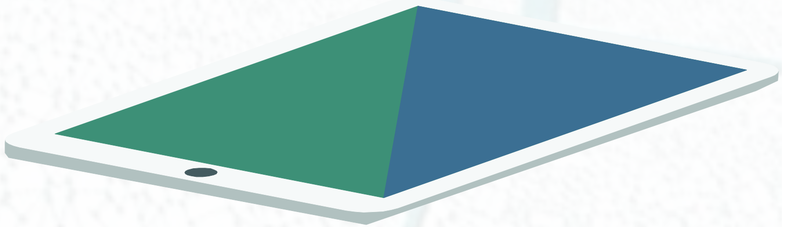
ITM
國際信任機器股份有限公司
International Trust Machines Corporation

「Trust As a Service」
區塊鏈雲端服務

Swanky Hsiao
ITM 技術研發總監

swanky.hsiao@itrustmachines.com



蕭宇程 (史旺基)

http://swanky.github.io/

Blockchain Believer / Java Enthusiast / Portrait Photographer / Growth Hacker

國立臺灣師範大學資訊工程博士

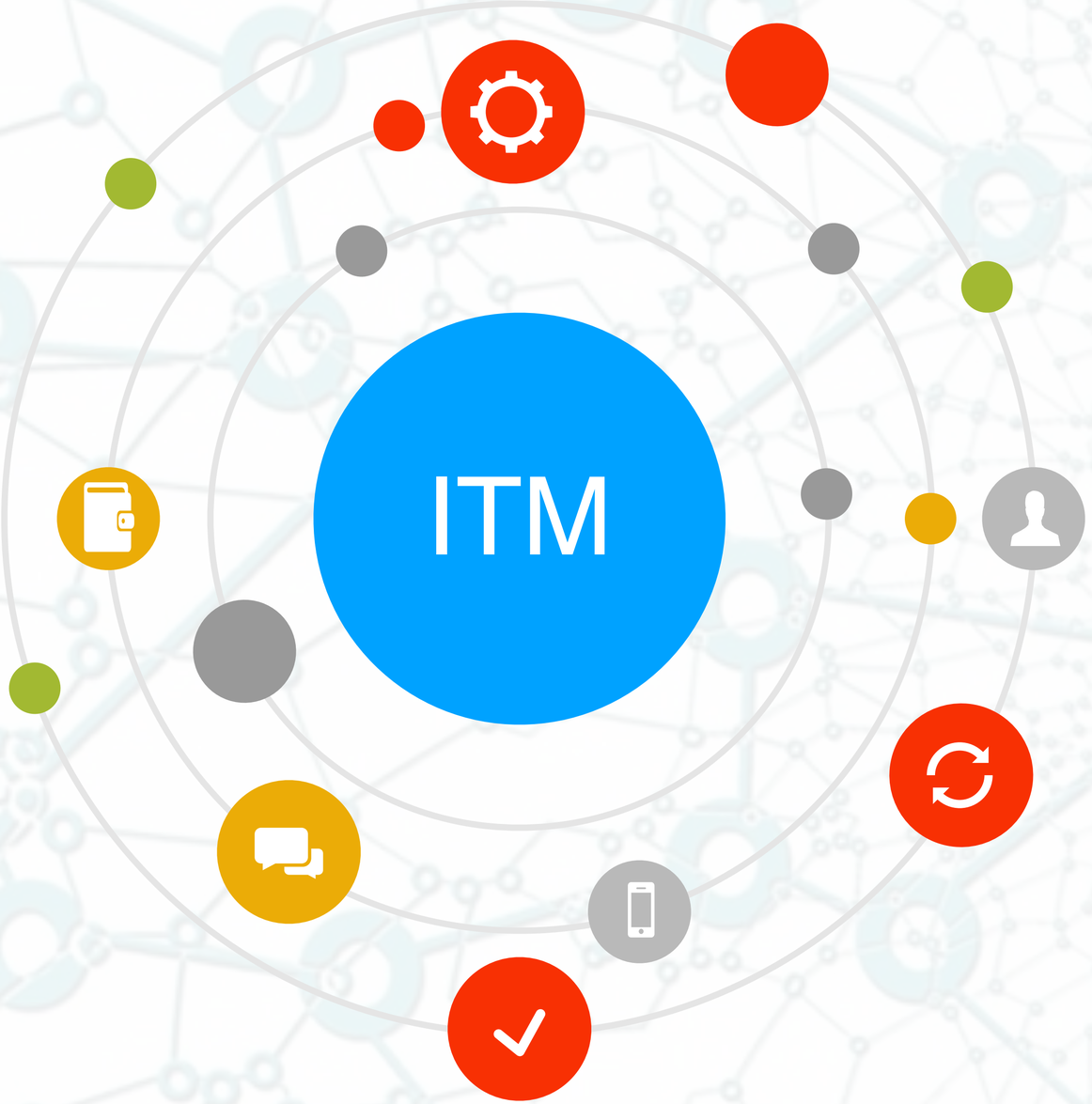
「史旺基加密貨幣交易實戰班」講師 / 密碼女孩計畫成員
東吳大學巨量資料管理學院兼任助理教授

