區塊鏈技術在智慧家庭數據應用現況與問題探討

成果報告

內政部建築研究所自行研究報告

中華民國 110 年 12 月

PR11012-0101

區塊鏈技術在智慧家庭數據應用現況與問題探討

成果報告

研究人員：林谷陶

內政部建築研究所自行研究報告

中華民國 110 年 12 月

ARCHITECTURE AND BUILDING RESEARCH INSTITUTE, MINISTRY OF THE INTERIOR

RESEARCH PROJECT REPORT

Blockchain Technology Application Issues of Smart Home Data

BY

KU-TAO LIN

December 2021

目　次

表　次

圖　次

摘　要

關鍵詞：區塊鏈、智慧家庭、社會住宅

我國 ICT 產業優勢推動智慧化居住空間科技，及政府推動「數位國家・創新經濟發展方案（106-114 年）」、「台灣 AI 行動計畫(107 至 110 年)」、政府開放資料深化應用等政策，為促進智慧化居住空間與人工智慧、物聯網及大數據分析等技術之整合，在建築物內導入智慧化相關系統及設備，以達到安全健康、便利舒適、節能永續之目的；本所歷年推動智慧建築也因應此一趨勢推動「智慧化居住空間整合應用人工智慧發展推廣計畫」，構思如何應用在智慧化居住空間中產生大的量數據分析，提升智慧化程度。

由於傳統智慧家庭、智慧建築的各種感測器、設備、系統的資訊，在 IoT 物聯網浪潮下，智慧家庭是民眾最有感發展，可能上到智慧社區、智慧城市與各種屬性不同的應用如智慧交通、遠距照護等等，產生更擴大的創新應用。然而，前述智慧家庭的這些設備應用的安全性差異很大，使用者不清楚對隱私的影響。因此，藉由持續探討區塊鏈技術，借鑒國外如何在智慧家庭的應用日益普及情形下，確保使用者數據的透明性，安全性和隱私性需求；及探討數據收集及交易模型，以鼓勵數據分享並創造新的建築價值鏈。

本報告主要是以文獻收集，回顧國內外有關區塊鏈技術內容、演進，與大數據人工智慧、智慧建築及相關產業應用案例之相關期刊論文、報告等，並搜尋目前國內外智慧家庭數據應用現況與問題，如門禁、健康照護、智慧家電、節能管理等數據產出之隱私安全進行探討，及區塊鏈可能的應用情境，初步了解區塊鏈在我國智慧建築基礎單位智慧家庭導入可能性，及數據共享應用的激勵機制，提供國內發展智慧家庭發展參考。

本案報告探討了解研究及產業有關區塊鏈保護智慧家庭隱私與數據安全、共享的網路架構，及保護智慧家庭數據隱私與數據安全可能的區塊鏈技術、建議社會住宅或公共住宅等智慧家庭數據應用區塊鏈架構、流程，並說明共享數據的獎勵機制，並儘可能彙整說明建築數位轉型、智慧城市、智慧家庭等應用區塊鏈趨勢與內容。

短期建議

建議一：尋找場域以初步進行智慧家庭物聯網環境結合區塊鏈數據分享應用實驗，驗證並示範其可行性，以促進智慧家庭數據分享並創新產業應用。

執行單位：內政部建築研究所

長期建議

建議二：探討歐盟智慧城市燈塔計畫之正能源建築及區塊鏈應用策略，觀察探討歐盟+CityxChange 計畫 IOTA tangle 技術結合其他建築科技，以借鏡中其應用的策略與方法，進一步提升我國淨零耗能建築技術。

執行單位：內政部建築研究所

Abstract

Keywords: blockchain、smart home、social housing

Due to the information of various sensors, equipment, and systems of traditional smart homes and smart buildings, under the wave of IoT, smart homes are the most felt development for the people, and may be applied to smart communities, smart cities, and various applications with different attributes, such as Smart transportation, remote care, etc., produce more expanded innovative applications. However, the security of these device applications in the smart home is very different, and users are not clear about the impact on privacy. Therefore, by continuing to explore blockchain technology, learn how to ensure the transparency, security and privacy of user data in the case of the increasing popularity of smart home applications in foreign countries; and explore data collection and transaction models to encourage Data sharing and creation of a new construction value chain.

This report is mainly based on literature collection, reviewing the content and evolution of blockchain technology at home and abroad, and related journal articles and reports on big data artificial intelligence, smart construction and related industry application cases, and searching for current domestic and foreign smart home data applications Current status and issues, such as privacy and security of data output such as access control, health care, smart home appliances, energy-saving management, etc., and possible application scenarios of blockchain, and a preliminary understanding of the possibility of blockchain in smart homes, the basic unit of smart buildings in my country , And the incentive mechanism for data sharing applications, to provide a reference for the development of domestic smart home development.

第一章 緒　論

第一節 研究緣起與背景

我國 ICT 產業優勢推動智慧化居住空間科技，及政府推動「數位國家・創新經濟發展方案（106-114 年）」、「台灣 AI 行動計畫(107 至 110 年)」、政府開放資料深化應用等政策，為促進智慧化居住空間與人工智慧、物聯網及大數據分析等技術之整合，在建築物內導入智慧化相關系統及設備，以達到安全健康、便利舒適、節能永續之目的；本所歷年推動智慧建築也因應此一趨勢推動「智慧化居住空間整合應用人工智慧發展推廣計畫」，構思如何應用在智慧化居住空間中產生大的量數據分析，提升智慧化程度；此外，希望促進智慧建築資料開放分享，整合人工智慧、物聯網，及新興資訊科技，發掘智慧建築安全安心、健康照護、便利舒適及節能永續之創新技術及解決方案，以擴大智慧生活服務，提升居住品質。

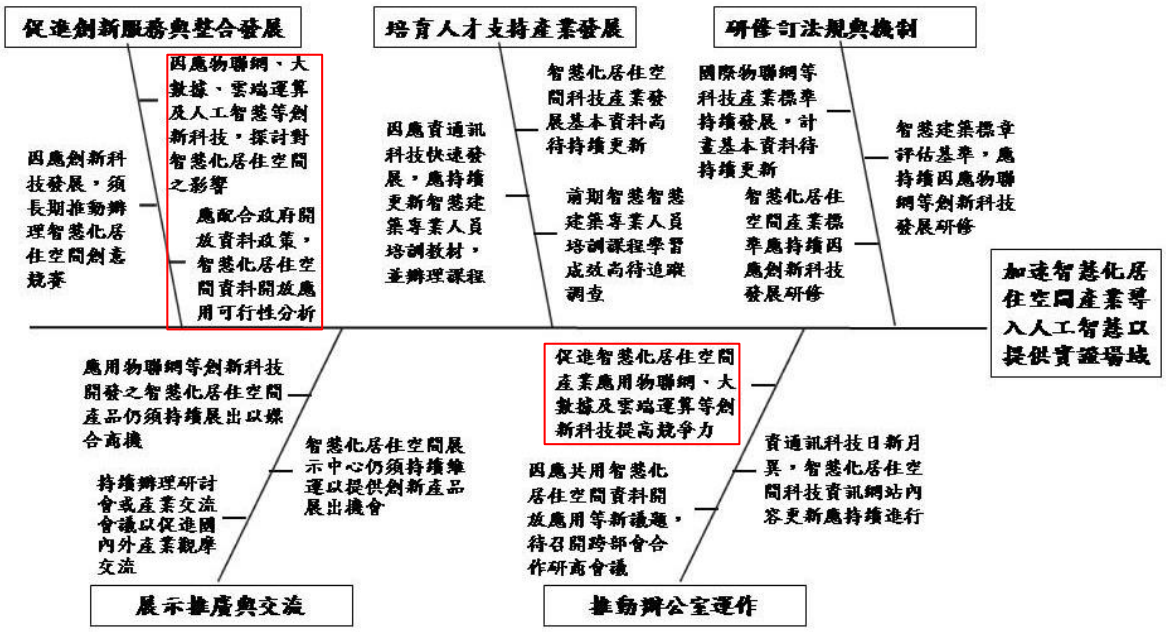


圖 1-1 「智慧化居住空間整合應用人工智慧發展推廣計畫」關聯圖

資料來源：內政部建築研究所「智慧化居住空間整合應用人工智慧發展推廣計畫(3/4)」

本案延續 108、109 年自行研究案「我國與日本推動智慧家庭數據應用環境政策比較研究」、「區塊鏈技術及營建產業應用案例探討」探討建築產業相關智慧化數據應用問題，初步了國外對智慧家庭數據應用的重視情形[1]，及區塊鏈技術、架構與在營建產業應用探討，瞭解到我國營建產業必須學習其他產業進

行數位轉型，引進先進國家非常關注的先進科技來提高計畫生產率；且唯有重新構思實體與資訊數據流程以提高資訊透明度，並提高產業對工作產品的可追溯性和可問責性的方法--需要思考導入區塊鏈，重新建構營建產業利益相關者之間的信任機制[2]。

第二節 研究目的

由於傳統智慧家庭、智慧建築的各種感測器、設備、系統的資訊，大多在所屬空間內的網路系統中傳遞，互動整合應用。但自從物聯網深入、擴大應用之後，據估計，智慧家用電器從燈泡和門鎖到電源開關和煙霧報警器，正在迅速出現在市場上，預計未來四年內將安裝超過 20 億台設備[3]，又根據 Harbor Research 的調查，2020 年全球智慧聯網產值將可達到 1 兆美元規模，智慧家庭就占四成，將迎來產業期待的龐大商機[4]。

前述各種感測器、設備、系統的所有資訊，在 IoT 物聯網浪潮下，智慧家庭是民眾最有感發展，可能上到智慧社區、智慧城市與各種屬性不同的應用如智慧交通、遠距照護等等，產生更擴大的創新應用。然而，前述智慧家庭的這些設備應用的安全性差異很大，使用者不清楚對隱私的影響。因此，本年度期望藉由持續探討區塊鏈技術，如何在智慧家庭的應用日益普及情形下，確保使用者數據的透明性，安全性和隱私性需求；及探討數據收集及交易模型，以鼓勵數據分享並創造新的建築價值鏈。

第三節 研究內容與方法

本報告主要是以文獻收集，回顧國內外有關區塊鏈技術內容、演進，與大數據人工智慧、智慧建築及相關產業應用案例之相關期刊論文、報告等，並搜尋目前國內外智慧家庭數據應用現況與問題，如門禁、健康照護、智慧家電、節能管理等數據產出之隱私安全進行探討，及區塊鏈可能的應用情境，初步了解區塊鏈在我國智慧建築基礎單位智慧家庭導入可能性，及數據共享應用的激勵機制，提供國內發展智慧家庭發展參考。

探討彙整出區塊鏈保護智慧家庭隱私與數據安全、共享的情境、網路架構；了解保護智慧家庭數據隱私與數據安全可能的區塊鏈技術、建議社會住宅或公

共住宅等智慧家庭數據應用區塊鏈共享數據的獎勵機制；及收集彙整區塊鏈與隱私法規的問題與可能權衡方向，建議，並儘可能彙整說明建築數位轉型、智慧城市、智慧家庭等應用區塊鏈趨勢與內容。

第二章 區塊鏈技術

區塊鏈是一種分散式數位帳本技術，它以安全、透明、防拆封(防篡改)，防破壞(防篡改)、分散式(即沒有集中的權限)、高效率且低成本方式的記錄交易。區塊鏈是比特幣和其他加密貨幣的基礎技術，自 2009 年比特幣問世以來而廣為人知。如今，區塊鏈的採用已遠遠超過加密貨幣，包括金融、保險、電信和醫療照護領域的應用。

第一節 區塊鏈原理與演進

相關區塊鏈原理與技術簡述如下,(本報告去 2020 年的研究[2]已曾詳細彙整相關文獻詳細說明，敬請參閱)。

一、區塊鏈原理

區塊鏈是一種數位帳本,由包含"提交區塊鏈網路已經驗證的真實交易清單"的區塊所組成。區塊鏈中的每個區塊都有一個區塊頭，由雜湊根(即儲存交易的區塊數據列表的雜湊摘要)、時間戳、上一區塊的雜湊摘要(區塊鏈的第一個區塊除外)和隨機值組成。由於每個塊標頭都具有前一個塊標頭的雜湊摘要，因此，更改區塊的將導致以下所有區塊中的不一致。因此，很容易檢測和拒絕任何先前已發布區塊的變更。

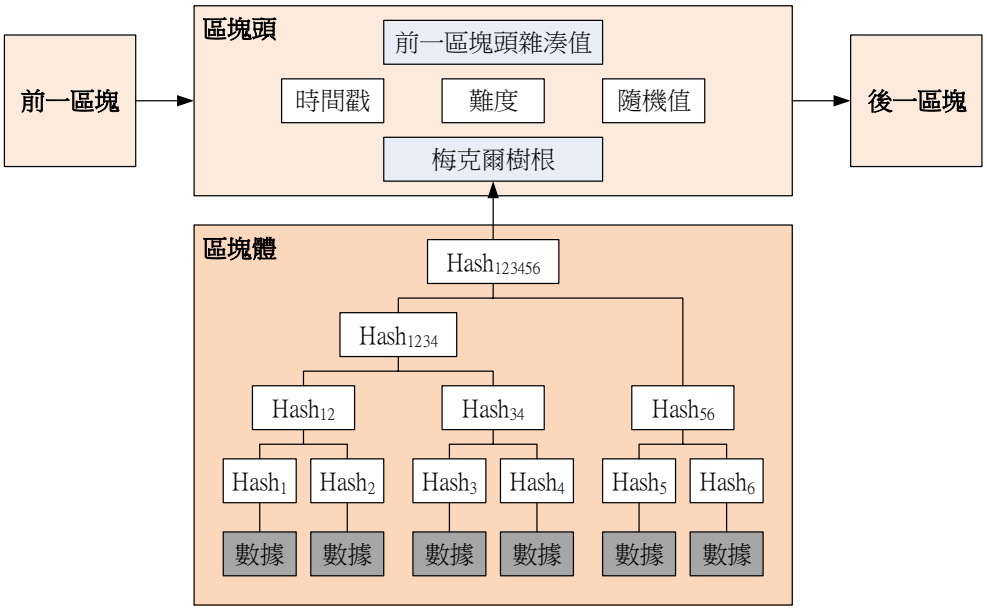


圖 2-1 樣本區塊鏈結構

資料來源：林谷陶，區塊鏈技術及營建產業應用案例探討，內政部建築研究所，2020.

圖 2-1 顯示了樣本區塊鏈的一般表示。美國國家標準暨技術研究院(NIST)將區塊鏈機制定義為:"區塊鏈是將加密簽名交易分組為多個區塊的分散式數位帳本。每個區塊在驗證並經過共識決定後都與上一個區塊進行加密鏈接。每當添加了新區塊，舊的區塊變得更加難以修改。新區塊將複製在網路內的所有帳本副本中，而所有不一致都將使用已建立的規則自動解決"[5]。

區塊鏈架構的另一個關鍵特徵是擁有分散式網路，而不是中心化或去中心化網路。在中心化網路中，網路參與者需要一個中央管理機構來相互通訊。去中心化網路具有多個管理機構，這些管理機構作為參與者次群組的中心化集線器。去中心化網路的參與者可以通過所屬集線器與其他人進行通訊。分散式網路比中心化和去中心化網路更靈活，它允許每個參與者在不需要中心點的情況下與其他人進行通訊(圖 2-2)。區塊鏈網路中的每個完整節點都保留了整個區塊鏈的副本，以確保交易的有效性。

圖 2-2 不同類型的網路的組織結構

(a)中心化網路，(b)去中心化網路，(c)分散式網路。

資料來源：Tatar, U., Y. Gokce, and B. Nussbaum, Law versus technology: Blockchain, GDPR, and tough tradeoffs. Computer Law & Security Review, 2020.

基本上，區塊鏈可說就是去中心化交易的分散式記錄或"帳本"，並利用加密技術並按時間順序儲存，等於是永久且幾乎不可更改的方式存儲交易紀錄。區塊鏈整合著各種資訊核心技術共同建構，其網路採取的演算法促進了去中心化共識、應用於交易驗證，並且寫入公共帳本(通常是分散的、不由中央機構(例如銀行或政府)管理)，並且一旦發布，就無法更改區塊鏈上的資訊。

二、區塊鏈的演進

目前區塊鏈主要分公共(或稱公有)及私有區塊鏈二種類型，其特性如圖 2-3 所示，其中私有鏈有時會再分出稱為聯盟鏈的類型。公共區塊鏈是指網路

中的任何人都可以非經許可即參與其中(例如：比特幣網路，以太坊)；而私有或聯盟鏈則必須經許可參與網路(例如：Hyperledger Fabric, Corda)，其中參與者是已知的，例如供應鏈中的相關業者。

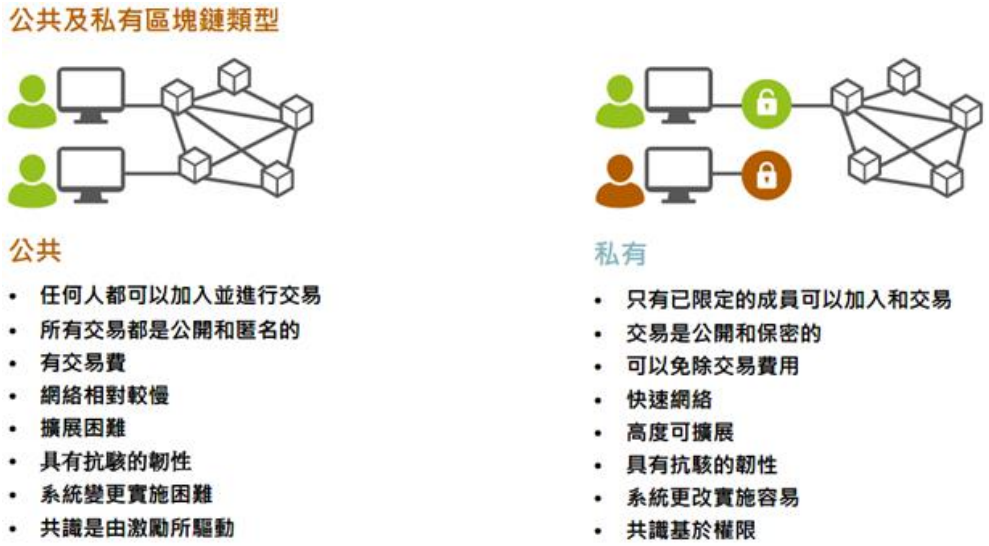


圖 2-3 區塊鏈基本分類特性

資料來源：林谷陶，區塊鏈技術及營建產業應用案例探討，內政部建築研究所，2020.

二種類型關鍵區別在於，公共網路需要激勵參與者共同運行網路並驗證交易。例如，以比特幣區塊鏈來說，每個節點必須付出電腦運算能力，以競爭驗證新交易並將其添加到區塊鏈中的機會。因為一旦每個新區塊都完成並廣播到網路成為區塊鏈，實施新塊的節點將獲得新的比特幣以及交易費用的獎勵。此過程也稱為"採礦"，其中在驗證過程中會創建新的比特幣。

由於網路是公共的，任何人都可以參與其中，因此還需要高度分散化，這使得網路可以高度靈活地抵禦駭客攻擊，但是相對較慢且難以實施整個系統更改。相反地，許可制私有網路是更為集中式的解決方案，就此網路治理的意義上來說,是由網路成員(節點)所共同驅動(這些成員是網路中已知的和經過驗證的參與者)。如此，可以參與者的業務關係為基礎來激勵參與者保持網路正常運行，而不用採取獎勵措施。

由於物聯網圖 2-4 所產生的大量數據已非比特幣的所構成區塊鏈網路所能處理，因此有各式各樣以比特幣原始區塊鏈為基礎，新的區塊鏈類型產生，主要分為三個演進世代，如圖 2-5。

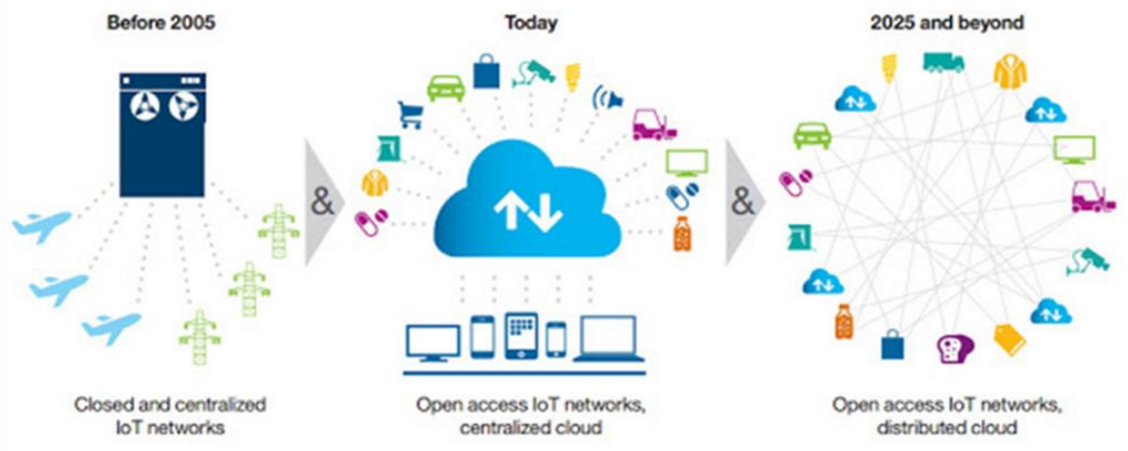


圖 2-4 區塊鏈結合物聯網是天作之合

資料來源：國家實驗研究院科技政策研究與資訊中心，"區塊鏈結合物聯網是天作之合？, 2017/12/11

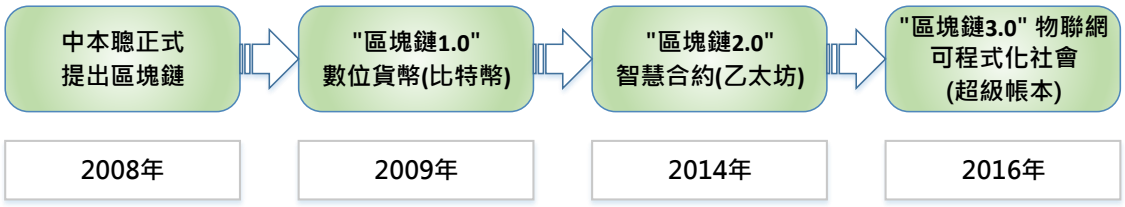


圖 2-5 區塊鏈技術的演進

資料來源：林谷陶，區塊鏈技術及營建產業應用案例探討，內政部建築研究所，2020.

第一代比特幣的區塊鏈功能，事實上就是進行單純加密貨幣交易的記帳功能而形成了一個連續帳簿，每個月的資料就相當於區塊，區塊與區塊之間透過雜湊鏈串聯起來。以比特幣來說，大約是每 10 分鐘產生一個區塊，區塊中主要包含交易事務資料以及區塊的摘要訊息。下圖 2-6 為比特幣中區塊鏈資料的組成示意圖

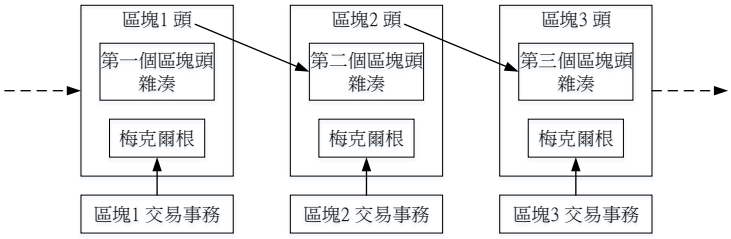


圖 2-6 比特幣區塊鏈的資料組成結構

資料來源：蔣勇, 文延等, "白話區塊鏈" 碁峯出版社, 2018.（本報告重繪）

隨著比特幣，大量區塊鏈實作案例相繼湧現。由於比特幣平行處理處理能力不強，也無法快速確認交易，更沒有智慧合約這種適應更廣的商業應用，這些有後發優勢的新成員在比特幣區塊鏈的基礎上做出了各種各樣的改進和最佳化，以適應廣泛的社會應用需求，最著名的就是"乙太坊"即區塊鏈 2.0。乙太坊(Ethereum)是一種新的去中心化區塊鏈協定，具備去中心化、開放和安全這三大特點，及可自行撰寫的智慧合約開發平台[6]。

區塊鏈 3.0 的架構中，超越了對數位貨幣或者金融的應用範圍，而將區塊鏈技術作為一種泛解決方案，可以廣用在極為廣泛的領域，例如行政管理、文化藝術、企業供應鏈、醫療健康、物聯網、產權登記等。產業應用一般需要具備企業級的屬性，例如身份認證、許可授權、加密傳輸等，並且對資料的處理效能也會有所要求，因此企業級情境下的應用，往往都是聯盟鏈或者私有鏈。代表性架構如下圖 2-7。

圖 2-7 區塊鏈 3.0 組成結構

資料來源：蔣勇,文延等,"白話區塊鏈"碁峯出版社,2018.

