時，就得運用密碼學的運算，產生出一串經過加密的亂碼，來確保每次交易的安全性。因此，當亂碼被破解，這筆交易即可輕易地被更改 (例如，將 100 元篡改成 200 元來消費)，以造成同一筆錢被雙重支付 (double-spending) 的問題。(資料參考來源：blocktrend.today -解讀中本聰的比特幣論文：什麼是比特幣？)

¹² 資料引用來源：Satoshi Nakamoto (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, pp. 6.

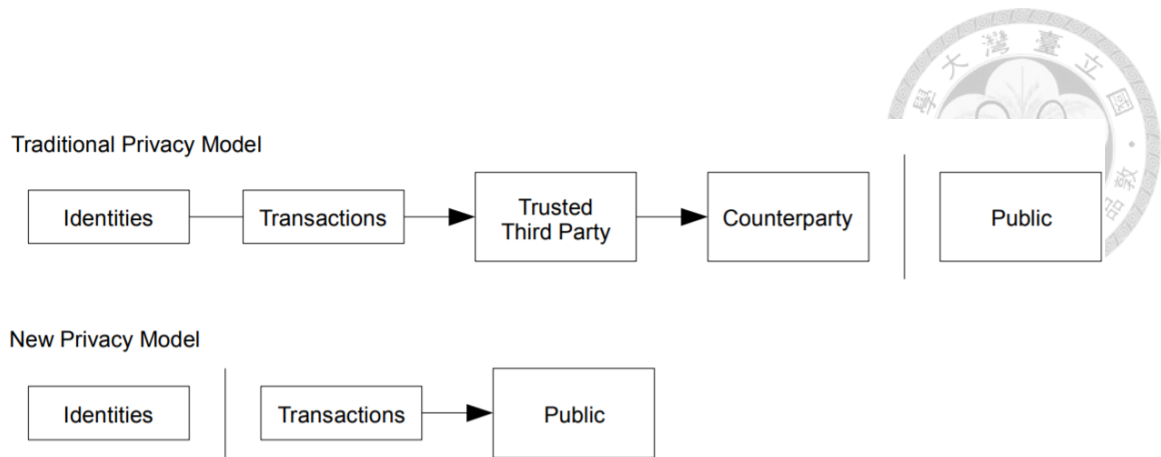


圖 4、傳統隱私模式與新隱私模式

資料來源：Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, pp. 6.

從上圖中可以清楚地看出，傳統隱私模式與新隱私模式的不同之處。在傳統線上交易中，銀行不但具有交易人身分、交易時間以及金額等重要資訊，也掌握著第三方取得交易細節內容的權限。而比特幣的交易缺乏實名認證，因此大眾可以看到有人向其他人發送一筆金額，但卻無法得知這筆交易的交易者的資訊【39】。這邏輯有如股票交易所釋出的交易資訊，公開個別交易的時間、金額和規模，但大眾並無法得知進行交易的人為何方神聖【15】。



3.1.2 個案之內容

比特幣興起的兩年後，一家利用比特幣進行非法地下買賣的匿名網路黑市「絲路 (Silk Road)」在 2011 年 2 月悄然興起。絲路因為有兩項技術得以使整個交易的過程變得非常隱秘：虛擬貨幣比特幣和網路匿名工具 Tor。¹³

由於，比特幣是種匿名、無國界、加密的網路貨幣，不受政府、公司、團體控制。再加上，Tor 是一個免費的、匿名通訊的自由軟體，主要用來讓使用者避免遭網路監控或政府相關單位鎮壓，常用國家包括中國大陸、伊朗和敘利亞等【6】。即便執法機構追蹤到某個可疑的電子數據，並且成功將其路由訊息解密，也只能查到訊息的上一個節點，然而，這個節點可能是在任何我們所想像得到的國家；接著，即使透過了外交的合作，查到這個節點的所在，所能再獲知的也只不過是再上一個節點的所在訊息而已，以這種往回追溯節點的方法追查到訊息的最源頭，恐怕也必須花個數年的時間【50】。¹⁴

許多默默的人群很快就意識到，絲路利用比特幣的匿名特性及還 Tor 洋蔥路由的技術，讓追蹤變得更加困難的超級安全性。因此開始大膽的在絲路網站上進行各種非法買賣，網站上商品超過 1 萬項，其中 70%左右的交易都和搖頭丸、海洛因、大麻、古柯鹼、安非他命等毒品有關，而剩下的 30%甚至還包括黑槍、盜取的信用卡用戶資料、色情服務、駭客服務等違法交易【50】。絲路運作有如一般的線上購物網站電子，並用郵寄的方式寄送。於 2013 年發布的一份調查報告顯示，絲

¹³ Tor (The Onion Router, 洋蔥路由器) 是第二代洋蔥路由 (Onion routing) 的一種實現，用戶通過 Tor 可以在網際網路上進行匿名交流。在洋蔥路由的網路中，訊息一層層地加密包裝成洋蔥一樣的封包，並經由一系列的網路節點傳送，每經過一個節點會將封包的最外層解密，直至目的地時將最後一層解密，目的地因而能獲得原始訊息。而因為透過這一系列的加密包裝，每一個網路節點 (包含目的地) 都只能知道上一個節點的位置，但無法知道整個傳送路徑以及原傳送者的位址。(資料參考來源：wikipedia.org -Tor & 洋蔥路由)

¹⁴ 路由 (routing) 就是透過互相連結的網際網路把資訊從源位址傳輸到目的位址的指令動作。(資料參考來源：wikipedia.org -路由)

路的註冊用戶超過 100 萬，而該網站對每一筆交易都徵收 8% ~ 15% 的手續費，觀察 2012 年半年內絲路的營收就成長兩倍，其獲利是驚人的豐厚，每月高達 170 萬美元收入【6】。



絲路雖然早 2011 年就被全世界的執法單位發現，但由於目標非常分散且難以追蹤，警方無法單靠鎖定幾個買家就解決這個龐大的非法地下買賣黑市。一名美國聯邦調查局探員在絲路網站臥底了近兩年時間，並努力去頻繁接觸該網站的管理人員。透過艱鉅漫長的數據分析，美國聯邦調查局在網路信息中查到，曾有人在一個比特幣論壇裡招聘技術人員，而也就在這時候，網路上第一次有人提到了絲路的名稱，因而斷定此人很可能就是該網站的創始人。根據所留下的電子信箱 rossulbricht@gmail.com，在 Google 公司的配合下，又查到了大量的信息。隨即，檢方將所圈定的若干嫌疑人，其中包括絲路創始人 Ross William Ulbricht 的所有網路通訊都秘密監控起來【50】。透過一次 Ulbricht 在絲路網站上，私下尋找一個殺手的交易中，在 2013 年 10 月，美國聯邦調查局終於成功逮捕 Ulbricht，並徹底搗毀了該網站，查封行動中共有 2.6 萬枚比特幣被沒收，約其總價值為 320 萬美元左右。在絲路網站被查封，以及 Ross Ulbricht 被捕的消息傳出後，比特幣的價值迅速下跌，從高達 145 美元跌為 123 美元【36】。

Ross William Ulbricht

Ulbricht 是一個非常聰明的人才。繼大學時期專攻物理學，獲得全額的學術獎學金；與致力於晶體學的研究，並獲得材料科學與工程的碩士學位之後，Ulbricht 開始對自由主義的經濟理論越來越感興趣，甚至參加大學辯論，以討論他的經濟觀點。於 2009 年畢業後，他多次創業失敗，使他有所轉變的是，在某次接觸到比特幣的生意。

起初，Ulbricht 只單純想用自由經濟理論來消滅高壓的政治和侵略，他想要建立一個完全沒有統治的、完全自由開放的經濟模式。於是自學，搭建了一個以比特

幣做交易的地下網站「絲路」，只能透過特殊軟體來進入此網站，且將貨品交易的所有過程全部加密。然而，他開始對自由意志理論有些走火入魔：「基於個人的選擇，只要你情我願，無論什麼交易都可以進行。」作為絲路的管理員，他每天也忙著提供給各種進行非法交易的賣家，如何躲避追蹤等各方面的資訊【26】。¹⁵

2015 年，因參與毒品交易、蓄謀違反毒品法、蓄謀非法入侵計算機、設立非法毒品交易市場、通過網絡參與毒品交易、散播虛假身份、洗錢七項指控，法官給予了 Ulbricht 最嚴厲的懲罰：終生監禁。2017 年 5 月，Ulbricht 被判上訴失敗，依舊收到了無期徒刑的判決結果，就此 Ulbricht 的故事真正被宣告結尾。但絲路的故事卻仍在繼續，絲路的「品牌價值」並沒有隨著 Ulbricht 被判處終身監禁而消失【26】。

絲路經歷了警方四次打擊又重新復活，以下為絲路從 1.0 版本進化到 3.1 版本的簡單介紹：¹⁶

絲路 1.0

於 2011 年 2 月，由 Ross William Ulbricht 所創建。根據 FBI 的調查，絲路總交易額為 950 萬枚比特幣，總計約 12 億美元，而 Ulbricht 也至少獲得了約 70 萬枚比特幣（約 8000 萬美元）的利潤。2013 年 10 月，Ulbricht 在舊金山的一家公共圖書館被捕，絲路 1.0 在之後也被美國聯邦調查局封停【26】。

¹⁵ 資料參考來源：合作媒體雷鋒網謝么（INSIDE 授權轉載，2017 年 6 月 3 日），兩年狂賺 360 億卻又終身監禁 暗網「絲路」創辦者的末路，INSIDE 硬塞的網路趨勢觀察。取自：
<https://www.inside.com.tw/2017/06/03/ross-ulbricht-the-creator-of-silk-road>

¹⁶ 資料參考來源：維基百科 wikipedia.org-絲路（購物網站），取自：
[https://zh.m.wikipedia.org/wiki/%E7%B5%B2%E8%B7%AF_\(%E8%B3%BC%E7%89%A9%E7%B6%B2%E7%AB%99\)](https://zh.m.wikipedia.org/wiki/%E7%B5%B2%E8%B7%AF_(%E8%B3%BC%E7%89%A9%E7%B6%B2%E7%AB%99))



絲路 2.0

在絲路 1.0 被封停之後，絲路 2.0 由 Ulbricht 的追隨者與原本絲路 1.0 論壇管理員之一 Blake Benthall，於 2013 年 11 月所創建。絲路 2.0 擁有超過 13,000 種危險物質，其中包括高達 1,800 種的迷幻劑；截至 2014 年 9 月，約有 15 萬活躍用戶和約 800 萬美元的月銷售額。Benthall 於 2014 年 11 月被捕，且以陰謀實施販毒罪、陰謀實施電腦駭客行為、陰謀販運偽造身份證件以及洗錢陰謀等罪名，最終也被判處終身監禁【3】。

絲路 3.0

絲路 2.0 關閉不久之後，就有人建立了絲路 3.0。至於，建立者的身分目前依舊不得而知。絲綢之路 3.0 的前身為早已存在的網頁 Diabolus Market，直到 2015 年 1 月，更名為「Silk Road Reloaded」重新上線。絲路 3.0 實現了新的匿名功能，包括 I2P 隱藏服務以及使用多種虛擬貨幣來支付，包括 Bitcoin、Darkcoin、Dogecoin 和 Anoncoin。但是，其經營並不順利，即使經過兩次對組織機構的人員進行大的調整和更換，亦無法吸引用戶。因此，在 2016 年 1 月，以技術原因為由暫停服務【26】。

絲路 3.1

據美國的娛樂社交新聞網站 Reddit 以及其他犯罪論壇宣稱，新絲路 3.0 和另一家暗網電商 Crypto Market 共用一個入口論壇，絲路 3.0 並沒有升級為 4.0。2017 年 9 月，絲綢之路 3.1 突然聲稱已經被不知名駭客攻擊並竊取了資金，因此宣布破產【38】。

地下網站不只有絲路一個，還有專門賣毒品的 Dream Market（夢想市集）、Alphabay Market、Amazing Shiny Flakes 等黑市，賣軍火的黑市有 Armory（兵工廠）、Black Market Team 等，而 USA Citizenship（美國公民）則是專門幫忙製造合

法的美國公民身份，綠卡、駕照等，在這些網路黑市，只要有比特幣就能買到軍火、毒品或是任何違法的東西【8】。



自從 2013 年美國聯邦調查局以打擊犯罪為名查禁了絲路，隨著其創辦人 Ulbricht 被判決無期徒刑，以及所有保存絲路的秘密伺服器曝光，也同時打碎了那些想利用虛擬貨幣來力爭網路隱私權、非政府主義者之夢想。伴隨著人們對於暗網市場的倫理逐漸忽略，以及這些秘密地下網站的消失，越來越多的網路黑市以捲款潛逃、將用戶存在帳戶裡的比特幣，在網站下線的同時一起帶走之方式退出市場【3】。