《制服・女孩 × 史旺基》系列與
《高校制服戀物論》攝影作者

朱學恒「阿宅反抗軍」及
「制服地圖」特約攝影師

JWorld@TW認證版主

曾任職 資策會前瞻中心
現為 ITM 國際信任機器股份有限公司技術研發總監



- 1.公司介紹
- 2.發展緣由
- 3.技術核心
- 4.技術實現
- 5.應用案例

01

公司簡介

ITM

國際信任機器股份有限公司

International Trust Machines Corporation

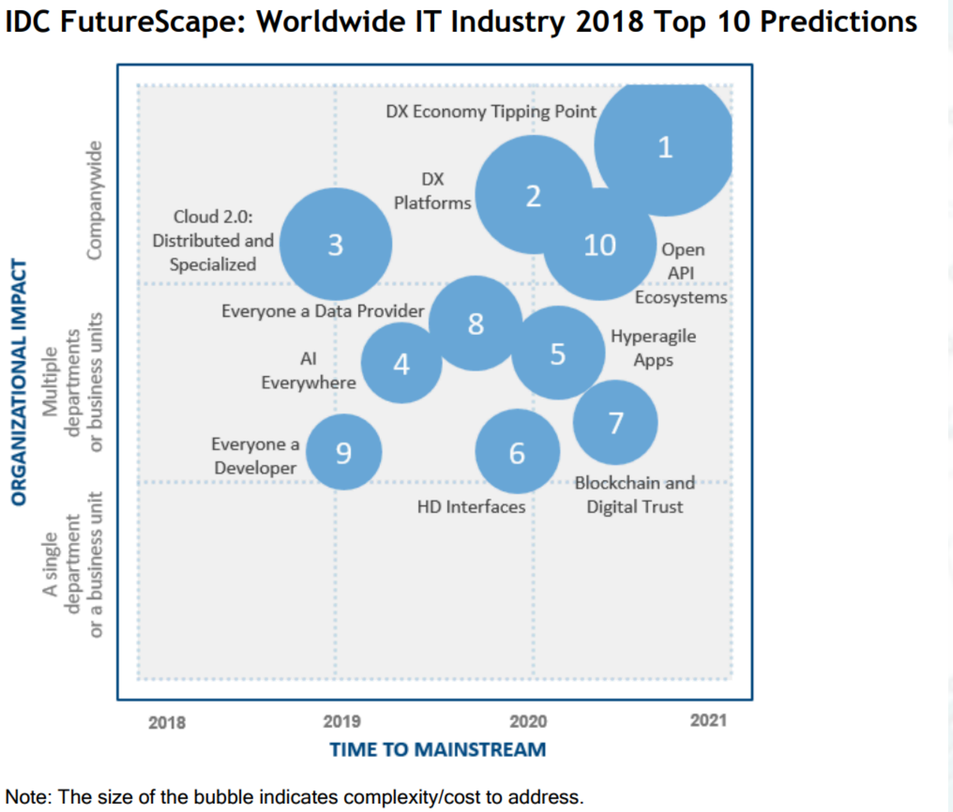
領先全球的區塊鏈擴容方案和區塊鏈IC推動者：

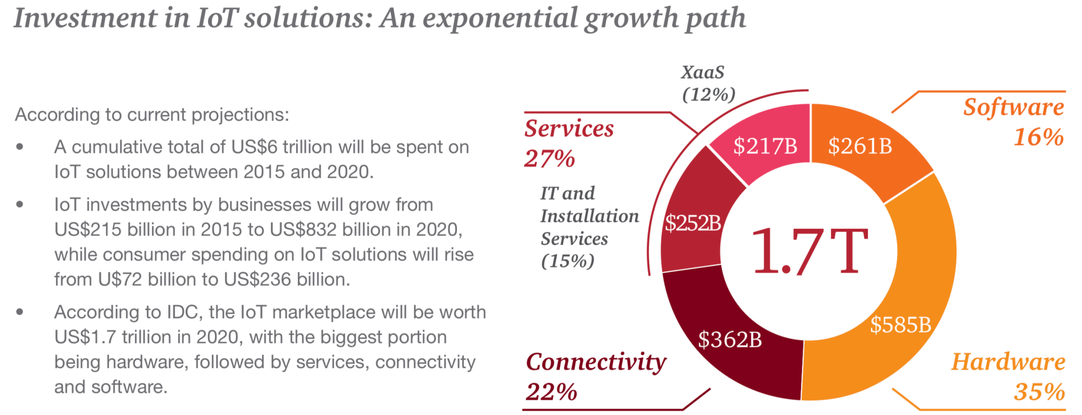
讓區塊鏈和物聯網整合成為可能

02

發展緣由

主流市調機構預測物聯網裝置上鏈將成趨勢

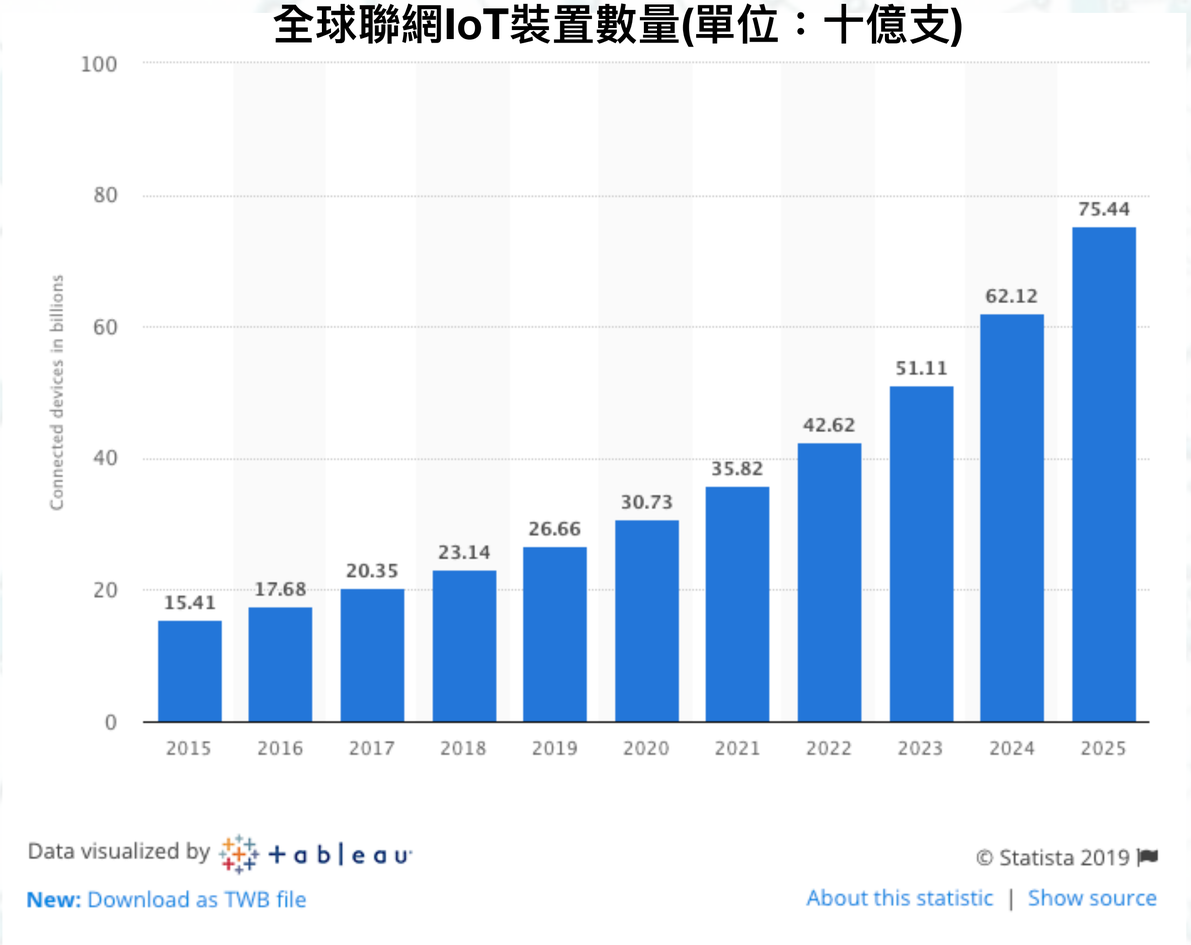




2019年，20%的物聯網環境都會具備最基本的區塊鏈上鏈功能(IDC).