區塊鏈 3.0 的代表就是超級帳本(Hyperledger)，這是由非營利組織 Linux 基金會發起成的、致力於企業級區塊鏈開發及應用的開放原始碼專案。願景是借助專案成員和開放原始碼社區的合力，制定一個開放、跨企業、跨國界的區塊鏈技術開放原始碼標準，打造可以跨企業的區塊鏈解決方案[6]。

第二節　物聯網與新興區塊鏈技術

物聯網概念由麻省理工學院的 Kevin Ashton 於 1999 年第一次提出，他認為，物聯網是通過射頻識別(RFID)技術和傳感器技術結合運用於日常生活中形成的網路。在 2005 年國際電信聯盟報告中，物聯網概念有了拓展："物聯網是通過 RFID 和智慧計算等技術實現全世界設備互聯的網路[7]。物聯網(Internet of Things, IoT)即萬物相聯形成的網路。在物聯網的概念下，能夠幫助人們利用已有的互聯網技術將其與實際生活中的物品充分融合，實現遠距離控制和高效率的操作；經過最近幾年的實際應用，物聯網的優勢已經得到了充分展現。

因應智慧城市多樣化服務需求，讓城市物聯網(IoT)基礎設施不斷擴展，於是便出現了稱為 IOTA 區塊鏈技術(也有人稱此才是區塊鏈 3.0)，這是一種有向無環(DAG)的新型分散式分類帳(如圖 2-8)，克服了目前區塊鏈設計的低效率問題，在去中心化的點對點解決方案中導入了一種新的共識方法[8]。

比特幣交易共識上鏈的效率一直比較低，，由於鏈式的儲存結構，整個網路中同時只能有一條鏈，導致出塊無法併發執行。針對此問題，Nxt 社群提出改變區塊的鏈式儲存結構，變成區塊 DAG。在區塊打包時間不變的情況下，網路中可以並行打包 N 個區塊，網路中的交易就可以容納 N 倍。此種方式類似側鏈的解決思路，不同的鏈儲存不同類型的交易，這樣降低出現雙花的可能，在之後某個節點需要合併的時候，幾個分支再歸併到一個區塊。

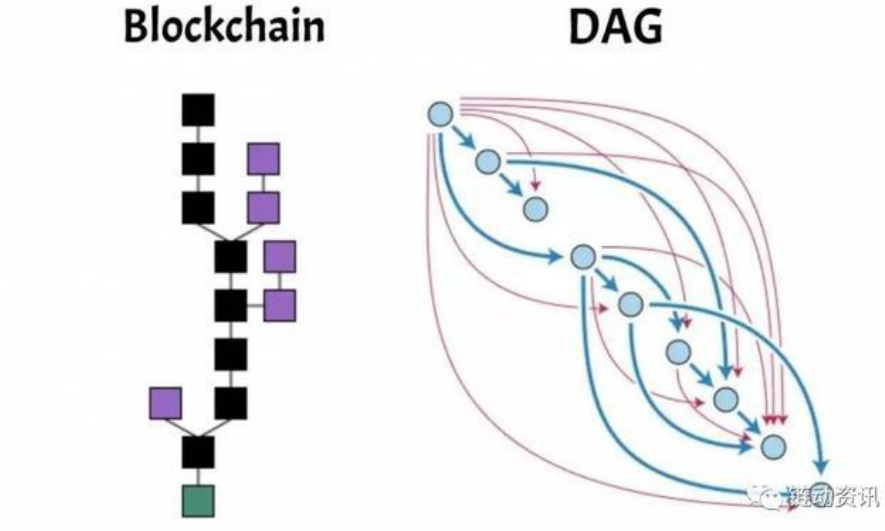


圖 2-8 傳統區塊鏈與 DAG 結構比較示意圖

資料來源：https://kknews.cc/tech/jb5g5gq.html，《秒懂：區塊鏈技術革命—DAG 技術》

由於傳統區塊鏈顧名思義都屬於有區塊的情況，無論是在比特幣還是以太坊中，出塊速度都很慢，比特幣每十分鐘出一個塊，6 個出塊確認需要一個小時，以太坊好很多，但是出塊速度也要十幾秒，無法適應物聯網成長的需求。所以 2015 年 Nxt 社區提出捨棄區塊的概念，把區塊和交易(此交易已不只是數位加密貨幣，更有可能指的是感測器間的訊號數據傳輸，但同樣具有分散式、無法竄改，不可否認，信任安全隱私的特性)融合到了一起，每一筆交易直接參與維護全網的交易順序。這樣交易被發起後直接跳過打包區塊的階段，直接鏈入全網，如此達到無區塊效果，且連打包交易出塊的時間都省去了。如前所述，DAG 最初跟區塊鏈的結合就是為了解決物聯網時代的效率問題，現在不用打包確認，交易發起後直接進入確認網路，理論上效率自然會提高很多。

以有向無環圖 DAG 理論(tangle 纏結技術)為基礎開發出來的已有 IOTA、byteball、hashgraph、InterValue 等知名區塊鏈平台。以最先出現的 IOTA 網路為例，即沒有區塊的概念，交易是進行共識的一個單位，它基於有向無環圖(DAG)的結構，同時提出了一種馬爾可夫鏈蒙特卡羅演算法(MCMC)，用於解決交易剛到達時，如何在 Tangle 中選擇附著點的問題。每一個 IOTA 節點既是交易的發起者，同時也是交易的驗證者。因此，網路中沒有礦工，也沒有挖礦，所有的 IOTA 代幣都在創世交易中創建出來。IOTA(也是數位加密貨幣的一種)的總數是(333-1)/2=2779 530 283 277 761[9]。

IOTA 作為區塊鏈 4.0 的代表，並沒有採用鏈式結構作為基礎，而是用有向無環圖(DAG)構建了 Tangle 網路。IOTA 的非區塊鏈架構有如下三個特徵。

- 可擴展性：隨著更多節點加入網路，IOTA 的網路結構讓它的吞吐量增加。
- 零費用：IOTA 網路上的轉賬不收取交易費；發送 1 個 IOTA，也正好收到 1 個 IOTA。
- 去中心化：在 IOTA 中，用戶就是驗證者。在用戶之外，沒有單獨的礦工或驗證者。理論上，這導致驗證更去中心化。

第三節 區塊鏈與大數據、人工智慧

正如前述物聯網(IoT)代表了本世紀最重要的破壞性技術之一。電腦的互聯網向嵌入式和虛實整合系統的自然演進是"事物"，儘管顯然不是電腦本身，但它們本身內部仍裝有微處理器。透過越來越便宜的感測器和更快更普及連接事物的網路，可以更細緻實現有關我們的世界和環境的數據與資訊收集分析應用。

內政部建築研究所於 2021 年召開 AIOT 特殊議題專家會議，結論也認為物聯網的出現可以降低降低現行智慧建築中綜合佈線與系統整合的技術與成本門檻。建築物內的機電、空調、照明、安全等次系統，由於物聯網技術(包含智慧手機與行動裝置)的運算能力與通信速度快速提高，逐漸由簡單控制邏輯的開/關或連動控制，轉換為佈建具備感測資料運算(edge computing)能力的感測器於建築空間，收集與紀錄大量資料提供雲端大數據與人工智慧分析[10]。

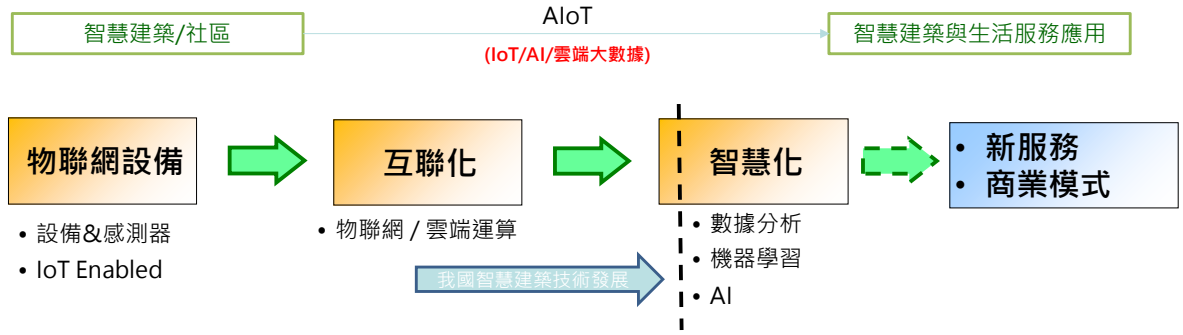


圖 2-9 物聯網人工智慧與智慧化居住空間的關係

資料來源：智慧化居住空間產業聯盟(秘書處)，2021 年 AIOT 特殊議題專家會議報告，內政部建築研究所

因此，IoT+AI 預期會在建築的全生命週期產生影響與衝擊，衍生出的服務會比以往推動智慧建築時更容易滲透入智慧家庭，同時對於實現智慧城市與城市治理，甚至改變都市的發展與規劃。

一、區塊鏈與大數據

物聯網的發展使數據呈現爆炸性的產出。在智慧家庭物聯網領域中，家用設備被改造成和傳感器等設備相聯的數位設備，每一個設備都能夠成為收集並產生數據的節點，而這些海量數據與以往不同的是，創造數據的主角由人變成了隨處可見的物聯網微型設備，同時相關企業通過物聯網可以收集到比以往任何時候都多的數據，這些數據能夠為企業管理者提供新的管理思路和分析策略，以適應新時代的競爭。

本來區塊鏈與大數據的發展，二者都是透過互聯網實現的技術，但因大數據的收集儲存與分析遇到了瓶頸，現有的大數據應用產業面臨著優質可用數據少、資訊壁壘嚴重、數據處理有困境、實踐應用障礙多、雲端管理失誤多五大困境[7]。而這些困境是由現有技術手段的不足造成的，因此，必須依靠新技術才能夠突破大數據產業發展領域的瓶頸。在大數據的發展面臨困境的同時，區塊鏈經歷前述的發展歷程，並針對物聯網時代需求出現新的區塊鏈技術成功為各大產業數據應用帶來了新的希望。

到了以雲端運算為基礎設施的大數據時代，以現在常用的分散式運算技術的代表 MapReduce 來說，大數據需要 MapReduce 將任務分解後進行分散式計算，然後將結果合併。因此，分散式的技術形成了一種去中心化的系統，其中的每個組成部分都是同等重要的。這與區塊鏈技術的去中心化思想與分散式帳本特性一致，並且區塊鏈通過時間順序將持續增長的數據整理成鏈式數據結構，系統中所有節點共同參與數據的記錄，這代表了一種從技術權威壟斷到去中心化的轉變。

在此層次上的意義，可以說有希望打破大型互聯網公司的壟斷行為。例如，大型社群平台公司掌握了所有互聯網所有民眾的活動數據。而通常的疑問是我們無法掌握得知這些大型公司對我們活動資訊數據監控、轉賣甚至被盜取產生了什麼後果，也根本無法對該公司產生任何質疑。他們甚至可以將整個社會輿論控制在手中，這顯然是十分不利於社會和諧安定的事件。

而當"分散式"的概念出現後，從根本上打破了技術權威壟斷的情況，形成了"無中心"的新技術。在分散式的系統中，所有參與者享有同等的權利。大數據的各個協同工作組件缺一不可，互相協調才能完成工作；因此利用區塊鏈技術特性的各個節點共同監督數據，每個節點都有質疑和被質疑的過程。

結合區塊鏈技術和大數據在分散式上的有兩個具體共同點：分散式儲存和分散式計算。因此，如果說大數據需求是資訊管理和儲存，那麼新興區塊鏈技術就是資訊加密和保護系統，它為大數據提供高度的安全性、確保個人資訊的私密性、幫助數據實現不同情境下的聚合、使得數據能夠發揮更強大作用。可

說區塊鏈是大數據的安全載體，為數據擁有者提供安全隱私；而區塊鏈技術的智慧合約與加密數位貨幣則可提供激勵共享數據的機制。

二、區塊鏈與人工智慧

區塊鏈的優勢在於實現數據的完整記錄和不可篡改，但對於數據的統計分析能力比較弱。當數據規模越來越大時，區塊鏈必然面臨技術上的不足。因為區塊鏈及其相關技術群涉及諸多環節，比如共識機制、安全機制、節點維護與更新等，每個環節都有大量的資訊數據要處理，人工智慧技術則可以提供諸如共識演算法的優化、節點智慧化負載均衡、風險識別等各項支援。在這一層次，人工智慧技術對區塊鏈有著輔助作用的期待。

另一個層次是人類社會正在邁向大規模協同合作的智慧型社會，對人工智慧的要求已經從個體智慧轉向群體智慧。群體智慧方面有待解決的問題非常多，例如，如何確保個體之間協作的約定問題？如何解決個體之間的信任問題？如何解決大規模協作的資訊儲存問題？種種問題的核心均指向需要一種信任的基礎設施[7]。

在群體智慧的應用中，個體之間要實現協作與協同，首先要解決個體之間資訊共享交換的問題，例如，人和人之間的協作，或者團體之間的協作，這些不同個體之間的資訊和數據如果不能被有效共享和交換，則無法進行協作產生群體智慧。可以說，資訊共享存取與交換是群體智慧應用的基石。因為區塊鏈本身就是一個去中心化的分散式數據和資訊共享平台，節點之間可以無障礙地、安全地進行資訊的共享和交換。區塊鏈的這一功能首先解決了群體智慧應用中個體協作所產生的資訊共享和交換的需求。

在群體智慧應用中，即使個體之間實現了資訊共享與交換，還有一個重要的問題需要解決，那就是安全問題，也就是需要保證個體之間資訊傳遞和處理中的安全與隱私。對個體之間的協作來說，資訊共享與交換在區塊鏈上可以很方便地解決，那麼下一步的問題就是如何保證個體數據資訊在傳遞的過程中的隱私，讓非此協作的相關者無法獲取相關資訊，同時如何保證數據資訊提供者的隱私和安全措施中的效率問題。這些問題凸顯了資訊安全對於大規模的群體

智慧應用的重要性。正如前述區塊鏈技術的匿名性、防竄改特性對數據資訊的傳遞已先做了匿名性，同時也保證了數據的真實性。

第四節 區塊鏈的發展與未來

建構區塊鏈打造"更好的星球"，是由世界經濟論壇倡議發起，MAVA 基金會贊助，與 PwC(PricewaterhouseCoopers)和 Stanford Woods Institute for the Environment 合作撰寫，為世界經濟論壇第四次工業革命會議所提一系列報告之一，提供環境與自然資源安全解決方向的建議[11]。

報告中將區塊鏈列為第四次工業革命的基礎新興技術，就像互聯網是上一次(或第三次)工業革命一樣。因其分散式且不變的帳本和先進加密技術，無需第三方中間人，即可在各方之間安全，低成本地轉移各種資產。與當今的互聯網平台公司不同，還設計實現了民主化機制，允許網路參與者藉由節點(區塊鏈上的設備)來擁有一部分網路，而不只是單純只是大家熟知的數位加密貨幣工具而已。從最根本的角度來看，它是一個新的，分散的全球計算基礎架構，可以改變商業，治理和社會中的許多現有流程。

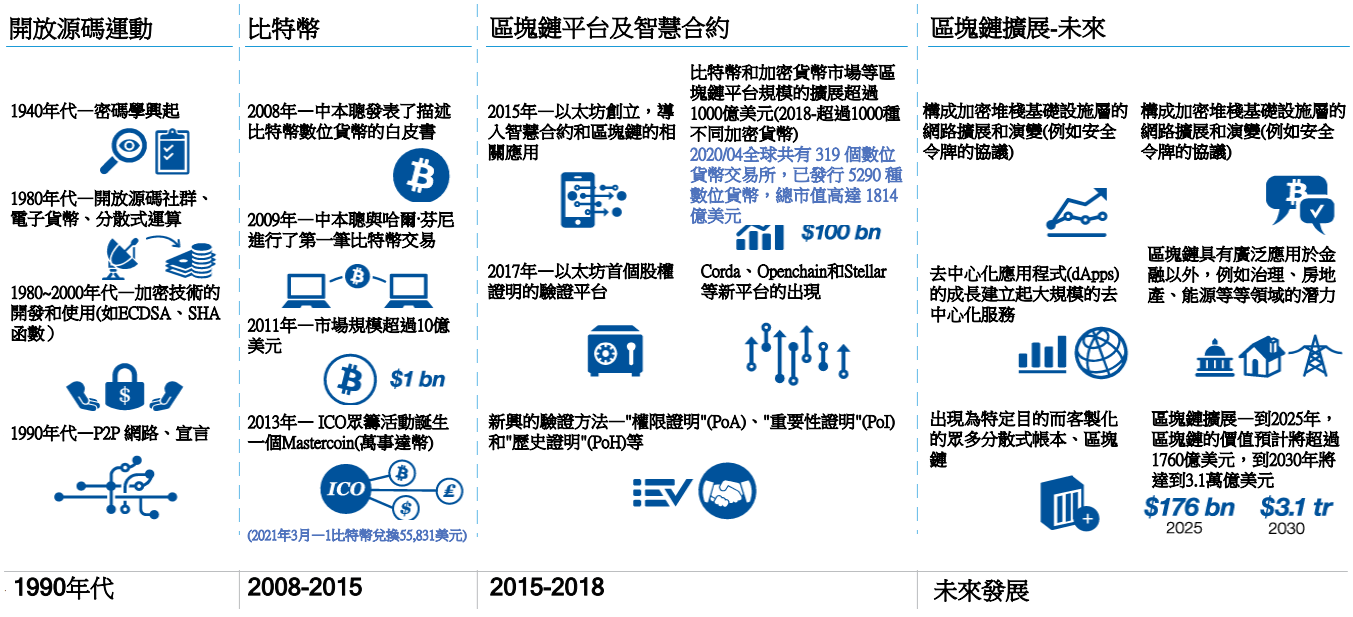


圖 2-10 區塊鏈發展時間軸與未來發展(本報告譯釋加註)

資料來源：Forum., W.E., Building Block(chain)s for a Better Planet: Fourth Industrial Revolution for the Earth Series., in Fourth Industrial Revolution for the Earth Series. 2018/09.

近幾年來區塊鏈受到各國政府和民間部門以及整個社會潛在影響的廣度和深度的廣泛討論，尤其比特幣等數位加密貨幣受到了相當大的炒作，接著是以太坊幣，以太坊作為通過智慧合約建構去中心化應用平台，激發了全新的"代幣經濟"；投票，數位身份，財務和健康方面的應用出現。世界經濟論壇統計截至2018年7月初，加密貨幣的總市值(涵蓋1,629種貨幣)約為2546.7億美元。其中因為區塊鏈技術日趨成熟，存在著廣大的機會來應用區塊鏈進行各種產業中的創開發與部署。

世界經濟論壇因應世界所面對迫切環境危機(例如氣候變化,生物多樣性喪失和水資源短缺),也提出區塊鏈的創新應用可面對這方面的各種挑戰時，包括因此得以改變管理我們全球環境的政治、公關方面最大制約的遊戲規則，並提出相關的解決方案。因此可以極大地突破目前環境保護行動受箝制的現況、系統和方法[11]。因此，可說世界經濟論壇極大重視區塊鏈，並視為是工業4.0可建設更好地球的數位科技。

第三章 智慧家庭數據問題與區塊鏈應用趨勢

由於智慧家庭新興家用電器，都能進入網際網網路，也是聯網設備的一部分；也就是智慧家庭物聯網(IoT)的出現，讓家庭變得越來越"智慧"，使家庭消費者能夠遠端監控和管理其家庭環境—可在遠端開關鎖門、控制照明系統，並且可以在煙霧警報器感測到火警狀況時由手機示警移報。美國調查顯示個人或家庭安全、財產保護、照明/能源管理和寵物監控是使用此類設備的首要動機，51%的受訪者願意支付超過 500 美元的費用配備全套智慧家庭系統[3]。

智慧家庭物聯網設備越來越多配備了傳感器(攝影鏡頭、麥克風、動態感測器等)和致動器(例如燈、揚聲器、鎖)如圖 3-1，這產生了前所未有的隱私和安全問題。例如，內建在監控設備中的攝影鏡頭和麥克風會被駭客侵入監視家庭活動。有報導稱，駭客侵入聯網中的嬰兒監視器，說髒話辱罵家庭成員的案例[12]。此外，一些物聯網應用與敏感水、電輸送和資產監控等密切相關，並且相關的應用處理程式，都有可能洩漏使用者、住戶的敏感資訊，例如他們的位置和活動，或者他們的健康情形和購買偏好等。

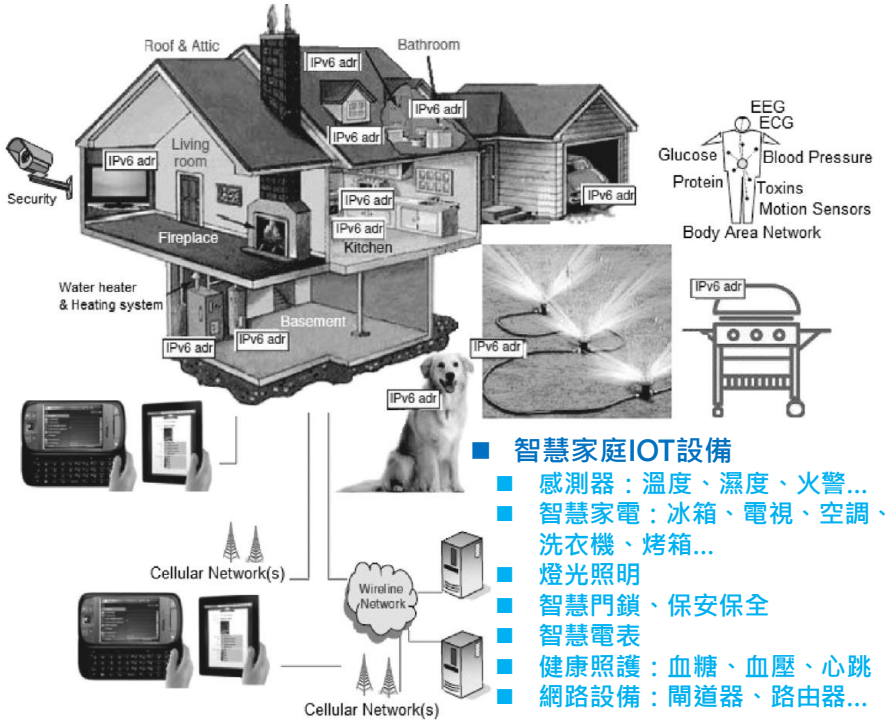


圖 3-1 智慧家庭設備示意圖

資料來源：Minoli, D., Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. Internet of Things, 2020.10.

