國立政治大學資訊科學系
Department of Computer Science
National Chengchi University

碩士論文

Master's Thesis

# 應用區塊鏈技術支援整合照護資料分享之認證與授權

# Authentication and Authorization for Sharing Integrated Care Records using Blockchain

研 究 生：黃振庭

指導教授：陳恭

中華民國一〇八年八月

August 2019

DOI:10.6814/NCCU201901178

# 應用區塊鏈技術支援整合照護資料分享之認證與授權

# Authentication and Authorization for Sharing Integrated Care Records using Blockchain

研 究 生：黃振庭　　Student: HUANG, CHENG-TING

指導教授：陳恭　　Advisor: Kung Chen

國立政治大學

資訊科學系

碩士論文

A Thesis

Submitted to Department of Computer Science

National Chengchi University

in partial fulfillment of the Requirements

for the degree of

Master

in

Computer Science

中華民國一〇八年八月

August 2019

DOI:10.6814/NCCU201901178

# 應用區塊鏈技術支援整合照護資料分享之認證與授權

## 摘要

醫療與照護資訊之整合有助於提升醫療品質與效率、增進人民福祉，但現下環境缺乏一套完善的整合系統供民眾進行資訊的授權與共享，由於共享醫療資訊牽涉到民眾隱私權等敏感的問題，因此整合系統必須具保密的特性來保護民眾的安全。本研究利用區塊鏈防竄改與共享帳本的特性實現具備細粒度的授權系統，細粒度意即民眾可以控制病歷資料的授權範圍與對象，提升對資料的自主權；為了節省區塊鏈的儲存成本，本研究的設計係基於病歷資料分散式儲存，但集中式的會員認證管理與資料索引，並搭配區塊鏈技術管理民眾授權之架構。民眾透過手機隨時隨地進行授權，並經由區塊鏈交易將授權紀錄寫入智能合約，即時分享給參與機構，照護人員也可透過系統查詢民眾分享的資料與授權紀錄，利用現行的安全網路進行資料調閱，即時取得所需之共享資料，以提升照護品質。

關鍵詞：區塊鏈、智能合約、數位憑證、醫療資訊授權、細粒度

DOI:10.6814/NCCU201901178

# Authentication and Authorization for Sharing Integrated Care Records using Blockchain

## Abstract

The integration of medical information and long-term care can help improve medical quality, effectiveness and enhance people's well-being. However, the current environment lacks a comprehensive and integrated system for people to authorize and share medical information. Because sharing medical information will involve people's privacy rights and other sensitive issues, the integrated system must have confidentiality features to make sure the safety of the people. This research uses the anti-tampering and shared ledger characteristics of blockchain to achieve a fine-grained authorization system. Fine-grained means that the public can control the scope of their medical records to enhance the autonomy of the data. Our system employs a decentralized data storage environment and provides a centralized data index to balance the cost and efficiency of data sharing. People can use mobile phone App developed by us to authorize anytime and anywhere. Through the blockchain transaction, the authorization record is written into the smart contract and instantly shared with the participating organizations. The caregiver can then query the information shared by the public through the system, and use the current secure network for data access, and instantly obtain the required shared materials to improve the quality of care.

Keywords: Blockchain, smart contracts, medical information sharing, fine-grained access control

**DOI:10.6814/NCCU201901178**

# 目錄



DOI:10.6814/NCCU201901178

DOI:10.6814/NCCU201901178

# 圖目錄



DOI:10.6814/NCCU201901178

# 第一章　緒論

## 1.1 研究背景與動機

隨著醫學的進步與發達、公共衛生設施及營養狀態的提升等因素，台灣乃至世界各國之平均壽命逐漸延長，台灣在民國 107 年高齡人口比例超過 14%，正式邁入高齡化社會，根據國家發展委員會推估，臺灣高齡人口比例將於民國 115 年超過 20%，邁入超高齡化社會。隨著未來高齡人口的快速增長，伴隨年齡增長的體能衰弱、失能之人口在未來將大幅攀升，同時由於少子化的影響下，小家庭所能提供的居家醫療與照護服務之負擔將日益加重，同時在人口快速老化的情形下，照護資源或照護人員不足的問題會逐漸顯著，造成家庭與社會均面臨此沉重的負荷。

在高齡化之環境因素下，具有整合各院所醫療與照護資訊之系統為社會所能提供之效益將日益增長，再者於現今醫療與照護體系中，不同機構、醫療服務提供之服務與個案問題日益多元，常會出現一件個案有多位工作人員提供服務的現況，導致每件個案都需要重述多次自身問題，造成資訊間的重複提供，同時服務提供者有可能因為訊息分散，無法掌握全面的資訊，以至於評估不完整，變相形成資源上的浪費。若能針對個案或家庭進行服務時，藉由醫療與照護整合系統將通報、療育、就學、醫療等資訊串接，讓每一階段之服務提供者可由整合系統之醫療資訊全面性的瞭解個案，透過資訊間的整合與互補得知個案過去曾經發生的問題以及接受過的服務，可避免重複性敘述，有效減少可能的重複性服務，也可讓醫療單位更具全面性的評估提供最適合個案的資源來協助並提供更具全人式的照顧，同時整合系統可增進跨資源單位照護整合的能力，以滿足民眾的多元需求。本研究以社區為基礎、以家庭為核心做整合，探討橫跨民政、社政、衛政之三方需求，針對不同角色之使用者與單位，以及彼此資料交換之模式分析，整合各種醫療、保健、照護、社工及福祉資訊，提出對未來推動照護之基礎架構，以發展全人健康與落實偏遠地區長照責任為目標。

## 1.2 智慧照護服務模式示範場域建構

為實作與評估出整合系統之可行性，本研究之示範平台以山地離島偏遠地區為執行區域，並選定連江縣為示範平台主要地區，運行狀況良好即可逐步擴散示範地區至其他偏鄉離島地區及本島並協同運作。平台運作範圍含括了連江縣立醫院、連江縣 4 家衛生所(北竿、東莒、西莒及東引)以及與臺灣本島支援連江縣 IDS[1]及醫學中心計畫之臺北市立聯合醫院、三軍總醫院、亞東紀念醫院及臺北市立萬芳醫院；示範場域建構之子系統包含已建置完成之電子病歷交



DOI:10.6814/NCCU201901178

換中心(簡稱 EEC 平台)[2]，最後本示範平台將針對社政、衛政、民政各職權角色之需求進行資料模式等定義，從中發展出跨體系與跨醫療院級的方式，其發展重點將提供一跨整合服務單位之平台，我們將其稱之為「整合平台」。整合平台將導入區塊鏈(Blockchain)技術以結合各領域專業單位執行整合性醫療與照護服務、醫療遠距照護、長照服務，協助完善連江縣之全人照護需求，並依成果可複製至其他區域進行推廣及移轉擴散。本研究之資料範疇定義與跨體系之資料交換標準模式可做為未來健康照護福祉相關開發案之基礎，完善總體健康照護福祉之資訊基礎。

## 1.3 區塊鏈技術

各體系之醫療與照護資訊間的整合與共享有其存在之必要性，但由於開放資訊共享將牽涉到民眾們較為注重的合法性授權問題，其中更涉及到個資法、電子簽章、資料交易及資料交換標準，民眾不免產生過去的看診紀錄與詳細病歷可能有外洩或公開出去的疑慮。過去傳統關聯式資料庫因為只會在伺服器上儲存一份資料的複本，在此情況下只要擁有更改資料庫內資料的權限(意即系統管理員權限)即可任意對儲存於資料庫內之內容進行更動，因此將較為敏感的授權資訊儲存於傳統關聯式資料庫中則有被醫療單位機構內部或取得存取資料庫權限之駭客竄改的風險，而萬一授權資訊遭到竄改則民眾之詳細病歷就可進一步的被非法調閱，因此使用傳統之關聯式資料庫對較敏感的授權資訊做儲存將存在被非法竄改與調閱的風險。區塊鏈分散式帳本的特性可保證存於鏈上之資料不會遭到非法竄改，利用區塊鏈則可以很好的解決上述傳統關聯式資料庫的問題。

前述提及之 EEC 平台雖然可以實現電子病歷交換，但 EEC 平台並不包含民眾自主授權以及調閱病歷時權限查詢自動化的服務，因此本研究基於 EEC 平台導入區塊鏈技術將民眾自主授權之授權表單儲存於區塊鏈上，一來可藉由區塊鏈上之智能合約的自動化特色實現自主授權與調閱權限查詢，二來可藉由區塊鏈不可竄改的特性以確保民眾授權之完整性，消除資訊安全性之疑慮。

本平台同時也利用區塊鏈共享式帳本的特性同步民眾在各醫院的授權表單實現調閱需求分流的目的；舉例來說，今天民眾想利用 APP 授權自己過去在聯合醫院的看診紀錄給亞東醫院，則此授權會經由聯合醫院的節點將資料上鏈，並同步到其他聯盟鏈內之所有節點，如此一來日後當各院醫護人員要在任一節點醫院查詢權限時即可在自己醫療院所的節點上進行查詢訪問，在查詢權限上即可達到分流的效果，提升查詢速度並降低區塊鏈的計算負擔，並免除掉中央式架構中單點被攻擊的風險。

區塊鏈技術具有匿名性、不可篡改、去中心化等特性，近年來許多研究機構進行區塊鏈相關的研究及探討區塊鏈可行的應用，在過程中研究者們漸漸發現區塊鏈也並非適用於現今的所有系統上，舉例來說，如果要做資料儲存相關應用的話，區塊鏈就並非是一個合適的平台，因為在區塊鏈上進行資料儲存必須支付一



DOI:10.6814/NCCU201901178

定的 Gas 費用，造成區塊鏈不像傳統的關聯式資料庫適合儲存大量的資料，因此在資料欄位的設計上該如何透過屬性將資料做分群處理後再儲存到區塊鏈內是一個值得思考的問題。因此在使用區塊鏈的時候必須根據實際遭遇的狀況，找到適當的關鍵點引入區塊鏈技術，藉此完全充分發揮出區塊鏈的特性。

## 1.4 細粒度授權

本平台之授權項目具有細粒度的特色，意在提升自主授權上的彈性，細粒度(Fine-grained)亦即資料本身具有可選取範圍的特性，使用者可以根據醫療照護人員的需求來授權所需要的部分病歷資料，實現針對不同層級的醫療照護人員授予不同的存取權限，使用者所擁有的授權表單內包含多個主項，每個主項中可細分出多個較為細節的授權細項，細粒度授權讓民眾進行授權時可以選擇要批次性的一次給予多個照護資料，或是可以選擇選取特定的授權照護資料進行授權，目的為增加資料授權時的彈性以及資料自主性，不但讓民眾可以方便的一次性給予照護人員多項照護資料，同時也兼具讓對自己的照護資料有控管意識的民眾可以選擇只給予部分照護資料的細項。

本照護平台之醫療與照護資料採用分層式資料結構以達到細粒度授權的目的。如圖一所示，民眾可以一次性的授權過去之所有病歷，或是選擇指授權大類別「健康促進」內之病歷資料，或是選擇只授權某一筆特定的病歷資料給醫療照護人員，透過此彈性化之分層式結構可達到具細粒度之自主性授權，同時將表單進行規格化存入區塊鏈內之智能合約中，以供日後服務提供者或醫療單位調閱時進行授權對象之比對與驗證，達到在整合系統中進行醫療資訊自主授權之目的。



DOI:10.6814/NCCU201901178


圖 一、具細粒度之授權表單

## 1.5 假設

關乎「授權」的議題是屬於較上層的應用層次，在此必須根據台灣醫療體系內現有的硬體設備及已建立的系統提出兩個假設以更進一步的確保在授權方面之研究的正確性，假設本系統(1)已經擁有完善且安全的分散式資料儲存空間，如此一來整合照護中各機構內龐大資料可個別儲存，不必整合系統所有相關資料儲存到區塊鏈上，並且假設(2)系統擁有一個安全的節點間資訊交換管道，健保署提供之「健保資訊網服務平台服務系統」(以下簡稱健保 VPN)，就是提供醫事機構(像是：醫院、診所)進行醫療費用的申報與健保醫療資料登錄及共享等服務。

