SOUTH CHINA QUARTERLY Vol.7, No.2 (Jun 2017) , 180—188

Bitcoin: Currency of the Future or Geek's Bubble?: Revealing the Mysteries of Blockchain as the Anchor for Innovative Currencies

Lionel Ming-Shuan Ni

Abstract: Over the past decades, the United States dollar inherited its status as the world's most dominant anchor currency (or reserve currency). However, the status became faltered due to the 2008 U.S. subprime mortgage crisis and the undertaken quantitative easing policy, leading to rethink what the world's anchor currency is. The "Bitcoin" began life in the mind of the brilliant creator Satoshi Nakamoto, whose true identity has not been revealed, and who published the ground-breaking white paper "Bitcoin: a peer-to-peer electronic cash system"in 2008. In 2009, the bitcoin system was generated and spread rapidly across worldwide. Compared with traditional currencies, bitcoin brings unprecedented two benefits: first, its underlying technology - blockchain - makes the bitcoin cost-effective, highly secure, convenient, transparent and the total amount is in control; second, to ensure stable operation of the bitcoin system, multiple techniques including encryption technology, proof-of-work consensus protocol, incentive mechanism and guarantee mechanism are fused. More importantly, the principle of the ledger technology blockchain is innovative, since it breaks through the centralized control from banks and governments, and makes use of mathematical algorithms to accurately control the circulation of 21 million bitcoin currency, which won the trust of the participants and lurkers, as well higher credit than that of the national central bank. Therefore, the worldwide central banks have invested in human resources and financial resources to develop the blockchain platform, in terms of system stability, application security, business model and so on. In 2016, the People's bank of China set up the institute of digital currency, seeking to hold the strategically active position in this international competition. The disruptive blockchain technology has become the critical engine of development of Fintech, shifting the way from primary stage to smart contract, and finally permeating into all fields of human society. It is believed that the fusion of the central bank's digital currency and emerging technology will have a massive impact on the financial infrastructure, currency policy, inclusive finance, regulatory policy and even the future digital economy. Blockchain is envisioned to have far-reaching implications in the era of Internet, and bitcoin will promote its unique advantages to lock the status of world anchor currency.

Keywords: digital currency; bitcoin; blockchain; anchor currency

Author: Lionel Ming-Shuan Ni received a bachelor's degree in electrical engineering at National Taiwan University in 1973, a master's degree in electrical and computer engineering at Wayne State University in 1977, and a doctorate in electrical engineering at Purdue University in 1980. In 1994, he was awarded the Fellow of the Institute of Electrical and Electronics Engineers (IEEE Fellow). In 2008, he became a member of the Hong Kong Academy of Engineering Sciences. His professional history also encompasses prestigious academic positions such as: Professor of Computer Science and Engineering at Michigan State University, Program Director of the U. S. National Science Foundation, Chair Professor of Computer Science and Engineering at the Hong Kong University of Science and Technology, and Chief Scientist of China "973 Program" project in wireless sensor networks. He is currently Chair Professor of Computer and Information Science and the Vice Rector (Academic Affairs) of the University of Macau. He has long been engaged in research, and his representative works are *Interconnection Networks: An Engineering Approach, Smart Phone and Next Generation Mobile Computing, Professional Microsoft Smartphone Programming.*

《南國學術》第七卷第二期（2017年6月），180—188

比特幣：未來貨幣還是極客幻想？

——“區塊鏈”創新貨幣之錨

倪明選

[摘 要] 世界貨幣錨定美元已達七十餘年。然而，2007年美國爆發的次貸危機以及隨後實行的幾輪量化寬鬆政策，使得全球重新思考世界貨幣錨定物的歸屬。2008年10月，中本聰發表了《比特幣：一種點對點的電子現金系統》的論文，提出了“比特幣”（BitCoin）這一概念。2009年，比特幣正式誕生，其“全網化”理念迅速傳播。相比傳統貨幣，比特幣具有以下兩大優勢：第一，它的核心技術——“區塊鏈”，使比特幣的數量可控、成本低、高保障、方便透明，從而突破傳統貨幣局限。第二，它的加密技術、工作量機制、獎勵機制、保障機制，都穩定有效地維持着比特幣系統的運行。更爲重要的是，比特幣利用區塊鏈記賬的原理，新穎高效，衝破了銀行和政府的中心化管制，並且利用數學演算法準確地控制2100萬比特幣的發行量，從而贏得了參與者和觀望者的信任，其信用度甚至高過國家中央銀行。因此，世界主要國家的央行紛紛投入人力、物力、財力對區塊鏈平臺進行研發，欲使它在系統穩定性、應用安全性、業務模式等方面早日進入成熟階段。2016年，中國人民銀行也成立了數字貨幣研究所，力圖掌握新一輪全球科技競爭的戰略主動。作爲比特幣的底層支撐技術，區塊鏈已經成爲新興金融科技發展的關鍵引擎，接下來會由初級階段向智能合約階段過渡，最終滲透到人類社會的各個領域。相信在不久的將來，中央銀行的數字貨幣將融合新興科技，對金融的基礎建設、貨幣政策、普惠金融、監管政策乃至未來數字經濟產生重大影響，“區塊鏈”將成爲互聯網時代的“寵兒”，比特幣或類似原理的數字貨幣將以自身優勢有機會鎖定新的世界貨幣錨定物的地位。