實際上，這些詳細數據轉換的知識，將可提高效率並在廣泛的應用領域中提供先進的服務，包括普及的醫療保健和智慧城市服務。但是，私人生活中的數據收集、處理和散播一方面，可來為使用者提供一系列精準複雜、個性化及有效的服務，但也越來越無形、密集和普遍，這引起了嚴重的安全和隱私問題。以下各節將就國外發現智慧家庭數據問題與區塊鏈應用趨勢進行分類說明。包括幾種新興智慧家庭物聯網設備的網路行為，包括智慧燈炮燈泡、電源開關、煙霧警報器、智慧門鎖和智或智慧家電，以及相關必要網路設備等，說明智慧家庭聯網設備的整體架構、實例及問題概述。

第一節 智慧家庭物聯網安全問題

由於智慧家庭中各項新興聯網的終端設備,可能包括消費性智慧家電(即智慧冰箱、智慧電視、冷暖氣機等等家用電器)、智慧照明燈具、智慧插座，及防災警報設備、智慧門鎖，以及智慧電表等；而對健康照護部份更有血糖、血壓、心跳等等量測設備,影像監測設備;最後這些訊號以有線無線方式透過閘道器、路由器網路設備傳送到遠端使用者(住戶)的行動設備上，或者由遠端監控單位進行監控維護。

智慧家庭應用程式處理家庭電器設備控制，包括使用 Amazon Alexa 或 Google Home 等智慧音箱裝置對廚房電氣設備進行語音控制(例如，管理冰箱、微波爐、洗衣機、恆溫器、烤箱甚至戶外燒烤架)、暖氣、通風和空調(HVAC)控制、家庭安全、包括影像監視、先進的煙霧和一氧化碳檢測、洩漏檢測、智慧電網和智慧電錶與家庭電器設備的整合、照明控制系統,包括進住感知系統、殘障人士和老年人的家庭自動化，包括電子化醫療照護的支持、嬰兒照護、和寵物照護。

這種裝置除了接收使用者語音(或者可行動的智慧機器人)溝通、指揮智慧家電運作功能外，也因此具有類似家庭智慧家電互動傳送之閘道器(網關)功能;由此看來現有的智慧家電都試圖藉由互聯網,來提高每個設備的智慧互動、遠端監控性能及衍伸的安全性問題；由於聯網與互動涉及相關的通訊機制和協

議，使得前述智慧音箱廠商藉由自有通訊機制和協議，綁定自有相關智慧家庭的各種設備，並收集數據不斷精進擴大智慧家庭商機。

一、基本智慧家庭物聯網

由於智慧家庭端點設備通常必須透過 IoT 閘道器互聯及路由器家庭外網際網路傳送。因此，在智慧家電環境中，這些閘道器通常部署在家庭中作為處理中心[13]，整體架構如圖 3-2 所示。

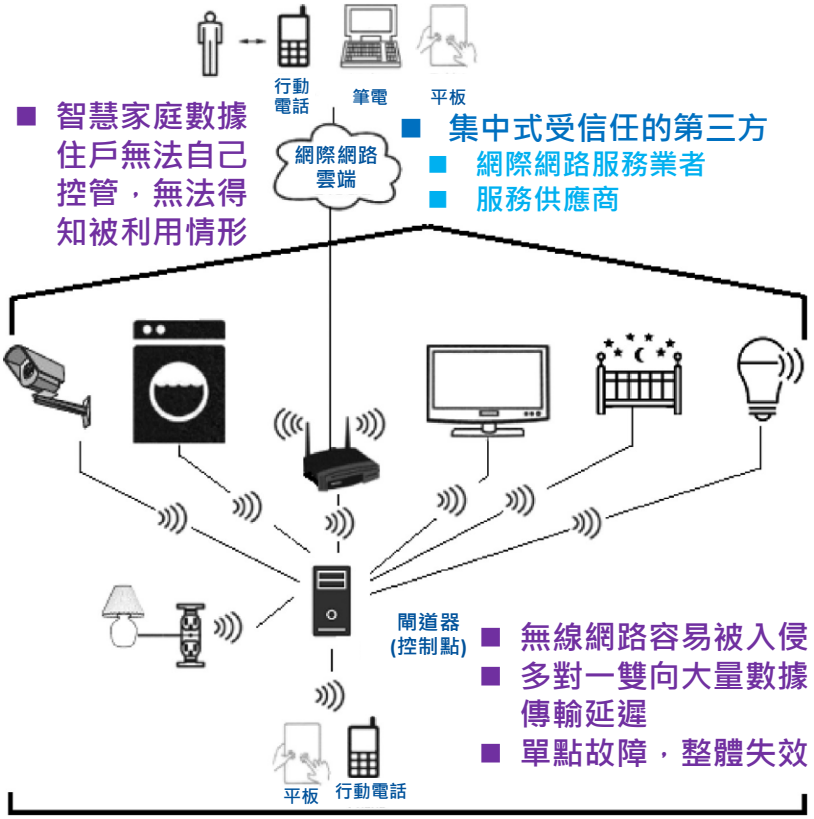


圖 3-2 智慧家庭物聯網應用範例

資料來源：Minoli, D., Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. Internet of Things, 2020.10.；本報告譯釋。

上圖可想見智慧家庭內容可能包含(但不僅止於此)：

1. 電器控制：冰箱、微波爐、洗衣機、恆溫器、烤箱甚至戶外燒烤架)、通風和空調(HVAC)
2. 家庭安全：包括影像監視、先進的煙霧和一氧化碳檢測、洩漏檢測、出入感知系統(智慧門鎖、入侵)。
3. 節能管理：智慧電網和智慧電錶與家庭電器設備的整合、照明控制系統。

4.健康照護：行動不便者和高齡者的智慧化醫療照護的支持、嬰兒照護、和寵物照護。

智慧家庭發展過程中，一般應用閘道器功能可處理空調HVAC、火災警報、照明元件、數位控制器、壓縮視訊(視訊監控)，家庭數據和語音以及娛樂視訊(衛星)等。市售物聯網閘道器可提供傳感器數據流的邏輯匯總、必要時進行感測器協定之間的轉換、預處理感測器數據再發送到分析系統(無論是本地還是雲端)以實現數據運算功能，並且還可能具有支持某些加密和授權/身份驗證的功能。

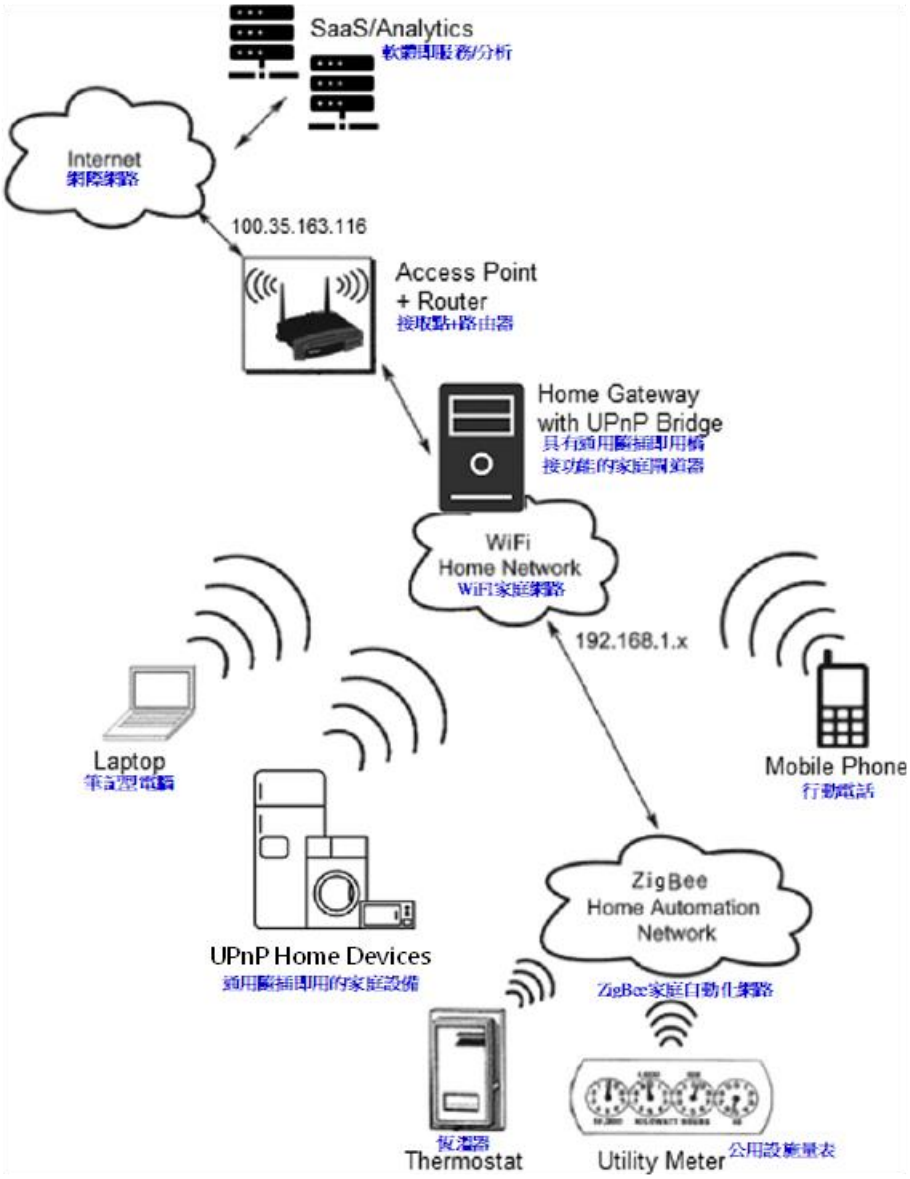


圖 3-3 一般智慧家庭閘道器橋接家庭自動化設備範例

資料來源：Minoli, D., Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. Internet of Things, 2020.10.；本報告譯釋。

許多網路基礎設施供應商都有提供閘道器，而在物聯網閘道器上執行的基本功能實際上支援了邊緣運算和分析，而它們提供的文件說明了還包括與 WAN 路由器或 WAN 本身的連接性(例如，LoRa 或 Sigfox WAN 服務)、對 IoT 數據進行加密/解密、因為大多數嵌入在"事物"中的系統沒有足夠自己的數據運算能力、IoT 設備的控制和管理，以及最後物聯網協定的轉換等其他功能。圖 3-3 描繪了支持內部協定轉換的 IoT 智慧家庭閘道器的典型環境。

但許多現有的家庭能源系統都不允許消費者通過智慧手機或平板電腦直接讀取或控制它們，即使它們靠近能源系統也是如此。因此，需要有支持從標準使用設備進行本地或網路遠端存取的閘道器功能，如圖 3-4 描繪了通常所謂用於智慧家庭服務的聯網安排，其中設備使用現有的 ISP 連接來存取特定的服務節點(例如，支持智慧家庭安全加值服務)。導入物聯網環境必須確定是否在網路邊緣配置一些可減少核心網路轉發傳感器經常產生的大量數據所需的頻寬量的閘道器圖 3-5；此外，亦可因此進行重要的數據決策可提高決策速度和整體可靠性，而無需集中干預。物聯網閘道器促進了更接近數據源頭和物聯網設備本身分析決策的執行。

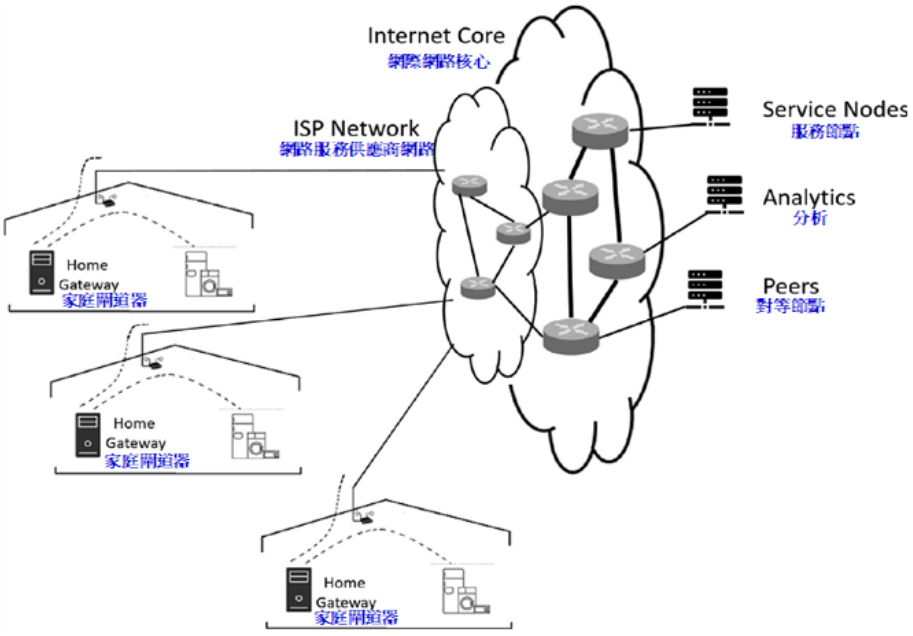


圖 3-4 智慧家庭服務運用物聯網家庭閘道器的範例

資料來源：Minoli, D., Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. Internet of Things, 2020.10.；本報告譯釋。

隨著智慧家庭應用設備的普及，家庭中智慧家電設備連接的數量增加，將此多個終端"事物"分別連接到管理或分析系統變得不切實際。一些終端系統設備在匯總中會生成大量瞬態數據，以致最後一里甚至核心中的通訊通道可能變得飽和。而邊緣物聯網閘道器執行許多關鍵功能，例如設備連接性、數據過濾和處理、身份驗證和安全性、協定轉換以及端點設備軟體的更新管理。

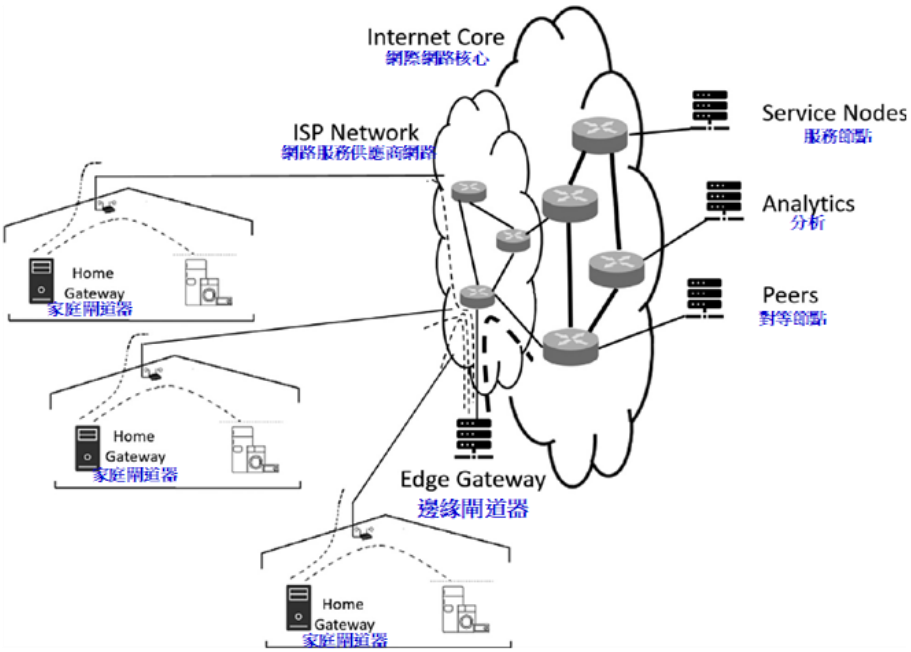


圖 3-5 智慧家庭服務運用 IoT 邊緣閘道器的網路範例

資料來源：Minoli, D., Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. Internet of Things, 2020.10.；本報告譯釋。

從以上說明，可知智慧家庭物聯網(IoT)，是由產生、處理和交換大量安全和關鍵性數據，以及敏感的隱私設備所組成。因此，成為各種網路攻擊的誘人目標。目前許多構成物聯網許新的可聯網設備，首要考量傳輸與運算等核心應必須具備低能耗、微型化的特性。這使設備支援安全性和隱私性任務的功能，顯得頗具挑戰及困難。此外，許多最新的安全架構是高度集中的，由於規模困難、多對一的流量性質和單點故障等，因此不一定適合物聯網。為了保護使用者隱私，現有方法通常會流露雜訊數據或不完整的數據，這可能會阻礙某些物聯網應用提供的個性化服務。因此，物聯網需要輕量級、可擴展的分散式安全和隱私保護措施。所以國際上普遍考量以具分散式、匿名、防竄改的區塊鏈技

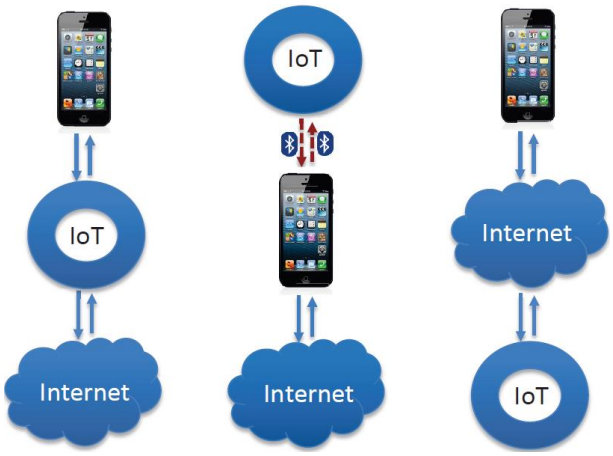
入因應解決，特別是支撐第一個加密貨幣系統比特幣的 Blockchain(BC)、以太坊等區塊鏈技術來克服上述的物聯網時代智慧家庭的各種安全隱私問題。

二、智慧家電

研究人員曾經針對 Phillips Hue 燈泡、Nest 煙霧警報器和 Belkin WeMo 電源開關進行實驗評估。證明了一般智慧家庭家電設備，缺乏加密、適當的身份驗證、消息完整性檢查，以及物聯網的隱私影響[3]。

針對上述問題，現有的解決方案都試圖藉由在每個設備上到物聯網時，予以提高安全性，但正如前一小節的說明，但這需要改變現有的上層網路通訊機制和協議，目的是強化加密、身份驗證和密鑰管理等方面。然而，研究文獻[3]指出，對全世界數百家智慧家庭物聯網設備製造商而言，幾乎不可能提出單一物聯網安全解決方案，可應對具有不同功能的各種物聯網設備的所有安全和隱私威脅。此外，由於許多物聯網設備體積小、有限的運算能力和電力資源，因此無法應用廣泛運算豐富的安全演算法。然而，我們的方法藉由應用一組動態的網路層規則來限制合法實體(如應用程式、伺服器和使用者)對物聯網訪問，從而確保安全性。

智慧家庭物聯網設備和通信協議範圍廣泛(WiFi、ZigBee、Bluetooth、…)，但不論如何，所有智慧家庭物聯網設備(IOT)運作模式，不外乎如圖 3-6 所示使用者、物聯網和製造商維護的雲端伺服器之間的三種主要通訊模型。"直接"訪問模型允許使用者直接與物聯網通訊設備(例如飛利浦 Hue 燈泡、WeMo 動作/開關)通過行動應用程式，然後如(a)所示，物聯網設備更新伺服器的目前狀態。也可以透過製造商提供的入口網站控制 IoT 設備。"Transit"(中繼)模型主要用於不具備與互聯網伺服器直接交換數據能力的物聯網設備。這些類型的設備(例如 Fitbit 健身追踪器)沒有 Wi-Fi 接口，通常使用其他通訊方式，例如藍牙和近場通信(NFC)。為了能與伺服器通訊而檢索所需的數據，利用使用者手機作為數據交換的中繼/橋接器，如(b)所示。最後，在"外部"模型中，使用者與物聯網設備沒有直接互動。(c)顯示物聯網設備(例如火警 Nest Protect 煙霧警報器)直接與外部伺服器通訊，使用者才能檢索到相關數據(例如目前狀態)。



(a) (b) (c)

圖 3-6 物聯網三種運作模式：(a)設備直接聯網及使用者端,(b)設備經使用者端中繼聯網, (c)設備經中繼聯網至使用者端

資料來源：Notra, S., et al. An experimental study of security and privacy risks with emerging household appliances. in 2014 IEEE Conference on Communications and Network Security. 2014.

Nest Protect 火警煙霧警報器而言，透過使用者行動應用裝置上的語音警告、嗶嗶聲、LED 燈和文字警報等組合方式傳達給使用者。但因這些設備通訊有被侵入、截收數據，而被分析出使用者何時在家、生活作息等等洩漏隱私。甚至覺得正在被監視和追踪的擔憂。以上述文獻為例，研究者進行煙霧警報器的通訊流程監測，發現所有數據上網交換都經過加密。因此，這項產品實際上是一款非常安全的產品。使得有意入侵者很難從 Nest 傳感器(如圖 3-7)和服務器之間的通訊中竊聽和截取有關使用者的訊息。

圖 3-7 Nest Protect 煙霧警報器

資料來源：https://tw.begin-it.com/501-how-to-set-up-and-install-the-nest-protect-smart-smoke-alarm

但在隱私方面，上述過程似乎顯示通知伺服器處理基本的煙霧警報功能，即從設備獲得煙霧警報狀態並以行動裝置應用程式通知使用者，但這留下了日誌伺服器上資料的問題。同時在通知之後，有可能從行動裝置或感測器本身獲得的使用者的隱私數據。

飛利浦 Hue Connected 燈泡，可讓使用者以行動裝置透過 Android 或 iOS 的飛利浦 Hue 應用程式遠端調整光的強度、設置自定義顏色、顏色組合和時間排程(如圖 3-8)。飛利浦的 Hue 非常的可以客製化，並且設定利用 If-This-

Then-That(IFTTT)服務，可根據其他平台(例如 Facebook)上的活動來更改燈泡狀態。例如，可以設計一套設定，讓使用者在照片中被標記而出現時將燈泡變成彩色，或者當使用者的手機超出 WiFi 範圍時關燈[14]。

圖 3-8 飛利浦 Hue Connected 燈泡應用情境

資料來源：https://www.pinterest.es/pin/354236326919952025/?amp_client_id=CLIENT_ID &mweb_unauth_id=&simplified=true

安裝飛利浦 Hue Connected 燈泡，除了智慧家庭必要網路環境外，還要安裝閘道器。使用者首先需要在飛利浦 meethue.com 網站註冊建立帳戶，以便與閘道器相聯接。閘道器本身也可作為所有燈泡的控制器。來自網路應用程式的所有通訊都先通過橋接器，再以 ZigBee Light 鏈接協議向燈泡發送適當的訊號進行所需的調控。不在家時也可以從 meethue.com 網站控制燈泡。

文獻[3]研究顯示，閘道器和應用程式之間交換的資訊為純文本，很容易顯示使用者名和閘道器 IP 位址。此外，還可辨識出回應名單，及當前燈光的狀態(亮度/顏色/色調/警報狀態等)，使攻擊者可以深入了解使用者家中目前狀況。Hue 燈泡在 2013 年的事件就是因為這個漏洞被攻擊的。從那時起，雖然飛利浦應用程式更改了建立使用者名的機制。但因通訊仍然是純文本。研究者仍然發現可以利用這個漏洞進行這種攻擊(文獻[3]研究人員將此攻擊程式放在 GitHub 上供大家參考)。攻擊者可能截取合法使用者和 Hue 閘道器的流量。然後利用截取的資訊擷取出閘道器 IP 和列入白名單的使用者，再使用前述程式碼連接到受害者的閘道器，一步一步最終完全控制閘道器及智慧家庭中的智慧燈炮。

BELKIN WEMO Insight Switch 智慧插座，只需在 AppStore 或 Google Play 應用商店，下載 WEMO 應用程式，即可透過 iOS 或 Android 作業系統的

智慧手機，透過 WIFI 或行動數據搖控隨時隨地開關家庭電器(例如檯燈、咖啡機、房間電熱器等)，或預先設定電器使用時間，也會即時透過手機通知你的設備使用狀態。此外，還有一項重要功能，就是可偵測記錄電器消耗多少電力(顯示在行動裝置 App 中)，提供已開啟時間、今日開啟時間和平均開啟時間，更可以輸入每度電費成本，計算電器的電費總和，讓使用者可以方便分析電力使用；使用者可以使用一台手機操控家中多台 WeMo 插座，或家中其他成員也有 Apple iOS 或 Google Android 智慧型手機，便可以控制同一網路內的 WEMO；此外，還可以結合各大廠牌的智慧音箱，進行智慧音控[15]。

圖 3-9 BELKIN WEMO Insight Switch 智慧插座應用情境

資料來源：https://online.senao.com.tw/mart/1260500?gclid=EAIaIQobChMI0_XqhNzr8QIVlaqWCh1sYQGhEAQYASABEgI2svD_BwE

