區塊鏈應用對半導體晶片之需求分析

鄭凱安
資深產業分析師兼產品經理
產業情報研究所(MIC)
財團法人資訊工業策進會
2020.12.10

andykacheng@micmail.iii.org.tw
mic.iii.org.tw

簡報大綱

- 比特幣與區塊鏈
- 區塊鏈主要晶片運算需求：挖礦
  - 工作證明proof of work
  - 全球挖礦晶片與礦機發展
- 區塊鏈物聯網應用之晶片需求
  - 下世代網路發展目標
  - 區塊鏈物聯網晶片案例：ITM
- 結論與後續觀察方向

比特幣與區塊鏈

2020年比特幣價格快速攀升

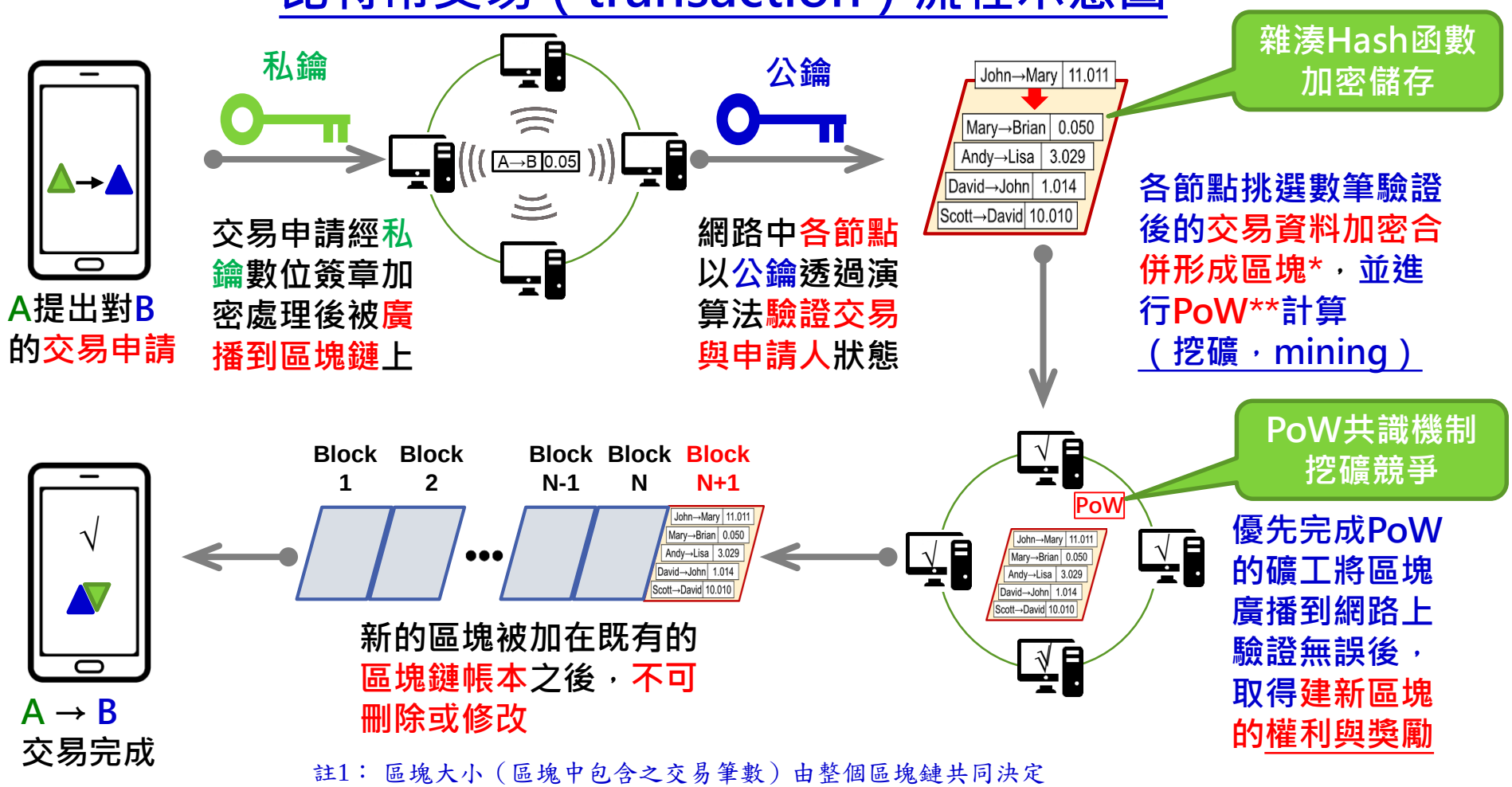
資料來源：coindesk，MIC整理，2020年12月

- 擔憂各國央行刺激經濟計畫引發通貨膨脹，投資人積極買進黃金、比特幣等具保值能力之金融產品，帶動比特幣價格自2020年初起快速增長
- Paypal於2020年10月，宣布2021年將導入加密貨幣支付機制，支援比特幣、以太幣、萊特幣等，推動比特幣價格衝破15,000美元

