第十章

密碼貨幣與區塊鏈

五南文化事業機構
WU-NAN CULTURE ENTERPRISE

10-1 去紙幣化

- 各國「去紙幣化」目標

區域	實施狀況
丹麥	1990年，約有80%的民眾使用現金和支票為主要支付工具。2014年約有75%民眾使用記名轉帳卡至線上購物，而現金和支票僅約25%。以訂定「貨幣全面電子化」為目標發展而言，自2012-2016年以來，約85%民眾用手機內的電子錢包作為電子交易支付工具。
瑞典	電子支付超過80%的交易總量，民眾普遍使用信用卡或智慧手機App程式（Swish）付款。根據國際清算銀行資料指出，瑞典全國現金交易僅占整體經濟活動約2%。
挪威	民眾使用現金消費比率已低於6%。
韓國	政府提供相關「減稅誘因」給消費者與商家，以提升刷卡消費利用率，進而取代現金支付。
台灣	2015年開始推動「無現金社會五年計畫」，要求公部門和大型醫院接受信用卡和悠遊卡等支付方式，以期將電子支付占個人消費支出比率，五年內由26%提高至52%的目標。
中國大陸	民眾透過支付寶、微信支付等方式，已從現金交易習慣改變成電子支付消費方式。另外，於2013年比特幣交易額已達世界交易額40%以上，許多大型企業亦開始接受比特幣支付方式。
美國	2015年民眾仍有47%以上仰賴現金交易。

10-2 比特幣的緣起與介紹

- 傳統貨幣與比特幣的不同點

特點	傳統貨幣	比特幣
樣式	紙鈔、錢幣、存摺數字	私鑰或比特幣錢包數字。
取得	勞動或贈送	挖礦或贈送
製造	中央銀行	P2P網絡挖礦
保存	錢包、皮夾、儲蓄	比特幣錢包
價值	國家信用與人民的信心	演算法、P2P網絡、人民信心
交易	現金、信用卡、金融卡	公鑰與私鑰進行

10-2 比特幣的緣起與介紹

- 傳統貨幣與比特幣的不同點

特點	傳統貨幣	比特幣
樣式	紙鈔、錢幣、存摺數字	私鑰或比特幣錢包數字。
取得	勞動或贈送	挖礦或贈送
製造	中央銀行	P2P網絡挖礦
保存	錢包、皮夾、儲蓄	比特幣錢包
價值	國家信用與人民的信心	演算法、P2P網絡、人民信心
交易	現金、信用卡、金融卡	公鑰與私鑰進行

10-2 比特幣的緣起與介紹

- 區塊鏈節點的國家分布

排名	區域	節點
1	美國	1,949（33.4%）
2	德國	792（13.57%）
3	法國	419（7.18%）
4	荷蘭	335（5.74%）
5	加拿大	271（4.64%）
6	英國	269（4.61%）
7	俄羅斯	170（2.91%）
8	瑞典	139（2.38%）
9	中國大陸	107（1.83%）
10	澳大利亞	105 （1.80%）

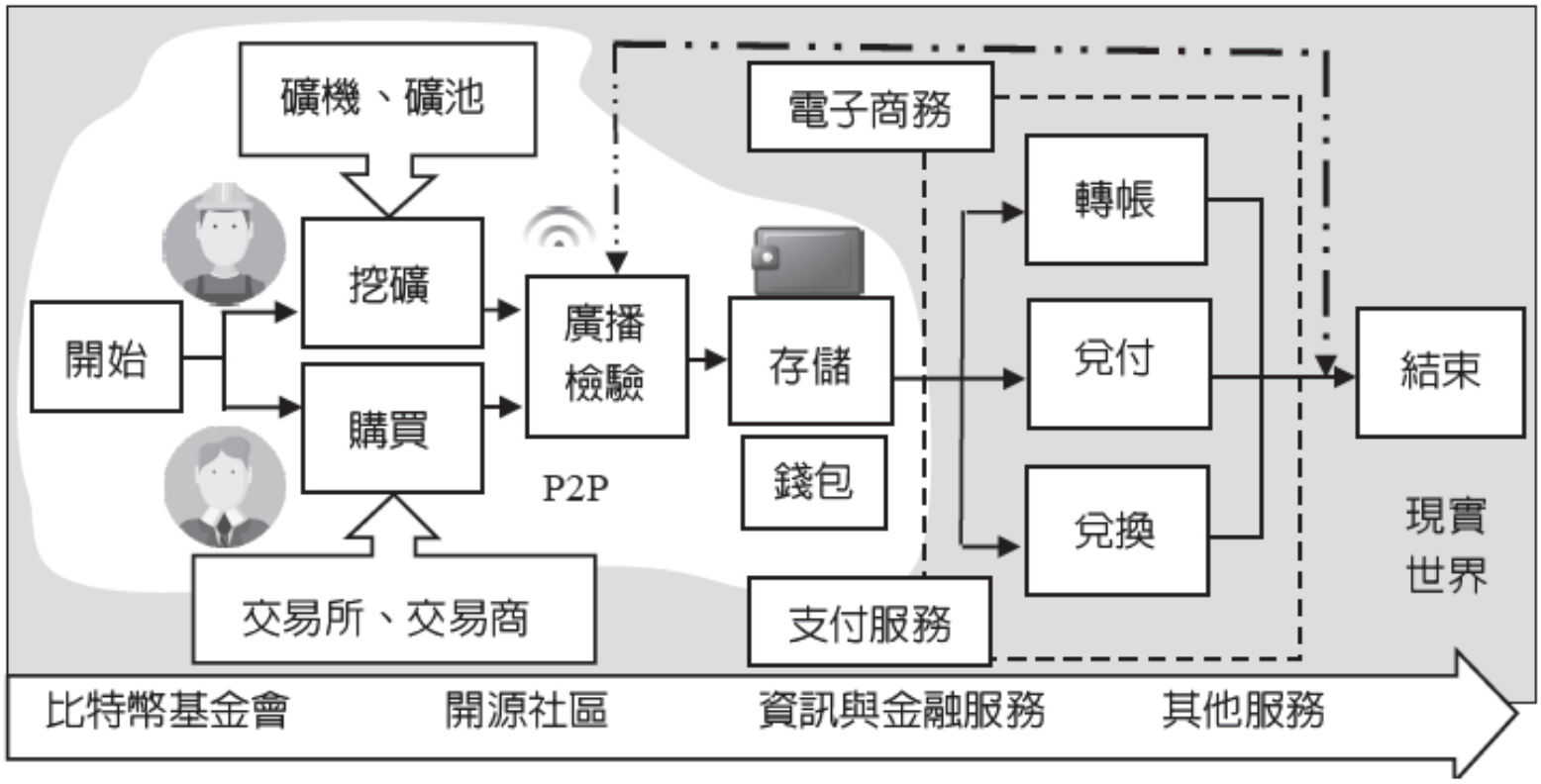
10-2 比特幣的緣起與介紹

一、虛擬通貨監管程度

區域	AML/CFT[1]適用現行法規或警示	證券代幣	合法性	稅務處理	平台須特許或註冊	禁止挖礦	禁止匿名帳戶	消費者警示	禁止ICO發行	金融業警示或禁止虛擬通貨	禁止掛牌	禁止使用
阿根廷	警示							v		警示		
玻利維亞									v			v
加拿大	修訂法規		v	v				v				
中國大陸					禁止	v			v	禁止		v
南韓	加強監管						v		v	禁止		
法國	現行法規			v				v				
德國	現行法規											
義大利								v		警示		
日本	新法規[3]		v		v			v				
南非								v				
英國	現行法規			v								
美國[2]	聯邦法			v	v		v	v	v			
澳洲	現行法規			v			v					
以色列											v	
台灣	現行法規	v		v			v					
香港、阿聯		v										
瑞士	修訂法規		v									
丹麥、印度				v								
俄羅斯	現行法規		v					v	v			
新加坡	新法規			v				v	v			