2020年物聯網的市場規模將達到1.7兆美元，2015年至2020年，物聯網的建置投資將達到6兆美元。

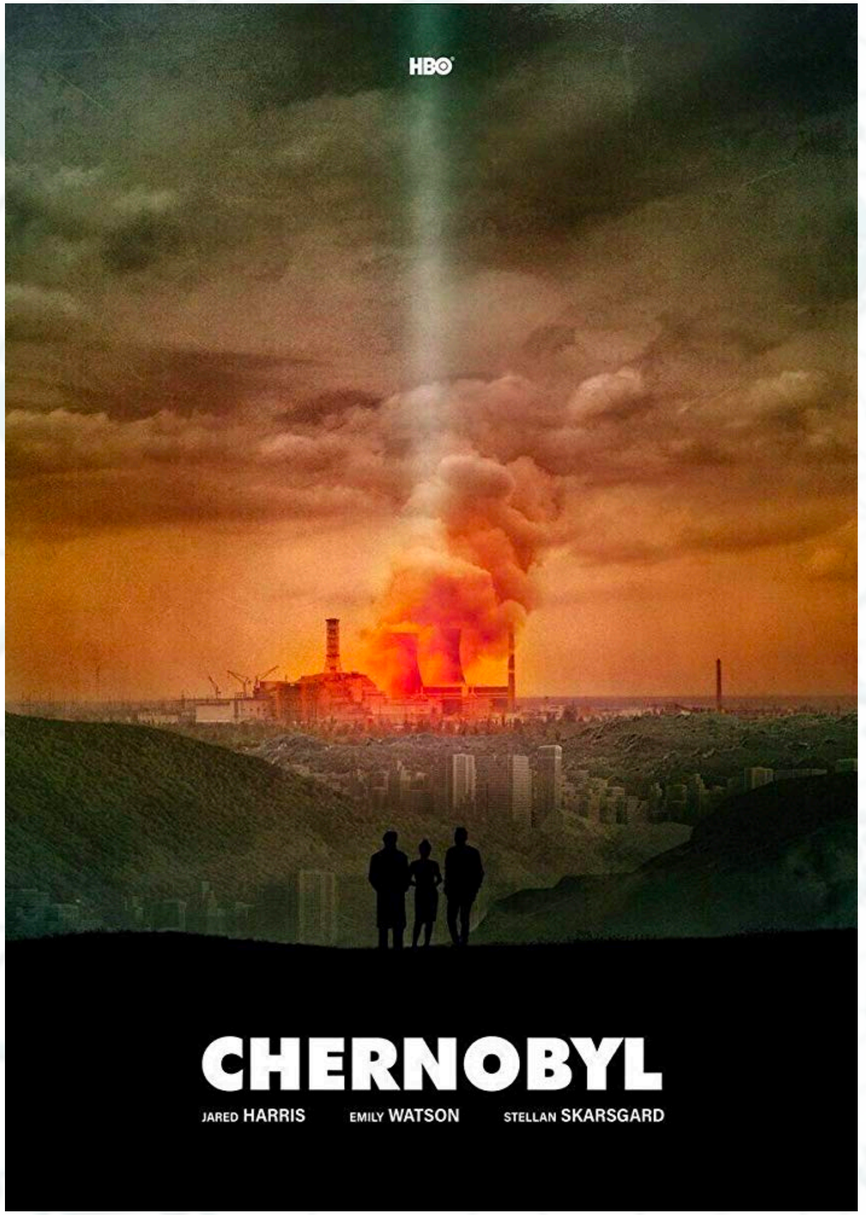
萬物聯網時代，連網裝置和資料量幾何式爆炸成長



- 2025年全球聯網裝置預計超過750億台，是現在全球人口的10倍！
- 每台裝置會長時間、大量地上傳各種類型資料(監控影像，量測數據，使用紀錄等)
- 巨量資料將在帶來各種前所未有的應用
- 但資料正確性和真偽所帶來的問題也會日趨複雜...

資訊造假、駭客攻擊問題嚴重，資料可信度將成為關鍵

- 互不信任的年代，資料（媒體，食安，醫療糾紛，金融交易等）真實性經常性地受到質疑
- 中心化「帳房」難以取信於大眾。即便是知名公司甚至政府部門公信力都時常遭到挑戰，知名企業甚至政府部門作假風波也時有所聞
- 資料收集深入人們日常生活甚至私密領域，資料造假或濫用的風險及代價日益增加
- 各種防堵/監控/稽核手段不斷的提高交易成本
- 必須面對GDPR日益嚴格管控



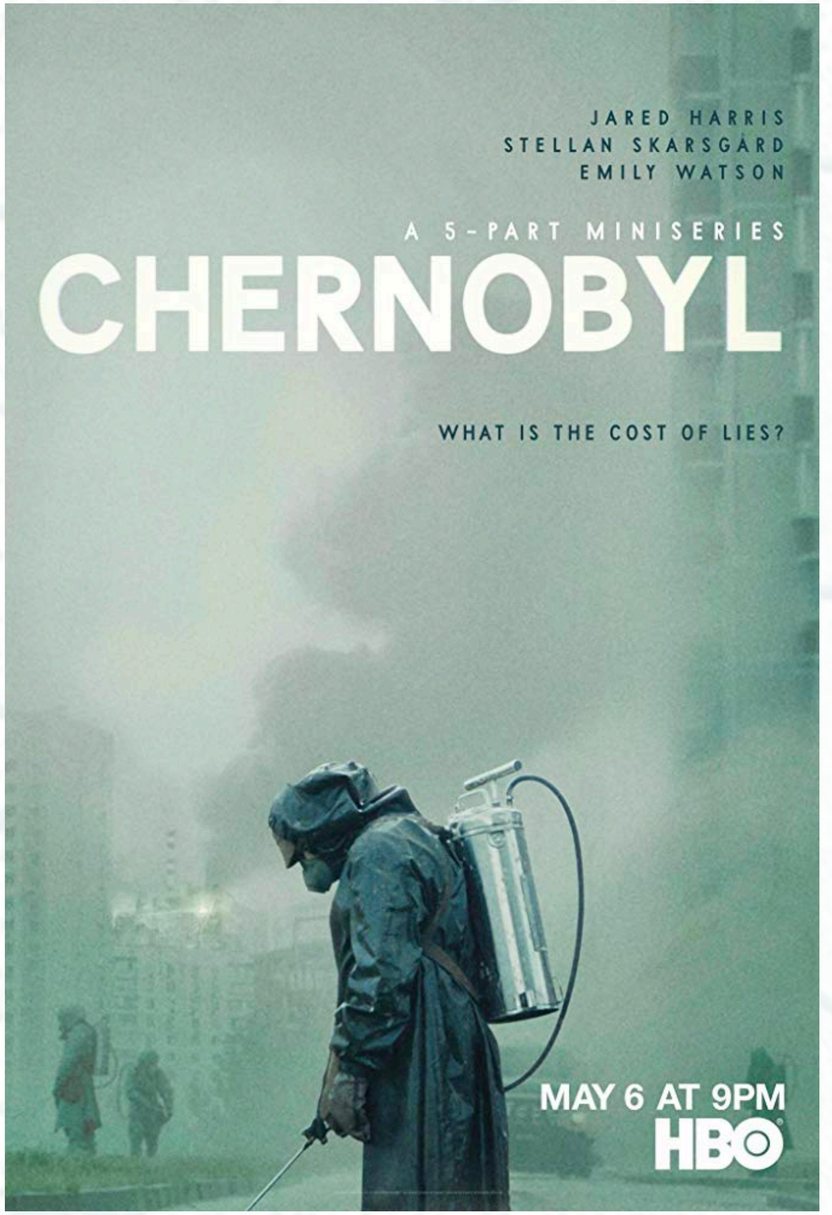
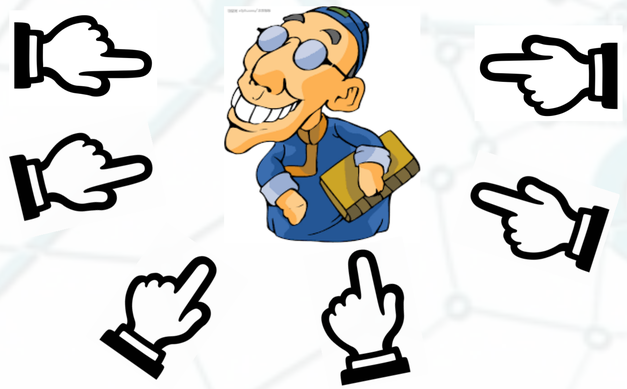