MIC

區塊鏈是支持比特幣交易的關鍵技術

比特幣交易（transaction）流程示意圖



註1： 區塊大小（區塊中包含之交易筆數）由整個區塊鏈共同決定
註2： PoW（proof of work）：工作量證明，是比特幣關鍵的共識機制

資料來源：gbksoft.com （2018），MIC整理，2020年12月

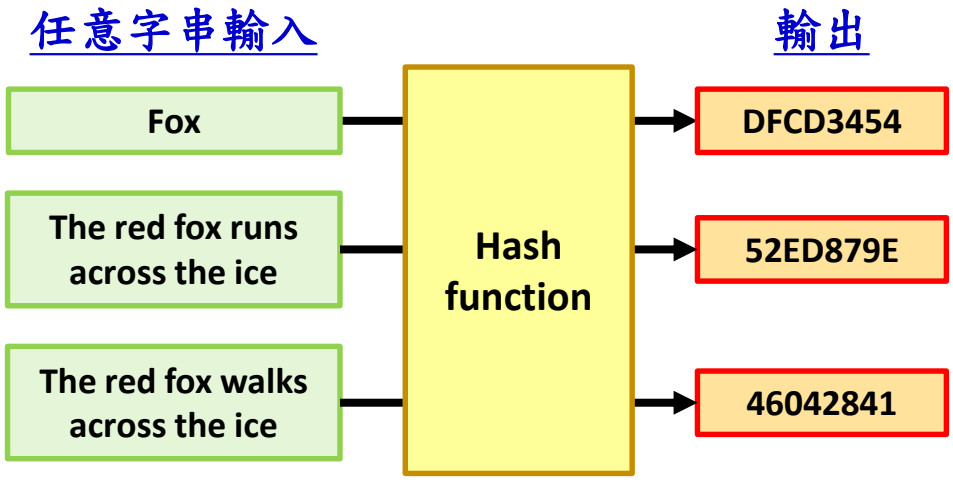
區塊鏈主要晶片運算需求：挖礦

區塊鏈的核心技術

1. 雜湊函數Hash Function

區塊鏈交易儲存之格式

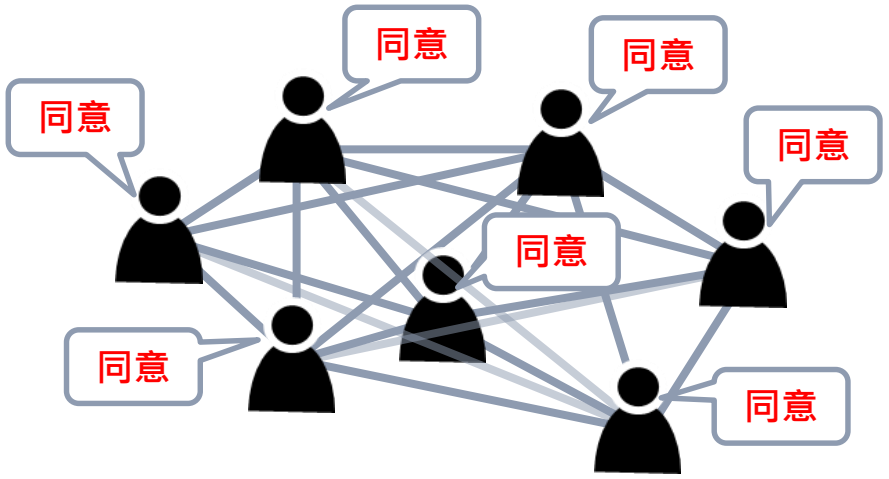
- 任意長度的字串輸入均可轉換為固定長度的字串輸出後儲存
- 將大筆資料以Hash字串摘要儲存
- 加密並節省儲存空間



2. 共識機制Consensus

區塊鏈建立信任之基礎

- 無銀行中介下，所有交易及區塊之記錄必須獲得多數節點的認同
- 確保區塊鏈版本一致性及公平性
- 加密貨幣須有共識機制認證交易

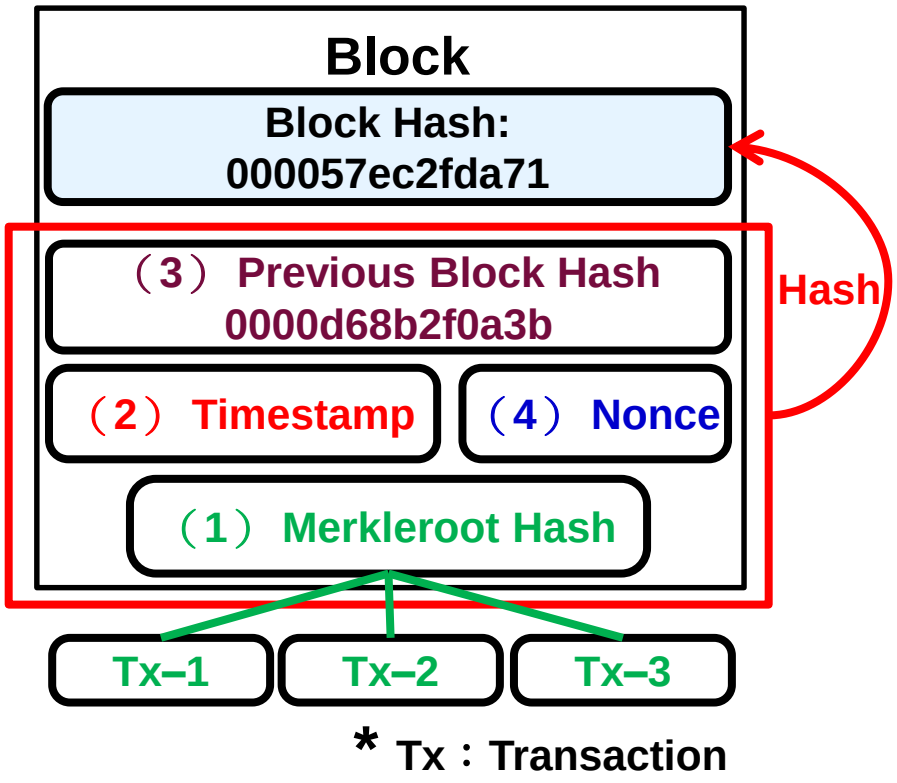


資料來源： MIC，2020年12月

比特幣區塊鏈中單一區塊的儲存內容

單一區塊內容包含：

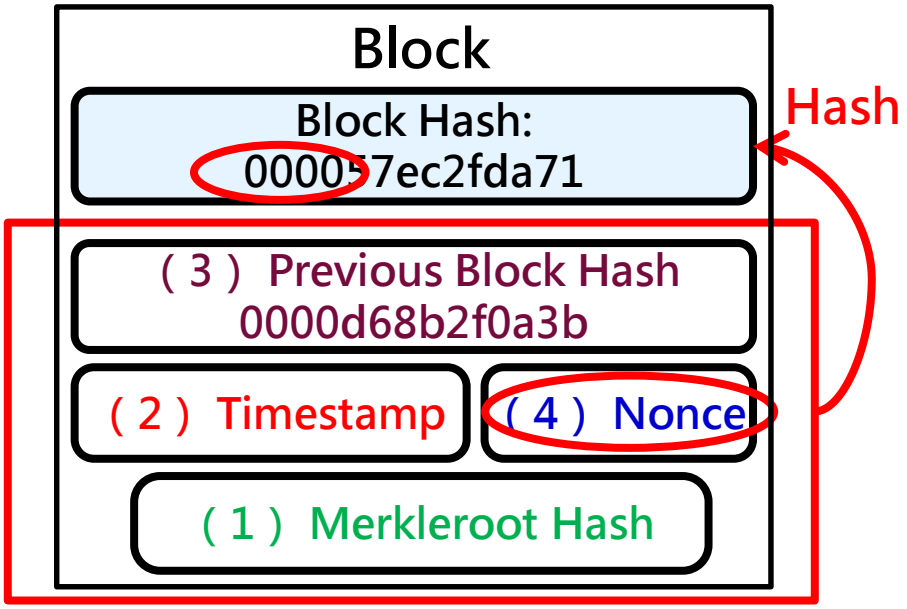
（1）交易資料的摘要hash值	每一區塊可容納多筆交易，所有交易記錄以一個Hash值摘要代表，維持固定表頭儲存空間
（2）時間戳記（timestamp）	時間戳記：在每一區塊中，記錄區塊建立時之時間，作為判斷不同區塊建立先後順序之用
（3）前一個區塊的hash值	前一區塊Hash值：記錄前一區塊之Hash特徵值，作為確立二區塊直接前後串聯的判斷依據
（4）可調參數Nonce值	配合比特幣規則，當區塊儲存內容轉為Hash值時，需要利用Nonce隨機數進行調整