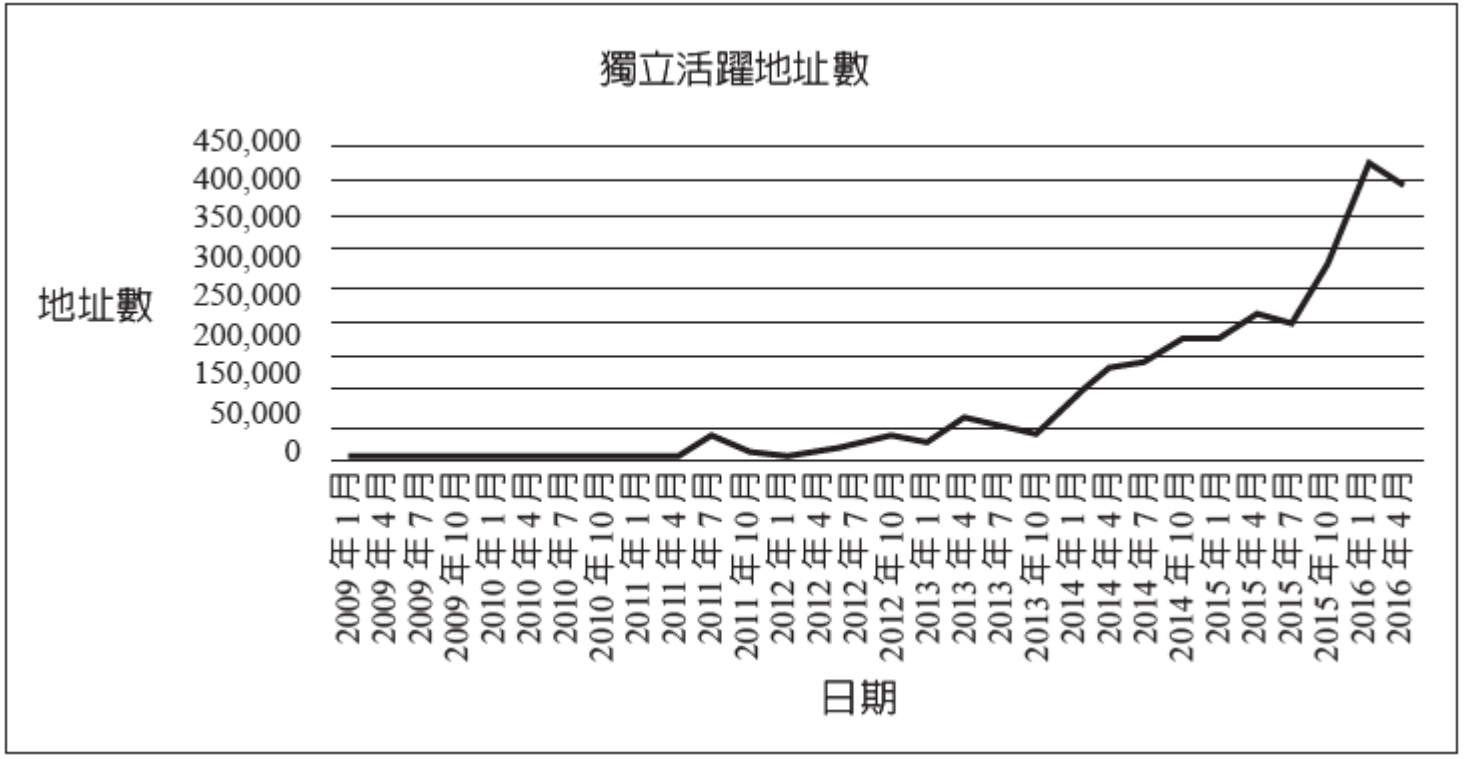
10-2 比特幣的緣起與介紹

二、比特幣流通



10-2 比特幣的緣起與介紹

二、比特幣流通



- 全球獨立活躍地址數

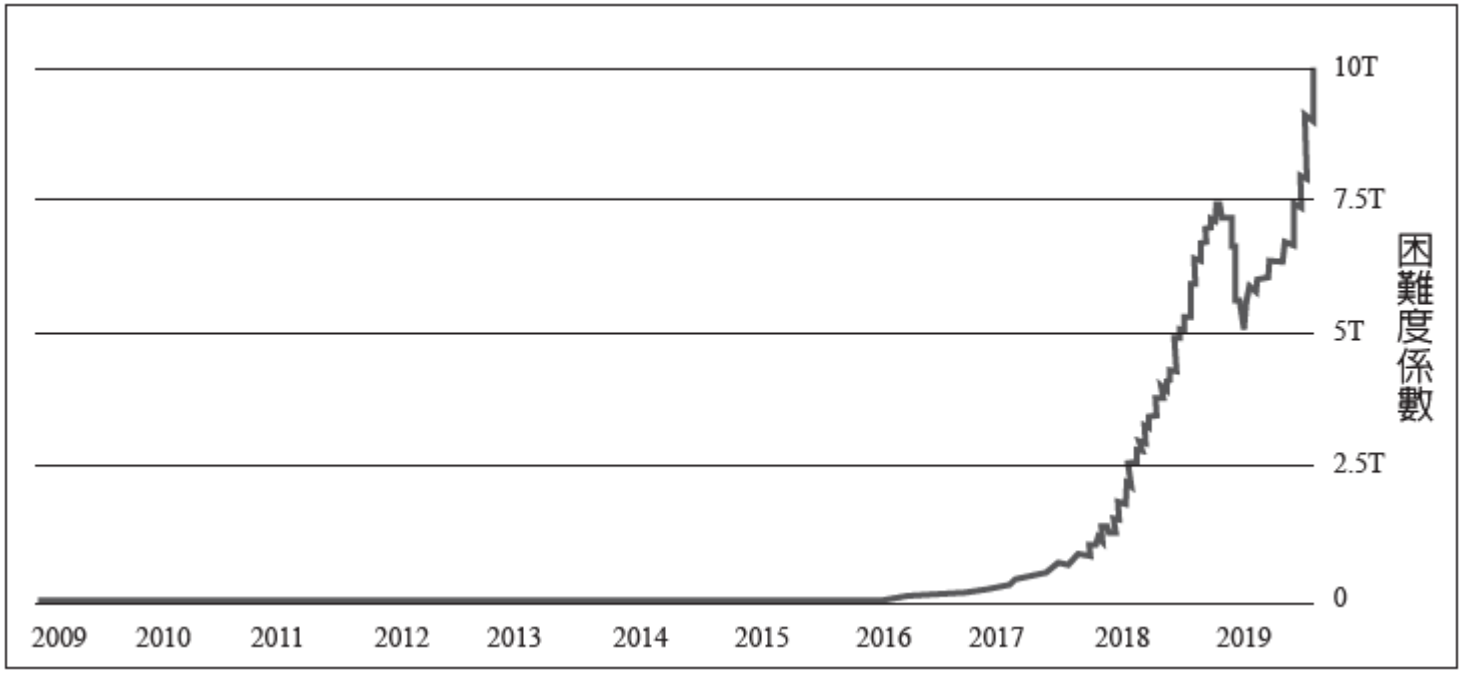
10-2 比特幣的緣起與介紹

三、挖礦（Mining）方式

- 礦工（Miner）下載比特幣專門運算挖礦免費程式，例如：GUI Miner、50Miner、CG Miner、Diablo Miner 等。輸入帳戶和密碼資訊後，按「運算」開始加入礦工們行列，進行類似挖掘金礦的挖礦競賽，此為比特幣生成的唯一途徑
- 自2014 年至2019 年困難度係數開始持續攀升到天文數字與倍數，說明挖礦實屬異常艱辛過程，因而衍生比特幣礦池與礦機產業興起

