Introduction to Blockchain
快速搞懂區塊鏈

2018-07-30

@juinc davidjuin0519@gmail.com

Taipei Ethereum Meetup

Outline 大綱

- Blockchain in One Sentence 一句話解釋區塊鏈
- Short History of Blockchain 區塊鏈簡史
- Technology 技術
- Blockchain Ecosystem 區塊鏈生態系統
- Applications 應用
- Challenges 挑戰
- Conclusion 總結

Blockchain in One Sentence (1)
一句話解釋區塊鏈 (1)

- Blockchain is a technology that decentralizes trust via consensus algorithm.

  區塊鏈是一種透過共識演算法實現信任去中心化的技術

Blockchain in One Sentence (2)
一句話解釋區塊鏈 (2)

- Blockchain is NOT just cryptocurrency, as Internet is not just Website.

  區塊鏈不只是密碼貨幣，正如同網際網路不只是網站

- Blockchain is NOT a bubble. Blockchain is a technology and technology does not bubble.

  區塊鏈不是泡沫。區塊鏈是一種技術，而技術不會泡沫化

- Some cryptocurrencies might bubble but more and more ideas will emerge.

  某些密碼貨幣可能會泡沫化，但會有愈來愈多新想法冒出來

Blockchain in One Sentence (3)
一句話解釋區塊鏈 (3)

- Bitcoin is the first cryptocurrency that utilizes blockchain technology.

  比特幣是第一個使用區塊鏈技術的密碼貨幣

- Bitcoin has one simple function: it can only be used as payment.

  比特幣的功能很簡單：它只具有支付功能

Blockchain in One Sentence (4)
一句話解釋區塊鏈 (4)

- Ethereum is the first distributed state machine that utilizes blockchain technology.

  以太坊是第一個使用區塊鏈技術的分散式狀態機

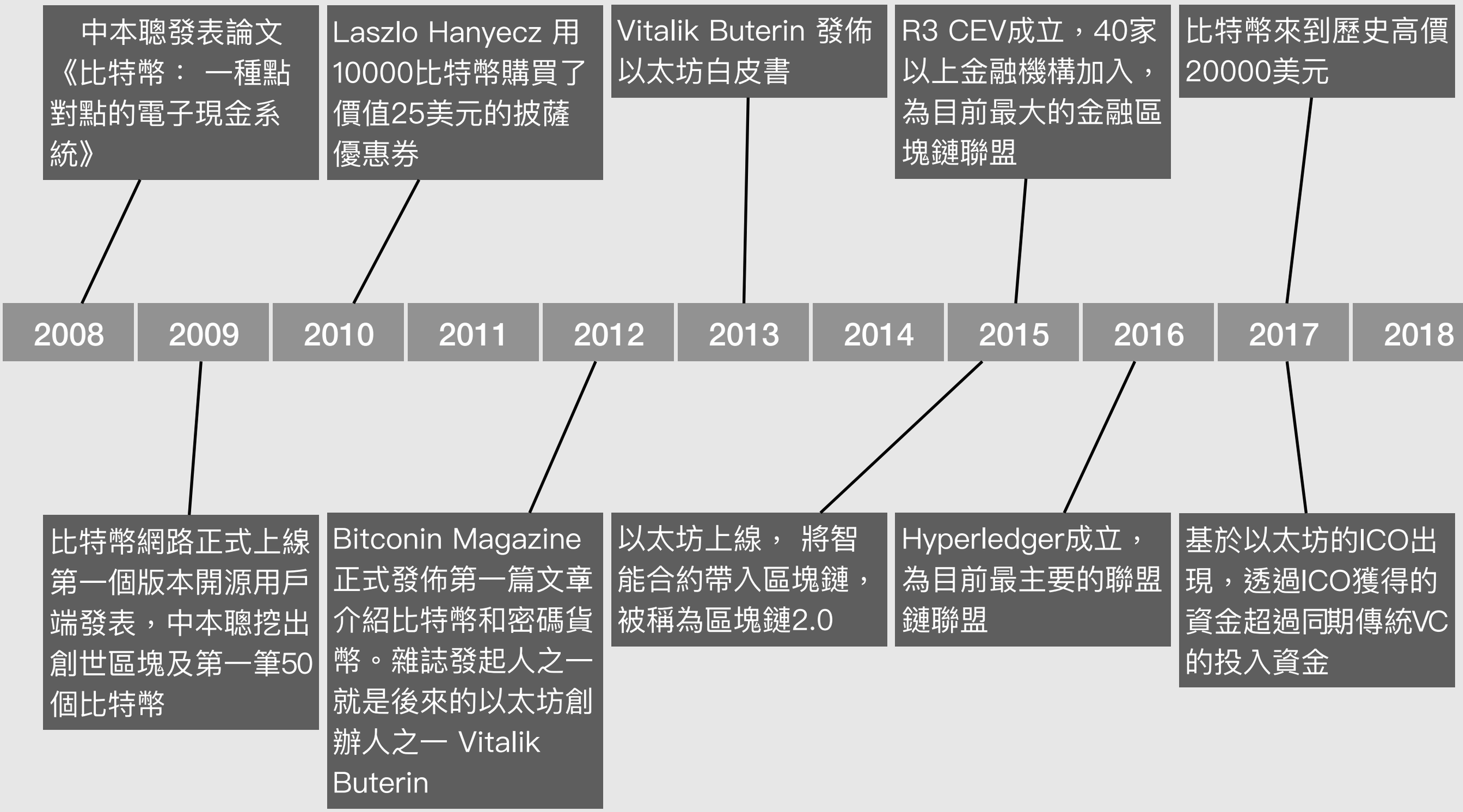
- Ethereum has more functions than Bitcoin: it can execute smart contracts.

  以太坊有較多的功能：它能夠執行智能合約

- Ethereum is a platform that runs various decentralized applications (DApp), just like the operating system in the smart phone.