WeMo 設備使用 SOAP API(簡單物件存取協定應用界面)進行應用程式和設備之間的所有通訊完全是純文本的，而這與前述飛利浦 Hue Connected 燈泡一樣，攻擊者可以從中學習出通訊格式，還可以從合法使用者那裡截取數據封包。而且文獻[3]研究人員發現 WeMo 設備未使用身份驗證方法來確保命令來自合法設備。這是重大漏洞，攻擊者可以很容易地利用它向設備發出格式正確的請求。

又 BELKIN WEMO 公開這些服務功能中所有操作(及其參數)，例如：控制開關(開/關)、獲取開關的當前狀態(開/關)、獲取通過接入點(包括它們的加密模式和信號強度)到這些設備的關閉列表，並且因為這些設備只有兩個固定傳輸端口，使其成為一個潛在的漏洞。入侵者可更輕易地偵聽使用者命令，從而針對發送到這些設備訊息加以收集分析破解，最終入侵利用。

隨著智慧家庭越來越多應用物聯網設備，例如韓國三星、我國禾聯碩不論是從智慧電視、智慧冰箱、智慧電表或是智慧聲控公仔著手[16]，安全和隱私都是重要問題。

三、智慧門鎖

物聯網(IoT)在我們的生活中佔了很大一部分。大量連接的設備可以顯示了這個現象。隨著物聯網設備的指數級增長，物聯網安全性變得越來越重要。尤其智慧門鎖系統是特別重要，因為它與使用者的門禁安全密切相關。但是，如同上述智慧家電一樣，現有的智慧門鎖系統發送和接收的數據容易受到偽造和駭客攻擊。

近年來，智慧門鎖系統已被廣泛成為家庭安全系統的主要部分，其應用甚至比家庭內部的智慧家電應用還快速(因為不只家庭居住用得到，旅館、民宿及辦公處所都有應用的可能)。因為，智慧門鎖系統基本上就是一種人員認證的智慧認證(進出)控制，以開鎖門禁。在許多情境下，入侵者試圖繞過門鎖系統來侵入住宅家中。因此，智慧門鎖整體物聯網系統一樣面臨著與數據安全性相關的挑戰。物聯網還具有大規模和分散式的網路特性，與此相關是數據儲存的安全性。門鎖的接取數據可回溯找出和人何時進出，因此如果發生可疑事件，我們可以預先警覺提防。不過，前提是我們必須保證門鎖接取數據的完整性，一定不能受到偽造和駭客的攻擊。

圖 3-10 威盛 VPai 智慧門鎖

資料來源：https://www.viatech.com/tw/2019/03/smart-locks-building-security-tw/

威勝 VPai 智慧門鎖整合的多種設備－動作檢測、具有夜視功能的廣角高畫質攝影機和於遠端通訊的雙向音訊，無需額外的設備。即可偵測每一位接近的訪客、觸發使用者(住戶)手機的警報(如果需要)以及開始錄影。被捕捉的任何影像都能存儲在雲端，並藉由應用程式或瀏覽器進行檢索以便日後查看；而縮圖和易於使用者界面可以進行剪輯。

當然，智慧門鎖關鍵功能為防篡改系統，因為數位鎖在遭到外來攻擊時可能會失效。雖然 VPai 智慧門鎖的防拆除開關可偵測是否有人試圖以暴力方式撬開，會向使住戶的智慧手機發送警訊的同時，也會為預防強制侵入而自動發出警報。但為了硬體的簡易維護，本產品可以執行遠端更新修正軟體，而無需企業 IT 人員奔波去手動更新每個裝置。但這就如同前述家電設備物聯網通訊過程可被破解入侵之外，在管理層級，超級管理員可能會在使用者不知情的情況下侵害安全，也就是維護後台本身的安全，評估是否具有惡意也是重要的[17]。有個著名的例子是 ZipaMicro，其系統保存客戶私鑰，並且可以很容易地被駭客竊取而獲取根權限立即打開門鎖[18]。

四、智慧家電

正如第二章的介紹，物聯網是工業 4.0 的基礎，但發展應用至今，大規模的實際建設仍沒有出現，主要的原因是建設和維護的成本太高和系統中設備數據的安全隱私無法確保。幾年前 IBM 和三星聯手打造的基於區塊鏈技術的物聯網"自動去中心化點對點遙測技術(ADEPT)系統"可說是物聯網的突破性應用，這款系統結合了區塊鏈的優點，彌補了物聯網建設中遇到的兩大缺陷。

ADEPT 系統利用區塊鏈數據庫建立的分散式設備網路，即建構了一個去中心化的物聯網系統，利用智慧合約可以讓各種智慧設備具有支付訂單的能力。根據文獻[7]說明，ADEPT 系統中的三星智慧家用電器可以在智慧合約執行下發布命令，例如洗碗機可以提醒洗滌劑供應商進行供貨，接收到供應商的支付確認資訊和發貨資訊後，洗碗機可以給主人的手機發送簡訊作為提醒，如圖 3-10。

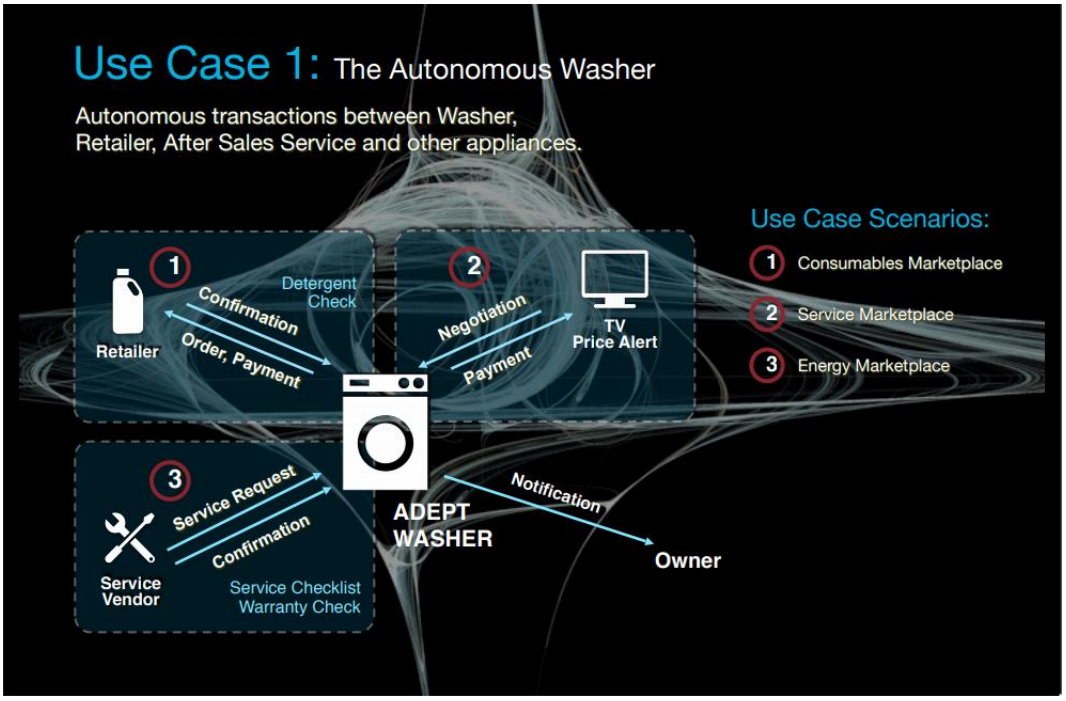


圖 3-11 三星智慧洗碗機應用區塊鏈的 IBM ADEPT 系統案例

資料來源：https://www.slideshare.net/_hd/ibm-adept

ADEPT 系統融合了區塊鏈技術，達成作為去中心化自治對等點啟用的設備私有的設備通訊設計、分散式共識的能力；一方面能夠讓設備實現自我管理和維護，例如上文提到的洗碗機就可以自行完成跟該設備有關的所有活動，而不再需要費用高昂的雲端控制管理系統，解決了物聯網應用成本高的問題；另一方面區塊鏈可以為各個設備生成私鑰，解決了物聯網中設備數據安全的問題。

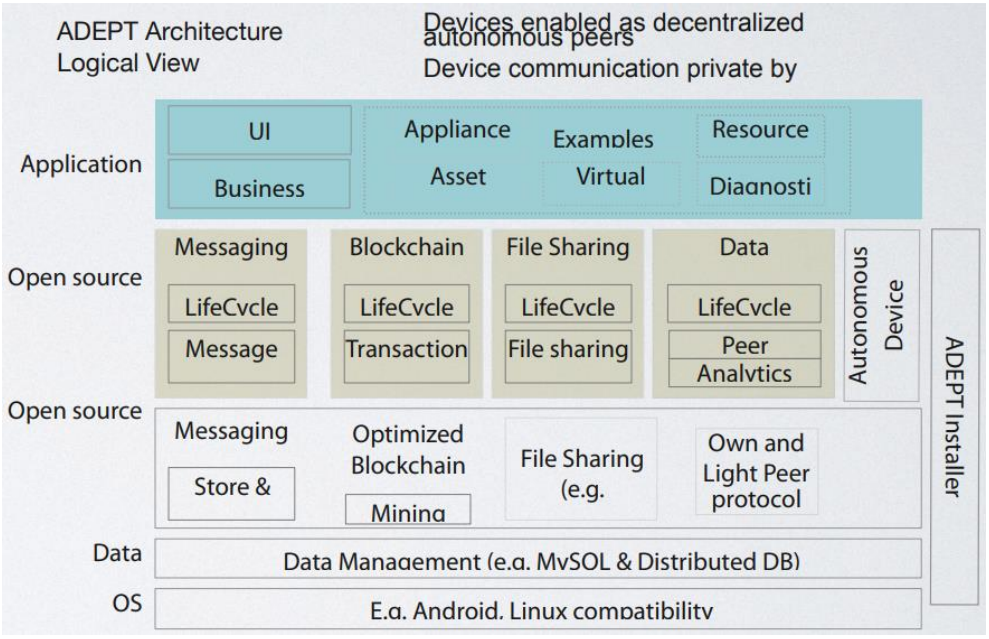


圖 3-12 IBM ADEPT 系統架構

資料來源：https://www.slideshare.net/_hd/ibm-adept

ADEPT 系統的成功應用證明了區塊鏈在智慧家電領域也有巨大的應用潛力。也證明在物聯網體系中，區塊鏈的技術能夠支持各式各樣物聯網設備的種類，大到自動駕駛汽車，小到溫室內的濕度器，都可以放心接入物聯網中而不必再擔心數據洩露問題和營運成本問題。

本合作開發案例早在 2015 年導入以太坊區塊鏈建置完成,推測是因為以太坊是那時首先推出具圖靈完備的智慧合約，可讓三星智慧家電依區塊鏈上智慧合約程式自動執行補充洗碗精、確認、交易付款等步驟。不過後續似乎並未得到廣大的回響，個人猜測仍然受限於以太坊區塊鏈的上鏈共識認證時間的延遲，以及運算 gas 及以太幣花費的限制問題。

而且 IBM 與 Linux 基金會及其他資訊科技龍頭公司共同投入，開發出開放原始碼各項模組合作的 hyperledger 超級帳本區塊鏈開發平台。因此三星智慧家電是否可能獨立維護原平台，或者有再持續更新導入新的區塊鏈技術，可能衍伸新問題等，值得再觀察。

第二節 智慧家庭數據共享激勵問題

智慧家庭讓使用者(住戶)可以輕鬆控制家庭環境的所有設備。但這些數據資訊其實非常具有價值，設備廠商收集這些數據可以精進改良其設備，並發掘客戶潛在的新需求,進而創造新商機(甚至將數據轉賣其他有興趣的新創公司進行新設備、新服務的創新應用，如前述 IBM 與三星合作方案)。

近年來，企業之間共享使用者數據的合作方法方面，技術創新和相關研究獲得了快速發展。但數據共享實踐非常需要在使用者隱私、促進使用者體驗和企業利潤之間的爭議中取得平衡。何時、何種數據應該與誰共享，以及數據所有者應如何獲得信譽或激勵以共享數據的問題，日益成為激烈辯論和研究的問題[19]。

因為使用者數據是由不同組織、企業所收集的，例如提供使用者的應用程式、社群網站等公司，其主要目的是在強化創新自己的業務模型，同時為客戶提供最佳服務。但是，使用者數據的收集涉及嚴重相關的隱私問題。有些數據

是使用者自願提供的，其他則是透過系統從使用者的活動中觀察獲得的，或者是藉由對自願或觀察到的數據進行進階分析推斷而來的。目前使用者數據所有權的主流模型(通常在服務授權協議之初同意的)，是假定所有權從使用者轉移到收集該所有權的企業，則共享有可能被轉移到整個企業網路的相關利益者[19]。儲存個人數據有著相關的隱私和安全問題。世界上不時傳出的線上服務公司、社群網站安全漏洞和數據被竊事件。因此，將信任賦予集中式服務供應商，以進行所有數據儲存時，可能造成所謂集中性問題的影響，特別是數據越集中、規模越大越容易引起駭客的興趣；此外，還有網站技術故障或被內部人員故意刪除使用者數據導致無法交付使用者或需要共享應用者。

另外，為了遵守嚴格的隱私法規，當共享數據以供其他系統使用時，需要再次徵得數據所有者的同意。但因為使用者看不到實際可獲得的好處來說，操作顯得太麻煩而不願意，形成對同意數據共享的障礙。通常，同意書很長且晦澀難理解(如信用卡)，他們沒讓使用者選擇他們願意共享數據及不願意的其他數據，以至於變成只是"接受或放棄"。使用者甚至不會閱讀它們，而是向下滾動並點擊"同意"，因為不點擊同意他們將無法使用服務。因此，使用者很難甚至無法記住他們曾經同意哪個企業，並追踪誰訪問他們的數據以及出於什麼目的。因此，需要一種靈活的機制，以同意獲取和更新數據的使用和共享，為使用者提供適當而有意義的激勵措施，讓使用者從數據共享中獲利並且保證透明化，以確保使用了解那些數據集已被訪問、由誰訪問、何種目的、什麼條件下被使用。

因此，建議應該建立智慧家庭使用者控制的隱私和數據共享策略，從而解決了這些所有安全性、隱私、使用者透明性和控制權以及數據共享的激勵措施等問題。其機制有支援創建激勵的機制，鼓勵使用者共享數據，讓使用者成為自身數據的真正擁有者，可以決定他們的數據如何被收集和被使用以及如何共享，這不僅可以從改進提升的個性化服務體驗中受益，而且，例如直接可以透過參與服務供應商產生的廣告收入中共享受益。

第三節 智慧家庭區塊鏈安全隱私的研究示例[20]

相關物聯網和智慧家庭的安全性和隱私性的損害已有前述各種案例，且不斷有研究證實，惡意者可侵入現有缺乏基本安全保護措施的各種智慧家庭設備物聯網設備，而即使有了家庭網路閘道器控制進出家庭的數據封包交換，智慧家庭也很容易受到使用智慧手機的攻擊[21]。現有的解決方案通常利用中央控制器來管理智慧家庭設備的系統，但是存在許多缺點。如果中央控制器受到損害或家庭與網路斷開連接，則隱私和安全性將受到損害。

為了解決上述問題與挑戰，已出版許多研究利用區塊鏈技術固有安全特性來增進智慧家庭系統的安全。目前大多以區塊鏈技術的核心優勢：身份驗證和權限控制，透過使用加密機制設定設備，實現無縫驗證，以確保內容的私密性和所有權[18]。所有這些都有助於建構適合複雜現實生活情境的安全隱私系統;但有關數據分享，尤其由智慧家庭使用者(住戶)控制自己擁有的生活數據，少有看到學術界研究探討；而在智慧家庭產業的導入應用，初步對於數據的分享應用大概聚焦於私有區塊鏈或聯盟區塊鏈的形式。

由於智慧家庭物聯網需要輕量級、可擴展的分散式安全和隱私保護措施。因此當世界上第一種去中心化數位貨幣比特幣於 2008 年推出。類似於 BitTorrent，比特幣由其使用者的電腦組成的對等電腦網路支撐。另外，可變的公共密鑰(PK)作為使用者的身份識別，提供了匿名性和隱私性。比特幣背後的主要技術被稱為區塊鏈(BlockChain, BC)，這是一個不可變的公共記錄，由對等參與者網路保護。BC 正在迅速普及，並有許多其他應用，包括智慧合約、分散式雲端儲存和數位資產等。BC 是由鏈接在一起的帳本區塊組成。對等網路中的任何節點都可以選擇成為礦工，這是一個實體可透過解決資源密集型密碼難題(稱為工作量證明(PoW))，負責將區塊附加至 BC 上。當發生新交易時，將被廣播到整個網路。收到交易的所有礦工都透過驗證交易中的簽名來進行確認。每個礦工將已驗證的交易追加到自己的等待開採的交易區塊中。多個礦工處理單一交易的事實確保了 BC 的強健性。但是，這種強健性是有代價的，因為多個礦工都必須花費大量的資源來挖掘同一筆交易，同時又增加了延遲。BC 以下突出特性徵使其成為解決上述 IoT 安全和隱私挑戰的誘人技術：

1.去中心化：非集中控制，可以透過使用所有參與節點的資源，並消除多對一流量來確保可伸縮性和強健性，從而減少延遲並克服單點故障的問題。

2.匿名性：提供本有的匿名特性，非常適合大多數使用者身份必須保持私密的物聯網使用案例。

3.安全性：區塊鏈可在不受信任的各方之上實現了安全網路，這在具有眾多型式、功能、通訊方式不同設備的物聯網中是非常理想的。

但是，在物聯網中採用區塊鏈並非易事(尤其是比特幣)，將需要解決以下關鍵挑戰：

1.挖礦特別耗費運算資源，而大多數物聯網設備都受資源限制。

2.挖掘建立區塊非常耗時，而在大多數物聯網應用中，需要低延遲。

3.隨著網路中節點數量的增加，傳統區塊鏈擴展性越差。物聯網網路預計容納大量節點。

4.基礎的區塊鏈協定會產生大量的通訊開銷(耗用電力能源及網路流量)，這對於某些頻寬受限的物聯網設備所不樂見的。

Dorri,A.et.al.,[20]研究智慧家庭物聯網導入以類似比特幣區塊鏈為基礎的架構，可提供輕量級且去中心化的安全性和隱私性。不僅保留了區塊鏈的優勢，同時克服了上述區塊鏈區缺點而整合到物聯網中的挑戰。

Dorri 等人的建議架構考量一種典型的智慧家庭環境：住戶 Alice 為她的家配置了許多智慧家庭物聯網設備，包括智慧恆溫器、智慧燈泡，IP 攝像機和其他幾種感測器。圖 3-13 所示提議的架構包括三層，即智慧家庭(或更普遍的說是本地網路)，覆蓋網路和雲端儲存。

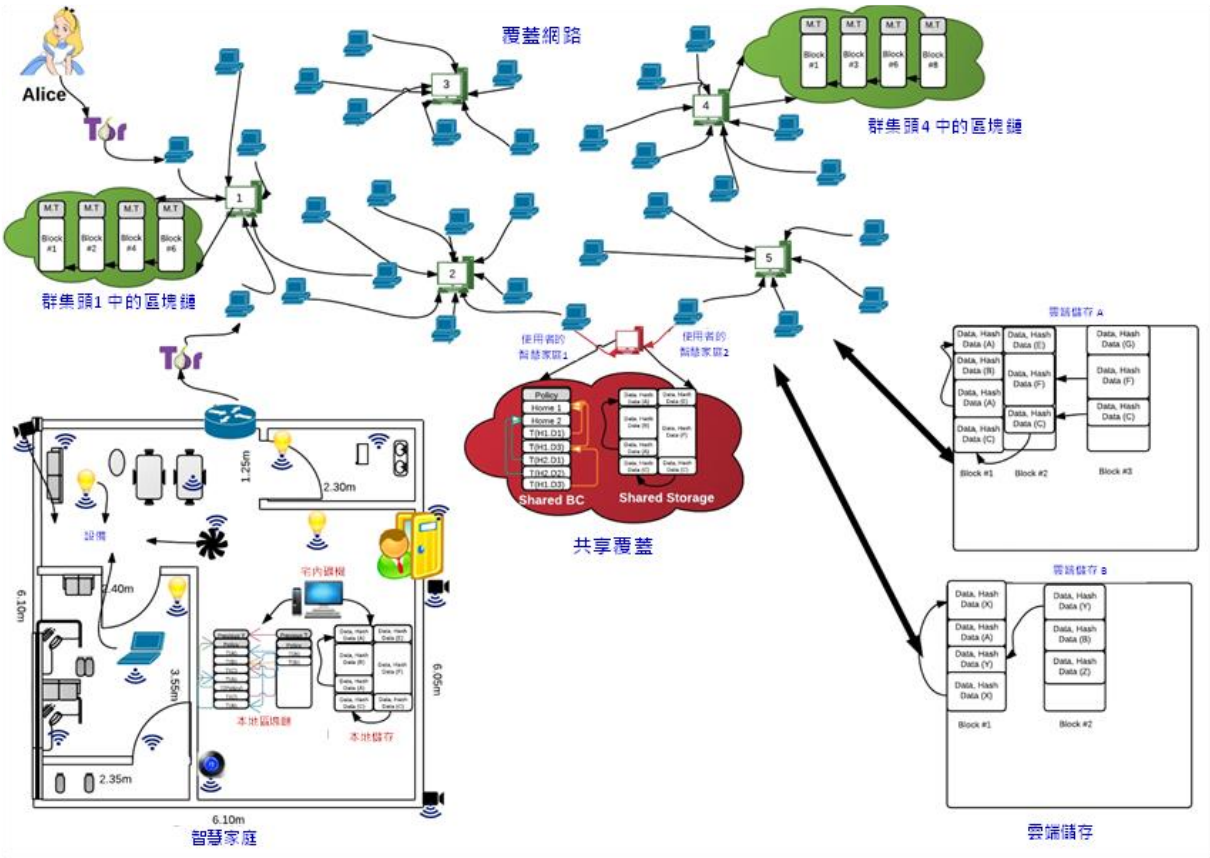


圖 3-13 智慧家庭物聯網導入區塊鏈研究示例(本報告譯釋)

資料來源:Dorri, A., S. Kanhere, and R. Jurdak, Blockchain in Internet of Things: Challenges and Solutions. arxiv, 2016.

