顛覆性科技－區塊鏈

廖世偉副教授　國立台灣大學資訊工程學系 2016/3

一、前言：區塊鏈與金融科技變革
二、區塊鏈的五大技術創新
三、區塊鏈不等於比特幣
四、區塊鏈技術應用範疇
五、區塊鏈未來發展趨勢
六、結語：區塊鏈是金融科技發展的必經之路

一、前言：區塊鏈與金融科技變革

傳統金融產業正面臨互聯網金融及金融科技（FinTech）的衝擊，而其中又以數位金融相關的區塊鏈（Blockchain）技術為新興顯學，吸引全球政府機關與金融業巨頭相繼投入研究。目前區塊鏈技術在西方國家研發可謂如火如荼，光是投資到新創公司的資金就超過 10 億美金，是 1990 年代中期對網際網路的新創投資的 4 倍金額。區塊鏈重金投資不只是在區塊鏈基礎建設而已，也在上層應用，諸如金融業的結算系統，數字憑證如股票的發行，及日常生活中的應用比比皆是。

美國 SEC（The US Securities and Exchange Commission）也在 2015 年 12 月批准了 Overstock 用區塊鏈發行股票的計畫。我們敬佩 CEO Patrick Byrne 引領時代，選擇創新，公平，公正，公開的區塊鏈技術，並大幅降低了發行成本。英國首相的首席科學顧問 Sir Mark Walport 也建議英國政府，在主要公共服務上，例如稅收、福利或簽發護照等採用區塊鏈技術。在中國大陸，區塊鏈相關研究也正積極開展，中國人民銀行行長周小川在 2016 年 2 月接受媒體採訪時，再次提到央行正研究發行“數字貨幣”。

金管會指導下的金融科技（FinTech）辦公室及臺灣金融總會正在探討區塊鏈技術之發展趨勢及其在金融業之應用。2016 年 3 月初金管會資訊處長兼金管會金融科技辦公室執行秘書蔡福隆在臺灣大學記者會上強調他對金融科技暨

區塊鏈領域的期許：他希望我們區塊鏈的研發能做好產政學的無縫接軌，扮演臺灣 FinTech 領頭羊的角色。

我們深信對區塊鏈的研發投入能成為推動金融業科技創新的動力，培養 FinTech 產業領導人才，並能創造臺灣新的明星產業。2016 年 3 月初，行政院長張善政指出，中央銀行總裁彭淮南至立法院報告，提到「數位貨幣」，是很重要的進展。行政院長請央行強化白皮書裡數位貨幣的章節，並請金管會、財政部共同配合。我們樂見政府不落人後，讓臺灣在下一代的互聯網佈局中不再缺席，提高臺灣的國際競爭力。

二、區塊鏈的五大技術創新

首先，區塊鏈的應用遠不只於金融業。上述時空背景讓這篇文章舉例時，多以金融應用為例，但我們深信區塊鏈將是遍地開花，不限於金融業而已。尤其本段探討技術，更是回歸本質，保持技術中立於物聯網，金融理財，數位健康，Business-to-Business 多中心化應用（如供應鏈協同供貨(CPFR)，食安履歷追溯追蹤，device democracy 感測器物聯自治，資源需量反應競標），及 Consumer-to-Consumer 多中心化應用（如身分證明與投票，智權構想保護證明，群眾募資專款專用，開放資料協作版控）之間。

對於非科技背景的人而言或許較難理解科技領域的發展和革新，消費者僅對於產品或程式本身使用上有感，要深究其背後的邏輯和技術則相對困難，區塊鏈技術的出現亦不意外，對於一般大眾而言，此項技術最早被大眾認識當追溯於 2008 年 11 月一份署名中本聰的比特幣論文被發表在網路上及 2009 年 1 月 3 日 50 個比特幣問世。大眾常以為 Blockchain 今天只是到了 7 年之轉捩點而已，但一個偉大的創新往往背後的技術不是萬丈高樓一日起的，而是多年的累積與醞釀，且讓我們概略介紹此項重大發明與其背後涵蓋之幾項核心技術。遠比以上 2008 年還早的數十年前就有五個技術領域的研發十分重要：