[關鍵詞] 數字貨幣　比特幣　區塊鏈　未來貨幣之錨

[作者簡介] 倪明選，1973年在臺灣大學電機工程系獲學士學位，1977年在美國威恩州立大學獲電子和計算機工程碩士學位，1980年在美國普度大學獲電機工程博士學位，1994年被評選爲美國電子電氣工程師學會院士（IEEE Fellow），2008年被評選爲香港工程科學院院士；曾任密西根州立大學計算機科學和工程系教授、美國國家基金委員會項目主任，香港科技大學計算機科學與工程系講座教授，中國“973計劃”中的無綫傳感網絡項目首席科學家；現爲澳門大學計算機與信息科學系講座教授、學術副校長；長期從事無綫傳感網絡研究，代表性著作有《互聯網絡：從工程角度來看》（*Interconnection Networks: An Engineering Approach*）《智能手機與下一代移動計算》（*Smart Phone and Next Generation Mobile Computing*）《專業智能手機編程》（*Professional Microsoft Smartphone Programming*）等。

自十九世紀以來，隨着經貿活動向全球拓展，貨幣流通區域擴展至人們生活的各個角落，促使世界發達國家開始尋找一種能穩定經濟、金融市場的強勢貨幣，進而使本國貨幣釘住這一強勢貨幣，與之建立起固定匯率。這種強勢貨幣類似於使船舶停穩的錨，因而被稱爲“錨貨幣”，亦即“貨幣之錨”。在二十世紀，第一個充當“貨幣之錨”的是美元。1944年7月，基於美國本土未遭受第二次世界大戰的衝擊，全世界三分之二的黃金都儲存於此，美國就邀請參加籌建聯合國的44國政府代表在新罕布什爾州的布雷頓森林舉行會議，最終確立了美元與黃金掛鉤、其他成員國貨幣與美元掛鉤的國際貨幣體系，即“布雷頓森林體系”（Bretton Woods system）。但是，自1958年後，美國持續的收支赤字導致美元在世界各地氾濫，動搖了人們對美元的信心；加之美國捲入越南戰爭，損耗了大量國力財力，法國因此於1965年拿出銀行的美元儲備，向美國兑換了黃金。其他國家見狀，也紛紛仿效，使得美國難以承受。1971年，美國總統尼克松（R. M. Nixon, 1913—1994）撕毀合約，宣佈美元與黃金脱鉤。脱鉤以後，美國還有一個重要武器，就是要求全世界石油的交易必須使用美元，因此，美元仍然是世界上的主要流通貨幣。1980年，美聯儲緊縮貨幣政策，導致美元升值；1985年，美國與日、德、法、英四國簽訂“廣場協定”（Plaza Accord），美元走弱；1987年2月的“盧浮宮協定”（Louvre Accord），終使美元匯率穩定，美元仍處於貨幣之錨的地位，直到2007年爆發“次貸危機”纔開始動搖。2008年，美國政府首次實施了量化寬鬆政策；接下來的幾輪量化寬鬆，使得全世界對美元失去信心，開始尋找新的“貨幣之錨”。

一　比特幣：國際貨幣新錨定物的誕生

美元之所以成爲貨幣之錨，在於各國追求外匯自由化、資本自由化和貿易自由化。在匯率浮動的作用下，強勢貨幣利用資本的自由流通，可以有定價權、議價權，從而獲得收益，所以，在國際貨幣體系下，確定貨幣錨定物至關重要。

（一）何爲理想貨幣？

在最新的國際貨幣體制下，哪一種類型的貨幣可以作爲一個錨，衆説紛紜。當前貨幣形式的主流是紙幣或硬幣，它既有容易流通、便於攜帶、數量可控制的優勢，又有可以僞造的劣勢和不足。雖然政府可以依靠中央銀行來保證貨幣流通的信用，但中央銀行的信用並不能保障國民的私有財產不受侵犯。因此，理想的貨幣應該滿足以下條件：（1）製造成本低。（2）維護成本低。（3）無法僞造。（4）攜帶方便（不佔用或少佔用實體空間）。（5）能夠保護用戶隱私。（6）發行量可以控制，流通過程容易監控，實現透明化管理。

