

區塊鏈發展趨勢及產業應用

臺灣大學資訊工程系副教授 廖世偉

區塊鏈亟需應用在各領域中，才能真正創造價值，永續發展，進而改變世界。然而 2019 年 7 月 17 日 G7 財長嚴正關切 Facebook 幣 Libra 恐威脅全球經濟¹，Libra 的生態預含 Uber、Lyft、Visa、MasterCard、eBay 等，但各國紛表疑慮，可見大規模落地若牽涉到貨幣改革，往往路途遙遠。若是小規模貨幣改革（幣改），如臺灣各地紛紛在喊的縣市幣，雖然風險較低，未引起政府及金融機構行動，但小打小鬧如何長成大開大合的福國利民？以某一離島幣為例，雖然在區塊鏈智能合約發行上限 100 億元（號稱 1：1 對新臺幣），有真正符合貨幣的三大功能嗎？還是只是把點數稱作貨幣而已？

反觀中國的主權數位貨幣發行，不等美國 Facebook 或 G7，福布斯（Forbes）在 2019 年 8 月 27 日表示：阿里與騰訊等 7 家公司將使用國家數字貨幣。² 雖然新聞未經中國政府證實，時程為今年與否並非關鍵點；重點是近期數位通貨發展的三階段已經昭然若揭。2017 年起盛行的 ICO（Initial Coin Offering）是近期第一階段：ICO 為虛擬代幣首發，其虛擬幣不規範虛實整合，往往成為空氣幣。2019 年 6 月 27 日金融監督管理委員會宣布的 STO（Security Token Offering）規範引進第二階段：證券型代幣首發（STO）。其試圖規範虛實整合，數位代幣證券化的時代到來。近期的第三階段則是數位代幣金融化，主權數位貨幣不是證券，而是日常交易及清算皆可派上用場，其真正進入貨幣系統，並可追蹤其流向。最後，下一階段則是區塊鏈群募階段。虛擬通貨支付新創 Circle Internet Financial 至今募資金額超過 2 億 5 千萬美金，已成為全球前百大企業，為市值榜單的獨角獸，並推出 USD Coin 穩定幣在市場上流通，進入虛擬貨幣系統，並可追蹤其流向。

¹ 〈Facebook 幣 Libra 恐威脅全球經濟，G7 財長嚴正關切〉，《中央社》Tech news，2019/7/19
<https://technews.tw/2019/07/19/facebook-libra-g7-concern-a-lot/>.

² “Alibaba, Tencent, five others to receive first Chinese government cryptocurrency,” Forbes, 2019/8/27
<https://www.forbes.com/sites/michaeldelcastillo/2019/08/27/alibaba-tencent-five-others-to-recieve-first-chinese-government-cryptocurrency/#734fe8991a51>.

金融平台也在逐漸優化。虛擬通貨衍伸性商品交易所 BitMEX 今年推出保險基金，紓解保證金短少時發生波動的即刻平倉問題。

區塊鏈產業應用逐步遍地開花，對基礎設施需求亦增溫，Oracle、IBM、Microsoft、Amazon 均以雲端平台為基礎，提供區塊鏈服務，以利 IT 人員簡化區塊鏈的開發和營運。這種「鏈即服務」(Blockchain-as-a-Service) 現今趨勢為結合區塊鏈 PoC (Proof-of-Concept)，故解決方案建置商紛紛出現，而不是只是如 IBM 這種基礎資源供應商。其實 IBM 還結合其全球業務服務動能，提供諮詢服務，加速企業導入。但臺灣各產業應用新創（即應用服務供應商）投入者眾，而技術整合力及價值鏈參與者皆不足，所以幾乎尚無能結合金融的規模化商轉。蓋金流才能真正烘實有價值的數據流，去閉環一個感動人心、激勵人心的服務，讓消費者有感。舉例供應鏈區塊鏈，若先把生產履歷上鏈，當然是好事，但把生產履歷從資料庫搬到區塊鏈，真能把貨價提高嗎？貨就賣得出去嗎？故其中最最有做頭的還是結合金融如供應鏈金融，這最有殺傷力：用戶有感，而不是供應鏈區塊鏈而已。

