

Hyperledger Fabric 第三組

組員

江羿賢 E94074029 資訊 111

林宛秀 H14061098 會計 110

陳柏劭 D54061182 經濟 110

吳佩恩 B14061263 經濟 110

張斯涵 B14051145 交管 110

Problem - 結合 IOT 與區塊鏈

將區塊鏈結合 IOT 有 5 種類型的困難：Easy Network Specification and Deployment、Rapid Business Logic Prototyping、Resource Sharing、Complex Privacy Management Support、External Interoperability and Data Federation

本論文專注於解決 Easy Network Specification and Deployment、Rapid Business Logic Prototyping，和四項要求，如圖：




 IoT requirements addressed	 Implementation directives	 End objectives
[REQ1] Effortless specification of blockchain infrastructure for existing IoT systems	Create easy, user-friendly workflows to specify blockchain infrastructures	BCaaS has an infrastructure specification component for a specific blockchain network configuration
[REQ2] Effortless blockchain infrastructure deployment	Make direct and straightforward workflows for ease of deployment of a user-specified infrastructure	BCaaS has a specifically tailored step-by-step deployment mechanism that is well-documented
[REQ4] Fast writing of complex, enterprise business logic	Creating automated processes of writing smart contracts with basic functionalities (minimum CRUD operations for digital assets)	Automated rapid prototyping of business logic in IoT
[REQ6] Automated deployment of business logic	Create blockchain-specific mechanisms for smart contract deployment	Smart contract deployment is rather effortless and semi/fully automated

Fig. 1. Hyperledger Fabric BCaaS IoT requirements addressed in this paper

REQ1 和 REQ2 是 Easy Network Specification and Deployment 類，共同目標為不費力的 HF 區塊鏈基礎設施架設及自動化佈署；REQ4 和 REQ6 是 Rapid Business Logic Prototyping 類，共同目標為利用自動工作流程和 instant-deployment 來使得「快速寫出複雜的智能合約」得以實現。

而這些要求都在解決 IoT 的關鍵困難：複雜且分布式的 IoT 裝置能夠以簡單的方式來創造或加入 HF 區塊鏈

Solution - 結合 IOT 與區塊鏈

Hyperledger Fabric Operator Modules (HFOM)

除了原本就存在的區塊鏈 layer，再建造另一層安全 layer 提供使用者、應用程式和區塊鏈基礎架設的溝通保護，

HFOM 會保存 app 憑證，直到其 access token 到期或憑證被 CA 撤回。具異步同取特性(asynchronous)。為了正確執行，需要區塊鏈網路是 yaml 形式，其被產生為 HFICG 的一部分。

為了解決 IoT 的低資源要求，HFOM 提供三種類型的佈署，分別適合不同資源來應用：

1. **有地方 HF 的全 HFOM**：此 HFOM 要求 HF peer node 被佈署在有運作 HFOM 的裝置上，因此節點間可以直間溝通而有最快的速度，其資料也都會被各節點保存，但同時需要配備最高，要至少 1Gb of RAM memory and a 1.3 GHz CPU, such as the Raspberry Pi 3B。於 Node.js 內執行。
2. **無地方 HF 的全 HFOM**：此 HFOM 連結到特定地方節點，其資料會被節點保存，需要配備較低，要至少 256Mb of RAM，如 Raspberry Pi 0, or Orange Pi 0。於 Node.js 內執行。
3. **Soft HFOM**：只連結到距離最近 HFOM (1 或 2)，經由 curl and HTTP or HTTPS 來傳送指令，適合資源有限者，如 128 Mb of RAM 以下(Onion Omega 2)。於 Node.JS, Python, and Bash 內執行。

Hyperledger Fabric Infrastructure Configuration Generator

自動化建立複雜區塊鏈網路，包含 organizations, channels, and various peer-channel connections，並給這些組成所需的實體機器。工作流程如下圖：