（二）何爲理想貨幣交易？

理想的貨幣交易應該具備四個特點：

第一，付幣方擁有足量的貨幣。當付幣方開出一張支票給收幣方，付幣方確定自身有錢的同時，還要避免雙花問題。例如：付幣方開完支票後，在收幣方還沒確認之前，付幣方不能重新支付。這就需要收幣方及時確認收幣，用以保證付幣方付款後，收幣方可以及時收到錢。

第二，交易成本盡可能降低。例如：在中國銀行匯款，即使是1美元匯到美國，也需要繳納15美元的交易費用；也就是説，它的交易成本遠高於1美元。而面對面交易，則沒有交易成本；一旦經過銀行，交易成本便會隨之顯現。

第三，交易過程方便及時。交易一旦發生了，這項交易就必須同時記載到雙方的賬簿中。

第四，交易雙方不被他人僞造，其安全性能夠得到保障。要保障付款的對象是正確的，付款人也是無誤的，就需要交易記錄明瞭簡化，易於記賬核查。

（三）何爲理想的記賬方式？

理想的記賬方式，應該滿足四個條件：（1）個人的交易記錄容易查詢，交易完成後能夠及時更新交易記錄。（2）賬簿可以永久保留。（3）任何集體或個人都無法更改已經發生的賬簿記

錄，從而保護使用者的隱私。（4）賬簿的維護成本低，盡可能做到零成本。

理想貨幣、理想貨幣交易、理想記賬方式構成一個理想的貨幣系統，但如何實現是一個難題。對此，諸多學者以及實踐者都在思考這個問題，並達成了共識，即中心化的銀行是難以讓民衆百分之百信任的。而隨着高科技的發展，互聯網催生了一種新的貨幣流通思想，即人們可以不去單一實體，轉而採用“点对点”（Peer-to-Peer）的互聯方式形成一張網，使全民參與記賬——全民參與，自動聯結，由此形成公共賬本。這便是“比特幣”（BitCoin）誕生的驅動力。

（四）比特幣的誕生過程

互聯網的出現，給最保守、最傳統的金融界帶來了新的革命。事實上，這一新風潮是互聯網帶動的風潮，有着很大的革命力量。2008年10月，中本聰（Dorian S. Nakamoto）在網絡上發表了一篇論文《比特幣：一種點對點的電子現金系統》（Bitcoin: A Peer-to-Peer Electronic Cash System）[①]。文章首先對“點對點”（Peer-to-Peer System, 簡稱“P2P”）做了解釋，即在互聯網上搭建一個系統。也就是說，系統內有幾千臺、幾萬臺機器連在一起，任何兩臺都可以相互連通。甲與乙要進行交易，不需要經過任何中介；並且，其他主體的相互交易，甲、乙也看不到；甲、乙要相互交易不需要經過銀行，他們可以通過“點對點系統”進行連接。基於此，中本聰撰寫了一本白皮書，闡釋這一構想，並最終完成了軟件製作。隨後，在2009年誕生了第一枚比特幣。

二　關於比特幣的技術解釋

（一）比特幣的基本概念

比特幣是一個全世界互通的貨幣，沒有中央銀行對其進行控制。然而，如果從全民監督的角度進行理解，又可以認爲比特幣是有控制的，其控制的程度足以獲得大衆的信任。而且，比特幣可以保證其發行量不超過2100萬個。事實上，這一點連黃金都做不到。因爲，如果南非挖出了一大堆黃金，那麼，黃金行情就有可能會出現下跌。而比特幣的可控性，是由該系統的演算法決定的。該系統是自給自足的，通過編碼來抵禦通貨膨脹，並防止他人對這些代碼進行破壞。每個比特幣有所謂“區塊”的概念，不同區塊記賬，很多賬本將區塊連在一起，被稱爲“區塊鏈”（blockchain）。比特幣最小單的交易單位是一個聰，被稱爲“0.00000001 BTC”。這個交易聰，是最小的交易單位。所以，比特幣作爲一種世界貨幣，沒有發行成本，連紙都不需要，是一種在網絡上流通的數字化虛擬貨幣。這是一個去中心化、沒有任何人控制、完全靠互聯網來運行的點對點的數字貨幣。