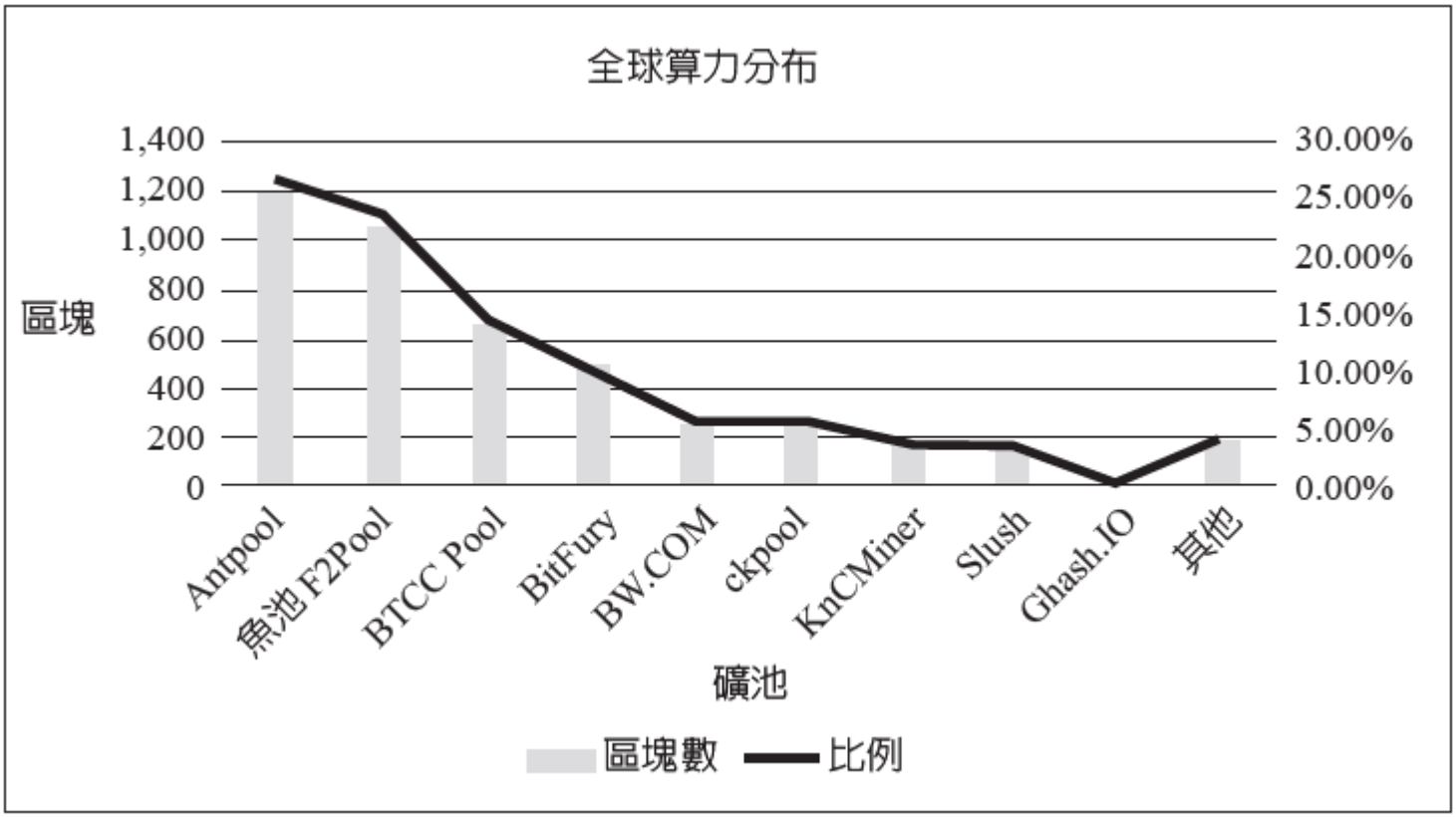
10-2 比特幣的緣起與介紹

- 比特幣難度係數



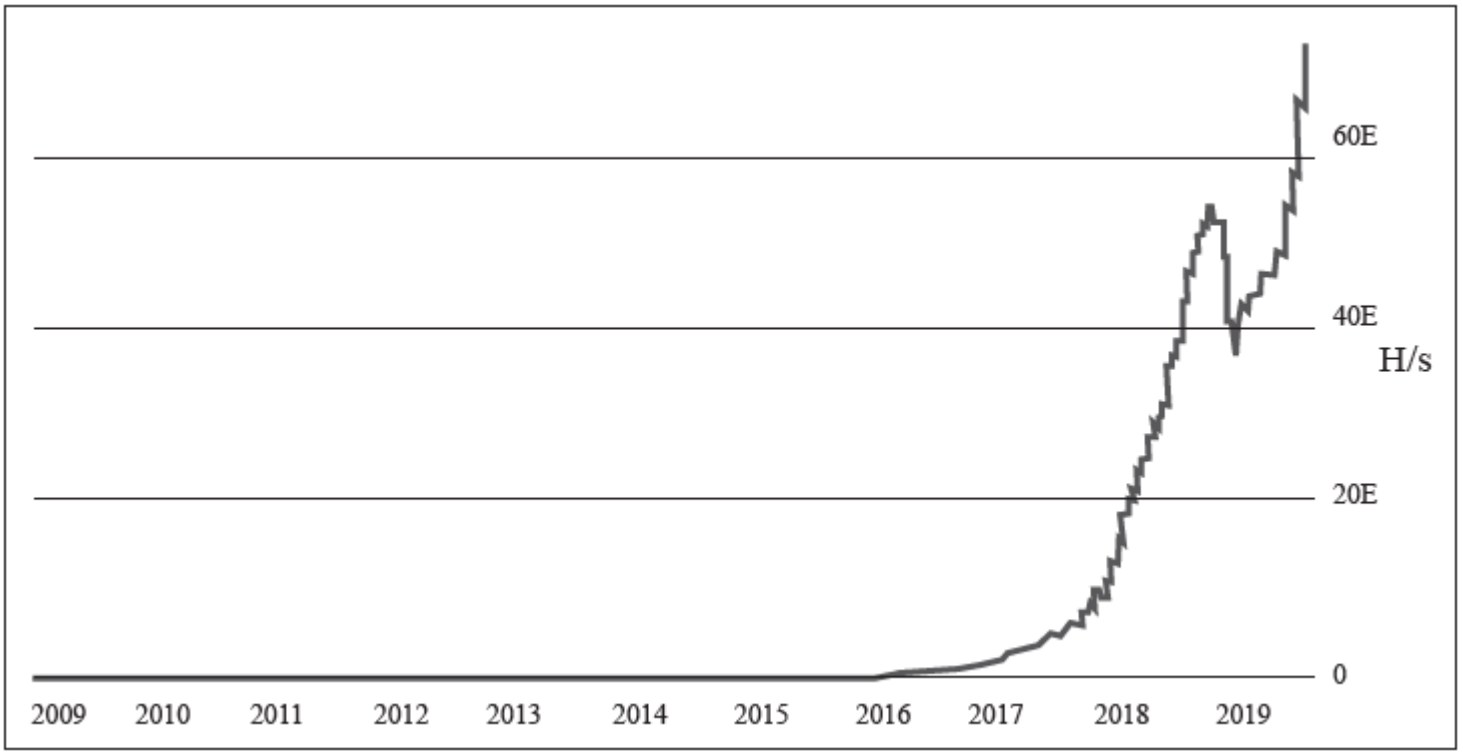
10-2 比特幣的緣起與介紹

- 全球算力分布



10-2 比特幣的緣起與介紹

- 全網挖礦總算力趨勢圖



10-2 比特幣的緣起與介紹

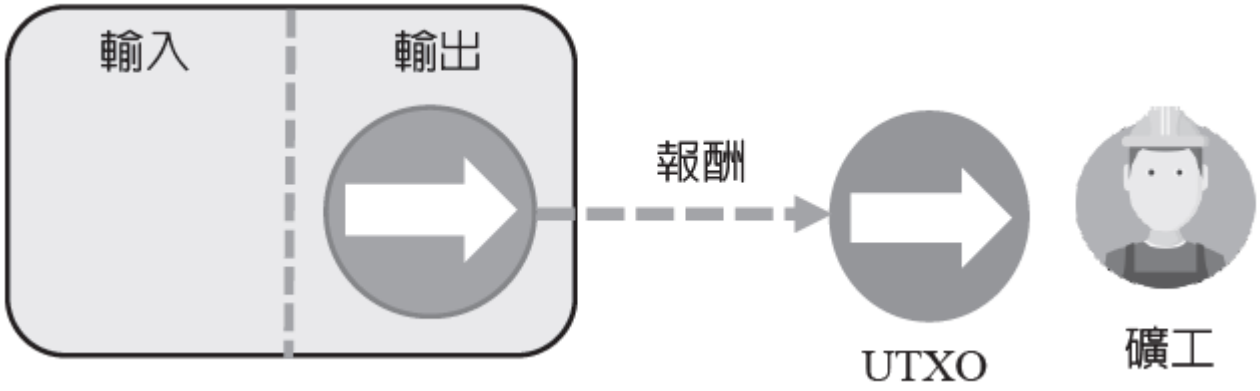
- 比特幣挖礦發展

日期	區域	規格	事件
2008		CPU	第一位礦工Hal Finney運用中央處理器（Central Processing Unit, CPU）挖礦。
2011		繪圖處理器（Graphic Processing Unit）	駭客利用GPU繪圖處理器編寫挖礦程式，促成比特幣礦業第一次產業升級。GPU的平行處理能力約CPU的50到100倍。
2011	中國大陸	FPGA（Field Programmable Gate Array）	第一、二代場效可程式邏輯閘陣列（FPGA）礦機，分別提供360-400MH/s，其速度超過GPU數倍。
2012.8.9		ASIC（Application Specific Integrated Circuit）	特定應用積體電路（ASIC）礦機公司（烤貓）向全球網友籌募資金，以每股0.1比特幣募集股權型眾籌，發行40萬股份。此礦機可提高哈希計算效能，增加挖礦效率。
2013.5.19			礦工（節點）數量達85,220個，占全球22.8%，名列全球第一。
2013.9		ASIC	ASIC.COM平台推出第一代ASICME Avalone系列挖礦機。
2013		FPGA（Field Programmable Gate Array）	場效可程式邏輯閘陣列（FPGA）可提供高電源效率和克服原有可程式邏輯閘陣列電路數有限的問題。
2013.4.30	瑞典	ASIC設計和生產	ORSoC與KNCminer合作開發礦機。
2013.5	中國大陸	雲挖礦代理	Dig Coin平台利用雲計算方式，組成礦機集群，透過計算力分享、技術研發和系統維護，協助客戶挖礦。
2013.6.29		Bit.sh V1 ASIC礦機	七彩神仙魚透過QQ（騰訊通訊軟體），以預付款方式籌資3,000比特幣，成功研發Beehive蜂巢式礦機。
2013.9.2			算力約達700 （TH/s），較6月成長6-7倍。
2016.6.21	中國大陸	Avalon礦機	嘉楠耘智公司發展數位區塊鏈設備，以人民幣30.6億元被收購。
2017.6.12	台灣	NVIDIA和AMD繪圖晶片	挖礦風潮帶動繪圖晶片需求暴增，使顯示卡和挖礦主機板受惠。

10-2 比特幣的緣起與介紹

四、生產交易紀錄（Coinbase）

- 電腦程式會利用演算法（Algorithm）計算與搜尋電腦64 位元數字，並透過資料探勘（Data Mining）方式開採。



- Coinbase 特殊交易紀錄

10-3 區塊鏈技術演進階段

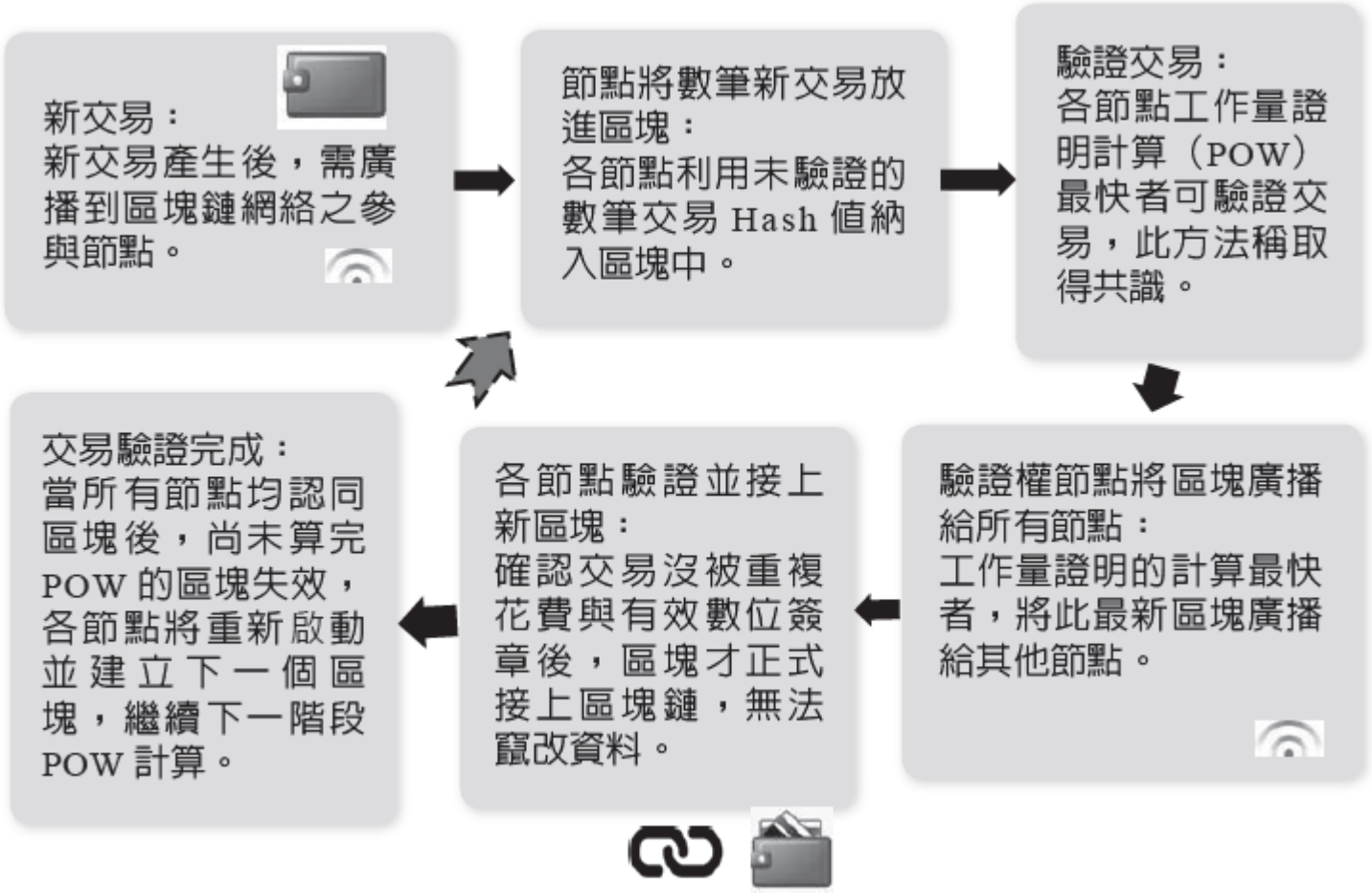
- 區塊鏈技術演進四個階段

階段	年代	名稱	技術演進
區塊鏈1.0：密碼貨幣	1982	密碼學網路支付系統	David Chaum提不可追蹤性、隱私安全密碼學網路支付系統。
	1985	橢圓曲線密碼學	Neal Koblitz和Victor Miller創立橢圓曲線密碼學（Elliptic Curve Cryptography, ECC），建置安全性高公開金鑰加密演算法。
	1990	不可追蹤的密碼學網路支付系統	David Chaum利用此網路支付系統，建置非去中心化的eCash。
	1991	使用時間截確保數位文件安全	由Stuart Haber和Scott Stornetta創造出此協議。
	1992	橢圓曲線數位簽章演算法	Scott Vanstone等人率先發展橢圓曲線數位簽章演算法（Elliptic Curve Digital Signature Algorithm, ECDSA）。
	1997	Hashcash技術和工作量證明機制（Proofs of Work, POW）演算法	Adam Back創造Hashcash技術，具不可逆性成本函數，易於驗證和難於破解的屬性。最早是運用於阻絕垃圾郵件。
	1998	匿名分散式電子現金系統（B-Money）	B-Money導入工作量證明機制，具P2P交易與不可竄改屬性。
		去中心化數位貨幣系統（Bit Gold）	Nick Szabo發表Bit Gold，參與者結合運算力，一起合力解謎。
	2002	Hashcash論文發表	Adam Back正式發表Hashcash系統論文。
	2005	可重複使用的工作量證明機制（Reusable Proofs of Work, RPOW）	Hal Finney發表可重複使用的工作量證明機制，將B-Money和Hashcash演算法連結，為密碼學貨幣創成之先驅。
	2008	比特幣	中本聰發表比特幣論文。
區塊鏈2.0：智慧資產	2012	彩色幣（Colored Coin）	區塊鏈開源協議（Open Assets Protocal）發行與轉移貨幣以外數位資產，如股票與債券交易。

階段	年代	名稱	技術演進
區塊鏈2.5：智慧契約	2014	代幣	代幣應用於金融領域聯盟制區塊鏈，如1：1美元法幣數位化。
		Ripple密碼貨幣	無交易所之國際匯款網路。
		Factom和MaidSafe密碼貨幣	資料層區塊鏈（Data Layers Blockchain）、分散式帳本（Distributed Ledgers）儲存、人工智慧（Artificial Intelligent）之金融應用。
區塊鏈3.0：複雜型智能合約	2014	Ethereum密碼貨幣	區塊鏈3.0導入政府、醫療、科學、音樂版權、文化與藝術領域。如再生能源、身分識別、生產履歷、票務交換、公證、仲裁、審計轉/分帳自動結算、簽證、投票、社會治理或網域名稱等事務。

