

2017年新興領域投資趨勢觀測系列（一）
比特幣與區塊鏈篇



范秉航 副研究員/ 林秀英 副研究員

台灣經濟研究院

2017年2月28日



- 1 比特幣與區塊鏈技術之基本介紹
- 2 比特幣與區塊鏈領域之投資分析
- 3 區塊鏈領域之27種應用與個案分析
- 4 國內比特幣與區塊鏈領域發展概況
- 5 比特幣與區塊鏈的展望與挑戰

壹

比特幣與區塊鏈技術之基本介紹

一、何謂比特幣？

何謂比特幣

- 比特幣(BitCoin) 是一種P2P形式的虛擬貨幣，最早在2009年由化名的開發者中本聰以開源軟體形式推出。由於其採用密碼技術來控制貨幣的生產和轉移，因此比特幣也被認為是一種電子加密貨幣（ Cryptocurrency ），由於其有特殊的隱秘性，經常被拿來當作非法交易的媒介。

如何取得

- 透過「採礦」的過程產生，參與者透過處理交易驗證和記錄來獲取作為手續費的比特幣，或取得新產出的比特幣
- 透過交易來購買

交易價格



不斷創新高的交易價格

Bitstamp : \$1,238 USD (38,192 TWD)

Coinbase : \$1,250 USD (38,563 TWD)

Bitfinex : \$1,237 USD (38,161 TWD)

BTC-E : \$1,222 USD (37,699 TWD)

*2017.3.8價格

二、何謂區塊鏈？

何謂區塊鏈？

- 區塊鏈是比特幣底層的基礎技術，區塊鏈技術由密碼學、數學、演算法及經濟模型所組成，結合點對點的網路關係(P2P)，並採用分散式共識演算法，來解決傳統分散式資料庫的同步問題，可說是一套整合跨領域技術的基礎建設



區塊鏈的運作模式

- Block 是一組有欄位的資料集合，因為不同的 (block) 以 “hash 值”建立起鍊結關係 (chain)，所以稱之為 block + chain。hashing 是 “防止電腦文件被竄改” 的程式演算法，有 hashing 才能建立區塊之間的鏈結關係
- 區塊鏈的正常運作是藉由「身分識別與防偽 (PKI 技術)」、「訊息傳遞與擴散 (p2p data communication)」以及「資料的保存與連結 (Block & Chain)」等技術的支撐。



區塊鏈的特色

- 難以造假
- 無法篡改
- 去中間化
- 透明易稽核
- 快速交易清算

適合區塊鏈導入的環境

- 交易過程包括多個參與方，彼此間信任程度不夠
- 需要完整的交易流程資訊，而非片段的雙方交易資訊。
- 資產所有權必須能隨時被檢驗，以免發生造假或 double spending 的情形。

不適合區塊鏈導入的環境

- 需要 “高頻交易”的環境。
- 資料量傳輸太大，會造成網路傳輸在實作時無法負荷。
- 交易資料的時序與事後確認，並不是主要的考量重點。
- 作業流程並不明確。

三、區塊鏈運作流程

一筆新交易產生時，會先被廣播至區塊鏈網絡中的其它參與節點

產生一筆新交易

每個節點會將數筆未驗證的交易Hash值收集到區塊中，每個區塊可以包含數百筆或上千筆交易

各節點將數筆新交易放進區塊

各節點進行工作量證明(POW)的計算來決定誰可以驗證交易，由最快算出結果的節點來驗證交易，這就是取得共識的做法

決定由誰驗證這些交易

交易驗證完成

各節點驗證並接上新區塊

取得驗證權的節點將區塊廣播給所有節點

所有節點一旦接受該區塊後，先前沒算完POW工作的區塊會失效，各節點會重新建立一個區塊，繼續下一回POW計算工作

其他節點會確認這個區塊所包含的交易是否有效，確認沒被重複花費且具有效數位簽章後，接受該區塊，此時區塊才正式接上區塊鏈，無法再竄改資料

最快完成POW的節點，會將自己的區塊廣播給其他節點

四、區塊鏈技術與金融交易流程

金融服务主要交易流程

交易發起

交易前驗證

交易審批

合約簽訂

交易處理

帳務處理

交易完成

Pain Points

人工發起

- 人工驗證
- 訊息分散
- 詐欺
- 多方驗證單位介入
- 耗時

紙本合約

- 交易時間遲滯
- 系統風險
- 人工處理

區塊鏈技術

系統自動觸發
(智慧合約)

- 快速實時驗證
- 無須第三方介入
- 訊息透明安全
- 反詐欺
- 無紙化審批

智慧合約

- 跨系統即時同步
- 最小化系統失誤風險
- 節省帳務處理工作

交易紀錄具永久性

五、區塊鏈技術的優缺點

區塊鏈技術早在2009年
比特幣出現的前十年就
已經陸續出現，經過巧
妙組合產生顛覆性創新

優點

- 去中心化：資產交易不再需要中介機構
- 可程式化：可以自動履行基本業務邏輯，建立智慧合約
- 安全性：每一筆交易紀錄均經查核驗證，維護審核線索
- 成本與資產效率：催生低成本與高資產效率的商業模式



這是一個還在尋找題目的解
決方案

By 李顯龍

缺點

- 未規模化：缺乏規模與網路效果，需付出高額邊際成本
- 先端應用：技術仍未成熟，巨量交易資訊的處理成效尚待驗證
- 建置成本：分散式帳本具高算力要求
- 共識：區塊鏈記錄要經所有參與者同意、認證，共識機制將可能影響交易速度