具備了上述的兩個假設後，該如何利用區塊鏈讓資訊交換更有信用且更加安全始得具備了討論空間，換句話說，已擁有充分條件可以開始研究資料交換間「授權」的問題。與上述兩個假設相同環境的台灣醫療環境中，在資料授權的問題上依然存在能夠更進一步的空間。

因此我們在這裡提出一個想法：藉由把資料做分散式儲存，再額外建立一個儲存權限之中央索引，將此索引儲存到區塊鏈上，利用智能合約判斷權限是否存在於中央索引中以達到資料授權自動化。如此一來在做醫療共享資料交換時就可以利用在區塊鏈上對資料存取者的權限做身分認證來確保醫療資訊的交換的安全性與隱私性，除此之外，可以藉由區塊鏈不可被竄改的特性來追蹤區塊鏈上的



DOI:10.6814/NCCU201901178

資料調閱紀錄。研究中同時引入數位憑證與身份見證人的機制來進行鏈外的實質身分查核，達到擁有第三方登入的效果，但又不需要犧牲個人隱私，目標為實現新型態的區塊鏈身份辨識服務。

## 1.6 研究問題與目的

無論是衛政體系中之預防保健、醫療照護、長期照護等系統，或社政體系中之社工及福祉資訊、早療、家暴性侵害、高風險家庭、獨居等相關系統目前均各自獨立，若家庭成員一次性發生多類型問題時，由不同單位提供照護不但缺乏整合性，也容易導致服務重疊或出現漏洞，使整體照護效能不佳且預防性不足，因此整合各片段之照護系統，跨系統介接進行家庭歸戶，將有助於舒緩有限資源、長照及社工人力之照護壓力，周全社區照護功能之廣度與深度，並有效提升醫療效率與品質。跨醫院之資訊整合圖示如圖二所示。

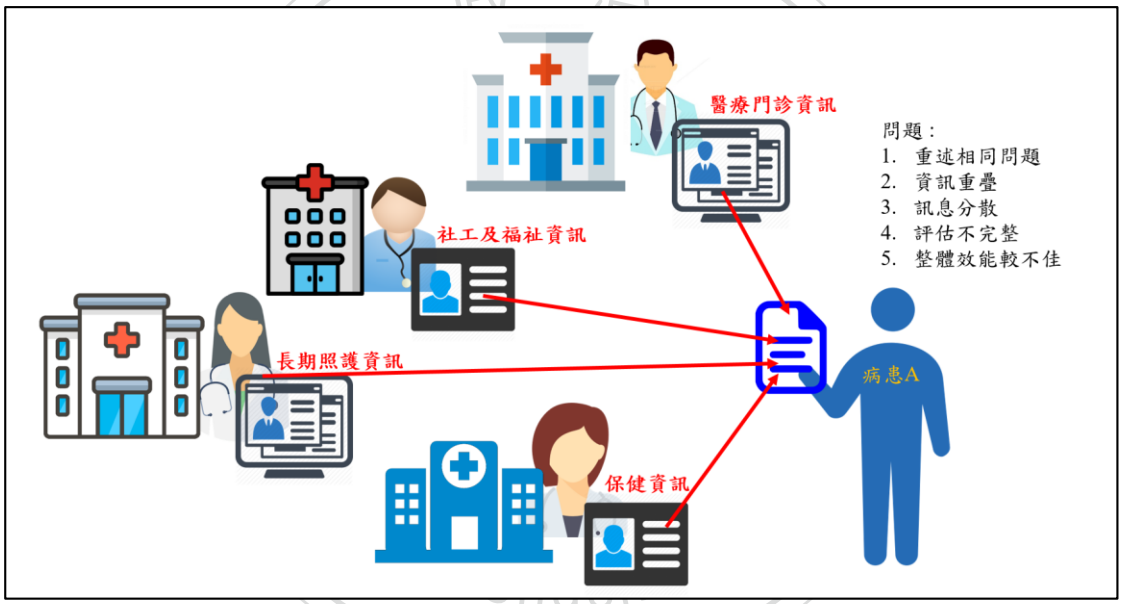


圖 二、跨院級之資訊整合問題

整合各院級機構內醫療資料，在傳統關聯式資料庫之數據交換存在隱私方面的問題，存於院所之數據資料通常屬於民眾較為敏感的醫療資訊，例如：醫療數據、個案內所提及之家庭問題等等，如果將這些敏感的醫療資訊藉由關聯式資料庫統一儲存在中心化的儲存空間內，將存在其資料可能會遭到單點攻擊導致資訊外洩的風險；同時也存在儲存空間的系統管理人員的信任問題，萬一存在惡意管理人員暗中一舉取得整合系統中所有個資並將其進行利益交換則無法防範。這些潛在風險不可避免的將會降低民眾主動分享醫療資訊的意願。

因此本研究採分散式儲存架以取代中心式儲存，各醫療院所將儲存在自己院內看診的詳細病歷資訊。同時整合系統替每一位病患建立一個專屬個人的智能合約來進行個人授權資訊的儲存與讀取，如此一來即可大幅降低中心化儲存所帶來的單點式攻擊風險。上述之授權資訊於本平台架設之聯盟鏈之各節點上均會保存



DOI:10.6814/NCCU201901178

一份，利用區塊鏈共享帳本的特性達到各節點間資料的同步，並利用區塊鏈不可竄改的特性讓醫療資訊的授權紀錄得到保障，並在必要時可進行查詢過往的授權紀錄，達到讓資訊交換更加安全的目的，旨在建立一個資料分散式儲存、中心式索引的照護資訊授權平台。

同時在使用者之身分認證的問題上，由於本整合系統關乎授權，必須確保使用者的確是本人，因此本研究透過引入身份見證人來進行身份認證的實質審查，讓使用者使用身分證字號申請帳號後必須經由身份見證人進行實質審查後才得以成功啟動帳號權限，所謂的身份見證人是預先經過各個照護機構認可可以進行帳號審查的特定單位。使用者帳號經過身份見證人認證後將啟動儲存於手機內的「數位憑證」以便日後的登入與授權動作，如此一來日後使用者不必透過第三方機構而是使用具唯一性之數位憑證進行登入，達成一次性實名驗證即可自主管理憑證，無形中也消除了透過第三方登入讓該機構可以追蹤使用者在網路上之個人活動的隱憂，除了提高個人資料的自主性，也確保了個人隱私的安全性。

上述的「數位憑證」是一個形象化的說法，實際上數位憑證的啟動流程是由申請者註冊會員後發送申請帳號通知到智慧合約上，再由身份見證人經過審查後到區塊鏈上以身份見證人自己的私鑰密碼進行區塊鏈簽核，對使用者的帳號申請進行認證後啟動使用者手機內的數位憑證。整個簽核流程在區塊鏈上可能只是用一串簡單的文字代表、保存。使用者的個人資料還是歸在各個照護機構，在區塊鏈上只會保留認證數位憑證的文字紀錄，以供日後查詢。最後，我們的訴求是藉由參照並延伸台灣現下的醫療環境，把區塊鏈應用在很好的最後一哩路上。

# 第二章　文獻回顧與探討

## 2.1 MedRec

MIT Media Lab 之區塊鏈專案：MedRec[3]同樣是在探討如何利用區塊鏈五對授權資訊本身進行保護，MedRec 為一利用區塊鏈技術的醫療紀錄管理系統，MedRec 中提出兩項醫療機構間醫療紀錄管理上的問題(1)各醫療機構間缺乏協調性的機制與管道來互相交換及共享病人的醫療紀錄；(2)醫療紀錄的管理權掌握在醫療機構手上，由於擔心洩漏醫療紀錄的保密性，造成會有民眾不願意揭露病情或者是避免就醫的情況。以上兩項問題造成民眾或醫療機構均缺乏動力參與醫療紀錄的維護。因此 MedRec 想要建置一個去中心化、可信任的分散式醫療紀錄存放平台，並讓病人擁有醫療紀錄的存取控制權，可以自己設定哪些醫療機構有權存取自己的醫療紀錄，同時日後可對自己曾經的授權紀錄進行查詢與變更，利用區塊鏈無法竄改的特性建立一個去中心化的分散式醫療紀錄系統。

本研究與 MedRec 的主要差異在於(1) 本研究為提升效能，各機構的病歷資料索引是集中儲存與快取管理於鏈外，但 MedRec 則是在鏈內的智能合約儲存民



DOI:10.6814/NCCU201901178

眾資料的索引，這會增加系統處理資料調閱所需時間與維運成本；(2)承上，本研究的系統不改變醫療機構現有的電子病歷系統之運作，而是透過一個外加的閘道程式取得資料索引與資料內容，MedRec 需要調整電子病歷系統，每當有新資料夾入時，要同步將資料索引寫入區塊鏈智能合約；(3)本研究運用以太坊[4](Ethereum)區塊鏈的產製公私鑰的機制，加上集中式身份見證的模式，就身份審核通過的使用者提供其電子簽章所需的數位憑證，存放於手機的安全儲存區，方便使用者直接以手機 App 進行授權書的區塊鏈電子簽章，寫入區塊鏈內，還提供代理人機制，MedRec 的論文則未提及有此部分之功能。

此外，本研究利用 PoA(Proof of Authority)來做為共識機制，由授權節點輪流產生新區塊，其餘節點僅能同步帳本，共享與共管民眾對照護資料的調閱授權紀錄。優點為只需一次性的節點建置成本，不需日常耗費資源又慢的挖礦共識成本。反觀 MedRec 利用 PoW(Proof-of-work，挖礦)作為共識機制，因此需要設計特殊的誘因機制，以補償參與機構的挖礦成本。最後，MedRec 僅在單一的醫學中心完成先導性實作，本研究已經在五家醫院與數家小型醫療機構上線運作。

## 2.2 Blockchain-based Bidirectional Updates on Fine-grained Medical Data

Blockchain-based Bidirectional Updates on Fine-grained Medical Data[5] 利用區塊鏈與智能合約達到可細粒度授權與更新授權並將歷史紀錄儲存於鏈上，旨在解決傳統的雲端加密儲存受限於集中式訪問可能的單點故障風險，於授權部分作者將完整的醫療數據切分成許多較小的片段，資料擁有者可以基於預設協議給予不同的訪問者共享不同的具細粒度之數據，具有相同特徵的對象則可以共享完整訊息的某部分特定資訊，可避免額外的數據干擾並保護專有數據不被洩漏，並利用 Bidirectional transformations(BX)使完整數據與分割數據間取的一致的同步，達到將鏈上共享資料與鏈下本地資料進行同步的目的；但即使將醫療數據作切割，這些數據成本依然會對區塊鏈造成不小的負擔，因此在這邊我們採用將完整醫療數據各自儲存在各節點的資料庫中，並只在區塊鏈上儲存使用者授權過的「授權索引」，爾後醫療照護單位要調用詳細病歷的話，就可以去區塊鏈上之授權索引訪問權限，如果從鏈上查詢到民眾確實有授權給該名醫療單位，則該醫療單位即可根據該授權權限向本地資料庫中透過 Gataway 調閱出詳細的病歷資料。

## 2.3 FHIRChain

FHIRChain[6]同樣也是藉由區塊鏈整合醫療資訊之平台，透過美國醫療數據標準 FHIR (Fast Healthcare Interoperability Resources)實現可互操作性之共享醫療 IT 系統；FHIRChain 使用基於公鑰密碼學之 digital health identities 驗證參與者身分，解決可識別之授權問題，被授權者會利用數字簽章獲得一個 Token，此 Token