第一，1982 年 Dr. David Chaum 提出注重隱私（privacy）的密碼學網路支付系統，如 e-cash，可算是比特幣區塊鏈支付技術在 privacy 方面的雛形，當然 e-cash 就犧牲了 traceability，與今日的區塊鏈不同。他的 privacy 研究影響深遠。直到今年（2016 年）初他還在 Stanford 的研討會上倡議新的 e-

cash，DigiCash，voting 方向，30 餘年如一日，令人敬佩。他 1982 年在美國加州大學 Berkeley 分校發表的論文，值得每位研究區塊鏈技術者拜讀： "Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups." 小結：Dr. Chaum 以來的 Privacy 研究十分重要，也奠定了比特幣支付技術應用的雛形。

第二，Scalability 是 Google 的拿手好戲，也是其競爭力的基礎。 現在比特幣區塊鏈是理論上可到 7 個 TPS（Transactions Per Second）。但 Visa 平時是 2,000 TPS, 尖峰時是 10,000 TPS。淘寶在 2015 年光棍節（11 月 11 日，即雙十一）的尖峰是 86,000 TPS。這些都是 value transfer。相對於以上 value transfer，若是 information transfer 的話，Twitter 平時是 5,000 TPS, 尖峰時是 15,000 TPS。For a reference，email networks 是每天有 183 billion emails。 183 billion emails 是 2,100,000 TPS。將來 IOT 時代會有相當高的 TPS，而且一定是多中心化的，如何估計到時 IOT value transfer 的 TPS，是我近期研究的課題之一。現在區塊鏈提供多中心化的 API－based value transfer，我們必須確保 scalability 及效率能跟上。比特幣區塊鏈現在大約 65 GB，新的 full node 加入時約需下載一整天。
如果做到 Visa 級別，約需 3.9 GB/day 或 1.42 PB/year。如果做到 150,000 TPS, 約需 214 PB/year. 光是比特幣區塊鏈本身，Roger Ver 預測未來兩年的 size 也會迅速成長，很快就會到 Terabyte 等級[1]。如此大規模運算時，我們系統的挑戰為何？開發者需要 simple and expressive 區塊鏈開發工具及模型。在系統層級，scalable， efficient，and fault-tolerant implementation 十分重要。

第三，Security and cryptography：區塊鏈過去 7 年多運行以來，接受到十分強大，從全世界來的 security 測試，但都沒有倒，除了 2011 年有一個 Value overflow incident。當然，這 incident 馬上獲得解決，也沒真正影響到比特幣的價值。該比特幣區塊鏈安全的原因主要是在於它背後強大的 core developers，問題發生後有馬上處理改善的能力。這種急戰力，open-source developers community 往往是我們華人相對較弱的地方。我之前在 Google 總

[1] Note: Giga 是 10 的 9 次方。Tera 是 10 的 12 次方。Peta 是 10 的 15 次方。

部開發 Android 時就有深刻的感受，部份手機廠沒有 Android core 的 development 能力，連改一行小問題都無法送 code 出來，只能一直求救，讓我感嘆競爭力強弱在這些小地方就可看的出來。如果我們沒有蹲馬步，沒有務本，投入 developers，投入真正核心技術的研發，將來在 open-source 及急戰力上只會輸的越來越多。

總而言之，Stress test 及 Penetration test 並沒有擊倒比特幣區塊鏈。社會上看到的比特幣被盜事件都跟區塊鏈安全無關，問題往往都是出在上層的交易所及人為因素。我們在臺灣大學的研究室對 security 著墨頗深，結合大數據，協辦眾多高科技金融犯罪事件。但若一寫又是一萬字，因這裡篇幅限制，將另篇文章探討。