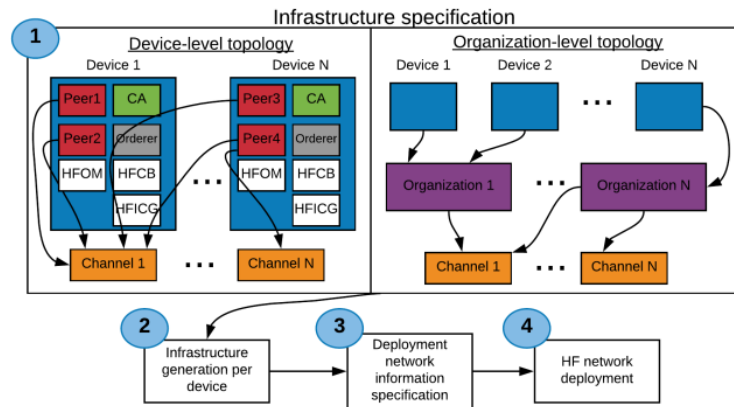


Fig. 2. Hyperledger Fabric Infrastructure Configuration Generator

步驟 1 為基礎建設是如何被規範的。HF 區塊鏈基礎建設被描述成 device-level 和 organization-level，利用 UI，可以藉由拖拉來增加 HF 和 BCaaS 組成。

產生的 HF 區塊鏈網路佈署包含：docker-compose file for the Ordering service, cryptographic material, genesis block, and a Bash startup script to bring up the Ordering service containers; docker-compose file (including: peers, state database and Certificate Authority - CA containers), cryptographic materials, channel creation and anchor peer configuration files, and a Bash startup script to bring up peers, state database and CA server configuration (including: channel creation commands, anchor peer update commands, channel join command per peer) per machine;

Hyperledger Fabric Chaincode Builder(HFCB)

完全自動建造並佈署智能合約，從描述智能合約到製造並執行都包辦在內。例如下圖中 case1，假設有應用程式想和區塊鏈互動，需要一個智能合約來處理新資料串流，可以藉由 HFCB 自動要求創造智能合約。