圖 3-13 中架構考量數據儲存和訪問的使用情境:Alice 能夠從她的智慧家庭遠端訪問數據，例如她臥室中的目前溫度。而且，智慧設備應該能夠將數據儲存在協力廠商(例如，智慧恆溫器供應商)供其分析運用。本報告引用此研究示例說明區塊鏈在智慧家庭可能的應用說明如下：

一般比特幣使用者將已知可變公鑰(PK)，在成立交易時向網路廣播以轉移資金。這些交易被使用者壓入一個區塊中。一旦區塊填滿後，透過執行挖礦過程將區塊附加到 BC(區塊鏈)。為了挖掘一個區塊，一些被稱為礦機的特定節點試圖解開一個名為工作量證明(PoW)資源消耗的加密難題,而解決難題的節點可首先將挖掘的新區塊加入 BC 中。在此示例中，因為物聯網環境中採用 BC(一般比特幣、以太坊區塊鏈等)並不簡單，並且帶來了一些重大挑戰，例如：解決 PoW 的資源需求高、交易確認的等待時間長，以及廣播交易導致的可擴展性低，並阻塞了整個網路。藉由消除 PoW 的概念和對加密貨幣的需求，提出了一種創

新的 BC 例證。此研究示例提出的架構依據分層結構和分散式信任來維護 BC 安全性和隱私，同時使其更適合 IoT 的特定要求。

在此示例中智慧家庭情境中的架構也適合其他物聯網情境的應用。設計包括三個核心層：智慧家庭，雲端儲存和覆蓋網路。智慧設備位於智慧家庭層內部，並由礦機(礦工)進行集中管理。智慧家庭與服務供應商(SP)，雲端儲存以及使用者的智慧手機或個人電腦一起構成覆蓋網路，如圖 3-13 所示。覆蓋網路類似於比特幣中的點對點網路，並將分散式功能引入此一體系結構中。為了減少網路開銷和延遲，覆蓋網路中的節點被分組為群集，並且每個群集都選擇一個群集頭(CH)。覆蓋群集頭們結合兩份密鑰列表共同維護一個公共 BC。這些密鑰列表是：請求者密鑰列表，即覆蓋網路使用者的 PK(公開密鑰)列表，允許它們訪問連接到此群集的智慧家庭數據；被要求者密鑰列表，它允許訪問此集群的智慧家庭 PK 列表。因此示例之智慧家庭設備是使用雲端儲存來儲存和共享數據。

此示例中智慧家庭採取區域和私有 BC(區塊鏈)的設計，以提供 IoT 設備及其數據的安全連接存取控制。藉由 BC 特性的不可變、按時間排序的交易歷史，該歷史可鏈接到其他層以提供特定服務。設計的安全性來自多種功能，其中包括：(1)間接連接存取的設備；(2)智慧家庭和覆蓋網路中的不同交易結構。為了實現輕量級的安全性，智慧家庭設備採用了對稱式加密，並證明智慧家庭內部可實現了機密性、完整性和可用性，阻止諸如連接攻擊和分散式阻斷服務(DDoS)之類的關鍵安全攻擊。最後，研究還模擬得出定量的結果，呈現相關的間接費用相對較小。

一、智慧家庭區塊鏈核心構成要素

1.交易(Transactions)(即數據通訊)

智慧家庭設備或覆蓋節點之間的通訊稱為交易。BC(區塊鏈)智慧家庭中有不同的交易，每個交易都是為特定功能而設計的。儲存交易是由設備發起以儲存數據。由 SP(服務供應商)或屋主發起存取交易以連結雲端儲存。屋主或 SP 發起監視交易，以定期監視設備資訊。透過創世交易(類似數位加密貨幣的創世區塊)將新設備添加到智慧家庭中，並透過刪除交易將設備刪除。所有上述交易

都使用共享密鑰來保護通訊。輕量的雜湊法用於檢測傳輸過程中交易內容的任何變化。與智慧家庭之間的所有交易都儲存在本地私有的區塊鏈(BC)中。

2.本地(家庭)區塊鏈(BC)

在研究設計中每個智慧家庭內都有一個本地(家庭)私有 BC 追踪交易,並具有使用者策略(執行規則)的區塊頭執行傳入和傳出的交易。從建立交易開始,每個設備的交易都鏈接在一起,成為 BC 的一個不可變的帳本。本地 BC 中的每個區塊都包含兩個區塊頭,分別是一般區塊頭和策略區塊頭,如圖 3-13 上部所示。一般區塊頭中具有前一個區塊的雜湊,以保持 BC 不可變。策略區塊頭則對設備進行授權,以及對屋主的房屋實施控制策略。可能的交易是:存入本地的儲存數據、在雲端儲存數據,存取設備的已儲存數據,以及監視特定設備的存取即時數據。

3.家庭礦機(類似數位加密貨幣區塊鏈的礦工)

智慧家庭礦機是一種集中處理與智慧能家庭之間來回交易的設備。此礦機可以與家庭的網際網路閘道器或其他獨立的設備整合,設置在設備和網際網路閘道器之間;與現有的集中式安全設備類似,礦機對交易進行驗證、授權和稽核。此外,礦機還能完成以下附加功能:產生創始交易、分配和更新密鑰、更改交易結構以及形成和管理群集。礦機將所有交易收集到一個區塊中,並將完整的區塊附加到 BC。而礦機管理本地的數據儲存,因此提供了整體覆蓋網路內外額外的儲存容量。

4.本地儲存

本地儲存是一種儲存設備,例如 設備用作本地儲存數據的備份磁碟。儲存可以與礦機整合在一起,也可以是單獨的設備。儲存設備採先進先出(FIFO)方法儲存數據,並將每個設備的數據儲存為鏈接到設備起點的帳本。

二、區塊鏈智慧家庭運作方式

基本上分為設備安裝的初始化步驟,及後續運作時之交易處理(數據通訊)和共享覆蓋(整體區塊鏈網路)。

1.初始化

智慧家庭中新增智慧家電設備和策略區塊頭添加到本地 BC 的過程。為了將設備添加到智慧家庭中，礦機使用通用的 Diffie-Hellman 加密演算法並藉設備的共享密鑰來產生創世交易。礦機和設備之間的共享密鑰儲存在創世交易中。至於定義策略區塊頭，屋主將根據我們自訂提出的策略結構產生自己的策略(規則)，並將策略區塊頭添加到第一個區塊中。

2.交易(數據通訊)處理

智慧設備可以彼此直接通訊或與智慧家庭外部的實體直接通訊。家庭內部的每一設備都可以從另一內部設備請求數據以提供某些服務，例如，當有人回到家時，燈泡從動作感測器要求數據以自動打開燈具。為了實現使用者對智慧家庭的交易控制，礦機應該將共享密鑰分配給需要直接相互通訊的設備。收到密鑰後，只要設備的密鑰還有效，設備就可直接通訊。為了收回或拒絕許可授權，礦機透過向設備發送的控制訊息將分散式密鑰標記為無效。這種方法的好處是礦機(及屋主)擁有共享數據的設備列表，及設備之間通訊由共享密鑰保護。

設備將數據儲存在本地儲存中是家庭內部的另一種可能的交易流。為了在本地儲存數據，每個設備都需要透過共享密鑰對儲存(磁碟裝置)進行身份驗證。要授予密鑰，設備需要對礦機發送請求，如果它具有儲存權限，則礦機會產生共享密鑰，並發送給設備和儲存裝置密鑰。本地儲存裝置接收密鑰後，將產生一個包含共享密鑰的起始位址。設備有了共享密鑰，則可將數據直接儲存在本地儲存裝置中。

設備之間也有可能會將數據儲存在雲端儲存中，這被稱為儲存交易。將數據儲存在雲端上是一個匿名的過程。為了儲存數據，申請者需要一個包含一個區塊號碼和一個用於匿名身份驗證雜湊的起點。雲端儲存既可以由 SP(服務供應商)擁有和管理，也可以由屋主付費和管理(例如 Dropbox 雲端儲存空間)。在前者，礦機藉由設備密鑰產生簽名的交易來請求起點。後者，付款可透過比特幣完成。無論使用哪種儲存類型，儲存裝置都將在收到請求後創建一個起點並將其發送給礦機。藉由接收請求，礦機授權設備將數據儲存在雲端儲存中。如果設備已獲得授權，則礦機從本地 BC 提取最後一個區塊號和雜湊、建立儲存交

易，並將其與數據一起發送到儲存裝置。在儲存數據之後，雲端儲存將新的區塊號返回給礦機，以進一步儲存交易。

其他可能的交易是連結存取和監視交易。這些交易主要由屋主在外時監視自家或由 SP 處理設備數據以進行個性化服務所產生的。透過從覆蓋(區塊鏈網路)中的節點接收存取交易,礦機檢查所請求的數據是在本地儲存還是在雲端儲存上。如果數據儲存在本地儲存裝置中，則礦機從本地儲存裝置請求數據並將其發送給申請者。另一方面，如果數據儲存在雲端中，那麼礦機要不是從雲端儲存中請求數據，然後將其發送給申請者，要就是將最後一個區塊號和雜湊發送給申請者。後一種情況使申請者能夠讀取設備在雲端儲存中所儲存的全部數據，且適合所儲存的數據用於唯一設備時。如此避免了使用者的隱私可能受到威脅和侵犯。

3.共享覆蓋(區塊鏈網路)

另外，如果個人擁有多棟房屋時，則不需要為每棟房屋分別設置礦機和儲存裝置，以降低成本和管理開銷，因此引用的研究示例定義了共享覆蓋。共享覆蓋包括至少兩個智慧家庭，這些智慧家庭由共享礦機進行如同單一家庭般的集中管理。共享覆蓋類似於智慧家庭,但是共享 BC 的結構與智慧家庭的結構不同。在共享的 BC 中，每個家庭都有一個創世交易，並且所有設備的創世交易都由共享覆蓋的礦機鏈接到其家庭的創世交易。共享覆蓋中的另一個區別是房屋與礦機之間的通訊。與礦機位於同一家庭中的設備沒有任何變化，而對於其他家庭中的設備,則在每個家庭中的網際網路閘道器之間建立虛擬專用網路(VPN)連接，而共享覆蓋的礦機將數據封包按此路線發送到共享礦機。

三、區塊鏈智慧家庭的安全性與效能

任何安全設計都需要滿足三個主要的安全要求，即機密性、完整性和可用性。機密性確保只有授權使用者才能閱讀訊息。完整性確保發送的訊息在目的地被接收而沒有任何更改，可用性意味著在需要時使用者可以使用每個服務或數據。而為了實現智慧家庭的設備可用性，應保護設備免受惡意申請的侵害。這可藉由區塊鏈機制在每個設備之間建立共享密鑰而實現可接受的交易(數據通訊)。

從覆蓋(區塊鏈網路)收到的交易在被轉發到設備之前，已被礦機驗證合法。並且所舉示例與現有的智慧家庭閘道器產品相比，BC 架構僅在交易(數據通訊)處理方面只有少量延遲，以及在增加新設備初始化期間，存在著額外產生和分發共享密鑰的一次性延遲。但總體而言，經驗證額外延遲並不嚴重，並不會影響智慧家庭設備的可用、即時性。

第四節 智慧家庭區塊鏈數據分享的研究示例

隨著資訊和通信技術的發展，智慧家庭物聯網生態系統正在經歷一場轉型。智慧家庭應用一直以來主要挑戰是確保安全性和隱私性。但越來越多從其他產業領域看到的趨勢，利用整個產業生命週期不斷產出的資訊，從中分析獲得創新發展的機會。

圖 3-14 智慧家庭與產業創新發展

資料來源：智慧化居住空間產業發展計畫(2005)

內政部建築研究所從推動智慧建築之初，就一直有著藉由推動智慧家庭發展創新價值產業的目標與期待，如圖 3-14。目前智慧家庭的應用日益普及，除了上述確保使用者數據的透明性，安全性和隱私性需求外。更因區塊鏈技術的發明，可利用其分散式、可信任、不可篡改、智慧合約等優勢，似可解決社會關注的智慧家庭各方面應用，可信數據收集，並激勵創造新價值鏈的問題。

區塊鏈技術可能適用於智慧家庭應用。這樣的一種應用是與第三方服務提供商(如醫院，超市等)共享智慧家庭數據。區塊鏈技術有助於消除該系統中潛在的潛在威脅並贏得用戶的信任。本節回顧了與區塊鏈的智慧家庭應用程式開發有關的目前趨勢。主要側重於智慧家庭數據市場，訪問控制管理，家庭護理，

自動公用事業付款和智慧城市服務。這些應用正在引起研究人員和產業的關注，並被許多人視為未來的智慧家庭物聯網服務。

如果可以讓使用者確實控制的數據隱私和共享策略，並解決所有安全性、隱私、使用者透明性和控制權以及數據共享的激勵措施等問題。使用者成為自身數據的真正擁有者，可以決定他們的數據如何被收集和被使用以及如何共享，這不僅可以從改進提升的個性化服務體驗中受益，而且，例如直接可以透過參與服務供應商產生的廣告收入中共享受益。因此，迫切需要一種適合智慧家庭數據分散的，安全特性的數據市場機制。

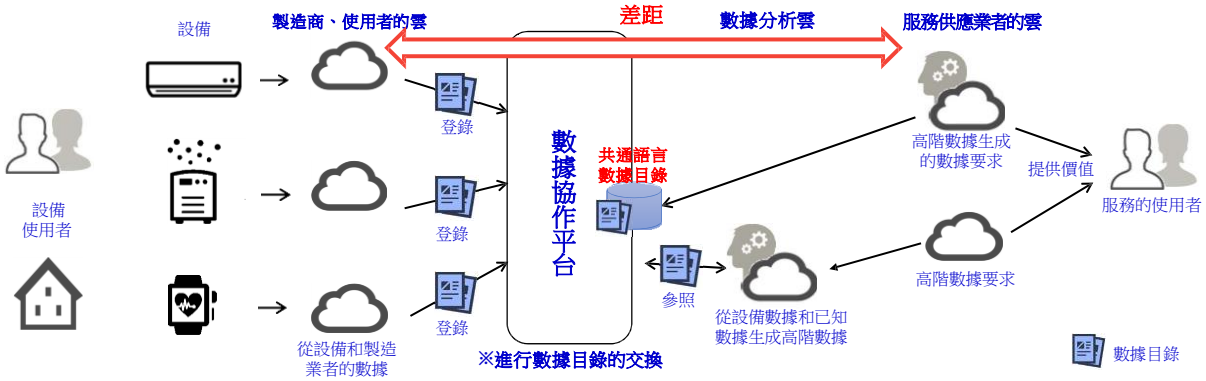


圖 3-15 日本智慧家庭數據目錄架構

資料來源：日本電子資訊技術產業協会(JEITA)，《JEITA スマートホームデータカタログ項目定義書V1.0》，2019

日本也是因為促進智慧家庭內外的所有設備、住房設備、服務等與生活數據相連結，以產出社會問題的解決方案和進行滿足消費者需求之先進的服務。日本經產省於 2019 年委託社團法人電子情報技術產業協會(JEITA)的研究[22]，制定"智慧家庭數據目錄項目定義文件 V1.0"中所提出的數據共享架構類似(如圖 3-15 所示)，只是必須透過網路查看數據目錄後，得知是誰擁有數據的元數據，再藉由實際聯繫取得原始完整的智慧家電廠商收集或使用者產出數據。

Moniruzzaman, M. 等人[23]所提的架構類似日本 JEITA 的構想，並導入區塊鏈不可否認、分散式、不可竄改及智慧合約的特性，建構可實際運作實現智慧家庭數據安全市場的交易的系統，如圖 3-16 所示；此研究示例說明有關區塊鏈如何可實現智慧家庭數據安全市場的交易步驟如下：

- 從智慧家庭數據生態系統中，部分匿名的數據和元數據將顯示給數據入口網站，以供潛在的購買者使用。

- 所有數據使用者都可以訪問此入口網站，一旦數據樣本和價格滿足消費者的需求，他們便要求向數據所有者(智慧家庭)進行交易。
- 根據提供者和消費者之間的商定價格，數位加密貨幣交易由智慧合約啟動。
- 一旦價金轉移到服務供應商或使用者的區塊鏈帳戶，就開始透過獨立通道將數據從智慧家庭數據儲存庫傳輸到數據消費者儲存庫。
- 當所有交易完成後，雙方都根據代表代理人的體驗質量(QoE)的等級量表(例如 1 到 5)相互推薦和評價。推薦的回饋資訊儲存在區塊鏈中，以便將來可能客戶得以更容易的分析。

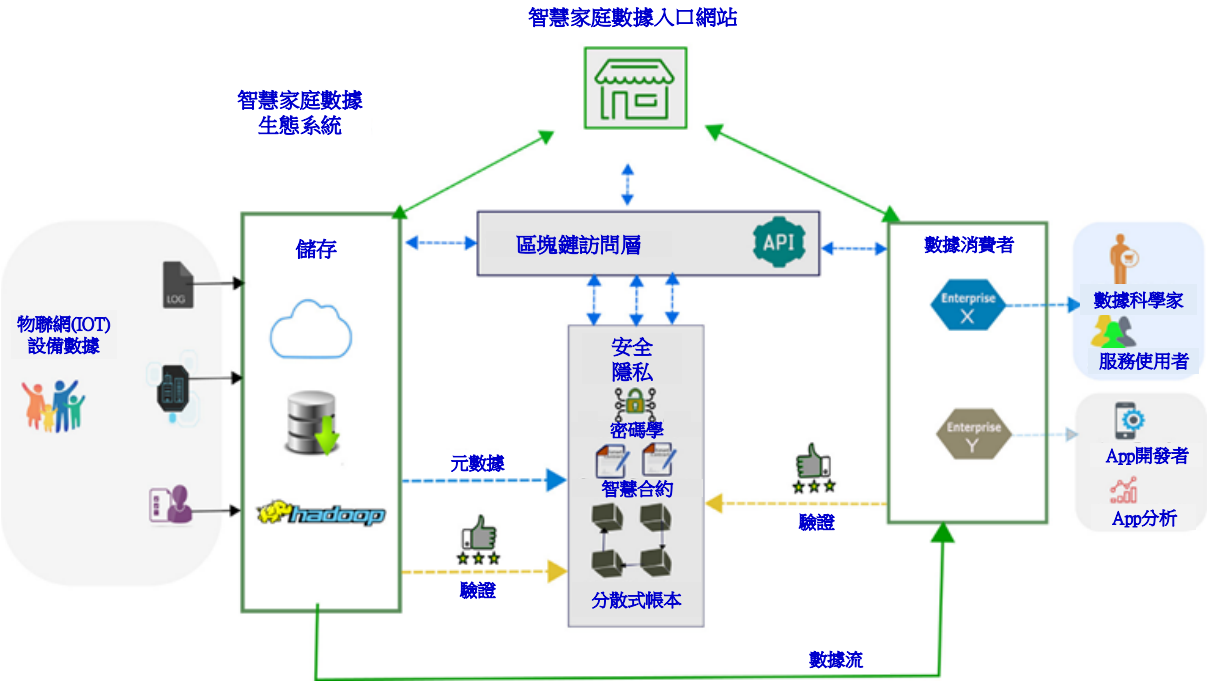


圖 3-16 應用區塊鏈的智慧家庭數據市場

資料來源：Moniruzzaman, M., et al., Blockchain for smart homes: Review of current trends and research challenges. Computers & Electrical Engineering, 2020.

1. 共享智慧家庭數據的機制

本示例來源文獻曾經收集探討一些區塊鏈技術在數據市場中使用的研究：有的將區塊鏈應用於異構數據產品，提出了數據市場架構的數據展示市場入口網站和用於公共交易對話的伺服器。數據集實質上是上傳到平台中的，而元數據則儲存在區塊中，以避免利用昂貴的區塊資源。以此輕量級的區塊鏈機制對於不熟悉可信任第三方供應商，是期待可達到智慧家庭使用者敏感資訊機密的

保持，惟此建議的體系結構中則尚未導入使用者之間的交易合約；有的研究是在數位分散式帳本基礎上，提出一種驗證數據的真實性和利益相關者的協議機制，想法是匯總由小規模生產者(例如當地藥局)產生的微型數據集，登入線上藥品入口網站以提供潛在有數據興趣者購買。但此該解決方案不能防範此數據市場中參與各方可能的欺騙行為；另有研究提出為回收產業客戶建立中央數據共享平台。例如，來自客戶的資訊，包括性能降低的產品、生產和消費後廢物管理，對於產業提高他們的效率和產品質量是有價值的。這種機制，智慧家庭回收設備的數據可以為家庭住戶和製造業雙方產生一些潛在的創新應用機會。

2.智慧家庭數據整合

研究示例彙整多項研究成果探索數據分享系統中使用區塊鏈技術，以確保數據市場的服務質量。其中是以以太坊區塊鏈開始導入的智慧合約功能可將產品元數據存儲在區塊鏈中，潛在有興趣買家可以訪問存取，並且如果滿足要求，他們需要藉助流數據支付協議和區塊鏈進行支付。在區塊鏈之上，還實施了一個額外的智慧合約，以推薦相關方的服務質量(QoS)。儘管使用兩個智慧合約的想法必然提供兩種服務，但是並未說明每種區塊鏈量身定制的詳細機制；為了提高數據的質量和完整性，也有其他研究提出一種審查系統(例如，推薦系統)，利用以太坊智慧合約，JavaScript 和 Node.js 在支持 IoT 的數據生態系統和潛在購買者之間進行數據交易，但不同建議的字符串長度將消耗較高的 Gas 值(即以太坊區塊鏈操作消耗的手續費)。

3.機器學習和 AI 用於智慧家庭數據交易

區塊鏈可以運用機器學習和 AI 交易機制。已有研究者提出了一種以區塊鏈為基礎的數據市場模型；此模型不使用 Hadoop 分佈式文件系統(HDFS)，而是使用群體文件系統(SFS)來存儲原始數據。SFS 返回文件處理程序，作為數據有效負載結構，加密模式和加密密鑰索引的加密雜湊的一種形式。從 SFS 到解決方案供應商的傳輸過程中，此技術可優化相關通訊與運算開銷。該模型提供了靈活的數據查詢機制。但是，將數據存儲到 SFS 需要 30 分鐘以上，這對於要求即時回應的關鍵系統是不可行的；另有新研究指出採用其他數學模型來因應複製和公平性等需求。此機制的關鍵部分是購買者提取從整個數據集中獲取的必需

特徵，而不是獲取整個數據集，從而顯著降低了間接費用。購買者不是從賣方或經紀人那裡購買原始數據，而是獲得準確性更高的機器學習算法。一旦達到預測精度，就可以提取收入，並將金額分配給所有利益相關者。這種方法極大地支持了小型智慧家庭數據所有者測量其數據質量並獲得更多收益。Moniruzzaman, M., et al.彙總以區塊鏈為基礎的智慧家庭數據市場技術，如表 3-1。

表 3-1 區塊鏈為基礎的智慧家庭數據市場機制比較[23]

文獻	區塊鏈機制	關鍵性	效益	限制
Nasonov et al.	基本架構	無關業務領域的去中心化市場入口網站陳列數據。	藉由分離元數據降低負荷，減少區塊中的搜索時間。	沒有考慮使用者之間的契約機制。
Banerjee et al.	未定義	不分類型業務域的數據市場。	確保安全、隱私、公平和遵守規定。	市場公平性不可擴展。
Lawrenz et al.	未定義	回收產業的交易平台。物聯網數據市場審查系統。	增進效率、數據安全。透過降低資源利用來增強審查數據的不變性。	未考慮數據品量。沒有考慮激勵機制。
Park et al.	以太坊智慧合約	物聯網數據市場審查系統	過減少資源利用來增強審閱數據的不變性。	沒有考慮激勵機制。
Ozyilmaz et al.	以太坊自證明檔案系統	物聯網設備供應商和 AI/ML 解決方案提供商。	優化數據傳輸開銷。	儲存區塊數據需要很長時間(大約 30 分鐘)。

我們可以理解早期為數不多的智慧家庭數據共享研究，大多為了解決安全性，隱私性，公平性漏洞相關的問題，這些問題被視為願意共享或出售其寶貴數據的智慧家庭住戶的障礙。但如上所述，可確認藉由區塊鏈的導入而解決這些問題。與集中式系統相比，區塊鏈技術對使用者完全透明，並且很有希望激勵使用者分享數據。它自然也支持根據智慧合約中的獎勵(小額付款或信譽)鼓勵使用者分享數據。

前述研究說明確保了使用者擁有數據的控制權，同時以去中心化方式支持不同企業間與數據科學家的數據共享。數據共享的某些議題與嚴重的隱私和安全因素有關。即使是最知名的社群平台也經歷了安全漏洞和數據被駭事件。前述研究示例的共享平台還需要一種有效的激勵機制，可在分配公平激勵的同

時，實現訪問使用者數據的透明化。而到目前分散式帳本技術廣為設計去中心化 P2P 網路的最有效手段之前，還沒有一種通用的方法，可用來追踪誰共享什麼、與誰共享、何時共享、什麼目的、在什麼條件下，及以可驗證的方式交換資訊。以區塊鏈和智慧合約為基礎的去中心化使用者數據共享平台，將使用者控制數據共享的實踐概念化。透過將智慧合約儲存在區塊鏈中，使用者可以保留數據所有權，並按照約定的條款進行激勵。

上述示例架構可確保實際使用者數據永遠不會暴露於區塊鏈。首先將使用者數據進行雜湊處理和加密，然後再將其上傳到鏈下儲存(此示例採用 hadoop)中。客戶端應用程式中的數據所有者可以將其直接儲存在鏈下儲存中。有關訪問使用者數據的條款和條件與數據的元數據和雜湊一起編碼在智慧合約中，並發佈在區塊鏈平台(以太坊)上。區塊鏈上數據的雜湊值可避免中介軟體篡改數據。以內容作為尋址的原理是利用數據的雜湊值作為檢索的標識符。當數據利用者調用智慧合約訪問使用者數據時，只有成功調用合約才能釋放解密使用者數據的密鑰。然後，受信任的程式從區塊鏈中提取雜湊值，使用雜湊值從鏈下儲存中檢索數據，進行解密並釋放給數據消費者，同時建立對數據所有者的激勵機制。區塊鏈和智慧合約透過向使用者提供有關誰、何時、何地訪問其數據的完全透明化的支持，允許使用者指定數據共享的目的、範圍，可以共享的數據種類以及應用類別/公司，即可以訪問數據並激勵使用者共享數據的公司(按照合約規定，按應用使用數據付費)。