10-3 區塊鏈技術演進階段

一、區塊鏈交易流程

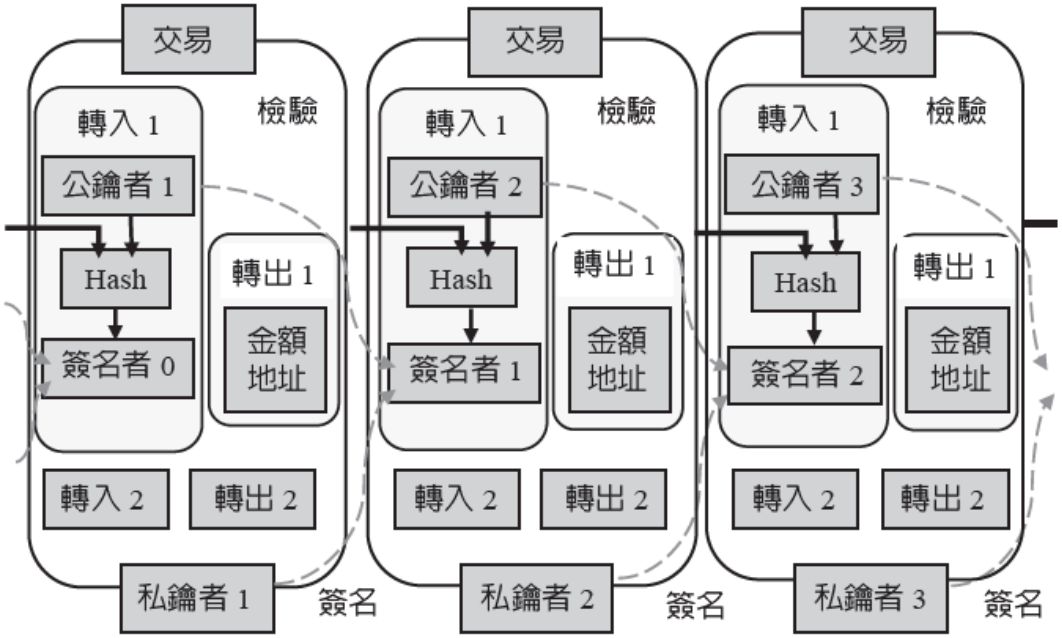


10-3 區塊鏈技術演進階段

二、區塊鏈關鍵技術

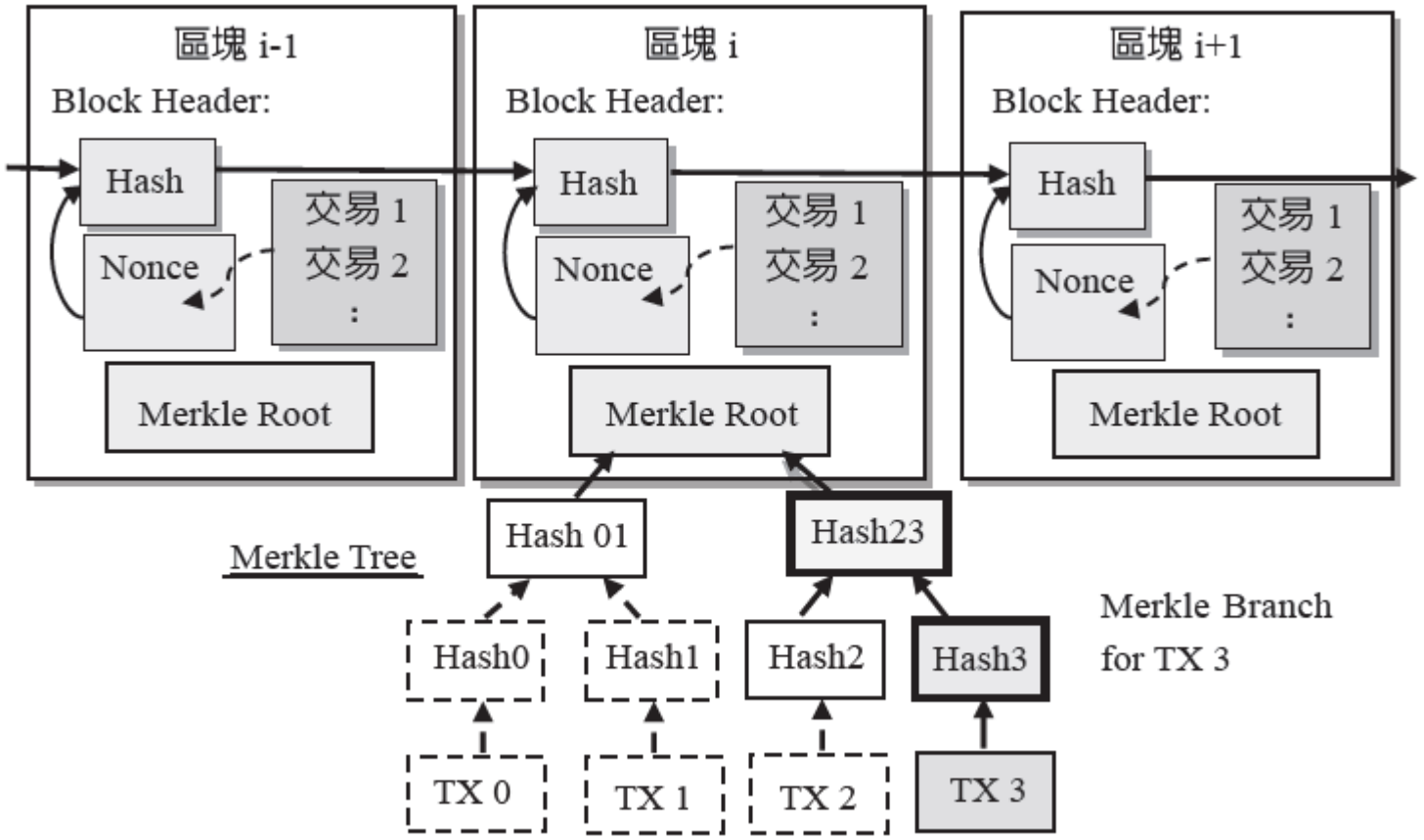
1. 哈希函數（Hash）

2. 交易網



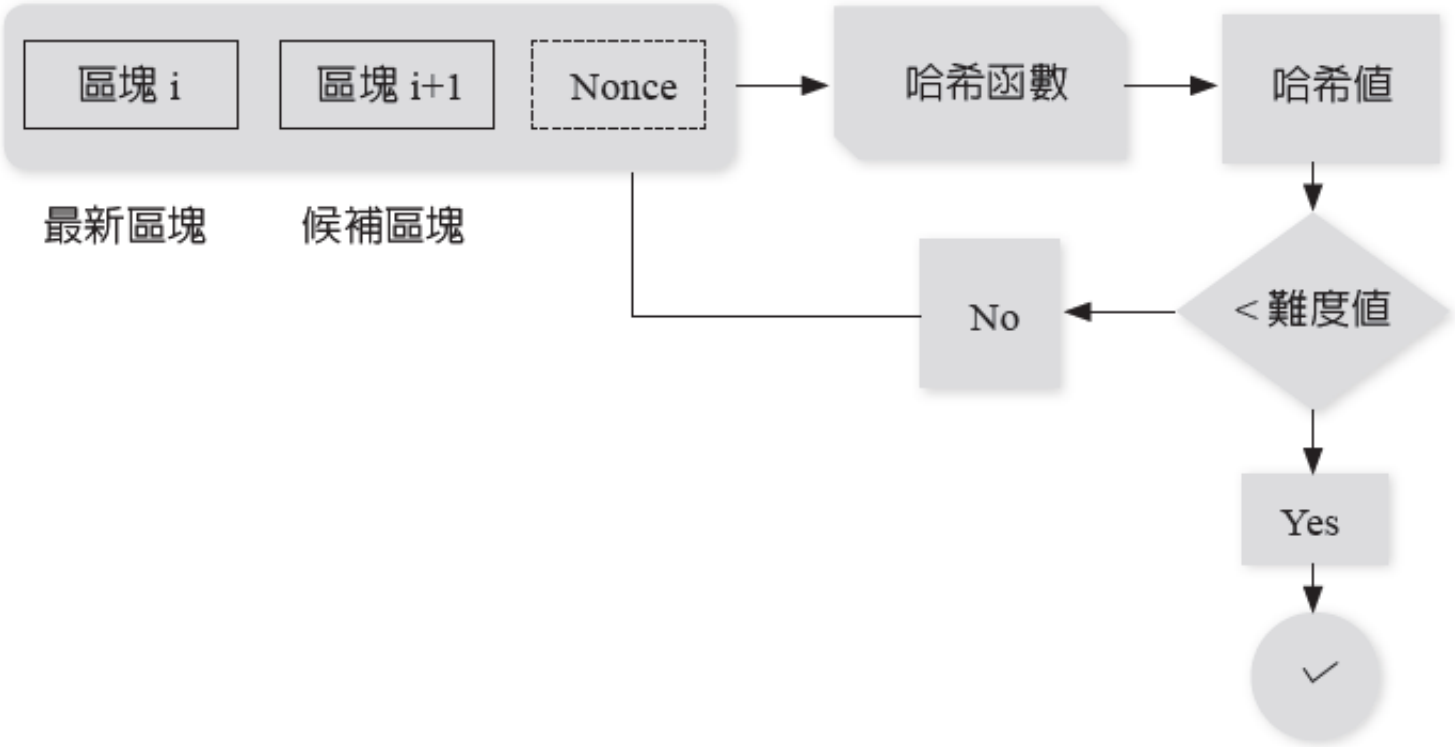
10-3 區塊鏈技術演進階段

3. 工作量證明機制（Proof of Work）與時間戳章服務器（A Timestamp Server）



10-3 區塊鏈技術演進階段

A. 以工作量證明落實去中心化和公平性目標

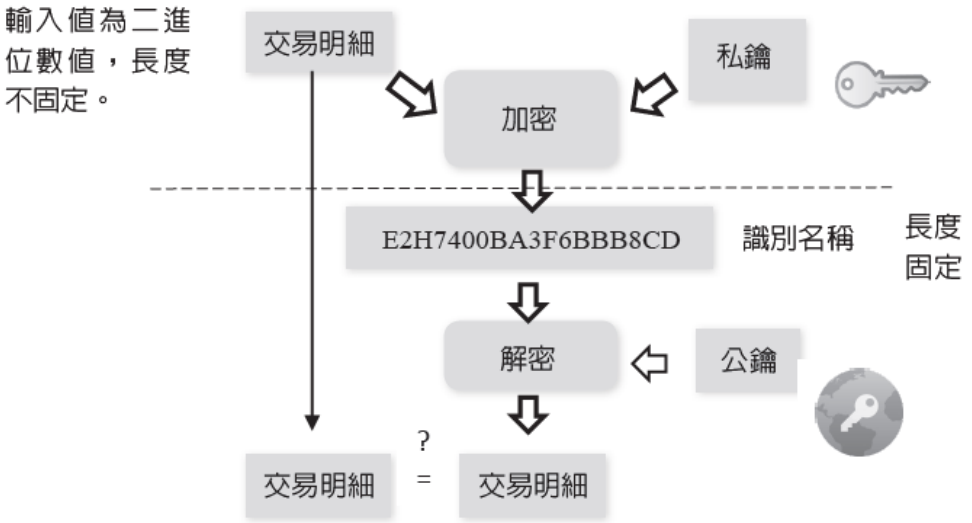


- 工作量證明系統

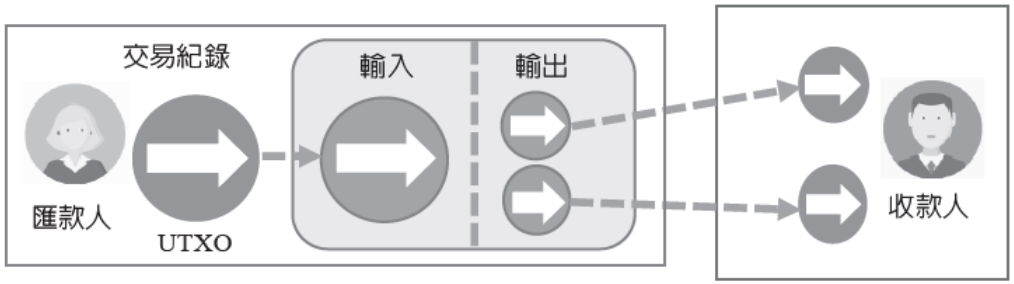
10-3 區塊鏈技術演進階段

B. 採用橢圓曲線之數位簽章演算法加密傳輸

- 加密解密過程



- 輸入與輸出總量一致



10-3 區塊鏈技術演進階段

C. 透過Hash演算法與多種Hash 函數來確保資訊不易被竄改

中本聰創造比特幣的主要貢獻在於引入P2P 機制，導入哈希演算法，並撰寫出相關程式。哈希演算法利用含有文字與數字的整數資訊，經由偽隨機性打亂混合出另一哈希值。

D. 以摩客樹（Merkle Tree）機制將許多訊息縮短為一個Hash 值

各區塊鏈中每筆交易均形成Hash，將其代碼廣播至各節點，並融入於各節點許多筆交易資訊之Hash 值中。

E. 運用時間戳章伺服器作區塊序列確認

