比特幣有機會成為新經濟時代的主流貨幣之一嗎？

⊙楊佳侑／中華經濟研究院WTO及RTA中心　助研究員

比特幣在2017年的金融市場上掀起一陣熱潮，許多投資者視比特幣為金融海嘯後的高潛力金融工具，但也有專家擔憂這將是下一場金融泡沫。到底比特幣是什麼？我們該擔憂還是期待？本文將從不同角度揭開比特幣神秘的面紗，並分析比特幣的優缺點及未來趨勢。

關鍵詞：數位貨幣、比特幣、礦工、區塊鏈、非理性繁榮

Keywords: cryptocurrency, Bitcoin, miner, blockchain, irrational exuberance

2008年的金融海嘯不只對全球經濟造成衝擊，更改變了政府使用貨幣來穩定經濟的政策思維。大型經濟體為刺激國內經濟，紛紛採取量化寬鬆政策，造成大量貨幣流通於金融市場，儘管這些資金在經濟低迷期間並未如預期般地大量流通於一般市場，造成通貨膨脹，但經濟復甦後各界專家擔憂金融市場所持有的大量資金可能引發下一波金融危機。另一方面，因潛在的通貨膨脹問題，經濟學家對於利率調升的時機持有不同看法，因此中央銀行是否能從量化寬鬆政策中全身而退還有待考驗。

基於各種不穩定的因素，人民逐漸失去對政府的信任感，間接促使人們尋求更加穩定的貨幣機制。貨幣經濟學之父傅利曼（Milton Friedman）在90年代末受訪時曾主張廢除美國聯邦儲備銀行（Federal Reserve Bank），他認為該銀行自創立以來並沒有確實執行政府所賦予的任務。另外，他也曾預言網路的發展在未來有助於降低政府在市場上的角色。儘管傅利曼未能親眼見證2008年金融海嘯的一切，部分投資者深信這位貨幣主義教父早已看見「數位貨幣」（cryptocurrency）取代政府貨幣機制的

趨勢。經過金融海嘯的大洗盤後，比特幣（Bitcoin）已作為「數位貨幣」崛起的代表之一，但是否真能成為未來的主流貨幣，則有待進一步探討。

比特幣的起源與機制

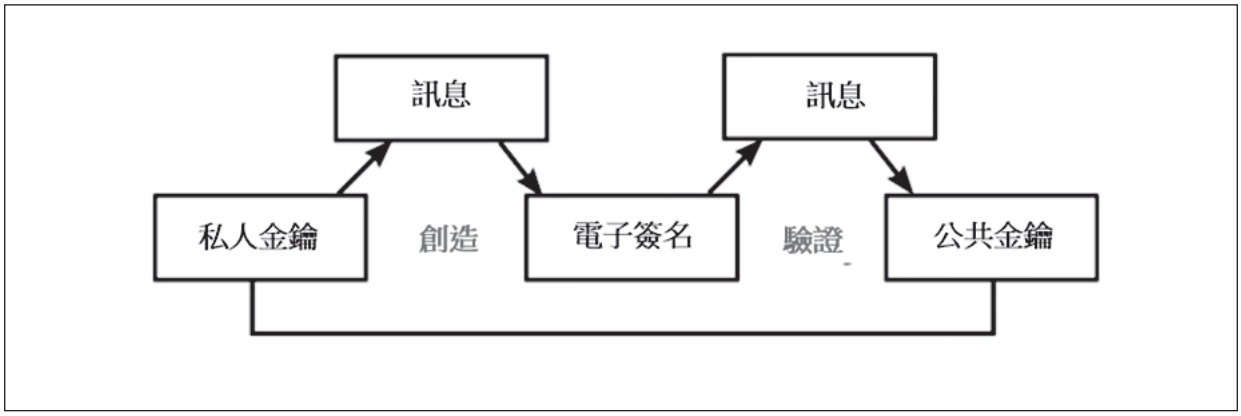
2009年一位自稱中本聰（Satoshi Nakamoto）的神秘程式設計師創立了全球第一個「分散性數位貨幣」（decentralized cryptocurrency），比特幣，並在金融海嘯期間開啟新的交易模式。不同於傳統貨幣，比特幣並沒有中央結算所或是政府機構在交易雙方之間進行結算。另外，該貨幣除了可用於購買實質商品及服務以外，不與任何國家的貨幣或大眾物資掛鉤。因此，比特幣理論上不受任何政府或金融機構監控、驗證和批准，而是通過「對等式網路」（peer-to-peer network）提供共享式服務。