  以太坊是一個能運行各種不同去中心化應用程式的平台，就像智慧型手機的作業系統一樣

Short History of Blockchain
區塊鏈簡史



Source: 台灣經濟研究院

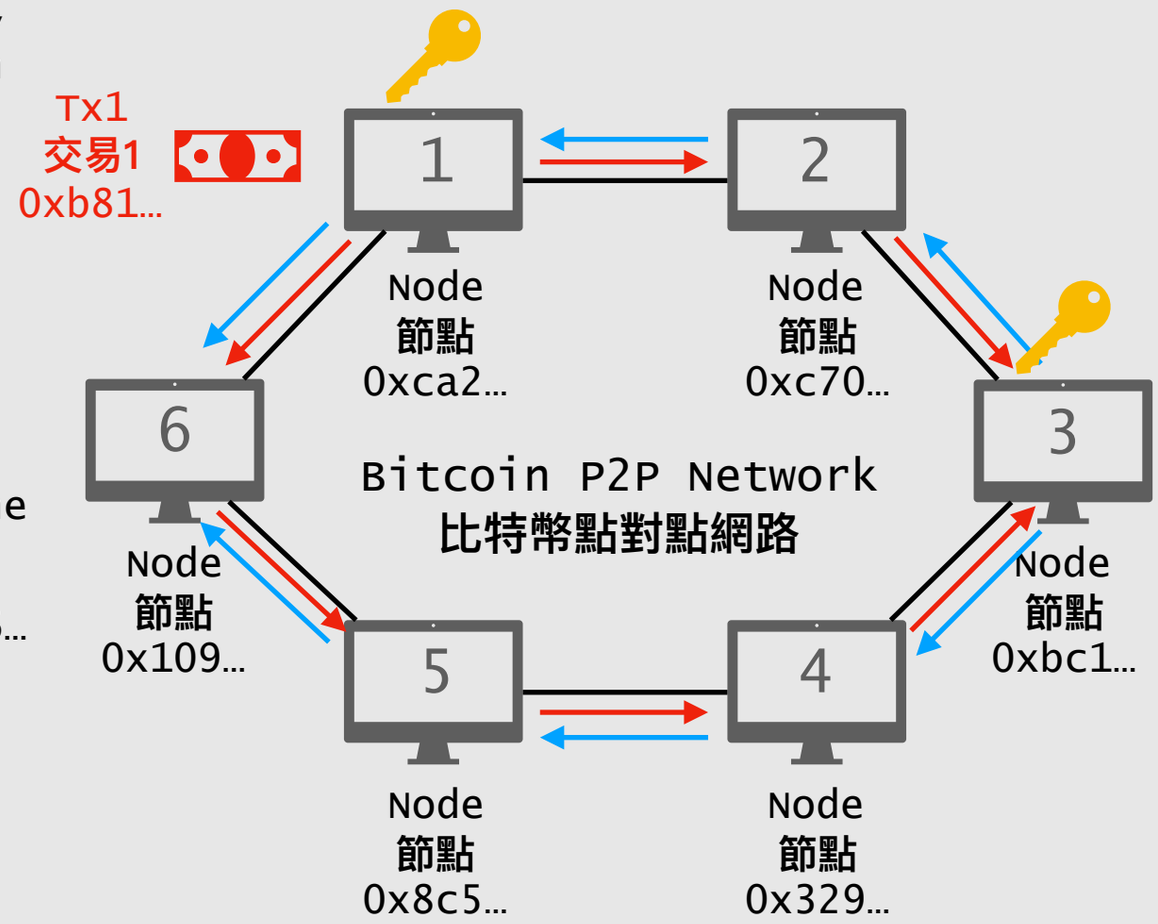
Technology (1)
技術 (1)

1.
Each node has a private key and each private key has an corresponding address
Ex: 0xa89…

每個節點都有一個私鑰，而每個私鑰都對應一個地址
例如：0xa89...

2.
Each transaction records the value transferred from one address to another
Ex: 0x123… pays 10 to 0x456…

每個交易記錄了從某個地址到另一個地址的價值傳遞
例如：
0x123... 支付 10 給 0x456...



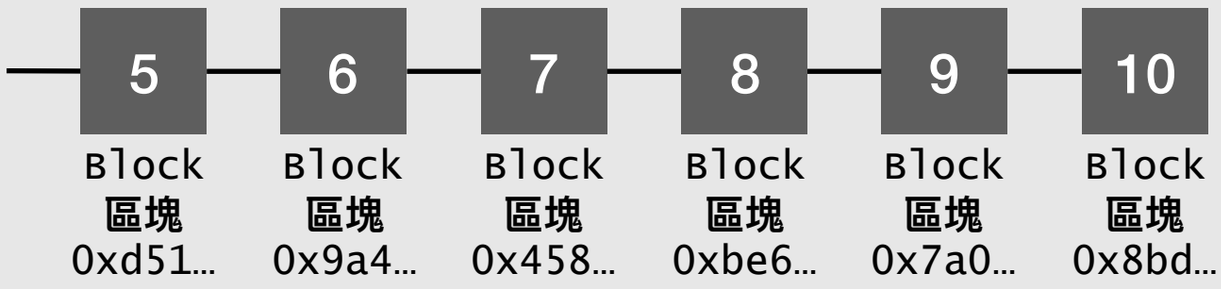
3.
Transactions are signed by the node that emits it by using private key and the digital signature becomes part of the transaction

交易會被發出該交易的節點用其私鑰簽署，數位簽章會成為交易資料的一部分

Tx2
交易2
0xc13…

4.
Signed transactions are broadcasted to every node in the network

簽署過的交易會被廣播至網路中的每一個節點

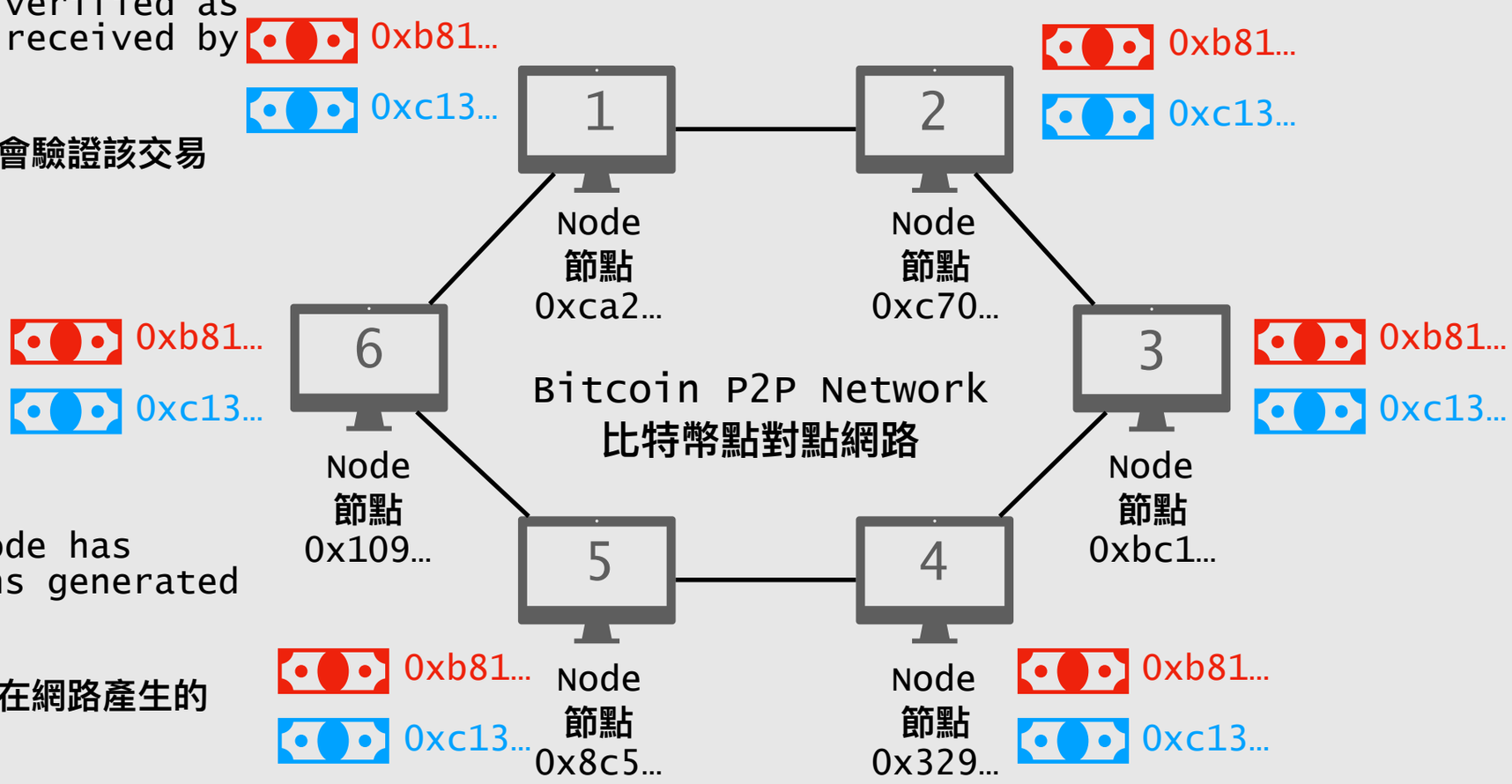


Technology (2)
技術 (2)

5.