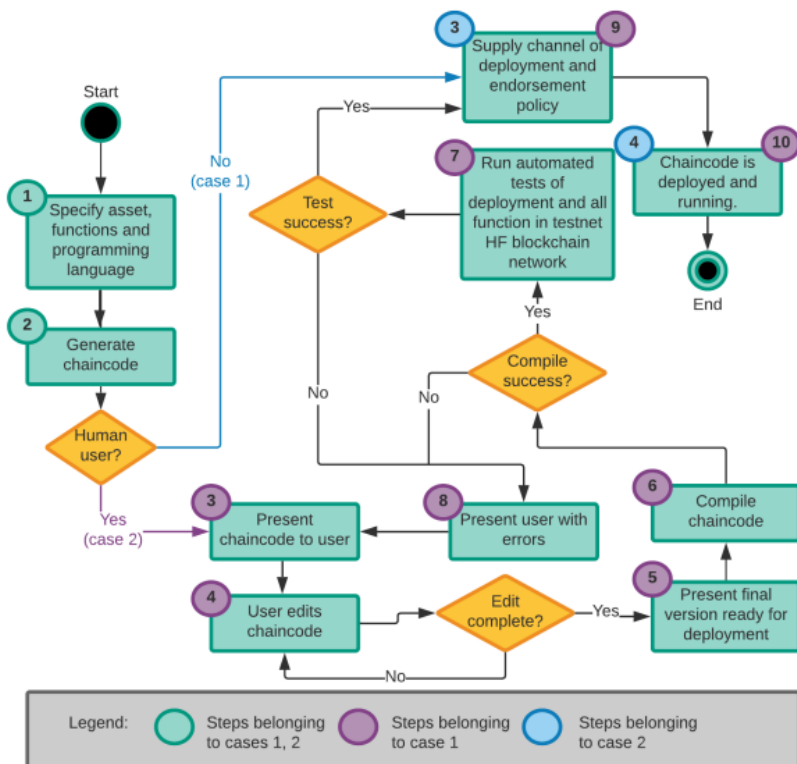


Fig. 3. Hyperledger Fabric Chaincode Builder

圖中 case2 代表，若使用者想和區塊鏈互動，程序為半自動化，可以編輯智能合約。

其他 - 結合 IOT 與區塊鏈

此解決方案已經在 3 個 IoT 佈署中實際執行：Agile IoT platform, the Arizona State University Blockchain Research Laboratory Carbon trading IoT platform, Asset Tracking fog computing solution。在執行期間，已產生 50 個不同複雜度 HF infrastructure configuration、150 智能合約 → 此解決方法已被證實為可行，而非只是紙上談兵。

Problem - 要使用何種網路協議及區塊鏈架構來實現有效並安全的 IoT 設備上來做使用

在 IoT 的設備端中，所需的要求有很多，並且有部分困難之處。首先在網路協定的部分需要能夠正常的通訊並且要能夠有儲存數據的功能並且在這之中還要節能，其中數據需要有 all-data all-the-time-connected(ADAT2C)的特

性，來確保說在 IoT 的終端設備中可以確實的更新資料並且也能夠達到最低限度的即時性。而在安全性的部分中則要讓設備有不同的權限提供設定，也要能夠確保資料不被更動，也要具有能夠檢測出異常並且隔離的能力。

Solution- 用 LoRaWan-Hyperledger robust network integrity on IoT devices 來實現

LoRaWan 提供了 IoT 的終端設備 node 以及安全性，而 Hyperledger 提供了權限策略並且不能被更改的帳本系統以及檢測異常等功能。

Hyperledger Fabric 架構

一種 DLT 的技術，利用去中心化的數據架構來使點對點網路同步一致性，可以達到讓交易紀錄不可被改變的功能，而其中的 Hyperledger Fabric 是一種通道支持許可的方式，透過給那些對等節點 certificate authority，來使在一個系統中，可以有多個通道以及節點來透過 Hyperledger Fabric 這個平台，透過一連串的步驟來完成交易，並且 Hyperledger Fabric 可以連線到 REST server 來做查詢，可以利用 Passport 來確認身分來使其訪問能夠訪問的地方。下圖是 Hyperledger Fabric 的架構圖：

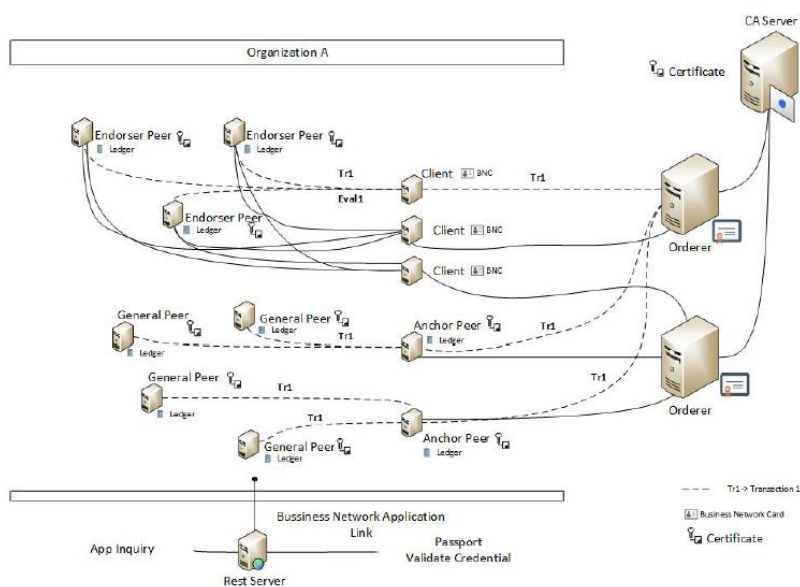


Figure 1. Hyperledger Fabric architecture for one channel

LoRaWan 架構

LoRa 是一種從 CSS 而來的 spread spectrum modulation 技術，是基於 LoRaWan 這種低功耗的協議，能夠在分配到的頻段上使用盡可能少的功率來傳輸數據，也有著一定的安全性，並且可以利用 OTAA 或者是 ABP 來 activation，並利用 AES-128key 來作為憑證，並一起發送 DevAddr 以及 NetID 以達到同步的效果，透過此種方式能達到良好的效果。下圖是 LoRaWan 的架構圖：