DOI:10.6814/NCCU201901178

會被記錄在智能合約上，當被授權者使用權限來訪問資料時該存取紀錄會被儲存於區塊鏈之 Log 中，以便日後任何可能需要的查驗；FHIRChain 將敏感醫療數據存於資料庫，並用 Pointer 指向對應之醫療數據，避免將敏感資料儲存於鏈上之洩漏問題；FHIRChain 利用區塊鏈實現細粒度授權，使面對面或遠端療程更具效率，但其共享之醫療資訊必須符合 FHIR 標準，此為 FHIRChain 之限制之一，且 FHIRChain 並未對儲存資料庫之醫療訊息加密，有可能在傳輸資料的途中被攔截或竄改，FHIRChain 未來會致力於使用零知識證明來加強資安的部分；本研究則是藉由各醫院將醫療資訊加上 Sault 後達到加密的效果，藉此保護敏感之醫療資訊；FHIRChain 藉由公鑰密碼學幫助驗證參與者之身分驗證，產生了私鑰管理上的子問題，而本研究之病患私鑰(憑證)則是儲存於各自的 APP 中，可有效解決管理私鑰上的問題。

# 第三章　研究方法

依本研究之目的與假設，本研究設計並開發了一個整合照護資料共享的授權平台，此平台的主要設計原則有(1)盡可能不改動各醫療機構現有的照護資料的儲存與管理設施，採外加方式，以具開放性與擴充性的架構建置授權平台；(2)以分散式儲存本平台使用者的詳細病歷資料，搭配儲存於區塊鏈上之授權權限中央索引；(3)應用區塊鏈技術開發使用者授權系統，包含使用者授權 App，提供以區塊鏈交易為依據的自主授權與查詢功能；(4)將共享資料分類與階層化，並以角色區分資料調閱人員，以提供細粒度資料存取控管功能；以下分幾個面向來說明本研究發展的授權平台如何實現以上設計原則。

## 3.1 開發流程

本研究欲在確保民眾隱私醫療資訊的安全性以及授權資訊之正確性的保護下，透過共享醫療與照護病歷達到促進醫療看診效率、增進人民健康福祉的目的。為了建置本照護平台，詳細之開發流程如圖三所示，流程共包含七大步驟，首先，第一步驟必須完成包含連江縣立醫院、北竿鄉衛生所、東莒衛生所、西莒衛生所、東引鄉衛生所、臺北市立聯合醫院、三軍總醫院、亞東醫院及萬芳醫院之硬體伺服器(1U、2U)設備的建置；第二步驟需要統一各單位之資料傳輸格式，包關相關 Json 格式的訂定以及定義照護資訊授權 APP、身份見證人 APP 對醫療機構資料間的介接 API 規範；第三步驟必須針對照護資訊授權 APP、身份見證人 APP 進行 UI 介面的討論與設計，同時定義出身份見證人角色以及服務提供者之機構與職業別，服務提供者與職業別將用於日後判斷該服務提供者是否被授予權限的查詢上進行比對，本研究中之服務提供者之職業別共有六種，分別是行政人員、居家服務人員、社會服務人員、長照服務人員、醫療照護人員、健康管理人員；第四步驟必須利用步驟二規範出之 API 建構出照護資訊授權 APP、身份見證人 APP，照護資訊授權 APP 可供民眾進行過去病



DOI:10.6814/NCCU201901178

歷資訊的授權與查詢，而身份見證人 APP 可供身份見證人對民眾的註冊申請進行實質審查；第五步驟必須在五大授權節點上建構區塊鏈節點以進行授權資料間的帳本同步；第六步驟必須完成智能合約的設計以及區塊鏈與 APP 端溝通之 Middle-tier 的編寫，將區塊鏈整合進 APP 中並進行相關測試；最後，第七步驟進行教育訓練，並於連江縣進行推廣與教學，在此期間也會對民眾進行訪談與回饋。

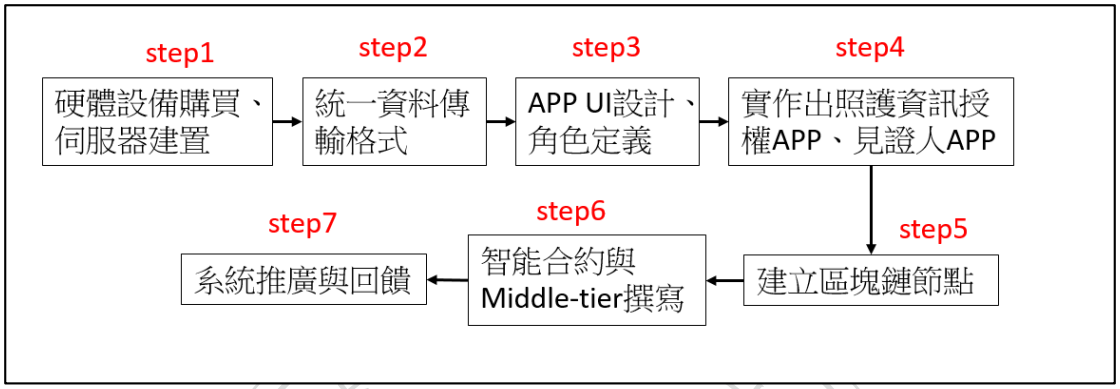


圖 三、整合系統建構流程圖

## 3.2 參與醫療院所機構與區塊鏈節點

目前有參與到健康福祉整合照護示範場域推動之醫療機構包含連江縣立醫院、北竿鄉衛生所、東莒衛生所、西莒衛生所、東引鄉衛生所、臺北市立聯合醫院、三軍總醫院、亞東醫院及萬芳醫院共 9 間醫療機構，規劃於每個機構設置 1 台閘道器(Gateway Server)共 9 組，如圖四所示。閘道器的功能為(1)機構內照護資料與外部資料溝通交換媒介之服務系統；(2)同時為智能合約(區塊鏈技術之一)之節點(Node)。接著再從這 9 個機構中，選取其中較為大型的 5 間醫療院所作為區塊鏈之授權節點，此 5 個節點分別為連江縣立醫院、萬芳醫院、北市聯醫、亞東醫院、三軍總醫院，一同執行智能合約授權管理功能。此外，臺北市立聯合醫院之閘道器配備較多的資源，也同時扮演本平台的整體服務入口角色，提供(1)使用者註冊智能合約讀寫；(2)使用者授權紀錄的寫入與查詢；(3)資料庫服務等功能。

簡言之，本授權平台係根基於參與醫療機構現有的照護資料的儲存與交換設施，透過外加的閘道器與區塊鏈網路來實現後台的使用者管理與資料共享的控管功能。未來有新的機構要加入此一平台，只要增加閘道器與安裝搭配的軟體即可，擴充上相對容易。



DOI:10.6814/NCCU201901178

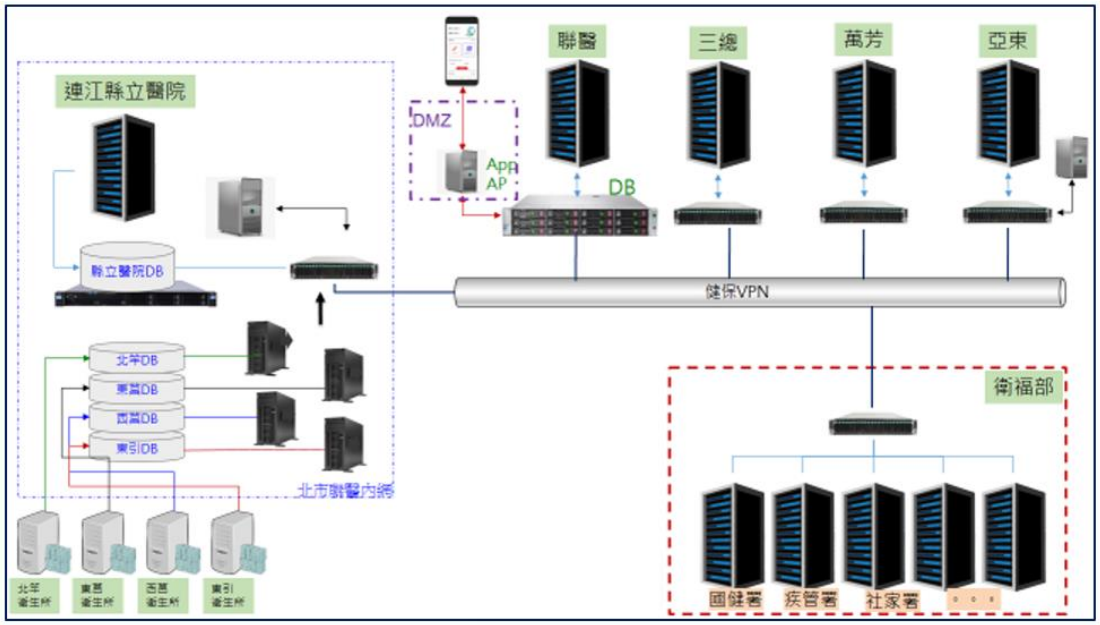


圖 四、資訊整合節點示意圖

## 3.3 整合系統架構

本系統整合平台之後端是基於 Nodejs 與 Express 做開發，並利用以太坊提供之 Web3[7]函式庫撰寫 Middle-tier 讓區塊鏈外部能與區塊鏈上之智能合約進行溝通，前端 UI 分別實作出照護資訊授權 APP 供使用者註冊、授權以及身份見證人 APP 供身份見證人進行實質審查，本研究之整體系統架構圖如圖五所示。



DOI:10.6814/NCCU201901178

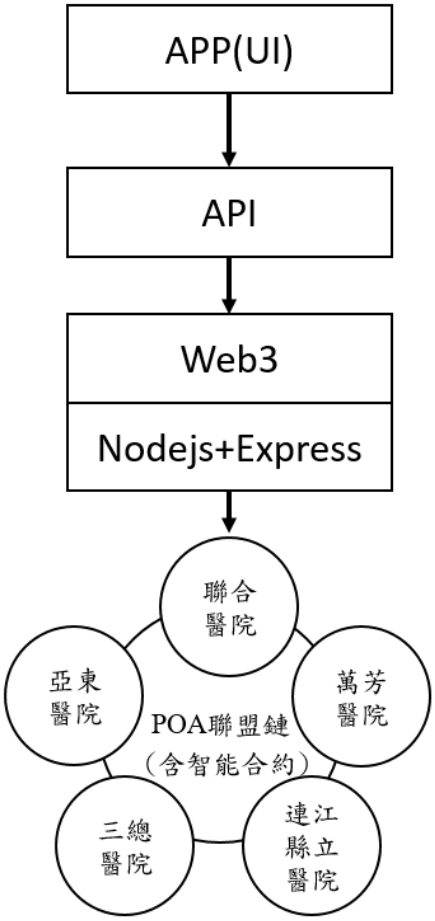


圖 五、整合照護之系統架構圖

除了 APP 與區塊鏈以外還必須有一個前端介面「服務提供者調閱系統」供醫療照護人員(例如醫生或社工人員)登入後可進行被予以權限之病歷資訊的瀏覽，這部分是由本計畫之合作公司-商之器實作之前端網頁，醫療照護人員可在註冊後登入進行瀏覽病患先前透過照護資訊授權 APP 所授權之醫療資訊，整體授權與調閱流程如圖六所示。