Transactions are verified as long as they are received by each node

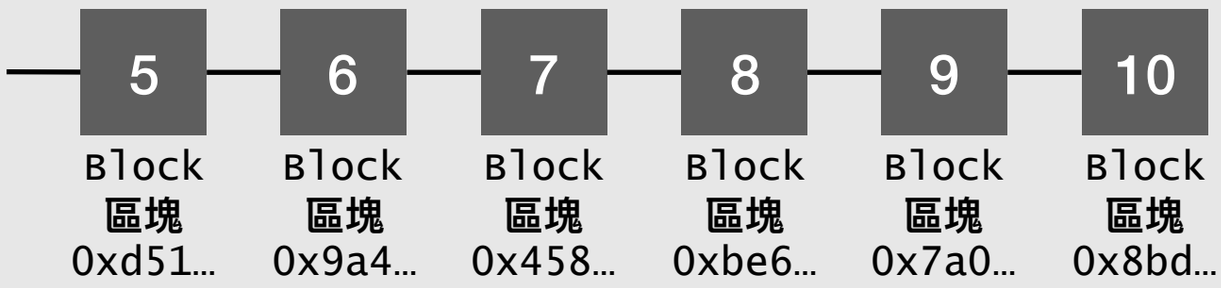
一旦節點接收到交易便會驗證該交易是否合法



6.

Ideally, every node has every transactions generated on the network

理想上每個節點會取得在網路產生的所有交易



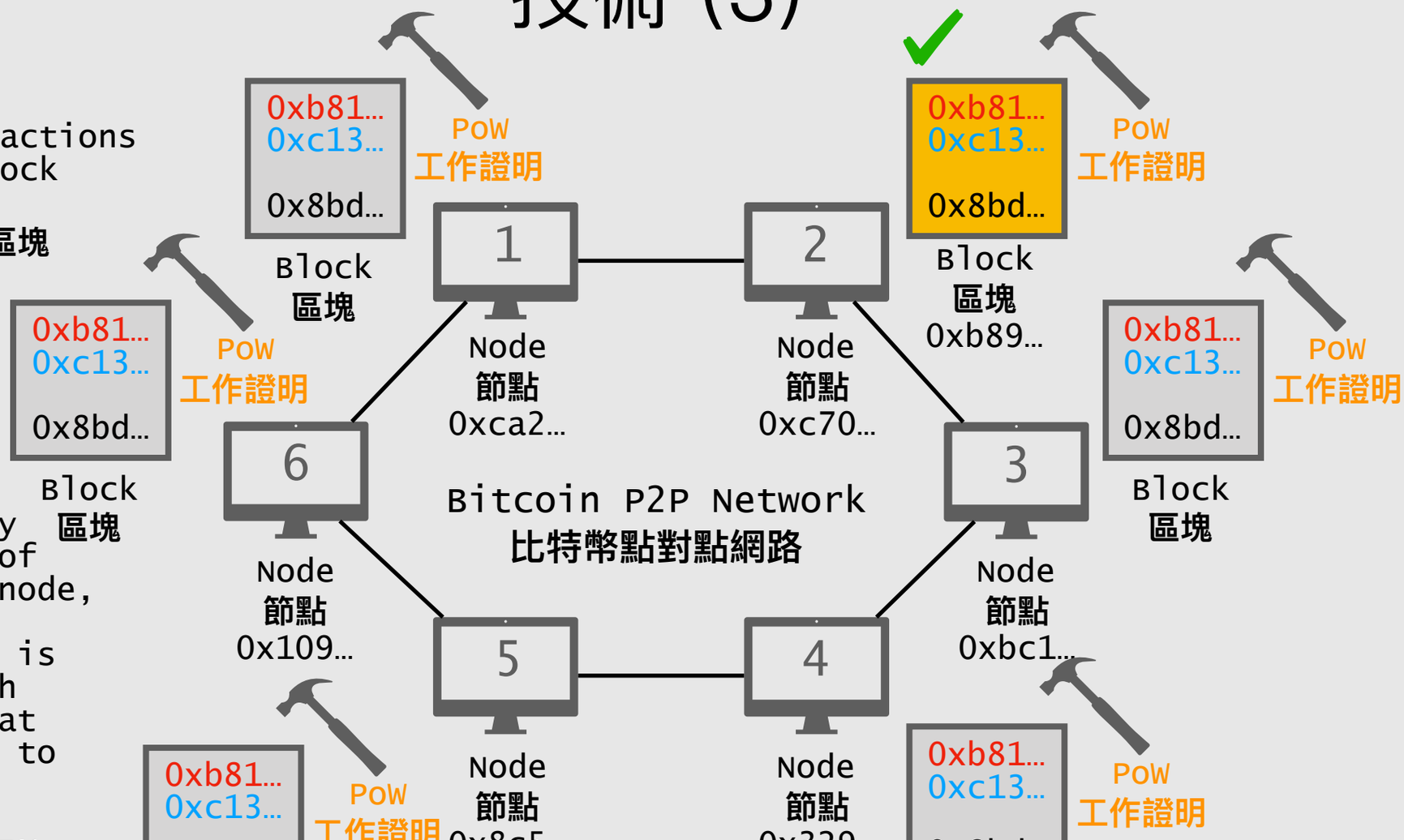
Technology (3)
技術 (3)

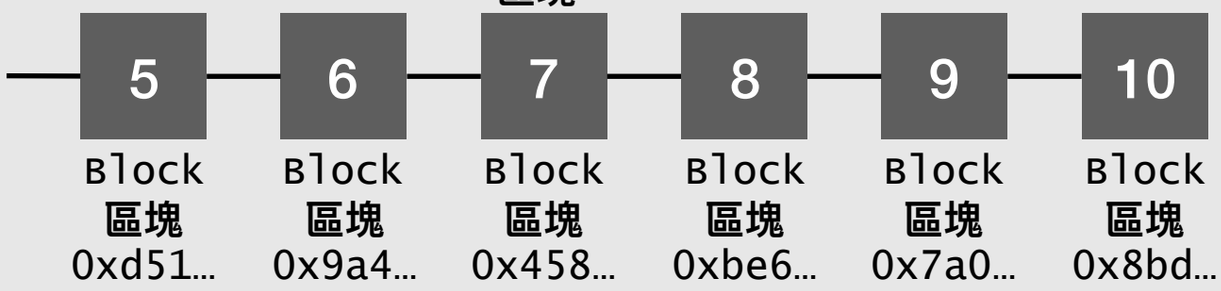
7.
In each node, transactions are wrapped in a block

節點會把交易會被打包成區塊

8.
Since there are many different versions of block made by each node, a mechanism called proof-of-work (PoW) is used to choose which version of block that every node is going to accept