3.2 現代版的龐氏騙局？¹⁷ 虛擬貨幣交易平台 Mt. Gox 之比特幣消失事件

3.2.1 世界第一大的比特幣交易平台 Mt. Gox

Mt. Gox，全名為"Magic the Gathering" Online exchange。¹⁸2010年7月，由Jed McCaleb所建立。之後，由於當時McCaleb面臨多起訴訟而無暇管理Mt. Gox，因此決定出售轉手給Mark Karpeles的Tibanne Co.。而2011年，第一次遭受駭客攻擊，當時損失價值約875萬美元的比特幣；與2013年3月、6月分別兩度暫停比特幣的提現業務，前者是由於其比特幣的挖礦軟體在更新過程中產生了一個小故障；而後者是以交易平台對接的銀行應接不暇為由，業務暫停時間長達兩個星期。造成Mt. Gox平台的比特幣價格暴跌的三起事件，並沒有對Mt. Gox平台造成非常大的影響。直到2013年11月，Mt. Gox不但占全世界虛擬貨幣市場份額高達80%、成為世界第一大的虛擬貨幣交易平台，同時亦宣布不再為匿名帳戶提供交易服務【19】。

Mt. Gox從2014年2月初開始走下坡，7日時因發生了較大規模擠兌的現象，而Mt. Gox聲稱是擠兌遇到了技術上的問題，而第三次暫停全部虛擬貨幣的提現業務。之後，該網站上的比特幣交易價格崩盤、暴跌高達80%，Mt. Gox發佈了一份堅稱是比特幣的挖礦軟體和協議機制存在根本缺陷之聲明，暫停了所有的內部帳號間交易和對外的提現業務，而該份聲明亦被外界解讀為「無限期暫停提現」。

¹⁷ 龐氏騙局 (Ponzi scheme) 是一種表面看似能獲利的投資機會，而實質建立在欺詐之上的操作。這種欺詐形式是相信一個不存在企業的成功，而這個成功是透過後來投資者所投資的資金支付給初始投資者的利息或回報來促進的。(資料參考來源：Mijiki.com-What is a Ponzi scheme?)

¹⁸ 資料參考來源：時間線：Mt. Gox 事件始末與比特幣的興衰。2014年3月13日。TECH2IPO/創見，取自：<http://tech2ipo.com/63750>



根據 CoinDesk 交易所當時舉行的調查投票結果，高達 68% 的 Mt. Gox 用戶搞不清楚 Mt. Gox 平台的交易是處於中止狀態還是可用狀態【19】。

24 日，Mark Karpeles 向比特幣基金會辭職、Mt. Gox 亦被從董事名單中除名。後續，Mt. Gox 在一份名為「危機應對草案 (Crisis Strategy Drafty)」的內部文件中提及：他們在一次重大的比特幣失竊案中，被盜將近 74 萬枚比特幣。(總價值高達約 3.6 億美元)。亦宣布停止全面的業務、關閉官方交易網站，並於 28 日，正式向日本法院遞交破產申請【19】。

下圖為 Mt. Gox 從建立開始到此事件發生的簡要歷程圖：

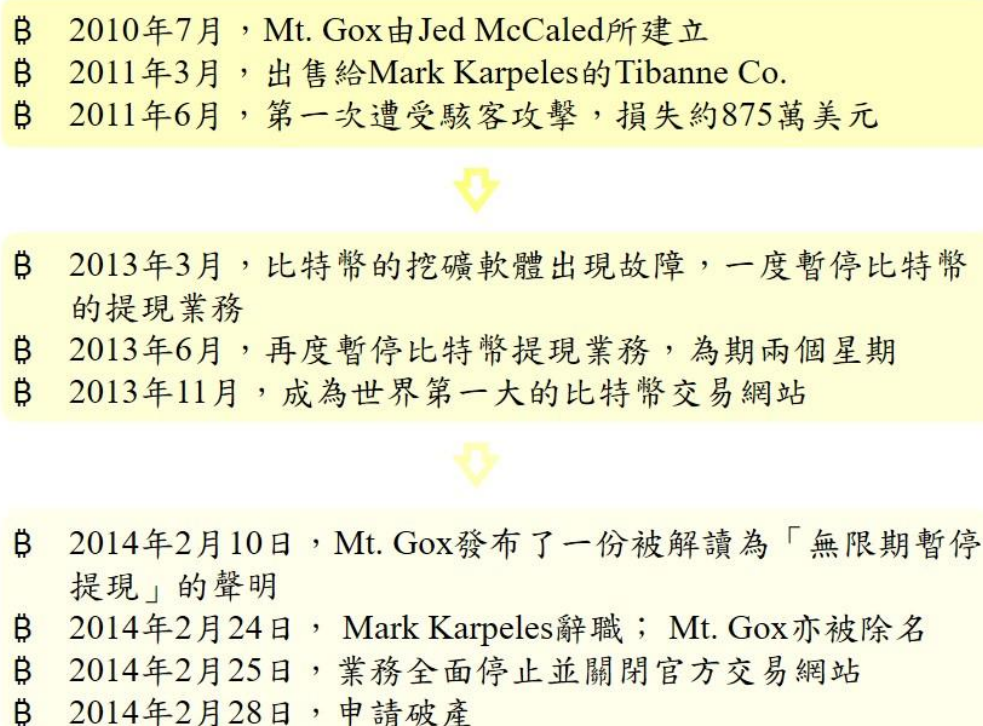


圖 5、Mt. Gox 簡要事件時間線

資料來源：tech2ipo.com



3.2.2 個案之內容

總部設在東京澀谷的 Mt. Gox 曾為全球最大比特幣交易所的，其於 2014 年 2 月 28 日訴請破產保護，同時聲稱不清楚是遭到駭客竊取或因技術問題，也可能兩者皆有，而造成屬於客戶的 75 萬枚與 Mt. Gox 持有的 10 萬枚比特幣，共約 85 萬枚比特幣（市價約值 4 億 8000 萬美元）從帳戶憑空消失，十數萬名的投資人蒙受損失。消失的比特幣數目約占全球 7%，以市價 565 美元計算，總價值超過新台幣 145 億元【41】。

有專業人士認為，由於中國比特幣市場的崛起和交易機構的繁榮，衝擊了 Mt. Gox 的市場地位，一定程度上間接導致 Mt. Gox 全球交易量從曾經的 80% 下降到不足 10%，而使營收受到影響；且在運營方面 Mt. Gox 選擇減少其相關的安全性支出，因而無法有效抵禦駭客攻擊。最終導致大量的比特幣被盜，平台不得不宣布停業，且瀕臨破產【19】。

但是，經過駭客攻破 Mt. Gox 的網站以及 Mt. Gox 執行長 Mark Karpeles 的個人微博，提取到了足以證明 Mt. Gox 管理層存在管理不善、內幕交易、詐騙事實的有力證據：從被破解 Mt. Gox 官網所獲得的資產負債表顯示，該公司仍持有 9.5 萬枚比特幣。亦即破產文件中所闡述「丟失」的比特幣，極有可能仍然以比特幣的形式存在，並被 Mark Karpeles 隱秘地控制，或是由 Mt. Gox 高層管理人員後台操作，目的是掩蓋該公司腐敗甚至涉嫌詐騙用戶的事實。駭客們發現了一個名為 TibanneBackOffice.exe 的可執行文件檔，並在其中發現了木馬的證據，而這個程序能夠在後台搜索到用戶的比特幣錢包，並將用戶的相關數據上傳到 <https://82.118.242.145/cgi-bin/sync.cgi> 這個網址【19】。¹⁹目前這個上傳網址亦已經被

¹⁹ 特洛伊木馬程式 (Trojan Horse) 是一種以尋找後門、竊取密碼為主的特殊惡性程式。和病毒 (Virus) 最大的不同是，木馬程式通常不會自我複製，且本身不帶傷害性，也沒有感染力。原則上



託管商所關閉。

Mark Karpeles 於 2014 年 3 月下旬在公司官網發表聲明，宣稱在一個舊錢包當中找到約 20 萬枚比特幣，並已經將其離線保存，但仍有約 65 萬比特幣下落不明。相關方面的專家亦表示，遺失的比特幣資產很難追回。Mt. Gox 也在 2014 年 2 月向東京地方法院申請破產保護，值得注意的是，Mt. Gox 申請了日本《民事再生法》的「倒產流程」，這意味著如果得到允許，Mt. Gox 將可以在免除一切債務的情況下恢復生產【19】。

「大部分國家並不否認這種虛擬貨幣的合法地位，比特幣交易並不受各國政府監管、審查和保護，是完全獨立於銀行體系之外的一種創新交易。」的緣故，關於此事件的發生，國際相關單位仍持保留態度。美國聯準會 (Fed) 主席 Janet Yellen 曾向國會表示，聯準會無權對比特幣進行規範，但也提醒美國財政部等管理部門需監控比特幣是否被用於洗錢等非法行動。越南政府則宣布國內比特幣交易為非法行為，警告越南國民避免使用與投資比特幣。而日本官方表示無力規範比特幣這樣的虛擬貨幣，但由於迫於壓力而對 Mt. Gox 的關閉事件展開調查【41】。

Mt. Gox 的破產也讓人匪夷所思，日本警視廳搜查二課表示，Mark Karpeles 曾兩度在所內的比特幣交易系統中進行不正當手段操控，同時他亦被調查出，他名下的美元帳戶虛增了 100 萬美元（而能進入 Mt. Gox 伺服器與數據庫，對餘額進行違規操作的系統管理者只有 Mark Karpeles 一人），且駭客也發現到 Mt. Gox 的系統中，尚有許多遭到篡改之處【29】。重重的疑點堆積起來使人們都開始認為 Mt. Gox 是一場精心策劃好的新版「龐氏騙局」。

它只是一種遠端管理工具，大多用來竊取電腦密碼。一旦不小心使用到一個含有木馬程式的軟體，該木馬就會被「種」到電腦裡，往後駭客便能透過你的電腦，竊取密碼、信用卡號碼等機密資料，還可以對電腦進行監視、控制、查看、修改資料等操作。（資料參考來源：answers.yahoo.com-木馬病毒是什麼）



2015 年 8 月，日本警方初步認定 Mark Karpeles 涉有重嫌，以涉嫌違規操控帳戶數據和侵占公款為由將其逮捕【22】。Mark Karpeles 以 10 萬美元被保釋出獄的一年多後，2017 年 7 月 11 日東京地方法院對被控業務侵佔公款等罪名的 Mt. Gox 交易所運營公司高層進行首次公審，但他矢口否認犯行，稱幕後黑手是外部駭客。如果 Mark Karpeles 挪用款項罪名成立，將被處以最高 5 年的監禁和 4000 美元的罰款【29、30】。

事件已經經過四年多的時間了，雖然索賠程序早已開始，但是 Mt. Gox 的很多客戶們至今還沒有要回任何一個比特幣【22】。此案件不但審理進展緩慢，破產程序也正在複雜繁瑣之中慢慢推進。涉及到虛擬貨幣的破產處理方式與一般破產案件不同，普通破產程序將破產公司的資產換算其價值轉為金錢，並將支付（貸款）給債務調查中的債權人即可。但此事件，四年前破產時的比特幣價格約為 5 萬日元，在 2017 年 12 月 20 日左右甚至超過了 200 萬日元的最高值。因為這種幣值劇烈動盪的原因，日本規定「以破產當時的比特幣價格為主」，在這種情況下，破產之時 20 萬枚比特幣約為 100 億日元；截至 2018 年 4 月 27 日為止，比特幣價格約 100 萬日元左右，亦即破產之時的 20 萬枚比特幣目前的價格評估約為 2,000 億日元。出現這 20 倍的差異，也使債權人不得不堅持破產【14】。

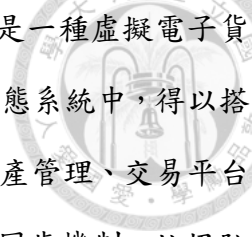


3.3 虛擬貨幣 NEM 外流失竊案

3.3.1 NEM 之背景與特性

NEM 的全名是 New Economy Movement (新經濟運動)，其是指一個建立整套經濟生態系統的運動，XEM 為其貨幣符號，中文名稱為新經幣，目前是世界第十大虛擬貨幣。在 2014 年 1 月 19 日，NEM 的創始者 UtopianFuture 在 bitcointalk.org 上號召人們投身於擁有平等主義分配方式的 NEM。NEM 的開發者包括：創立突破性技術 POI(Proof of Importance, 重要性證明)的 UtopianFuture、Jaguar0625、Gimre、Makoto、Thies、BloodyRookie 五位核心開發者，前端及 web 開發者 Krysto 和設計人 TranLoi (有一部分為匿名)。開發團隊的目標在於實現 UtopianFuture 所憧憬的平等與公平，讓 NEM 成為富人、早期參與者無法透過使用強勁的挖礦機來獲得「收穫(Harvest)」，或依靠單純大量買進而獲得可觀份額的第一個虛擬貨幣【20】。