Image from https://www.imdb.com/title/tt7366338/

區塊鏈 = 分散式帳本

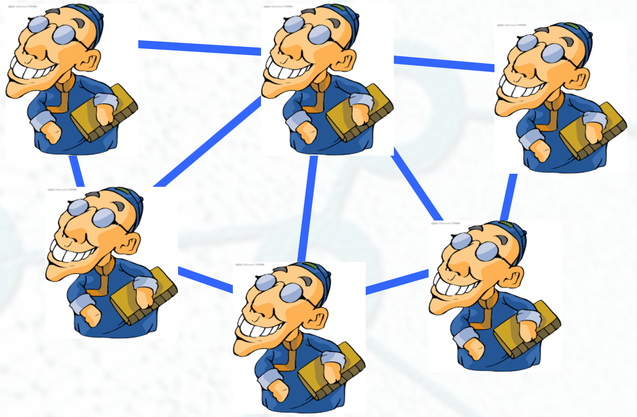
信任機制是核心價值

傳統「中心化」資料庫



1.資料由一位帳房保管，帳本只有帳房有。
2.資料多少，是否真實無竄改只有帳房知道，他人無從查。
3.帳本可以竄改。船過水無痕，買賣雙方互相猜忌。
4.經常需要「公正第三方」介入，信任成本高。

區塊鏈「去中心化」資料庫



1.人人都是帳房，每人一本帳本，隨時都可查帳。
2.每筆帳都需要所有帳房承認（共識）後才記入。
3.凡走過必留下痕跡，難以竄改。
4.不需要任何第三方認證機構或保險機制，大幅降低信任成本。

現有區塊鏈應用在物聯網的瓶頸

Scalability (擴容性)

- 目前主流公有鏈全球每秒能紀錄的資料(TPS – Transaction Per Second)不到15筆(Bitcoin = 7, Ethereum = 15)
- 全球數百億聯網裝置每分每秒不停上傳資料，根本無法處理
- 每筆資料紀錄上鏈前需要鏈上建立共識。交易時間長達數十分鐘甚至數小時
- 對於每分每秒傳送資料的IoT裝置，這種反應時間無法接受

Data privacy (資料隱私)

- 許多資料雖然牽涉信任機制(e.g., 金融/房地產交易紀錄、醫療紀錄等)，但牽涉隱私問題資料不方便紀錄上鏈讓所有人查核
- 區塊鏈的不可竄改性與資料的隱私性取捨成為兩難
- GDPR對於資料的抹除和遺忘的權力和區塊鏈上資料不可竄改的特性相互矛盾

Cost (成本)

- 每紀錄一筆資料上鏈都要付記帳費(礦工費)。以IoT資料量來計算費用將是天文數字
- IoT裝置若具備上鏈能力，其生產成本必須降低

現有解決方案難以兼顧

HYPERLEDGER

r3.

AMIS

Azure

IOTA

FILAMENT

私有鏈/聯盟鏈

- 如 IBM Hyperledger、Microsoft Azure、或其他各式自建區塊鏈
- 信任機制被犧牲 – 帳本數目有限，且可能都掌握在少數人手上
- 擴容性可能還是不夠 – 由TPS 15 提高到 TPS 數千，對於大規模應用可能還是不夠
- 沒有解決MCU Edge Device無法上鏈的問題
- 成本高

代理人機制

- 如IOTA：交易成本、交易確認時間、搜尋時間？
- 有區塊鏈膨脹及安全疑慮的問題
- 現階段沒有智能合約功能

設備上鏈機制

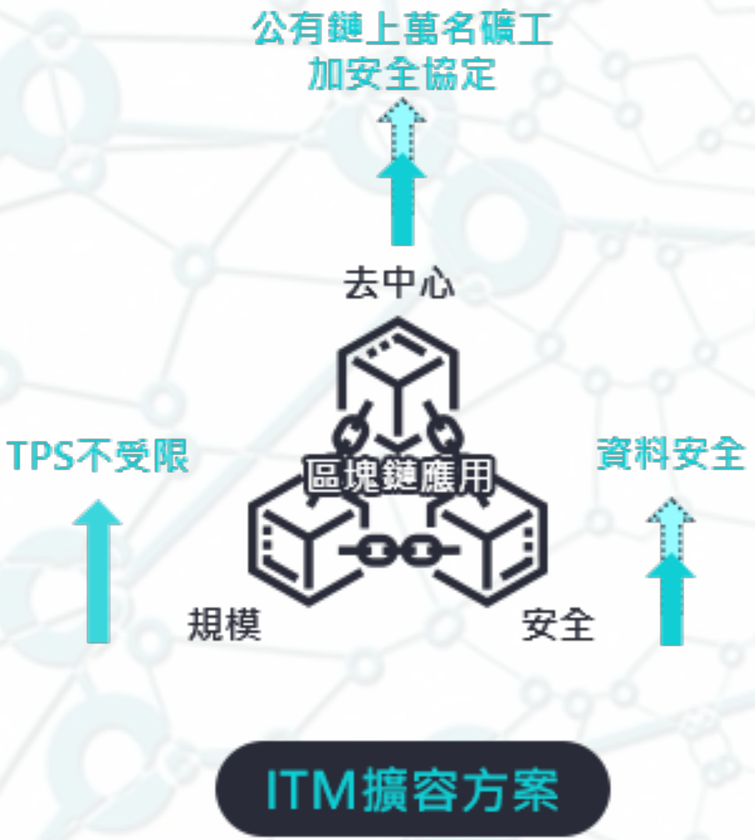
- 美國的Filament's Blocklet USB Enclave (https://filament.com)
- 區塊鏈的TPS太低且礦工費太高