由於每個節點都有各自的區塊，因此一個稱為工作證明的機制被用來決定哪一個區塊將被所有節點接受



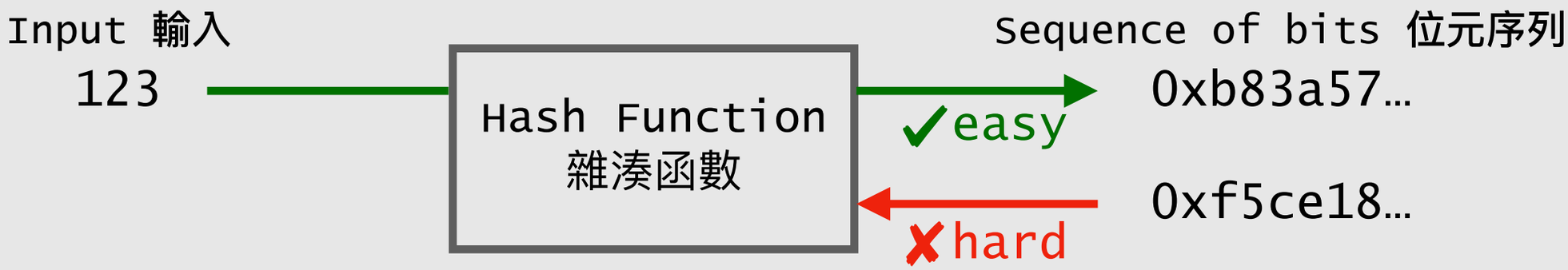


9.
If the block is successful in PoW then it is a valid block. A valid block has a blockhash
Ex: 0xb89...

若區塊成功通過工作證明，則該區塊為合法。合法區塊會有區塊雜湊值
例如：0xb89...

Technology (4)
技術 (4)

Hash Function 雜湊函數



- Hash function maps an input to a certain sequence of bits.

  雜湊函數會將輸入映射到一組特定的位元序列

- It is infeasible to map the sequence back to the input.

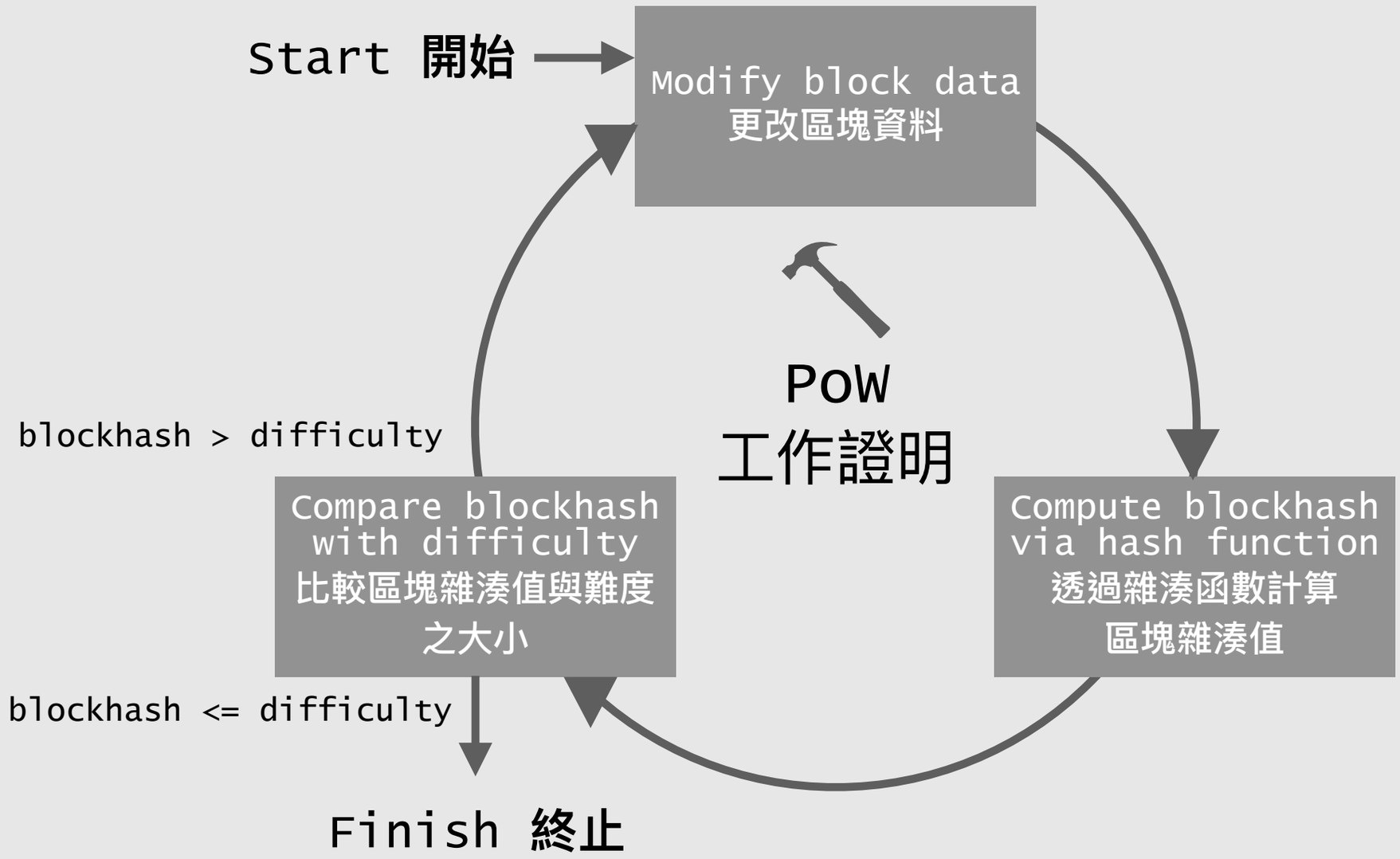
  幾乎不可能由序列映射回輸入

- Hash function is useful in producing message digest.

  雜湊函數能用來產生訊息摘要

Technology (4)
技術 (4)