POI 的算法提供一種分佈更為平均的挖礦方式。人們既不需要使用性能強勁的機器設備，也不需透過持有更多的股份來獲取更多的獎勵，只需要向整個 NEM 經濟體證明 (P: Proof) 自己的重要性 (I: Importance) 來獲取收穫，其真正看中的是交易量、活躍度、以及交易往來對象的重要性等，這能讓持有 XEM 虛擬貨幣的用戶更會主動去進行交易，進而提高整個系統的流動性。由於無需特殊的挖礦硬體，因此它相較於其他虛擬貨幣的挖礦來說更為省電，亦即相對於 POW (Proof of Work, 工作量證明)，這套方案可以解決在比特幣生態中的大量資源浪費和挖礦設備之間競爭的問題。且其設計從頭到尾都使用人們最為熟知、廣泛使用的電腦程式設計語言 Java 來開發，而得以獲得廣泛的保障【20】。



和比特幣不同的是，做為一個金融生態系統，NEM 不僅僅是一種虛擬電子貨幣，它本身就可以是整個金融生態系統運轉的核心。在此金融生態系統中，得以搭建包括電子商務、訊息的安全與加密、社交網路與媒體、數位資產管理、交易平台等特定應用程序的實現。且 NEM 還有節點聲望系統、P2P 時間同步機制、垃圾防衛機制和多重簽名 2.0 協議 (Multisig 2.0) 等特點。^{20、21、22}NEM 將多重簽名之技術加入至平台中，舉例來說，在 NEM 經濟體中若預先設定在 X 個人當中必須有特定的 Y 個人簽名，意即一定要在上述的 Y 個人簽名後，區塊鏈才會執行交易。多重簽名是一個用於增強用戶的虛擬貨幣錢包及交易安全性的技術，其需要一個以上的用戶簽署才得以進行交易，而這也表示，駭客無法僅透過盜取 NEM 經濟體中單一個人的虛擬貨幣錢包來進行交易【20】。

3.3.2 個案之內容

日本東京的虛擬貨幣交易所 Coincheck 遭駭客入侵，造成約 580 億日圓（逾台幣 157 億元）的虛擬貨幣「NEM」外流，此為目前世界上最大宗的虛擬貨幣失竊案。

下圖為 Coincheck 的 NEM 虛擬貨幣被盜的紀錄。2018 年 1 月 26 日上午 0 時

²⁰ **節點聲望系統**：NEM 是首個採用 EigenTrust++ 算法，來監測網路內的節點行為之虛擬貨幣。在 EigenTrust++ 算法中，工作的質量尤為重要，這使得 NEM 網路更有效率的運行和維護。而其他虛擬貨幣則使用工作量證明等算法維護其區塊鏈，工作量證明的算法中，是透過一個節點的運算量大小來確定其工作量，以維持整個系統穩定運行。（資料參考來源：wikipedia.org - 新經幣）

²¹ **P2P 時間同步機制 (P2P Time Sync for Nodes)**：NEM 如同其他大多數的虛擬加密貨幣一樣，依靠交易和區塊的時間戳 (time stamps)。在理想的情況下，網路中的所有節點應該在時間上有所同步，但節點仍可能具有與實際時間偏差超過一分鐘的現象，而這會導致這些有時間偏差的節點拒絕有效的區塊或交易，因此需要有一個同步的機制來確保所有節點在時間上得以達成一致。而 NEM 也是首次在網路節點中使用了 P2P 時間同步機制的虛擬貨幣，使其能有效地保障區塊鏈的安全性。（資料參考來源：blog.nem.io - P2P Time Sync for Nodes）

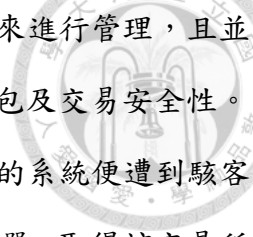
²² **垃圾防衛機制 (Spam Guard)** 能有效地偵測垃圾交易並透過提升交易手續費的方式來抑制它們，這能有效地防止一些特別的用戶所產生大量的垃圾交易，同時不影響其他正常的交易。（資料參考來源：steemit.com - NEM 的基本介紹及背景資料整理）

2 分起，Coincheck 交易所開始有些微的 XEM (NEM 的交易單位) 流向其他的虛擬貨幣帳號，透過多次轉向同一帳號的交易，截至 0 時 21 分時已有高達 5 億 2300 萬 XEM (約 576 億日圓) 流向某個特定的虛擬貨幣帳號。在這短短的 20 分鐘之內，就被轉走了這個事件損失額 580 億日圓的 99%，然而，後續在凌晨的 3 時、4 時，甚至到上午 8 時也陸續有虛擬貨幣從該特定帳號流出、流入至該特定帳號的頻繁交易狀況，Coincheck 卻直到上午 11 點 25 分左右才發現異常【42】。為此，Coincheck 在當日下午 4 時 30 分時，宣佈暫時中止交易所所有種類虛擬貨幣的所有服務，包括買賣、存款以及兌換回日元等的服務。公司高層亦舉行了記者會，向所有受害的客戶致歉，並檢討客戶的補償方式【16】。

#	Timestamp	Amount	Fee	Sender	Recipient
1	2018-01-29 12:25:14	1	0.4	NCGLW2SVASDP2X4T07JBOM65PRIFZ2PSPSHDGL4	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
2	2018-01-28 01:27:18	1	0.7	NBY320KZ0PTWAQV5P5TLWJZDQNTZ5HZ3L3NAU3	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
3	2018-01-28 00:21:03	1	0.3	HEKCVZ2BUJDSXLUZD4BAZEVIXE3MRKYKVINPWYQ	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
4	2018-01-27 22:04:51	0	0.25	NAUF1PHWAAFJWLE5C33W365I5B0V320DLDFEBK	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
5	2018-01-27 17:24:42	1	0.25	NCJQZGJLMVPCOZAUUSI7V7BJHMOG02TZCQFPHC	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
6	2018-01-27 03:41:31	0	0.7	NAUF1PHWAAFJWLE5C33W365I5B0V320DLDFEBK	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
7	2018-01-26 23:42:01	300,000	1.25	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G	NCM6WE7SjFDVTLSP1MZ08UJZUETDYIN1TILS3DCIz
8	2018-01-26 20:27:35	0	0.2	NAZAS0SA2DPAR55RA3SNHUKBLUZGCDWYWWBIFAY	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
9	2018-01-26 18:46:30	0	2	NBXA6FYUETSRB5FTXGLULQOEVFNDEPE7N4HATAR	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
10	2018-01-26 18:06:48	1	0.1	NCMKWNFVUULEVCKBSONZM5658XU4N2G8JTUB7K	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
11	2018-01-26 17:23:58	1	0.2	NCVGTCTV7YGGCUTOWRSEALEVHVTDFRJS4BQYDKTI	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
12	2018-01-26 08:26:13	800,000	1.25	NC3B3DNMR2PGE0OMP2NIXQGSAAKMS7GYRKA5CSZ	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
13	2018-01-26 04:33:20	1,000,000	1.25	NC3B3DNMR2PGE0OMP2NIXQGSAAKMS7GYRKA5CSZ	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
14	2018-01-26 03:35:09	1,500,000	1.25	NC3B3DNMR2PGE0OMP2NIXQGSAAKMS7GYRKA5CSZ	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
15	2018-01-26 03:29:54	92,250,000	1.25	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G	NA6J5WNF24Y7DVUVPRNAY7TPOFJJ7G2URL7KJ5
16	2018-01-26 03:28:44	100,000,000	1.25	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G	ND0ZVF32WB3LWRNG3VGHCOCAZWCNCRNGZJVCJII
17	2018-01-26 03:18:07	100,000,000	1.25	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G	NB4JQLCTZVWVFRFBEMFOONQZFDH3V5IDK3G524
18	2018-01-26 03:14:09	100,000,000	1.25	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G	NDZZJBH6JZPY9WRPRYHALWMTWH0VYQGXRS3HAW
19	2018-01-26 03:02:12	750,000	1.25	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G	NBKLQYXEVEEGARYPUM6ZUIFHA3Y6R4LAPUNP4
20	2018-01-26 03:00:33	50,000,000	1.25	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G	ND00XOWEIZGJSMELURKACF4EHC2C8706T56V75Q
21	2018-01-26 02:58:42	50,000,000	1.25	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G	NA75Z5KF629Q26TRKJ0J8WVPSK2H45PXCKW
22	2018-01-26 02:57:24	30,000,000	1.25	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G	NCTNFOOV1TRZY5YIGQ3PE33MV625KMED53EWFQ
23	2018-01-26 00:21:14	3,000,000	1.25	NC3B3DNMR2PGE0OMP2NIXQGSAAKMS7GYRKA5CSZ	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
24	2018-01-26 00:10:36	20,000,000	1.25	NC3B3DNMR2PGE0OMP2NIXQGSAAKMS7GYRKA5CSZ	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G
25	2018-01-26 00:09:22	100,000,000	1.25	NC3B3DNMR2PGE0OMP2NIXQGSAAKMS7GYRKA5CSZ	NC4C6PSUW5CLDT55XAGJDDJGZNESKFKSMCN770G

圖 6、Coincheck 之 NEM 虛擬貨幣被盜的紀錄

資料來源：ITmedia.co.jp

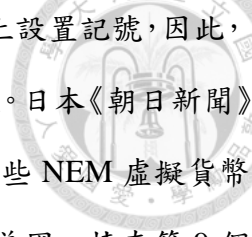


Coincheck 的 NEM 虛擬貨幣錢包是使用線上的 Hot Wallet 來進行管理，且並沒有使用多重簽名 (Multisig) 之技術來保護用戶的虛擬貨幣錢包及交易安全性。²³數名職員在開啟了內含惡意程式軟體的電子郵件之後，交易所的系統便遭到駭客入侵，駭客透過竊取員工的電子郵件帳號滲透 Coincheck 的伺服器、取得該交易所平台 NEM Hot Wallet 的私人金鑰，而得以進行將大量虛擬貨幣傳送到外部的動作。然而，對於並未使用離線的 Cold Wallet 進行管理之理由，與沒有加入多重簽名 (Multisig) 技術之原因，Coincheck 交易所的技術總監—大塚雄介並沒有多做解釋，以有其他優先事項、執行難度高等藉口含糊帶過，只向民眾不斷地重申「Coincheck 一直都以安全性作為第一優先考慮」【16】。²⁴

由於 NEM 的交易紀錄與過程都會公開記錄在區塊鏈上，Coincheck 在事件經過 4 天後，宣佈成功追蹤到失竊贓款的交易流向。透過使用可查看 NEM 經濟體中各個帳戶的交易及匯款紀錄的「NEM BlockChain Explorer」，搜索與此 NEM 大量失竊事件有關的所有可疑帳戶，便可發現當天共有約價值 580 億日圓的 NEM 以不同管道匯款至該特定帳戶的交易紀錄【17】。而根據詳細的交易紀錄調查，更發現被奪走的鉅額虛擬貨幣以 9 個不同的虛擬貨幣帳戶分開進行匯款之事，並已經鎖定了某個可能為駭客的戶口號碼【42】。

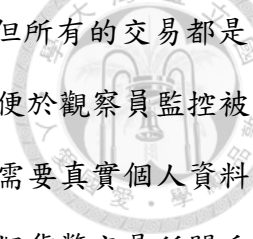
²³ **Hot Wallet (熱錢包)** 是將貨幣資料都存放在網路上，無需下載整個虛擬貨幣網路的數據，完全依靠網際網路的連線。如同把錢存在銀行，一般來說存放在虛擬貨幣交易所的虛擬貨幣，就是一種熱錢包。因為聯網，所以提領或交易上快速、方便；也因為聯網，使得駭客有機會透過網路攻擊取得錢包帳號的私人金鑰，將錢包中的虛擬貨幣轉走。(資料參考來源：nionionote.com -什麼是冷錢包、熱錢包？這篇總整理)