此示例組織結構提出了底層的鏈下使用者數據儲存機制，此機制或可由可信第三方管理的集中式數據儲存。當信任處於所有數據儲存和管理集中的服務供應商之內時，很難減輕各種風險，例如，數據未經使用者同意而濫用、駭客入侵或出售給任何其他機構，甚至在公司的預設下被銷毀。因此，另外建議一個具有獨立私有許可制的區塊鏈新平台，稱為 MultiChain，作為鏈上和鏈下數據儲存、加密、雜湊和數據追踪，以及利用以太坊進行訪問控制的解決方案。MultiChain 可以成功實現數量有限的點對點鏈下區塊鏈儲存使用者數據。使用者可以選擇將任何已發布的數據以鏈下方式儲存，從而節省了儲存空間和頻寬。Shrestha et al.,[19]提出儲存鏈下數據並透過 MultiChain 訪問存取它

們，和其他人例如 Yang 等人(2019)及 Ferrer-Sapena & Sánchez-Pérez(2019)等的研究，也提出了類似的想法。MultiChain 節點處理關鍵操作，例如對使用者數據進行雜湊處理和加密、在本地(區塊鏈外部)儲存加密文件、在區塊鏈上提交文件的雜湊、搜索所需數據、驗證數據並交付數據。

第五節 國內智慧家庭應用區塊鏈初探

推動智慧城市及智慧建築有很多方面，例如智慧健康醫療、智慧交通、智慧電網、供應鏈管理、金融系統和數據中心網路，其實就是物聯網甚至萬事聯網(IOT)的展現。此外，還有如何應用數位科技進行公共治理的問題，區塊鏈技術優勢(分散式、可信任、不可篡改、智慧合約等)解決傳統中心化大數據、人工智慧應用過程中，數據孤島、數據安全威脅、數據確權與加值應用等問題。

智慧家庭的應用日益普及，對確保使用者數據的透明性，安全性和隱私性需求非常重要。一樣可結合區塊鏈技術優勢，從社會關注的智慧家庭應用家庭照護和第三方醫療系統之間的互動需求、智慧電網中輔以 P2P 的能源交易，智慧家庭可信的數據收集及交易平台，以激勵數據收集並創造新的價值鏈。

以下簡單介紹目前所知的國內智慧家庭應用區塊鏈

一、智慧照護服務應用區塊鏈

台灣受恩股份有限公司主要從事基於物聯網的智慧照護產業，發展居家、社區照護據點及城市服務中心等連續性智慧照護服務整體方案；並與優質第三方的產品、系統及服務合作，形成開放、包容、合作、共贏的產業發展新模式，並期望善用科技提升高齡者生活品質，讓照護人員縮短瞭解被照顧者的習性與需求，提供個別化的服務，使長輩感受到尊重，並能讓被照顧者家屬在第一時間關心安心長輩的狀況；因此，台灣受恩積極運用智慧照護系統，發展個別化服務，讓家屬安心，長輩開心，實踐在地老化[24]。觀察受恩得出二項重點：

- 以物聯網+互聯網，創新養老照護服務
- 以跨界平台整合，營造長照產業發展契機。

但就如本報告前述分析物聯網數據收集過程一定遇到的安全隱私，以及後續數據分享機制等等的問題。受恩為了串聯二者一樣需要收集大量的數據進行分析研判，對受照護者而言可得到更即時貼心的客製化服務；對受恩而言人力運用更為妥適與人性化。對公司而言管理更有所本與方便，並能持續發展創造新的商機。這些都是進一步導入區塊鏈之後各方更能放心提供數據共享之後的效益，如圖 3-17。

圖 3-17 台灣受恩物聯網區塊鏈的智慧照護服務

資料來源：內政部建築研究所, 第 12 屆『創意狂想 巢向未來』2019 智慧化居住空間創意競賽專輯

二、智慧家庭應用區塊鏈保護用電隱私

國內家電大廠禾聯碩公司是台灣一間以電子工業為業務核心的企業，一開始投入液晶顯示器產業。其前身為聯碩光電，於 2009 年更改為現名。在國內市場全力經營"HERAN"之自有品牌；目前產品包含空調、視聽產品、冰箱、廚房家電、生活家電、洗衣機，並以擴大到商用液晶、冷凍匱、空調等產品。

禾聯碩集團近幾年又跨入集合住宅的建設，充分利用本身智慧家電及 AIOT 產品的優勢，建設智慧化集合住宅建築。事業集團考量智慧建築全生命週期中的服務需求，提供客戶真正有感的智慧住宅。如圖 3-18 所示，除了智慧建築、智慧家庭內部可應用禾聯碩的智慧化產品，並在此智慧化基礎上衍伸出相關生活服務，包含各種生活繳費、付款、外送、叫車，遠距醫療服務；內容服務主

要包含各種線上影音服務；結合外部線上電商提供更便利的服務。於此整合平台可讓合作的上下游廠商共享數據資訊，進行分析提供不同住戶更有感貼心便利的客製化服務。不過正如本報告關注的重點，即智慧家庭住戶的數據隱私保障，及鼓勵分享的激勵機制；禾聯碩目前也意識到住戶的數據隱私的重要性，因此透過區塊鏈加密分散儲存並進行鎖碼確保資訊安全。

圖 3-18 禾聯碩 AIOT 智慧家庭產業鏈示意圖

資料來源：建築空間導入 AIoT 技術應用(節能管理類)交流座談會活動《禾聯碩 AIOT 智慧家庭產業鏈報告》

從上圖可以看出禾聯碩平台與前述研究示例在智慧家庭內側就採用區塊鏈的保護數據機制不同，禾聯碩在智慧家庭內側的產出數據的保護，是採用硬體加密模組，依據硬體模組上的安全策略做即時的加解密運算；具了解，目前重點聚焦在於智慧家庭節能管理，將家庭內部用電量傳輸到共享平台，不僅讓住戶了解家庭用電情形，並提供聯盟廠商的分析應用為使用者提供最適化服務，進行節能管理獲得經濟效益；因此，在共享平台上導入區塊鏈以保障數據的隱私、安全性等，並可促進產業間之合作。

第四章 智慧社區應用區塊鏈機制建議

智慧城市應用涵蓋了許多領域，包括基礎設施管理、地方政府房地產管理、實體安全、交通、運輸和流動性、污染和環境監測、電力和其他公用事業(還包括公用設施的人孔監控)、減輕洪水、智慧城市照明、實物資源分配物流及可居住性。從許多智慧城市文獻中可以發現，智慧城市涵蓋項目大多包含智慧家庭。

因為智慧建築、智慧家庭是智慧城市的基本單元，而我國土地狹小人口密集的情況下，很難有獨立的智慧住宅，尤其都會地區絕大部分是社區型態的集合住宅。最近幾年政府為了解決都會工作者的居住困境，鼓勵大量興建社會住宅或公共住宅提供租住。為了提升這些社會住宅與公共住宅的生活品質，達到安全、健康、便利與節能的目標，一定要求導入智慧化設備或系統，取得智慧建築標章。所以不論社會住宅單元或所屬公共空間，既然導入智慧化就會有各種設備感測與服務數據的產出，可以進一步分析，以提升更安全、健康、便利與節能的效能，甚至利用數據分享創新加值應用。

第一節 智慧建築、社區導入區塊鏈的需求

社會住宅(social housing)，在歐洲又稱「社會出租住宅」(Social Rented Housing，更強調其「只租不賣」的精神)，簡單的說是指政府（直接或補助）興建或民間擁有之合於居住標準的房屋，採只租不賣模式，以低於市場租金或免費出租給所得較低的家戶或特殊的弱勢對象的住宅。

一、國外趨勢概述

我們可以建築全生命週期的方式來思考社會住宅，即規劃設計、建造、招租入住，管理維護及最後更新拆除重建等，每一階段其實都可應用區塊鏈技術，其中規劃設計、營建過程區塊鏈的應用，可參考作者去年報告[2]或所附參考文獻。其中亦有初步介紹日本積水建設之租賃部門導入區塊鏈進行租屋仲介、及與其他產業聯盟合作創新加值的應用。似乎房地產業者導入區塊鏈技術成立仲介平台進行仲介業務已蔚為潮流[25]。甚至有學者以以太坊區塊鏈建構房屋租賃系統解決方案[26]，提出無中介的方式實現租房來源資訊透明的點對點共享

機制，將傳統租賃協議轉化為區塊鏈智慧租賃合約。不僅提高租賃流程效率，並為租賃流程儲存交易記錄，為租戶和房東提供不可否認、無法竄改的法律，且區塊鏈智慧合約自動執行的保障。該系統組成還利用 IPFS(星際檔案系統)在內的大數據新興分散儲存技術，用於鏈下儲存較大量資訊數據，以太坊鏈上的智慧合約則用於管理 IPFS 資訊清單的雜湊值,除減少區塊鏈各節點共識計算及通訊的開銷外，並可確保鏈下儲存數據資訊的正確性。

二、國內需求概述

國內建設社會住宅不論中央與地方，正如前述規劃設計建造大多要求導入智慧化，取得智慧建築標章；以臺北市政府為例規劃要求社會住宅成為智慧社區示範場域，以營建經費外加 3-5% 建置智慧化設施，尤其強調設置智慧三表(水表、電表、瓦斯表)；因此，為使建築物設備及系統在運轉時可達到更高的能源使用效率，公開徵求提案尋求合適廠商協助 AI 大數據分析-智慧電表數據，希望透過商業大數據蒐集與判讀，以圖像化儀表板提供局處與住戶節能建議。其他新北市政府與桃園市政府都有類似需求，只是解決方式相信是由所建構的所謂戰情中心紀錄匯集數據進行分析，至於是否有類似台北市政府進一步藉由 AI 大數據分析應用，因為未曾訪問調查，尚未可知。

從以上台北市政府公共住宅公開徵求提案的作為可知，目前是希望在使用管理維護階段的電力節能管理的重要性，是首先被認知與付之開始行動的項目。台北市社會住宅管理單位目的是希望在住戶尖、離峰 24 小時用電期間，運用智慧電表數據進行 AI 大數據分析，分析各個用電迴路用電狀況，透過商業大數據蒐集與判讀,以圖像化儀表板提供局處與住戶節能建議,透過 APP 和 Line 進行節能通知,並提供局處與社區於擬定節能發展策略時的重要參考依據[27]。

然而，台北市政府的社會住宅標案，都是要求取得銀級以上智慧建築標章。除了系統整合、綜合佈線、資訊通訊、設施管理基礎指標之外，功能性指標應該不僅只於節能管理，至少一般都還具有安全防災，社會住宅有的兼具健康照護功能，而我們從前章智慧家庭研究示例及國內案例，知道其實對住戶有感的是舒適便利的智慧家電等設備。

社會住宅既已取得智慧建築標章，表示公共空間已具備一定程度的智慧化功能，且如上述台北市政府更進一步達成均衡負載住宅單元用電，及依日本智慧家庭組成[28]顯示此節能管理功能或可擴充成真正的家庭能源管理系統(Home energy management)(如圖 4-1)，並成為智慧社會住宅社區的單元各戶智慧家庭功能的基礎平台。

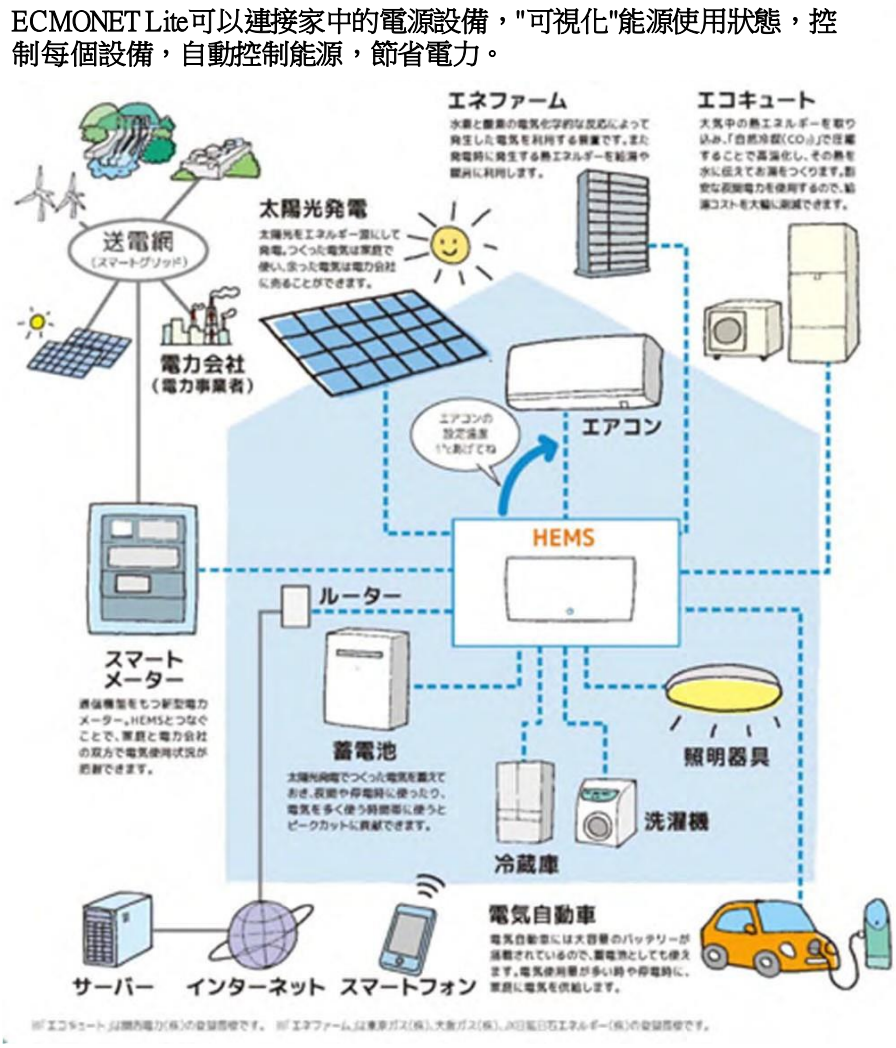


圖 4-1 日本智慧家庭組成示意圖

資料來源：笹川雄司, スマートハウスビジネスの現状. 2018.

因此初擬社會住宅(集合住宅)智慧家庭單元功能共有四大面向：1. 健康照護方面：在居家環境中利用感測器與自動控制系統，進行紅外線影像監測，與緊急求救裝置，預防意外發生無人反應進行救護。2. 安全防災方面：透過感測器辨識與偵測可疑入侵事件，與火警感測訊號移報，自動傳輸影像與聲音警示給住戶及管理單位。3. 節能管裡方面：透過感測器偵測室內的電力、用水、瓦

斯等使用，分析使用模式並提供可視化介面，管理單位與住戶雙向均衡需量負載，達成節能與節費。4. 便利舒適方面：提供照明、空調等智慧家電設備感測回傳數據進行分析最佳化調節，達到居住環境的舒適度。提供智慧家電租賃維修服務、生活各項繳費、電商等生活便利服務。

初步參考相關文獻[13, 18, 19, 29-34]，綜合建議住宅、社區區塊鏈應用情境如下圖所示。

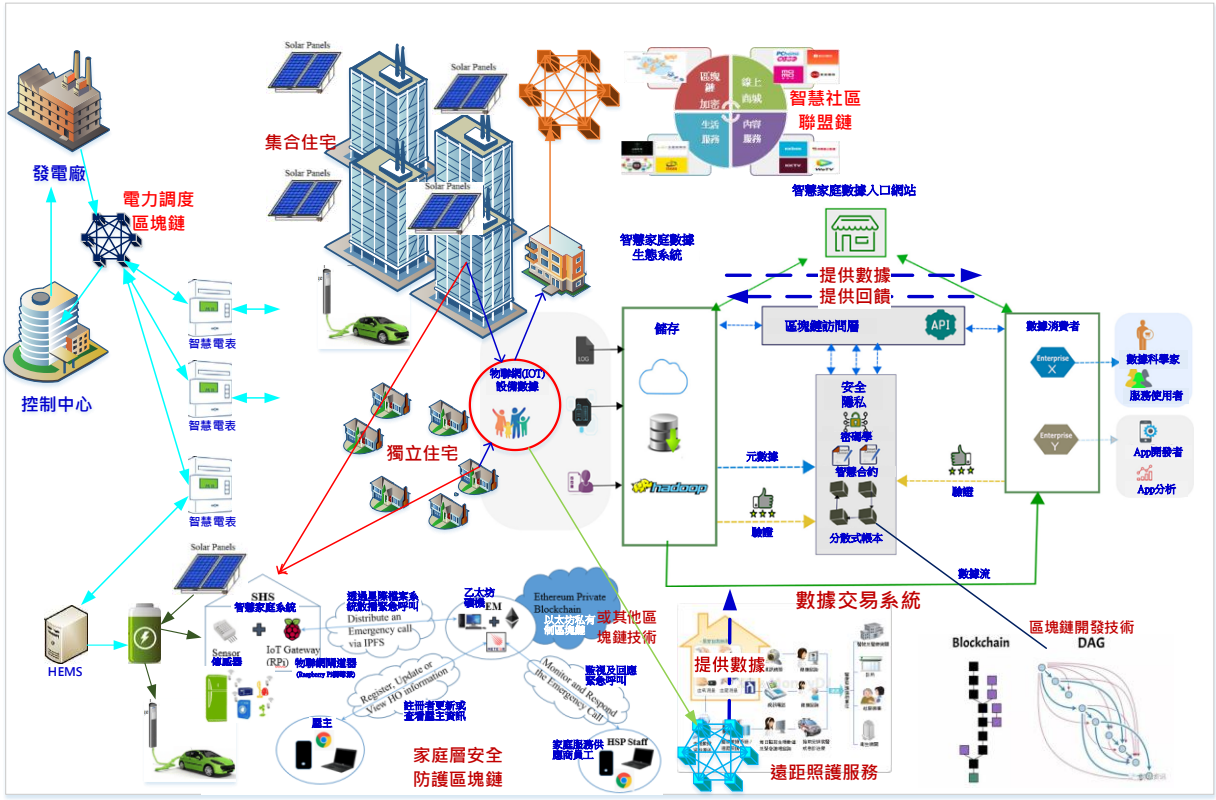


圖 4-2 智慧家庭、社區區塊鏈應用情境圖

上圖情境中包含集合住宅(社會住宅)及獨立住宅中智慧家庭環境住戶、家電設備、感測器等所有可產出安全、健康、節能、便利等等所有可被收集數據應用的情境。如電廠、大樓、住宅、再生能源、電動車甚至與第三方能源管理公司合作等彼此之間形成微電網，進行電力數據分析及調度；住戶健康數據收集提供遠距照護服務分析建議，甚至數據經過加密安全的與生物、醫藥科技公司共享，以分享研發成果獲得實質激勵效益；另外，家庭娛樂、家庭相關維修服務數據即時共享，提升整體服務品質及生活水準；圍繞家庭、社區生活的各種服務需求，都可透過區塊鏈安全隱私、透明不可否認的特性，實際促進住戶

與服務供應商良性互動，讓數據分享的提供與實質激勵成真，新興智慧化關聯服務產業興盛發展。

第二節 智慧家庭、社區(社會住宅)導入區塊鏈的建議架構

都市化是世界共同的趨勢，人們向城市中遷移居住在社區，造成城市基礎設施能力的挑戰，為了滿足市民對能源、水、交通、醫療、教育和安全的需求。智慧城市技術是對城市永續發展的重要貢獻，使智慧城市成為現實。家庭自動化的概念必須考慮到新技術和新的智慧化使用者，家庭、住宅將不再被視為一個單一的實體，而是新社區乃至城市概念的基本組成部分。智慧社區、城市的理念發展極其迅速，將智慧電網、服務、建築、住宅和家電設備整合在一起，這些設備、子系統必須都能夠偵知、聯動、連接和分析(不論遠端、雲端或霧、邊緣運算)並協同作業控制，以實現更好的生活品質、可持續性、節能、社會經濟發展。智慧城市的普及進步很大程度上決定在一般民眾、管理者、服務供應商及政府治理部門對 ICT、IoT 和 BC(區塊鏈)的理解和掌握處理的能力。

到 2025 年，全球智慧電表和家庭自動化市場將增長到 440 億美元，智慧家庭設備的市場潛力正在高速成長不僅在能源效率方面，而且在安全、福利和健康服務方面的潛力也越來越大 重要的是,未來家庭住宅將融入更多連接到網路的技術，所有設備都是智慧和可互操作的系統[35]。目前有能源、水和天然氣、太陽能系統生產、充電站、健康照護設備、娛樂和安全家電設備等的智慧計量。所有這些都將能夠為新住宅提供控制措施和優化管理。智慧特性不僅包括所有連接的系統都將受到控制，而且還包括即時和優化的管理；以下針對上述圖 4-2 情境，說明如何以區塊鏈和物聯網(BC+IoT)來實現智慧家庭與社區，及數據分享應用與激勵機制。

圖 4-2 情境的構想是不論是獨立住宅、透天厝、公寓、社會住宅(在此視同集合住宅),其實單元都是智慧家庭,差別在集合住宅具有公共設施及服務空間。

一、智慧家庭、社區設備層

要達成上述描述情境，需要智慧家庭、社區(甚至城市、國家)有著必要的網路基礎建設，才能在此基礎搭建各種軟硬體平台；但在建築、社區私領域部分，包括建築與家庭內部的智慧化，必須讓環境、設施設備等具有感知、互聯、及互動的功能，如下圖 4-3 底層設備層；這些底層設備彼此的偵測、感知、聯動過程中，必須確保如監視攝影機不被入侵保護隱私、智慧門鎖等門禁系統不被不被入侵的安全性；甚至如所前所分析智慧家庭可能被惡意入侵者透過網路入侵閘道器、設備、感測器等從而發起各種攻擊的可能性

雖然針對家庭智慧化設備，相關防毒軟體業者已開發出硬體防範保護設備，但僅止於防備從網路路由器進來的異常行為，並無法提供智慧家庭底層設備彼此之間互聯互動的安全保護需求；因此以簡單、傳輸速率快，無須交易費用的區塊鏈技術；相較於傳統區塊鏈技術，要將感測數據(即交易)層層進行雜湊運算，上傳鏈結等程序，速度方面無法達到即時監測控制的反應需求；因此，以數學圖論有向無環圖 DAG 發展而來的 Tangle 技術(如 IOTA)，就可提供單筆交易(數據)驗證串聯，達成不可竄改、透明、安全且即時的應用。