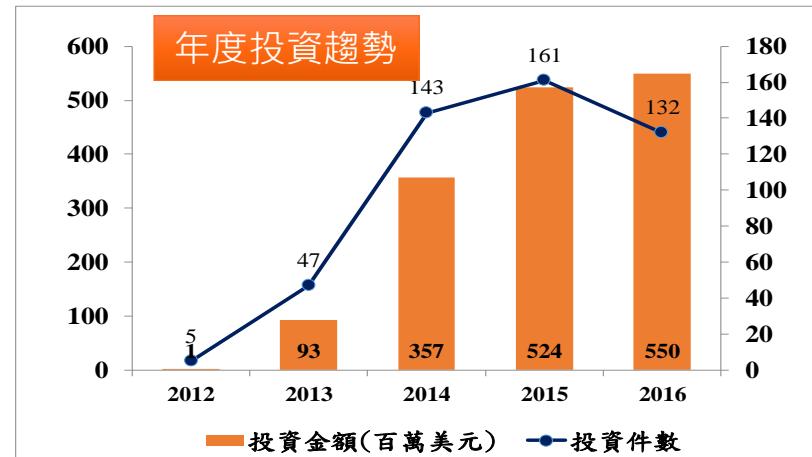
貳

比特幣與區塊鏈領域之投資分析

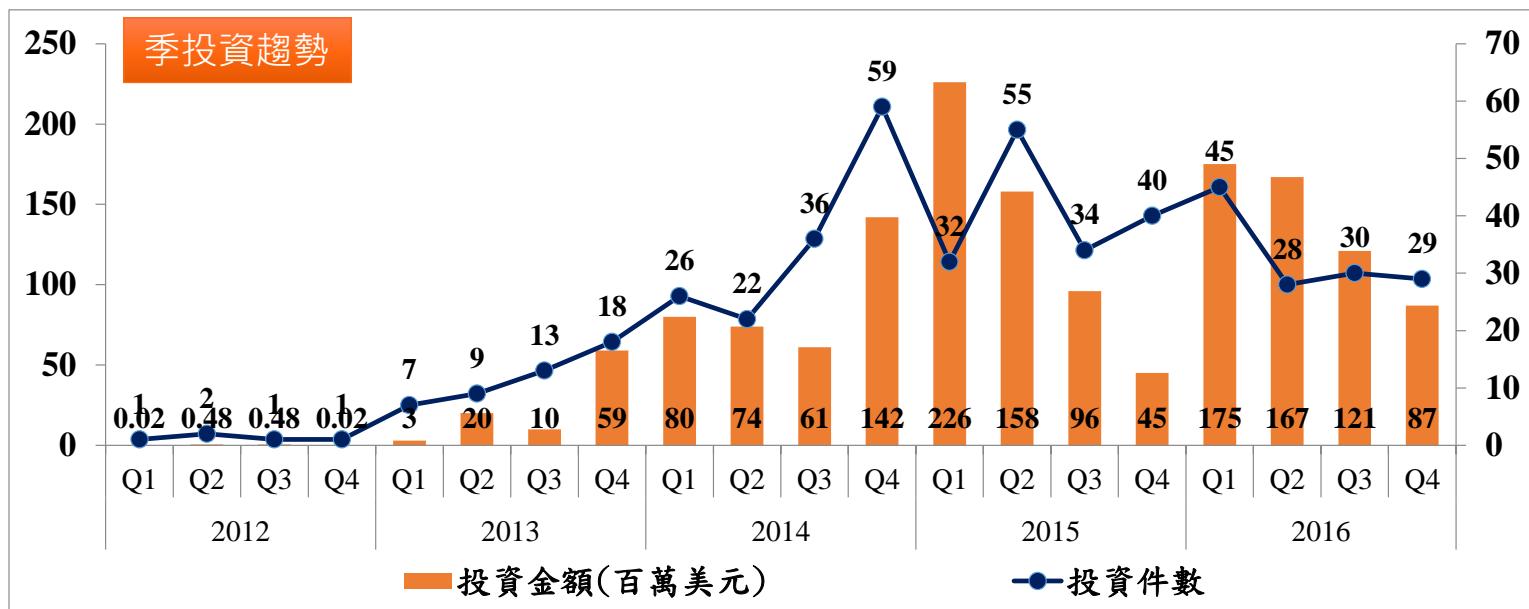
比特幣與區塊鏈科技獲投趨勢

- ◆ 投資件數：2009-2011年僅有零星3件獲投交易，直到2012年起投資交易才密集出現，2015年161件創新高，2016年下滑18%至132件，尚低於2014年的水準。
- ◆ 投資金額方面：2015-2016二年間每年投資金額都超過5億美元以上，2016年儘管投資金額成長趨緩，但仍為歷史新高

2015	161件 ▲13%	5.24億美元 ▲47%
2016	132件 ▼18%	5.50億美元 ▲ 5%



Source : CB Insights (2017)



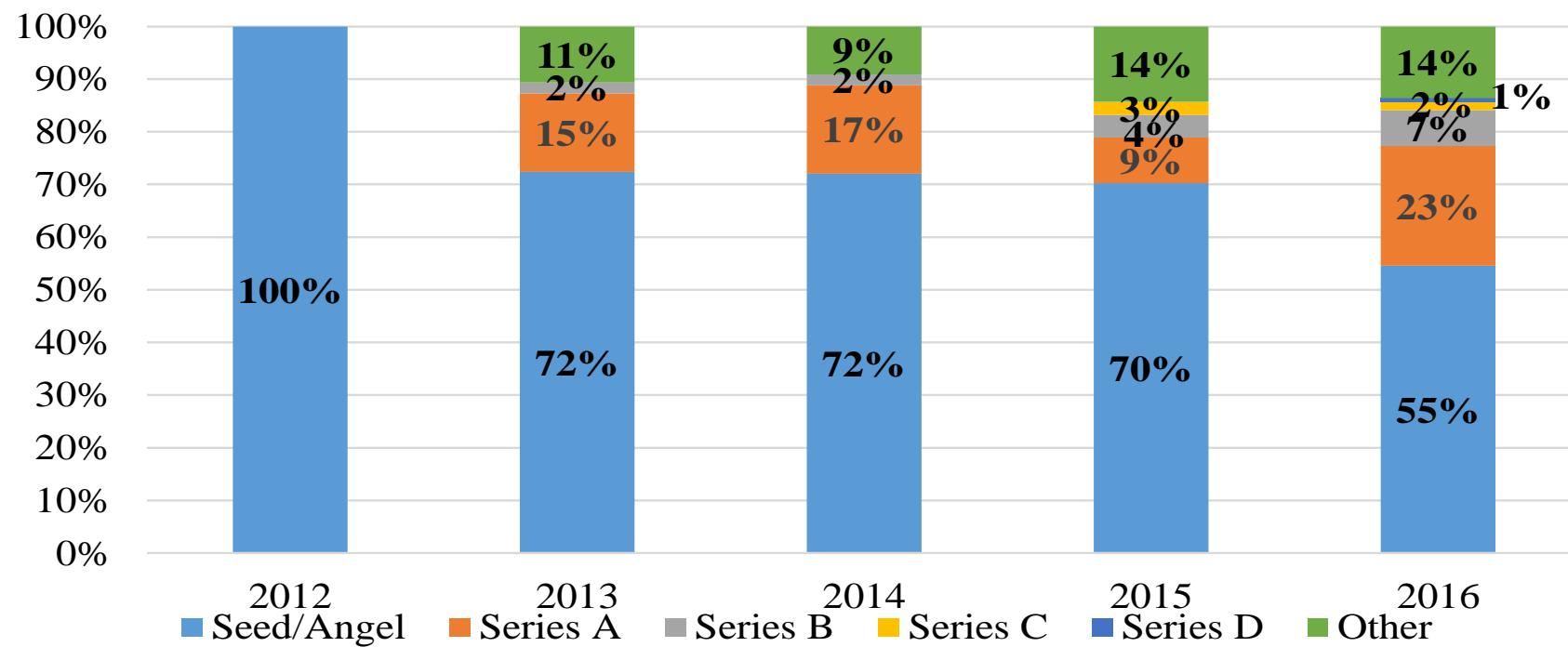
Source : CB Insights (2017)

早期投資（種子輪/天使輪、A輪）的件數比重

- 比特幣與區塊鏈為新興領域，2012年投資的案件皆為種子輪與天使輪
- 隨著近幾年的發展，投資人持續對具潛力的企業進行追加投資或新投資，使得2016年A輪獲投比重上升，同時也首次出現D輪投資（Circle/ 6,000萬美元）