作為比特幣的核心技術，採取符合安全性高和成本低的哈希演算編程方式，透過其資料檔嵌入區塊鏈中，以表彰存在性證明，並使用時間戳章服務器。

10-3 區塊鏈技術演進階段

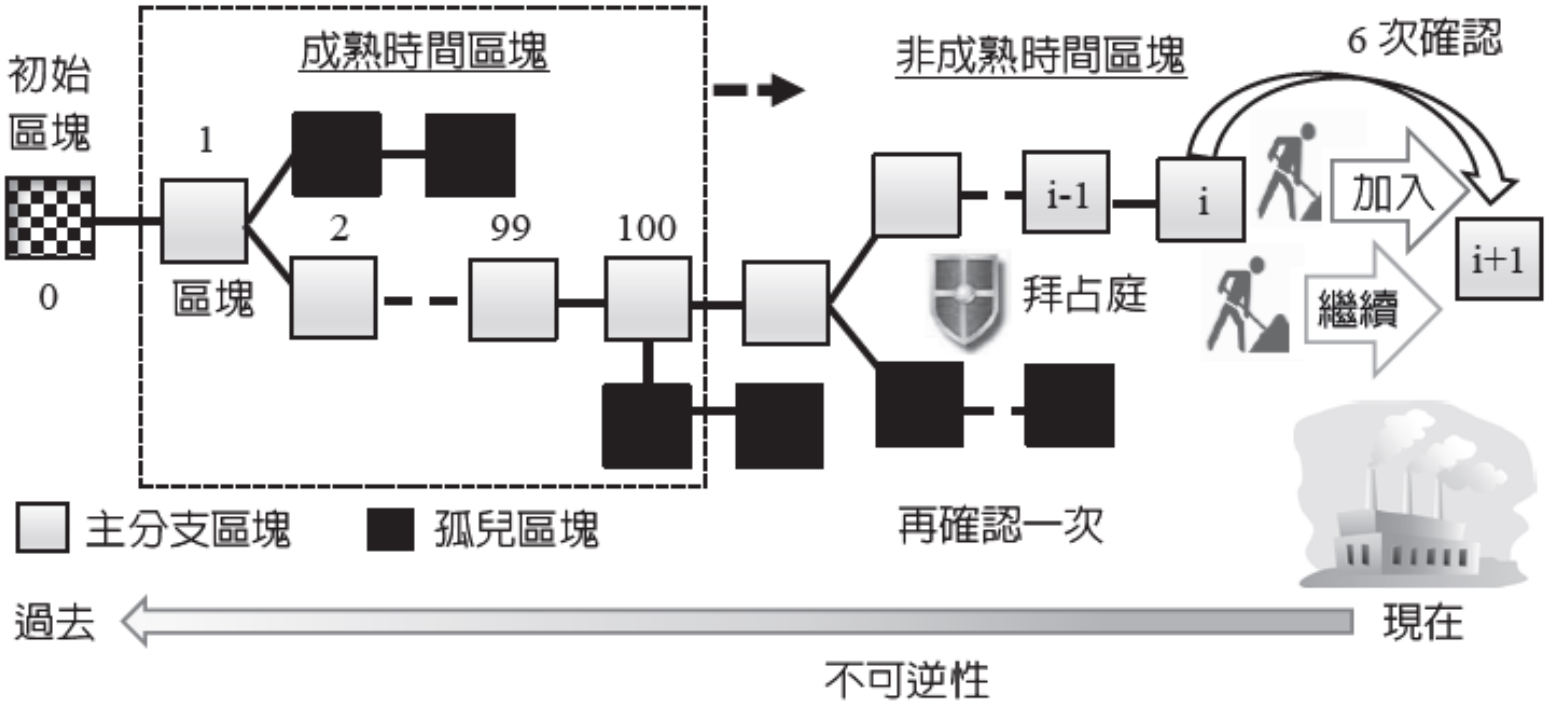
三、區塊鏈分支的形成

- 區塊結構

數據項	描述內容	更新時間	大小
魔術數字（Magic No.）	例如：0xD9B4BEF9		4 bytes（位元組）
區塊尺寸（Block Size）	到區塊結束的位元組長度		4 bytes
區塊頭（Block Header）	1. 版本（Version）：追蹤區域鏈協議升級版本。	更新軟體	4 bytes
	2. 前區塊之哈希值（Hash Previous Block）：為SHA-256位哈希值，確認區塊序列與正確的歷史紀錄。	新區塊生成時	32 bytes
	3. 摩克根（Merkle Root）：摩克樹演算法匯集過去交易紀錄計算出哈希值。	接受交易時	32 bytes
	4. 時間截章（Timestamp）：以秒為單位的目前截章。	每幾秒更新	4 bytes
	5. 難度值（Difficulty Target）：工作量證明演算法過程乃依難度遞增之線性調整的目標值。	當挖礦難度調整時	4 bytes
	6. 隨機數（Nonce）：從0至32位隨機，表示執行工作量證明演算法的次數。	每回Hash生成而隨機數增加	4 bytes
交易數量（Transaction Counter）	輸入與輸出數量均為正整數。		1-9 bytes
交易資訊（Transactions）	每一筆於區塊中的交易資訊		依交易數量bytes