資料來源： bitcoin.org （2008）、 kocpc.com.tw （2013），MIC整理，2020年12月

比特幣共識機制：Proof of Work工作量證明

- 比特幣對挖礦難度的設定（2018年）：區塊的Hash值**前18位起始數字為0**
- Proof of Work （PoW）
  - 礦工（節點）合併交易形成區塊時，依照上述規定計算Hash值
  - 若Hash值不滿足前18位為0，則持續**調整Nonce大小**後重算
  - 優先得出正確Hash值的礦工，將結果廣播到網路由**多數節點認證**，獲得建立新區塊的權利

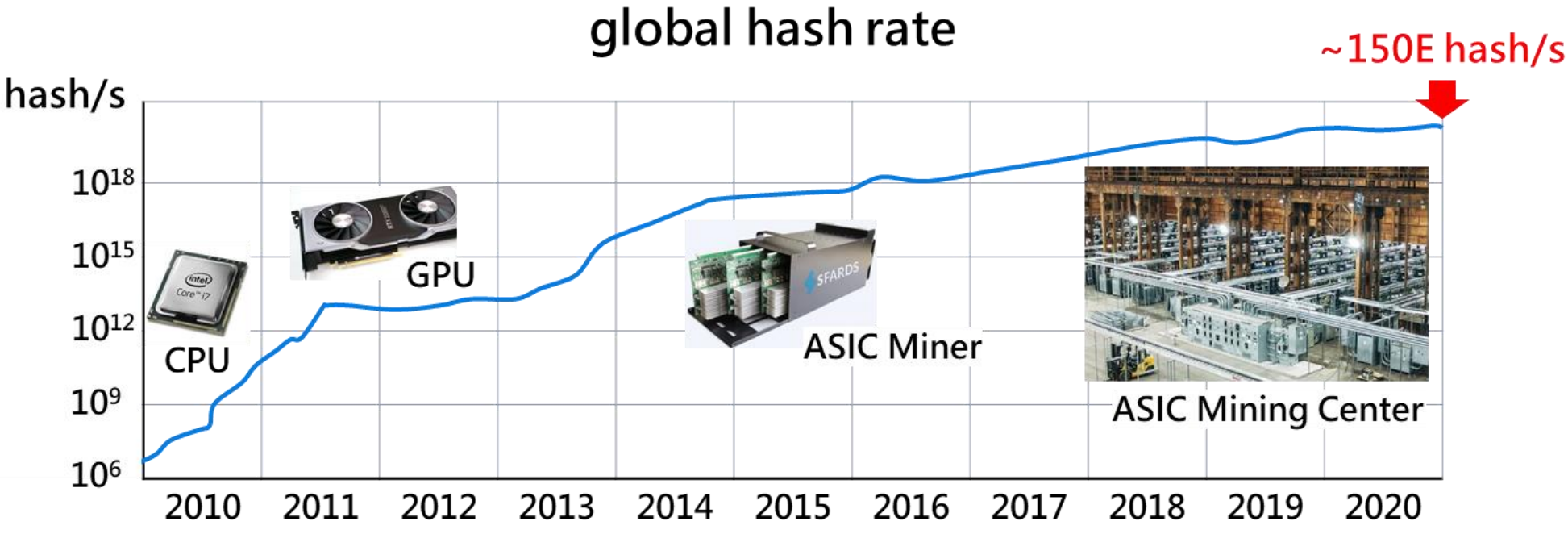


- 簡單說明 try and error 猜到正確Hash值的難度（目標：Hash首位為0）

輸入字串	Hash值
CoinDesk rocks!	6b1f6fde5ae60b2fe1bfe50677434c88
CoinDesk rocks!!	66925f1da83c54354da73d81e013974d
CoinDesk rocks!!!	c8de96b4cf781a6373766c668ceac0f0
CoinDesk rocks!!!!	9ea367cea6a2cc4a6f5a1d9a334d0d9e
CoinDesk rocks!!!!!	b8d43387d98f035e2f0ac49740a5af38
CoinDesk rocks!!!!!!	0fe46518541f4739613b9ce29ecea6b6

資料來源： CoinDesk （2017），MIC整理，2020年12月

PoW對晶片效能需求持續攀升



備註：E = Exa = 10^{18}

資料來源： bitinfocharts.com，MIC整理，2020年12月

- 比特幣挖礦的運算需求反映在全球hash rate的增長
- 隨著全球彼特幣用戶數量增加，比特幣挖礦難度持續提升，比特幣交易所需之hash運算數量快速攀升，已達到 150Exa hash/s
- 競爭挖礦需要之高效能的運算裝置，適合大量平行運算的GPU與適用特定hash演算法的ASIC成為首選

比特幣價格急遽攀升又將掀起挖礦潮？

資料來源：Coindesk、億邦國際，MIC整理，2020年12月

- 比特幣的存在使挖礦成為常態需求，故長期而言，挖礦機與挖礦晶片的需求將穩定成長，挖礦ASIC將與GPU、手機晶片、AI晶片競爭先進製程產能
- 比特幣價格急遽提高，是否再引發另一波短期挖礦潮，將成為2021年半導體晶片供需的變數

區塊鏈對運算晶片的需求僅限於PoW

加密貨幣	共識機制	Hash演算法	是否挖礦	使用晶片
Bitcoin	**PoW**	SHA256	Y	ASIC
Ethereum	**PoW**	Ethash	Y	GPU / CPU
Ripple	RPCA		N	
DASH	PoW / PoS	X11	Y	ASIC
Litecoin	PoW	Scrypt	Y	ASIC
Monero	PoW	Cryptonight	Y	GPU / CPU
NEO	DBFT		N	
IoTA	Tangle		N	
EOS	DPoS		N	
Stellar	PoS		N	
Vertcoin	PoW	Lyra2RE	Y	GPU / CPU
Decred	**PoW** / PoS	BLAKE256	Y	GPU / CPU
Bitcoin Gold	**PoW**	Equihash	Y	GPU / CPU