第四，Flexibility：Flexibility 包含智能合約（Smart Contract），Virtual Machine，Governance Structure，及 Business Logic。Flexibility 是區塊鏈系統研究人員常常忽略的，因為系統人員或系統公司往往忽略應用。而做區塊鏈應用的又往往技術紮根不足，無法徹底解決 Governance Structure 及 Smart Contract 的問題。但 Flexibility 十分重要。區塊鏈若要遍地開花，落實在現實世界，雖然底層 scalability 十分重要，但同樣重要，或甚至更重要的是 Governance Structure 及業務邏輯的實踐。可以說沒有 Flexibility，就沒有落地。臺大黃茂榮教授曾說過，所有有用的技術，都必須接受商業實踐的檢驗。Flexibility 這正是 GCoin 區塊鏈的強項之一。GCoin 的 G 正是代表 Governance Structure 及 Global。前者代表 Flexibility，後者（Global）代表 Scalability。因篇幅限制，兩年多來鑽研 Flexibility 及 Scalability 的心血結晶將另文著述。

第五，Consensus Algorithm：區塊鏈雖然在隱私安全，密碼學，經濟模型上都有跨領域的突破，我們認為最重要的創新應是在算法算力，特別是共識演算法的創新突破。相較之下，區塊鏈在其他領域方面的貢獻比較像是十分漂亮的跨領域結合與設計，當然這些也展現了不凡的系統功力與設計實力，但我們還是要特別強調其在共識演算法的突破才是讓區塊鏈被稱為“Trust Machine”，並且稱得上是實至名歸。關於 Trust Machine，讀者可以參閱經濟學人雜誌 2015 年 10 月 31 日的封面文章，講述區塊鏈即為 Trust Machine。

現在區塊鏈百家爭鳴，百花齊放，例如做 Database 的研究人員說區塊鏈不過是分散式 Database（帳本），做 Networking 的人員說區塊鏈就是 P2P network，做 Programming Language 的老師說區塊鏈就是 一個 Programming Platform，做 Virtual Machine 及 Compiler 的研究人員說區塊鏈是 Smart Contract，做密碼學的研究人員說區塊鏈只不過是 PKC（Public Key Cryptography）的下一版。所以我們更要回歸到區塊鏈的本質：Trust Machine。例如，如果沒有 Trust 在我們討論的範疇，記錄東西時就用 Database 即可，不用扯到區塊鏈。如果沒有 Trust 在我們討論的範疇時，要點對點傳遞訊息就用 P2P network 即可，不用硬拉區塊鏈進來。其他領域也是類似情形。我們秉持追求真理，追求 Trust 的心，必能讓區塊鏈的研究突飛猛進。正本清源，我們不希望用 marketing 的名詞哄抬 blockchain，所以我們接受的英文名詞即為 blockchain 及 trust machine，接受的中文名詞即為區塊鏈。之前我們有用一中文名詞當作 trust machine 的中文翻譯，但我們發現該名詞幫助大眾理解 blockchain 的效果有限，反被當成 marketing term，所以我們還是中文就用區塊鏈，也不再翻譯 trust machine 一字了。

金融業與 Trust（區塊鏈的本質）息息相關。 我在美國近 1/4 個世紀，在 1/4 個世紀前，美國人常常稱銀行是“Trust Company”。這是一個有趣的稱謂，可見銀行跟 Trust 是息息相關的。當然，過去 1/4 世紀來，發生了多次金融危機，漸漸美國人就不再稱銀行是“Trust Company”了，而“Bank”這個字更流行了。為何金融業與 Trust 息息相關？這要回到金錢的本質。之前人們發現若隨時攜帶全部財產在身上，並不方便。若各自放在家裡，一不安全，二缺乏公信力。一個人說他有多少財產在家裡，並不取信於人。所以就有了“Trust Company”應運而生。當您把您的財產，例如一塊金條，放在 Trust Company，Trust Company 會給您一個 receipt，即為錢。最早是有多少金條，Trust Company 就發多少個 receipt，以維持公信力。這就像若您家裡有兩個兒子（這在古早時候，尤其是重要人力資產），但您不發您有兩個兒子的證明（receipt），而發您自己有 20 個兒子的證明，希望大家需求人力時都到您這裏來，遲早會碰到週轉人力問題及公信力問題。但當今 Trust Company 是多發相當多的 receipts 的。量化寬鬆（Quantitative Easing）以來，更是如此，