「農業區塊鏈貸款」即為幫助青農從全國農業金庫融資的成功應用。農科院結合臺大的 AIOT 區塊鏈技術與弱勢農民，讓農民不再因為沒有會計三表或農舍抵押而借不到錢。蓋大部分青農都沒有會計三表及農舍所有權，但他們可以利用物聯網區塊鏈，讓他們的生產與生態取信於人，這是自證部分。他證部分則是由出貨紀錄在區塊鏈上而取信於人。因為只要農民真正有在耕種，是接地氣的「陸軍」，貨又賣得出去，則信評加分。反之，有資金的農民，雖然會計三表上好看，但可能是沒在耕種的假農民，這種「空軍」因是空殼，有捲款潛逃的可能。

以上提到三種區塊鏈業者類型，離消費者距離從遠到近順序如下，我們以「農業區塊鏈貸款」來闡明：

- (一) 基礎資源供應商：為亞馬遜。因我們使用 Amazon Web Services，另一類基礎資源業者是礦機礦池業者，但現今暢銷的礦機晶片為中國製造，臺灣沒有跟上。
- (二) 解決方案建置商：為臺大共識實驗室。謹遵前臺大校長傅斯年的「貢獻於宇宙」精神，互聯網式的開源無償，系統及原始碼皆交給應用服務供應商運營。
- (三) 應用服務供應商：為農科院；服務使用者為農業金庫與農民。臺灣以農立國，而農科院以農民為念，鏈結農民來使用區塊鏈服務。

第四種業者為底層技術開發商，如柯賓漢的 Dexon。公鏈大概是世上最難項目之一，其沒有成功，並非臺灣技術不行，而是上層應用服務業者不足及領導人的問題。

我國提出應用者多，解決方案者次之，其他兩類業者都很缺乏，值得鼓勵更多人投入。

國發會於 2019 年成立區塊鏈產學聯盟，開始積極統計業者，有回應的區塊鏈新創業者共 30 家以上，除上述生產履歷及供應鏈融資（2019/9/5 新聞〈突破傳統金融授信框限，新款 APP 助農民申貸〉），光在 2019 年 9 月發布的落地應用還有冷鏈物流（2019/9/2）、鏈上電表防盜電（2019/9/3），及醫療區塊鏈（2019/9/23 新聞〈宏達電健康醫療推新 AI 平台〉）。可見區塊鏈應用仍然前仆後繼，雨後春筍。業界趨勢是結合上述供應鏈融資及冷鏈物流，利用區塊鏈及時共享特性，讓小微電商不用自建平台、物流倉儲或銀行對接，即可享受跟大型電商自建倉儲物流與金流一樣的效率。

另一發展趨勢為：Dapp（智能合約開發之應用）及益趨成熟的硬體環境將綜效出安全的 Oracle（外部服務），再結合去中心化身分（Decentralized Identifiers, DID）驗證機制，將讓智能合約與區塊鏈錢包可以無縫接軌外部服務；舉例如鼎新的 Enterprise Resource Planning（ERP）資訊，或國安較真的物聯網資訊。最後，近年來由於零知識證明的到來，基於區塊鏈網路建立隱私交易狀態通訊協議已是可行，資訊的即時與隱私保護已是標配，應用如數位版權存證、生態健康指標自然將發生，跨單位的資訊流通經濟必將影響通證經濟。倘若上述 Data Economy 與 Token Economy 互相對標、相得益彰，必能提升消費端頻繁使用之獎勵機制。臺灣許多區塊鏈新創皆以此為商業模式，但通證價格支撐點尚未驗證，這是圖靈獎得主 Silvio Micali 所說現階段仍無解之題，Token Economy 是如 $P=NP$ 的圖靈獎級題目。