投資件數占比-按階段



比特幣與區塊鏈領域獲投新創企業的市場範疇分布

電子錢包與貨幣移轉服務

電子錢包公司主要開發安全的軟體錢包用以儲存加密貨幣。

貨幣服務公司主要經營加密貨幣匯款或移轉平台。



P2P交換和P2P借貸平台

指區塊鏈基礎的P2P交換市場，用戶可以不需中介直接交換貨物。區塊鏈基礎的P2P借貸平台則是允許用戶與同業（非傳統金融機構）進行貸款交易



交易所和加密貨幣交易

係指建立加密貨幣的交易或加密貨幣交易平台的公司，在交易平台上，消費者、企業和專業人士可平台上交換法定貨幣或其他有價值商品的加密貨幣。



資本市場和金融服務

主要為金融機構和中介機構開發清算、結算和數據管理等解決方案的公司，以及建立於區塊鏈基礎的投資公司



企業服務和貨幣

為不同用途與不同使用者的開發區塊鏈操作系統、API和協議的公司。或為客戶建立獨特和客制化的加密貨幣和數位代碼(tokens)的公司



社交和瀏覽器

開發區塊鏈基礎的社交網絡與構建區塊鏈安全的Web瀏覽器，通常涵蓋微交易功能。



物聯網、身份辨識和內容管理

物聯網公司提供分配實體資產具區塊鏈安全的數位簽章。身份辨識公司提供身份辨識的管理應用程序，確保身份識別數據。

內容公司主要經營區塊鏈基礎的內容平台，並參與對內容使用的微型小額交易



加密貨幣採礦

加密貨幣的採礦設備和服務公司是主要構建或操作開採加密貨幣的硬體、軟體、雲端礦池(cloud-based pools)和其他服務的公司。



存儲、安全和監管

使用區塊鏈安全技術進行客戶的數據儲存。安全和監管公司則是透過組合加密貨幣地址的追蹤評估區塊鏈的風險與加密貨幣的犯罪行為。



商家服務

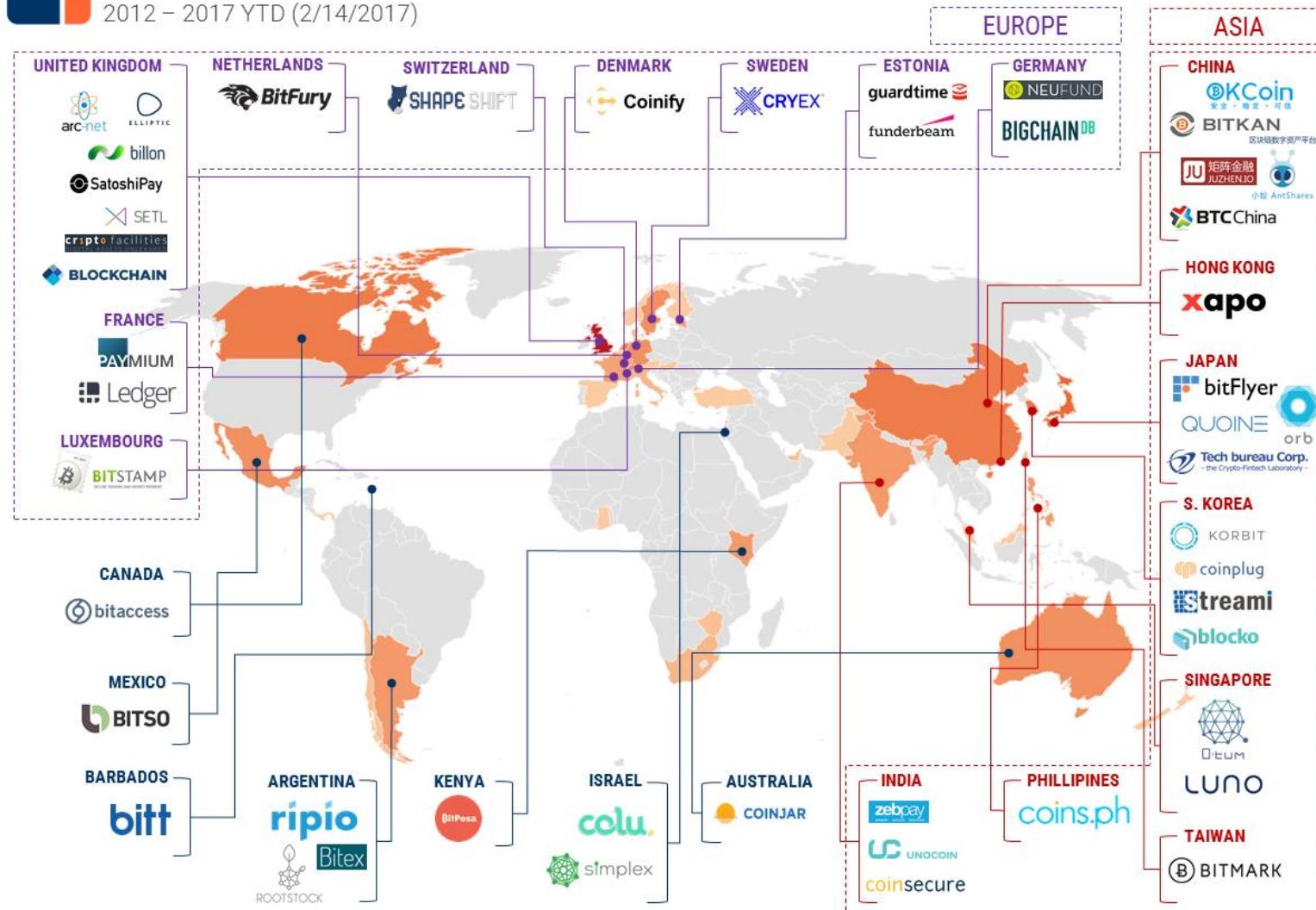
為商家和賣家開發加密電子貨幣和區塊鏈解決方案的公司，如提供區塊鏈支付服務、獎勵等的解決方案。



Source : CB Insights, 本研究整理

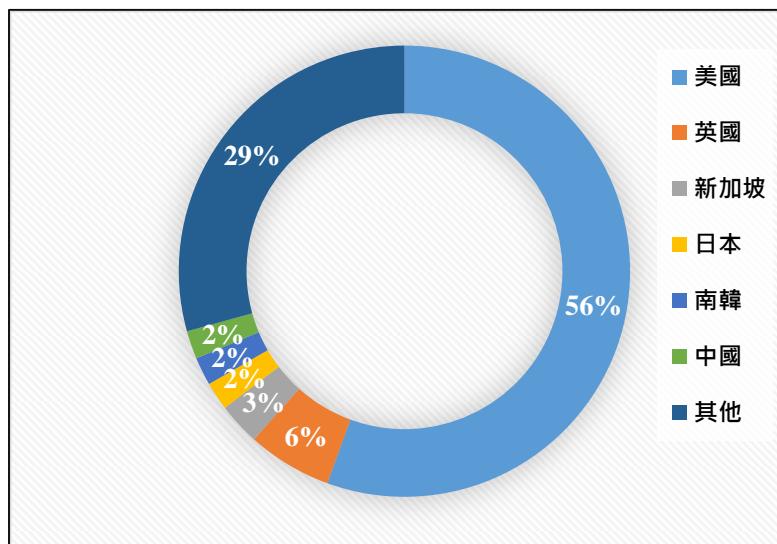
比特幣與區塊鏈領域獲投新創企業的市場範疇分布

GLOBAL BITCOIN & BLOCKCHAIN COMPANIES 2012 – 2017 YTD (2/14/2017)



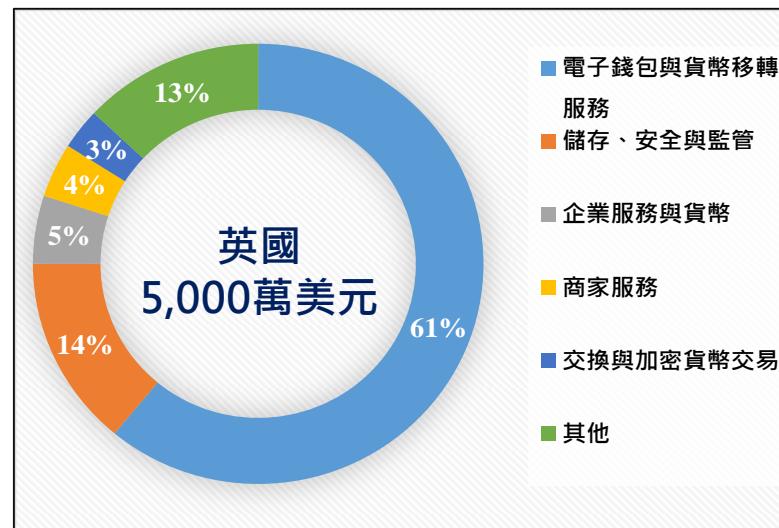
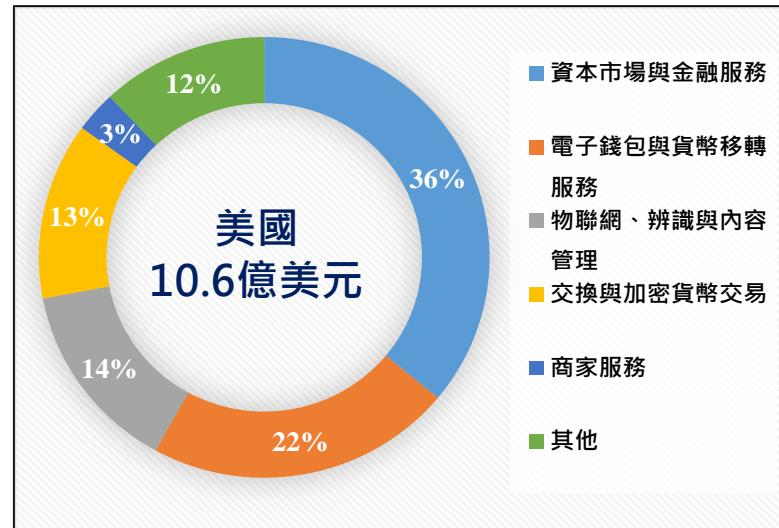
比特幣與區塊鏈領域獲投地區分布

獲投件數占比 ~ 依國家區分
2012-2017(2/14/2017)



Source : CB Insights (2017)