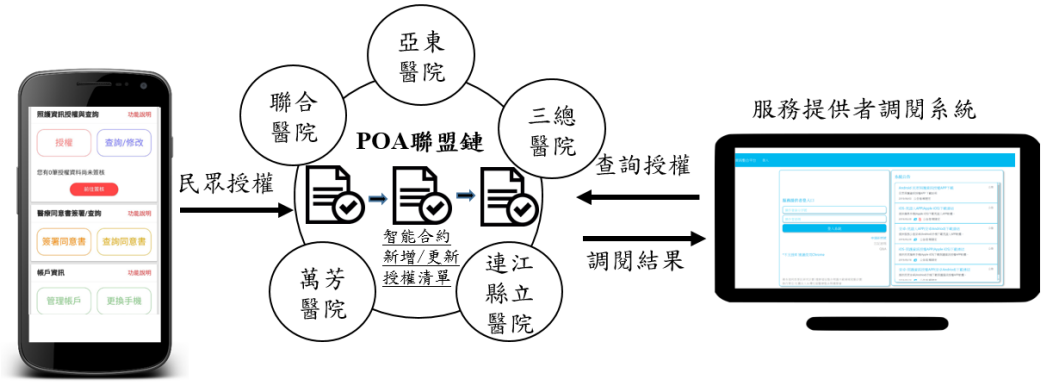


圖 六、授權與調閱流程圖



DOI:10.6814/NCCU201901178

## 3.4 POA(Proof-of-Authority)共識機制

本系統整合平台之區塊鏈利用 PoA(Proof of Authority)之共識演算法讓本系統之 9 個醫療機構擁有並同步同一份「帳本」，帳本內容可以是各類授權資料或病歷索引。PoA 與 PoW(Proof of Work)最大的不同是，因為 PoW 的共識機制是建立在節點互相不信任的情況下，因此需要經過工作量證明「俗稱挖礦」來互相競爭以進行節點間帳本的同步；還有一種共識機制是 PoS(Proof-Of-Stake)，此共識機制中的區塊鏈節點擁有較多的代幣(Token)則擁有較大的權益，權益越大的節點就越有機會負責產生新的區塊，PoS 的出現試圖以另一種不同的競爭機制取代原本的 PoW、減少比拚算力的資源浪費，但 PoS 中判斷權益的大小是透過比較節點中 Token 的多寡，因此 PoS 某種程度上也是屬於挖礦的一種，仍是用 Token 來取代原本 PoW 的礦工機制，跳脫不了必須使用 Token 的限制。

而整合平台所採用之 PoA 共識演算法則是基於區塊鏈上已批准的身份(節點)，這些授權節點都為是先被驗證過之組織、彼此信任，因此在確認交易時不需要去彼此競爭、浪費運算資源，也不必在區塊鏈中創造 Token，因此在可信任環境的前提下 PoA 不失為一更有效率的共識機制。本研究中設立區塊鏈節點之 5 間醫療機構皆為在台灣知名且有信譽的組織，因此採用 PoA 作為共識機制。最後，本研究所建置之區塊鏈為第一條台灣政府所使用且為跨醫院系統整合之鏈，可視為台灣區塊鏈應用之重要里程碑並作為未來實現區塊鏈應用之指標與參照。

## 3.5 醫院內外網與資訊安全

醫院機構對於資訊安全的層面上特別注重，因此必須在導入區塊鏈前先擬定所需要的 ip 位置與 port，讓各院間防火牆之相互開放，同時為顧及照護資訊交換之安全性，照護資訊授權 APP 與平台網頁服務設置於外部網路，利用與內部網路之間的非交戰區域 (Demilitarized Zone, DMZ)作區隔，避免外部網路被攻破後即可長驅直入進醫院內網，防止嚴重的資訊洩漏問題，另外各機構間經由健保 VPN 進行資料交換，且資料不存放於 DMZ 區域，資安與資訊流示意圖如圖七所示。



DOI:10.6814/NCCU201901178

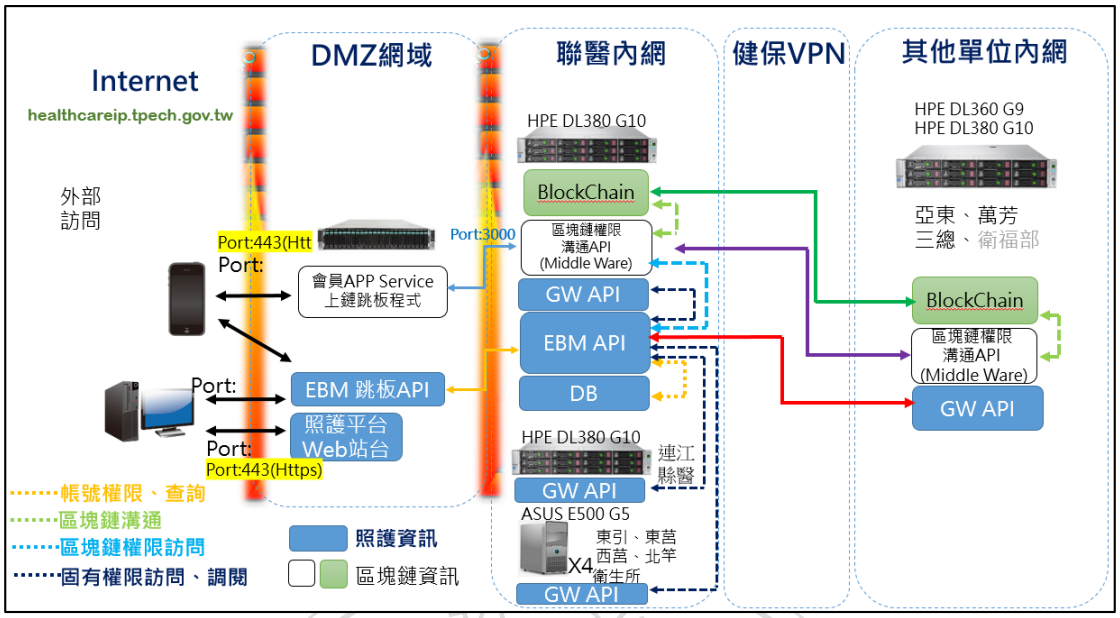


圖 七、資安與資訊流示意圖

## 3.6 角色介紹

本研究之照護資訊授權 APP 平台之使用角色主要分為三種：(1)使用者(病患、代理人)；(2)服務提供者；(3)身份見證人。

(1) 使用者(病患、代理人)：

當使用者需要進行醫療資訊授權時可以使用照護資訊授權 APP 進行區塊鏈上的簽核並授權，不使用網頁進行授權的目的是要確保授權動作的合法性，使用者在申請帳號並由身份見證人驗證身份後將會啟動與身分證字號做綁定之憑證，經過此具唯一性之數位憑證對醫療機訊進行授權即可確定要進行授權的病患即為本人，以此來確保資料授權的合法性。另外為了加速開發流程，本研究使用 Cordova 開發可跨平台(包括 Android、IOS、瀏覽器)之照護資訊授權 APP、身份見證人 APP，Cordova 為一開源的開發框架，允許使用標準的 Web 技術包含 HTML5、CSS、JavaScript 進行跨平台開發，達成開發過程中只要編寫一次程式後就能夠在各種平台上運行，提升開發的效率同時降低開發成本。

(2) 服務提供者 ：

在定義服務機構的職業別時，本研究就實際各院所之參與單位將服務提供者分為六大單位，分別是行政人員、居家服務人員、社會服務人員、長照服務人員、醫療照護人員、健康管理人員。當服務提供者需要調閱使用者的授權資料時，因為調閱屬於單純的資料讀取動作，不牽涉到資料的寫入動作，不同於民眾必須使用 APP 授權之限制，因此可透過服務提供者之網頁平台，登入系統後即可對已被予以授權之病歷進行瀏覽及調閱詳細內容。

(3) 身份見證人 ：



DOI:10.6814/NCCU201901178

照護資訊授權 APP 之帳號註冊與認證透過引入「身份見證人」來進行實質審查帳號註冊人的申請。所謂的身份見證人是預先經過各個照護機構認可可以進行帳號審查的特定人群。身份見證人之實質審查是一次性的，一旦通過這道審查程序就代表照護系統同意自此後該手機裝置可全權代表使用者本人，因為手機裡有專屬於使用者自己的一個具唯一性的數位憑證，使用者即可在未來掌握自己過去所有的病歷資訊並可自主授權，實現自主個人資料的目標。

## 3.7 照護資訊授權 APP

照護授權 APP 主要功能有 4 種，分別為會員註冊、代理人註冊、申請新憑證、照護資料授權之功能，以下就設計目的與方法進行分別說明。

### 3.7.1 會員註冊、代理人註冊

會員註冊與資訊授權示意圖如圖八所示，使用者下載 App 並進行會員註冊後，本系統替使用者創建一區塊鏈帳戶（即研究中使用之以太坊區塊鏈平台的地址，區塊鏈帳戶地址係由公鑰產生，具有一對一之關係），包含公私鑰一組，並與會員之身份證字號連結，用以辨識會員並提供會員執行區塊鏈資料寫入功能時（即授權照護資料），進行電子簽章之用，我們簡稱這個以太坊帳戶與公私鑰為區塊鏈憑證，此憑證經加密後儲存於手機內。

但是這個憑證不會馬上生效，註冊完後使用者必須等待身份見證人之驗證，才能成為正式會員，並啟用其區塊鏈憑證進行照護資訊授權。身份見證人扮演類似 PKI 中 RAO(Registration Authority Officer，憑證註冊審驗人員)之角色，並由各機構管理者授予及管理。本系統藉由引入身份見證人的機制來實質審查註冊者之真實身份，讓會員帳戶具備真實性與唯一性。

有鑒於區塊鏈擁有不適合儲存大量資訊的特性，使用者註冊後系統只會將其個人資料其中的重要欄位(身分證字號、以太坊帳戶地址)存入系統之會員管理智能合約中作為辨識管理之用，藉由只存入會員之必要資訊來節省區塊鏈上的儲存空間。

此外，系統同時會幫會員部署一個「授權合約」到區塊鏈上，並將其「授權合約地址」與會員之以太坊帳戶地址做綁定，每個使用者各自擁有一份授權合約，此授權合約將用於未來會員做醫療資訊授權，用於儲存與管理該會員之醫療資訊授權資料。



DOI:10.6814/NCCU201901178

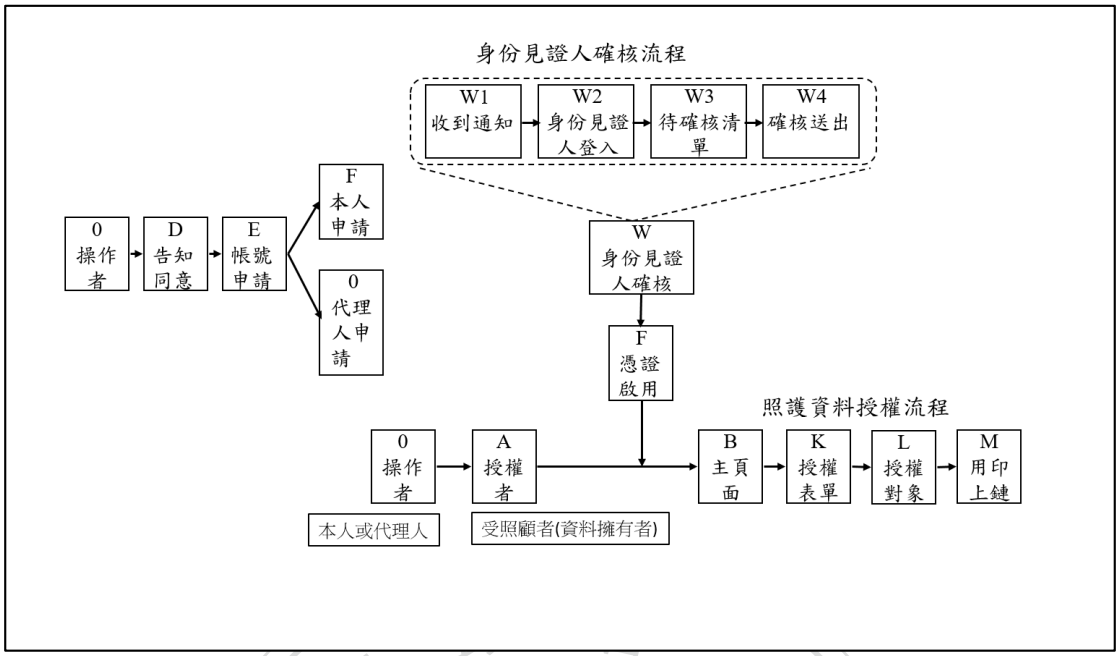


圖 八、區塊鏈數位 ID 會員註冊與資訊授權流程圖

為顧及無行為能力者以及不熟悉手機操作之民眾，本 APP 提供民眾管理其其代理家屬(無手機或未成年者)之功能，代理人代替其家屬進行註冊後產生之區塊鏈憑證將會存放在代理人的同一支手機上，未來進行授權時也必須使用該手機進行授權，實現一機多憑證的目的。同時為達「關注全家」及「個資隱私保護」，App 也提供民眾自主管理其家屬成員清單(如圖九所示)，此清單可幫助服務者於查詢照護資訊時提供一個全人、全家及全程照護之環境。