到當今連負利率政策都出台了。難怪 Trust Company 這字越來越少聽到，而 Bank 及肥貓一詞越來越常聽到了。

講到共識演算法，就必須介紹著名的“拜占庭將軍問題”。這是 Leslie Lamport 在 1982 年提出的 formulation。Leslie Lamport 在 2013 年得到計算機科學領域最高榮譽－Turing Award。 他的獲獎原因特別值得一提： Leslie Lamport imposes “clear, well-defined coherence on the seemingly chaotic behavior of distributed computing systems, in which several autonomous computers communicate with each other by passing messages.” 這正是 Blockchain 共識演算法及拜占庭將軍問題努力的目標。

如 Wikipedia 所述：拜占庭位於現在土耳其的伊斯坦堡，是東羅馬帝國的首都。由於當時拜占庭羅馬帝國國土遼闊，為了防禦目的，因此每個軍隊都分隔很遠，將軍與將軍之間只能靠信差傳消息。在戰爭的時候，拜占庭軍隊內所有將軍和副官必需達成一致的共識，決定是否有贏的機會才去攻打敵人的陣營。但是，軍隊可能有叛徒和敵軍間諜，左右將軍們的決定，擾亂軍隊整體的秩序。在進行共識時，結果並不代表大多數人的意見。這時候，在已知有成員謀反的情況下，其餘忠誠的將軍在不受叛徒的影響下如何達成一致的協議，拜占庭問題就此形成。以上 Wikipedia 的描述應用在分布式計算上時，即是指不同的計算機透過訊息交換，嘗試達成共識；但有時候，系統上的 Server Computer or a Computer node 可能因系統錯誤並交換錯的訊息，導致影響最終的系統一致性。拜占庭將軍問題[Wikipedia]就根據錯誤計算機的數量，尋找可能的解決辦法，這無法找到一個絕對的答案，但只可以用來驗證一個機制的有效程度。

跟比特幣論文發表同年（2008 年）得到計算機科學領域最高榮譽－Turing Award－的 Dr. Barbara Liskov 也對 Consensus Protocol 共識演算法做出重大貢獻。她 1988 年發表的 Argus，"Distributed programming in Argus"，是一個值得 Turing Award 的成果。Dr. Leslie Lamport and Dr. Barbara Liskov 對 Byzantine fault tolerance, distributed computing, 以及 Practical Byzantine Fault Tolerance (PBFT) 的貢獻，奠基了幾十年後 Blockchain P2P network 及其 consensus protocol。以下我們會在“挖礦”章

節做更深入的解說。最後，值得一提的是 Dr. Liskov 在 Stanford 的指導教授 John McCarthy 也得過 Turing Award（1971）。師生前後登科，傳為美談。我有幸在 Stanford 上他們的課及演講，受教大師風範，讓我深覺做區塊鏈研究不能是比特幣炒手心態，必須蹲馬步練功，回到以上講述的幾十年技術的本質，做好研發，為這片土地深耕技術，才能真正紮根，否則一窩蜂心態容易被誤導，將有愧大師風範。

小結：我們在本段解釋了區塊鏈的技術背景，分成五大面向討論：Privacy，Scalability，Security，Flexibility，Consensus Algorithm（區塊鏈上最重要的創新）。當我們解釋區塊鏈是怎麼來的，交代了區塊鏈的技術背景之後，接下來，我們將探討區塊鏈近幾年的興起背景。

三、區塊鏈不等於比特幣

比特幣

探討區塊鏈的興起，我們必須先了解比特幣的運作方式和原理。比特幣是種是一種全球通用的加密網際網路貨幣和線上支付系統，它是經由一種稱為「挖礦」的密碼技術產生，參與者貢獻他們的計算能力處理交易驗證並記錄到公開帳本中，獲取比特幣作為報酬。使用者可利用電腦、手機、平板上的電子錢包軟體來進行比特幣的交易。2009 年 1 月比特幣網路正式上線後，由於比特幣缺乏法定監管的機制，且比特幣基本上屬於匿名交易，所以常被用於地下經濟，成為不法分子洗錢或黑市買賣的管道，加上比特幣的匯率波動十分不穩定，較不具價值儲存等功能，故非大眾普遍接受的交易媒介。