美國與英國獲投金額占比 ~ 依領域區分
2012-2017(2/14/2017)



Source : CB Insights (2017)

貳、比特幣與區塊鏈領域之投資分析

比特幣與區塊鏈科技獲投前十大企業 -2012 ~ 2017 (YTD 1/30/17)

名次	公司	次類別	國別	獲投金額 (百萬美元)	投資輪次數
1	Circle Internet Financial		電子錢包與貨幣移轉服務	愛爾蘭	136
2	Coinbase		交易所和加密貨幣交易	美國	117.21
3	21 Inc		加密貨幣採礦與API交易	美國	121.05
4	Ripple		資本市場和金融清算、結算和數據服務	美國	93.6
5	BitFury Group		加密貨幣採礦	俄羅斯	90
6	Blockstream		資本市場和金融清算、結算和數據服務	加拿大	76
7	Digital Asset Holdings		資本市場和金融清算、結算和數據服務	美國	67.2
8	Chain		資本市場和金融清算、結算和數據服務	美國	43.7
9	Xapo		電子錢包與貨幣移轉服務	美國	40
10	bitFlyer		交易所和加密貨幣交易	日本	36.11

資料來源：CB Insights (2017) ; Crunchbase ; 台經院FINDIT整理

比特幣與區塊鏈科技獲投前十大企業個案



Circle Internet Financial

- 成立時間/地點：2013年成立於愛爾蘭都柏林
- 產品與服務：以比特幣區塊鏈為中心的 P2P金融技術公司。
- 獲投：歷經4輪股權投資，共獲得1.36億美元。
- 競爭優勢：
 - Circle在2015年11月獲得紐約州的首張BitLicens，成功進軍美國市場；2016年在獲得英國的電子貨幣許可證後，已將其比特幣交易服務範圍擴展至歐洲的多個國家。
 - Circle 允許用戶美元、英鎊和歐元收發互兌，提供便捷即時、免手續費（相互轉賬無手續費、信用卡在Circle上購買比特幣，不需要支付手續費）、匯率最優，能在競爭舞台上脫穎而出。



Coinbase

- 成立時間/地點：2012年6月成立於美國加州舊金山
- 產品與服務：線上比特幣錢包與收付平台。
- 獲投：歷經5輪股權投資，共獲得1.17億美元。
- 競爭優勢：
 - CoinBase為美國第一家取得合法執照的比特幣交易平台，擁有良好的聲譽，也是全球最大的比特幣交易市場。
- 新事業：2016年7月在比特幣兌換服務添加了以太幣，並將平台正式改名為全球數位資產交換所（GDAX）。

比特幣與區塊鏈科技獲投前十大企業個案



2

21 Inc

- 成立時間/地點：2013年5月成立於美國加州舊金山
- 產品與服務：比特幣採礦機、API交易市場、提升採礦效率的特製晶片。
- 獲投：歷經2輪股權投資，共獲得1.21億美元。
- 競爭優勢：
 - 提供價格低廉、即插即用的電腦採礦設備，讓大眾可理解與實踐採礦。
 - 研發高效採礦晶片-Asic晶片，提升運算力
 - 推出一種21 Micropayments Marketplace（小額支付市場），能夠創建API應用程式，允許買家和賣家使用比特幣進行數位商品交易。



Ripple

- 成立時間/地點：2012年成立於美國加州舊金山
- 產品與服務：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（Ripple協議），不用担心匿名方涉入交易之中，協助銀行讓跨境支付更便捷與安全。
- 獲投：歷經7輪股權投資，共獲得9,360萬美元。
- 競爭優勢：
 - 不斷增長的銀行夥伴數，該公司宣稱已建立了30多個合作試點項目，並與全球top 50銀行中的15家有合作，其中包括瑞銀與渣打，其中10家處於商業化合作階段。
 - 銀行痛點之一是大量低價值的跨境支付交易，Ripple讓銀行在國際支付時，在數秒內即可完成交易，減少33%的成本

比特幣與區塊鏈科技獲投前十大企業個案



BitFury Group

- 成立時間/地點：Bitfury於2011年在俄羅斯成立，後業務轉型並在美國華盛頓、舊金山，荷蘭阿姆斯特丹、英國倫敦以及中國香港均設立分支機構，並在冰島和格魯吉亞建立了運營資料操作中心。
- 產品與服務：最早為區塊鏈採礦硬體與晶片製造，後拓展至區塊鏈基礎資料服務和交易處理服務。
- 獲投：歷經4輪股權投資，共獲得9,000萬美元。
- 競爭優勢：
 - 比特幣開採是一個高能耗產業，電費是最大的成本，因此，高能效設備是盈利的先決條件。Bitfury擁有領先業界的ASIC晶片、數十天內即可構建超級數據中心的專業技能與實踐力。
 - 開發一系列區塊鏈技術開放平臺，並與不同的機構合作測試區塊鏈技術應用的各類場景。
 - 成功國際化拓展，特別是比特幣交易金額大的城市，均已設點服務。



Blockstream

- 成立時間/地點：2014年成立於加拿大魁北克省。
- 產品與服務：為一家擴大比特幣協議層功能的公司，主導研發側鏈（sidechains）技術的擴展機制，建構區塊鏈系統合平臺，透過雙向定錨機制，將比特幣的區塊鏈與其他不同區塊鏈系統整合，可擴展作智慧合同、小額支付等。
- 獲投：歷經3輪股權投資，共獲得7,300萬美元。
- 競爭優勢：
 - Blockstream的側鏈產品能夠複製特許區塊鏈功能性的技術，被視為區塊鏈技術的應用開發中最好的解決方案，透過側鏈能夠讓更多的人參與開發，從而發掘比特幣區塊鏈的潛力。
 - Blockstream擁有一支全明星開發團隊，包括比特幣核心開發者Gregory Maxwell、Jonathan Wilkins等。

比特幣與區塊鏈科技獲投前十大企業個案



Digital Asset Holdings

- 成立時間/地點：Digital Asset 於2014年在美國紐約市成立
- 產品與服務：定義為一家軟體提供商，利用「分布式基礎設施」，提供企業級區塊鏈服務（如：資產結算）和客戶端 API服務」。去年底公佈最新產品GSL（全局同步日誌）的新型區塊鏈技術，可結合隔離分類帳和數據執行協議。
- 獲投：歷經2輪股權投資，共獲得6,720萬美元。
- 競爭優勢：
 - 將其開放式帳本項目的代碼貢獻給Linux基金會，並獲得IBM，摩根大通等銀行投資與允諾，將進行合作開發。
 - Digital Asset公司專注金融市場，有非常清晰的命令，他們對整個豎向結構非常瞭解。



Chain

- 成立時間/地點：2014年成立於美國加州舊金山
- 產品與服務：Chain是一個區塊鏈技術公司，協助金融公司合作建立和佈局區塊鏈網絡，以轉變市場。
- 獲投：歷經3輪股權投資，共獲得4,370萬美元。
- 競爭優勢：
 - 該公司的Chain Open Standard開源平台，將其 Chain Core 軟體的開源式版本向廣大開發者公開，獲得銀行與金融服務巨頭的投資與合作機會。