資料來源：https://blog.csdn.net/qq_41185868/article/details/85263084，MIC整理。2020年12月

- 區塊鏈的運算需求主要為加密貨幣PoW共識機制演算，極度消耗電腦運算資源，需透過專用ASIC或GPU進行運算
- 除PoW外，其餘區塊鏈應用共識機制目前並無大量運算需求

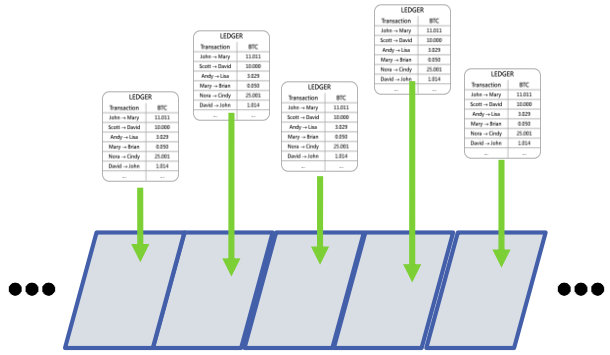
區塊鏈物聯網應用之晶片需求

區塊鏈產業應用的關鍵特性

不可竄改（可追溯性）

資料儲存的改變

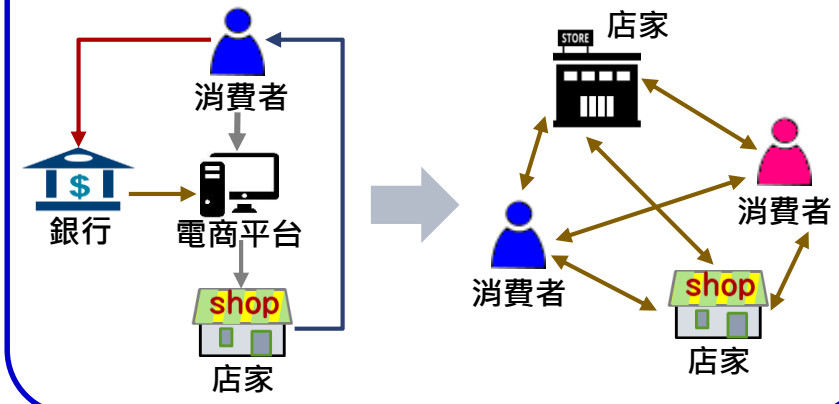
- 區塊資料依照**時序累加**在原有區塊之後
- 每一個區塊資料都**包含前一區塊**的資料
- 提升資料**安全性**，增加**信任**