²⁴ **Cold Wallet (冷錢包)** 也稱作離線錢包，類似於實體錢包，將虛擬貨幣的數據存放在不連接網際網路的電腦、硬碟、手機等方式。不同於交易所使用帳號密碼登入，冷錢包是直接使用密碼／私人金鑰來開啟，因此只要電腦不故障、使用者沒有忘記密碼或是私人金鑰，就不必擔心有所損失。因為利用離線的方式，也就不必擔心駭客可以透過網路攻擊，進而盜走錢包中的虛擬貨幣資產。(資料參考來源：nionionote.com -什麼是冷錢包、熱錢包？這篇總整理)



為了封殺犯人的交易，Coincheck 在上述所鎖定的犯人戶口上設置記號，因此，當鎖定的戶口與其他人進行交易時，交易的另一方亦會留下記號。日本《朝日新聞》分析此事件之 NEM 外流帳號的交易紀錄發現，2 月 8 日清晨這些 NEM 虛擬貨幣被分散至 45 個帳戶保管，再由這些帳戶將 NEM 虛擬貨幣匯到美國、捷克等 9 個貨幣交易所，每次大概匯款的額度約值 60 萬至 90 萬日圓的虛擬貨幣。犯人的所為極有可能是為了逃避相關單位的監視，另外，也發現這些交易紀錄當中，只有紐西蘭交易所不斷的有虛擬貨幣匯出、匯入的交易，光從 NEM 外流帳號匯款到紐西蘭的帳號，2 月 1 至 8 日共有 21 次的交易紀錄。然而，外界並無法確認各國交易所內的動向，匯到紐西蘭交易所帳戶的 NEM 很可能已換成其他的虛擬貨幣。日本也有熟悉虛擬貨幣網路保全之專家推斷，駭客可能早有網路攻擊的計畫，為了得以交換成其他種類的虛擬貨幣而在紐西蘭的交易所開戶【43】。

Coincheck 已經向存有 NEM 的客戶作出補償，總額達到 460 億日元（逾台幣 125 億元）。Coincheck 在受到駭客攻擊之後，開始聯繫各大虛擬貨幣交易平台並告知所被偷的錢包地址，試圖將其列入黑名單。當時全球還有 33 個交易所接收 NEM，所以理論上駭客其實尚有足夠的選擇，將所竊取的 NEM 交換成其他種類的虛擬貨幣，但在這其中只有 8 間交易所所有 NEM 總交易量超過 100 萬美元的紀錄。因此，推斷駭客能夠找到一個平台去大量的「洗黑錢」是一件非常困難的事情。另外，NEM 的基金副總裁 Jeff McDonald 也有聲稱道：「駭客們正試圖在多個交易所銷贖，我們也在看到『交易提醒』的第一時間去聯繫了那些交易所。且 NEM 的強大之處在於，它在區塊鏈上是非常顯眼的。當駭客在其他平台交易時，交易提醒依然會顯示原貨幣的代發平台。所以如果有人試圖向他們存入標有 Coincheck 的 NEM，那麼交易就會被提醒。」專家亦認為，駭客若為了避免監視、審查，將偷盜來的 NEM 透過電腦自動化進行分裝並且分開存放在新的錢包中也是一個繁瑣的過程，最後他們的收益可能連總價值的百分之一都還不到【34】。



區塊鏈的特性是不需要任何真實身份信息便可進行交易，但所有的交易都是公開的，每一筆交易都會被記錄下來且交易過程能被輕易追蹤，便於觀察員監控被盜資金的流動情況，從而追蹤駭客的帳戶與 IP 位址。除非使用需要真實個人資料的交易方法，不然追蹤犯人仍是一件非常困難的事。然而，在虛擬貨幣交易所開戶時，必須登記姓名、電子郵件等個人資料，且在大筆的匯款手續時還需要確認本人身分的文件，因此只有等待犯人將贓款兌換成現實貨幣時，相關單位才有辦法展開進一步調查行動【35、36】。

經過分析東京網路安全公司被盜 NEM 的在線交易紀錄，駭客曾設立網站公開招募接贓人士。總部位於東京的安全公司 L Plus 證實，有一個於 2 月 7 日建立地下網站的紀錄，而 NEM 被盜基金的帳戶截至 3 月中下旬顯示的餘額也為零。這個特別的地下網站很明顯地為被盜的 NEM 兌換其他加密貨幣提供了機會。雖然已經鎖定且標記了一些特定的虛擬貨幣帳戶，但相信幾乎所有被盜的 NEM 已經被「洗淨」了【2】。

事件發展到最後，出於未知的原因，新加坡的 NEM 基金會在 3 月 20 日下午宣布將停止再繼續追查被盜 NEM 虛擬貨幣的下落【18】。就目前情況而言，這些 NEM 已經兌換成了如比特幣等其他加密貨幣分布於多個不同地址的多個虛擬錢包中，其中每一個虛擬錢包都包含著價值數億日元的比特幣。然而，若這些虛擬貨幣的兌換，在海外交易所較沒有遵守嚴格的 KYC 或 ID 規範之情況下，洗錢者預計也有辦法將自己的虛擬貨幣兌換成現金【2】。²⁵NEM 基金會指出，目前還不清楚是否有任何被盜的虛擬貨幣資金已被兌現，但已經執行有效防止駭客進行真實金錢兌換之措施，並向警方提供了與此失竊案相關的資料【18】。

²⁵ KYC (Know Your Customer) 政策，即充分了解你的客戶，是金融機構用於防範洗錢的基礎制度。不僅要求實行帳戶實名制，了解帳戶的實際控制人和交易的實際收益人，還要求對客戶的身份、常住地址或所從事的企業與業務進行充分的了解，並採取相對應的措施，像是政治人物與其相關親屬的帳戶進行強化審查等。(資料參考來源：baidu.com - 在銀行中 KYC 是什麼意思)



第四章 虛擬貨幣相關之洗錢風險

在 1960 年代國際毒品的走私犯罪猖獗，由於經濟自由化與跨國間資金往來的便利，形成犯罪組織透過洗錢（Money Laundering）之方法，以試圖湮滅其犯罪證據、隱藏其不法犯罪之所得，使政府相關之司法機關難以追查。2017 年，根據國際貨幣基金組織（International Monetary Fund）之調查報告與聯合國（United Nations）的預估結果，世界各國每年在國際上流通的洗錢金額約達 8,000 億至 2 兆美元不等，占全球國內生產毛額的 2% 至 5%。²⁶最早明確提及「反洗錢（Anti-money Laundering）」一詞的是美國的《銀行保密法（Bank Secrecy Act of 1970, BSA）》，該法案旨在規範金融業針對不法金流有申報的義務，規定金融機構或個人必須保留支票等金融交易的影本和紀錄，而對某些特定的金融交易尚須向財政部長報告，使執法機關得依所留下紀錄之證據，追查犯罪活動的起源以及不法收益之流向。

4.1 洗錢的故事與定義

洗錢（Money Laundering）這個名詞的來源是，在二十世紀初美國著名的芝加哥黑幫犯罪集團老大——艾爾卡彭（Al Capone），除了諸多犯罪行為之外，也經營投幣式洗衣店。由於，美國人很少有晾衣服的習慣，多半是使用烘衣機來弄乾衣物，因此洗衣店在美國的某些區域是相當普遍的。艾爾卡彭非常有技巧地利用經營投幣式洗衣店，掩飾他的犯罪行為，尤其是犯罪所得。他對於洗衣店的生意獲利並無興趣，他將非法活動的所得謊稱為洗衣店的現金收入，藉此將不合法的資金合理化並重新流入正常的金融體系中。²⁷因此，美國政府當年才一直無法找到他的犯罪證

²⁶ 國內生產毛額（Gross Domestic Product, GDP）是一定時期內（一個季度或一年），一個區域內的經濟活動中所生產出之全部最終成果（產品和服務）的市場價值（market value），在衡量一個國家或地區經濟狀況和發展水準時，有相當的重要性。（資料參考來源：wikipedia.org - 國內生產總值）

²⁷ 資料引用來源：Daniel Wang（2018 年 2 月 4 日），洗錢：定義，歷史。取自：https://aml.watch/aml_definition_history/

據。



「洗錢」亦稱資金洗淨、清洗黑錢，係指犯罪者為了隱藏其犯罪行為、掩飾其不法行為所獲得的資金或財產之來源（犯罪及不法行為中，諸如販毒、擄人勒贖、搶劫、經濟犯罪、貪污等），透過各種交易管道或金融機構等仲介者的作業，轉換成為合法來源的資金與財產，以避免司法的追溯與偵查。在法律上，今日世界各國對於洗錢的定義尚未達到共識【51】。

台灣是最先體認到防制洗錢之重要性的國家，並於 1996 年制訂《洗錢防制法》，是亞洲國家的第一部防制洗錢專法。²⁸該法的第二條內容，將洗錢定義為下列行為：

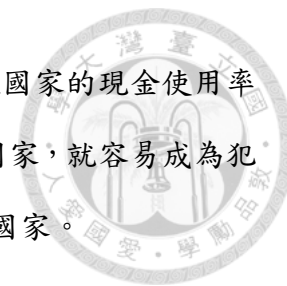
- 一、意圖掩飾或隱匿特定犯罪所得來源，或使他人逃避刑事追訴，而移轉或變更特定犯罪所得。
- 二、掩飾或隱匿特定犯罪所得之本質、來源、去向、所在、所有權、處分權或其他權益者。
- 三、收受、持有或使用他人之特定犯罪所得。

防制洗錢金融行動工作組織（Financial Action Task Force, FATF）對洗錢採取較廣義的定義，將其定義為：「隱匿或掩飾犯罪行為所收取的財物的性質、來源及資金流向，稱之為洗錢；另外，協助非法活動者規避其應負法律者，也屬於洗錢行為」。²⁹根據 FATF 推測，光是販毒所漂白的黑錢，每年就約有 850 億美元。且犯罪

²⁸ 資料引用來源：《洗錢防制法》。2016 年 12 月 28 日。全國法規資料庫（法規類別：行政＞法務部＞檢察目），取自：<http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=G0380131>

²⁹ 防制洗錢金融行動工作組織（Financial Action Task Force, FATF）是一個政府間機構，1989 年由七大工業國組織 G7（成員包括美國、加拿大、英國、法國、德國、義大利及日本）所組成。FATF 的任務在於制定標準去促進法律、監管和執行措施的實施，以有效地打擊洗錢、恐怖主義的資助（Combating the Financing of Terrorism, CFT）等威脅到國際金融體系之完整性的相關事情。（資料參考來源：The FATF Recommendations (February, 2012), INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION.)

組織的不法所得，絕大多數會採用現金交易的方式，然而，先進國家的現金使用率低，因此，現金使用額度占國民生產毛額比率高達 20% 以上的國家，就容易成為犯罪組織執行國際洗錢的大本營，如：中南美洲和部份東南亞等國家。



4.2 洗錢之方法

現金是非法交易的主要媒介，因為現金流動性最好、難以追蹤且也不須認定所有權。但是，當額度龐大時，採用現金交易的方式會有太過顯眼、搬運不便等問題，因此，非法交易之所得逐漸透過存款於金融機構或是轉換成其他適當的、具有價值的物品。

FATF 根據各國發生案例，歸納出洗錢的操作方式具有金額密集、多次轉移、國際化等特性；整個錯綜複雜的洗錢過程，大致可分為三個階段：存放、多層化移轉、整合。洗錢者透過將上述三個階段，以跨越國界、反覆重疊執行的方式，便可以加重追查非法得益及其來源的困難度。

一、存放 (Placement Stage)

為了掩飾犯罪不法所得之來源與線索，將黑錢 (Dirty Money) 以不同的方式藏匿或轉換，以避免司法機關的查獲。方法大概可分為金融與非金融方式。前者主要透過銀行、證券、期貨等金融機構的交易管道來洗錢，小額換大鈔、大筆錢分多次小額提領、利用人頭帳戶做為國內及跨國洗錢等皆為常見的案例；而非金融管道更是變化多端，如利用賭場、不動產買賣、購買貴重金屬等方式。

二、多層化移轉 (Layering Stage)

藉著創造許多複雜的金融交易來分散其不法所得，經歷豐富的洗錢者甚至還會將各國的政治與經濟穩定性、匯兌管制情形、當地銀行

的專業性、租稅結構等因素加以考量並分析出適合進一步做不法交易的國家。



三、整合 (Integration Stage)

此階段的目的是將所有不法之所得合法化。經過多次上述階段的漂白掩飾後，黑錢已經具有合法的外貌，因此，一般人也難以覺察到其非法性質和來源。洗錢者將這些被清洗的資金轉移到與犯罪集團／分子無明顯聯繫的合法機構或個人的名義下後，再以投資為由等方式，投放到正常的社會經濟活動中，使相關執法單位更加無法追查。

隨著科技的進步，新的洗錢形式包括 ATM 卡、手機支付、虛擬貨幣等基於網際網路的支付系統。且這些新手法的洗錢，通常發生於金融機構部門之外。犯罪分子可以透過購買合法的 ATM 卡或智能卡，將其所收益的黑錢存入卡中，即得以從世界上任何地方的任何 ATM 領取到洗清的資金。此外，即使洗錢分子居住在可被追蹤—有網際網路的環境，他們仍可以透過電子支付轉帳可以隱藏錢的來源，並保持所有者的匿名性；而在中東國家，手機支付是一種特別流行的交易方法，這種進行交易的方式也為洗錢者提供了一個躲避反洗錢機構的途徑；比特幣等加密虛擬貨幣亦是近年來常見的洗錢工具，基於其匿名性，可自由、不記名地產生不同的虛擬貨幣錢包，並可在錢包中放入不同虛擬貨幣之服務，更增加了追蹤洗錢分子真實身分的困難度【51】。³⁰

³⁰ 資料引用來源：Brigitte Unger, Johan den Hertog (April 2012), Water always finds its way: Identifying new forms of money laundering 【Electronic payment forms money laundering】.