比特幣與區塊鏈科技獲投前十大企業個案



Xapo

- 成立時間/地點：於2012年在美國加州帕羅奧圖，近年將總部遷移至瑞士
- 產品與服務：比特幣的安全存儲（比特幣電子錢包與保險庫）解決方案提供者
- 獲投：歷經2輪股權投資，共獲得4,000萬美元。
- 競爭優勢：
 - Xapo錢包不收費、不延遲、無地域限制，與Xapo金融卡直接綁定，發行全世界第一張比特幣金融卡。
 - Xapo在2017年1月獲得瑞士金融市場監督管理局有條件許可，加速其比特幣使用的機會。
 - 在KPMG 2016年全球金融科技百大中排名第28名，僅次於Circle(第20名)



bitFlyer

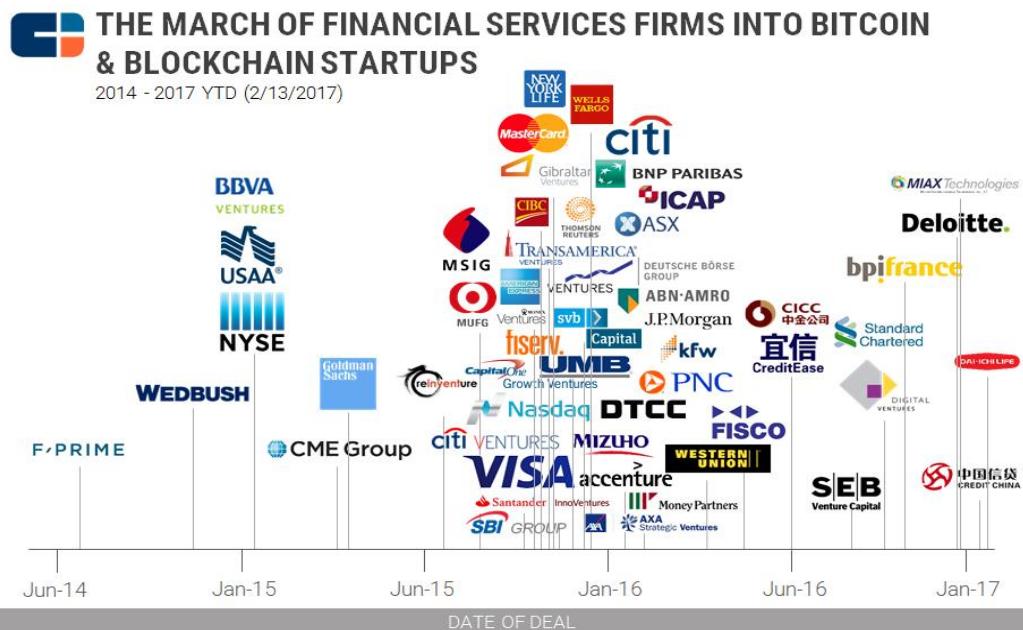
- 成立時間/地點：2014年成立於日本東京
- 產品與服務：大型比特幣交易平台
- 獲投：歷經7輪股權投資，共獲得3,611萬美元。
- 競爭優勢：
 - 日本新的金融法規預計2017年5月生效，在新的法規中比特幣被視為貨幣，有助於Bitflyer比特幣交易。
 - Bitflyer為日本領先的比特幣交易平台，利用區塊鏈技術為各行各業創建核心系統，成功的吸引了主流金融機構和銀行的投資，包括：瑞穗金融集團和三井住友金融集團等重量級投資人。

比特幣與區塊鏈科技前十大投資人 2012~2017 (YTD 1/30/17)

名次	投資人
1	<u>Digital Currency Group</u>
2	<u>Blockchain Capital</u>
3	<u>Tim Draper</u>
4	<u>Pantera Capital</u>
5	<u>RRE Ventures</u>
5	<u>Y Combinator</u>
7	<u>500 Startups</u>
8	<u>Draper Associates</u>
9	<u>Fenbushi Capital</u>
10	<u>Andreessen Horowitz</u>

資料來源：CB Insights (2017).

- ◆ 值得關注，**金融服務業**在過去3年逐步加大對比特幣和區塊鏈新創企業的策略性投資，投資高峰出現在2015第三季到2016年第四季。
- ◆ 包括：
 - 保險提供業者 (TransAmerica, MSIG, New York Life)
 - Payments firms (Visa, MasterCard, AmEx)
 - Banks (Citi, Santander, CIBC)



資料來源：CB Insights (2017).



區塊鏈領域之27種應用與個案分析

Source: 1.CB Insights, 2017/2/7, "Banking Is Only The Start: 27 Big Industries Where Blockchain Could Be Used."

2.台經院整理。

區塊鏈技術要解決的是「信任」問題，提高整個系統的運作效率。

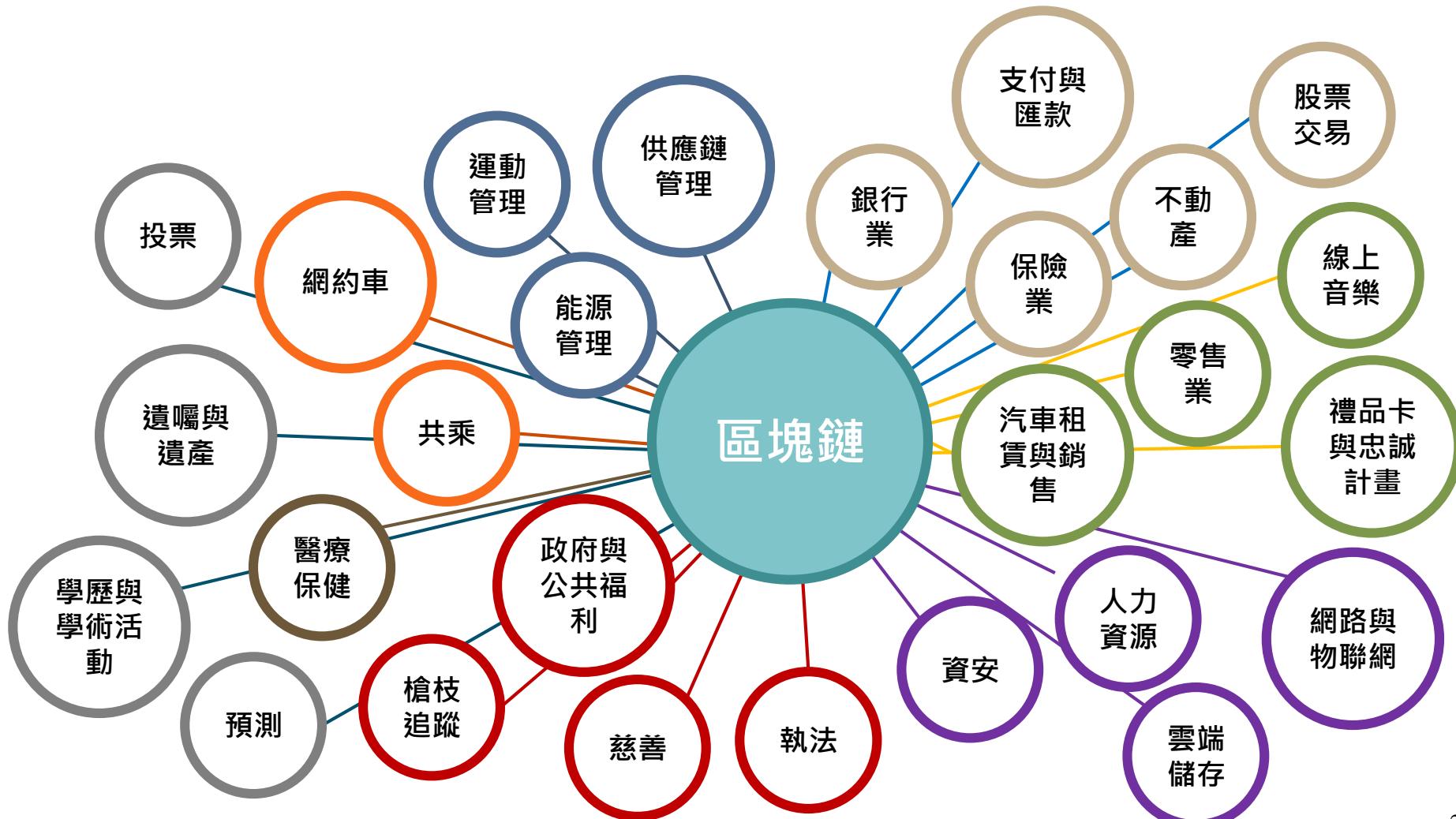
區塊鏈1.0-數位貨幣



區塊鏈2.0-金融領域應用



區塊鏈3.0-非金融領域應用

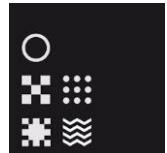




銀行業

- 銀行本質上所扮演的角色是安全的價值儲存與移轉的中心，同樣地，具備安全與防篡改的數位帳本技術，區塊鏈可擔任相同的角色，而瑞士瑞銀集團與英國巴克萊銀行正在試驗其加速後台功能與結算方式的可行性。金融服務巨頭不但積極投資區塊鏈新創公司，R3 CEV也在50家銀行加盟下，為金融行業開發區塊鏈解決方案。
- 新創團隊Thought Machine開發Vault OS，使用私有鏈技術，提供安全的端到端金融系統。

Thought Machine



保險業

- AirBnB、途家、Wimdu等公司提供住宅短租媒合服務，使臨時性資產交換成為可能，但問題是幾乎不可能在這些平台上對這些資產保險。Deloitte、支付業者LemonWay與新創企業Stratumn合作發布LenderBot區塊鏈解決方案，為共享經濟提供微型保險。還在poc階段的LenderBot允許人們透過Facebook Messenger註冊客製化微型保險，將比特幣區塊鏈建立為貸款合約中的可信第三方，目標是替個人間交換的高價值資產進行保險，以區塊鏈確保保證的不變性，並提供更高的透明度。

Deloitte.