（二）比特幣的加密技術

甲、乙進行交易，中間不需要任何人參與，這得益於密碼學的原理。密碼學有一個著名理論，叫“非對稱密碼系統”（asymmetric cryptographic system）。該系統中需要一對密鑰，一個是私有密鑰（private key），另一個則是公開密鑰（public key），如果用公開密鑰對數據加密，祇能使用對應的私有密鑰解密。反之，如果用私有密鑰加密，祇能用對應的公開密鑰解密。從私有密鑰可以推出公開密鑰，但公開密鑰永遠推不出私有密鑰；換言之，這是不可逆的。從這種簡單的數學觀念中，可以得到比特幣這樣的產物。舉例來說，甲要送東西給乙，乙把他的公開密鑰對甲發佈，這是可以公開的東西，私有密鑰絕對機密，甲把他的數據用乙的公開密鑰來加碼，擺在外面，祇有擁有私鑰的乙可以打開。也就是說，公私要配對，公開密鑰可用不同形式公開，私有密鑰祇有自己知道，由自己保存，通過密碼學原理保障交易無法抵賴和破壞。

更接近現實的例子是，如果張三要把0.3個比特幣給李四，首先，李四會把他的比特幣地址用二維碼宣佈出來（類似李四的公開密鑰）給張三，張三掃描李四提供的二維碼。這個二維碼，

① Dorian S. Nakamoto，“Bitcoin: A Peer-to-Peer Electronic Cash System”(PDF)，*Satoshi*，2009-05-24 .

就是比特幣位址。之後，張三打開他的比特幣電子錢包，他有李四的比特幣位址，張三發起一次比特幣支付，把錢轉到那邊去，一筆交易因此完成。以上闡述的是，張三保證將比特幣送給了李四。從李四的角度來看，李四是否能夠收到呢？因爲，張三用李四的公開密鑰來加密，李四用自己的私有密鑰解密，別人看不到，衹有李四收得到。那麼，李四怎麼知道是張三送的，而不是別人送的？張三送的時候要簽名，簽名是由張三的私有密鑰產生的，是不可逆的計算，所以張三要用他的私有密鑰做數字簽章，然後李四用張三的公開密鑰來論證這就是張三。也就是說，這個系統能保證張三送給李四的，李四一定收得到，而且一定是張三送的。

從整個系統的角度來分析，張三要給李四這筆錢，用了李四的比特幣位址，放到網絡上，別人收到是沒關係的，因爲比特幣位址是公開密鑰，衹有李四的私有密鑰纔能打開，別人是打不開看不到的。那麼，如果把這筆交易提交到互聯網，全球互聯網參加這個交易系統的人在幾秒鐘之內都會知道有這筆交易。然後，它會把很多交易結成一個區塊，這個區塊被論證以後，這交易便確定了，即成功了。張三付比特幣給李四，李四打開比特幣錢包，看看是否收到這個交易的錢。衹有他能打開，別人打不開。所以，這裏面最重要的東西是很多人把交易放在網絡上面，每一臺參與的電腦都會把交易去變成一個區塊，要確認交易能不能成功。打個比方，如果把參與者稱爲挖金礦的礦工，那麼，他們是通過“挖礦”來處理區塊，也就是爭取記賬權，即要驗證的交易是不是有效達成共識。如果有效，這個區塊就加到區塊鏈裏面；交易被認證了，保證就成功了。

（三）工作量證明機制

“工作量證明”（Proof of work）是一個數學問題，所有節點平等地計算該數學難題，最先獲得答案的節點將獲得這個區塊的記賬權。舉個簡單例子，看如何解決該問題。首先列出1到100，從中隨機抽一個數字，抽到1就贏了，抽不到1則繼續，直到抽到1爲止。1代表着記賬的權利，沒有抽到1的便再次抽取。最後總會有臺電腦搶到1，所以該電腦就可以記賬。這叫做證明工作量。那麼，1到100你抽取1，需要花一點時間；那如果要從1到1000抽取1，則需要的時間更多，工作量也更多。如果從1到1萬抽取1，電腦需要花費很多時間來計算，以爭取記賬的權利，這樣便耗費了更多的工作量。一言以蔽之，工作量證明函數決定計算方法，區塊決定輸入數據，難度值決定所需的計算量。

（四）獎勵機制

之所以要爭取工作量，是因爲獎勵機制的作用。2009年，該系統開始運作。如果第一個把區塊放上去，系統會贈送50個比特幣；如果又發現一個區塊搶上去，則又會有50個比特幣，總共100個。繼續進行，如果再次搶上，又賺到50個比特幣。最終，產生前21萬個區塊，都能獲得50比特幣。一個區塊是10分鐘，大概花費4年時間。2012年，當達到21萬區塊後，獎勵降一半，改爲搶到區塊贈送25個比特幣，同樣花費4年。2016年，獎勵的比特幣再減一半，爲12.5個比特幣。每4年減一半，一直減一半，減到2140年，就不能再減了，再沒有比特幣了。以這樣的一個演算法計算出來的比特幣，總數加起來是2100萬，不會超過這個上限，這就是比特幣保持發行2100萬的原因。該系統運行初期，由於沒有中央銀行，因而需要全民參與。所以，系統便設置贈送比特幣當做獎勵，比特幣由此得到增值。直到產生2100萬比特幣後，動機消失，參與者想退出，因而變成付費交易，再後面進入交易費獎勵階段，希望大家繼續參與、全民參與。大約到2140年，2100萬比特幣都發放完畢了，然後交易費用增加，這是另外的獎勵。