區塊鏈

在比特幣的應用中(下同)，區塊鏈是一個分散式的帳本系統，採用密碼技術(挖礦)來確保交易的正確性(挖礦的原理將在下一小節介紹)，不同的區塊鏈技術採用不同的共識機制。最早使用區塊鏈這個技術的例子即是比特幣的交易系統，比特幣參與者們集體維護的一個具時序性的帳本系統(區塊鏈)。之中的每一個區塊網路之參與者都是一個節點，一套完整的帳本因為這些節點而得以保存，帳本中記錄了所有的歷史帳戶訊息，任何一個節點需要發起一個交易

行為都需要將交易行為訊息傳遞到區塊網路中的其他每一個節點中，如此可以確保此保存於所有節點上的帳本能精確地更新且驗證這一筆交易行為。

挖礦

最古老的區塊鏈共識機制是由一種稱為挖礦的過程產生，目的是決定記帳權共識：確認交易並把交易納入區塊鏈之中。挖礦能確保區塊鏈時間順序的正確、保護網路的中立性。有待確認的交易資料會被打包至某個區塊之中，而為了防止區塊被惡意篡改，區塊必須滿足一項非常嚴格的密碼學規則，隨意篡改的區塊會因為不符規則都變得無效，藉由這個機制，沒有一個人能控制區塊鏈中能包含哪些交易，或是任意更動區塊鏈的某一部份。

Andreas M. Antonopoulos 的精通比特幣一書中對挖礦有很好的比喻，我們可以把挖礦想像為一個大規模的多人數獨遊戲，一旦有人解出答案，這個數獨遊戲會根據解出所花的速度自動地調整困難度，若太快被解出則增加難度，若太慢被解出則降低難度，使得每次遊戲需要大約 10 分鐘被解出。一個幾千行乘幾千列的數獨，就需要很多時間才能被解出。一個已經近乎被完成的數獨，則可以很快地被驗證。我們認為這每十分鐘 advance 一次 state 的 state machine，用算法算力保護的 state machine，形成強大的 trust machine，是區塊鏈的最重要創新點。所以我們認為區塊鏈的本質是這個 state machine，trust machine，而非應用層面的 database 或 p2p network 觀點。

公鑰、私鑰、地址

在一筆交易中，我們只會看到收款對象的地址，一個收款者能夠擁有不只一個地址，也就是說，地址與收款者並無法做到準確的對應。每筆交易的付款與收款對象均可以有一個或多個，由於我們無法得知這些對象實際上是否為同一人，故能達成基本的匿名性。相對於傳統中心化機構的會員申請，要產生一個地址是相對容易很多的，只要符合一定的格式，都會被網路所接受。地址的產生，是私鑰透過一連串的雜湊函式產生，後段我們將對私鑰（private key）、公鑰（public key）和地址（address）的產生方式，做進一步說明，並介紹他們之間的關係。

私鑰 (private key)

私鑰可以用來管控相對地址的所有資產，從資產的傳送到交換，都需要用私鑰來簽名認證。私鑰基本上可以寫作 256 位元的二進位數，所有符合此一格式的私鑰約有 2 的 256 次方個，寫成十進位的話有足足 78 位數，所以只要隨機程度足夠，是非常不容易跟別人相同的。要產生一個隨機程度足夠的私鑰，最簡單的方法是丟一枚硬幣，人頭取 1，字面取 0，這樣一直丟個 256 次，就會得到一組跟其他人不一樣的私鑰。從私鑰到地址的過程中，私鑰會先透過一個橢圓曲線加密的對應函數得到一個長度為 512 位元的公鑰，橢圓曲線加密的數學式在此不再贅述。

公鑰 (public key)