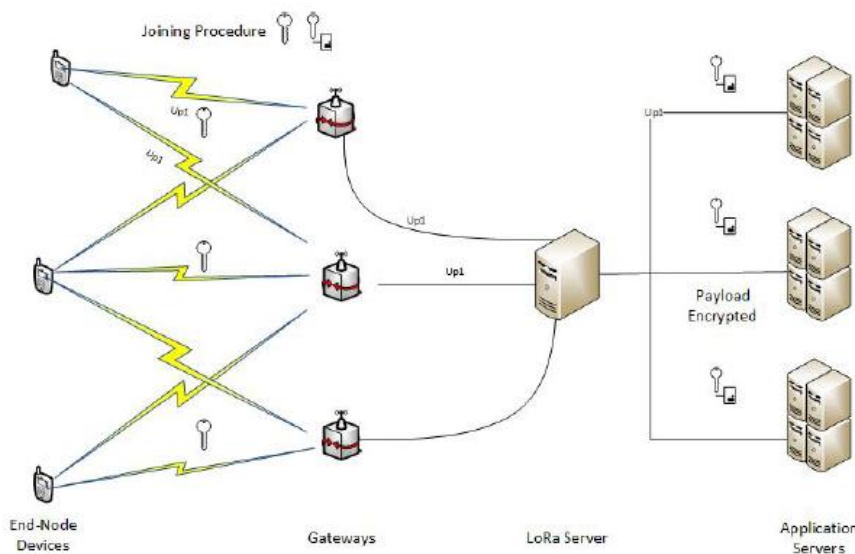


Figure 2 LoRaWan architecture

LoRaWan-Hyperledger 架構

透過 LoRaWan 與 Hyperledger Fabric 的結合可達到安全、身分管理、數據蒐集、數據歷史、數據儲存、高效能的目的，混合架構的 LoRaWan 可以做為 endorsement、anchor 以及 Hyperledger Fabric 網路上的對等點，而對設備來說也有一個最低限度的要求，LoRa server 也可以做為 Hyperledger Fabric 的 client，可以在 LoRa server 上先註冊之後再交 proposal 給 endorsement，之後再將其傳給 Orderer。

而這邊也提供給每個人一個 Certificate，安全度以及可信度已經受到保證，LoRaWan 以及 Hyperledger Fabric 的結合是非常強大的，而終端的節點每天都會發送 certificates，LoRa server 提供這一些資料給 Hyperledger Fabric 來做驗證，就可以將交易 submit 到 Hyperledger Fabric 上。

而在 Replica attack defense 的部分，利用看每個終端節點的時間來去評估這個傳入交易中的是惡意與否，會看他的驗證時間，如果異常的話會進到隔離通道確認。

下圖是 LoRaWan-Hyperledger 的架構:

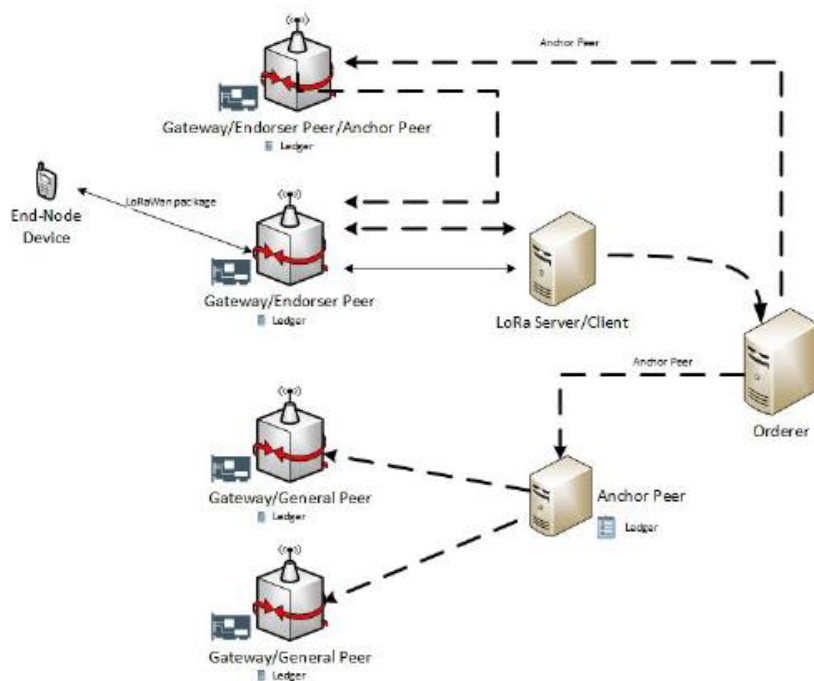


Figure 3, LoRaWAN-Hyperledger hybrid network

結論

透過 LoRaWan-Hyperledger Fabric 的這種架構提高了資源的使用效能以及安全性，也能夠檢測到異常狀態並且提供隔離通道來進行驗證，系統的可行性也得到了證明。

其他- 自行補充內容

在這邊上面所述的 LoRaWan 有非常好的安全機制以及低功耗，不過有一些缺點是傳輸速率較慢以及通訊的頻段會容易受到干擾，其中在目前的技術中也有其他的網路架構也有些類似的功能，不過就並不是太專用於 IoT 以及區塊鏈中。這邊我想要補充的是 Named Data Networking(NDN)，在現在 IP 有可能會不夠用的時候，NDN 算是一個能夠解決這個問題的方式，且能夠專注於所需的內容，也具有安全性，NDN 可以透過 producer 來對每個 packet 簽名，從中就可以得知資料來源，也有支援 fine-grained 可以知道到底能不能信任，也可以透過 SDSI 來做更多的

驗證，讓資料和密鑰是可以獨立的，而透過使用多路徑的轉發可以去偵測其 prefix 看有沒有異常現象，所以很難針對特定的 NDN 進行攻擊。而關於其中傳遞的封包的東西可以看 Content-Centric networking(CCN)，其中有兩種封包分別是 data packet 跟 interest packet，其中的 table 有 PS、PIT、CS、FIB，可以透過改善一些 replacement policy 來去讓 hit rate 提升，其中轉發的部分是一個關鍵，且 CS 和 FIB 之中的剔除方式也是一大關鍵，之前和同學有嘗試過在單一台電腦中模擬過小的架構，有嘗試過在 CS 中使用 LRU 等 policy，後來有再嘗試先利用 DFS 算法來去獲取距離表，再來依照最遠的 router 資料來進行剔除，效果還不錯，FIB 目前還尚未嘗試優化過，而在 data queue 以及 interest queue 有嘗試使用的是 aging，來去針對 hop 的大小來去做剔除。不過這個都是在單一電腦上模擬的，可能要再更深入一點到有一個架構的模型才能夠真正知道在真實世界中甚麼樣的轉發以及傳送的效率以及 hitrate 會最好。不過這項技術目前具我自己所知應該是尚未到非常普及，離要與 IoT 以及區塊鏈技術結合可能還遙遙無期，不過我認為這個 NDN 以及 CCN 的技術是有淺力的，說不定會有在 IoT 以及區塊鏈的領域中有意想不到的應用。

Problem - 面對 IoT 大量資料上鏈所產生之擴容性問題

IoT 最吸引人的應用之一，是要求分散式裝置之間能夠彼此互動，無須經由中央服務進行協調。這一類系統通常還要求記錄這些活動，以便進行監督或管理，而區塊鏈正好提供了讓系統可在多個位置同步建立此類紀錄的機制，同時還有保持其一致的防篡改特性，並可以透過智慧合約機制來支援裝置間的條件是互動，因此被視為是釋放物聯網潛力的關鍵之一。