如上所述，區塊鏈產業已經超越數年前的證書區塊鏈以及生產履歷，不再只是存在性證明，而是聚焦這四大問題：（1）融入金流及信度追蹤的供應鏈金融，閉環服務而不是存在性證明，以真正幫助小微電商或農民；（2）區塊鏈身分認證及權限管理的成熟，加上硬體安全下，Oracle 串接鏈上鏈下，讓區塊鏈走向落地，從 offline 到 online；（3）區塊鏈隱私技術的成熟，零知識證明讓聯盟彼此放心隱私，生態可以組建，資料經濟到來；（4）物聯網資料經濟到來，對標通證經濟。最後，近年在 Google 帶領下，聯邦式學習（federated learning）成果紛紛公布，資料的聯邦互通（federation），如區塊鏈一樣鏈起來，可以幫助人工智慧學習（AI learning）。我們相信資料經濟及聯邦式學習（federated learning）是未來重要趨勢。

過去數年，臺灣有許多區塊鏈不可竄改性的成果，我們結合多個單位做的成就系統（證書、證照、資格、公益紀錄）、食安履歷及環境指標區塊鏈、捐贈金流追蹤皆開源無償。現在我們已經超越不可竄改性，聚焦痛點：降低 DLT（Distributed Ledger

Technology) 摩擦係數，解決隱私以增加流通性，串接鏈下以落地應用，讓區塊鏈是真被使用，而非炒作。除了證券型代幣 (security token) 外，「幣用不買」是消費者自我保護的防線：幣不是為了炒買，而是就像悠遊卡，是拿來用的。

過去 25 年來，網際網路已然發生，食衣住行娛樂乃至廣告紛紛數位化，而如本文所言，下一階段的身分認證將發生，ID 數位化勢在必行，但進度遲緩，監理與資安比網際網路複雜。網際網路是 Online-to-Offline，用於食衣住行是多多益善；但數位 ID 卻是 Offline-to-Online：關乎權益時，再小的投票都需實名制，金融的本質導致 Offline-to-Online 必然性。Offline-to-Online 是一小群一小群區塊先鏈起來，需要時間。這也是筆者與 Tapscott 寫的「區塊鏈革命」的觀點相左之處。我們不能為區塊鏈而區塊鏈，必須先闡明該區塊鏈應用真有解決信任問題，列舉該應用解決的信賴安全模型及威脅模型 (security model and threat model)，以及符合三個標準：(1) 該問題需要一個高就地取用性，高度分散性的服務 (highly available, distributed directory service)；(2) 該問題需要能事後提出可被稽核的日誌紀錄 (audit trail)；(3) 該問題在合規要求 (compliance) 下，或提出最終真理版本 (final version of truth) 要求下，必須有系統提供取消能力 (revocation)。最終真理版本往往是多方共識的。

最後我們談社會十分關心的監理問題。美國證券交易委員會 SEC (Securities and Exchange Commission) 是採取開放積極的監理。例如其積極管理利益衝突，當 Telegram 申請證券型代幣首發 (STO) 時，SEC 即要求 Telegram 退幣之前從 ICO (Utility Token) 募得之 17 億美金，而且這要求退幣已是慣例。所以區塊鏈金融的應用在推行代幣經濟時，必須十分確定其代幣在豪威測試 (Howey's test) 之下的屬性問題。科技金融的開放金融 (DeFi) 時代到來下，筆者觀察四周年輕人往往用科技金融的服務，而不是坐等金融科技的产品。圖 1 是近日自 coinlend 截圖之存放款服務利率，目前很多學生利用這所謂的「開放金融」、而不是網路銀行來滿足他們的需求。開放金融的用戶與純網銀的客群重疊，但如圖所示，這些 ML (Machine Lending, 機器合約交易) 相當地高利吸金、高利放款。因為虛擬通貨價格波動大，高利放款可行，而平台有很多商機，如圖中的 Bitfinex 放款免收費，而 coinlend 收 5% 的利息，Poloniex 放款收 15% 利息費用，Liquid 放款則收取 50%。用戶直接借出 1:1 對美元、日幣等法幣的所謂穩定幣，這些應用都如雨後春筍般紛紛出現。

我們以兩個創新創業者高度關心的局勢收尾：第一，政府對科技監理是否開放積極。第二，監理如何面對開放金融中存放拆匯的金融服務。這個可以從國發會區塊鏈聯盟的報名情況看出來，一半業者報名法規調適，而另一半報名產學合作及應用推廣。姑不論政府的時程表，事前自律及自動科技監理將事半功倍，也不牴觸政府監理。適度監理將能健康長遠，而自律及自動科技監理則可作為日後監理的參考。🌀