去中心化（流程簡化）

網路架構的改變

- **點對點**進行資料交換，提升**效率**
- 去中心化，避免中介者**剝削**或造成**不對等資訊**傳輸
- 減少資料接觸者，保障**隱私**

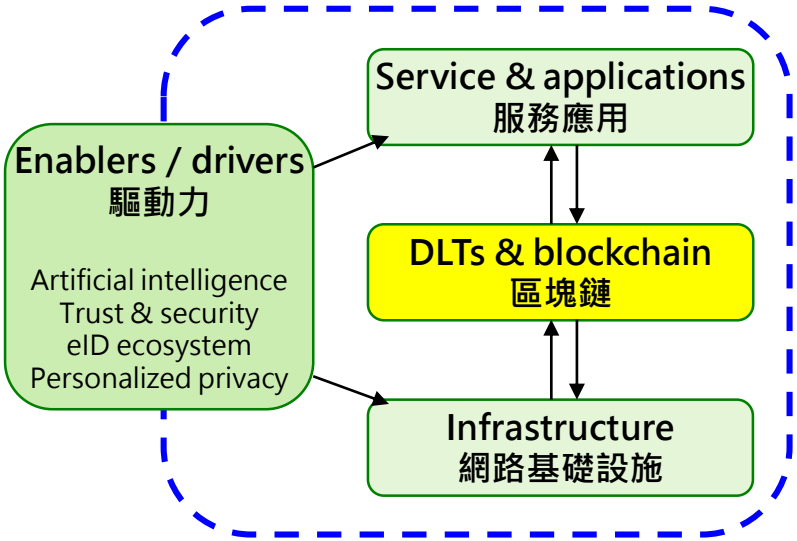


資料來源： MIC，2020年12月

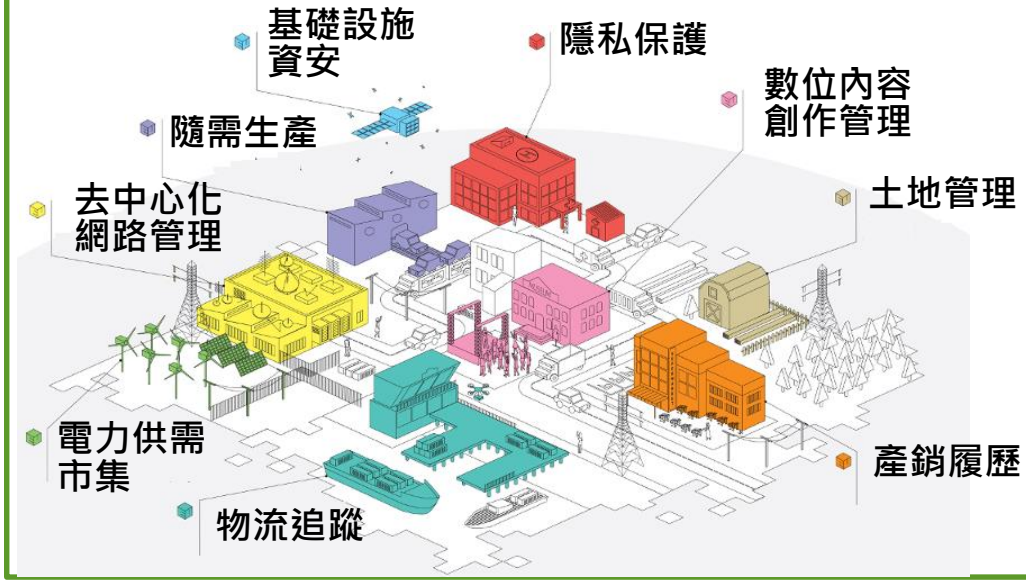
區塊鏈提供網路身分與資訊傳遞的認證

歐盟下世代網路規劃

NGI Architecture



#Blockchain4EU

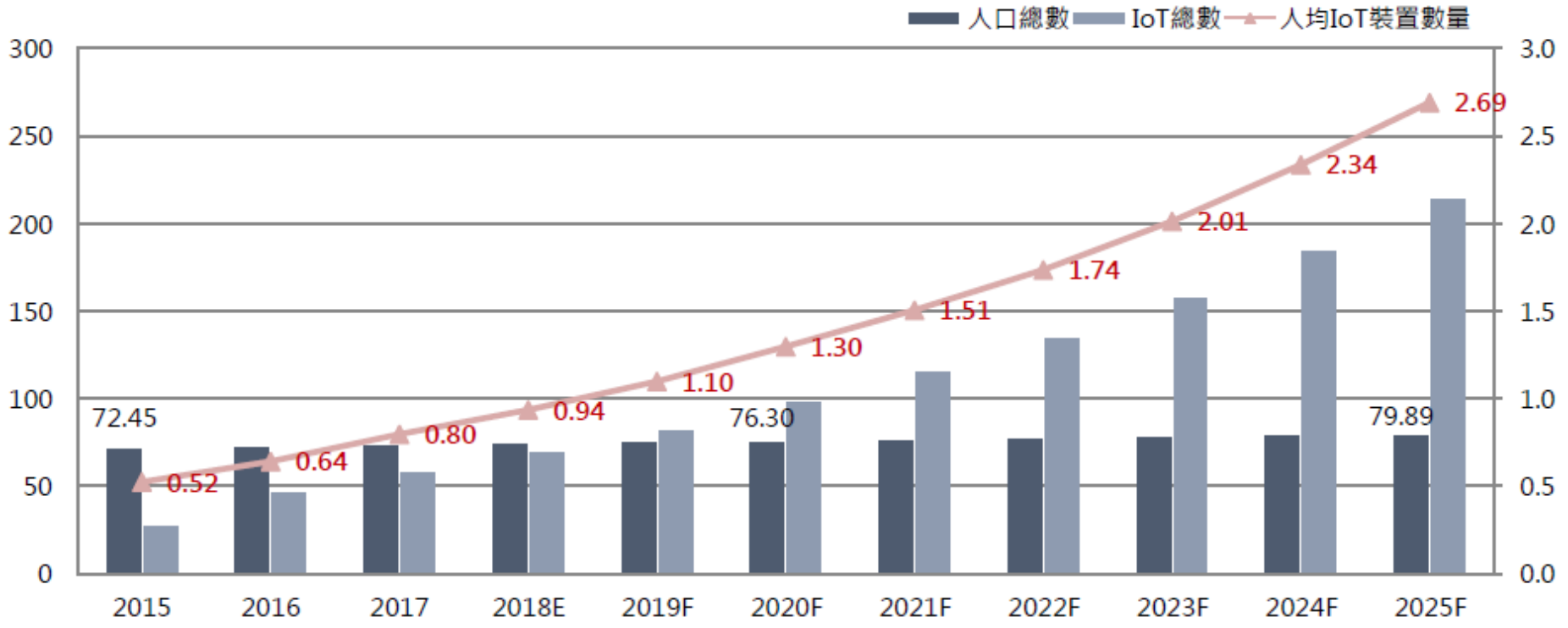


資料來源：INSCI 2017 Conference （2017）、#Blockchain4EU （2018），MIC整理，2020年12月

- 歐盟提出將以下世代網際網路（NGI）整合B5G行動通訊構建智慧網路smart networks，其中區塊鏈的存證、認證與去中心化特性，切合資料經濟生態系和網路需要，將在智慧網路架構中居關鍵地位
- 歐盟將啟動#Blockchain4EU計畫，支持區塊鏈未來應用於產業轉型中之服務與情境探索

物聯網快速發展，涉及人類生活各層面

全球人口與IoT裝置數量



資料來源：IoT Analytics （2018）、Cognizant、Deloitte，MIC整理，2020年12月

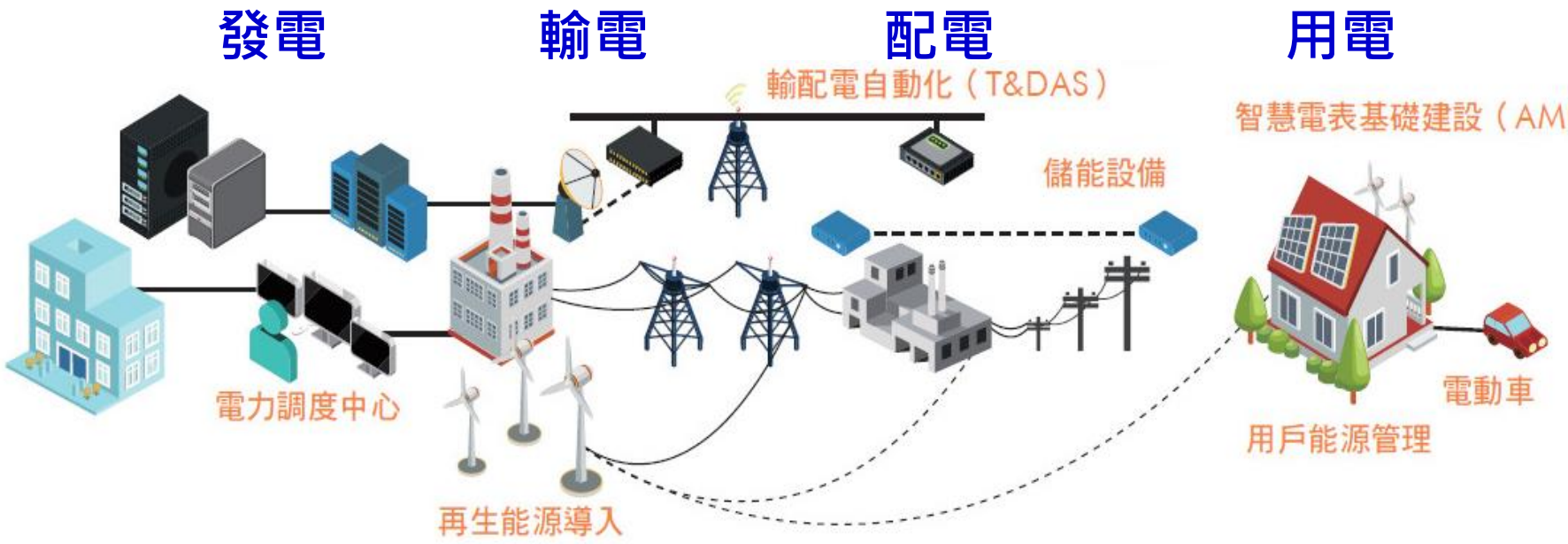
- 根據IoT Analytics預測，2023年以上全球IoT聯網裝置數將超過200億個
- 2025年人均IoT裝置數達到2.69個，IoT將充斥於生活與工作各層面