公鑰最主要的功能，為驗證財產的擁有權。每筆交易中需要轉出任一財產的時候，須提出公鑰以認證該財產擁有權，並以私鑰對整筆交易簽名認證，用以確定財產擁有者同意此一財產的轉出。當礦工在驗證交易時，會檢查該公鑰是否配對於該財產，也即要能與該資產的地址對應，並同時檢查此一簽名是否屬於該擁有者。雖然私鑰僅能單向轉換成公鑰，但由於公鑰對私鑰而言，公鑰是取得私鑰的最後一道防線，所以我們會希望公鑰盡可能不要太常出現在公開的區塊鏈上，而前言提到，在轉出財產的時候一定需要公鑰來驗證，所以我們只保護收入端所顯示的公鑰。在收入財產的部分，我們再對公鑰做一層的雜湊函式，用以保護公鑰，此一雜湊函式的輸出即為地址。

地址 (address)

透過由 SHA256 與 RIPEMD160 所組成的雜湊函式，一個 512 位元的公鑰將會先由此雜湊函式轉換為 160 位元後，再編碼為地址，因此轉換途徑依序為私鑰、公鑰以及地址，僅由後者是難以回推出前者的。此地址可用於收取別人轉交給你的財產，擁有此地址相對應的公鑰與私鑰，便可以再把裡頭的財產轉出。

小結

區塊鏈技術最早是由於比特幣的流通為人們所認知，但是區塊鏈的應用卻不僅於此。過去幾年比特幣與其他使用區塊鏈技術的虛擬貨幣（統稱為Altcoins）的發展熱潮逐漸消退，市場也開始發覺區塊鏈的真實價值遠遠不僅是促成一個無政府虛擬貨幣的流通。北美與歐洲的投資人、科技新創、金融機構、以及政策制定者目前關注的方向已經從比特幣轉移到區塊鏈技術與既有產業生態的連結。

四、區塊鏈技術應用範疇

延續上文的介紹，讀者對於區塊鏈當有初步認識，本段落將就其現階段的發展狀況進一步闡述。區塊鏈在現階段的發展，其實已漸漸不再是一項新的技術，若以交通舉例，最初的區塊鏈可能是一家汽車公司推出的一款高級車內之技術，此款車有特別的引擎系統與路線規劃能力，能幫助駕駛人更快也更有效率的到達目的地。然而現在的區塊鏈發展已不僅於此，除被廣泛應用在其他的車款，甚而如店家等其他定點，當更多的車款與商家加入這項系統和使用其路線規劃技術，路線的規劃就更為準確，也因此，區塊鏈相形而言是一項基礎建設。本段落將就幾項較知名的應用做較為詳細的介紹和討論，發揮一些筆者的想像力，以期望協助讀者更加明白其中意涵。

以 Nasdaq 之 Linq 為實例探討

知名美國證券交易單位 Nasdaq 亦以區塊鏈技術為基底發展了一項相關應用產品—「Linq」，在去年年底問世，為業界首個在證券領域使用區塊鏈技術的私人企業。以證券交易為例，當每筆交易被數位化，且紀錄時間能被更加細化且有效率的被整理並紀載於帳本中，舉例而言，從以日為單位的紀錄到以 10 分鐘為單位的紀錄再甚至到秒鐘等更小的時間單位做記錄，此技術不但大幅降低了紀錄時間成本、金錢成本，也由於每筆交易被更有系統地紀錄著，在未來若要追蹤某筆交易時也大幅提升了效率。讓我們以搜尋引擎舉例做比喻，試想過去在尋找資料時，我們若想知道某個時期的貨幣的發展狀況，例如「唐朝的貨幣」，我們得從大批的圖書分類中先找到商業類別，再找到其中的金融類別，接著再從金融類別的圖書中找到所需要的和貨幣關聯之書籍，最後再去尋找貨