Proof of Work 工作證明



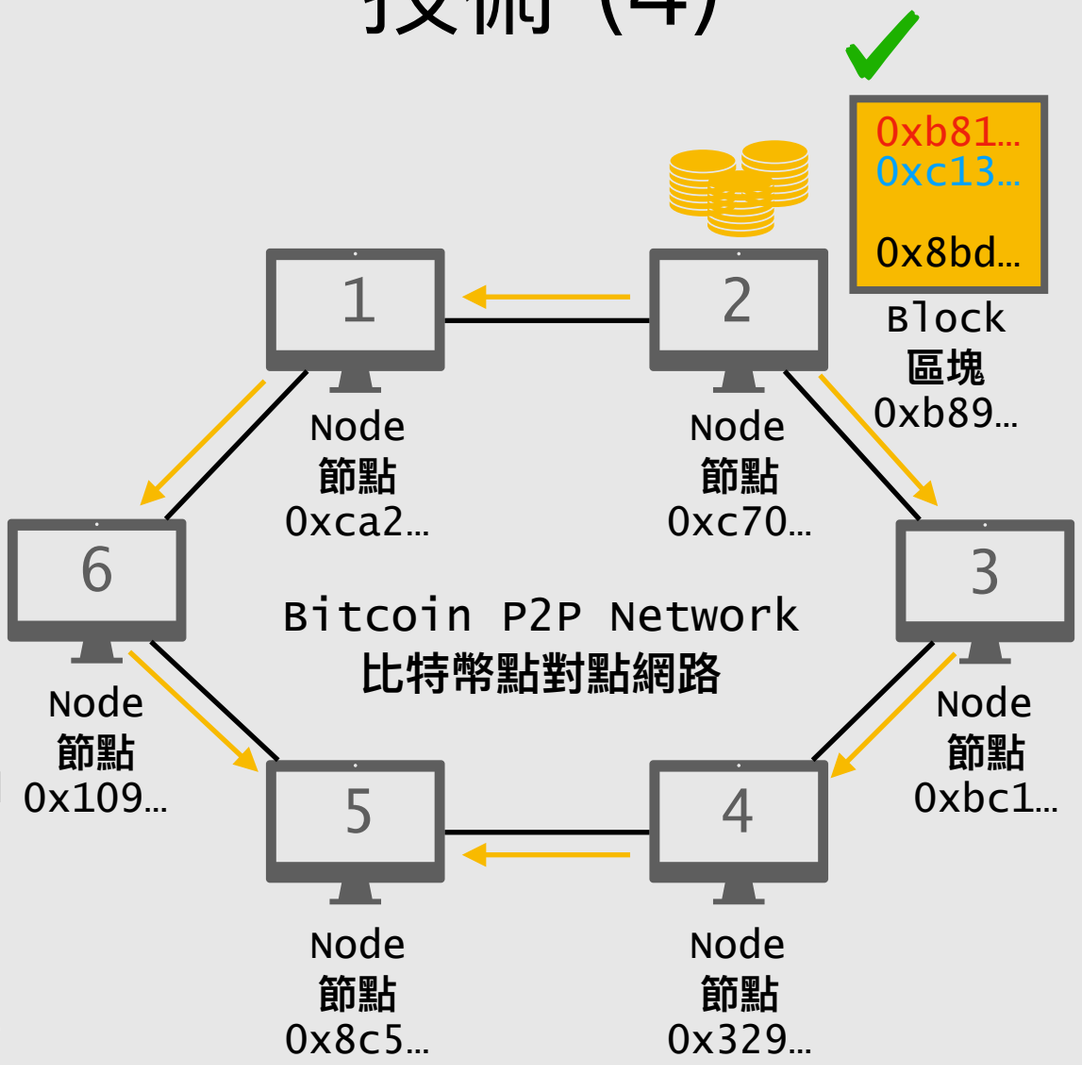
Technology (4)
技術 (4)

10.
Each block includes the blockhash of the previous block

每個區塊都會包含前一個區塊的雜湊值

11.
The valid block is broadcasted to every node in the network and is appended to the chain of older blocks to form a new blockchain after validation.

合法區塊會被廣播至網路中的每一個節點並且於驗證後會被增添至舊的區塊上，形成新的區塊鏈

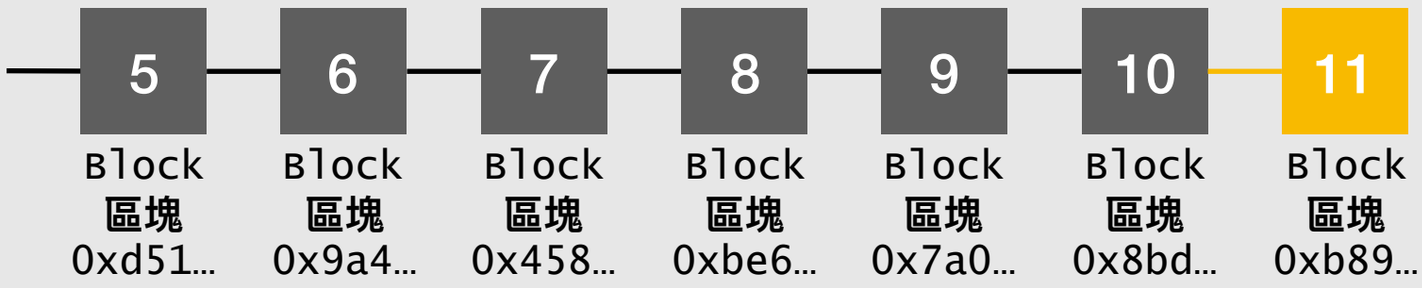


12.
Every node maintains the same version blockchain and transaction set

每個節點皆維護同一個版本的區塊鏈及交易資料

13.
The node which finds the valid block is rewarded

找出合法區塊的節點會被獎勵



Technology (5)
技術 (5)

- The transaction only gets processed by one single bank in the current banking system.

  在現行的銀行系統中，交易只會被單一銀行處理

- Banking system is centralized and it provides authority but has the risk of corruption and hacking.

  銀行系統是中心化的，它提供了權威性但也有腐敗與被駭的風險

- Decentralized trust makes centralized system that provides authority unnecessary.

  去中心化的信任使提供權威性的中心化系統不再是必要的

Technology (6)
技術 (6)

Scenario 適用場景

Multiple Participants
眾多的參與方

若參與方包括多個生產商、供應商、客戶、服務提供商、運輸服務提供者、監管機構以及可能涉及的稅務機構，則區塊鏈技術將是一個絕佳的解決方案

Complicated Process
複雜的流程

面臨大量複雜商業目的公司團體，在交易生態體系中建立區塊鏈可產生巨大效益。區塊鏈可實現資產收購、融資、擔保、保險、監管合規和公共安全等多項事宜的一體化同步管理

Long-term Record Saving
需長期保存紀錄

若多方都需要在較長時間內獲得、創建以及維護記錄(如數十年的資產生命週期或患者全生命周期)，區塊鏈能夠提供理想的解決方案。此外，在許多監管事項的處理方面，區塊鏈能夠為記錄合規情況、開展合規管理提供可靠支援

Real-time Assets Transferring and Transacting
實時資產轉移與交易

區塊鏈能夠消除支付週期和資產轉移滯後的情況，有助於降低成本、提高精准度並提升合規效率。此外，區塊鏈的透明特性還有助於在多方網路環境下簡化貿易融資或供應鏈融資流程，提升效率

Source: 台灣經濟研究院

Blockchain Ecosystem (1)
區塊鏈生態系統 (1)

Wallets and Cryptocurrency Transfer Services
電子錢包與貨幣移轉服務
電子錢包為管理密碼貨幣私鑰的軟體。貨幣服務公司主要經營密碼貨幣匯款或移轉平台

Exchanges and Cryptocurrency Trading
交易所和密碼貨幣交易
係指建立密碼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密碼貨幣

Enterprise Services and Tokens
企業服務和代幣
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幣(tokens)的公司

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

Decentralized Exchanges
去中心化交易所與借貸平台
指區塊鏈基礎的P2P交換市場，用戶可以不需中介直接交易代幣。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