物聯網多元應用須保障資料交換安全性

資料來源：各業者、媒體網站，MIC整理，2020年12月

- 物聯網是將實際物體加載嵌入式感測器和 API 等裝置，透過網際網路形成互相連通，所形成的訊息連結與交換網路。
- 資料交換中的資料認證與資安防護對於車聯網、健康照護、智慧製造、安全監控等產業應用至為關鍵。

物聯網於能源領域之應用：智慧電網

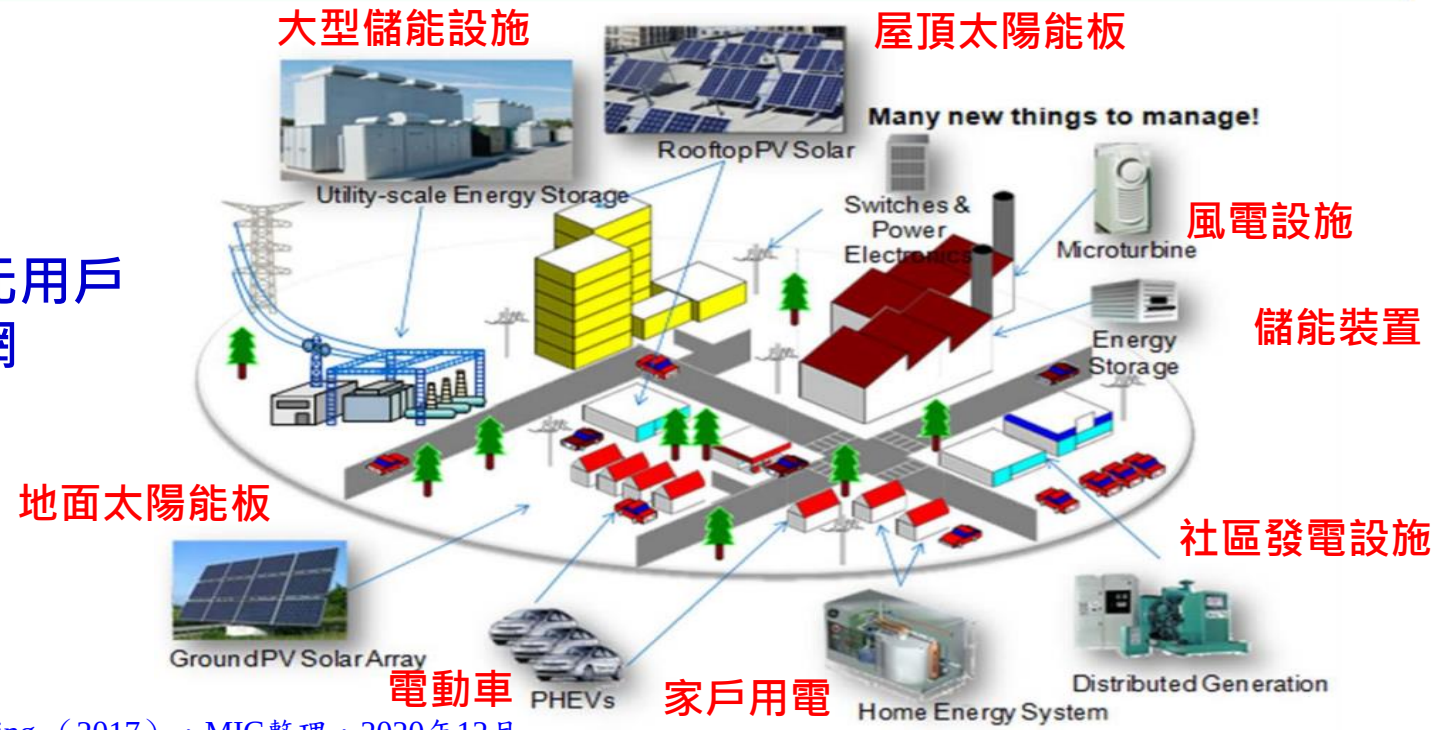


資料來源：經濟部能源局智慧電網總體規劃方案（2017），MIC整理，2020年12月

- 電網主要四大組成：發電、輸電、配電、用電
- 智慧電網透過智慧電表等裝置偵測與收集電網的電力供應與使用狀況，再依據這些資訊調度電力的生產、輸送與分配，或調整用戶的用電價格與模式，有效降低電力損耗、達到電力供需最佳化
- 智慧電表基礎建設（AMI）以智慧電表收集用電資訊後經通訊網路傳輸至電力公司，由電力公司分析後擬定或調整相關供電方案