LEMONWAY





股票交易

- 為能簡化股票交易過程，區塊鏈解決方案可以更有效地實現自動化與安全的交易過程。Overstock的子公司TØ.com期望使用區塊鏈技術實現線上股票交易。根據Wired的報導，Overstock已使用區塊鏈技術發行私人債券，而SEC更批准TØ.com發行公債。
- 區塊鏈新創企業Chain則正與納斯達克合作，通過區塊鏈促進企業股票交易。



不動產

- 不動產交易存在痛點，如交易前後缺乏透明資訊、大量的文書工作、潛在的欺詐風險與公共記錄中的錯誤。基於此，區塊鏈提供了減少對紙本記錄的依賴，並加速交易流程的解決方案。不動產區塊鏈可用於記錄、追蹤土地產權、財產契據與留置權的移轉，並有助於確保文件準確與可驗證性。
- Ubitquity為金融機構、所有權與抵押公司提供平台，用於文件確保，同時提高交易透明度與降低成本。



支付與匯款

- WEF指出去中心化的支付技術(如比特幣)可為過去100年來幾乎未有改變的貨幣移轉模式，帶來結構性的變化。區塊鏈可建構一個更直接的支付流程，去除中介，連接付款人與收款人、境外與境內，提供極低的費用與幾乎即時的移轉速度。
- Abra利用區塊鏈技術，客戶可透過行動裝置，轉換實體貨幣至數位貨幣，並提供簡便的存、提、匯款等金流服務。





汽車租賃與銷售

- Visa與DocuSign在2016年底發布一個概念驗證(proof-of-concept)的合作計畫，應用區塊鏈技術簡化汽車租賃，成為「點擊、簽章、駕駛」的簡易流程。客戶選擇欲承租的汽車，紀錄於區塊鏈的公共帳本上。之後在駕駛座上簽署租賃協議與保單，並同步更新區塊鏈訊息。同樣的模式亦可應用於汽車銷售與汽車登記上。



線上音樂

- 許多音樂家正尋求區塊鏈解決方案，使線上音樂共享更加公平，透過更直接的支付方式與使用智慧合約自動解決音樂授權問題。
- PeerTracks開發音樂串流平台，利用區塊鏈技術讓用戶支付價金並下載音樂，亦創造藝術家和客戶之間更多的接觸
- Ujo Music期望解決串流音樂與創作者的問題，並利用智慧合約自動優化歌曲編目模式。
- 由葛萊美獲獎者Imogen Heap創立的Mycelia，將歌曲嵌入智慧合約，讓音樂家可直接向大眾銷售，無需透過唱片公司





禮品卡與忠誠計畫

- 區塊鏈應可令禮品卡與忠誠計劃系統更加便宜與安全，減少中間人處理發卡與銷售業務，過程將更有效率，且具成本效益。同樣地，透過區塊鏈的加密驗證功能，可提高欺詐預防，並降低帳戶盜用的風險。
- Gyft是一個用於禮品卡購買、發送與兌換的平台，其與區塊鏈基礎設施開發商Chain合作，為數千家小型企業提供禮品卡服務，Gyft Block。



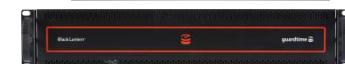
零售業

- 目前零售系統的信任基礎建立在中介的交易場所上，不論實體或虛擬，如Amazon。
- OpenBazaar正在開發的區塊鏈應用，可用於串接買家與賣家，去除中間人與相關的費用。對系統的信任將來自區塊鏈交換和智慧合約的安全性。該公司至2016年底完成兩輪募資，達400萬美元，投資者包含了Andreessen Horowitz與Union Square Ventures



資安

- 區塊鏈的帳本雖然是公開的，但數據通信(更新)需透過加密技術驗證與發送。確保數據源的正確，且任何內容無法被攔截竊改。消除客戶對中介的需求即是減少資安風險的一種簡單方法，廣泛利用的區塊鏈技術將使駭客攻擊機率下降。
- 愛沙尼亞資安公司Guardtime專注於應用區塊鏈技術的工業級網路安全方案





人力資源

- 應徵員工時所做的背景調查與驗證學經歷是一項耗時的工作，應用區塊鏈技術則可排除這些紀錄偽造的可能性，簡化審查過程。
- Recruit Technologies與scribe.io合作開發支援區塊鏈技術的加密證書，建立一個更加透明且容易驗證的就業歷程系統。



雲端儲存

- 企業通常在集中式的伺服器上提供雲端儲存服務，保護客戶的數據，而這也意味著風險增加。區塊鏈的分散式特性應用於雲端儲存方案，將可降低導致系統性損壞與數據遺失的風險。
- Storj為beta測試版的區塊鏈雲端儲存網路，以提高安全性，並降低資訊儲存成本。用戶亦可租出未使用的空間，打造雲端儲存市場。



網路與物聯網

- IBM與三星正在研究如何使用區塊鏈技術形成物聯網設備分散式網路主幹，ADEPT。ADEPT為自主的分散式點對點遙測技術，區塊鏈將用於大量設備間的公共帳本。CoinDesk指出，ADEPT不再需要中央控制系統協調設備間的通訊與進行設備識別，設備將能自主溝通，管理軟件更新，偵錯誤或進行能源管理。
- 另外，新創企業Filament也在開發將區塊鏈技術應用於物聯網平台，建立分散式網路，用於傳感器之間的溝通，2015年獲得Verizon與Samsung Ventures的A輪投資500萬美元，2017年2月更獲投948萬美元。





供應鏈管理

- 區塊鏈技術最普遍適用之處在於能夠更安全與透明地監控交易，供應鏈基本上是由連串的交易節點構成，連接上中下游的產品直到最終銷售。區塊鏈則可將供應鏈交易記錄在分散式帳本中，減少時間拖遲、成本增加與人為錯誤。
- 新創公司Provenance構建了原料與產品的可追溯性系統；Fluent與Skuchain則基於區塊鏈打造了B2B供應鏈金融平台。



Fluent

skuchain



運動管理

- 運動員投資集中於體育管理機構，但區塊鏈技術可使投資過程分散化，透過群眾的參與，資助潛力運動員，並取得投資回報。
- Jetcoin Institute提出虛擬加密貨幣(Jetcoins)的概念，球迷可投資於喜歡的運動選手，並有機會獲得選手未來收入的一部分作為回饋，或是取得VIP活動與座位升級等福利。Jetcoin正與意大利維羅納足球俱樂部進行合作嘗試。

jetcoin



能源管理

- 能源管理是另一個高度集中的行業，能源移轉須透過一個可信的能源機構，如美國的Duke Energy、英國的National Grid，或電力轉售商。
- Transactive Grid是由能源管理公司LO3 Energy與以太坊開發公司ConsenSys所合資的企業，提供以太坊區塊鏈技術，使客戶能夠在分散式能源發電計劃中有效地生成、購買和銷售能源。



LO3 ENERGY



TRANSACTIVEGRID



共乘

- Uber作為車輛調度中心，使用演算法控制車隊並收取的費用，商業模式與區塊鏈概念相反。根據Bloomberg，以色列新創公司La'Zooz並非使用集中式網路叫車模式，用戶透過La'Zooz找到類似旅行路線的其他人，並以虛擬貨幣(如比特幣)交易的方式乘坐，而這些貨幣可用於未來的共乘。用戶則可透過讓應用程式跟蹤位置以賺取虛擬貨幣。