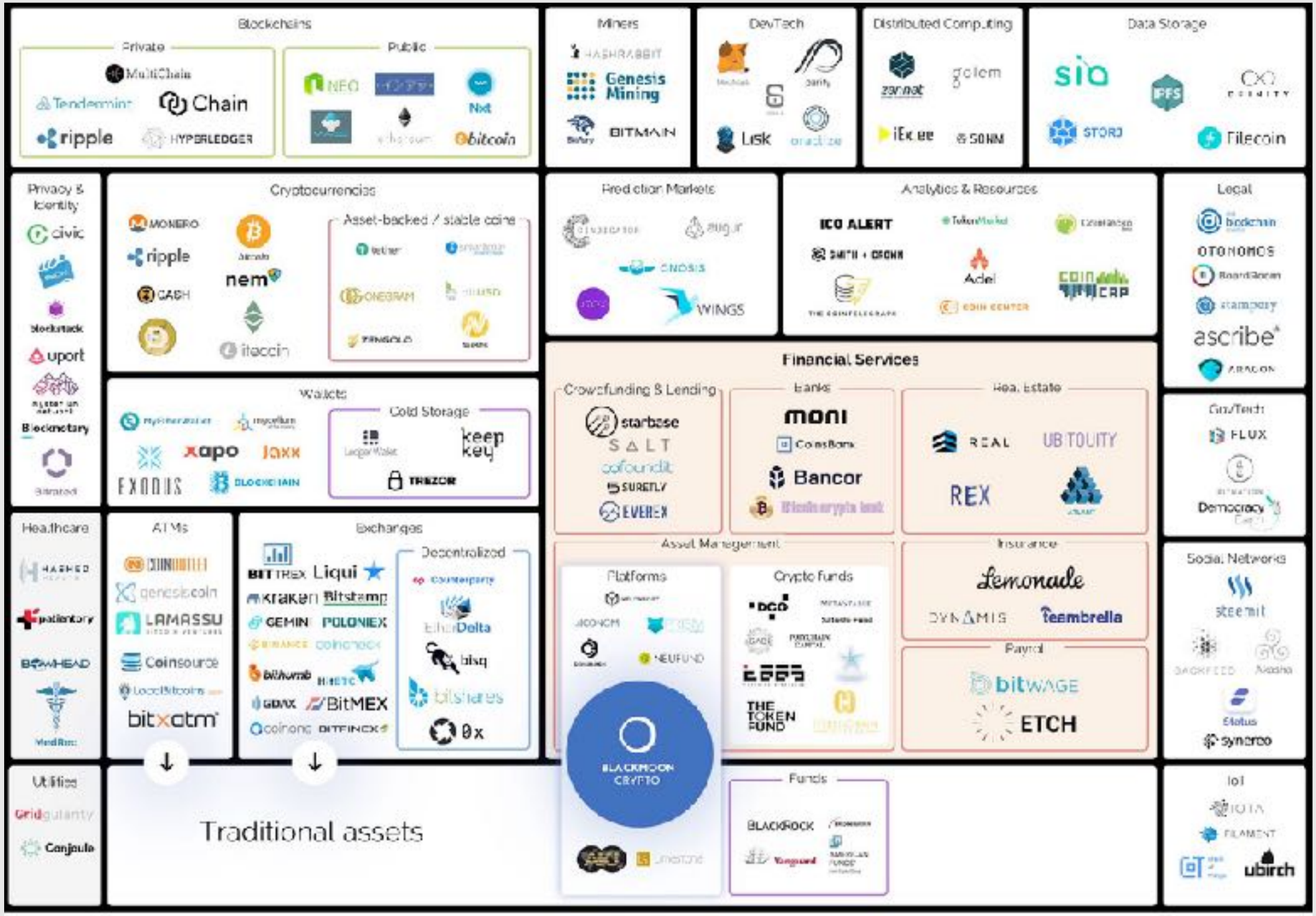
Capital Markets and Financial Services
資本市場和金融服務
主要為金融機構和中介機構開發清算、結算和數據管理等解決方案的公司，以及建立於區塊鏈基礎的投資公司

IoT, Identity and Content Management
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

E-commerce Services
商家服務
為商家和賣家開發加密碼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

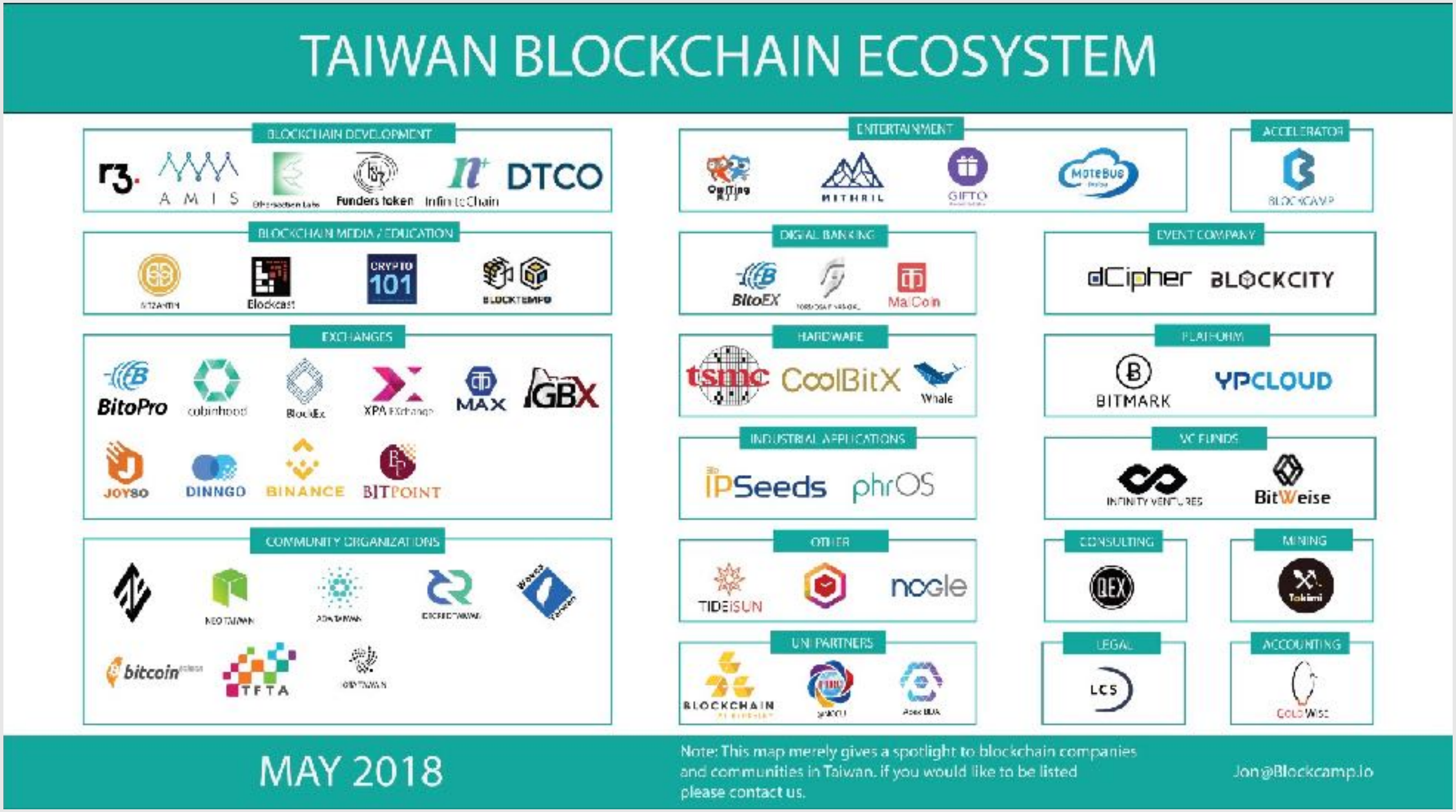
Source: **台灣經濟研究院**

Blockchain Ecosystem (2)
區塊鏈生態系統 (2)



Source: https://news.blackmooncrypto.com/the-crypto-ecosystem-v2-aea76bde5457

Blockchain Ecosystem (3)
區塊鏈生態系統 (3)