區塊鏈應用於智慧電網之考量

多元供電與多元用戶的智慧電網

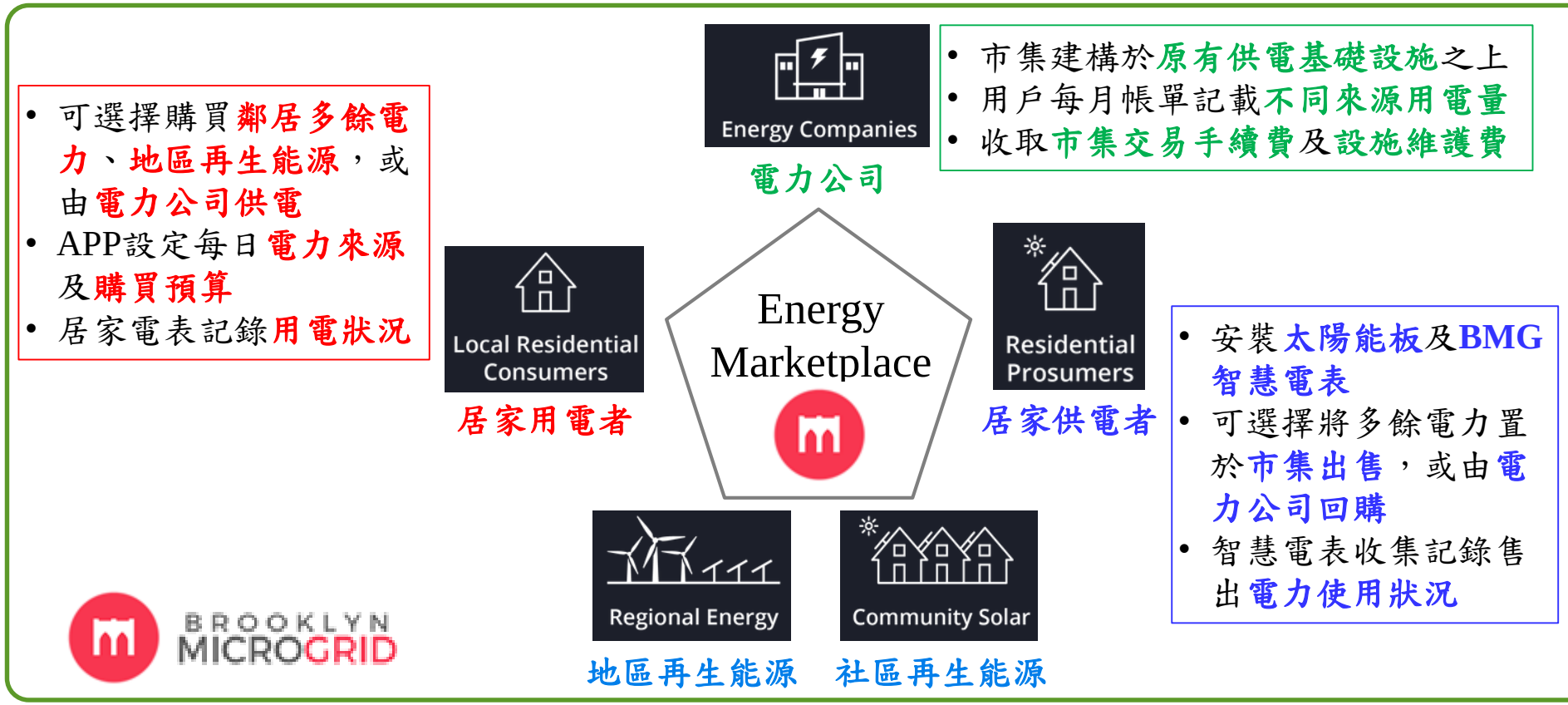


資料來源：Concord Engineering（2017），MIC整理，2020年12月

- 未來的智慧電網中，將包含電力公司與居家再生能源等**多元供電**來源、電力中介商，以及業者、家戶、電動車等**多元用戶**，供需關係複雜
- 供電者的發電量與獲利、併網用電與儲電之分配、使用者用電量與收費、具備發電能力用戶的特殊計價等，都需要**透明化呈現與精確計價**
- 區塊鏈**不可竄改**之溯源特性，以及**智能合約**之自動執行能力，將建立可信任之去中心化電力供需交易體系，甚至衍生**新商業模式或服務**

區塊鏈應用於智慧電網之案例分析（1/2）

LO3 Energy + Siemens讓Brooklyn居民與鄰居交易電力

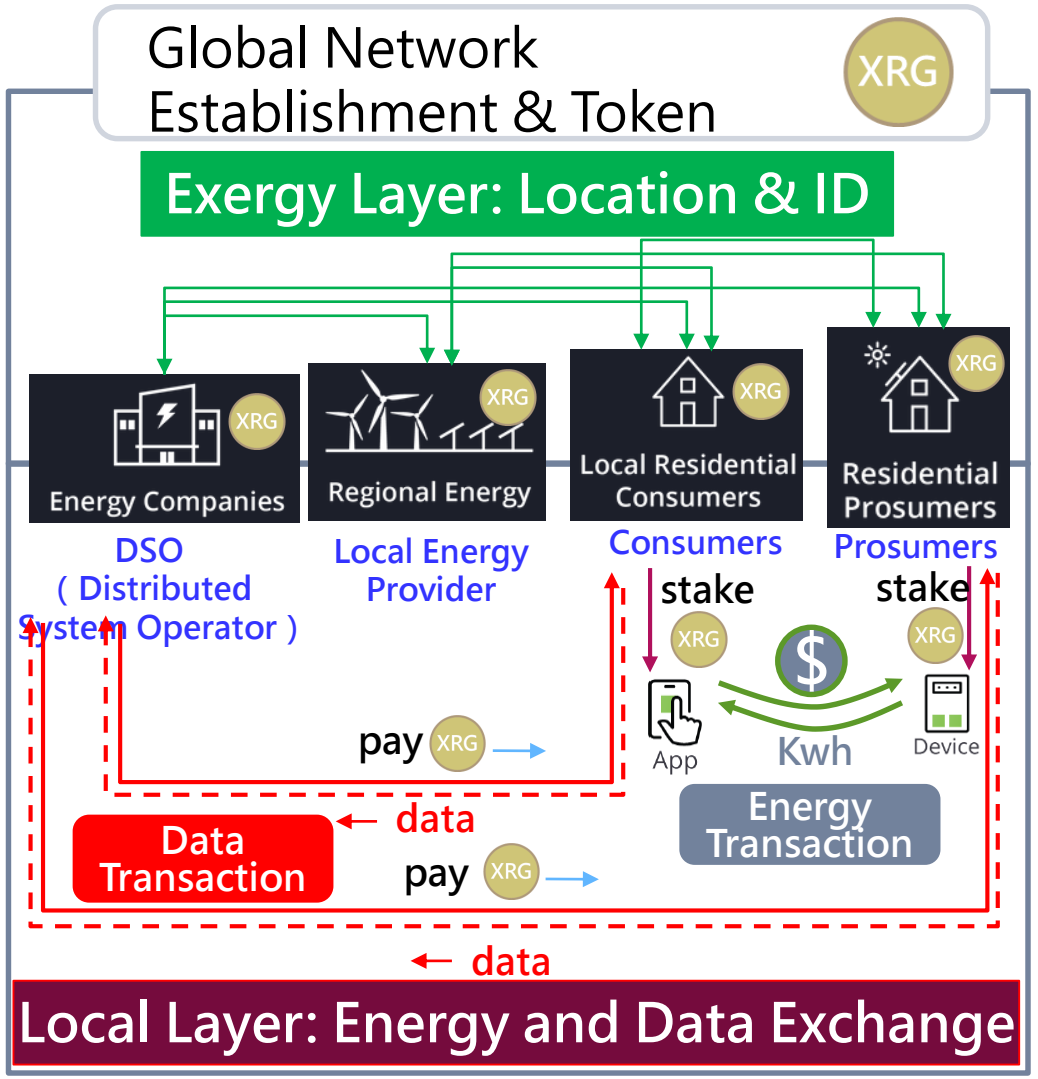


資料來源：LO3 Energy、Brooklyn Microgrid （2019），MIC整理，2020年12月

- ❖ Brooklyn MicroGrid（BMG）主要由傳統電力公司、地區及社區再生能源供應者、居家供電者與居家用電者組成，形成一社區再生能源市集
- ❖ 區塊鏈記錄用電之來源比例、用電狀況以及費用計算，確保交易透明可信