網約車

- 叫車服務公司如Uber與Lyft往往必須處理監管與勞動條款的問題，而區塊鏈解決方案可能為乘客和司機間提供新的選擇。
- 位於德州奧斯丁的公司Arcade City建立一區塊鏈平台，允許司機建立自己的金融交易形式，每位司機都可提供個人的交通服務。



政府與公共福利

- 區塊鏈可應用於社會援助與福利的分配，簡化並確保公共治理的落實。
- GovCoin Systems Limited專注於英國政府福利分配的區塊鏈技術平臺開發，以期減少每年因為社會福利與援助分配中所產生高達1兆美元的摩擦與欺詐成本。





槍枝追蹤

- 難以竄改的區塊鏈可連結公共記錄，可防止不適合的申請人取得槍支。此外，結合醫療記錄與槍支所有權，可在槍枝擁有者與暴力事件連結時，提醒當地執法單位。
- 新創公司Blocksafe開發一區塊鏈系統，可用於追蹤用戶的槍支位置以及解僱紀錄。



慈善

- 慈善捐助常年來的問題在於對組織的質疑，以及對捐助資源的利用。區塊鏈可用於準確追蹤捐款進行的流程、到達哪些單位、用在那些地方。
- BitGive Foundation使用區塊鏈安全且透明的分佈式帳本，讓捐贈者看到預期的捐助對象獲得援助，並且能降低資金轉移與慈善組織經營的成本。



執法

- 在執法調查中，保持證據的完整性至關重要，而區塊鏈的分散式記錄可為證據處理過程提供更多的安全保障。
- Chronicled募集近500萬美元的資金用於開發具有近端通訊晶片、可封存、防篡改的儲存裝置，透過區塊鏈系統驗證，可用於證據確保與儲存應用。
- Elliptic則是募資超過700萬美元的新創公司，其正開發持續掃描比特幣註冊管理機構，並標記可疑交易記錄，以利執法人員的調查。



ELLIPTIC



醫療保健

- 醫療機構的痛點在於無法安全地跨平台分享數據，而更好的數據協作意味著更高的確診機率、有效治療可能性，以及在醫療保健系統中提供更具醫療成本效益的能力。區塊鏈技術允許醫療保健價值鏈中的醫院、付款方與其他團體，在不損害數據安全性和完整性下，共享資源。
- 新創企業Gem的**Gem Health Network**是一個具有多重簽章與多要素認證技術的以太坊區塊鏈平台，提供安全的統一數據基礎設施。Tierion則同樣以區塊鏈技術，在醫療保健領域建立數據儲存與驗證平台。Gem、Tierion與Philips Healthcare合作，於飛利浦區塊鏈實驗室進行平台開發。

PHILIPS
Healthcare



預測

- 區塊鏈技術將撼動研究、分析、諮詢與預測領域。Augur為一開源的分散式市場預測平台，該平台對用戶而言如一般的博彩交易平台，但從下注到彩金交付的整個過程將透過分散式帳本紀錄。下注的標的不僅限於運動與股市，其他主題如選舉、自然災害等亦可。此概念如同未來事件交易所，運用群眾智慧，打造「預測市場」。





學歷與學術活動

- Holberton School是加州的軟體技能計劃，其將利用區塊鏈技術認證學術證書，確保未通過課程的學生無法冒用認證，保障通過認證的學生。若有更多學校採用透明的學術證書，成績單與文憑系統，可更容易地降低學術欺詐，更可避免人工與紙本文件審查所耗費的時間與成本。



投票

- 選舉需要選民身份認證，保存投票記錄，以及信任的計數以確定當選者。區塊鏈可作為投票、紀錄與計票的媒介，消弭舞弊、遺失記錄的問題。在區塊鏈內的投票交易，每位選民可自行計票，且驗證確保投票未被更改或刪除。
- Follow My Vote在Kickstarter發起募資，目標在於提供端到端可驗證的線上投票系統



遺囑與遺產

- 遺囑屬於特定類型的合約，且適用於區塊鏈智慧合約的解決方案。
- Blockchain Technologies Corp的法律顧問Eric Dixon指出大多數的遺囑訴訟案件都涉及對其真實性的挑戰。區塊鏈的應用將有利於識別事實訊息，鏈接及驗證與遺產相關的文檔，確保更可信的資料庫。

肆

國內比特幣與區塊鏈領域發展概況

肆、國內比特幣與區塊鏈領域發展概況

政府
學術界
研究機構



衛福部將利用「區塊鏈」(blockchain)的技術，加入食品安全追蹤溯源系統。



工研院與微軟合作，開發運動區塊鏈實作－「BraveLog」。



工研院發起臺灣的區塊鏈產業聯盟
臺大成了金融科技暨區塊鏈中心，臺大資工系副教授廖世偉擔任中心主任，研發出臺灣第一套自行開發的區塊鏈協議Gcoin。

銀行/
金融服務

1. 中國信託宣布加入R3，並成立50人規模的跨事業群區塊鏈實驗室。
2. 富邦宣布要區塊鏈金融聯盟，並支持成立臺灣第一家商用企業區塊鏈公司AMIS（帳聯網）。區塊鏈技術社群平台基本成員包括AMIS帳聯網公司、微軟、富邦金控、工研院等，以聯盟的形態合力打造全球首個運動區塊鏈實作－「BraveLog」，主攻運動賽事的記錄及建立選手參賽履歷。
3. 富邦、國泰人壽、玉山：透過區塊鏈平台，催生「帳聯平台」，串接電子病例、建構支付場景與優化理賠作業。
4. 財金公司：集結臺灣45家銀行，組成「金融區塊鏈技術研究與應用委員會」。
5. 2017年2月24日臺灣金融科技協會成立

新創企業

數位貨幣

比特幣錢包與交易中心



MaiCoin



萊特幣礦機



區塊鏈應用

BITMARK

區塊鏈技術的電子
資產註冊系統



數位資產價
值傳遞



區塊鏈聲波
支付

DTCO

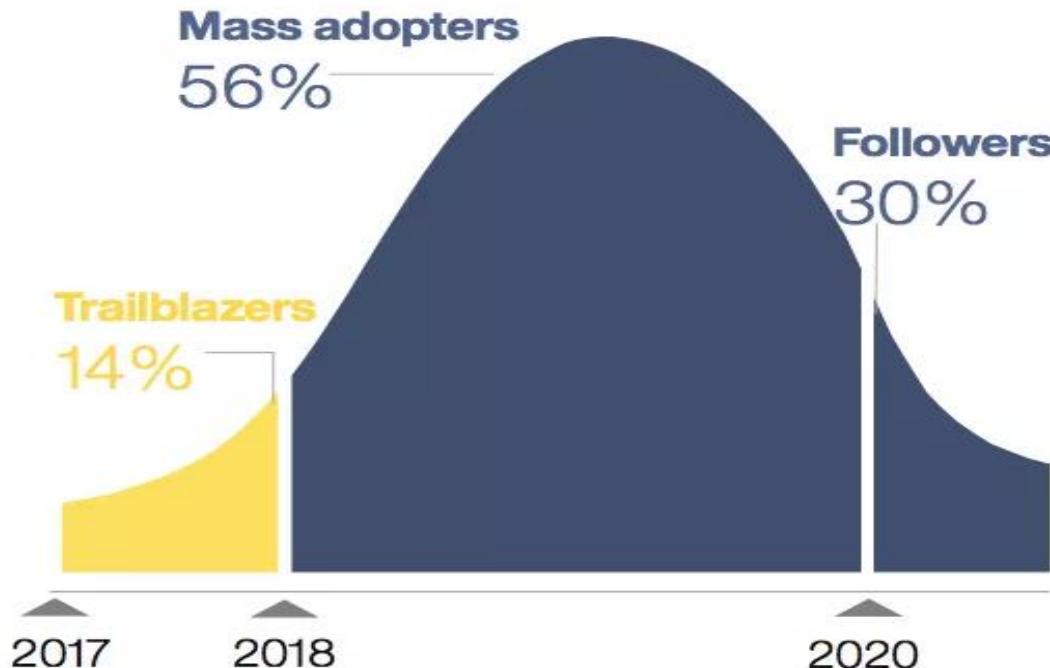
比特幣安全電
子錢包與區塊
鏈API

伍

比特幣與區塊鏈的展望與挑戰

一、大型銀行或金融機構將成為探索區塊鏈技術應用的先行者

- IBM最近調查全球200家的金融市場機構，指出**2017年會有14%的金融市場機構和15%的銀行會採用全面性、區塊鏈技術商用解決方案**，65%的銀行在三年內會採用區塊鏈技術。
- 對銀行來說，節省交易的時間、金錢、降低風險是三大使用區塊鏈技術應用的主要好處。