4.3 虛擬貨幣之洗錢風險³¹

首先，這些貨幣比傳統的非現金支付方式允許更高的匿名性。虛擬貨幣系統可於網際網路上進行交易，通常以非面對面的客戶關係為特徵，且允許匿名募資（透過虛擬交易所提供的現金資金或第三方資金，但沒有正確識別資金來源）。若未適當辨識匯款方與收款方，這些貨幣亦允許進行匿名轉帳【11】。

去中心化運作的系統特別容易遭受匿名風險（anonymity risks）。舉例來說，作為帳戶使用的比特幣位址，設計上就並未包括姓名或其他顧客身份識別資料，且其系統並沒有中央伺服器或提供服務的業者。比特幣協議（The Bitcoin protocol）並未要求參與方提供相關之身份識別資料以及驗證資料，亦不會產生與現實世界身份必要相關的歷史交易記錄。比特幣目前並沒有中央機構監督，且也沒有洗錢防制軟體可用於監視與識別出其中可疑交易的模式。執法機構無法鎖定單一中央位置或存在實體（管理員）進行調查或扣押資產（雖然主管機關可以鎖定個別交易平台，要求其提供可能蒐集到的客戶端資訊）【11】。³²因此，提供了傳統信用卡與金融卡或更早期的線上支付系統（如 PayPal）所無法提供的匿名程度。

虛擬貨幣的全球性，同樣的提高了其洗錢防制／打擊資助恐怖主義的潛在風險。虛擬貨幣系統可透過網際網路（包括透過行動電話）存取，且可用於進行跨國支付與資金轉帳。此外，虛擬貨幣通常採用複雜的基礎架構進行資金轉帳或執行付款交易，且通常分布、涵蓋於數個國家的多個實體單位。上述服務的區隔，也代表了洗錢防制／打擊資助恐怖主義之遵循法規與監督、執行的責任（AML/CFT

³¹ 資料引用來源：FATF REPORT (June 2014), Virtual Currencies Key Definitions and Potential AML/CFT Risks, pp. 9-10.

³² 管理員（**administrator**）係指從事發行（放入市場流通）中心化運作的虛擬貨幣、建立使用規則、維護集中支付帳簿以及有權贖回（停止流通）虛擬貨幣之業務的個人或實體。（資料參考來源：FATF REPORT (June 2014) -Virtual Currencies Key Definitions and Potential AML/CFT Risks）



compliance and supervision/enforcement)，可能劃分得並不明確【11】。

顧客與交易記錄可能由不同的實體單位所持有，且通常這些實體單位也位於不同的司法管轄地區，使得執法機關與監管機關更難以取得這些記錄。此問題，因去中心化運作的虛擬貨幣技術與營運模式之快速演化而更加嚴重，包括提供虛擬貨幣支付系統服務之參與方的數量與種類、角色不斷改變。更重要的是，虛擬貨幣體系的組成可能處於一個沒有洗錢防制／打擊資助恐怖主義，得以執行控管措施的管轄地區【11】。

中心化運作的虛擬貨幣系統也可能進行洗錢活動，且可能蓄意尋求洗錢防制／打擊資助恐怖主義機制較薄弱的管轄區進行。去中心化的可轉換虛擬貨幣（decentralised convertible virtual currencies）亦允許人與人之間匿名交易，上述這個方式，其體系很可能會完全處於任何特定國家管轄範圍之外的地區【11】。

4.4 各國對於虛擬貨幣之洗錢防制

FATF 警示虛擬貨幣為法規帶來的諸多挑戰，鑒於全球比特幣及其他虛擬貨幣的快速發展，比特幣等去中心化可轉換的虛擬貨幣，其交易均可於網路進行，且具有相當程度的匿名性，跨越了各國政府長久以來建構的、以金融機構為核心的洗錢防制機制。加上虛擬貨幣可透過法定貨幣購買，可兌換為當地的法定貨幣，使得這類虛擬貨幣被各國政府視為洗錢防制的大敵【11】。

虛擬貨幣交易所或交易平台可將虛擬貨幣轉換為法幣進入金融體系。透過註冊登記成立公司組織之後，於所在國家之銀行開設帳戶，便得以接收消費者匯入之法幣。於是各國政府執行虛擬貨幣洗錢防制的重點就在於對虛擬貨幣交易所或交



易平台進行規範【12】。

4.4.1 FATF

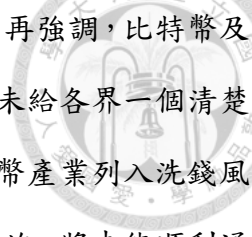
2015 年 6 月，FATF 進一步所提出《虛擬貨幣：風險基礎方法之指導方針（Guidance for a Risk-based Approach – Virtual Currencies）》，探討虛擬貨幣支付產品與服務（適用中心化和去中心化運作的虛擬貨幣）和相關的防制洗錢／打擊資恐議題。並將重點放在可轉換的虛擬貨幣兌換商，著眼在控制虛擬貨幣進入、進出受規範金融體系的途徑，以達到防制洗錢的目的。

FATF 並非建議各國政府將虛擬貨幣交易所或相關交易平台禁絕，而是將虛擬貨幣交易所、錢包或相關交易平台納入既有金融機構定義的範圍，適用與金融機構相當的洗錢防制規範，包含虛擬貨幣業者登錄制度、確認客戶身分和保存交易記錄等【31】。

4.4.2 臺灣

2018 年 4 月初，台灣的國家洗錢及資恐風險評估（National Risk Assessment, NRA）初步結論出爐。根據 NRA 歸納，台灣較為常見和比較嚴重的犯罪類型，其中包含多項具有高風險及非常高風險的洗錢威脅態樣：毒品、貪瀆、詐欺犯罪、逃稅、證券詐欺、組織犯罪和專業洗錢（例如地下匯兌等違反銀行法的洗錢服務犯罪）。而初步結論雖然尚未將金融科技和虛擬貨幣產業納入評估範圍，但是，性質較微接近的電子支付和第三方支付則被列為中風險等級【46】。

台灣即將在 2018 年下半年接受亞太防制洗錢組織（Asia/Pacific Group on Money Laundering，簡稱 APG）的洗錢防制成效相互評鑑。在中央銀行的呼籲之下，於 2018 年 4 月 10 日，法務部所召開的跨部會議討論中，法務部已初步贊同將虛擬貨幣交易平台納入我國洗錢防制法規範，並配合執行反洗錢措施；金管會也要求



銀行加強對虛擬貨幣交易業者開戶及金流的控管。兩大部會都一再強調，比特幣及虛擬貨幣的交易應列入洗錢防制規範，但以何種方式管制，還尚未給各界一個清楚的說法。未來在 APG 評鑑時，非常有可能將金融科技和虛擬貨幣產業列入洗錢風險評估之範圍，如果台灣未能提出有效抵減相關風險的規範及措施，將未能順利通過評鑑，而被列為洗錢高風險國家，在國際金融及貿易上也將可能會面臨到國際制裁或抵制等類似的不利處境【1】。

4.4.3 美國

美國對於任何從事人與人之間，或從某個人至另一個地點的可轉換虛擬貨幣收授與傳輸作業之自然人與法人（包括交易所與管理人）都有管制，均需遵守防制洗錢／打擊資恐之義務，包括註冊、辨識客戶身份、記錄與通報等要求【11】。

美國聯邦政府的防制洗錢／打擊資恐法規適用於使用虛擬貨幣跨境洗錢的行為，如：涵蓋了中心化運作和去中心化運作架構的虛擬貨幣；適用於在美國境內沒有實體存在，但在美國境內全部或大部分經營業務的境外虛擬貨幣交易所／管理人等。目前美國紐約州金融廳（NYFSD）已公佈一項要求部份虛擬貨幣事業取得「比特幣執照」並遵守防制洗錢／打擊資恐義務、消費者揭露規定、資本要求以及投資規定的法規【12】。

根據《砍柴網》於 2017 年 10 月 10 日所發布的一則「美國虛擬貨幣監管借鑑」中提到，為了適應變化的金融科技，美國財政部的金融犯罪執行網路（Financial Crimes Enforcement Network, FinCEN）早於 2011 年 7 月對其和貨幣服務事業（Money service business, MSB）有關的規定做了整體的修訂：聯邦每個州的虛擬貨幣管理機構受聯邦銀行保密法案（BSA）的約束，虛擬貨幣的交易仲介必須按照 MSB 的標準在 FinCEN 進行登記註冊，以防止利用虛擬貨幣洗錢或其他與虛擬貨幣相關的金融犯罪。



4.4.4 日本

FATF 曾在國際上點名批評日本政府限制洗錢和從事恐怖活動資金的對策過於寬鬆，也認為日本的制度本身存在著漏洞。原因之一便是日本在開設銀行帳戶之際身份確認過於寬鬆，即使沒有臉部照片的證件，也可以作為身份證明用以開設帳戶，此種方式增加了透過他人名義開設的帳戶向海外匯出非法資金的風險。同時還指出日本沒有有效的法律手段來阻止犯罪組織等在日本國內匯款等【23】。

日本於 2017 年開始陸續針對虛擬貨幣交易平台及業者之銀行帳戶進行登記並管制，日本政府開始施行新修訂「關於資金支付之法律」及「關於防止犯罪收益移轉之法律」，明文定義「虛擬貨幣」及「虛擬貨幣交換業」，並規定虛擬貨幣交換業者應先向政府申請登錄始能進行業務，並針對虛擬貨幣交換業者的業務監督，將虛擬貨幣交易納入既有關於資金支付的法律中【31】。

4.4.5 中國

2013 年 12 月 3 日，中國和其產業與資訊科技部、銀行監督管理委員會、保險監督管理委員會以及證券監督管理委員會等共同發出比特幣風險預防通知。此通知規定，提供包含比特幣註冊、比特幣錢包和比特幣兌換等服務的機構，應善盡其防制洗錢／打擊資恐義務，並採取措施辨識其客戶身份與記錄身份資訊。金融機構與付款服務提供方也必需針對比特幣服務，採取強化的監督措施，以避免相關風險。此外，中國在世界各地的銀行分行必需研究比特幣相關的洗錢風險，並針對可疑的交易採取相當的行動（包括強化的監管行動和強化監督），以減緩風險【12】。

然而，於 2017 年 9 月中國監管部門決定全面封禁中國的比特幣等加密貨幣的交易渠道，指責它被用來炮製各種非法集資、金融詐騙和行銷騙局，包括洗錢、躲避政府監管向海外轉移巨額資金等。2018 年，中國開始關停國內的比特幣礦場，

並透過取締比特幣挖礦，積極引導企業退出虛擬加密貨幣的挖礦產業。其中國央行副行長更指出，國家和地方政府應該要禁止並查封為虛擬貨幣提供交易的場所，例如提供做市、擔保、清算服務的個人和機構、在線錢包服務的提供商等【4】。