圖 九、一機多憑證與維護親屬關係頁面圖



DOI:10.6814/NCCU201901178

### 3.7.2 申請新憑證

為了處理遺失手機等特殊狀況，本系統設有申請新憑證的功能，當使用者更換手機並登入後，可以進行申請新憑證，此申請同樣會寄送通知給身份見證人進行審查，身份見證人審查通過後系統將會給予該帳號一組新的區塊鏈數位憑證，使用者即可在新手機上進行授權動作。

申請新憑證的設計原因是因為整合系統中使用者的區塊鏈數位憑證會存放於原本手機上，使該手機與區塊鏈憑證彼此具備唯一性，因此萬一使用者不慎把手機遺失或是在更換新手機的情況下，就必須登入新手機後向利用申請新憑證的功能產生一個新的區塊鏈憑證至新手機上，並且新憑證申請送出後也同樣需要等待身份見證人來做實質審查，審查通過後即會對該區塊鏈憑證進行啟用。

### 3.7.3 授權照護資料

民眾完成註冊與會員審查後，可透過本 App 進行照護資訊查詢與授權功能。首先，App 提供民眾查詢自己的照護資訊索引，此時系統會將民眾在各機構的照護資訊紀錄以索引方式回傳，並以群組或單筆方式供民眾瀏覽，以選擇全部或部分進行授權；授權內容分為授權對象（機構、職業別)及授權期間（從一日到永遠)，勾選完成後 App 會將授權內容規格化，生成以太坊區塊鏈之寫入交易，並要求輸入 App 密碼以啟動私鑰，對交易進行電子簽章，再傳送至後端，寫入民眾於區塊鏈上之專屬授權合約內，最後並透過區塊鏈的同步機制，分享給區塊鏈網路上的各個節點，日後民眾也可以透過 App 隨時查詢及改變授權內容。

之後，當服務提供者欲透過調閱平台調閱民眾在其他醫療機構之照護資訊時，系統會對民眾的授權合約發出徵詢，以確認民眾是否有授權該服務提供者調閱其資料。民眾照護資訊授權及查詢管理如圖十所示。


圖 十、民眾照護資訊授權及查詢管理圖示



DOI:10.6814/NCCU201901178

## 3.8 服務提供者調閱資料

服務提供者可於服務提供者調閱系統上調閱已授權之照護資料，照護資訊查詢與調閱之流程如圖十一所示，服務提供者進行調閱照護資訊之操作情境說明如下(以醫療照護資料為例)：


圖 十一、照護資訊查詢與調閱

步驟一：服務提供者以民眾身分證字號進入系統調閱照護資料，系統自動由區塊鏈智能合約比對可被調閱(符合授權項目及期間者)項前啟用(Enable)「已授權」字樣。

步驟二：點下「授權」字樣後，服務提供者即可查詢到詳細照護資料(第二類資料)。

由於服務提供者必須透過部署在區塊鏈上的「授權合約」中的函數來調閱資料，因此任何調閱紀錄(包含調閱者所屬機構、調閱者身份、調閱病歷之唯一辨識值)將會被儲存在區塊鏈的 Log 上，區塊鏈對於寫入之資料具有不可篡改的特性，因此保存之調閱紀錄都可以用來幫助未來追查非法調閱的問題。將調閱



DOI:10.6814/NCCU201901178

紀錄儲存在 Log 上的另一個好處為，在未來查詢調閱紀錄的時候，就不必進入區塊鏈中去撈取調閱資訊，可以在區塊鏈外對 Log 資料進行查詢，此方法可增加查詢的速度同時可以省去查詢時的 Gas 成本。

## 3.9 智能合約之模組化

研究中為了實現模組化分工，提升程式可讀性與維護效率，因此在設計上將智能合約依照功能性做切割，分別是(1)註冊合約；(2)授權合約。合約內部結構與關係如圖十二所示，為了節省區塊鏈之儲存空間，註冊合約內只會儲存使用者身分證字號、使用者以太坊地址、授權合約地址，而非將所有的會員資料上鏈，此外，每個使用者會對應到一份授權合約，授權合約內儲存著使用者的醫療授權資訊，授權合約內同時記錄著該名使用者之註冊合約地址以作綁定。

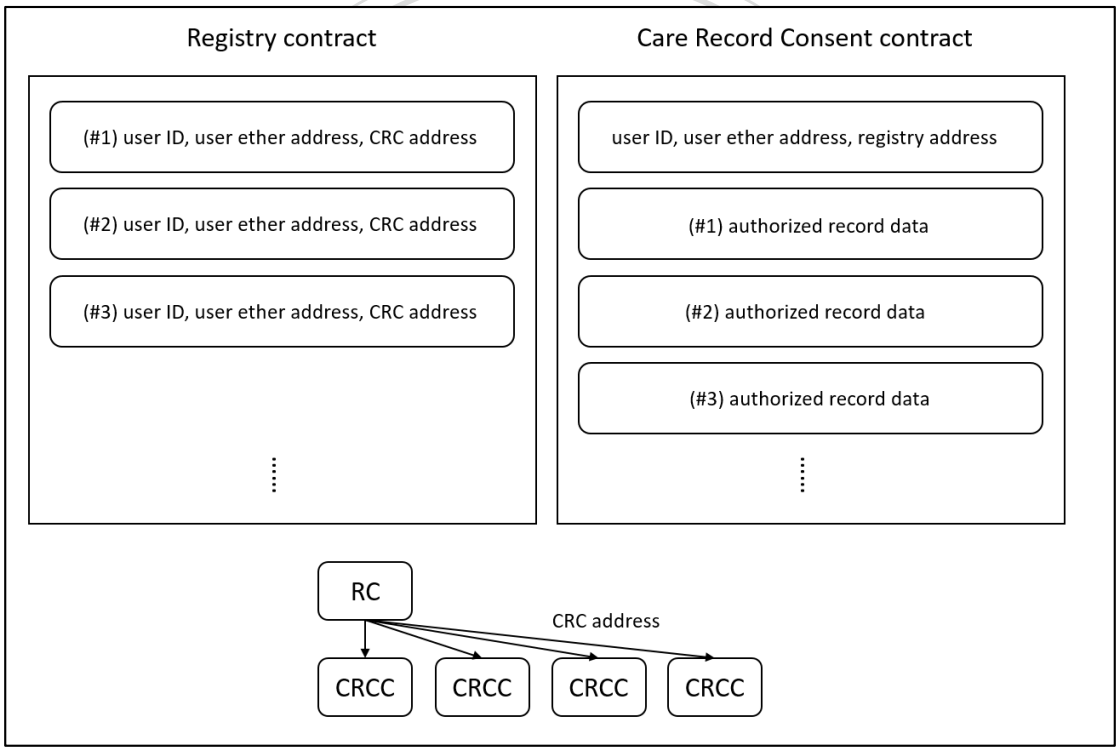


圖 十二、智能合約概念圖

## 3.10 授權醫療資料之種類與設計

在資料「授權」的設計上，有鑑於考慮到各種情況下之授權情形，此段將由醫療授權情境加以著重說明，授權類別可分為兩種：(1)事前授權；(2)當場授權，每種類別又可向下區分出兩種情況：(1)本人授權；(2)非本人授權，因此共有四種授權情境，授權流程圖如圖十三所示。



DOI:10.6814/NCCU201901178

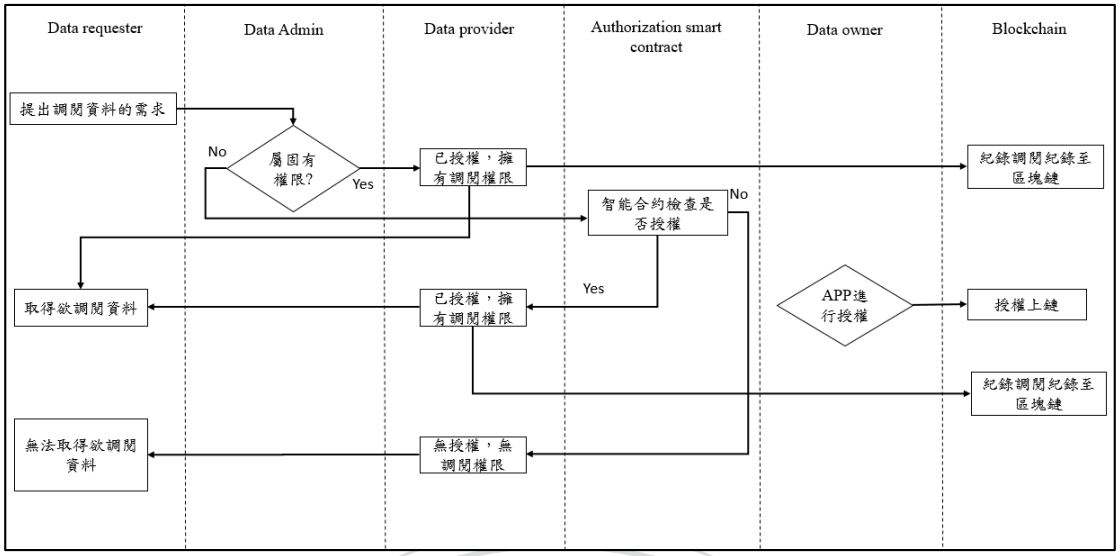


圖 十三、授權流程圖

「事前授權」以醫療照護為範例說明。病患進行初次看診時，系統會根據病患之身分證、醫院、科別、醫生生成事前權限，實現共享醫療資料以便日後的看診，有助於提升未來醫療品質。其中，「固有授權」屬於事前授權的一種，當病患至一醫院看診並由該醫院產生病歷，則該醫院就屬於此病歷之固有授權範疇。

「當場授權」以醫療照護為範例說明。病患可透過照護資訊授權 APP 平台進行當場授權，APP 內部授權之角色分成兩種，分別是(1)操作人；(2)授權人，以建立操作人與授權人角色上的差別。如果是病患本人要進行授權，則病患本人可選擇自己的帳號與密碼登入，此時操作人為病患本人，本人登入後於選擇授權人頁面中，選擇病患自己為授權者帳號，表示病患本人同時為授權人，登入後如欲進行授權則可進入授權清單勾選欲授權項目，最後輸入密碼進行區塊鏈簽核，完成授權。病患本人授權之圖示如圖十四所示。

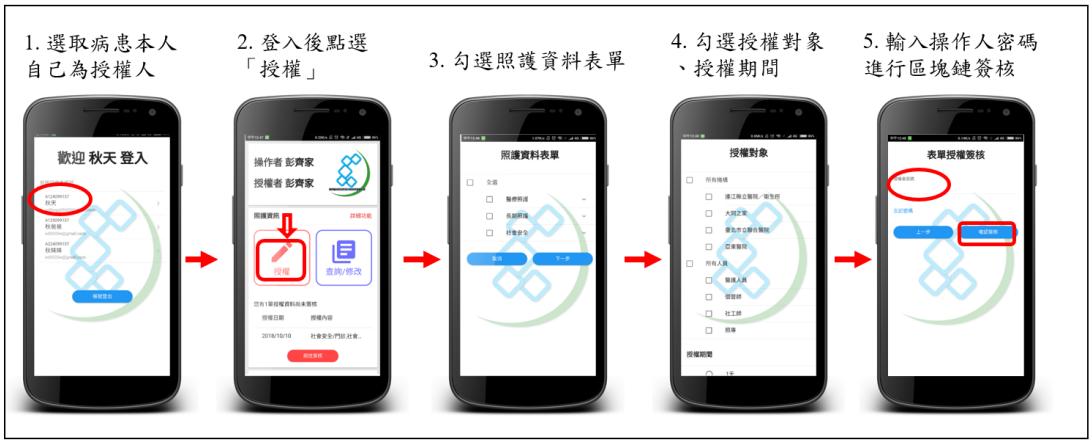


圖 十四、本人進行授權之 app 內操作流程

考慮到在特定情況下，會存在無行為能力人或身體不便之民眾欲進行資料授權以進行照護或看診，就此情況下將衍生出由代理人授權之需求，於此情境



DOI:10.6814/NCCU201901178

下代理人登入系統後於選擇授權人頁面中，為了避免被代理人之密碼外洩下仍能進行代理授權，此時代理人允許輸入被代理人之身分證字號與電話號碼代表授權人為被代理之病患。代理人授權之圖示如圖十五所示。