10萬台裝置，每10秒產生一筆裝置資料。

每分鐘會有60萬筆資料，相當於每秒鐘1萬筆資料。

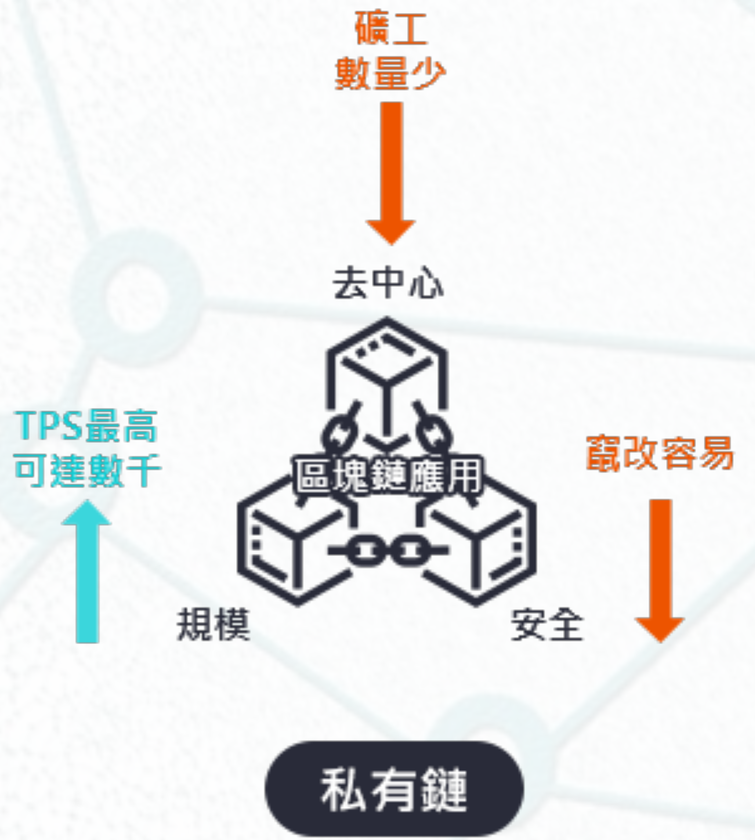
TPS = 10000

ITM突破區塊鏈三難困局



ITM擴容方案

公有區塊鏈



私有鏈

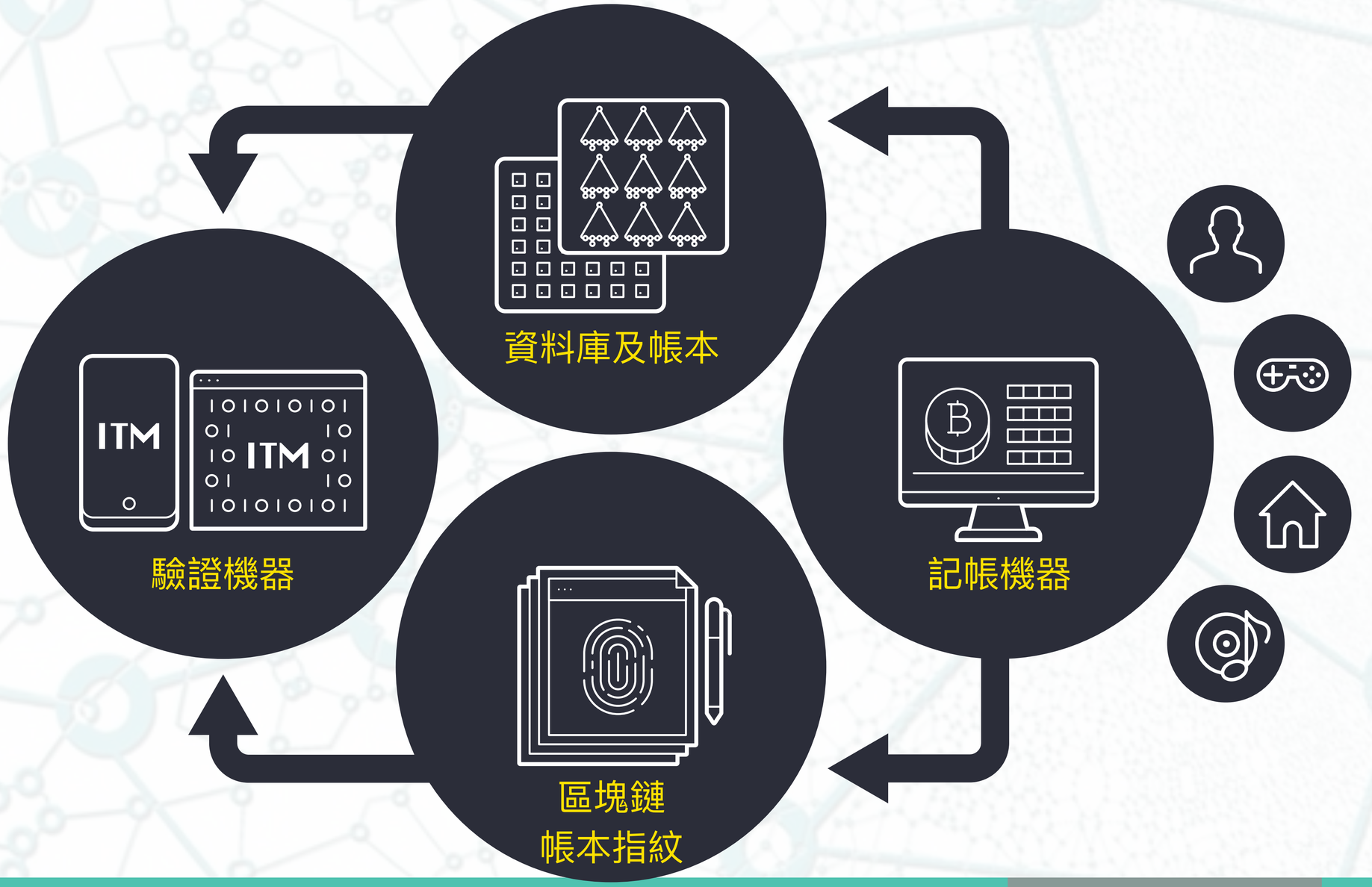
03

技術核心

ITM的核心能力

- **區塊鏈主鏈上一個交易可以用來清算鏈下一百萬筆交易，改善效率一百萬倍**
- 解決公有鏈頻寬不足與私有鏈缺乏全球共識的問題
- 架接中心式系統和去中心區塊鏈的最佳方案
- 可同步加速帳本、支付和智能合約

ITM區塊鏈解決方案



ITM特色

- 基於交易定位摩克樹的安全協定，非節點或側鏈技術 (專利申請中)。
- 由主鏈上的礦工來執行各項安全協定。
- tp摩克樹（transaction positioned - Merkle tree）支援帳本快篩 (專利申請中)。
- 具有智能合約功能的主鏈都能使用。
- 支援下列各式區塊鏈:
  - 公有鏈
  - 聯盟鏈
  - 私有鏈