Source: https://medium.com/@blockcamp/taiwan-blockchain-alliance-6bd34eaf5ae4

Applications (1)
應用 (1)

Financial Business 金融業務

Problem 問題

現今的金融體系架構透過嚴格的審批流程、大量人力與時間的投入、第三方的參與確保，來達成目前的金融業務需要，然而這樣的方式造成了冗長的流程、人力與時間投入的高成本、錯綜複雜的多方參與，且人為失誤與詐欺仍然不斷發生

Solution 解決方案

透過智能合約的功能系統可以自動發起交易，系統可快速且實時地驗證及審批交易資料，資料亦實時在鏈上揭露，當中不需第三方的參與，大量降低人為過程，可以確保資訊安全與可被信任，同時防止欺詐事件，亦將失誤的機會降至最低

Case 案例

Ripple試圖取代SWIFT。SWIFT是單向的資訊傳送，與電子郵件非常相似，透過與銀行現有的分類帳直接集成，而Ripple的xCurrent產品為銀行提供了一種更快以及雙向的通信協議，允許實時通信和結算。據Ripple所提供的估算，若完整使用其所提供的服務，可降低60%的費用

Source: 台灣經濟研究院

Applications (2)
應用 (2)

Supply Chain and Logistics 供應鏈與物流

Problem 問題

供應鏈的參與者眾多，同時流程以及溝通繁雜，例如全球貿易90%仰賴貨運產業， 但其中參與者包含陸運供應商、貨運業者、報關行、政府機關與海運業者，過程中可能充滿爭議；此外，傳統的中心化服務，也成為駭客覬覦的目標

Solution 解決方案

區塊鏈最普遍適用之處是它能夠更安全與透明地監控交易。供應鏈基本上由一系列交易節點構成，連接上中下游的產品直到最終銷售。隨著產品從製造到銷售的供應鏈上轉移，這些交易可以記錄在一個永久的分散式帳本中，減少延誤時間、成本和人為錯誤

Case 案例

IBM + MAERSK。全球80%貨物是由海運運送，其市場總值可達一年4兆美金。但光是要把貨櫃從丹麥運至荷蘭，中間需要經過30個節點，以及超過200份紙本作業，光是處理紙本作業就會佔運輸成本的 20%。IBM 與 Maersk 使用其區塊鏈 Hyperledger Fabric，可以追蹤貨物流向，還能用智慧合約將紙本作業全部自動化，大大節省成本與時間

Source: 台灣經濟研究院

Applications (3)
應用 (3)

Medication 醫療

Problem 問題

醫療數據在跨單位不具互通性，此外，難以結合如穿戴裝置或其他環境數據，原因之一來自於資料的隱私問題與來源的分散， 此也阻礙了醫療技術的發展。每當發生索賠問題時，患者需要透過各種協商，調用多個不同系統的電子健康記錄，因此，完成整個索賠過程需時冗長

Solution 解決方案

落實醫療數據的歸戶，民眾可將資料授權，醫院可與分院、診所、健檢中心、保險公司等機構連結，透過節點裝置來存取病患數據

Case 案例

DTCO與台北醫學大學附設醫院攜手推出phrOS健康醫療區塊鏈作業系統。phrOS可作為病患個人健康紀錄的作業系統，除區塊鏈底層技術外，也整合了身分認證、線上授權、分佈式儲存技術、聯盟鏈管理等技術開發；醫院可藉此為有需求的民眾開立個人健康資訊帳戶，並逐步將健康檢查報告、就診資料輸出至該帳戶，使民眾保有並累積自己的健康資訊

Source: 台灣經濟研究院

Applications (4)
應用 (4)

Energy 能源

Problem 問題

隨著技術的進步，越來越多小規模的發電單位進入了能源市場，所在的地區若有多家能源供應商，購買不同來源的電力在目前架構上較難有效率的運作，如果想要買到再生能源，查證電力來源同樣是難題

Solution 解決方案

區塊鏈結合電網可以解決這些問題。透過區塊鏈追蹤能源的生產與消費，讓能源數據放上公用分布式帳本，讓生產及交易的來源與目的地更加透明。此外，消費者可以自行出價，建立有別於過去的電價系統

Case 案例

SOLA Bloc 太陽能資產管理平台。SOLA Bloc 透過監控物聯網將每個太陽能電廠的發電數據記錄在雲端伺服器中，透過資產平台立管理太陽能資產，並能透過智能合約，進行轉投資、捐款或參與各項新創計畫，創造更多的可能性

Source: 台灣經濟研究院

Applications (5)
應用 (5)

Tracing 溯源

Problem 問題

傳統的溯源方式是中心化的記錄模式，但產業鏈利益各方錯綜複雜，都有可能竄改紀錄，這使得消費者不信任，反過來使得企業對溯源缺少動力

Solution 解決方案

區塊鏈可實現數據難以竄改，同時可突破訊息孤島，增進消費者的信任，此外也更容易處理如商品招回的行動，提升整體服務品質

Case 案例

1. 台灣新創度度客提供了一個募資平台，透過區塊鏈實現愛心捐助金流透明並可追溯
2. 產銷履歷結合區塊鏈。台灣新創奧丁丁市集推出全球第一個食品區塊鏈溯源系統 OwlChain，透過區塊鏈技術可打造出公開透明，且不可竄改食品履歷溯源系統，消費者僅需掃描 QR CODE 食材包裝袋，即可看各種生鮮食品生產過程

Source: 台灣經濟研究院

Applications (6)
應用 (6)

Identity Proof 身份證明

Problem 問題

跨組織的資訊不流通，在各機構辦理各式身份文件時，重複著相同的作業流程，無形浪費許多時間；而資料的調查與驗證經歷也是一項耗時的工作。此外，許多商品礙於身份限制而限縮了出售的地點；而以出示證件方式人工查核，又透露過多不必要的資訊

Solution 解決方案

將身分資訊與相關證明建置在區塊鏈之上，個人可將必要的資料授權給需求者審核，無須透露其他資訊。同時應用區塊鏈可排除這些紀錄偽造的可能性，簡化審查過程

Case 案例

Civic身分認證系統。Civic是一個基於區塊鏈和生物識別的多因素身份認證系統，可以在移動端無需用戶名和密碼的情況下進行準確安全的用戶身份識別，目前已經開發出手機app和API等功能用於對接商業應用

Source: 台灣經濟研究院

Applications (7)
應用 (7)

Internet of Things 物聯網

Problem 問題

根據McKinsey的預估，到2025年時可能超過250億個連網裝置，現有的中心化雲端服務方式可能無法承受如此巨量的傳輸與運算需求。巨量的裝置也帶來龐大的數據資料，中心化的服務可能未經用戶授權即收集和分 析使用者資料、控制使用者設備的許可權；此外，中心設備壞損或遭受攻擊時，對使用者隱私和安全造成很大威脅

Solution 解決方案

相較於傳統網路環境的中心化結構，區塊鏈的對等網路傳輸，可避免單點遭駭問題以及中心伺服器的負荷極限，且數據(或數據的存證)都具可追溯性，確保數據的真實性。同時去中心化的架構以及身分與交易中皆運用大量加密方式，強化整體安全性

Case 案例

工廠設備安全解決方案。Xage提供的設備安全解決方案中， 包含防竄改系統、邊緣認證、訪問控制以及設備生命週期管理

Source: 台灣經濟研究院

Applications (8)
應用 (8)