（五）系統的保障機制

系統要合理、持續、穩步運行，一個合適的保障機制必不可少，這一點可以用“拜占庭將軍問題”（Byzantine General Problem)來解釋。該問題主要研究的是，在缺少可信任的中心節點和通道的情況下，分佈在網絡中的各個節點如何達成共識。也就是說，一個交易或區塊產生了，參與者都將知道，每一臺電腦參與者都有全部的戰略，都有每個其他產品電腦的戰略，這增加了某

些參與者將其篡改甚至是丟棄的可能。比較極端的例子是“拜占庭將軍問題”：同盟軍總司令說，我們是打仗還是投降？下面的將軍等待命令。其中有一個將軍是間諜，他並不聽從總司令的命令。這個機制得以實現有一個前提，即各個將軍都不能互通，如果某將軍收到的命令說要攻擊，但是這個將軍叛變，他就會說投降。那麼，其他將軍怎麼知道收到的命令是打仗還是投降呢？爲了解決這一問題，系統設置了一個機制，即某命令的數量超過一半就執行。因此，在區塊鏈裏面，除非有一半以上的電腦想要篡改，否則，整個系統仍將進行下去。然而，由於超過一半作假的代價過高，因此很難篡改。

（六）比特幣的關鍵技術：區塊鏈

世界上第一個區塊是2009年1月由中本聰產生的，他本人賺了50個比特幣。表面上看，這似乎僅僅是一件單獨發生的交易事件。然而，在這之後，系統中所有的交易，以及所有參加交易的電腦，都因爲這個交易以廣播方式傳播到比特幣網絡上的所有節點。這意味着，這項交易放到區塊裏面了。通過論證以後，將區塊加入到區塊鏈內部，交易便成功了。這是一個交易戰略，參與者都能夠看到這個記賬方式形成的賬本，衹是參與者之間設有密碼，是不能看到相互賬本的。這裏面涉及一個更爲科學的技術問題。簡單來說，很多人在做的事情，要保證不能重複，但事實上可能會重複，不過這個問題可以通過交叉口技術解決。

在技術上，每一個區塊1兆字節空間，存放了很多交易，所有新交易以廣播方式傳播到比特幣網絡所有節點，每個節點試圖運行“挖礦程序”（mining program），通過“點對點”網絡監聽交易廣播並收集未經驗證的交易到區塊中，通過上述的工作量計算機制以爭取把它的區塊加到區塊鏈上，最快完成工作量計算的節點將此區塊廣播給所有節點。衹有大部分的節點都驗證通過，這條交易纔會被記錄到區塊鏈當前的區塊中，所有節點以當前區塊鏈後面創建下一個區塊的方式表明接受這個區塊，記賬成功，“挖礦”即爲創立區塊的過程。至於記賬的原因，就是上述的獎勵機制，記賬成功了能獲得比特幣，成功以後進入區塊鏈基本上便不能修改，除非一半以上的人要修改纔能被允許，但這基本上是不可能做到的，由此可以規避少數參與者惡意破壞數據。在這個機制中，基本上每10分鐘能把拿到的區塊加到區塊鏈上，然後準備搶佔下一區塊的記賬權，所以挖礦即爭取把交易數據添加到歷史公開賬目上面，即區塊鏈。這是區塊鏈的基本概念和技術概念，區塊鏈是一種新的記賬技術，是新的計算技術。

（七）區塊鏈的好處

區塊鏈是一個衆多機器在互聯網上共同使用的交易記錄平臺。它的好處有四：（1）所有參與機器均有完整備份。比特幣從誕生至今已運行了8年，整個區塊鏈所佔的字節空間還不到70千兆，共產生了45萬多區塊，並沒有佔據很大空間。即使少數機器損壞，也不會影響系統運行。對比來看，目前銀行系統最擔憂的便是機器癱瘓，一個備份不夠用，兩個備份仍擔心出問題。爲避免地震等地質災害將機器全部摧毀，銀行還需要在幾十公里以外進行備份。然而，採用區塊鏈方法，全民參與，大家都可以備份，而且不會出現單一機器宕機崩潰問題。（2）由於過高的成本，基本不會出現篡改機器運行結果的情況。除非超過一半的機器惡意欺騙，但這基本不可能發生。（3）系統能有效地保護交易記錄隱私。用密碼學原理，能保證相關記錄發生時序，所有的記錄不管時點相隔遠近，都不可能把後面記錄放在前面。（4）交易記錄透明和不變更。區塊鏈能夠保證交易記錄無法更改、無法刪除，從記賬角度看，這是一個最偉大的發明。