ITM技術源起

- **Efficient Real-time Auditing and Proof of Violation for Cloud Storage Systems. Gwan-Hwan Hwang and Hung-Fu Chen.**

  - Accepted as a research track paper for publication in the 9th IEEE International Conference on Cloud Computing (IEEE Cloud 2016), June 27 - July 2, 2016, San Francisco, USA. Acceptance rate: 15% (This paper received the best student paper award Runner-up) (Corresponding author: Gwan-Hwan Hwang)

- **InfiniteChain: A Multi-chain Architecture with Distributed Auditing of Sidechains for Public Blockchains. Gwan-Hwan Hwang, Po-Han Chen, Chun-Hao Lu, Chun Chiu, Hsuan-Cheng Lin, and An-Jie Jheng.**

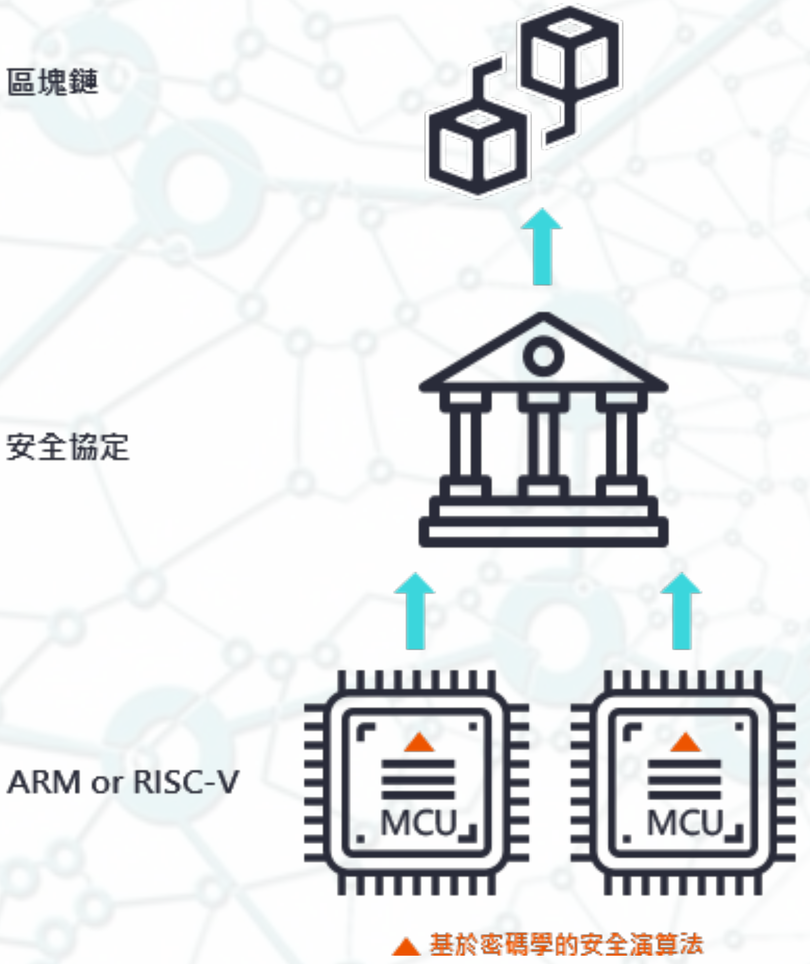
  - Accepted for publication in research track of 2018 International Conference on Blockchain (ICBC 2018), June 25 - June 30, 2018, Seattle, USA. This paper received THE BEST PAPER AWARD. (Corresponding author: Gwan-Hwan Hwang)