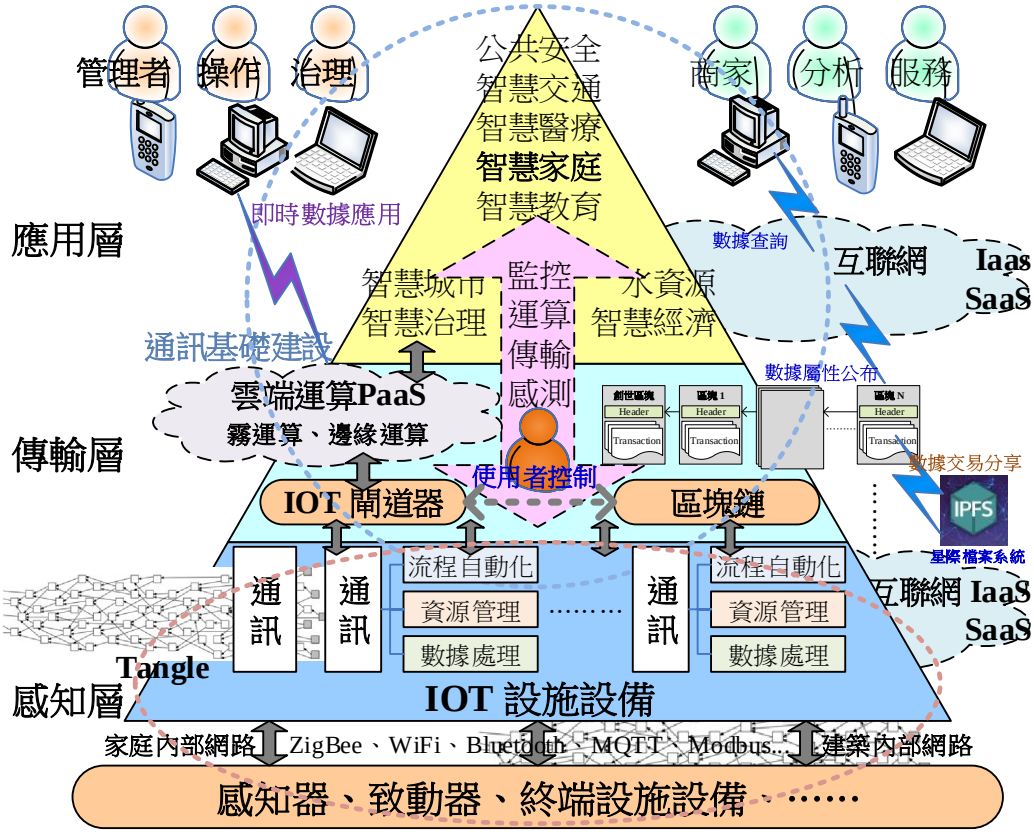


圖 4-3 智慧家庭、社區導入區塊鏈的建議架構

二. 智慧家庭、社區應用層

我們知道智慧家庭的應用不應僅止於家庭內部設備的自動化帶來的安全監控、節能管理、健康照護、便利舒適的更能外，更希望所產出的數據，能夠促進數據的共享應用，讓相關服務產業得以因應環境社會的變遷而創新發展。

相關服務產業可分為二方面：一是智慧家庭內部、二是社區公有部分的相關服務。

每個家庭因為成員組成，生活習慣不同，導入應用的設施設備也不同，所需的服務也不同，必須個別提供及客製化；例如，健康照護，每個人年齡不同所需要的醫療照護屬性就不一樣，更何況每人都有自己屬意的醫生診所、醫院的；家庭內部設施設備、家具裝修等等日常的保養維護更新，也都是不同的服務提供者；各戶家庭安全監控也因為成員組成屬性不同，內部門禁入侵、火警預防警告等防範需求也不同，不見得願意參加社區共同導入的服務平台。因此智慧化外部服務供應商較難組成企業聯盟型式，以共享數據分析聯動控制，或提早提供維護管理；通常在此個別家庭狀況所需智慧化相關服務，可能是由某一服務供應業者率先提供某項服務。例如安全監控或健康照護業者提供專業的智慧化服務，再隨著住戶本身需求的增加，而就原有平台新增不同的服務。如，保全業者新增健康照護服務、健康照護服務業者新增電子商務售貨的便利服務。

由於家庭注重隱私及安全，是否借重外部保全服務的提供，都需要更進一步的安全及隱私保障；因此在此情形下最適合在設備層導入號稱第四代非區塊鏈的 Tangle 技術，讓感測、設備之間形成自我保護，可互相驗證的節點。

至於智慧家庭數據共享方面，需要將智慧家庭相關偵知、感測數據對外傳遞，以獲得反向傳達提供服務的需求者，則可在分二個面向說明：一是需要提供外部個別服務供應商所需數據，仍然需要安全與隱私，並與供應商有著服務約定的關係。因此較適合圖靈完備功能具智慧合約運算能力的區塊鏈類型，如以太坊或 Hyperledger(超級帳本)。尤其 Hyperledger 可建公有鏈、私有鏈或聯盟鏈等彈性，交易(傳遞數據)速度也較快。這方面的需求包含健康照護、安全監控、配合家庭能源管理系統進行能源調度的節能管理服務(如圖 4-1)等。

二是將數據去識別化後，累積成數據檔案提供第三方數據需求者購買(如圖3-16)，例如建康醫療數據可供醫療機構或學術分析研究，或者提供用電數據提供第三方調度者、甚至電力公司發電、輸配電參考應用等等，這些數據檔案經由區塊鏈的加密及雜湊演算，形成具公信力及隱私保護的數據庫；但累積之後數據量越來越大、提供者也越來越多時，區塊鏈本身的交易區塊並不適合。因此，建議可依前述日本智慧家庭數據目錄方式，以標準格式提供數據屬性(metadata)配合區塊鏈不可否認性、防竄改的特性，保證公布於公有雲上的數據資料的可信性，可公開讓所有有意者搜尋目前有哪些數據可資應用；此時，可再配合建置具有智慧合約功能的公有區塊鏈進行競標，自動媒合數據檔案的洽購。媒合成功後由智慧合約自動提供購買者取檔網址，及去識別化數據檔案之解鎖秘密給購買者，區塊鏈智慧合約則自動強制轉帳給數據提供者，激勵數據所者提供數據，讓創新應用得以發展。

圖 4-4 DLT 增強雲結構(本研究釋譯)

資料來源：E. Exposito, H.H., Layth Sliman, Motaz Hassine, Abed Samhat, Ernesto Expósito, Mourad Kmimech, Tangle The Blockchain: Toward IOTA and Blockchain integration for IoT Environment, in International Conference on Hybrid Intelligent Systems. 2019/12: Sehore, India.

此一架構有關數據儲存的部分，合併網路基礎建設、雲端儲存、數據存取簡化 4-3 圖，正符合文獻[36]所建議以分散式帳本技術(DLTs)增強雲結構如圖 4-4 的意旨。整體架構亦符合文獻[29]所建議的模型如圖 4-5。其中 Notary 為預設公證節點以提供區塊鏈的分散式網路架構設備之間的共識機制，而無需與

中心進行驗證。而此公證節點同時行一種區塊鏈網路形成一種虛擬閘道器，使一個或多個節點被攻陷，整個網路系統的數據仍然是可靠和安全。

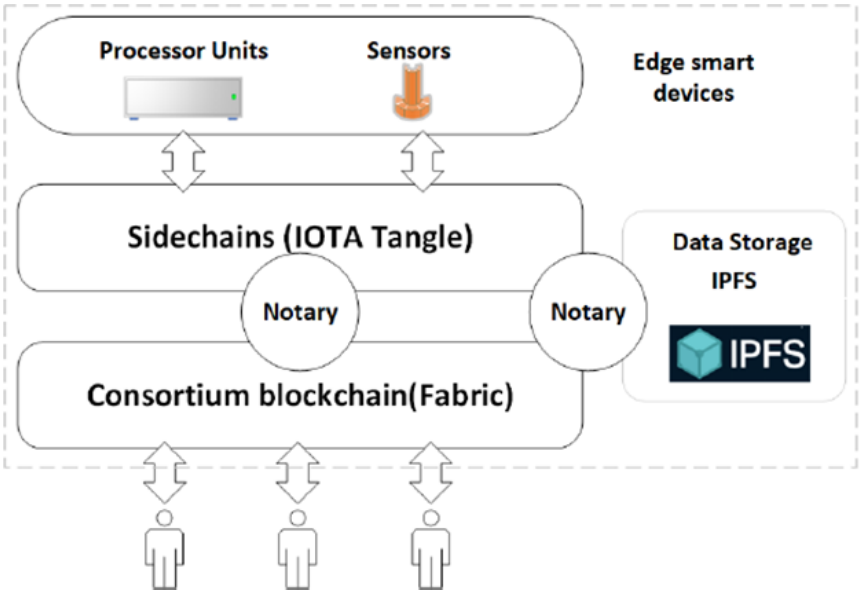


圖 4-5 多層區塊鏈模型

資料來源：Jiang, Y., et al., A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management. Sensors, 2019. 19(9)

三、智慧家庭、社區傳輸層

區塊鏈上的儲存成本很高，同時物聯網數據量不斷增加，因此智慧家庭相關產出的實際數據的傳輸儲存檔案是一個巨大的挑戰。本研究建議架構參考了文獻[29, 36]，有關傳輸層因應激勵數據共享應用的需求，建議使用近年來因應去中心化分散式儲存的趨勢而興起，並配合區塊鏈進行協同運作的雲端存放處 IPFS 星際檔案系統來解決這個問題；當數據檔案上傳 IPFS 星際檔案系統，檔案將被分塊分散儲存內容可尋址，所有內容都是被多重雜湊校驗和作為整個網絡上唯一識別，類似區塊鏈形成不可竄改的功能；IPFS 星際檔案系統不是區塊鏈，前述數據分享達成共識後，有意者循址至此取得，解鎖合併檔案進行分析應用。其數據流程如圖 4-6 所示。

在此必須使用加密公鑰和私鑰機制。在 IPFS 上上傳和存取檔案時，我們可以藉由使用收件人的公鑰對數據進行加密來授予特定使用者存取權限。於 Hyperledger 區塊鏈編寫智慧合約程式和 PKI(公開金鑰基礎建設)來進行安全存取控制。另外，依據文獻[29]的說明在設備端還必須提供以區塊鏈技術建構物聯網設備產品數據庫。數據庫記錄了物聯網設備的完整歷史資訊，用來驗證

來源、真實性和所有權。以便在 Tangle 上標記實體機器的 mac 身份進行存取管理，將數據的完全控制權交給設備所有者。

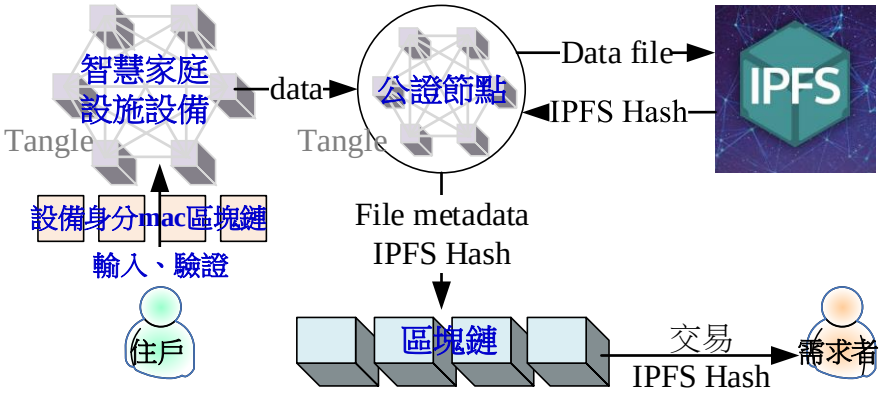


圖 4-6 數據存取流程圖

資料來源：本研究繪製

第三節 智慧建築、社區導入區塊鏈的挑戰

在圖 4-2 的構想情境中，智慧化設備的導入，網際網路、物聯網的建構，都已逐漸成熟，要達成安全監控、健康照護、便利舒適似已不成問題。而區塊鏈的技術也越來越成熟，在台灣各行各業也興起導入區塊鏈的熱潮，尤其已金融、智慧財產、醫療照護產業等尤其熱衷，似乎是只待專業並跨領域區塊鏈人才更為充足的時機而已；而營建產業、智慧建築及智慧家庭的區塊鏈應用導入，其實就是長久以來營建產業導入先進科技的情形、趨勢一樣；雖是號稱火車頭產業，但在轉型方面卻總是在其他產業之後。

依目前數位轉型的趨勢來看，個人認為這已不只是傳統產業內彼此的競爭力而已。而是整體社會、環境、經濟、科技等大環境浪潮所造成。有可能傳統室內、建築設計甚至城市規劃，因為虛擬實境的成熟，變成有跨領域專長，例如，可以虛擬實境進行協同設計業者的專業；仰賴人力的營造業的工作，變成跨機電領域，如操控機器人業者的專業。

回到智慧家庭與社區中導入區塊鏈的課題而言，其中最重要的關鍵在於家庭與社區是否需要智慧化? 因為，沒有智慧化的設備、沒有數據傳遞交易的需求，區塊鏈應該也無用武之地；再就已往家庭優先導入智慧化安全監控，並成為其他需求的整合平台而言，也有所變化；目前，因應全球暖化節能減碳，已

成建築必要優先考慮的項目，因此家庭、建築、社區電力調度供應的節能管理系統越來越重要。

一、微電網與節能管理系統

以往我們說智慧家庭、建築最重要基礎設備之一為智慧電表，有了智慧電表可讓我們了解自己的用電模式，從而調整自己的用電行為。但這已不夠，更重要的是要有智慧電網、微電網的建設，其中又涉及電力自由化的問題。為了保證智慧家庭中電力的合理調度和利用，去中心化電力供應(電力自由化，且有第三方的電力調度服務供應商)的智慧家庭需要向電力調度控制中心發送電力資訊，電力調度控制中心會向智慧家庭發送控制指令。在這智慧家庭與電力調度控制中心的雙向互動，有可能產生一系列的技術與安全問題，例如智慧家庭的智慧電表採集精準的即時用電數據上傳至調度控制中心，有可能因此洩露使用者的隱私，或者對電力調度控制信任產生懷疑。因此，區塊鏈的去中心化信任，透明、不可竄改、智慧合約等特性及功能正可以用來解決，並促進智慧微電網的應用。

例如日本電信業者 NTT 早於 2018 年開始與關西電力、東京大學、日本 Unisys Japan 和三菱 UFJ 銀行聯合開發建立一種區塊鏈機制並開始實證研究，實現讓擁有自己的太陽能發電設備的消費者(電力產消者)，將產生的剩餘電力直接與消費者交易如圖 4-7。根據消費者和發電消費者的期望價格，通過多種方式確定交易價格，並在區塊鏈上進行交易；所開發區塊鏈技術則持續推廣與日本各地電力公司合作[37]。

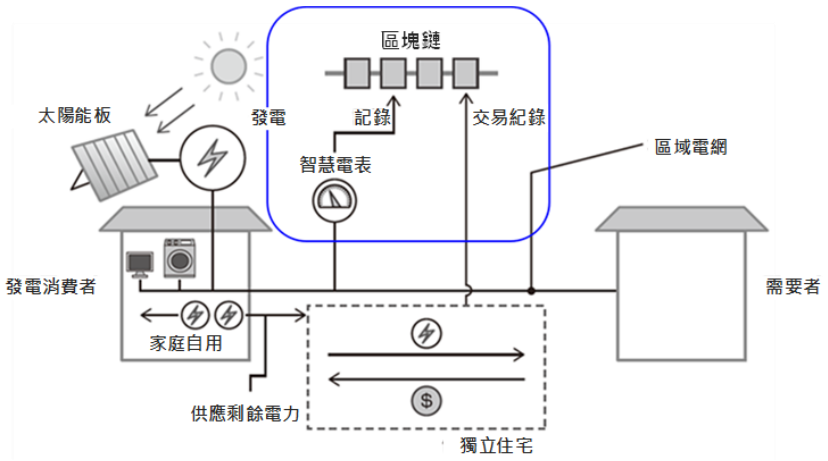


圖 4-7 區塊鏈 P2P 電力交易概要示例[37]

資料來源：ブロックチェーン技術の電力事業への活用とP2P電力取引, in NTT DATA 2019/01/28.

2021年2月，日本Keychain與關西電力株式會社合資合作，進行電力P2P交易實驗示範計畫。示範證實了透過利用Keychain的區塊鏈技術，可以應對現有技術無法解決的網路攻擊，進而提高了可靠性。此外，關西電力也利用區塊鏈技術深化推動電力P2P交易和環境價值交易等安全新服務的商業化[38]。

因此，我國應不僅止於開放民間電廠的投入而已，還必須開放鼓勵智慧家庭、建築、社區的電力自由化，成為電力產銷者，由此區塊鏈才有促進P2P電力產銷調度，達成淨零耗能的目標。本研究在4-2圖構想中的智慧家庭、社區的電力能源調度控制，涉及即時的用電數據收集上載分析，反向控制家庭用電需量，或卸載輪停等措施；抑或是電動車充分利用離峰電力，甚至充當家庭除能電池於用電尖峰負責提供一部分用電負荷，減輕整體供電系統供電壓力，或於停電時共同提供緊急用電需求;因電力調度涉及權利義務、效益權衡等因素，因此需要具有智慧合約功能的區塊鏈，以運行相關程式自動協同作業最佳化調度電力控制設備等；此外，家庭能源管理系統因此還能成為家庭智慧化的基礎平台，建築、社區、城市也是如此。

二、數據分散處理與儲存的安全性

集中式數據庫資料外洩、駭客入侵與損毀事件全世界都不斷在發生，例如今年2萬5210件高中學習歷程檔案上傳後遺失,這是單一數據庫單點故障的例子。因此，為了在網路中提供去中心化分散式儲存的數據安全性，區塊鏈技術是最好的解決方案。此外，人工智慧與雲端運算都已朝向分散處理、儲存發展，然而，產業及政府部門建置資訊系統似乎都只強調集中式亦於控管監視的好處；個人認為這是區塊鏈在台灣發展的另一個挑戰。

三、混和區塊鏈的類型需更多分析實驗

因第一代區塊鏈(如比特幣)因不具智慧合約功能，且係公有鏈性質需挖礦建立共識，耗時且須付出加密代幣費用，並不適合導入；而私有制區塊鏈較適合企業或組織內部應用，組織間信任程度較低。第二代區塊鏈以太坊雖是第一個可運行智慧合約的區塊鏈，並有文獻以此建立電力調度機制研究，但仍須運

作共識機制，同樣也較耗時及付共識費用；本文所提智慧家庭、智慧社區(集合住宅)情境中，各個服務供應商都是互相已知身分的組織，不適合建構比特幣類型的公有制區塊鏈；個人認為最適合的是可在銀行之間的支付結算、多個企業之間的物流供應鏈管理、政府部門之間的數據共享的聯盟鏈；此外，聯盟鏈系統一般都可建立嚴格的身分認證和許可權管理，節點的數量在一定時間段內也是確定的，適合處理組織間需要達成共識的業務。

情境中各種外部服務供應商，包括集合住宅物業管理、家庭內部設備、家電維護保養、健康醫療照護，電力調度控制，及各種電商之間都可形成組織間互相合作。因此，在此層級導入的區塊鏈技術類型應屬聯盟鏈技術。其中典型代表就是前述由Linux基金會管理維護的開源區塊鏈平台Hyperledger(超級帳本)。但本研究所建議的架構智慧家庭底層設備間須結合有向無環圖DAG的tangle技術才能應付不斷增長的物聯網設備及數據交易需求，雖符合近幾年文獻所探討的建議；然而在此之前，尚需有足夠的實驗，以量測家庭、建築、社區、城市等不同規模尺度所適合的技術、架構、模型。

四、區塊鏈與其他AIOT技術的結合

本報告前面說明均以智慧家庭、社區物聯網為基礎進行說明，但目的是為智慧化居住空間產出數據的共享與激勵回饋；而數據收集本身的並無意義，而是收集之後的處理、分析與應用，即大數據分析與人工智慧的應用。

1.區塊鏈與大數據分析

大數據面對的是海量數據，重點在於數據的廣度和數量，以粗糙的方式統計分析，注重相關關係而非因果關係；而區塊鏈技術處理的數據量小，處理方式則更細緻。隨著大數據被重視與快速發展，發現現有的大數據產業面臨著優質可用數據少、資訊壁壘嚴重、數據處理有困境、實踐應用障礙多、雲管理失誤多五大困境，而必須依靠區塊鏈技術才能夠突破大數據行業的瓶頸[39]。

因為大數據產業發展的三大基礎：雲端運算、物聯網、行動互聯網的特徵與趨勢剛好都是分散式機制；由此，導入區塊鏈正好不謀而合，並且區塊鏈技術的分散式帳本和加密技術，使用者的數據可以形成一條透明、可監管、可溯源、防篡改且私密可供大數據信任使用的數據來源。我國除了大數據產業並未

成形外(數據共享平台或應用平台尚未成熟)，也未認識到大數據產業中，以去中心化的理念為基礎，利用區塊鏈技術構建新的底層系統，能夠開發出保障數據安全的應用體系，加快數據共享和流通開發的價值。

二、區塊鏈與人工智慧

智慧家庭乃至智慧城市的社會實現需要大規模的協作，而大規模的協作又需要強有力的多方信任機制作為保障，信任機制源自安全機制，而安全機制基於數據與資訊[40]。因此，區塊鏈技術可以提供數據與資訊層存取共享服務，在此基礎上可提供群體智慧實現所必需的安全機制、信任機制，乃至關鍵的協作平台以及大規模互操作、管理和激勵機制;區塊鏈在不同領域的智慧化應用，將促進全新的經濟模式和產業發展模式。

從區塊鏈的發展歷程觀察，這已不是單一的創新，而是多元、系統性的創新；區塊鏈雖然以技術的形像出現，但已不僅僅是技術創新，更是社會創新、商業創新。可以預測，人工智慧的下一個熱點就是群體智慧以及建構在群體智慧基礎上的智慧社會，而區塊鏈正可以扮演邁向智慧社會的關鍵角色。

三、區塊鏈與元宇宙(Metaverse)

元宇宙(Metaverse)一詞自從傳出臉書 Facebook 要改名元宇宙著重相關建設[41]，及各大資訊龍頭公司紛紛表態投入之後，已成為眾所矚目的發展潮流，又可譯為元宇宙、後設宇宙、形上宇宙、元界、超感空間、虛空間；Metaverse 來自 1992 年 Neal Stephenson 的科幻小說 Snow Crash(潰雪)一書；其實元宇宙指涉的是一個虛擬的城市環境，使用者可以通過高品質的個人虛擬現實眼鏡，或通過低品質的公共虛擬現實眼鏡進入，並與彼此或軟體客戶端進行互動[42]。

元宇宙是一個集體的虛擬共享空間，包括所有虛擬世界和網路的總和，但並不等同於增強現實技術。常用於描述網路的未來版本，是指由永續共享的眾多虛擬空間相連而成的虛擬宇宙。其中一項關鍵的技術就是區塊鏈，因為元宇宙的其他特質包括數位持久化和同步，這意味著元宇宙中的所有事件都是實時發生的，並具有永久的影響。元宇宙生態系統包含了以使用者為中心的要素，

例如身分、內容創作、虛擬經濟、社會可接受性、安全和隱私以及信任和責任。等必須解決的問題，正是區塊鏈可以為元宇宙賦能效力的地方；由此可見區塊鏈已是新興科技必要併行、多方創新應用的技術之一。

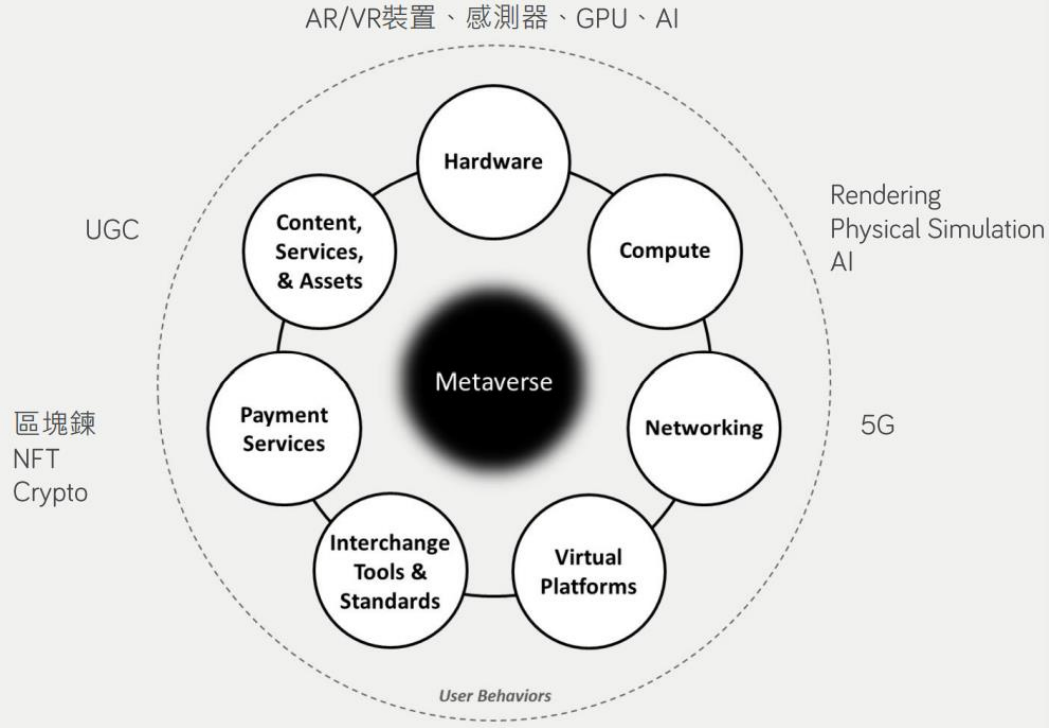


圖 4-8 元宇宙的核心賦能技術

資料來源：簡韶逸,台灣在 Metaverse 時代的機會和挑戰,2021

第五章 結論與建議

未來全球將有 70%人口居住城市的趨勢，城市面臨基礎設施能力的挑戰；為了滿足民眾對安全、健康、節能、便利的需求，智慧家庭與智慧社區是未來社會發展的主軸，以因應社會、經濟及環境的變化。我們必須正視智慧家庭、建築與社區技術可以永續發展做出重要貢獻；家庭自動化的概念必須考慮到新技術和新的智慧化使用者，住宅將不再被視為一個單一的實體，而是智慧城市概念的基本組成部分；將智慧電網、服務、建築、住宅和家電設備整合在一起，這些子系統必須能夠感知、偵測、聯動並和遠端協同控制作業，以實現更好的生活品質、永續節能、社會經濟發展。而智慧化的普及與社會各界對資通訊科技、物聯網和區塊鏈的理解和整合應用的處理能力。