圖 十五、代理人代替授權之身分識別

## 3.11 授權合約設計

在授權合約之設計中，本研究將授權清單之病歷資訊分成兩類儲存在智能合約中(1) 以全部、大類別、次類別儲存；(2) 以單筆病歷資料的識別碼[1](SourceKey)儲存，以此分類設計增加授權的彈性以及加速日後查詢與比對是否已授權時的速度。

如果在勾選授權清單時，如果使用者勾選單一的病歷資料，本系統就會將該筆病歷資料儲存到區塊鏈上；如果使用者勾選大類別(次類別)代表願意授權其中所有的子項目，因此本系統將該類別資訊以陣列的方式儲存到智能合約內。例如，使用者選擇將病歷「全部」授權出去，則系統會以陣列[0]的方式代表將類別「全部」儲存在智能合約內，日後當服務提供者對一使用者進行病例調閱時，智能合約只要比對到該調閱資料包含在某一被授權的大類別(次類別)中，則系統就會給予該服務提供者合法授權的權限，如此一來就不必去比對到單筆的病歷資料就可以判斷是否授權，此設計幫助系統在授權時進行細粒度授權，並在服務提供者調閱詳細病歷資料時加速權限查詢的速度。

而服務提供者在調閱病歷時，在考量到 Gas 消耗量的情況下，通常在調閱時需要比對多個單筆資料的情況下會需要用到 for 迴圈來比對多筆授權資訊，但在區塊鏈中使用 for 迴圈所消耗的 Gas 會比較昂貴，因為 for 迴圈包含一些加法與其他運算元，這些運算元將會增加執行調閱時的 Gas 消耗，增加成本。因此為了節省 Gas 消耗量，本研究將另外在 middle-tier 中撰寫程式，並將該 for 迴圈放到區塊鏈外去進行，因此比對時只要將把一筆一筆的授權資料傳入智能合約中做比

[1] 識別碼是由單筆資料的內容經安全雜湊函數計算得出，採用識別碼是為了保護病患隱私。



DOI:10.6814/NCCU201901178

對，省去在合約內寫 for 迴圈的必要，藉此避免執行調閱時在區塊鏈內執行 for 迴圈，以達到節省 Gas 消耗的目的。

授權表單中除了上述病患之細粒度病歷資料外，還包含該筆病例之(1)被授權機構；(2)授權對象；(3)授權之時間長度，以上授權資訊之儲存資料結構如圖十六所示，合約中使用 mapping 將被授權機構映射到被授權對象再映射到病歷，最後再映射到授權時間，藉由此 mapping 資料結構方便日後醫護人員調閱步驟之檢查權限之需求。其中授權對象將以數字代替，可減少儲存空間，例如，假如使用者要將醫療資料授權給「醫療照護人員、長照服務人員」的話，系統會以陣列[0,1]的形式將以上兩種授權對象儲存到智能合約，以利事後調閱時的身分比對。

如果服務提供者調閱病患醫療資料之時間坐落於病例授權之開始時間與結束時間之間且調閱人員之身分符合當初授權之機構與對象，則區塊鏈將會予以權限供該名醫護人員進行調閱更詳細之病歷資訊。

由於撰寫智能合約之語言 Solidity 不支援傳遞字串陣列 String[]，而一筆病例可能授權給多個機構以及對象，因此本研究將授權機構與授權對象先做 keccak256 加密轉換成 Byte32[]陣列之後才儲存到智能合約中，其中 keccak256 為 Web3 提供之加密函數，日後服務提供者在調閱時也會將該服務提供者之所屬機構與所屬單位做 keccak256 加密後送進智能合約中進行比對來檢查是否有權限存取該筆醫療資訊。

```
// 授權機構=>授權對象=>sourceKey=>授權開始時間
mapping(string => mapping(bytes32 => mapping(bytes32 => uint))) sStart;

// 授權機構=>授權對象=>sourceKey=>授權結束時間
mapping(string => mapping(bytes32 => mapping(bytes32 => uint))) sEnd;

// 授權機構=>授權對象=>類別=>授權開始時間
mapping(string => mapping(bytes32 => mapping(uint => uint))) lStart;

// 授權機構=>授權對象=>類別=>授權結束時間
mapping(string => mapping(bytes32 => mapping(uint => uint))) lEnd;
```

圖 十六、病例儲存之資料結構

為了保護使用者個人資料的隱私，以及區塊鏈上不適合存放大量資料的特性，本研究會將使用者的授權細項經過 Hash 函數轉換後將結果存證於區塊鏈上，因此區塊鏈上只存放授權項目的 Hash 值，日後服務提供者在調閱時也是利用這些 Hash 值進行比對，判斷使用者授權哪些範圍的病歷給該服務提供者，至於詳細的病歷資料會存放於各醫療機構中並透過 Gataway 來進行資訊傳輸。

# 第四章　區域實施與民眾反饋

本研究於系統開發前 2018 年 8 月至 10 月對連江縣的居民做科技意向之調查，如圖十七所示，可以顯現出願意對照護資料做自主授權的比例有 87.44%，其中 75.81%的民眾更是願意提供醫療資訊供研究使用，而調查顯示連江縣居民



DOI:10.6814/NCCU201901178

願意預約臺灣本島醫師視訊看診的比例高達 97.67%，可以顯現出偏鄉離島居民們對於自主授權的高度意願以及醫療資訊共享對於連江縣民眾的重要性。

因此本研究欲進行搭配區塊鏈之照護資訊授權 APP 之開發，一方面可以整合醫療資訊、實現醫療資訊共享，讓病患可以在連江縣當地縣立醫院進行醫療設備檢查(例如照 X 光或斷層掃描)，並透過照護資訊授權 APP 進行自主性授權，將檢查結果提供給臺灣本島醫師，即可提升視訊看診的醫療效率、提供更完善的醫療服務；一方面也可以實現多數民眾願意嘗試的自主授權，達到增進醫療效率、增進人民福祉的目的。

且在這完整的診治過程中，區塊鏈扮演著保護授權資訊正確性的角色，藉由將授權資訊儲存到區塊鏈上，利用區塊鏈不可竄改的特色可避免授權資訊遭到竄改以至於被非法調閱。同時本研究利用區塊鏈分散式帳本的特色將授權資訊同步到各節點上，可幫助爾後查詢授權時將查詢請求作分流，降低區塊鏈的負擔、提升運行速度，並免除掉中央式架構中單點可能被攻擊的風險。

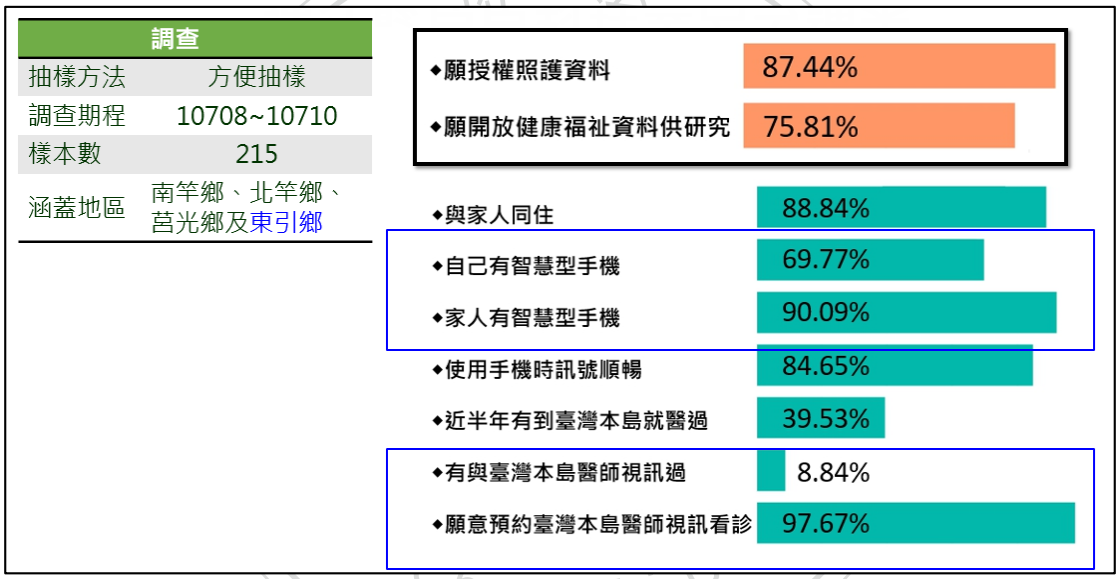


圖 十七、民眾科技意向調查

截至 2019 年 6 月 5 日止，照護資訊整合平台共計 719 位會員，其中居住地為連江縣者計 654 位(91%)，臺灣本島各縣市共計 65 位(9%)；其中南竿鄉計 242 位(34%)、北竿鄉 190 位(26%)、東引鄉 147 位(20%)及莒光鄉 75 位(10%)，如圖十八所示。