幣發展歷史，然而有時此項資訊卻非被紀錄在貨幣的專書中，我們若想找到這項資訊反而得去尋找歷史書籍，找到唐朝的歷史，再於其中尋找關於其貨幣的使用與發展，如此才可找到我們想要的資訊，既耗時又費心力，而搜尋引擎直接幫助我們把所有資料系統化完整地紀錄儲存，我們僅需在搜尋列上輸入貨幣、空格、唐朝即可找到相關的訊息，大幅降低了搜尋的成本。而此項應用的關鍵在於搜尋引擎如何將龐雜的訊息整理收納，讓不同類型的資訊互通，並在搜尋時有效率地提供我們所需要的資訊。在金融領域和區塊鏈的應用中，我們可以想像我們想查詢某家在 Nasdaq 上市之公司某一天某一時間點的證券交易狀況，由於系統化的整理歸類，我們可以更有效率的找到該家公司在我們所期待的交易日時間的交易狀況，此項優勢除了讓公司自己有更好的參照數據，還讓相關投資人能更快速的針對該公司做研究，此外，對於懷疑其犯罪的相關單位，例如當相關單位質疑其有內線交易之嫌，也可以透過搜尋該期間交易狀況並和其他數據做比對，基於交易紀錄時的不可竄改性和可追蹤性，讓資訊更加透明，也因事後被找查紀錄更加容易，協助降低犯罪的可能性。「透過此項區塊鏈應用，我們將革新資本市場的基礎系統」Nasdaq 的執行長 Bob Greifeld 在 Linq 推出並使用後振奮的如此說著，當提及的是在 Nasdaq 的應用中最大的改變是降低其清算交易所需的成本。

上述介紹的乃是區塊鏈對於資料庫技術革新所可能造成的改變，除了資料庫外，區塊鏈仍有其他應用範疇。

再以 Chain.com 為例

Chain.com 為一新興的網路平台，協助金融機構將金融商品分割發行，近來獲得 Visa、Citi Ventures、Capital One 和 Nasdaq 等具代表性的單位投資達 3000 萬美元，足以彰顯其於未來發展備受重視的潛力。在過去的年代裡，諸如股票、債券等資產的發行，需要中間商作憑證，進行拆分。透過區塊鏈的技術，電子股權、數字化資產都變為可能，新的智能資產交易平台仍可讓融資方與投資方皆便利地在平台上交易，股權可拆分成較小的單位，提高流動性，而優勢在於企業本身有更多的控制權，且不需中間機構。而在 Nasdaq 加入投資

之列後，兩者間的關係更不可言喻，未來數位資產和實體資產間勢必也將出現更為微妙的互動，此乃拜區塊鏈應用在資產數位化領域所賜。

本段雖僅就兩項實例作探討，當然區塊鏈仍舊具備許多可能的應用機會，其碎片化商品、商品可追蹤性、和分散式交易等特性可被應用至更多更廣泛的領域。

五、區塊鏈未來發展趨勢

基礎建設的概念其實是近來才出現的格局，在 2015 年之前的金融科技主要在於現有技術的優化、以及使用者體驗上的提升，但是並沒有涉及到金融行業的基礎架構；而現在隨著區塊鏈的技術提升，即將進入金融科技 2.0 的時代，全面革新金融業傳統的基礎架構，區塊鏈在不久的將來無疑是金融行業的基礎建設！

區塊鏈之於金融業的益處

(1)區塊鏈能提供更簡易的清算系統，讓發生交易即為清算，不需要花費額外的時間做清算的動作，且發生交易的當下即產生新的區塊，而新的區塊就會被寫入公開的分佈式帳本之中。

(2)區塊鏈去中心化的特性，讓所有的收付手續更加簡易，無需中間機構的介入，且所有的交易達成都必須足夠節點認證才算完成能夠寫入帳本中。

區塊鏈技術發展：過去、現在、未來

(1) 前期-數位貨幣(Digital currency)

區塊鏈最早的應用於 2009 年的比特幣(BitCoin)，且區塊鏈的基礎建立在節點彼此不信任上，因此區塊鏈就像提供了一台信任機器，讓交易完全透明公開，但是節點卻匿名僅存在一個公鑰的 IP 位址，在這樣特殊的機制下建立彼此信任。

(2) 中期-協定(Consensus)