三　比特幣和區塊鏈技術的潛在用途與不足

（一）區塊鏈的潛在用途

目前，滙豐銀行（HSBC）和蘇格蘭皇家銀行（RBS）等正在開發一個落地的、標準的區塊鏈技術，以便於銀行之間溝通。另外，很多聯盟也在開發不同的區塊鏈平臺，很多應用可以由區

塊鏈平臺來實現。區塊鏈就是一個大的、保證可信的記賬簿，它是一個由互聯網衆多機器共同使用的交易記錄平臺。它的用途體現在多個方面。

第一，銀行業在區塊鏈應用上可以有很多探索和實踐，包括系統建設、技術研究、創業孵化、風險投資，金融產品等等。例如，韋爾銀行（CBW）推出了即時支付系統，愛沙尼亞銀行（Bank of Estonia）推出了數字加密技術保障的存款證明，荷蘭銀行（ABNAMRO Bank）研究區塊鏈如何應用於銀行支付系統，澳大利亞聯邦銀行（Commonwealth Bank of Australia）與瑞士聯合銀行（Union Bank of Switzerland）共同研究探索區塊鏈技術在金融服務中的應用，巴克萊銀行（Barclays Bank）將三家初創公司加入到該銀行的金融科技孵化器中，高盛集團(GoldmanSachs)向波士頓比特幣創業公司（Circle Internet Financial，簡稱“Circle”）注資五千萬美元，西班牙對外銀行（Banco Bilbao Vizcaya Argentaria）參與位於美國硅谷的比特幣公司“Coinbase”的C輪風險投資，德國銀行用瑞波幣進行國際匯款，花旗銀行（Citibank）已開發了三條區塊鏈並測試運行了“花旗幣”。各大銀行都在關注比特幣，全世界一些傳統上最保守的機構都在研究該項技術的應用。①

第二，電子發票。目前財務報銷的程序繁瑣，耗費人力，保存發票方面工作量也較大。如果改用區塊鏈完成，以後便不需用紙質的發票，所有發票從開票—流轉—報銷—存檔的全過程，均可用區塊鏈技術保存起來。它的功用就是可以進入整個發票的過程，保證發票是唯一的、不會更改、不會重複報銷以及真實有效。

第三，區塊鏈支付。2016年10月，中國工信部發佈《中國區塊鏈技術和應用發展白皮書（2016）》，指出“區塊鏈+支付”的應用場景，在跨境支付領域尤爲明顯。②例如，甲獲得10美元的稿費，但通過銀行，需要支付手續費15美元，而且需要兩個星期時間。如果運用區塊鏈技術，可以減少對賬成本以及提高速度和效率，也爲不符合實際的小額跨境支付開闢了廣闊空間。據統計，區塊鏈技術將降低約一半的企業間（B2B）跨境支付結算成本，使得流程更加透明，免除中轉銀行費用，付款方和收款方銀行直接聯繫，加快了總體交易速度。據麥肯錫調查研究，區塊鏈解決方案使得企業間跨境支付不再需要中轉銀行。③

第四，智能合約。普通合約的內容和程序繁雜，項目冗長，執行合約是一件很複雜的事情。如果把整個執行合約的流程或者過去簽訂的合約放入區塊鏈當中，便能夠形成智能合約。當合約人的條件全部滿足後，合約便會自動生成；如果貨到了，便會自動轉過去。學術界關於智能合約的研究始於1994年，現在區塊鏈技術出來以後，人們發現，這是能夠支持智能合約的最好平臺，終於可以通過區塊鏈實現智能合約的頒佈。

第五，驗明正身。據聯合國的統計，全世界共有15億人沒有身份證明。④這些人既沒有受教育的權利，也沒有生病看病的權利。聯合國一直試圖解決這個問題，區塊鏈則可以提供一個方向。也就是説，以區塊鏈爲基礎的數字身份證，衹要經過簡單的授權、證據和許可，就可以將自己的瞳孔、指紋等個人數據結合在一起，進行驗證。使用區塊鏈技術這項應用，還能對政府與商業治理產生積極影響。

第六，安全性。區塊鏈技術相對來説安全性比較高。例如，鑽石交易商擁有區塊鏈，就可以使每一顆鑽石有一對公開密鑰和私有密鑰。這就代表所有鑽石的交易過程，交易商都會有記錄。鑽石是稀有的高價值物品，用區塊鏈的方法提供了一個很好的交易平臺。