然而，想要整合區塊鏈和物聯網，其中一個問題便是「如何讓龐大的資料上鏈」。面對 IoT 所產生數千筆交易資料要上鏈時，可能因為運算資源不足等原因，造成 TPS (transaction per second)降低或是 latency(延遲時間)增加，降低了性能。

Solution - 引進 Accelerator，利用其 Multi-batch

Scheduling 改善性能

為了改善 blockchain-based IoT application 的性能，論文中引進 Accelerator 這項新的交易處理機制，並衡量出

TPS 在不犧牲 latency 的情況下，利用 Accelerator 能夠比沒有利用時增加 8 倍。

Accelerator 介紹及其運作

Accelerator 將可以在不改變 consensus algorithm 的情況下提升效能，其有 2 項特點:

1. 獨立模組化的結構：

Accelerator 將在 client 和 blockchain network 中間進行作業，解決 IoT 遠端設備可能沒有足夠運算能力去多跑改善效能的 process 的問題。

2. 多批適性排程引擎(Adaptive multi-batch scheduling engine)：

Accelerator 提供一項簡單卻有用的 transaction process algorithm，依據交易的性質及剩餘的運算資源，決定最適的 batch size，將大量的 transaction 打包成多個 batch 後再上鏈，進而增加處理效能。



Fig. 1. Overall structure of Fabric network with Accelerator

以下為運作的示意圖：

並透過記錄不同程序下的 TPS，找到瓶頸所在以及觀察 Accelerator 如何影響改善。

T1 - from Caliper to Accelerator

T2 - from Accelerator to endorser

T3 - from endorsers to Accelerator

T4 - from Accelerator to orderer

T5 - from validating peer to Accelerator

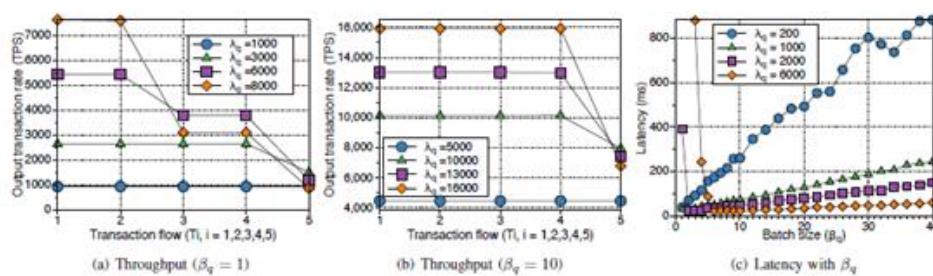


Fig. 5. Impact of Accelerator on throughput and latency

可以發現瓶頸來自 endorsement 以及 validation 兩個流程，因為缺乏計算資源。而在透過 Accelerator 的 Multi-batch Scheduling 後，有效解決 endorsement 流程運算上的瓶頸，validation 流程上的效能也有效地改善。

補充

除了 Accelerator Multi-batch Scheduling 的技術可以改善 IoT 上鏈時擴容性的問題外，台灣 ITM 國際信任機器團隊善用台灣 IC 產業優勢，研發的摩克樹技術及摩克樹帳本快搜技術 IC 化。其透過密碼學技術將 100 萬筆的資料量濃縮成 32 位元的「指紋」，再將指紋放在以太坊或其他區塊鏈上，由於只將 32 位元的指紋放置於區塊鏈上，因此解決了過去資料上公有鏈必然會出現的擴容與隨之而來的成本這兩大問題。

另一方面不可竄改的只有區塊鏈上的指紋，後方的資料只要通過指紋驗證，仍然可被修改，這也就可符合 GDPR 規範中的被遺忘權。

此外，將交易及記錄透過 SPO(Security Protocol Operator)送到公有區塊鏈並讓晶片進行稽核，藉由嘗試「區塊鏈 IC」，達成大量擴容、高安全、保護隱私、低成本的 IoT 上鏈需求！