Social Platform 社交平台

Problem 問題

目前社交網路是中心化結構，由使用者創造內容，根據社交網站設定規則、儲存內容、分享內容。使用者間互動透過中心化的社交網路實現，進行人際關係溝通與維持、獲取朋友動態等資訊，而作為服務提供方的社交網路則掌握了使用者產生的資料，並透過這些資料，實現獲益

Solution 解決方案

在區塊鏈技術下將使用者資料和資訊的控制權歸還給個人，並激勵有貢獻的用戶。此模式保證個人的資料安全，也透過機制刺激用戶貢獻

Case 案例

Steemit，去中心化的社交平台 Steemit 是基於區塊鏈的社交媒體平台，在 Steemit上發表內容、回文、討論等可以獲得獎勵，獲得的讚數對應代幣，形成代幣經濟模式

Source: 台灣經濟研究院

Applications (9)
應用 (9)

Distributed Computation and Storage 分散式運算與儲存

Problem 問題

許多領域對電腦算力與儲存的需求大幅增加，而多數時候許多電腦設備又都處於閒置狀態，此外，目前提供雲端運算與儲存服務的企業通常以集中式伺服器保護客戶的資料，但這意味著當遭受駭客攻擊時會增加資料毀損的風險

Solution 解決方案

去中心化的概念或許能銜接電腦算力與儲存供需兩方達到資源的有效利用，且區塊鏈的分散式特質應用在雲端儲存上，則可降低系統性損壞與資料遺失的風險

Case 案例

出租你的硬碟空間。Storj是使用區塊鏈的雲端儲存網路，以提高安全性並降低在雲端儲存資訊的成本。Storj 用戶還可以利用P2P方式出租其未使用的雲端儲存空間，成為雲儲存容量市場

Source: 台灣經濟研究院

Applications (10)
應用 (10)

Digital Property Right 數位財產權

Problem 問題

過去數位資產因易於複製與散布，難以確保原創者或所有權人的權益，也造成此類內容難以安全、合理地授權甚至分潤，以及二次創作的利潤歸屬

Solution 解決方案

區塊鏈的不可竄改性提供了確認產權的機制，同時讓數位內容可更有效率、安全的方式對外授權使用，同時在搭配智能合約的設計下，可讓授權後的利潤分配可更有效率地達成

Case 案例

音樂授權分潤。KKFARM以Bitmark技術將數位內容加密且標示內容所有權等資訊，每次授權均以獨立 Bitmark ID標示授權內容，在授權取得、使用管理與營收分潤，藉由智慧合約，針對每一項內容授權標明版權持有者、分潤者，以及各個分潤者取得比例，一旦授權內容產生使用營利，即可自動依據各個分潤比例撥款給不同分潤者，進而減少整體溝通往返、取得授權與確認的反覆流程

Source: 台灣經濟研究院

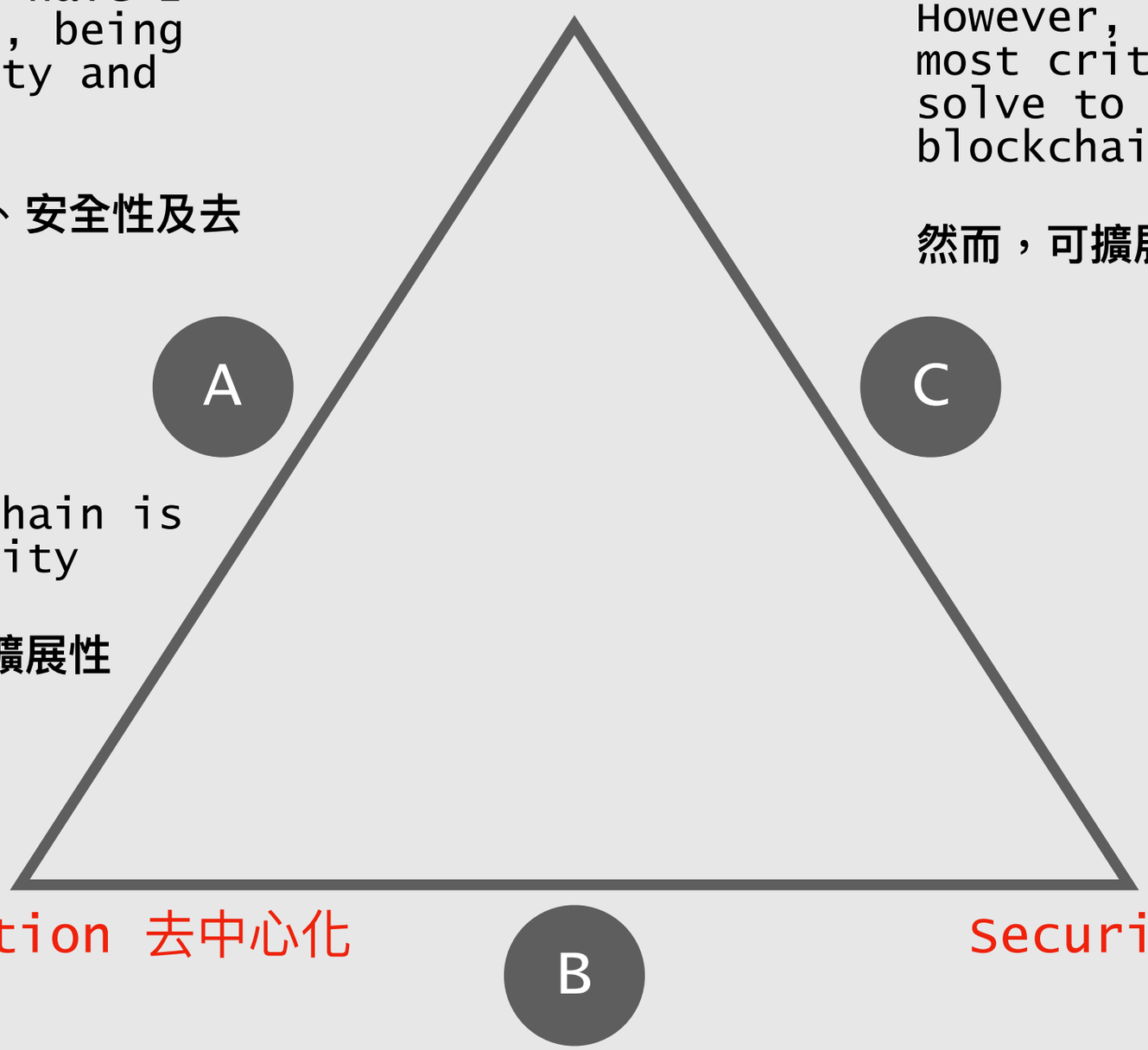
Challenges
挑戰

Blockchain can only have 2 of the 3 properties, being scalability, security and decentralization

區塊鏈只能擁有可擴展性、安全性及去中心化中的兩項特性

The existing blockchain is lacking of scalability

現今存在的區塊鏈缺乏可擴展性



However, scalability is the most critical problem to solve to popularize blockchain

然而，可擴展性是普及區塊鏈的關鍵

Source: 台灣經濟研究院

Conclusion
結論

- Blockchain is still experimental and immature

  區塊鏈仍是實驗性且尚未成熟的技術

- Blockchain is challenging but worth learning and investing

  區塊鏈具有挑戰性，但值得學習以及投資

Source: 台灣經濟研究院

Thank You
謝謝

@juinc davidjuin0519@gmail.com

Taipei Ethereum Meetup