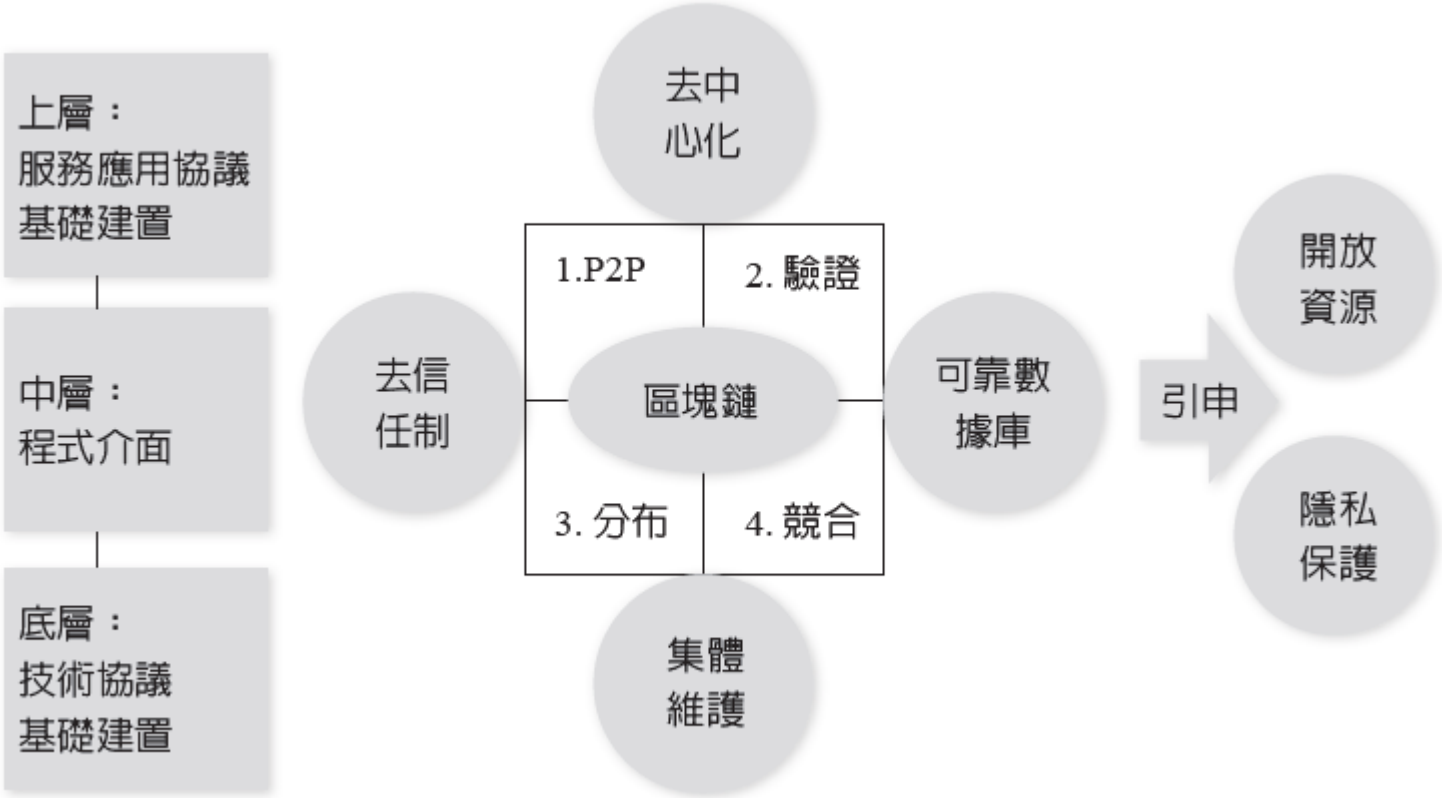
10-3 區塊鏈技術演進階段

- 區塊鏈生成



10-4 區塊鏈要素與特性

一、區塊鏈要素



- 區塊鏈基本要素與主要特性

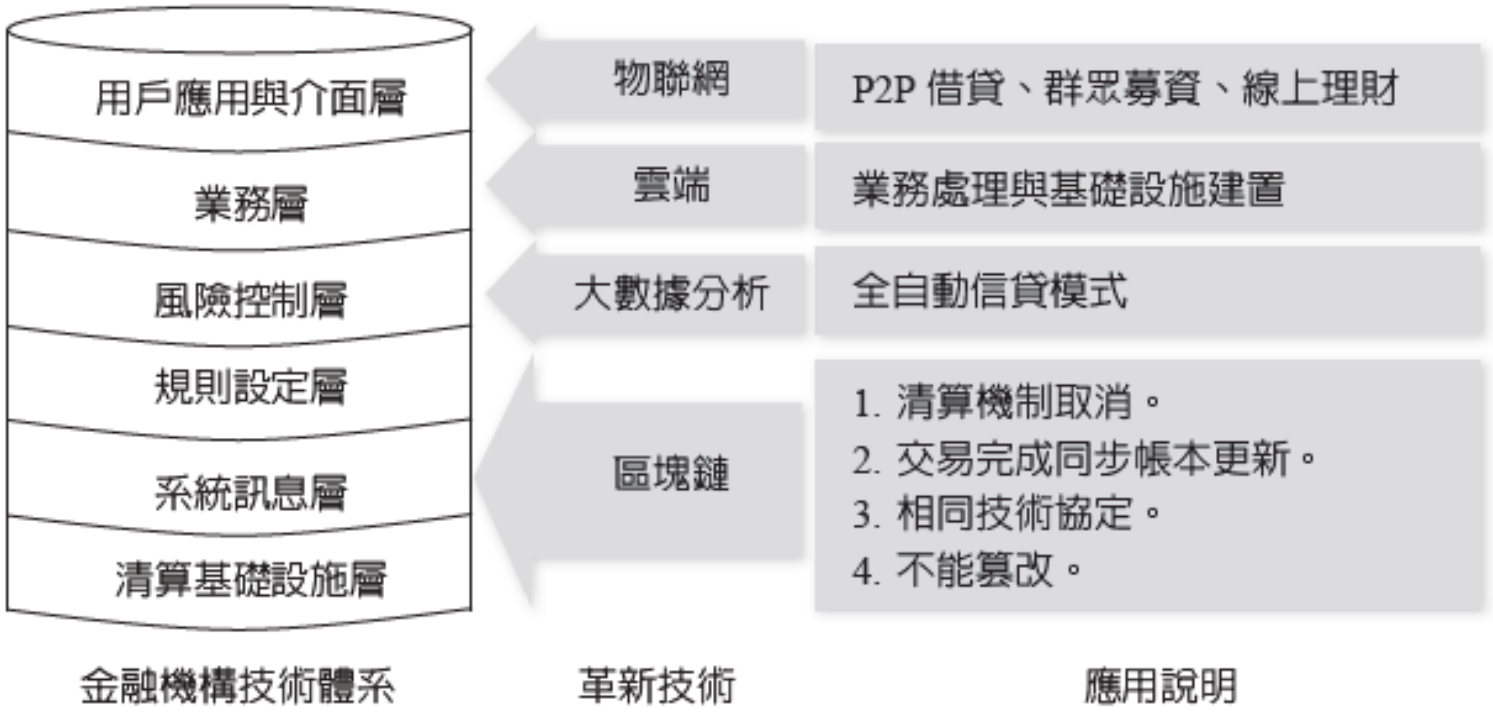
10-4 區塊鏈要素與特性

二、區塊鏈特性

1. 去中心化（Decentralized）
2. 去信任制（Trustless）
3. 集體維護（Collectively Maintain）
4. 可靠數據庫（Reliable Database）
5. 隱私保護（Anonymity）
6. 開放資源共享（Open Source）

10-4 區塊鏈要素與特性

三、區塊鏈技術應用與優勢



- 區塊鏈應用於金融業

10-4 區塊鏈要素與特性

- 區塊鏈技術優勢

金融服務交易環節	金融交易發起	交易前驗證	交易審核	契約簽訂	交易處理	帳務處理	交易完成
現有流程問題	人員發起與人工干預	1. 人工驗證／審核。 2. 資訊分散、不透明。 3. 詐欺事件。 4. 多方介入：公證、律師。 5. 等待時間較久。		契約傳送成本高	1. 交易時間延滯。 2. 系統失誤與不兼容。 3. 手工處理。		
區塊鏈技術優勢	系統自動觸發（智能合約）	1. 迅速實行驗證／審核。 2. 無須第三方參與。 3. 資訊透明、安全性高。 4. 實施反詐欺。 5. 無紙化作業。		智能合約	跨系統資訊即時同步和最小化誤差。	無	永久交易紀錄且不能篡改。

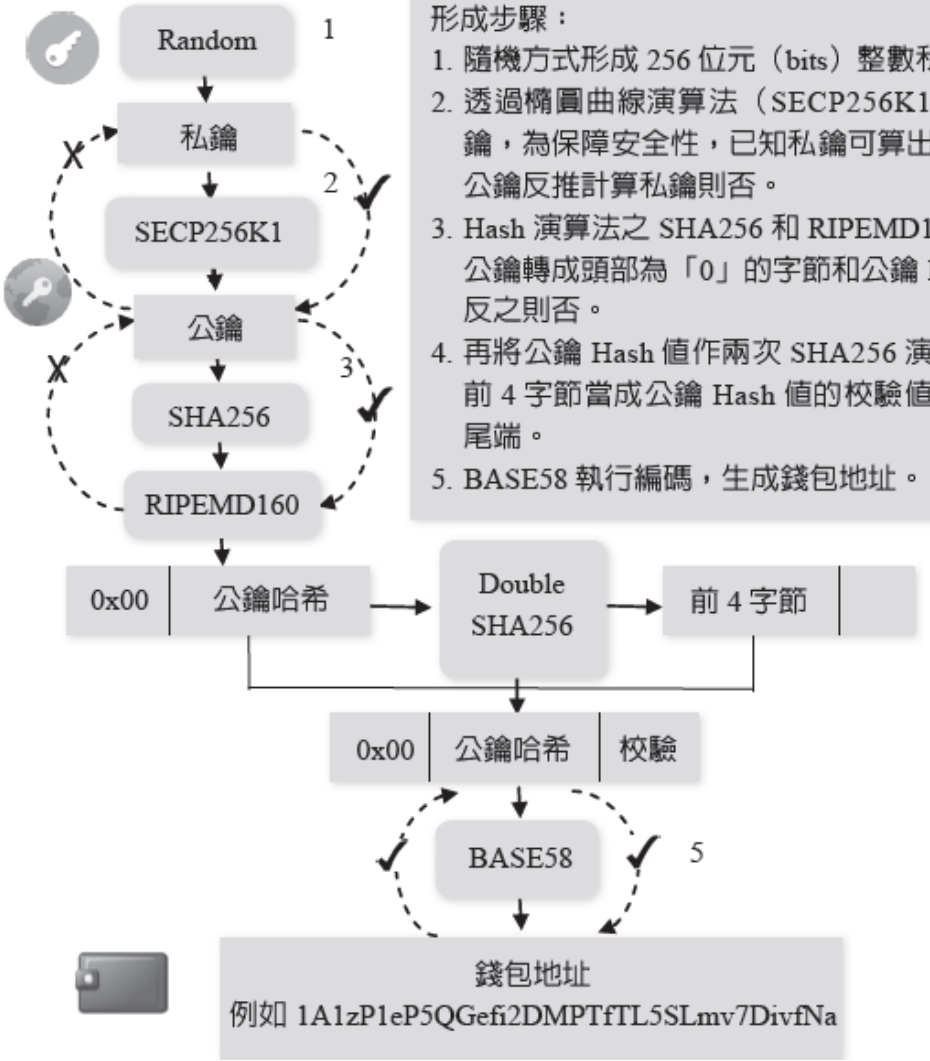
10-5 比特幣交易所

- 比特幣交易所的功能

項目	Mt. Gox	Bitstamp
交易買賣	比特幣	比特幣、XRP幣
加值	由銀行、平台、錢包進行儲值至用戶帳戶。	由銀行、平台、錢包進行儲值至用戶帳戶。
提現	從帳戶提取至銀行、平台、錢包。	從帳戶提取至銀行、平台、錢包。
帳戶	查看加值、提現、歷史交易紀錄。	查看加值、提現、歷史交易紀錄、未完成訂單、驗證、安全、設置等。
商家中心	提供商家使用相關功能。	
安全中心	提供附加安全措施，增加帳戶安全。	
設置	提供個性化資訊、密碼修改、認證申請等。	
常見問題	服務支援、客戶論壇等。	
新聞與概覽	提供官方消息。	提供官方與市場交易資訊。
訂單簿		買賣家報價資訊。

10-5 比特幣交易所

- 虛擬錢包地址的形成

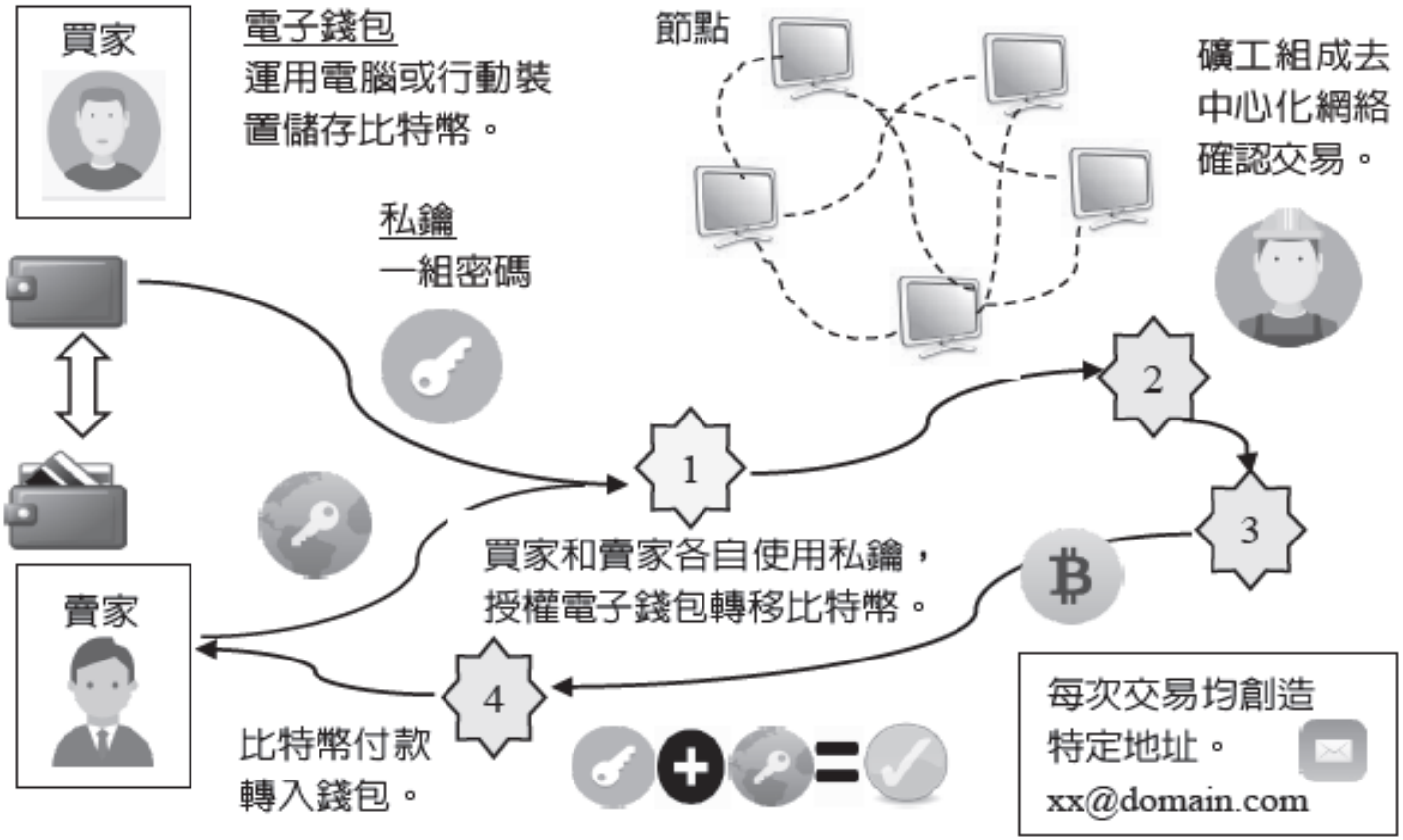


形成步驟：

1. 隨機方式形成 256 位元（bits）整數私鑰。
2. 透過橢圓曲線演算法（SECP256K1）取得公鑰，為保障安全性，已知私鑰可算出公鑰，而公鑰反推計算私鑰則否。
3. Hash 演算法之 SHA256 和 RIPEMD160，可將公鑰轉成頭部為「0」的字節和公鑰 Hash 值，反之則否。
4. 再將公鑰 Hash 值作兩次 SHA256 演算，並將前 4 字節當成公鑰 Hash 值的校驗值，連結於尾端。
5. BASE58 執行編碼，生成錢包地址。