Source: IBM

二、大型銀行或金融機構區塊鏈技術的佈局策略



Source: EVRY (2015); INNOVALUE (2015)

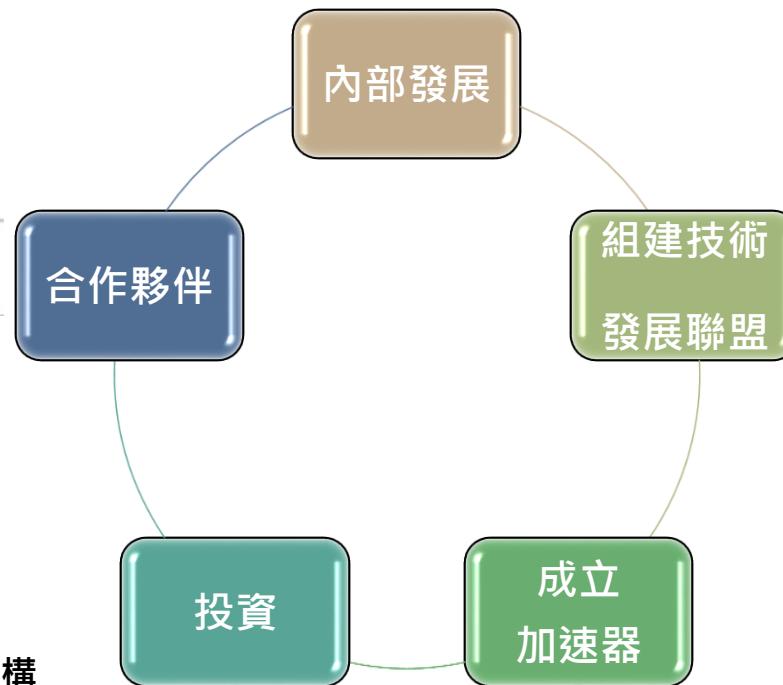


Source: EVRY (2015); INNOVALUE (2015)

投資區塊鏈新創企業的金融機構



Source: LTP (2016)



Source: EVRY (2015); INNOVALUE (2015)

區塊鏈發展聯盟-R3 CEV
2015.12.17



Source: r3cev.com(2015)

企業以太坊聯盟-Enterprise Ethereum Alliance
2017.02.28



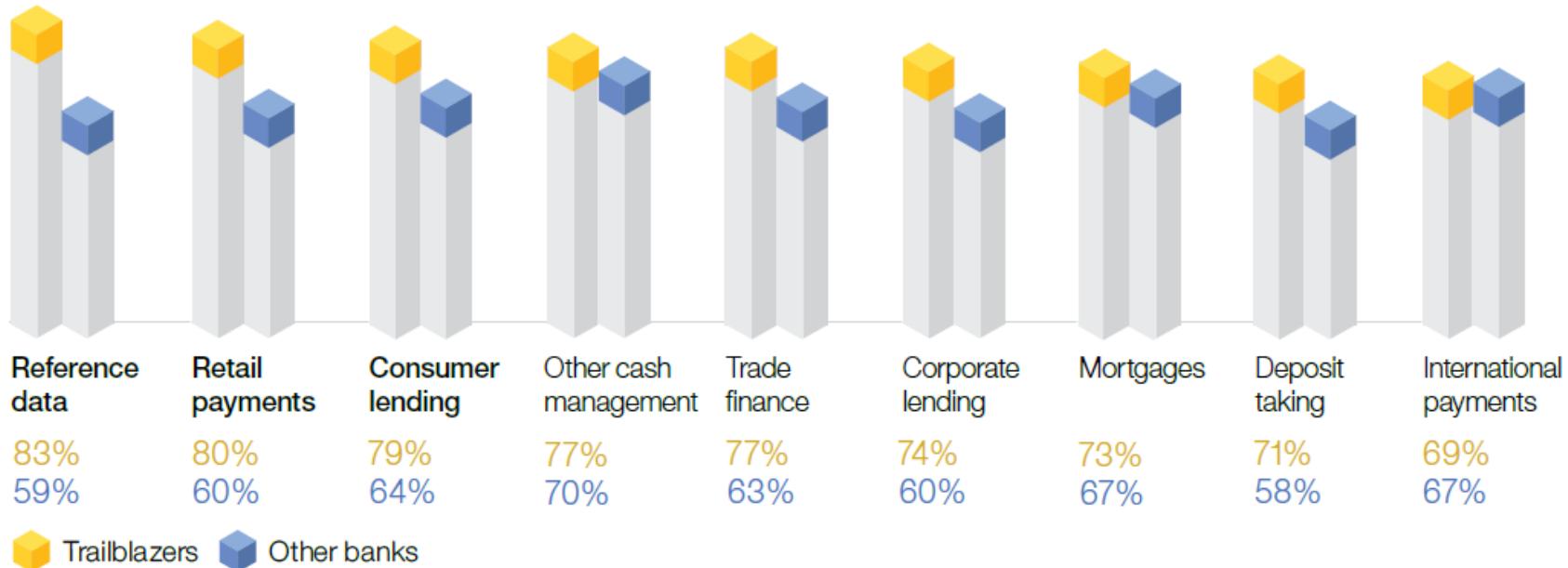
Source: winbuzzer (2016)



Source: EVRY (2015); INNOVALUE (2015)

三、受益於區塊鏈技術落實的行業與對象

- 根據IBM的調查，**區塊鏈技術的落實對於參考資料（Reference data）、零售支付（Retail payments）和消費者貸款（Consumer lending）最有利**
- 50%的中小企業缺乏融資管道，信用缺口估計達2兆美元，區塊鏈技術（智慧合約）能夠幫助這些企業**提高信用程度，並降低徵信難度**。



Source: IBM Institute for Business Value, "Leading the pack in blockchain banking—*Trailblazers set the pace.*"

四、區塊鏈的未來展望與挑戰

1

區塊鏈的目的是要解決的是系統中的「**信任**」問題。反之，若「**痛點不痛**」，如系統中「不存在」信任問題或解決信任問題的成本遠高於延續舊系統，區塊鏈技術難以進入商業化階段

2

技術難題：平台很多，但僅有比特幣及以太坊應用略具規模。區塊鏈技術尚未成熟，目前多屬概念與基礎技術開發階段，未達完整解決方案，距離行業標準化甚遠，如跨平台的基礎協議、針對高頻或超大容量的數據節點技術之適用

3

安全性：「**安全不是絕對，而是相對的**」。區塊鏈技術可保證每筆支付都是真實的，全網驗證機制拉高駭客攻擊的難度。然，算力過於集中的風險，以及過去因「**人為因素**」導致數起虛擬貨幣遭竊事件，均是待解的安全性隱憂

4

市場需求：目前區塊鏈技術仍缺乏「**剛性需求**」。從「集中式」帳本轉換為「分散式」帳本需要更具說服力的情境，哪些應用領域是「**Essential**」，而不是「**Nice to have**」？是否存在殺手級應用？商業化的解決方案與獲利模式為何？

5

專業缺口：企業需要創建測試與學習結構，以實際操作方式導入區塊鏈方案。但不論是專業外包、收購或自行開發，區塊鏈「+」金融、保險、資安……等，核心在於「**IT**」專業與「**行業**」專業的結合，從新的平台商業模式、流程與產品中，帶出更大的數位轉型價值

4

監管與法規：點對點的分散式系統需要全新的監理技術與法規環境進行治理，增強資訊安全與確保經濟效益。如因區塊鏈技術產生金融與數據服務的「模糊地帶」，監管機構該因應去中心化數據的機制為何？如何規範資訊透明度？身分管理與共識系統的法規調適機制？



簡報結束 敬請指教