（二）區塊鏈的不足

區塊鏈技術目前仍處於初級階段，還有一些不成熟的方面。

① http://www.coindesk.com/8-banking-giants-bitcoin-blockchain/
② http://finance.ce.cn/rolling/201610/24/t20161024_17068760.shtml
③ https://buzzorange.com/techorange/2016/06/06/mckindsey-report-blockchain/
④ http://www.chinatimes.com/cn/realtimenews/20160817002353-260410

區塊鏈平臺評估的指標有三：（1）及時處理大批交易的能力；（2）交易記錄被確定的能力；（3）交易記錄被查詢的速度。從前兩個方面來説，由於一個區塊每10分鐘能產生大概4000多個交易，區塊鏈平臺是按照交易量大的優先原則處理，除非交易量小的多付交易費，纔可以先處理該小交易量的交易。這樣一來，大額交易可能要等一個小時，在區塊裏面誰也不能再改，大概到一個小時要保證這個交易不能取消，所以，這種處理大批交易的能力和交易記錄被確定的速度還不夠迅速。從交易記錄被查詢的速度來説，人們需要調取數據時的速度迅捷、查詢結構簡單，但這項新技術仍然存在很多探索的空間。從比特幣到區塊，從技術方面看，仍停留在原型設計階段，而且可擴展性還沒有經過大規模實驗考核。統一的區塊鏈技術標準尚未形成，在系統穩定性、應用安全性和業務模式等等方面尚未成熟。此外，除了比特幣，還缺乏更多其他的成功應用案例；況且，比特幣仍存在交易確認速度慢、區塊同步速度慢、系統反復運算更新進展緩慢、單位時間處理交易峰值數有限等缺陷。

目前區塊鏈仍處於互聯網的1.0時代，該技術主要應用於數字貨幣和驗證支付領域。它容易出現兩個問題：首先是安全問題仍待解決。例如，在電腦裏面有電子錢包，如果要進行支付，通過掃描，甲給乙把比特幣位址送來了，但如果甲的計算機被“黑客”（hacker）襲擊了，密碼中的私有密鑰也被偷走了，那麼，錢包裏的錢就會在瞬間消失。2014年，世界最大規模的比特幣交易所運營商“Mt. Gox2”因遭到黑客攻擊，85萬枚比特幣被盜一空，損失了4.67億美元。2016年，全球最大的美元交易平臺“Bitfinex”，也被黑客盜了價值7000多萬美元的12萬枚比特幣。因此，需要專門準備一個常用的“熱錢包”，單獨下載到電腦裏；交易完成後，不再放進電腦的“冷錢包”中。

另一個是洗錢問題。近年來，比特幣價格被炒得很高，已達到能夠洗錢的目的。據《經濟參考報》報道：2011年4月前，每一枚比特幣的價格一直都在1美元以下；之後，不斷攀升。2017年5月24日，已漲至2400美元。“過去4年間，比特幣價格大約上漲了113.3倍。”①這樣一來，一些人可以在國內購買比特幣，支付本國貨幣，購買以後送到國外再賣掉，就可以將黑錢全部洗白了。此外，曾經在全世界最有名的網絡黑市“絲綢之路”裏，黑客技術、販毒、武器都可以在上面買賣，它的交易全都使用比特幣。因此，相關機構需要防範監管，加強金融法規制定，對交易諮詢進行審查，調查資金來源是否合法。但是，這些制度建設，仍需付出持久的努力。

四　比特幣和區塊鏈在全球及中國的發展

比特幣和區塊鏈技術，已被美國高德納諮詢公司（Gartner）評價爲新興技術。2016年11月，該公司共計申請和接受與區塊鏈或數字貨幣有關的專利356件，是同年1月份的兩倍以上。包括帶頭的技術人員在內的金融界許多研發機構，紛紛進入該領域。據統計，截至2016年12月，至少有1300家公司在開發與區塊鏈有關的技術。②

比特幣不僅受到科技人員的重視，也活躍在證券市場。2017年2月12日，比特幣數量已達到1600萬，市值約160億美元。從當天的交易量來看，在過去的20小時內，已發生25萬筆交易，平均每小時交易在10萬筆以上。③這個數據是完全透明化的，參與者都能夠看得見。

根據2016年5月的數據顯示，世界上已有6318臺電腦參與其中（包括500餘臺超算機），其數量仍然在持續增加。自從比特幣觀念傳播以後，隨着比特幣的不斷升值，中國有些聰明人看到了“挖礦”能夠帶來收益，最早算出來者能有更大的收益，所以，開始動用大規模機群或特製芯片進行比特幣系統計算。根據《2014—2016全球比特幣研究報告》的統計顯示，全球算力排名前

① 周武英：“風口上的比特幣價值幾何”，《經濟參考報》，2017-05-26。
② https://www.finextra.com/finextra-downloads/newsdocs/pwc%20global%20fintech%20report.pdf
③ http://www.coindesk.com/price/