區塊鏈應用於智慧電網之案例分析（2/2）

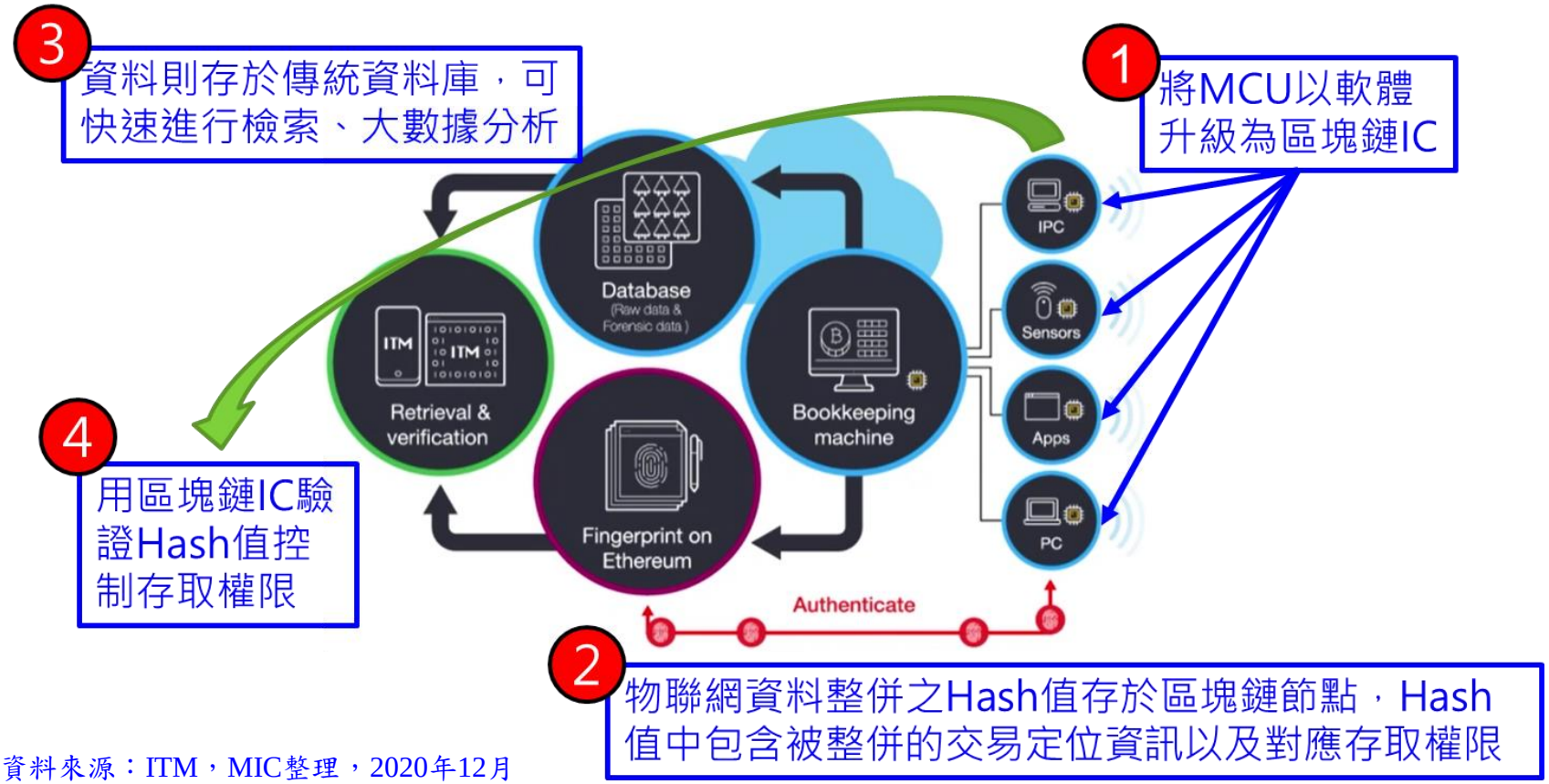
代幣經濟應用的體現



- Exergy區塊鏈代幣XRG
  - ERC20-compliant（基於以太坊）
  - 啟動mobile app與Exergy裝置
- 上層區塊鏈：Exergy Layer
  - 管理能源市場參與者全球網路
  - 以XRG激勵供電及用電者參與Exergy網路
- 底層區塊鏈： Local Layer
  - 分散全球的區域（local）區塊鏈
  - 能源資料的記錄與管理，由參與者設定資料之買賣運用
  - 含供電用電設定之激勵機制
- 使用代幣的優勢
  - 代替現金進行獎勵措施
  - 便於區塊鏈網路交易與儲存
  - 不受供需市場價格浮動影響

資料來源：Exergy-BIZWhitepaper（2018），MIC整理，2020年12月

將物聯網MCU轉化為區塊鏈晶片：ITM



資料來源：ITM，MIC整理，2020年12月

- 以軟體升級既有MCU成為區塊鏈物聯網晶片，免除專屬晶片需求
- 資料認證管控與儲存分離，避免大量資料加密儲存後，檢索與分析的困難
- 避免大量資料產生後儲存於區塊鏈所需耗費之加密運算需求

結論

區塊鏈產業應用考量與晶片需求

區塊鏈產業應用特性

不可竄改

- 加密儲存
- 多節點備份
- 建立信任

去中心化

- P2P資料交換
- 文件共享
- 效率提升

區塊鏈專屬晶片之需求分析

加密貨幣挖礦

- 部分加密貨幣PoW需高算力
- 節點數量多
- ASIC效能較佳

產業應用

- 視共識／認證機制需求而定
- 節點數量少
- 不需專屬晶片

物聯網應用

- 數位ID與資料認證需求
- 節點數量多
- 軟體+MCU

資料來源：MIC，2020年12月

智慧財產權暨引用聲明

- 本活動所提供之講義內容或其他文件資料，均受著作權法之保護，非經資策會或其他相關權利人之事前書面同意，任何人不得以任何形式為重製、轉載、傳輸或其他任何商業用途之行為
- 本講義內容所引用之各公司名稱、商標與產品示意照片之所有權皆屬各公司所有
- 本講義全部或部分內容為資策會產業情報研究所整理及分析所得，由於產業變動快速，資策會並不保證本活動所使用之研究方法及研究成果於未來或其他狀況下仍具備正確性與完整性，請台端於引用時，務必注意發布日期、立論之假設及當時情境