比特幣與傳統貨幣最大的不同點在於交易雙方不需具有信任基礎，驗證工作可透過第三方電腦的數學解碼演算方式進行。由於比特幣系統採取匿名制，使用者將共享「電子分類帳簿」（ledger）裡的資料，每筆交易的過程會公布於系統給使用者做更新。大致上，比特幣的交易過程可分為以下七個步驟：

1. 付款人使用「電子錢包」（wallet）支付比特幣給某方；
2. 該筆交易與其他待決之交易一同被公布於比特幣的網路系統；
3. 系統中的「礦工」（miner）大約每十分鐘會將收集到的幾百項待決交易組合成一個「區塊」（block）；
4. 「礦工」需相互競爭，解決一組困難的「雜湊函數公式」（hash function），以驗證「區塊」中的交易。最先將數學公式解出的「礦工」則獲得進一步處理該「區塊」的權利，但工作證明必須公布於比特幣網路給其他「礦工」驗證；
5. 當其他「礦工」證實了交易的有效性，且批准了該「區塊」的交易，負責開採的「礦工」將獲得25枚新的比特幣（現值約為415,000美元）作為獎勵。該機制運用「礦工」的計算能力，並自動調整題目的困難度，以保持比特幣的穩定供應量；
6. 開採過的「區塊」將增添至比特幣網路的「分類帳簿」中，成為交易紀錄「區塊鏈」（blockchain）的一環；
7. 最後，收款人可使用「電子錢包」查詢比特幣是否已進入帳戶。

每筆交易在「加密金鑰」（encryption key）的保管之下難以遭到駭客竊取，系統透過複雜的數學公式將兩把「加密金鑰」相互連結，其中一把「私人金鑰」（private key）保有付款人的密碼，另外一把「公共金鑰」（public key）則提供收款人驗證的密碼。如圖1所示，在比特幣交易之下，付款人使用

「私人金鑰」加密訊息，並建立一組「電子簽名」（signature）用來分辨訊息的來源和真偽；收款人獲得「電子簽名」的加密訊息後可驗證該筆交易是否與「公共金鑰」相互對應。由於電子簽名是由「私人金鑰」和訊息組成，因此「電子簽名」無法重複使用於其他交易，另外，隨意篡改「電子簽名」則會導致驗證失敗。



資料來源：本研究參考網路資料自製。

圖1　比特幣加密金鑰的關係鏈

技術上來說，沒有結算機構的比特幣系統存在安全漏洞，因為付款人可以把錢轉出後馬上取消交易，最終導致收款人的損失。首先，交易順序並非由執行時間界定，而是根據解題的速度排列順序，因此有機會發生舞弊現象。例如，甲方向乙方付款，並趁乙方將貨品寄出的期間將同一筆資金寄往自己的帳戶，於是甲方可能既拿了貨又保留了金錢，造成乙方財貨兩失。然而，比特幣的「區塊鏈」機制在設定上避免了該情況發生的機會，除非甲方的解題速度可以與整個系統的用戶抗衡，否則使用假照訊息覆蓋原先交易訊息的機率相當低。一旦原先訊息的區塊加入「區塊鏈」後，匯款將進入乙方帳戶，而被驗證過的交易則無法再作使用。簡單來說，「對等式網路」提供了比特幣系統用戶互相制衡的效果，理論上沒有任何人可以獨自操控和竄改「區塊鏈」的資訊。