四的礦池均來自中國。這四個礦池的算力在全球的佔比分別爲26.36%、20.63%、12.87%、11.37%。[①]“中國礦池”已佔到總算力的70%以上，全網算力已超過每秒10—18次“哈希碰撞”（Hash collision）。當然，計算機完成如此龐大的計算量是要耗費大量電力、電費的，目前每小時的耗電量已大於60萬度。這也從側面反應出，如果有某臺計算機想私自更改賬簿，其成本也是巨大的。

區塊鏈帶來的技術對金融業來講是創新的技術，數字貨幣引起各國央行關注也是必然。由於要提前進行佈局，要明確參與區塊鏈應用的策略，快速推進業務應用場景的實施試點，協同落實監管的政策、參與標準，美聯儲（The Federal Reserve System）十分關注以比特幣等爲典型代表的數字貨幣對銀行業務、經濟活動和金融穩定的影響；英格蘭銀行開始討論由中央銀行發行法定數字貨幣的可行性，委託倫敦大學負責研發的數字貨幣“RSCoin”已進入初步測試階段；加拿大中央銀行正在開發電子版加元“CAD-Coin”，通過分散式總賬科技發行、轉移或處置央行資產；俄羅斯中央銀行宣佈成立旨在研究區塊鏈技術和分散式賬簿的金融科技和研發部門之後，俄羅斯國家結算存管局不久前也宣佈把NXT區塊鏈技術引入電子投票系統。而自詡爲數字貨幣產業中心的瑞士小鎮楚格鎮已於2016年5月3日開全球先河：該鎮議會決定，接受比特幣支付其會費和公共事業，以此作爲加密貨幣試驗的一部分。[②]在日本，《支付服務修正法案》於2017年4月1日生效，比特幣等虛擬貨幣支付手段合法性得到承認。在澳大利亞，自2017年7月1日起，比特幣將被視爲貨幣，廢除比特幣商品與服務稅。[③]

區塊鏈對金融業的最大好處是降低交易成本，提升效率和用戶體驗。中國的銀行位置都處在各城鎮最好的地段，在方便客戶借錢的同時，也加大了自身的成本。後來誕生的阿里巴巴小額支付發展迅速，就是因爲不需要這項成本。而且，2016年中國人民銀行成立數字貨幣研究所也表明，中國正在抓住科技革命的機遇，努力掌握新一輪全球科技競爭的戰略主動；同時，通過大量引進人才，研發中國自己的數字貨幣系統。不難想象，未來央行的人民幣，可以成爲不需要實物的人民幣，而是使用數字的人民幣。如果能用區塊鏈來控制整個系統，那麼，交易產生的區塊，每個納稅人承擔多少稅金，與誰交易等信息，都會有記錄；並且，通過低廉的成本，可以有效控制逃稅漏稅洗錢行爲，有助於健全貨幣監控制度，有利於豐富貨幣指標體系，成爲一個全透明的數字貨幣系統。

綜上所述，全球貨幣體系被美元主導了七十多年，但美元仍處在量化寬鬆的趨勢中，世界各國需要尋找未來貨幣之錨，以促進全球貿易。這一“錨貨幣”必須具有兩個“穩定性”：一是自身的穩定性，能約束貨幣發行；二是幣值的穩定性，能與全球經貿往來有一定的關聯，確保滿足實體經濟對流動性的需求，還能有效協調幣值穩定與流動性供給之間的矛盾。而類似比特幣這樣的新技術，自然會成爲人們的首選。隨着科學技術越來越迅捷地改變着全球的經濟形態和社會生活方式，從傳統貨幣到數字貨幣已是大勢所趨。區塊鏈作爲比特幣的底層支撐技術，已經成爲新興金融科技發展的關鍵引擎，金融界將迎來新一輪革命浪潮。雖然目前還處於區塊鏈的1.0階段，仍是以研究數字貨幣爲重心，接下來將會向由智能合約開啓的區塊鏈2.0階段過渡，最終滲透到人類社會的各個領域。相信在不久的將來，中央銀行的數字貨幣將會融合新興科技，對金融的基礎建設、貨幣政策、普惠金融、監管政策乃至未來數字經濟產生重大的響，“區塊鏈”也將成爲互聯網時代的“寵兒”。

〔編者註:2017年2月15日，倪明選教授應邀在“互聯網+金融系列講座”發表演講；受《南國學術》編輯部委託，魏萌、柯慧玲整理出了文字稿，作者、編者又對整理稿做了較大的修改。〕

① http://slide.tech.sina.com.cn/internet/slide_5_18966_70159.html
② http://www.cankaoxiaoxi.com/finance/20160513/1158289.shtml
③ 周武英:“風口上的比特幣價值幾何”，《經濟參考報》，2017-05-26。