DOI:10.6814/NCCU201901178

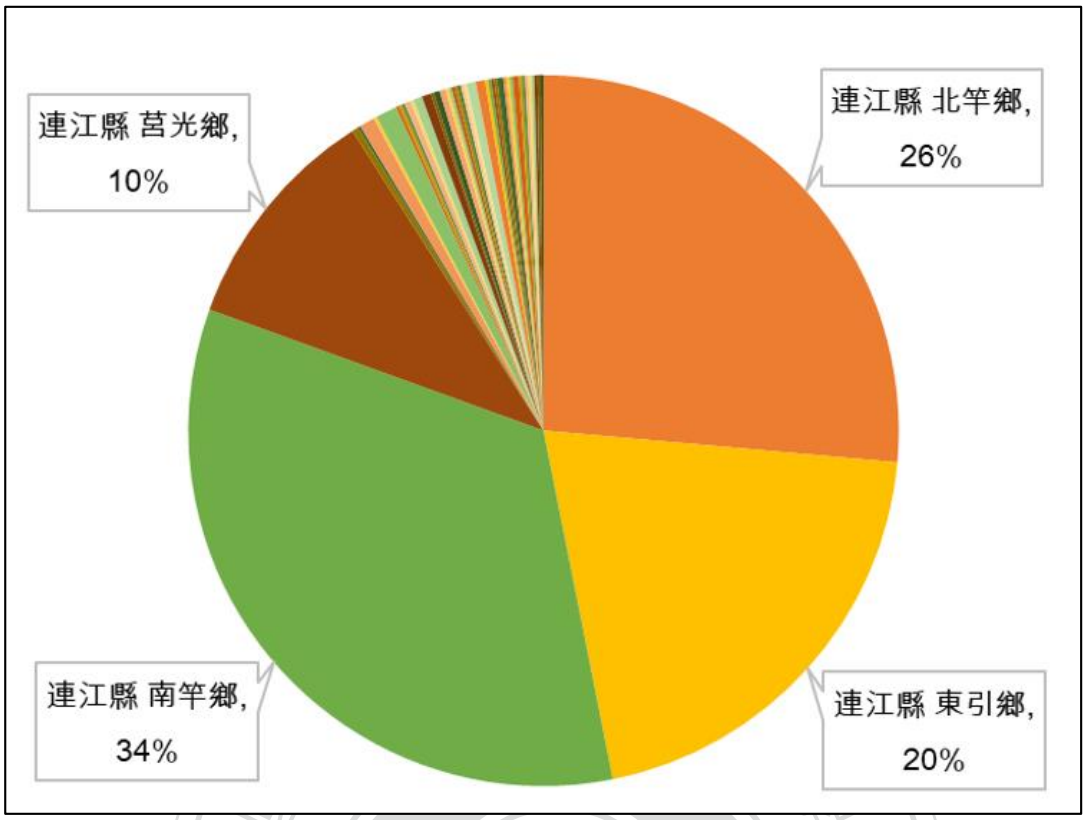


圖 十八、照護資訊整合平台會員居住地分佈

會員年齡區間以 55 至 59 歲為多，50 至 54 歲次之，60 至 64 歲再次之，整體觀之，會員年齡區間多分佈於 35 至 69 歲之間，如圖十九所示。

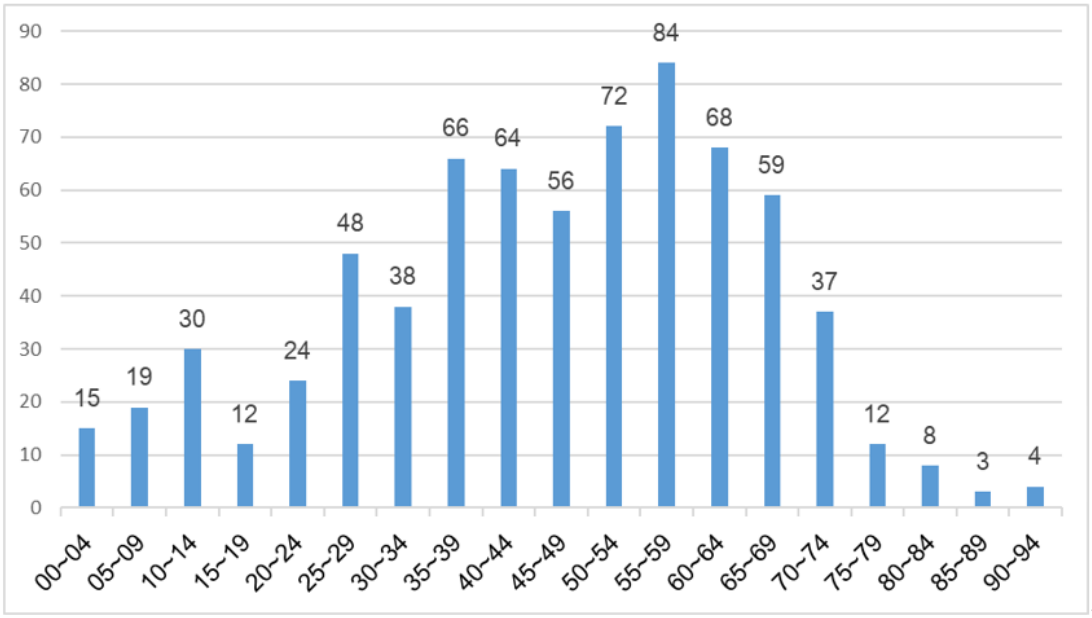


圖 十九、照護資訊整合平台會員年齡分佈

會員選擇全項目永久授權予所有機構計 199 筆之比例最高，選擇大分類授權永久授權予所有機構計 114 筆次之，選擇大分類授權一週予部分機構計 69 筆再次之，如圖二十所示。



DOI:10.6814/NCCU201901178

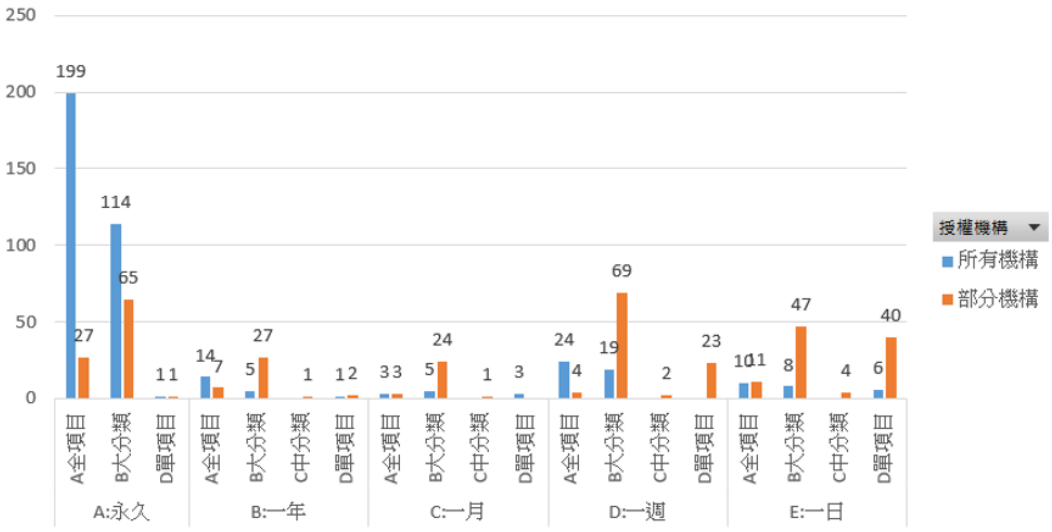


圖 二十、照護資訊整合平台會員資料授權情形

會員授權對象選擇醫療照護人員計 741 筆之比例最高，選擇授權長照人員 314 筆次之，選擇授權行政人員計 289 筆再次之，如圖二十一所示。

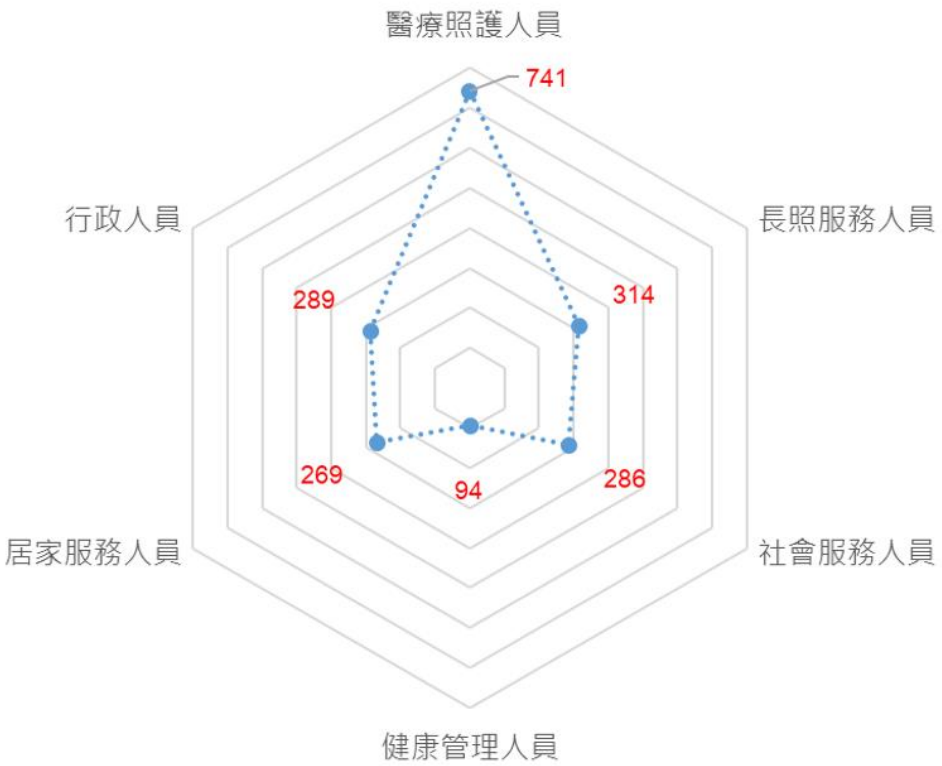


圖 二十一、照護資訊整合平台會員授權對象統計

從統計顯示會員授權情形不難發現到，選擇將所有病歷授權出去之比例最高，約有 302 位使用者(占比約 39.6%)，顯示民眾普遍是以方便快速為主、且相信本系統對於授權內容的保密性以及對服務提供者的信任，而在單項目病歷授權的部分則只有 77 位(占比約 10%)，顯示民眾普遍不會去選擇細粒度較細的項目，雖然這樣看似會降低細粒度設計的價值，但其實這 10%使用者對於病歷資



DOI:10.6814/NCCU201901178

訊的自主授權相對來說其實是比較有意識的，細粒度的設計可以幫助這些對於個資要求較高的使用者提供更完整、精確的授權服務，甚至或許在不久的將來，在民眾個資自主性的意識增強後，會有更多的民眾願意選擇細度較細的項目進行授權，以達到更精準的權限控管，而本系統之細粒度設計將可以很好的應對這種未來可能發生的狀況。

於 2019 年 5 月底本研究團隊於連江縣將本系統向連江縣民進行使用與推廣，以連江縣長照個案為例，流程如圖二十二所示，照護員首先發覺個案病況有變化時，即安排台北市立聯合醫院醫師進行居家訪視，北市聯醫醫師即可根據個案的需求協助民眾進行醫療資訊的授權，授權完成後醫師即可對民眾的詳細病歷資訊進行調閱，同時確認個案病情與藥物運用狀況，最後透過整合各方面的醫療資訊執行立即改藥的動作，由此可見，整合照護的方便性得以讓即時醫療的效率獲得改善，且因為醫師擁有所需要之各方面對於個案的資訊，不論是家庭狀況或是個案過去歷史紀錄都可以運用病患的自主授權加以瞭解，醫師即可針對個案做最客製化的醫療服務。


圖 二十二、連江縣長照個案流程圖

從連江縣長照個案中即時改藥的個案可發覺到，整合系統藉由自主與代理授權實現共享醫療資訊可有效完善長期照護與居家醫療的個案資訊完整度，進一步的增加看診時的醫療效率，讓民眾享有更優良的醫療品質，此外，整合系統也可對現有基層服務據點之資訊服務功能做優化，如圖二十三所示，在連江縣的民眾可以透過自主預約位於台灣台北的視訊醫師，以往因為缺乏醫療共享的資源，因此看診時會造成資訊不完全、醫療效率降低的結果，透過醫療整合照護 APP 民眾即可將自己過去的醫療資訊共享出去給位於台北的醫生，即可突破空間限制讓醫療的品質與效率獲得提升，最後醫生透過照護資訊整合平台即可調閱出被民眾授權的醫療項目的詳細資訊。



DOI:10.6814/NCCU201901178

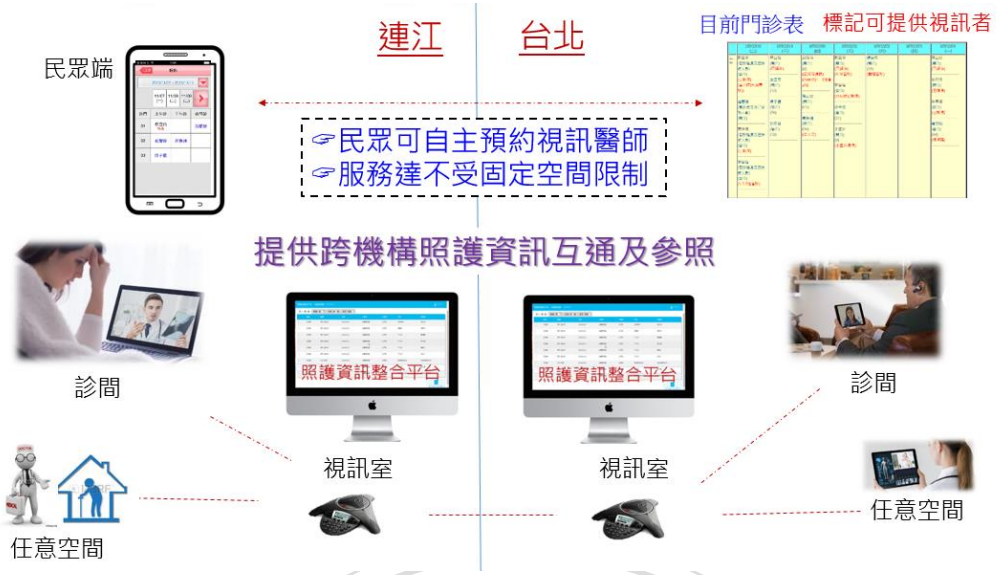


圖 二十三、共享醫療資訓與跨地區視訊看診示意圖

本研究團隊於 2019 年 5 月底期間於連江縣對居民進行系統使用與推廣，期間有對民眾意見進行調查，調查結果如圖二十四所示，結果顯示民眾對於本系統之整體評價為 88.79 分，顯示本系統可以切入到現有醫療照護系統之痛點，成功統合各機構之資源。同時在推廣期間有對連江縣民眾做意見調查，回饋意見如圖二十五所示，其中不少民眾表示希望能夠增加或開放更多的醫療機構與院所進入到本系統，未來會朝這方向努力，達到促進醫療效率與品質的目的。