現今趨勢及熱潮

比特幣在發行後不久，網路上便散佈著大量文章說服民眾提早入市換取高報酬及抵抗惡性通膨的機會。事實上，比特幣的美元價格從2010年發行以來，由最初的6分美元上漲至2017年12月的1.91萬美元，成長幅度已超乎任何金融投資。近期在許多投資專家及學者的預期下，比特幣的價值已大幅下滑至少25%，現值約1.35萬美元。截至2018年1月止，市場上流通的比特幣以達到1,670萬枚，距離2,100萬枚的總量限制還有一段差距。當

系統在2030年達到總量限制時，「礦工」將再也收不到新的比特幣；作為採礦的替代獎賞，「礦工」將在交易雙方之間收取小額的驗證手續費，目前已有部分比特幣交易平臺向使用者收取手續費的情況。

投資者對比特幣的狂熱既是近幾個月來比特幣大幅上漲的原因，也是價格居高不下的結果。芝加哥商業交易所（Chicago Mercantile Exchange, CME）於今（2017）年12月1日對外宣布，比特幣的期貨合約將從12月18日起正式在CME進行交易，此消息一出，更進一步推動了比特幣的上漲。在金融市場的助力下，越來越多人使用比特幣交易，這意味著比特幣的需求將提高，因此價值也將隨之上漲。不過，比特幣究竟為何如此吸引人呢？第一，比特幣的有限供給性降低了貨幣持有人對於量化寬鬆所導致的通膨疑慮；第二，資金和帳戶採匿名制可保護個人隱私；第三，該貨幣不受政府監管且難以追查，因此許多不肖與恐怖份子利用此系統籌措犯罪資金或是避稅。

不過，近期比特幣在市場上引起高度需求更合理的解釋原因是其價格正在迅速上漲。如同金融泡沫歷史學家金德爾伯格（Charles Kindleberger）曾說的：「沒有甚麼比看到自己朋友致富後更能影響一個人內心幸福感和判斷力的事情。」比特幣買者並不是因為生活需求而購買比特幣，而是因為他們都相信下個買家會用更高價向他們收購比特幣，因此造就當今的比特幣繁榮，這波熱潮與諾貝爾得主席勒（Robert Shiller）所形容的「非理性繁榮」（Irrational exuberance）極為相似。

比特幣的優缺點

從非投資的角度來看，比特幣的好處大致分為幾點：第一，政府不能操作資金的來源和去向，也無法增加比特幣的供給量，藉此杜絕惡性通貨膨脹的可能性；第二，匿名帳戶可防範個資外洩，大幅提高用戶的隱密性，簡單來說，該貨幣可以被任何人在任何地點使用；第三，全球手續費可能低於一般金融系統，但不會是免費，因為比特幣系統需要經費維持硬體和能源的供給。

然而比特幣並非完美的貨幣系統，尤其在貨幣兌換方面，並非所有經濟體都接受比特幣，因此比特幣持有者必須透過其他途徑兌換。另外，比特幣的隱密性特質經常被許多不法份子利用在違法交易上，如毒品買賣、洗錢和恐攻集資等。從資源消耗方面來看，「採礦」所需要的能源相當龐大，特別在未來數學演算難度提高後，電腦的處理能力要耗費更多電力。目前全世界有60％以上的採礦能力集中在中國大陸，因為其電費比較便宜，數據中心也較容易架設。在安全考量方面，比特幣系統確實存在某些疑慮，過去曾有使用者因遭到駭客盜取線上金庫而受到損失，但該系統並無申訴管道，使用者只能默默承受損失。