4.4.6 歐洲

歐洲銀行管理局 (EBA) 目前並沒有此類一套全面規範做法的長期建議。EBA 認為一個可能的長期規範做法，需要有一個具體的規範機關而且需要包含 (但不限於) 針對數個市場參與者制定的治理規定、區分客戶帳戶、資本要求以及建立負責虛擬貨幣計畫及其重要成份的誠信度之「計畫主管機關」，包括協定與交易框架。EBA 於 2014 年 7 月提出，建議各國監管機關使金融機構注意到購買、持有或出售虛擬貨幣的風險，並鼓勵消費者們不要購買、持有或出售虛擬貨幣。EBA 也建議歐盟的法規單位考慮宣布虛擬貨幣兌換屬於「義務實體 (obliged entities)」，必需遵循歐盟的防制洗錢指導綱領中制定的防制洗錢與資恐規定。而以上的建議，委員會在進行協調後並未採納【12】。

根據英國《衛報》於 2017 年 12 月 6 日的報導，英國財政部表示，儘管眼前還沒有太多證據顯示虛擬貨幣已淪為洗錢的工具，但很明顯的「這項風險正持續擴大」，英國政府及歐盟皆擔心比特幣及其他虛擬貨幣的匿名性助長洗錢及逃稅。英國財政部已在 2017 年 10 月向英國國會提出修法提案，打算立法要求比特幣交易平台針對交易者進行身分調查等，並且希望能夠在歐盟層級達成共識。而歐盟也打算立法要求比特幣線上交易平台事前查證交易者身分，並及時向主管機關呈報可疑交易。

4.4.7 俄羅斯

根據有關俄羅斯中央銀行的聯邦法律第 27 條，蘇聯禁止發行代理貨幣。2014

年 1 月俄羅斯的中央銀行在其官方網站上發佈「用於執行交易的虛擬貨幣（尤其是比特幣）相關須知」。俄羅斯中央銀行警告個人、法人以及主要是信用機構與非信用的金融機構不要使用虛擬貨幣換取商品、服務或實際的盧布或外幣。因為由人數不限的個人發行的虛擬貨幣，以及使用此類貨幣進行交易均具匿名性，所以非常有可能在不知不覺中涉入非法的活動，包括洗錢／資恐。因此，使用虛擬貨幣換取實際的盧布或外幣以及商品和服務，都將被俄羅斯銀行視為可能讓人從事現行防制洗錢／打擊資恐法案中提到的可疑交易。為了減緩和虛擬貨幣有關的洗錢／資恐的風險，財政部和俄羅斯中央銀行共同制定了禁用電子代理貨幣和禁用電子代理貨幣交易的草案【12】。

下表為統整幾個重點國家對於虛擬貨幣交易平台之監管情形：

表 3、國際間對虛擬貨幣交易平台之監管情形

監管方式	國 家
禁止	中國大陸、俄羅斯、越南、印尼
公開示警	香港
業者自律	瑞士
研議中	台灣、印度
擬採登記制	歐盟央行（ECB）、英國、新加坡、馬來西亞、南韓
登記制	美國、日本、德國、法國、加拿大、菲律賓、澳洲、紐西蘭

資料來源：新時代的貨幣銀行學概要（二版），李榮謙編著



第五章 虛擬貨幣相關之洗錢防制

5.1 針對本文個案之洗錢防範提案

經由本篇的三個虛擬貨幣相關之洗錢事件，與上一章節所探討之洗錢風險，我們可以了解到，由於虛擬貨幣的匿名性，再加上其透過網際網路的全球性等特性，想預防虛擬貨幣的洗錢交易是非常困難、且幾乎不可能的事情。

5.1.1 利用虛擬貨幣進行買賣交易的網路黑市一絲路

匿名網路黑市絲路，透過 Tor 的隱密交易服務與比特幣的匿名性，使得用戶得以在網站上進行非法交易，而不需要有被相關司法機關追蹤的憂慮。而其中的 Tor 洋蔥路由的技術，更加劇了匿名性的特性，使得執法機構難以追蹤特定的可疑交易。因此，此案件使美國聯邦調查局在絲路網站臥底長達兩年時間才得以破案。

地下網站的原本是要保護美國情報通訊而開發的軟體，主要用於軍方內部以及軍艦間，而建立隱蔽性高的通訊網路。而到後來，出現像是此個案中絲路創始人 Ulbricht 的駭客，為了實現真正「網路自由」等自由主義的理論想法，完全隱匿的 IP、用戶名，讓在極權國家、網路被封鎖的民眾也能夠瀏覽到真正的網路。但是，被駭客發現有利可圖之後，而開始建立了充滿犯罪的網路黑市，讓警察機關無法追蹤，才使得地下網站被認為是犯罪的天堂【7】。

自從比特幣問世之後，由於比特幣並不屬於世界上的任何一個國家所擁有，且為了保護地下網站黑市裡的賣家、買家，幾乎每個地下網站黑市都限定以比特幣交

易，使比特幣成為目前網路上流通最廣泛虛擬數位貨幣【7】。亦可以推定說，只要是透過虛擬貨幣交易的地下網站，都有執行洗錢的可能性。因此，針對此個案的預防虛擬貨幣洗錢之方法，應該回到「如何預防地下黑市的形成」這個最初的問題點來解決。然而，這並非本篇論文應要討論的議題，在此便不加以贅述。

5.1.2 現代版的龐氏騙局？虛擬貨幣交易平台 Mt. Gox 之比特幣消失事件

曾為全球最大比特幣交易所 Mt. Gox，雖聲稱遭到駭客竊取或因技術問題，而造成共約 85 萬枚比特幣（市價約值 4 億 8000 萬美元）從帳戶憑空消失。經過駭客攻破 Mt. Gox 的官方網站以及其執行長 Mark Karpeles 的個人微博之後，重重的疑點使司法相關機關初步認定，Mark Karpeles 在比特幣交易系統中進行不正當手段操控帳戶數據和侵占公款的嫌疑。

通過 Mt. Gox 事件使比特幣在安全性和透明性方面，存在巨大問題的情況浮出水面。以這一事件為契機，FATF 發佈了指導方針，要求對虛擬貨幣兌換所實行註冊制和許可制，進行洗錢監管，呼籲為應對日新月異的技術進步，有必要進行法律方面的調整。此外，各國還自主制定了對虛擬貨幣的監管舉措：美國和英國將在相關法律下對虛擬貨幣的結算處理和兌換業務進行管理；歐盟則將虛擬貨幣交易所指定為準金融機構；中國儘管並未對個人用途的比特幣進行限制，但禁止金融機構從事虛擬貨幣業務；俄羅斯也宣佈了使用虛擬貨幣的行為屬於違法的方針【44】。

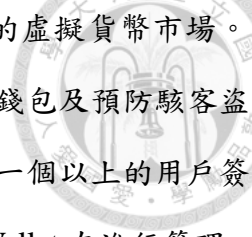
此個案中最大的癥結點在於，身為 Mt. Gox 的執行長兼系統管理者 Mark Karpeles 能進入交易平台之伺服器與數據庫之系統中。Mt. Gox 宣告破產之事發生後，很多國內外的比特幣投資者開始強烈要求虛擬貨幣交易平台，公布其交易平台

的比特幣冷錢包位址，以證明沒有挪用用戶存放在交易平台的比特幣或者其它數位虛擬貨幣。而除了將防治虛擬貨幣之洗錢的重點放在交易平台之外，「交易平台資金第三方的託管」也成為了此個案所特別衍生出的特別解決方案【48】。

交易平台資金第三方的託管，主要是為了避免交易平台因為經營不善或者如此案件之挪用用戶資金、侵占公款，而造成交易平台的用戶損失其本金的風險。國內外比特幣交易平台為了證明自家業者之清白，專門設計了「100%準備金驗證方案」。實行交易平台資產第三方的存管，要徹底把交易的資產和交易過程進行切割，交易平台只負責撮合用戶的交易，而交易資產則存放在其它機構。如此，不但使可以投資者放心地在虛擬貨幣平台進行投資交易，對交易平台來說，也大大地降低了系統上的風險。但是，由於缺乏政府公權力的介入，「交易平台資金第三方的託管」單純依靠行業自律，目前的執行狀況也並不如預期【48】。

5.1.3 虛擬貨幣 NEM 外流失竊案

日本的虛擬貨幣交易所 Coincheck，在數名職員開啟了內含惡意程式軟體的電子郵件之後，交易所的系統便遭到駭客入侵，造成約 580 億日圓（逾台幣 157 億元）的虛擬貨幣「NEM」之損失。而到 2018 年 4 月，有消息人士透露 Monex 預計將支付數十億日圓，以獲得 CoinCheck 公司大多數股權，並且會任命一支全新的管理團隊，在自己監督下重建這家虛擬貨幣交易所。面對如此龐大的虛擬貨幣失竊案，日本金融廳表示，為了要杜絕網路的非法入侵，而造成資金外流的問題，所有虛擬貨幣交易所必須貫徹安全對策。並擬調查日本國內所有虛擬貨幣交易所的安全管理系統，必要時要派員到交易所內部進行檢查。



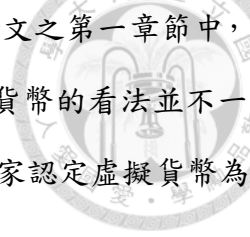
在此個案中，Coincheck 未能升級系統，以跟上快速成長的虛擬貨幣市場。Coincheck 不但未使用多重簽名之技術，來增強用戶的虛擬貨幣錢包及預防駭客盜取 NEM 經濟體中的虛擬貨幣錢包來進行交易（多重簽名是需要一個以上的用戶簽署才得以進行交易）。且交易平台所使用的 NEM 錢包尚以 Hot Wallet 在進行管理，而這項正呈現著 Coincheck 其管理上欠缺考量的重大疏失。

虛擬貨幣錢包之存放方式分為 Hot Wallet（熱錢包）及 Cold Wallet（冷錢包）兩種。Hot Wallet 是完全依靠網際網路的連線，雖然其有提領或交易上快速、方便的優勢，但一當拔除網路線時，也正是駭客伺機而動之時。簡而言之，將虛擬貨幣存放在需連接網路的 Hot Wallet 裡，即是成為了駭客眼中的下手目標。虛擬貨幣交易所為了防止駭客入侵，一般都會用 Cold Wallet 來存放虛擬貨幣。Cold Wallet 類似於實體錢包，可以將虛擬貨幣的數據存放在沒有連接網際網路的電腦、硬碟、手機等，也就是若伺服器離線時，亦可以執行 Cold Wallet 中的虛擬貨幣來進行管理。

5.2 防範虛擬貨幣洗錢行動之提案

以上為針對本篇之三個案，所個別提及之其可行的解決方法。而以下將闡述之防範虛擬貨幣之洗錢方法，除了可適用在本篇的三個個案，亦可以運用到其他之虛擬貨幣相關洗錢案例當中：

由於在虛擬貨幣交易平台 Mt. Gox 的破產訴訟中，東京地方裁判法院指出：在日本現行之法規下，持有者在虛擬貨幣上並不能成立所有權，因此，虛擬貨幣的交易不能適用物權的規則。虛擬貨幣都不能成立所有權的原因，除了在於其匿名的特性，比特幣等數位虛擬加密貨幣不具有實體性，且有如我們所熟悉的通貨貨幣一樣，



比特幣持有者並不能對其進行排他性的支配【45】。也如在本篇論文之第一章節中，談討各國對於虛擬貨幣之態度，可得知目前世界各國對於虛擬貨幣的看法並不一致。雖說迄今多數國家將其認定為金融／普通商品，但亦是有國家認定虛擬貨幣為私人貨幣，甚至是違法商品。

因此，首先應當急速將虛擬貨幣納入各國的法規當中，或另針對虛擬貨幣立法規範。又由於虛擬貨幣非由中央銀行負責發行，也無政府機構負責管理，因此，可以透過像 FATF 等的國際間組織，在國際之法律上，清楚定義虛擬貨幣的價值與定位。透過國際協議的正式發佈，可以明確界定虛擬貨幣的法律性質和業務範圍，與虛擬貨幣交易平台之相對應的經營規則和監管規則等，也可以為往後任何有關虛擬貨幣的訴訟案件訂定一套得以遵循的標準【45】。

美國商品期貨交易委員會（CFTC），已於 2017 年 12 月核准芝加哥商品交易所集團（CME Group）及芝加哥選擇權交易所（CBOE），於全球市場發行比特幣期貨的申請，並開始正式掛牌交易。虛擬商品可在期貨市場開始交易這項事情，顯示出虛擬貨幣之性質漸漸開始趨向原油、大豆、黃金、小麥等大宗商品。然而，美國證券交易委員會（SEC）則以虛擬貨幣存在監管風險為由，接連否決比特幣之指數股票型基金（ETF）申請案。由上述情況可見，CFTC 與 SEC 的兩大美國金融監管單位對虛擬貨幣之監管風險存有不一樣的想法【21】。