第一節 結　論

由於智慧家庭越來越多的 IoT 設備，連接網路的數據傳輸和命令執行目的，原為促進安全性，舒適性和可接取性。但智慧家庭系統的相互連接性和複雜性，導致網路攻擊、網路擁塞和資訊洩漏的脆弱性更高。利用區塊鏈技術固有安全特性、身份驗證和權限控制、透過使用加密機制設定設備，區塊鏈技術可實現無縫驗證，以確保數據傳輸的私密性和安全性。而區塊鏈的智慧合約功能可實現時間設定、多層級控制、這些都有助於建構適合複雜現實生活情境智慧家庭系統。

未來電力基礎設施及自由化，智慧家庭、建築、社區都成為電力產銷者後，就有賴於電力合理調度和利用以達成淨零耗能的目標。去中心化智慧家庭需要向電力控制中心發送電力資訊，電力控制中心需要向智慧家庭發送控制指令。然而，智慧家庭與電力控制中心的雙向互動可能會導致一系列安全問題，例如智慧家庭的智慧電表採集精緻的即時用電數據並上傳到控制中心，這有可能因此洩露使用者的隱私。除了區塊鏈特性可解決隱私問題外，區塊鏈的設備是可點對點驗證，以確定網路中設備是安全的還是有被駭客惡意篡改了。因此其他設備可拒絕被駭控制設備的連接。

高齡者在宅健康照護需求不斷提高，智慧家庭及使用者穿戴式設備監測受照護者的數據傳送醫療照護機構進行分析判斷，並且累積的數據資料有分析研究價值；因此，區塊鏈固有安全特性，並憑藉內置的加密技術能夠保證所有數位事件的記錄不可篡改也不可能被破解，整個醫療照護數據變得更具應用價值，使用者對醫療數據的掌控度提高並得到激勵，因此更願意進行數據分享；此外，醫療院所之間利用區塊鏈技術，醫療數據可以實現加密共享的目標，能夠實現分散式互動；如果現有的 HIT 智慧醫療系統基礎上融入區塊鏈技術，就能夠替換現有醫療數據交互的第三方業者,大大提高數據流通的可靠性和效率。

第二節 建　議

本報告探討了智慧家庭相關物聯網與區塊鏈文獻，均正面看待導入區塊鏈技術能解決現代智慧家庭安全隱私、節能管理、健康照護等相關問題；本報告建議以適合物聯網底層設備應用的 tangle 技術,將智慧家庭內部設備形成一自我防衛並可即時傳遞監測與控制數據的區塊鏈；與外部服務供應者的應用，則結合傳統區塊鏈的分散式、可信任、不可篡改、智慧合約等各種特點，尤其 Hyperledger 超級帳本平台技術，建立聯盟區塊鏈獲得整合服務效果；建議導入分散式儲存的星際檔案系統，以建立使用者充分掌握數據所有權，激勵分享獲取回饋機制。此外，為了推廣讓其他需求者了解有那些可信任數據，從何處取得等，建議建立去識別化的元數據庫及公有制區塊鏈媒合機制，以加速智慧家庭數據的分享應用。

因應氣候變遷，全球對建築、城市節能減碳已有共識；淨零耗建築已成先進國家對能源使用的目標；其中歐盟更為建設宜居和功能齊全的城市，提出 +CityxChange 正能源燈塔城市計畫。由 NTNU 與 32 個合作夥伴,包括 7 個城市、大型工業、中小企業、非政府組織和學術界協調合作。其中挪威 Trondheim Kommune(TK)和愛爾蘭 Limerick City & County Council(LCCC)作為燈塔城市與 Alba Iulia（羅馬尼亞）、Písek(捷克)、Sestao(西班牙)、Smolyan(保加利亞)與 Võru(愛沙尼亞)等 5 個追隨城市發展可行和實現正能源的示範計畫

[43]；其中歐盟認定 tangle 技術的 IOTA 適合用於建築群間進行電力調度，因此選擇與推動 IOTA 的 IF 基金會合作，結合其他先進規劃技術以改進科技、公民、能源的互動規劃方式，實現開放式創新模式下的智慧城市。

以此看來，歐盟已認定先進區塊鏈技術是這些示範城市、數位、正能源促進氣候和永續城市環境轉變，提高生活質量不可或缺的技術。因此，建議進一步觀察探討 IOTA tangle 技術結合其他建築科技，借鏡歐盟+CityxChange 計畫中應用的策略與方法，進一步提升我國淨零耗能建築參考。

因此總結建議：

建議一：尋找場域以初步進行智慧家庭物聯網環境結合區塊鏈數據分享應用實驗，驗證並示範其可行性，以促進智慧家庭數據分享並創新產業應用。

建議二：探討歐盟智慧城市燈塔計畫之正能源建築及區塊鏈應用策略，觀察探討歐盟+CityxChange 計畫 IOTA tangle 技術結合其他建築科技，以借鏡中其應用的策略與方法，進一步提升我國淨零耗能建築技術。

附錄 一

110 年度自行研究「區塊鏈技術在智慧家庭數據應用現況與問題探討」期初審查會議紀錄

一、時間：110 年 3 月 26 日(星期一)下午 2 時 30 分

二、地點：本所簡報室

三、主席：王所長榮進　　記錄：林谷陶

四、出席人員：詳簽到簿

五、主席致詞：（略）

六、研究案主持人簡報：（略）

七、發言要點(依簡報順序)：

1. 本案研究題目原則可行，但請特別針對國內家電業者導入區塊鏈應用情形、目的與效益進行了解。
2. 建議構思區塊鏈技術如何於社會住宅場域或本所 Living 3.0 智慧化展示空間進行應用示範。

八、會議結論：

請參考與會同仁之寶貴意見，並請納入研究內容參採修正，使研究成果更為豐富完整。

九、散會：（下午 5 時整）

附錄 二

110 年度自行研究「區塊鏈技術在智慧家庭數據應用現況與問題探討」期中審查會議紀錄

一、時間：110 年 8 月 12 日(星期四)上午 9 時 30 分

二、地點：本所簡報室

三、主席：羅組長時麒　　記錄：林谷陶

四、出席人員：詳簽到簿

五、主席致詞：(略)

六、研究案主持人簡報：(略)

七、發言要點(依簡報順序)：

台灣電力股份有限公司(王主任金墩、王主辦建策、李組長信璋、陳組長群達、陳組長以彥)：

陳組長群達

本案簡報提出之智慧社區、智慧家庭有關區域電網、微電網運用區塊鏈保障數據安全、隱私及分享機制，建請於期末報告中詳予論述說明。

陳組長以彥

1.建請收集國內外智慧家庭導入區塊鏈進行用電調度案例，以供參考。

2.區塊鏈之興起部分原因係因應資安問題，唯實際應用有節點愈多效能愈慢之缺點，請參考探討。

社團法人台灣智慧建築協會(溫名譽理事長琇玲、黃副理事長健瑋)：

溫名譽理事長琇玲

1.有關智慧家庭、智慧建築數據問題現有資訊技術已可解決，導入區塊鏈應用之目的建議應先說明，俾釐清研究目的；此外，區塊鏈技術並非無法可破，亦宜說明澄清。

2.本案研究為架構型研究，至期中報告階段大多為文獻搜集分析，簡報提出之架構應予詳細論述說明。

3.有關國內智慧家電廠商關心智慧家庭使用者數據安全隱私，及國外連線標準聯盟(Connectivity Standards Alliance, CSA)倡議之 Matter 智慧家庭標準於 2021 年底發布後，未來亞馬遜、蘋果與 Google 等國際資訊大公司之智慧家庭橋接器如 Nest Hub 和 Nest Audio 等裝置

可透過軟體更新支援 Matter 標準，將使 Google Assistant 可以遙控相容的智慧家庭設備，甚至還能使用 Siri 和 Alexa 進行遙控並收集介接智慧家電使用數據，進一步應用並擴大智慧家庭設備數據標準優勢。因此，建議應鼓勵國內家電業者積極採用國內 TaiSEIA 101 智慧家庭物聯網通訊協定標準，以保護國內家電業者商機及使用者數據安全。

黃副理事長健瑋

國內住宅建築業者對智慧建築產出數據部分，仍以智慧建築標章評估之資訊安全內容較為關注，建議本案可以此關聯說明著墨。

資訊工業策進會(周研究員晨蕙)：

1.本案初步建議電網電力交易導入區塊鏈應用架構，建議可參考日本みんな電力、日本ユニシス、関西電力等電力交易平台案例。

2.持續探討所提智慧家庭初擬架構產出相關數據之收集、應用與分享機制，並詳細說明。

中華民國全國建築師公會(何建築師欽欽 書面意見)：

1.區塊鏈技術仍有可能有安全性問題，例如智慧合約可能有程式漏洞，建議增加風險課題探討。

2.後續如有實際導入可能，建議評估是否需要建立監督機制。

本所－

工程技術組

劉副研究員青峰：

1.建議補充有關區塊鏈傳輸資訊安全性之相關說明。

2.建議補充說明有關物聯網應用新區塊鏈 IOTA 之 tangle(纏結)技術之共識機制。

陳助理研究員士明 書面意見：

1.本案預期成果包括收集智慧家庭數據隱私與數據安全可能的區塊鏈技術、智慧家庭隱私與數據安全、共享的區塊鏈案例，及建議社會住宅智慧家庭數據應用區塊鏈共享數據機制，預期對本所未來區塊鏈技術應用有極高參考價值。。

2. 本案研究目的之一為持續探討區塊鏈技術及與 BIM、物聯網、大數據、人工智慧發展的關聯性，特別是與建築數位轉型、智慧城市等應用趨勢，建議評估於住宅、社區區塊鏈應用情境初擬中加入 BIM 應用。

環境控制組

游助理研究員伯堅：

後續建議事項建請詳細具體說明。

主席：

1.智慧家庭、智慧建築數據取得困難有，以致後續無法分析應用，甚至創新發展，後續請持續針對政府社會住宅租賃型式透過合約與住戶達成數據收集協議，與一般集合住宅如何鼓勵住戶分享數據持續探討。

2. 建議再收集本所歷年辦理「創意狂想 巢向未來」競賽得獎案例中可供參考資料。

執行單位回應(計畫主持人 林副研究員谷陶）：

1.感謝各位委員提供寶貴意見，本案簡報所提智慧社區、智慧家庭運用區塊鏈保障數據安全、隱私及分享機制，相關結論與建議當於期末報告中詳予說明。

2. 本案探討目的主要延續去(109)年自行研究案「區塊鏈技術及營建產業應用案例探討」發現先進國家營建產業已積極佈署導入，且國內亦有案例營運中，並檢討認為我國推動智慧建築過程中數據收集之安全隱私顧慮及缺乏激勵措施。因此，本(110)年度持續探討智慧家庭導入區塊鏈，以文獻收集及國內外案例討方式，了解國際發展趨勢，提供後續研究發展參考，並建議社會住宅可能的區塊鏈導入架構。

3.有關區塊鏈技術安全性問題，主要發生在某種區塊鏈平台建立之初參與者不多(節點少)時，共識機制容易被進行 51%的攻擊，第二確實如委員所提智慧合約撰寫不完全，第三是交易所被駭入取走加密數位貨幣，甚至將來量子電腦成熟，則現有區塊鏈及日常資訊通訊應用的加密演算法、共識演算法都有危險。但各區塊鏈平台也都有因應措施(如智慧合約測試鏈)，並且區塊鏈技術在各國產官學各界積極投入下也都不斷進步中。

3.有關產業是否一定導入區塊鏈技術問題，例如世界經濟論壇、世界大型顧問公司等也有研究進行提出是否適合導入的評估程序報告；其主要建議觀點在於安全隱私、參與者共識及分散式儲存的需求而定。尤

其針對營建產業而言，導入區塊鏈的優勢是可改善營建產業各關係利益者之間的信任關係。

4.感謝委員提供日本有關電力交易運用區塊鏈資訊，後續當再收集參考及補充；至有關區塊鏈結合 BIM 技術確是國際營建產業發展的趨勢，後續收集有關智慧家庭相關案例分析供參

5.本案後續當依主席指示針對社會住宅及一般集合住宅數據收集所需情境進行分析探討，並重新了解歷年創意競賽得獎案例是否也有類似導入情形或意向。

八、會議結論：

請參考與會同仁之寶貴意見，並請納入研究內容參採修正，使研究成果更為豐富完整。

九、散會：(上午 11 時 30 分)

110 年度自行研究「區塊鏈技術在智慧家庭數據應用現況與問題探討」期末審查會議紀錄

一、時間：110 年 11 月 30 日(星期二)上午 9 時 30 分

二、地點：採實體與視訊併行會議(實體會議於本所討論室(一))

三、主席：羅組長時麒　　紀錄：林谷陶、張怡文、呂文弘

四、出席人員：詳簽到簿

五、主席致詞：(略)

六、計畫簡報：(略)

七、綜合討論：

中華民國全國建築師公會(張建築師文瑞)：

1.本案期末報告已針對期中審查意見回應修正，惟請再就文獻、圖號等詳加校對修正。

2.報告除已提出智慧家庭、社區導入區塊鏈應用情境、架構及流程外，又說明區塊鏈技術也是元宇宙、正能源建築等熱門議題中的重要技術，值得重視參考。

財團法人資訊工業策進會(周研究員晨蕙)：

1.本案報告符合預期成果。

2.有關區塊鏈不可竄改特性與歐盟 GDPR 調適問題，其中"刪除權"用語，建議改用"抹除權"一語；此外，似已有最新解決 GDPR"抹除權"區塊鏈技術，建議持續探討提供國內各界了解。

社團法人台灣智慧建築協會(繆經理嘉成)：

1.研究內容紮實，蒐集智慧家庭數據安全可能的區塊鏈技術，並說明與 BIM、物聯網、大數據及人工智慧等之關聯。

2. 本案提供國內家電大廠禾聯碩住宅建築已導入區塊鏈案例,說明智慧家庭數據互相應用時代已來臨，可供國內家電、建築業者參考。

3. 建請就區塊鏈中 P2P 對等節點本身如何可被驗證詳加說明。

本所一

徐副研究員虎嘯：

1.本案報告符合預期成果。

2. 本所開放綠建築、智慧建築標章等資料均有去識別化的疑慮，且有資料格式統一問題；區塊鏈技術在智慧家庭等傳遞交易等相關應用，是否也有必要建立標準資料格式問題，建議規劃持續探討。

陳助理研究員士明：

1.本案對區塊鏈技術在智慧家庭數據應用已有廣泛探討，研究成果極具參考價值。

2.研究目的之一為持續探討區塊鏈技術與 BIM、物聯網...等的關聯性。但似乎較偏向智慧家庭內部物聯網的探討；建議未來持續探討區塊鏈技術之去中心化、匿名性、不可竄改性、共識機制、加密等五大特色，與 BIM 關聯應用機制與技術。

主席(羅組長時麒)：

後續研究建議以實際案例驗證區塊鏈技術在智慧家庭應用可行性。

計畫主持人回應（林副研究員谷陶）：

1.感謝各位委員提供寶貴意見，本案報告頁碼、圖號、文字疏漏部分，當於成果報告再詳加校閱修正。

2.感謝委員有關修正歐盟 GDPR"抹除權"用語之建議，惟歐盟 GDPR 資料保護與區塊鏈技術調適問題，確已有研究提出解決方案，然是否成熟及或歐盟認可尚非本報告重點，後續當予就教並持續關注。

3.有關區塊鏈中參與節點 P2P 數據傳遞之節點驗證問題，以公有區塊鏈(非許可制)而言，是任何人都可參與並不對節點驗證，而傳遞交易係以全網 51%以上節點取得共識方式成立；私有制或聯盟區塊鏈(許可制)等則是已知參與者即節點身分已經識別。

4.區塊鏈技術與營建產業 BIM 應用確實是熱門的研究及應用趨勢，109 年度自行研究已有初步探討，並國內已有初步應用及研究；因此，本年度探討重點在於區塊鏈技術智慧家庭社區的應用，未來可持續關注探討。

八、會議結論：

(一) 本次會議期末報告，經審查結果原則通過。請業務單位將與會出席代表及本所人員意見詳實記錄，以供計畫主持人參採，並於報告中妥予 回應。

(二) 請注意圖示及圖表的智慧財產權，如有引述相關的資料，應註明資料來源。整份報告的結論與建議事項，應考量具體可行，並鼓

勵將研究成果投稿建築相關學報或期刊。

九、散會(上午 11 時 30 分)

參考文獻

1. 林谷陶, 我國與日本推動智慧家庭數據應用環境政策比較研究. 2019, 內政部建築研究所.
2. 林谷陶, 區塊鏈技術及營建產業應用案例探討. 2020, 內政部建築研究所.
3. Notra, S., et al. An experimental study of security and privacy risks with emerging household appliances. in 2014 IEEE Conference on Communications and Network Security. 2014.
4. 陳宗慶, 智慧聯網應用 邁入新紀元, in 工商時報. 2015/09/25.
5. Tatar, U., Y. Gokce, and B. Nussbaum, Law versus technology: Blockchain, GDPR, and tough tradeoffs. Computer Law & Security Review, 2020. **38**: p. 105454.
6. 井底望天、武源文、趙國棟、劉文獻, 區塊鏈與大數據: 打造智慧經濟. 2018/04, 台北: 上奇時代.
7. 楊永強, 蔡., 劉雅卓, 區塊鏈+大數據：突破瓶頸，開啟智能新時代. 2019.5, 北京: 機械工業出版社.
8. Emilio, M.D.P., IOTA 技術將如何改變物聯網設計？, in 電子工程. 2020/01/16.
9. 曹源, 張., 丁兆云, 姜新文, DAG 區塊鏈技術: 原理與實踐. 2018: 機械工业出版社.
10. 智慧化居住空間產業聯盟(秘書處), 智慧化居住空間產業聯盟"建築 AIoT 特別議題工作小組(SIG)"第一次會議報告：從產業界觀察建築 AIoT 發展. 2021/07/01, 內政部建築研究所.
11. Forum., W.E., **Building Block(chain)s for a Better Planet: Fourth Industrial Revolution for the Earth Series.**, in Fourth Industrial Revolution for the Earth Series. 2018/09, In collaboration with PwC and Stanford Woods Institute for the Environment.
12. Abramson, A., Baby Monitor Hacking Alarms Houston Parents. 2013/08/13, abcNEWS.
13. Minoli, D., Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. Internet of Things, 2020. **10**: p. 100147.
14. Philips Hue. Available from: https://www.philips-hue.com/en-hk/explore-hue.
15. BELKIN WEMO. Available from: https://www.belkin.com/us/smart-home/c/wemo/.

16. 林祐祺. 智慧家庭最後且最重要的一塊拼圖－智慧家電. 2020/3/2; Available from: https://makerpro.cc/2020/03/smart-home-appliance-for-smart-home/.
17. Han, D., H. Kim, and J. Jang. Blockchain based smart door lock system. in 2017 International Conference on Information and Communication Technology Convergence (ICTC). 2017.
18. Yang, L., X.Y. Liu, and W. Gong. Secure Smart Home Systems: A Blockchain Perspective. in IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2020.
19. Shrestha, A.K., J. Vassileva, and R. Deters, A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives. Frontiers in Blockchain, 2020. **3**(48).
20. Dorri, A., S. Kanhere, and R. Jurdak, Blockchain in Internet of Things: Challenges and Solutions. arxiv, 2016.
21. Dorri, A., et al. Blockchain for IoT security and privacy: The case study of a smart home. in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). 2017.
22. 電子情報技術産業協会（JEITA）, 般., JEITA スマートホームデータカタログ項目定義書V1.0. 2019.
23. Moniruzzaman, M., et al., Blockchain for smart homes: Review of current trends and research challenges. Computers & Electrical Engineering, 2020. **83**: p. 106585.
24. 台灣受恩. 台灣受恩創造智慧福祉生活. Available from: https://www.stipendiary.com.tw/edcontent_d.php?lang=tw&tb=1&id=2505.
25. Daley, S. 17 Blockchain Companies Boosting the Real Estate Industry. May 9, 2021; Available from: https://builtin.com/blockchain/blockchain-real-estate-companies.
26. Qi-Long, C., Y.R.-H. , and L.F.-L. , A Blockchain-based Housing Rental System. Computer Technology, Information Science and Communications, 2019(CTISC 2019): p. 184-190.
27. 社會住宅智慧電表數據-AI 大數據分析進行實證計畫提案書, 臺北市政府都市發展局, Editor. 110/06/20.
28. 笹川雄司, スマートハウスビジネスの現状. 2018.

29. Jiang, Y., et al., A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management. Sensors, 2019. **19**(9): p. 2042.
30. Ali, G., et al., xDBAuth: Blockchain Based Cross Domain Authentication and Authorization Framework for Internet of Things. IEEE Access, 2020. **8**: p. 58800-58816.
31. Guan, Z., et al., Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities. IEEE Communications Magazine, 2018. **56**(7): p. 82-88.
32. Lee, Y., et al., A blockchain-based smart home gateway architecture for preventing data forgery. Human-centric Computing and Information Sciences, 2020. **10**(1): p. 9.
33. Zhang, S., J. Rong, and B. Wang, A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain. International Journal of Electrical Power & Energy Systems, 2020. **121**: p. 106140.
34. Lazaroiu, G.C. and M. Roscia. Blockchain and smart metering towards sustainable prosumers. in 2018 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM). 2018.
35. Moreno, M.Z., M.A.; Skarmeta, A.F., **User-centric smart buildings for energy sustainable smart cities.** Trans. Emerg. Telecommun. Technol., 2014. **25**: p. 41-55.
36. E. Exposito, H.H., Layth Sliman, Motaz Hassine, Abed Samhat, Ernesto Expósito, Mourad Kmimech, Tangle The Blockchain: Toward IOTA and Blockchain integration for IoT Environment, in International Conference on Hybrid Intelligent Systems. 2019/12: Sehore, India.
37. ブロックチェーン技術の電力事業への活用とP2P電力取引(**利用區塊鏈技術進行電力業務和P2P電力交易**), in NTT DATA 2019/01/28.
38. TIMES, 株.P. ブロックチェーン技術を活用したデータ信頼性向上実証実験を実施(利用區塊鏈技術進行數據可靠性提升示範實驗). 2021/03/22; Available from: https://prtimes.jp/main/html/rd/p/000000027.000021131.html.
39. 楊永強, 蔡., 劉雅卓, 區塊鏈+大數據：4.2　區塊鏈如何助力大數據實踐應用. 2019.5, 北京: 機械工業出版社.

40. 曲強, 林., 區塊鏈+人工智能 下一個改變世界的經濟新模式. 2019/04, 北京: 人民郵電出版社.
41. DJ, M., 元宇宙超夯！傳 Facebook 將改名、騰訊成立 F1 遊戲工作室, in 科技新報. 2021/10/21
42. 簡韶逸, 台灣在 Metaverse 時代的機會和挑戰. 2021.
43. Periodic Reporting for period 2 - CityxChange (Positive City ExChange). 2019-11-01 to 2021-04-30.