04

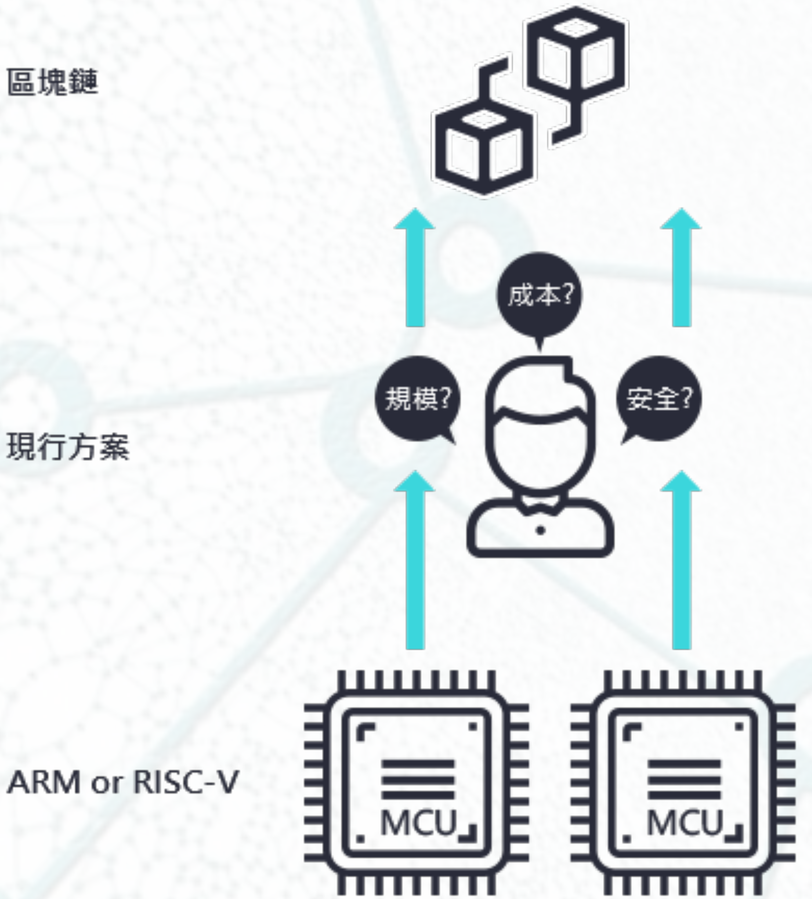
技術實現

ITM 區塊鏈 IC 架構

依照ITM的安全協定，在通行的IC中置入基於密碼學的安全演算法，
達成大量擴容、高安全、保護隱私、低成本的IoT上鏈需求。



▲ 基於密碼學的安全演算法



ITM Blockchain-enabled IC

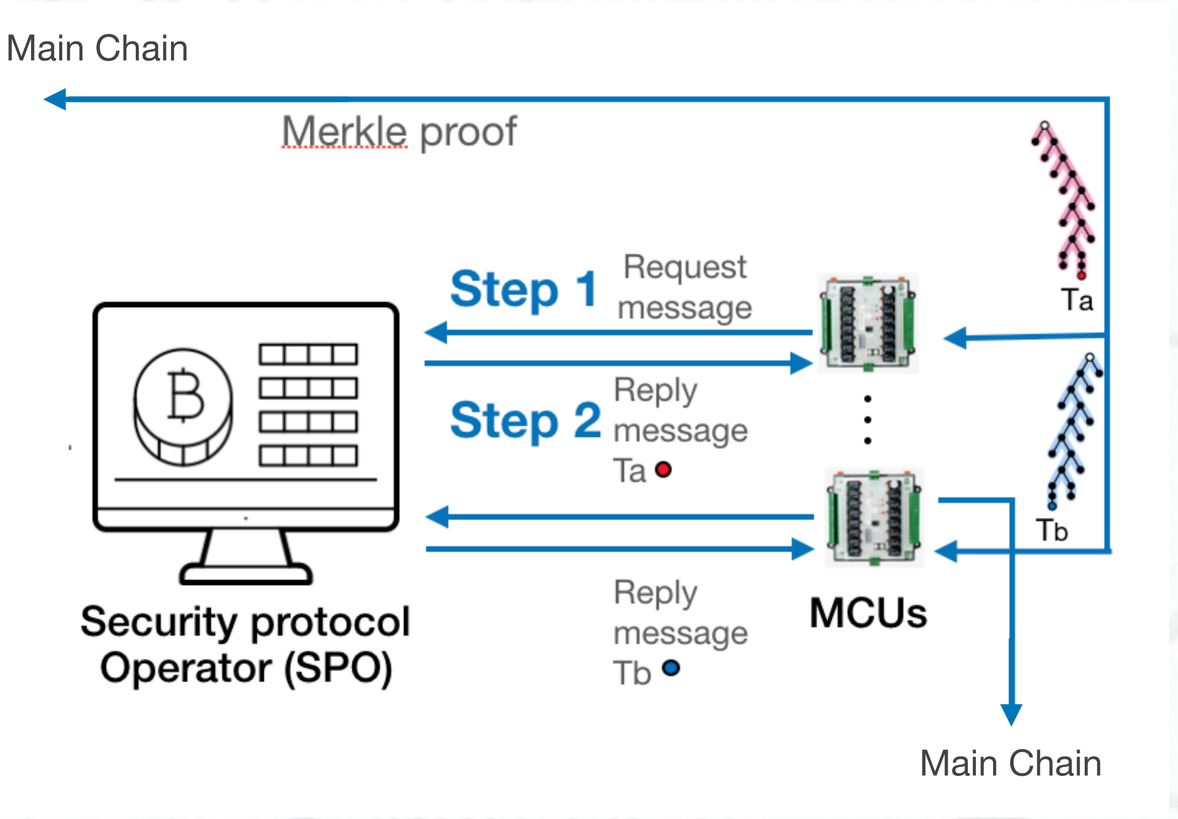
- ITM的技術可以讓晶片以最精簡的運作模式，將交易及記錄透過SPO送到公有區塊鏈並讓晶片進行稽核
- 晶片只要具備以下功能：