期貨是為了讓投資人避險而產生的機制：買賣交易的雙方對標的商品未來價格走勢有不同看法，因而在交易所依自己所能接受的期貨價格成交，且並沒有要求實體交割，而是以合約到期時期貨價格之價差做為獲利與否的衡量；而與 ETF 最大的不同之處在於，ETF 投資人有權利要求將 ETF 兌換為所表彰的實際標的，或提出實際標的請求發行 ETF。期貨的監管風險僅在市場參與者未來能否落實履約



之義務，但以匿名位址進行交易的虛擬貨幣，除非改為實名認證而得以證實其當下為比特幣位址的所有權人，否則在 ETF 上想執行虛擬貨幣交易確實是一大難題【21】。

第二種方法即是將虛擬貨幣交易平台採「實名制」的方式。而目前最先提出此方式的為南韓政府。南韓政府認為當地的比特幣交易已趨於過熱，政策協調辦公室發布聲明，強調將嚴加規範虛擬加密貨幣之交易，具體措施包括交易實名制，甚至授權有關當局關閉交易所等；亦將會禁止未成年人與非韓國居民來交易虛擬貨幣，並且稅務監管機關也將重審關於虛擬貨幣的稅收政策。藉由加強對虛擬貨幣交易平台的監理與管制，以及實施實名制的方式，不但可以提高有效預防可疑交易的機率，也可以避免虛擬貨幣的炒作而造成泡沫化的經濟危機。雖然，這項作法與當初虛擬貨幣受人青睞的匿名性相違背，若執行可能會造成虛擬貨幣的價格暴跌等影響，如：當南韓政府宣布將虛擬貨幣實名制時，比特幣價格一度「嚇跌」至 13,672 美元（較 2017 年年初下滑了 11%）【35】。但此並非本篇論文所關切之重點，本篇論文旨在期望能有效預防虛擬貨幣之洗錢的發生。

然而不幸地，若無法預防到虛擬貨幣之洗錢活動，透過地下網站所交易的虛擬貨幣、或是交易平台之系統管理者挪用用戶所存放的虛擬貨幣、抑或是遭到駭客盜取的虛擬貨幣等不法來源之收益，已經經過轉換成為其他虛擬貨幣的洗清。強化銀行在虛擬貨幣交易所的反洗錢責任便是最後一道防線。在虛擬貨幣交易所開戶時，必須登記姓名、電子郵件等個人資料，且在大筆的匯款手續時還需要確認本人身分的文件，因此，此時若發現任何可疑的虛擬貨幣交易，司法相關單位便可展開進一步的調查行動。



在面對虛擬貨幣之洗錢防制，銀行方面亦可比照實體貨幣之洗錢防制來嚴格監控。根據金融監督管理委員會金管銀法之洗錢防制法條文：

第三條、金融機構確認客戶身分之情形、方式及程序等規定。

第四條、金融機構應婉拒建立業務關係或交易之規定。

第五條、金融機構就客戶身分之持續審查規定。

第六條、金融機構依風險基礎方法執行確認客戶身分，及採取加強確認客戶身分之範圍及方式。

第七條、金融機構依賴第三方執行確認客戶身分應符合之規定。

第八條、金融機構對客戶及交易有關對象之姓名及名稱檢核。

第九條、金融機構對客戶帳戶或交易之持續監控。

第十條、金融機構對擔任重要政治性職務人士確認客戶身分之強化規定。

等審查條例，若就確認客戶身分、紀錄保存及金額之後，發現有疑似洗錢或資恐交易之處，便必須法務部調查局申報，以便進一步的防制。

其中，我們更可以根據一些虛擬貨幣的交易特徵，找出其與實體貨幣防制洗錢的差異，來提高虛擬貨幣洗錢之防制效果。像是：台灣目前的虛擬貨幣交易平台為兩家 BitoEX 和 MaiCoin 所壟斷，因此其交易之手續費也相當的高。在這種情況下，使用虛擬貨幣的洗錢手法，就無法透過實體貨幣「多次小額存款的方式存入」之洗錢手法來完成，因此便得以縮小搜查範圍，而金融體系也得以提高發現可疑交易之機率。但是，在科技不斷的進步之下，未來也非常可能會出現無需手續費的虛擬貨幣交易平台，因此，我們更要必須不斷地更新法制規範。



5.3 國際已擬定之可行方案

根據 FATF 於 2015 年 6 月所發布的《虛擬貨幣：風險基礎方法之指導方針 (Guidance for a Risk-based Approach – Virtual Currencies)》，面對目前虛擬貨幣交易所帶來的挑戰，FATF 擬定了可能的解決方案來應對：

一旦提供去中心化虛擬貨幣的支付產品與服務，應要求金融機構與指定之非金融事業或人員 (Designated non-financial business and profession)，針對此類產品／服務遵守客戶身份建立確認以及監督交易等規定。鑑於分散式、可轉換的虛擬貨幣帶給法律遵循以及執行方面的挑戰，金融機構、指定之非金融事業或人員、開發商、投資者以及在虛擬貨幣領域內的其他各方參與者，均應努力開發有助於提升法律遵循性的科技，解決此問題。舉例來說，開發商也許能創造新的虛擬貨幣科技技術，如：提供客戶身份辨識資訊的應用程式設計界面 (application programming interfaces, APIs)；或允許金融機構或指定之非金融事業或人員，限制交易的規模與速度；或制定、建立各種必需執行某個虛擬貨幣交易前的滿足條件，藉以減少與特定虛擬貨幣交易有關的洗錢／資恐風險。

利用線上收集到的資訊來擴建客戶的基本資料檔案，並協助偵測任何可疑活動與交易之可能性，是另一個有助於提升防制洗錢／打擊資恐法律遵循以及執行的重要領域。與防制洗錢／打擊資恐合規性相關的創新，可以採取改善既有的虛擬貨幣協議，或開發全新的、奠基在完全不同基礎的協議之上的虛擬貨幣等形式。在改善或是在開發新的虛擬貨幣協議的同時，期望能夠內置累積風險減緩的措施，或有助於客戶身份辨識與交易監督。

開發第三方數位身份系統，也有益於提升防制洗錢／打擊資恐之合規性，且這項可能更適用任何虛擬貨幣的交易。舉例而言，第三方數位身份保管方本身就應被管制，以確保身份／確認過程的誠信度。為了響應到國際標準的防制洗錢／



打擊資恐的法律實施規定，這些系統可以往牽涉到第三方數位身份保管方和其他實體單位為特定的 CDD 方案【12】。³³

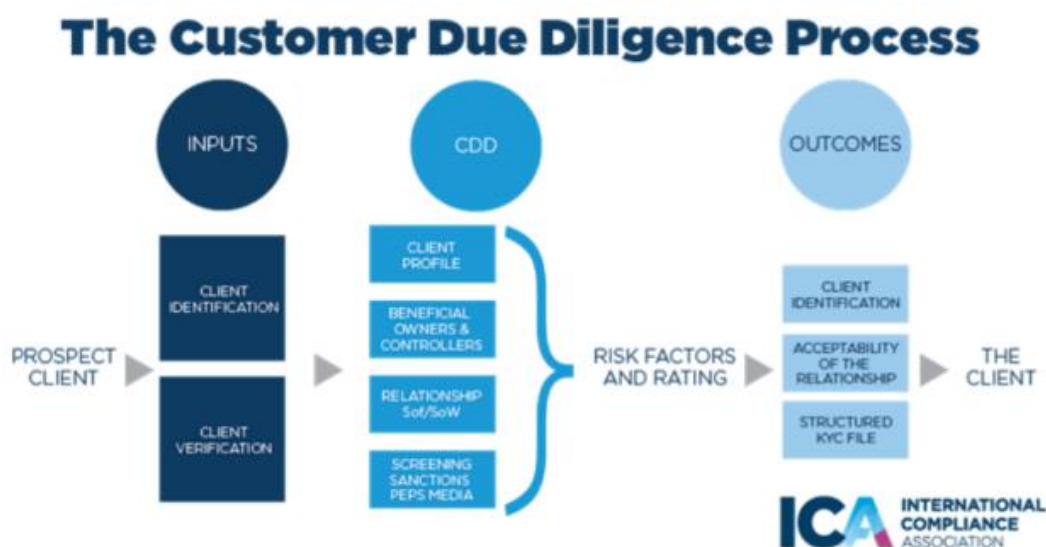


圖 7、CDD 客戶審查之流程圖

圖片來源：int-comp.org -What is Customer Due Diligence (CDD)?

金融機構與指定之非金融事業或人員還可以探索發展中的商業模式，以促進客戶身份辨識／確認、交易監控以及遵守其他相關反洗錢與打擊恐怖融資之法規要求。例如，參與傳輸、轉讓虛擬貨幣的機構，可考慮成立一個含有審查虛擬貨幣交易風險的產業協會，並制定會員應遵守的政策、做法並實踐，使他們能夠確認所執行的相關 CDD 客戶審查，且能方便辨識正在執行的相關交易監控之特定交易。

³³ CDD (Customer Due Diligence) 盡職調查包含關於客戶的訊息事實，而該事實使組織能夠評估客戶，並了解到該客戶會使自己的組織暴露於各種風險的程度。上述的風險包括洗錢和恐怖融資。基於為了防範假冒和身份欺詐；遵守相關法律法規的要求；向金融情報機構提交可以報告之後調查客戶的信息；提供可用的信息使組織能夠協助執法等...上述原因，組織必需要「了解他們的客戶 (Know Your Customers)」。(資料引用來源：int-comp.org -What is Customer Due Diligence (CDD)?)



5.4 國際新科技

企業開始利用科技為金融市場創造更便捷的服務，因此而發展了我們所熟知的 Fintech (金融科技)，但由於金融創新可能會與法律相抵觸而受罰，為了監管市面上的各項服務是否合乎法律，現今又出現了一個新的科技。

RegTech，監管科技，為 Regulation Technology 的縮寫。³⁴可以透過 RegTech 管理快速變動的市場，將原先的監管制度加入技術後，就可以利用 RegTech 管理各家公司是否合規。監管科技公司可以利用機器學習、人工智慧等科技來管理各金融公司，運用科技來管理資安、交易安全、洗錢之法律遵循等問題，並且有助於提升公司透明化。

根據《INSIDE 硬塞的網路趨勢觀察》的硬塞科技字典提及，利用 RegTech，監管者也可以實時監測業者的營運活動，並且協助業者隨時做到法令遵循。RegTech 的導入將大幅降低原先的監理成本以及業者為了要配合法令遵循所產生的成本，目前英國金融監理總署 (FCA) 也極力推動相關 RegTech 的發展。

³⁴ 資料引用來源：【硬塞科技字典】什麼是監管科技 (Regtech)？。2016 年 9 月 1 日。INSIDE 硬塞的網路趨勢觀察，取自：<https://www.inside.com.tw/2016/09/01/what-is-regtech>



第六章 結論

虛擬貨幣的匿名性與全球性，將其洗錢防制／打擊資助恐怖主義的困難度提升到近乎不可能的地步。

透過參考 FATF 防制洗錢金融行動工作組織針對虛擬貨幣洗錢所擬定的可行辦法，與本篇論文之三個個案的分析探討，可歸納出三項可應用於任何防制虛擬貨幣洗錢案件的通則：

一、明確界定虛擬貨幣的法律性質和業務範圍

透過國際間組織所商討，並將協議的正式發佈，以清楚定義虛擬貨幣的價值與定位，與其交易平台之相對應的經營規則和監管規則等，並為往後任何有關虛擬貨幣的訴訟案件訂定一套得以遵循的標準。可採取改善既有的虛擬貨幣協議，或開發全新的、奠基在完全不同基礎的協議，期望兩者能夠內置累積風險減緩的措施，或有助於客戶身份辨識與交易監督。

二、採取「實名制」

為了提高有效預防可疑交易的機率，避免虛擬貨幣的炒作而造成泡沫化的經濟危機，可藉由對虛擬貨幣交易平台實施實名制的方式。虛擬貨幣交易所或交易平台可將虛擬貨幣轉換為法幣進入金融體系，因此，各國政府執行虛擬貨幣洗錢防制的重點也就在於對虛擬貨幣交易所或交易平台進行規範。

三、強化銀行在虛擬貨幣交易所的反洗錢責任

可比照實體貨幣之洗錢防制來嚴格監控，以提高偵測任何可疑活動與交易之可能性；或制定、建立各種必需執行某個虛擬貨幣交易前的滿足條件，藉以減少與特定虛擬貨幣交易有關的洗錢／資恐風險。