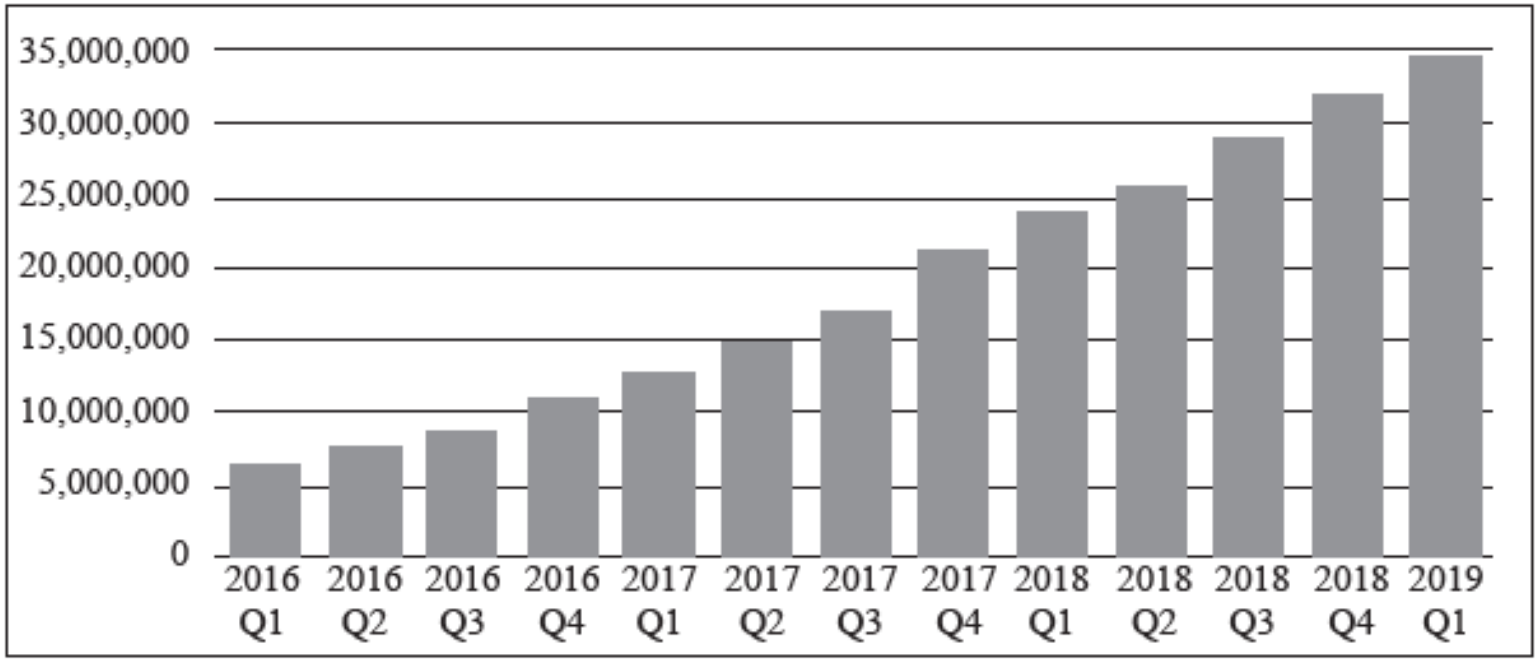
10-5 比特幣交易所

- 比特幣交易支付流程



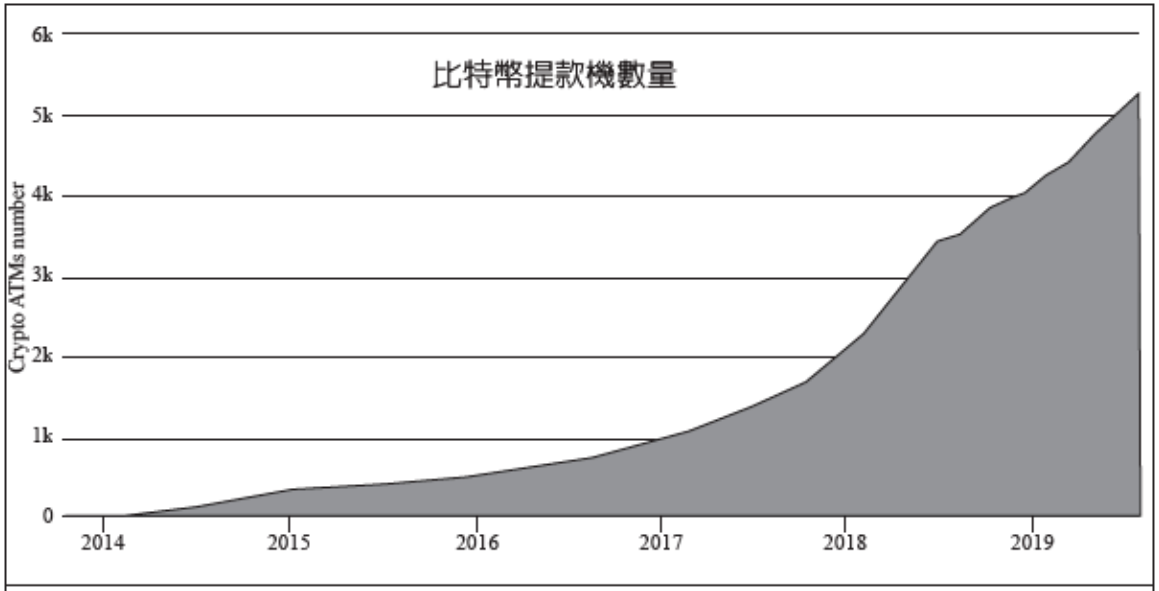
10-5 比特幣交易所

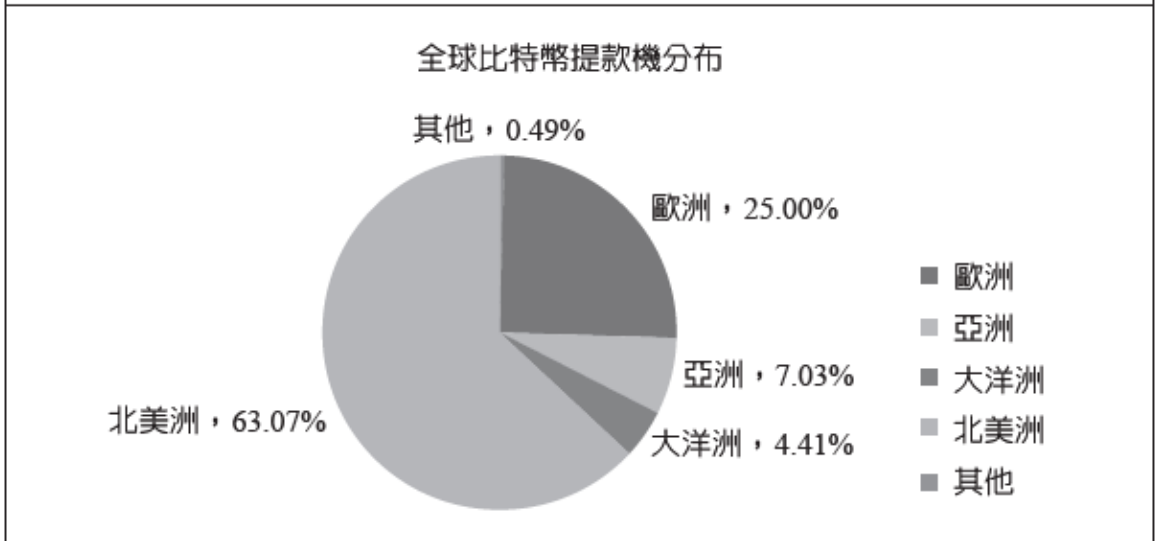
- 錢包用戶總數



10-5 比特幣交易所

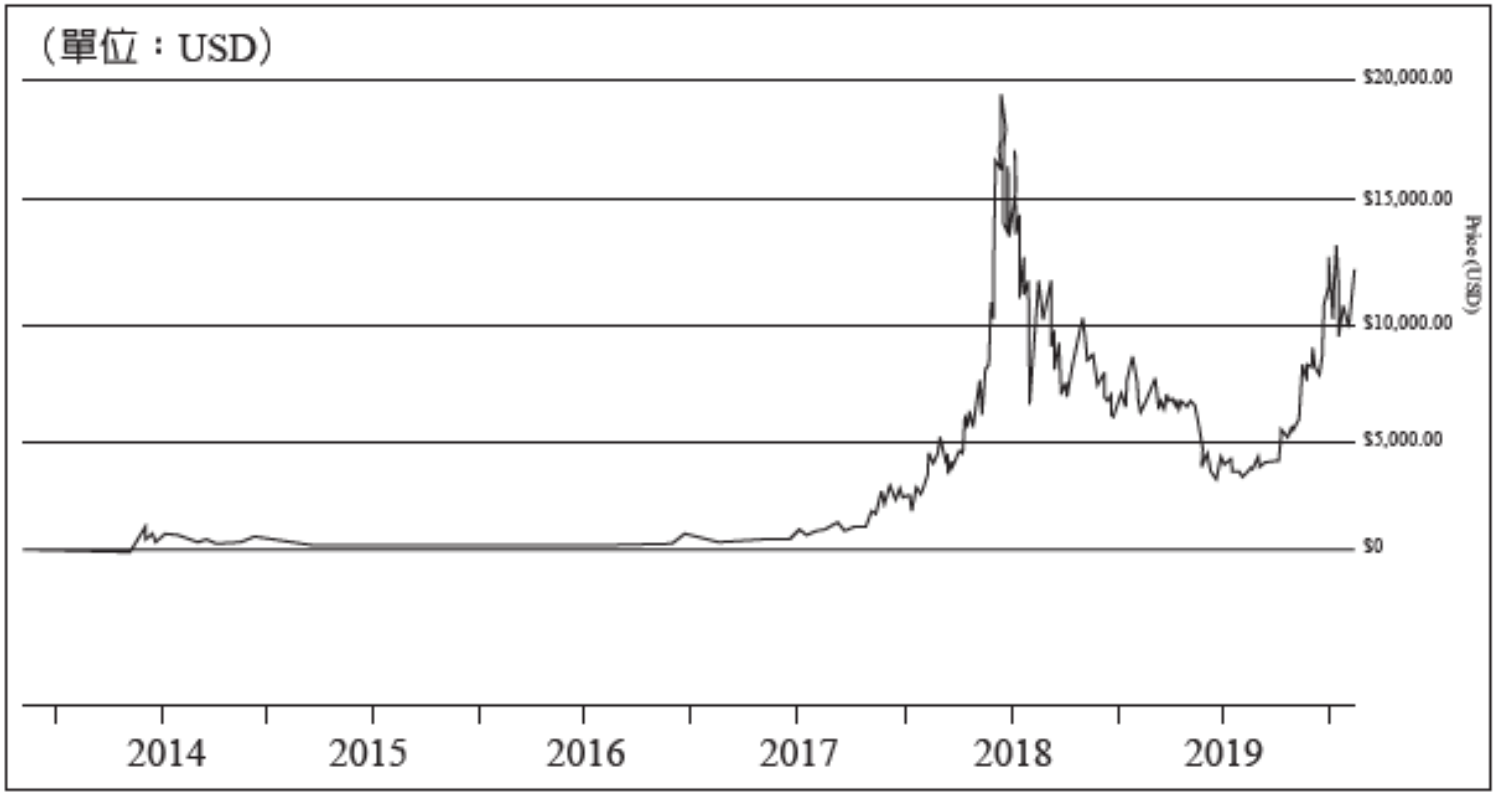
- 全球比特幣提款機裝置統計





10-5 比特幣交易所

- 比特幣價格走勢



10-5 比特幣交易所

- 加密貨幣負面事件

日期	地點	事記
2011.2	美國	「絲路」網站允許用戶匿名交易比特幣，並發展「洋蔥路由」技術，使追蹤非常困難，而受非法人士利用。
2011.5		比特幣是「史上最危險貨幣」，可能擾亂經濟，使走私猖獗。
2011.6		確認比特幣永久失去數量為18,838.32。
2011.6.13		首宗比特幣竊盜案，網路用戶宣稱2.5萬枚被盜。
2011.6.20	日本	Mt.Gox交易平台遭駭客攻擊，客戶資料被盜，比特幣暴跌。
2011.7	波蘭	Bitomat公布遺失1.7萬枚比特幣的訪問許可權。
2011.8		My Bitcoin遭駭客入侵而關閉，78,000多枚被盜。
2012.6	英國	Bitcoin Exchange交易平台被駭客盜走18,547枚比特幣。
2012.7	俄羅斯	BTC-e虛擬貨幣兌換所遭駭客入侵盜走4,500枚比特幣。
2012.8	美國	比特幣交易平台Bitcoin Savings and Trust宣布關閉。另一家Bitcoinica遭法院起訴為「龐式騙局」。
2012.9		總統候選人羅姆尼收到恐嚇信，要求100萬美元等值比特幣。
2013.3.12		使用0.8.0版本用戶端礦工建置新區塊鏈與0.7.0舊版之區塊鏈不相容，因而產生區塊鏈分叉衝突。
2013.3.23	中國大陸	比特幣交易平台發生錯誤操作，267枚比特幣以10元人民幣賣出。