經過正反兩面的觀察後，不難發現比

特幣的特性擁有許多值得多方發展的潛力，但同時也擁有不少法規漏洞和技術限制。首先，近期比特幣交易流量暴增，造成驗證時間過長；使用者為加速個人交易處理速度而支付手續費，導致系統手續費用高漲，此現象與預期的低續費有落差。第二，從徵稅方面來看，利用比特幣向某人報銷產品或服務的行為被視為易貨貿易，因此稅收難以執行（避稅或逃稅的可能性）。法規的漏洞使許多法規制定者擔憂該貨幣將成為不法人士避稅的金融工具。

比特幣內戰

當比特幣的系統越大，內部的分歧就越多，主因是不同系統開發商對於比特幣的未來走向看法不一。為了確認比特幣未來的走向，許多人開始追尋比特幣的定位，到底該貨幣應該更像黃金還是現金？而探討比特幣本質的過程也再次引起長久以來貨幣思想學派的兩大分歧。「金屬本位學派」（metallism）主張貨幣應該是一種由下往上發展的支付工具，它的存在是因為交易雙方尋求有效的交換媒介，以降低交易成本；基於此，貨幣可視同黃金一般，擁有儲存的價值。另一方面，「紙鈔學派」（chartalism）認為貨幣是政府由上往下發展而成的支付工具，其主要用途為稅收管理和債務支付等，因而創造出交易的大量需求。比特幣的特別之處在於該貨幣擁有兩者的特性；人們可以自由選擇進入系統，並且在不受政府的限制下從事支付和投機行為，這點與「金屬本位學派」相當吻合。然而，比特幣機制是由中本聰先生所訂下的，除了系統參數早已被設訂好以外，「區塊」容量和貨幣總量流通限制也是事先制定的，因此許多機制也與紙鈔學派的論點相似。

目前比特幣社區分為三個派系：「巨大化區塊派」主張增加「區塊」容量，並讓比特幣系統增長到必須由少數團體來管理的龐大等級，因為屆時「區塊鏈」已經大到無法透過個人電腦系統進行驗證；「隔離見證派」認為系統應維持現有「區塊」的容量，並以其它技術將較小的交易密集綑綁於同個「區塊」，以緩解系統擁塞的問題；「綜合派」則希望同時納入上述兩派的作法。僵持不下的結果已造成部分開發商由原先的比特幣系統獨立出來，成立一條新「區塊鏈」。在面臨內部分歧的同時，比特幣也受到外部競爭的壓力，許多新興數位貨幣的崛起可能隨時取代比特幣在市場上的地位。

未來發展潛力

在人類的文明發展中，金錢以不同形式成為經貿活動間的重要媒介，舉例來說，大平洋上的雅浦島（Yap）直到20世紀初，仍使用島上的大石盤作為大筆開銷的支出，如女兒的嫁妝。由於大石盤相當沉重，支出後也不方便移動，因此每筆以大石盤做出的交易便透過更改所有權進行，並以口述方式紀錄該石盤的歷史。根據交易歷史，島民們可追

朔大石盤的所有權，以確保同一塊石頭無法同時被使用兩次。隨著時間與經濟活動的演變，人們對於金錢的定義逐漸具體化，也間接改變了人們交易的模式。

比特幣作為新時代的產物，其應用系統並非得侷限於支付功能。目前，如同比特幣般的「無需許可創新」（permissionless innovation）衍生應用技術已在市場上型成一股新的高潛力商機。該技術以比特幣系統作為雛型，將所有權移轉的想法應用在金融財產或其他物品上。財產持有者在分散性交流的系統之下，透過第三方的驗證直接與任何人進行交易，例如，汽車租、借方可以使用比特幣等媒介作為發動汽車的關鍵金鑰。利用同樣的方法，許多資產的管理和租借將變得更加方便和簡單，尤其對於短暫的點對點租借更為有利。