  (1) 電子簽章

  (2) 由TP-Merkle proof推出Root hash

  (3) 和區塊鏈節點及SPO的通訊能力

- 目前市面上的IoT晶片都可以安裝這些功能

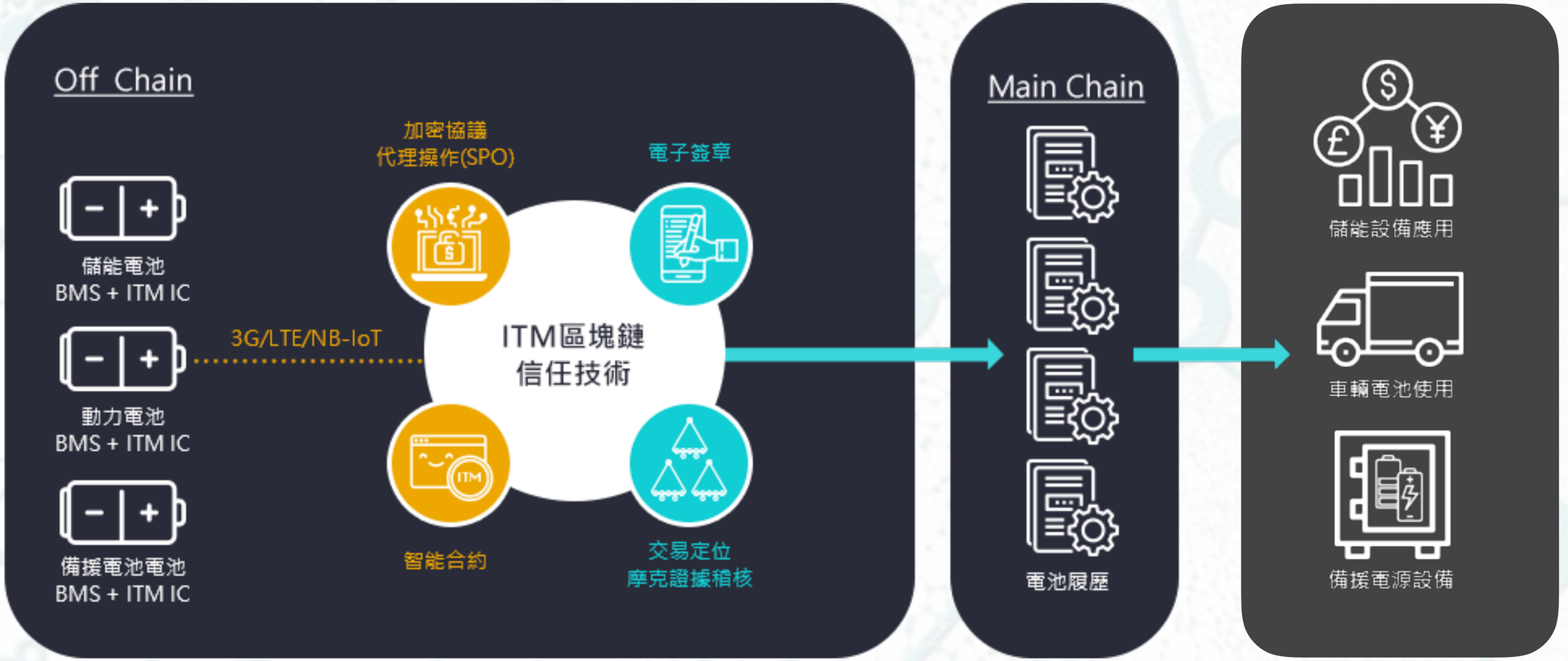


05

應用案例

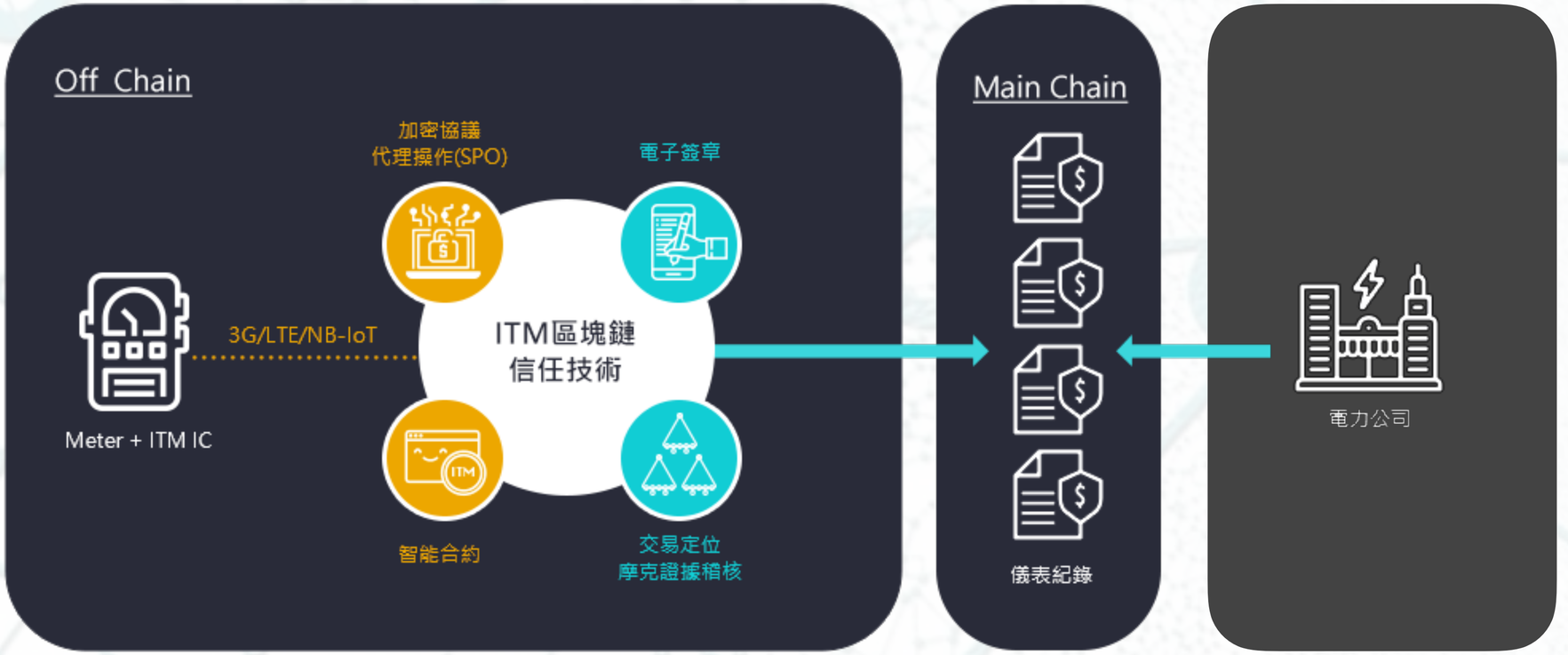
應用場景：電池履歷管理

透過ITM擴容方案及區塊鏈IC技術，建立車用大型電池的健康履歷，
建立跨國電池交易市場的公平標準，確保電池二手 三手的交易價格



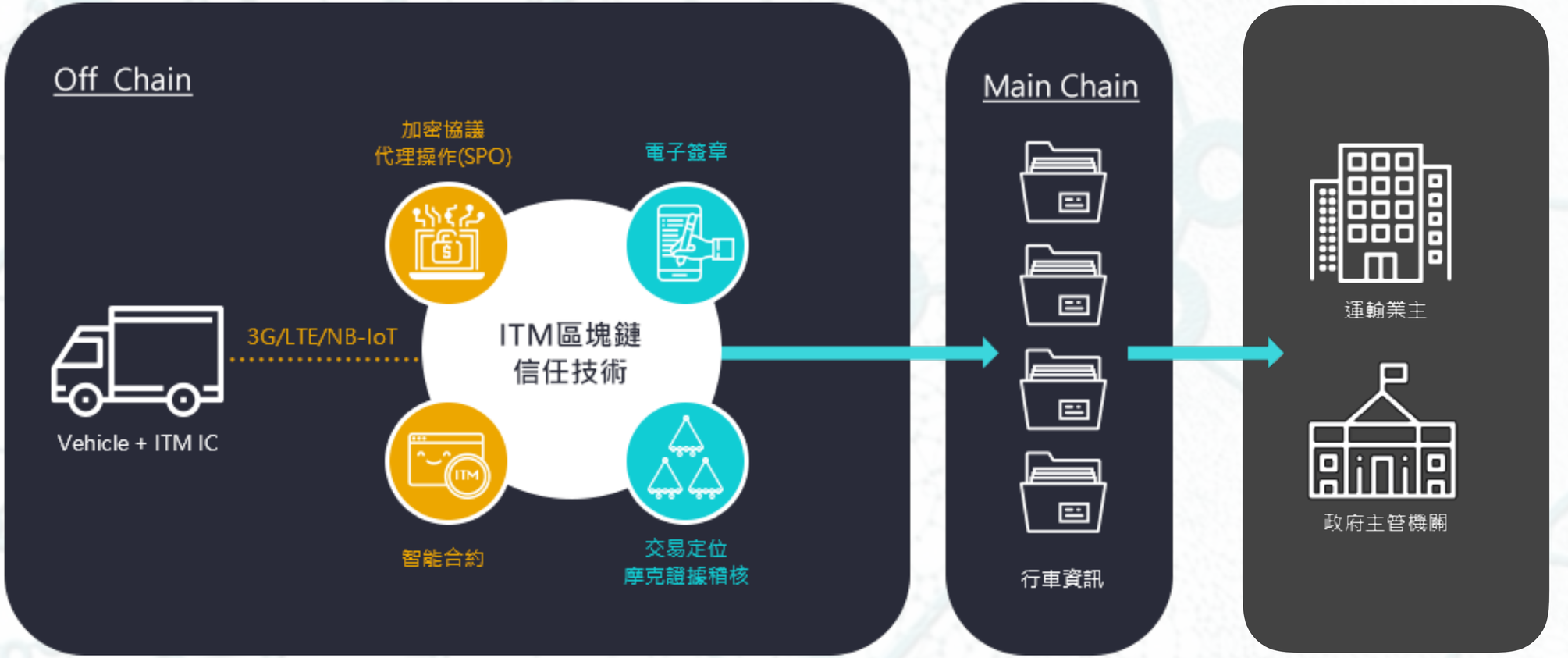
區塊鏈智慧電表

透過ITM擴容方案及區塊鏈IC技術，讓現行的智慧電表資料上鏈，確保用電資訊安全且不可篡改。
(ex: 日本富士通應用區塊鏈改善電力控管，將需量調度成功率提高40%)



區塊鏈智慧運輸

透過ITM擴容方案及區塊鏈IC技術，將行車資訊上鏈，具有公信的資料，
可以作為車隊管理，物流管理，供應鏈金融及政府監管的依據



國際信任機器股份有限公司

International Trust Machines Corporation

領先全球的區塊鏈擴容方案和區塊鏈IC推動者