日期	地點	事記
2013.3	美國	財政部表示虛擬貨幣從事交易或轉帳，屬於「貿易服務業」，需提交相關資訊與說明避免洗錢之措施。此舉引發比特幣相關企業遷移至巴拿馬。
2013.4		發現1,503個與比特幣相關的病毒，電腦感染會被盜取比特幣，甚至幫駭客挖礦。
2013.4	美國	BTCGuild礦池算力接近50%，引發社群對算力投票51%攻擊憂慮。當算力投票操過45%，該礦池主動採取限制，依協定關閉伺服器和新用戶註冊，使算力投票降低至40%以下。
2013.4.12	日本	Mt.Gox宣布暫停交易。
2013.4.12	美國	諾貝爾經濟獎得主保羅．克魯曼在紐約時報發表見解，認為比特幣挖礦是浪費社會資源和不明智之舉。
2013.5.28		聯邦檢察官指控設立於哥斯大黎加的「自由儲備」虛擬貨幣交易所，涉及全球洗錢活動。
2013.6		國土安全部決議凍結Mt.Gox銀行帳號。
2013.6.4		比特幣平台Bitfloor關閉，償還客戶資金。
2013.7	泰國	政府缺少相關法規和資本管制，宣布禁止比特幣交易。

10-5 比特幣交易所

- 加密貨幣負面事件(續)

日期	地點	事記
2013.10.3	美國	因懷疑比特幣毒品交易，聯邦調查局查封比特幣交易網（絲路），沒收約2.6萬枚比特幣。
2013.11.12		Bitfunder比特幣股票交易所關閉。
2013.12.5	中國大陸	比特幣發行與流通快速發展，已非政府能管控，將比特幣列為「非法貨幣」，並要求相關金融和支付機構停止交易。
2013.12		發現第一個勒索比特幣惡意程式CryptoLocker。
2013.12.30	台灣	央行與金管會聯名新聞稿，標題「比特幣並非貨幣，接受者請注意風險承擔問題」，指出比特幣具有高度投機的特性以及欠缺法律保障的風險性。
2014.2	新加坡	比特幣交易網站執行長自殺身亡。
2014.2.28	日本	知名比特幣交易網站Mt.Gox約有價值91億台幣的比特幣被駭，隨即宣告破產。
2014.9	美國	比特幣基金會前副董事長認罪，其經營「絲路」網站從事非法匯款和共謀洗錢。
2014.9		雲端儲存名模和女星等裸照遭駭客竊取，並以比特幣交易。
2015.1.4	英國	Bitstamp交易網站遭駭客入侵。
2015.1	台灣	BTCEXTW交易平台遭駭客盜幣，因而導致關閉。
2015.6	香港	港星主持經營比特幣交易平台疑發生倒帳情形。
2015.8	台灣	香港「氪能－比特幣礦業」赴台灣從事比特幣詐欺活動。
2015.10.28		香港東方明珠石油主席涉及詐欺、洗錢案獲交保，赴台療傷未歸，遭擄人勒贖7,000萬港幣等值比特幣匯至指定帳戶。
2016.4	日本	正式立法規範虛擬貨幣交易所，須向金融廳登記。
2016.6.6	台灣	網路勒贖軟體詐財猖獗，自2015年-2016年案件量倍增，比特幣淪為網路犯罪與洗錢工具。
2016.8.1	香港	Bitfinex平台電子錢包被盜11萬枚，損失約6,500萬美金。
2016.11.16	台灣	老鼠會手法投資黑暗幣、霹克幣涉詐財。

10-5 比特幣交易所

- 加密貨幣負面事件(續)

日期	地點	事記
2014.9	美國	比特幣基金會前副董事長認罪，其經營「絲路」網站從事非法匯款和共謀洗錢。
2014.9		雲端儲存名模和女星等裸照遭駭客竊取，並以比特幣交易。
2015.1.4	英國	Bitstamp交易網站遭駭客入侵。
2015.1	台灣	BTCEXTW交易平台遭駭客盜幣，因而導致關閉。
2015.6	香港	港星主持經營比特幣交易平台疑發生倒帳情形。
2015.8	台灣	香港「氪能－比特幣礦業」赴台灣從事比特幣詐欺活動。
2015.10.28		香港東方明珠石油主席涉及詐欺、洗錢案獲交保，赴台療傷未歸，遭擄人勒贖7,000萬港幣等值比特幣匯至指定帳戶。
2016.4	日本	正式立法規範虛擬貨幣交易所，須向金融廳登記。
2016.6.6	台灣	網路勒贖軟體詐財猖獗，自2015年-2016年案件量倍增，比特幣淪為網路犯罪與洗錢工具。
2016.8.1	香港	Bitfinex平台電子錢包被盜11萬枚，損失約6,500萬美金。
2016.11.16	台灣	老鼠會手法投資黑暗幣、霹克幣涉詐財。

日期	地點	事記
2016.8.1	香港	Bitfinex平台電子錢包被盜11萬枚，損失約6,500萬美金。
2016.11.16	台灣	老鼠會手法投資黑暗幣、霹克幣涉詐財。
2017.9	中國大陸	全面禁止比特幣交易所與ICO發行。
2017.12.9	斯洛維尼亞	NiceHash挖礦公司慘遭入侵。
2018.3.15	日本	加密貨幣交易所被駭客非法移轉價值約5.23億美元的新經幣（New Economy Movement, NEM）。
2018.1-3	美國	Facebook和Google禁止比特幣、其他加密貨幣、ICO廣告。
2018.5.3	英國	蘇格蘭的醫院設置加密貨幣上癮症勒戒所之醫療服務。
2018.5.25	美國加拿大	計畫掃蕩部分ICO投資案。
2018.6.12	南韓	交易所Coinrail駭客入侵。
2018.8.24	美國	SEC否決9檔比特幣ETF申請。
2018.9.27		Facebook部分解禁ICO廣告，允許美國和日本刊登。

10-6 比特幣SWOT 分析

優勢（Strength）	劣勢（Weakness）
1. 去中心化：可避免央行不良的貨幣政策與人為操作，可能造成通貨膨脹的隱憂，可降低交易成本。 2. 信用效益：具有防偽、不能撤銷、無限分割和無假幣的特點。 3. 總量恆定：演算法設定發行上限，採稀少性發行，有保值的作用。 4. 支付媒介：流通於各種交易、償還債務、工資和繳稅等。 5. 社交性：礦工挖礦和使用期間，透過彼此討論而加強緊密聯繫關係。 6. 匿名性：保障使用者的個人資訊之匿名與自由度，例如：捐贈。 7. 普遍性：交易便捷性，使日常購買活動接受度提高。 8. 避稅效果：交易不受政府管轄，可享避稅好處。 9. 挖礦：礦工用特定程式生產。	1. 價格變動：比特幣價格具有暴漲暴跌的趨勢，屬於原始流通階段。 2. 風險性：為避免被盜和遺失造成無法回復之風險，需將比特幣地址備份，並將其密碼保管妥善。 3. 不穩定性：交易平台屢遭駭客侵擾、資金缺乏、和市場發展尚未成熟，導致部分平台倒閉，甚至捲款潛逃，使用戶蒙受損失。 4. 法律規範不足：各國相關法律規範付之闕如。用戶若因權益受損而起訴訟，法院恐無法受理。 5. 限制交易：部分國家規定禁止銀行、第三方支付機構、相關金融機構等從事比特幣交易活動。 6. 技術性問題：區塊鏈分叉事件顯示擁有巨大計算力技術的礦工，會對比特幣系統造成安全威脅。

10-6 比特幣 SWOT 分析

機會（Opportunity）	威脅（Treat）
1. 激勵性：吸引許多企業開展多種密碼貨幣、新型支付方式、和創新研發虛擬貨幣。 2. 全球一體化：比特幣技術發展與應用已成熟，順應全球經濟一體化的趨勢，各大知名企業陸續表態接受比特幣支付和交易活動。 3. 保值效果：比特幣總量恆定與開採難度漸增，價格具高度波動上升格局。且大約78%投資者帳戶尚未有任何交易，屬長期持有狀況。 4. 區塊鏈：許多國家政府與知名企業等，全力研究區塊鏈技術與應用結合的開展。 5. 透明性：原始碼可從比特幣網站獲取，公開討論技術問題，及時糾正、系統不斷演進與自我修復能力等。 6. 創造性：比特幣的架構可延伸至金融結構與商業合作模式，開創新型交易系統。 7. 開放式資訊組織：比特幣基金會是社群唯一類似的官方組織，依靠捐款維持營運，負責核心協定、用戶端升級、安全監督、確認進化模式、法律規定、和政府協商等角色。 8. 穩定性：吸引商家和用戶加入，使用比特幣交易付款，將有助於貨幣穩定。	1. 駭客入侵：一旦遭駭客侵入盜取比特幣，將使投資者損失不菲。 2. 糾紛頻傳：因匿名制導致無法追蹤的情況，容易產生糾紛。 3. 恐怖活動：萬一遭恐怖分子利用，其後果令人擔憂。 4. 非法行為：有些國家已將比特幣投資和交易視為非法活動，可能會使其他國家跟進。 5. 血本無歸：價差振幅過劇，投機意味濃厚，投資不當可能全盤皆墨。 6. 交易平台風險：駭客藉由比特幣高價時，進行借幣放空。同時，利用大規模分散式拒絕服務攻擊，企圖癱瘓平台造成恐慌，在低檔承接。 7. 其他密碼貨幣：由於比特幣價格處於高檔、開採難度日增等因素，使擁有開發技術者另闢蹊徑，推出新型優化的密碼貨幣企圖搶食市場。 8. 消耗資源：比特幣採礦非常耗電，屬於能源密集型挖礦。 9. 算力投票：算力具有投票權，任何用戶端相關改進建議、協議修增，必須接受算力投票至少達51%之門檻監督和發行權控制，才能視為有效。亦為蓄意發動比特幣網路攻擊起點的隱憂。如修改交易紀錄、阻止有效區塊等。

10-7 比特幣生態圈

- 比特幣生態圈與產業鏈