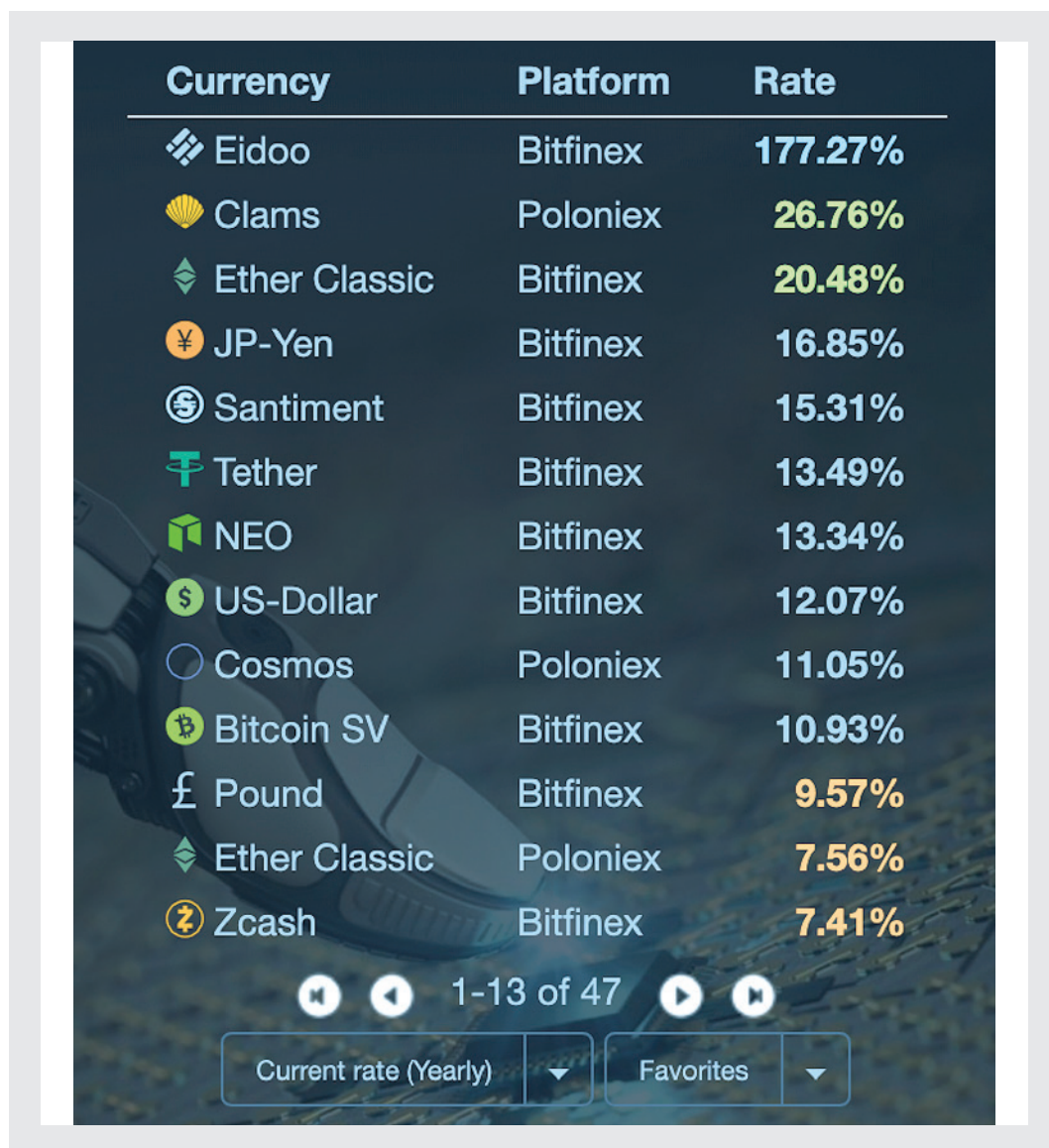


圖 1 開放金融的存放款利率

註：2019/9/4 自手機截圖。