DOI:10.6814/NCCU201901178

# 民眾意見調查

| | |
|---|---|
| **第一部分：照護資訊授權 APP 有用性** | |
| 4.26 | 1. 照護資訊授權 APP 可以完整呈現需要授權的照護資料 |
| 4.27 | 2. 我覺得照護資訊授權 APP 有助於照護人員瞭解我的照護需求 |
| 4.08 | 3. 我覺得照護資訊授權 APP 在資料的交換與傳送是安全的 |
| **第二部分：照護資訊授權 APP 易用性** | |
| 3.98 | 4. 我覺得照護資訊授權 APP 的操作相當容易 |
| 4.07 | 5. 我覺得照護資訊授權 APP 的畫面設計清楚 |
| 4.12 | 6. 我覺得透過照護資訊授權 APP，能隨時進行個人的資料授權 |
| **第三部分：使用 APP 態度** | |
| 2.14 | 7.* 我使用照護資訊授權 APP 的經驗 *註：數字2.14意為使用照護APP的週平均次數 |
| 4.02 | 8. 我未來會願意繼續使用照護資訊授權 APP |
| 4.07 | 9. 我會樂於推薦照護資訊授權 APP 給親朋好友使用 |
| **第四部分：滿意度** | |
| 4.12 | 10.我滿意照護資訊授權 APP 所提供的授權功能 |
| 4.18 | 11.我滿意使用照護資訊授權 APP 可提升照護人員對我的照護需求的瞭解 |
| 4.07 | 12.我滿意照護資訊授權 APP 的資料傳輸速度 |
| **整體評價** | |
| 88.79 | 13.您對照護資訊整合平台整體評價___分(請以 0 至 100 分評分 ) |

圖 二十四、民眾意見調查表

| | |
|---|---|
| 新資訊很受教(受用) | 綜效 |
| 做得很好 | 綜效 |
| 對於個資安全還是有疑慮 | 個資 |
| 下次能帶一點健康資訊 | 內容 |
| 希望未來新增更多醫療機構 | 介接 |
| 多開放一些療院所 | 介接 |
| 台大榮總的連結 | 介接 |
| 介面可以更美化 | 介面 |
| 1.字太小。老花不容易辨識。2.白色底，自顏色淺，不易閱讀。 | 介面 |

圖 二十五、連江縣民眾意見回饋整理



DOI:10.6814/NCCU201901178

# 第五章　結論

本研究設計並開發了一個整合照護資料共享的授權平台，此平台的主要特色有(1)資料分散儲存於參與機構的內部，沿用既有的資料管理設施，降低整體建置成本；(2)集中管理使用者與各機構的資料索引，安全與效能有保障；(3)基於區塊鏈技術的使用者資料分享授權系統，提供醫療機構防竄改與自動分享的數位授權紀錄； (4)具分類與階層化的照護資訊，提供基於角色的細粒度資料分享控管；(5) 透過閘道器(Gateway Server)介接使用者，區塊鏈與既有資料管理設施，降低擴增參與機構數量的單位成本；(6)開發使用者授權 App，提供以區塊鏈交易為依據的自主授權與查詢功能，確保授權紀錄之真實性與防竄改；(7)設立「身份見證人」的機制來實現帳號實質審查，並利用數位憑證綁定手機達到擁有第三方登入的效果且具身份識別唯一性，卻又不需要犧牲掉個人隱私；(8)利用智能合約實現自動化授權之架構。目標為實現新型態的區塊鏈身份辨識服務。

初版之照護資訊授權 APP 平台以及用於審查使用者註冊與申請新憑證之身份見證人系統 APP 已於 2019 年 4 月實作完成，使用者可順利於本平台進行註冊、授權醫療資訊、申請新憑證、維護親屬關係、代理他人註冊與授權之功能，並可將註冊資訊與授權資訊上架至區塊鏈上，同時系統會將查詢歷史紀錄儲存於區塊鏈中，方便日後查詢非法調閱。

本平台歷經近一年的開發，已經順利上線，並於 2019 年 5 月以連江縣民眾為先期對象，進行實際場域之測試與驗證。雖然實施期間不長，但已經陸續開始發揮作用，得以透過民眾授權，提供照護人員更完備的照護紀錄，進而提升醫療與照護品質，達到增進人民福祉的目的。

# 第六章　未來工作

未來工作會基於密碼學技術對「授權」本身進行加密，目的是想要透過一種加密演算法達到保證授權內容保密的情況下，資料擁有者可以即時的進行重新加密處理並分享給資料接收者，在此過程中明文不會被洩漏。代理重加密(Proxy re-encryption)即為一種可將密文做轉換的演算法，PRE 可透過特定的重加密密鑰將可解開密文的對象由 A 轉換成 B，且重加密過程可由任意的三方執行，在此過程中文件明文不會被洩漏。同時區塊鏈可作為共享與維護金鑰之管理系統，避免單點被攻擊則全系統淪陷的風險，並藉由區塊鏈不可竄改的特性維護金鑰的正確性並利用智能合約實現自動化管理。

PRE 概念流程圖如圖二十六所示，PRE 技術可實現更為方便且隱密的資料共享，假設資料擁有者為 Alice，資料接收方為 Bob，Bob 想要在 Alice 允許的情況下獲取她的某些資料，但 Alice 不想直接用 Bob 的公鑰進行加密，避免 Bob 此後可以保留對資料的擁有訪問權限，在此情況下藉由代理重加密技術將可解開密文的對象由 Alice 轉化為 Bob，讓 Bob 可以直接用自己的私鑰對密文做解密，其中重加密過程可由任意第三方進行，在此過程中資料的明文不會被洩漏，基本之



DOI:10.6814/NCCU201901178

PRE 主要步驟流程如下 ：

1. Alice 用自己的公鑰 pKa 加密訊息 m（加密後的訊息稱為 Ca）
2. Alice 用自己的私鑰 sKa 與 Bob 的公鑰 pKb 產生 re-encryption 用的金鑰『rKa->b』
3. Alice 把 re-encryption key 『rKa->b』跟 加密後的訊息 Ca 交給 Proxy，讓 Proxy 用 re-encryption key『rKa->b』 再加密 Ca（再加密後的訊息稱為 Cb）
4. BoB 收到 Cb 後，使用自己的私鑰 sKb 直接將 Cb 解回訊息 m

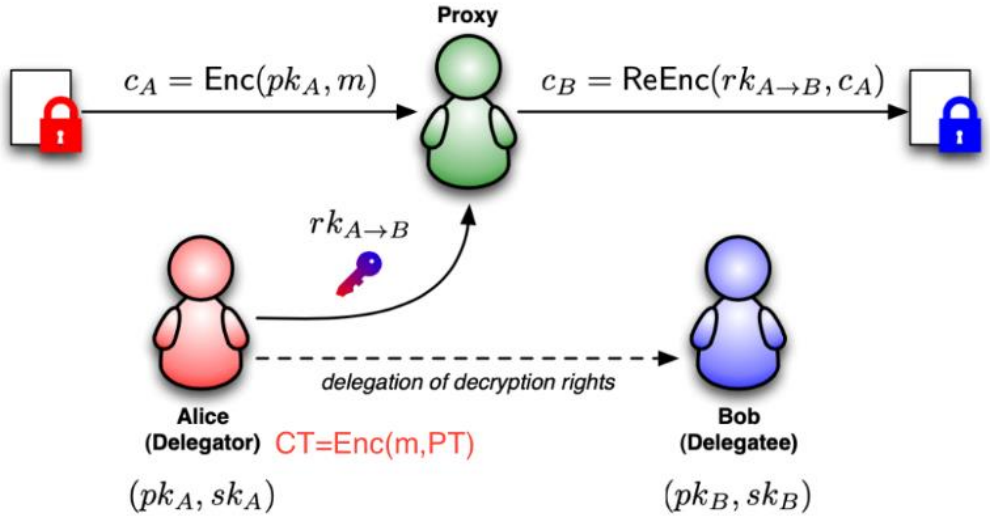


圖 二十六、Proxy re-encryption(PRE)概念流程圖

接著可針對 PRE 對加密共享資料之 Symmetric Key 一併導入區塊鏈做應用，假設今天 Alice 欲共享資料(例如 X 光照片)給 Bob，Alice 首先將欲對外共享的個人資料用 Symmetric Key 加密後將其儲存到區塊鏈上，同時使用公鑰將該 Symmetric Key 加密後也儲存到區塊鏈上，之後 Bob 去索要資料時，Alice 可以根據自己的私鑰與 Bob 的公鑰產生一重加密金鑰並發送給 Proxy，Proxy 即可根據重加密金鑰將已加密之 Symmetric Key 經由 PRE 轉換，然後 Bob 可以到區塊鏈上下載加密資料與重加密密鑰，並可用 Bob 自己的私鑰解密出相同的 Symmetric Key，最後用該 Symmetric Key 去將從區塊鏈上下載下來的資料做解密。上述之詳細流程如下 ：

1. Alice 用自己的私鑰 sKa 與 Bob 的公鑰 pKb 產生 re-encryption 用的金鑰『rKa->b』。
2. Alice 用『 Symmetric key』『m』加密訊息『PT』，加密後的訊息稱為『CT』，Alice 把加密後的訊息『CT』放到區塊鏈或 IPFS。
3. Alice 用自己的公鑰 pKa 加密 Symmetric key 『m』，加密後的 Symmetric key 稱為『Ca』。
4. Alice 把 re-encryption key 『rKa->b』跟 加密後 Symmetric key 『Ca』 交



DOI:10.6814/NCCU201901178

給 Proxy。

5. Proxy 用這把 re-encryption key『 rKa->b』 再加密 『Ca』，再加密後的 Symmetric key 稱為 『Cb』。
6. Bob 收到 再加密的 Symmetric key 『Cb』後，使用自己的私鑰 sKb 直接將 『Cb』 解回原始 Symmetric key『 m』。
7. Bob 用 Symmetric key『m』將 加密後的訊息『CT』解回『PT』。

未來將探討 PRE 導入本系統之授權機制的可行性，以實現更安全、更具隱私性的整合授權系統。

# 第七章　參考文獻


[1] 衛生福利部，民 102，「全民健康保險山地離島地區醫療給付效益提昇計畫」，(取得日期：2019 年 8 月 15 日)，[available at http://www.nhi.gov.tw/Resource/webdata/16991_2_1020001831-IDS 修正條文-公告版.pdf]

[2] 許明暉，民 104，「全國電子病歷交換系統簡介」，*政府機關資訊通報*，第 327 期

[3] Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman. 2016 .MedRec: Using Blockchain for Medical Data Access and Permission Management. *2nd International Conference on Open and Big Data*

[4] Gavin Wood. 2014. ETHEREUM: A secure decentralised generalised transaction ledger

[5] Chunmiao Li, Yang Cao, Zhenjiang Hu and Masatoshi Yoshikawa. 2019. Blockchain-based Bidirectional Updates on Fine-grained Medical Data

[6] Peng Zhang, JulesWhite, Douglas C. Schmidt, Gunther Lenz and S. Trent Rosenbloom. 2018. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational and Structural Biotechnology Journal 16* 267–278

[7] Fabian Vogelsteller, Marek Kotewicz, Jeffrey Wilcke and Marian Oance. 2019. web3.js Documentation




DOI:10.6814/NCCU201901178