在 2014 年之後，區塊鏈因為其 P2P 的特性，除了被應用在虛擬貨幣上，之後開始被延伸使用於多樣資產的移轉上面，諸如股票、證券、土地等資產的交易上，上文提及的 Nasdaq 即為一例。

(3)未來-整合的共同協作平台

區塊鏈開放 API，不侷限於金融行業的應用，將會成為眾多平台的平台，不論會計、物流、房產、保險各個領域將可以利用區塊鏈的技術進行革新，藉由開放原始碼，讓人人創新創業成為可能。

值得再次提及是區塊鏈技術的出現和應用並非擊敗現有的金融、物流等體系，其乃針對現有體系下不足的部分進行改善，並促發新機會的誕生。

金融產業應用區塊鏈的可能挑戰

(1) **大眾認可**

對一般無相關知識的大眾而言，要理解並認同此一新興技術是相對有挑戰的，相關的宣導和基本概念必須能夠傳遞給一般消費者，讓大眾對此有基本的理解。

(2) **法規制定**

法規的出現和制定總是走在最後，新興技術往往對現有法規產生挑戰，相關的約束和現有法條的編修勢必得有所因應，此乃保障大眾和企業，也對整個體系而言。

區塊鏈未來趨勢展望

現今海外許多先進國家已投入大量資金於區塊鏈的技術研發中；而眾多海外區塊鏈應用的新創公司例如 G Coin,、Hyperledger、Consensys、 Eris blockchain 等等亦紛紛興起。截至 2015 年 10 月創投公司累積投入區塊鏈領域的資金高達九億兩千一百萬美元；而且有 30 家以上的銀行以及金融機構已經開始投資並分析區塊鏈領域的科技，證明區塊鏈成長潛力無窮。

底下概略介紹三間應用區塊連技術且仍在持續發展的公司做舉例：

(1) **Ripple 公司：**

主要業務在於海外的跨境支付，在各家銀行帳目系統不同的基礎上，建立一個統一的金融清算系統，得以提高跨境支付的流動性。

(2) **R3CEV 公司：**

其與 30 多個會員銀行共同合作，其中包括美國銀行，摩根士丹利，德國商業銀行等組成；藉由區塊鏈在於金融行業的基礎建設，建立共通且公開分布式存儲的帳本、執行更簡易的交易清算系統，讓所有程序更簡化。

(3) **Guardtime 公司：**

打造全世界的資訊驗證系統，不論在電信業、航空業、金融業、保險業都需要這樣便利的KSI無鑰簽章認證系統；KSI signatures會與區塊鏈連結，能夠不需要經過第三方即可驗證數據資訊的正確性。

甚至在可以預見的未來，區塊鏈會能夠打造國家級的應用，實現智能政府利用區塊鏈Crypto 2.0的分佈式存儲以及去中心化的特性，幫助政府更加便利的收稅、發放簽證、提供更簡易的土地登記等服務；建造一個國家級的帳聯網。

六、結語：區塊鏈是金融科技發展的必經之路

網際網路起點，始於1973年TCP/IP協議，它打破了由中心傳遞資訊的傳統方式，突破訊息在傳遞過程中地域、物理及成本的限制；區塊鏈正是TCP/IP協議的升級版，以共識機制確保資訊的真實性。區塊鏈將推動嶄新的共享經濟，形成與資產鏈結的全球開放信用體系(Trust Machine)。

國際對於區塊鏈的重視已不在話下，較為領先的國家如美國、歐洲和大陸等國在相關領域的投入逐年攀升且日益成長，台灣早先受限於法規，其實處於一相對落後的局面，近來金管單位對與金融機構投資約束的鬆綁著實有助於臺灣繼續邁進，搭上此班技術變革的列車。廣闊的看，長遠的看，現在我們正在面臨一個抉擇點，繼續缺席創新，還是擁抱創新？我們衷心期望臺灣在下一代網際網路開發不缺席：掌握下一代網路技術及應用創新，區塊鏈這trust machine將源源不絕的鏈出可信data ，使社會從IT到DT (Data Technology)，並真正進入open data，big data，及data streamline時代。