各類型的「智慧型財產」（smart property）能有效地將「區塊鏈」升級為實體資產的全球登記網，並擴大其運用範圍。或許該商業模式看似天方夜譚，但目前市面上不乏許多創業公司朝「智慧型財產」的應用發展，如Coloured Coins和Mastercoin即將推出能夠交易股票和債　等金融資產的軟體。另外，「以太坊」（Ethereum）也企圖推動類似比特幣的新區塊鏈，利用編程語言來進行金融工具和其他合約的編碼。未來加密程式的應用將取決於網路容量，雖然目前的網路容量可能不足以應付龐大的未來需求，但根據以往的經驗，科技最終總能解決問題。

比特幣可能成為主流貨幣嗎？

現今法定貨幣制度主要建立在人民對於政府的信任，交易雙方透過金錢移轉獲取所需的商品及服務。人民深信由政府作為保障的紙幣可換取等值的物品，不過一旦人民對政府失去信心，貨幣的流通則將停擺。一般而言，金錢提供三個目的：（一）可作為交易的媒介；（二）有儲存的價值；（三）能作為計量單位。

作為交易媒介，目前比特幣的功能還差強人意；除了驗證工作較為費時之外，願意接受比特幣的店家還不算多數，因此方便性沒有使用者所預期的高。另外，比特幣的儲存價值更是格外難以預測，主要傳統貨幣在中央銀行保守的政策下，價值隨著穩定的通膨率而逐年下降，但比特幣的價值確難以預估，可能隨時上升50％也可能下跌80％。從計量單位來看，一枚比特幣即使受到匯率浮動，依然保持一枚比特幣的價值。然而，目前商品與服務的計價方式仍以傳統貨幣為基礎，因此比特幣匯率的波動對消費者有相當大的影響。

平心而論，任何浮動貨幣都避免不了匯率的波動；以美元為例，90年代末美元貿易加權飆升50％，隨後又下降了30％，2008年時又上漲約20％左右。即使是美元如此成功的貨幣也不免受到波動的影響，更何況是尚未成熟的加密貨幣。長遠的匯率波動確實會對總體經濟造成影響，但短期來說，一般美

國民眾對於匯率波動的影響較無感，因為美國是個龐大的經濟體，貿易占GDP的比重相當小，且幾乎大部分的消費都是以美元做計算。除非交易內容以貿易成分居多，否則外匯波動的意義對消費者來說並不大。

不幸的是，目前能使用比特幣來消費的產品或服務大多是以美元計價，因此匯率變動格外重要。簡而言之，商品的訂價短期內無法與比特幣兌美金的匯率脫節關係，基於上述論點，比特幣尚未擁有獨立貨幣的特質。另外，商品本身雖能以比特幣計價，但中間財和內部的供應鏈，如勞動成本，仍然使用傳統貨幣。在此交易之下，比特幣無法與美元或其他主流貨幣脫鉤，而匯率的波動也將影響使用者的意願。

不過，現今比特幣的運作模式在未來並非完全不會改變；假使未來比特幣的購買力越強，其使用意願就越高，需求則越趨向穩定發展。未來，企業家為避免匯率風險，可能考慮使用比特幣當作支付供應商和勞工的工具，間接加強經濟體對比特幣的需求，屆時外匯波動的影響可望縮小。

作為全球第一個分散性數位貨幣，比特幣在遇上類似「擠兌」（bank run）的情況時可能導致交易量大幅下降，甚至是系統崩盤的情形。然而，傳統貨幣在同樣情況下則會獲得中央銀行貨幣供給的支持，給予貨幣持有者足夠信心而不至於演變至崩盤的情勢。原則上傳統貨幣是由政府直接作保的法定貨幣，一切責任皆由主政機關對其公民承擔。另一方面，比特幣屬於「社區貨幣」（community currency），需用戶自行管理。即使自行管理對某些人來說是一項具有吸引力的特性，但整體而言，比特幣系統開源合作的方式仍有很大的改善空間。目前，一般民眾仍期望將貨幣擔保的責任賦予政府；除非這種思維在未來有所改變，否則比特幣不會成為真正的主流貨幣。