另外，針對本篇論文之虛擬貨幣交易平台 Mt. Gox 個案，所衍生之「交易平台資金第三方的託管」方法。若再開發第三方數位身份系統辨識，也有益於提升防制洗錢／打擊資恐之合規性，且這項可能更適用任何虛擬貨幣的交易。

隨著虛擬貨幣的快速擴張與廣泛應用，世界各國除了必須要加緊腳步制定出一套管制虛擬貨幣之法律規範，亦必須要時時注意發展的動向，以更新法律規範之內容。



參考文獻


- 【1】 admin (2018 年 3 月 5 日)，各國對虛擬貨幣態度，雪花新聞。取自：
<https://www.xuehua.us/2018/03/05/%E5%90%84%E5%9B%BD%E5%AF%B9%E8%99%9A%E6%8B%9F%E8%B4%A7%E5%B8%81%E6%80%81%E5%BA%A6/zh-tw/>
- 【2】 admin (2018 年 3 月 5 日)，據報道被盜的價值 5500 萬美元的 NEM 已被洗白，雪花新聞。取自：
<https://www.xuehua.us/2018/03/27/%E6%8D%AE%E6%8A%A5%E9%81%93%E8%A2%AB%E7%9B%97%E7%9A%84%E4%BB%B7%E5%80%BC5500%E4%B8%87%E7%BE%8E%E5%85%83%E7%9A%84nem%E5%B7%B2%E8%A2%AB%E6%B4%97%E7%99%BD/zh-tw/>
- 【3】 Amy Lin (2016 年 1 月 19 日)，購物網站「絲路」下線 暗黑網路布局夢醒，科技新報 TechNews。取自：<https://technews.tw/2016/01/19/silk-road-dark-web-is-dead/>
- 【4】 BBC NEWS (2018 年 1 月 12 日)，比特幣禁令：清理挖礦、禁止交易 中國還是最大玩家嗎？。取自：<http://www.bbc.com/zhongwen/trad/business-42660591>
- 【5】 Chris (2015 年 11 月 3 日)，金管會曾銘宗：「比特幣在台灣是不合法的支付工具」INSIDE 硬塞的網路趨勢觀察。
取自：<https://www.inside.com.tw/2015/11/03/bitcoins>
- 【6】 ETtoday 新聞雲 (國際>國際焦點，2013 年 3 月 25 日)，非法「絲路」線上賣毒品 月 170 萬美元進帳。
取自：<https://www.ettoday.net/news/20130325/180976.htm#ixzz5F5uNCmFk>
- 【7】 ETtoday 新聞雲 (社會>社會焦點，2013 年 4 月 13 日)，暗黑絲網路／見不得光的都在這交易 「暗網」大揭密。
取自：<https://www.ettoday.net/news/20170413/902872.htm#ixzz5IZ2Vnzw3>
- 【8】 ETtoday 新聞雲 (社會>社會焦點，2017 年 4 月 13 日)，暗黑絲網路／違法的..「暗網」都賣 警：各國都難抓。
取自：<https://www.ettoday.net/news/20170413/903813.htm#ixzz5FR1byEK9>

- 
- 【9】 ETtoday 新聞雲 (財經>財經焦點, 2018 年 1 月 30 日), 日本首例! 比特幣也可買房 547 枚就可入手市價 1.7 億商業大樓。
取自: <https://www.ettoday.net/news/20180130/1102603.htm>
- 【10】 European Central Bank (2012), Virtual currency schemes OCTOBER 2012.
- 【11】 FATF (June 2014) -Virtual Currencies Key Definitions and Potential AML/CFT Risks.
- 【12】 FATF (June, 2015), GUIDANCE FOR A RISK-BASED APPROACH—VIRTUAL CURRENCIES.
- 【13】 Harry (政府法令, 2018 年 2 月 7 日), 美國參議院聽證會對加密貨幣的看法, 幣東 CoinEast。
取自: <http://coineast.com/mei-guo-can-yi-yuan-ting-zheng-hui/>
- 【14】 M&A Online (2018 年 5 月 1 日), 2,000 億円のビットコインが眠る MTGOX の行方。取自: <https://maonline.jp/articles/tsr0129mtgox>
- 【15】 Satoshi Nakamoto (2008), Bitcoin: A Peer-to-Peer Electronic Cash System.
- 【16】 UNWIRE.HK 玩生活·樂科技 (科技趣聞·資訊保安, 2018 年 1 月 27 日), 日本交易所 Coincheck 被盜 42 億虛擬貨幣 買賣提款全部停止。
取自: <https://unwire.hk/2018/01/27/coincheck/fun-tech/>
- 【17】 UNWIRE.HK 玩生活·樂科技 (資訊保安, 2018 年 1 月 30 日), 日本 Coincheck 已鎖定 42 億被盜 NEM 虛擬貨幣行蹤。
取自: <https://unwire.hk/2018/01/30/coincheck-3/tech-secure/>
- 【18】 UNWIRE.HK 玩生活·樂科技 (資訊保安, 2018 年 3 月 21 日), 停止追查被盜 43 億虛擬貨幣下落 被盜 NEM 基本上已被「洗淨」。
取自: <https://unwire.hk/2018/03/21/nemmosaicend/tech-secure/>
- 【19】 worm2ipo (2014 年 3 月 13 日), 時間線: Mt. Gox 事件始末與比特幣的興衰, TECH2IPO/創見。取自: <http://tech2ipo.com/63750>
- 【20】 Xtester (Aug 9, 2014), The New Economy Movement, Medium.
Retrieved from <https://medium.com/@xtester/the-new-economy-movement-fb9bb67eb9fe>

- 
- 【21】 工商時報主筆室（2017 年 12 月 11 日），工商社論《比特幣會泡沫化嗎？中時電子報 CTnews》。
取自：<http://www.chinatimes.com/newspapers/20171211000030-260202>
- 【22】 巴比特資訊（2017 年 7 月 14 日），門頭溝 85 萬個比特幣被盜一空！東京公審他竟拒絕認罪！。取自：<http://www.8btc.com/mt-gox-mark-karpeles>
- 【23】 中村亮（2014 年 9 月 30 日），日本反洗錢對策很薄弱？，NIKKEI—日本經濟新聞中文版。
取自：<http://zh.cn.nikkei.com/politicaeconomy/efinance/11249-20140930.html>
- 【24】 中華人民共和國中央人民政府（2017 年 6 月 23 日），廣東佛山探索「區塊鏈政務應用」推進「互聯網+政務」。
取自：http://big5.gov.cn/gate/big5/www.gov.cn/xinwen/2017-06/23/content_5204956.htm
- 【25】 台灣金融研訓院，貨幣的定義。
取自：<http://service.tabf.org.tw/fbs/Doc/Preview/67043.pdf>
- 【26】 合作媒體雷鋒網謝么（INSIDE 授權轉載，2017 年 6 月 3 日），兩年狂賺 360 億卻又終身監禁 暗網「絲路」創辦者的末路，INSIDE 硬塞的網路趨勢觀察。取自：<https://www.inside.com.tw/2017/06/03/ross-ulbricht-the-creator-of-silk-road>
- 【27】 全國法規資料庫（法規類別：行政>法務部>檢察目，2016 年 12 月 28 日），《洗錢防制法》。
取自：<http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=G0380131>
- 【28】 吳必然、張嘉予、郭彥彤（2018 年 2 月 24 日），FINTECH 專欄：虛擬貨幣管制逐漸趨嚴？，風傳媒 The Storm Media。
取自：<http://www.storm.mg/article/402229>
- 【29】 李忠謙（2015 年 8 月 1 日），史上最大比特幣消失事件 Mt.Gox 社長涉有重嫌在日被捕，風傳媒 The Storm Media。
取自：<http://www.storm.mg/article/59621>

- 
- 【30】 宋俊賢、林安邦、董澤平（2014年6月），虛擬貨幣於電子商務之發展及其法律上之衝擊，電子商務研究 12 卷 2 期。
- 【31】 谷湘儀、李偉琪（2018年1月28日），FINTECH 專欄：虛擬貨幣的洗錢防制—管制而非禁絕，風傳媒 The Storm Media。
取自：<http://www.storm.mg/article/390797>
- 【32】 李榮謙（2014年8月28日），新時代的：貨幣銀行學概要（二版），智勝文化事業有限公司。
- 【33】 金卡生活（2017年7月7日），「反洗錢」從反洗錢角度看美國虛擬貨幣監管制度，每日頭條 kknews。
取自：<https://kknews.cc/finance/m3mla5g.html>
- 【34】 知乎專欄（2018年2月6日），想用虛擬貨幣去洗錢？區塊鏈上的黑名單！。取自：<https://zhuanlan.zhihu.com/p/33626266>
- 【35】 林信男（2017年12月28日），南韓政府將推虛擬貨幣「實名制」比特幣嚇跌 11%，鉅亨網。
取自：<https://news.cnyes.com/news/id/4001254>
- 【36】 虎嗅網（2013年10月3日），迄今為止最大的比特幣「翻船」事件！比特幣應用的大本營絲路網站被 FBI 查抄。
取自：<https://www.huxiu.com/article/21082/1.html>
- 【37】 金融監督管理委員會（公告資訊>新聞稿，2017年12月19日），金管會再次提醒社會大眾投資比特幣等虛擬商品的風險。
- 【38】 郭佳（2017年8月5日），暗網電商「絲綢之路 3.1」被黑 宣布破產，雷鋒網。
取自：<https://www.leiphone.com/news/201708/JCcsWWup1v09jRG9.html>
- 【39】 區塊鏈勢 blocktrend（2017年8月22日），解讀中本聰的比特幣論文：什麼是比特幣？。取自：<https://blocktrend.today/08-22-2017-satoshi-nakamoto-bitcoin-a-peer-to-peer-electronic-cash-system>

- 
- 【40】 區塊鏈有話說 (2017 年 9 月 28 日)，比特幣：站在十字路口，數字貨幣的未來是什麼樣的，每日頭條 kknews。
取自：<https://kknews.cc/finance/ax3a4bv.html>
- 【41】 傅莞淇 (2014 年 3 月 1 日)，比特幣交易所 Mt. Gox 受駭宣告破產，風傳媒 The Storm Media。取自：<http://www.storm.mg/article/28003>
- 【42】 黃菁菁 (2018 年 1 月 30 日)，日虛擬貨幣 NEM 系統堪憂 20 分內被盜 157 億卻無感，中時電子報 CTnews。
取自：<http://www.chinatimes.com/realtimenews/20180130001909-260408>
- 【43】 黃菁菁 (2018 年 2 月 9 日)，日警鎖定 被盜虛擬貨幣在紐西蘭頻繁交易，中時電子報 CTnews。
取自：<http://www.chinatimes.com/realtimenews/20180209002953-260408>
- 【44】 鈴木大祐 (2017 年 7 月 11 日)，Mt. Gox 比特幣被盜事件首次公審，NIKKEI—日本經濟新聞中文版。
取自：<http://zh.cn.nikkei.com/politicaeconomy/efinance/25978-2017-07-11-07-09-54.html>
- 【45】 楊東、陳哲立 (資訊保安，2018 年 3 月 23 日)，虛擬貨幣立法：日本經驗與對中國的啓示，衆籌金融研究院。
取自：<https://www.jinse.com/bitcoin/173157.html>
- 【46】 蔡昆洲律師、Enlighten Law Group 創辦人、Fintech Taiwan 專家會員 (2018 年 4 月 25 日)，專家傳真—虛擬貨幣交易洗錢風險 對台灣的潛在威脅，中時電子報 CTnews。
取自：<http://www.chinatimes.com/newspapers/20180425000249-260202>
- 【47】 蔡依琳 (2016 年 1 月)，虛擬通貨之近期發展，財經資訊季刊 85 期。
- 【48】 潘國力 (2017 年 1 月 11 日)，從 MTGOX 倒閉事件，淺談比特幣交易平台第三方存管，壹讀。取自：<https://read01.com/OD270g.html>
- 【49】 謝秉芸 (2017 年 9 月 20 日)，日本變比特幣最大交易市場！強推虛擬貨幣「J-COIN」搶回 Apple Pay 使用者數據，科技報橘 TechOrange。
取自：<https://buzzorange.com/techorange/2017/09/20/japan-jcoin-and-bitcoin/>

- 
- 【50】 饅頭老妖 (2013 年 10 月 16 日), 「絲綢之路」被查抄 比特幣不再是法外之地, 果殼網。取自：<https://www.guokr.com/article/437485/>
- 【51】 蘇南桓檢察官 (2014 年 1 月 7 日), 洗錢防制簡介, 臺灣高等檢察署臺南檢查分署。取自：
<http://www.tnh.moj.gov.tw/ct.asp?xItem=134795&CtNode=24055&mp=005>