Regular Paper

Communications of the CCISA
Vol. 27 No. 4 Nov. 2021

一個安全的行動通訊區塊鏈 SIM 架構

李佳璇[1] 陳麒元[3]
國立宜蘭大學資訊工程學系[1, 3]
[1]tyuor596g82@gmail.com、[3]chiyuan.chen@ieee.org

摘要

隨著科技的推移與進步，人們對資訊安全日益看重，在這通訊發達與駭客猖獗的時代，傳統 SIM 卡與 eSIM 的集中式儲存方式、資料存放的問題與傳輸的方法，皆帶來了安全性的隱憂，以及隱私性問題。為此，本研究提出了一種區塊鏈為基礎的 SIM 架構，以區塊鏈作為分散式帳本，透過與智能合約的結合，利用去中心化與不可竄改的等特性，將改變過去集中式儲存所帶來的安全性問題，同時也確保了資料的完整性，其次通過二次加密的方式，也使得隱私性問題獲得了改善，最後我們也介紹了如何使用我們所提出的架構來實現 SIM 的主要功能。

關鍵詞：SIM、區塊鏈、智能合約、隱私性

Regular Paper

Communications of the CCISA
Vol. 27 No. 4 Nov. 2021

A Secure Blockchain-SIM Architecture for Mobile Communications

Jia-Xsuan Lee[1], Chi-Yuan Chen[2]
[1, 2]Dept. Computer Science and Information Engineering, National Ilan University
[1]tyuor596g82@gmail.com, [2]chiyuan.chen@ieee.org

Abstract

With the progress and advancement of technology, people pay more attention to information security. In the age of advanced communications and rampant hackers, the centralized storage of traditional SIM cards and eSIMs, the data storage and transmission all bring security concerns and privacy issues. Therefore, the study proposes a block-chain-based SIM architecture, which uses the block-chain as a distributed ledger through the combination with smart contracts, and the use of decentralized and non-manipulative features will change the security problems caused by centralized storage in the past. In our approach, the problem has also been improved to ensure the integrity of the data as well. Finally, we also introduced how to use our proposed architecture to implement the main functions of SIM.

Keywords: SIM, Blockchain, Smart Contract, Privacy

壹、前言

現今通訊網路幾乎成為每個人必備的需求，第一代行動通訊技術，簡稱 1G (the first generation) 到現在的第五代行動通訊技術，簡稱 5G (5th generation mobile networks)，已經有了突破性的改變與成長。其中用戶識別模組 (Subscriber Identity Module)，通常簡稱為 SIM 卡，SIM 卡的發展可以追朔至 1991 年，德國 Giesecke & Devrient GmbH 開發了世界上第一張 SIM 卡，並賣了 300 張給芬蘭無線網路運營商 Radiolinja。隔年，他們售出了第一隻附有 SIM 卡的全球行動通訊系統 GSM 手機。該晶片儲存了行動電話用戶的信息、加密的密鑰以及用戶的電話簿等內容，可供營運商根據前述資訊對 GSM 用戶進行身份鑑別，並對用戶通話時的語音信息進行加密。

隨著全球通訊終端市場趨於飽和，傳統 SIM 卡由於其使用壽命短、操作環境要求苛刻，且必須有卡槽以及只能綁定單一運營商等特點，使得業務擴張遇到瓶頸；為了解決前述的問題，人們想出將其 SIM 卡直接嵌入電路板以解決困境，而這也就成為現今的嵌入式 SIM 卡 (Embedded-SIM, eSIM) [19]；電訊標準組織 (GSM 協會，GSMA)，於 2016 年發佈 eSIM 遠端配置管理架構和規範並持續更新，此規範獲得全球多數營運商、晶片商的支持，包含蘋果、三星、Google 等手機製造商。eSIM 主要優勢在於用戶可以隨時更換運營商，可對 SIM 進行遠程配置，實現運營商配置文件的下載、安裝、啟用、停用及刪除等功能，遠程管理平台可以對 eSIM 進行生命周期管理，有效縮短產業周期，滿足用戶多樣化選擇。

隨著科技發展網路安全性更顯著重要，現今個人資料保護日益受到重視，SIM 卡以及 eSIM 皆為我們的生活帶來了便利性，但集中式管理也帶來了隱私性問題，同時也暴露了安全性問題。2019 年 9 月，行動網路資安業者 AdaptiveMobile Security 近日揭露了存在於手機簡訊與 SIM 卡上的安全漏洞，名為 Simjacker [9]，這隻攻擊程式不同於過去透過簡訊傳送的惡意程式，使用者得進一步開啟連結才能觸發攻擊，而是直接透過簡訊發送惡意程式，以入侵目標對象手機的 SIM 卡，進而執行惡意命令；同年同月，另一家安全公司 Ginno Security Labs 亦發現類似的攻擊手法，名為 WIBattack [10]，主要是電信公司為提供用戶更多進階的簡訊服務，於 SIM 卡上運行採用 Wireless Internet Browser (WIB)技術，並透過電信公司採用 OTA 形式進行相關服務選單的更新，駭客可傳送惡意簡訊開採 WIB SIM 瀏覽器的漏洞，取得受害手機的遠端控制權，執行各種惡意行為。

除了安全性與隱私性，表 1 我們也整理出我們所觀察到的相關問題，為了解決這些困境，因此我們提出了區塊鏈為基礎的 SIM 架構，利用區塊鏈去中心化特性，來解決集中式管理所帶來的問題，同時由於每筆交易都須經過驗證，因此我們也可以辨識發訊者的真實性，以避免收到惡意訊息等相關問題，但是區塊鏈所有交易都是公開透明，所以我們將所需隱匿的資料進行加密，藉由智能合約 (Smart Contract) 來執行應用程式以及處理交易。

表 1：傳統 SIM 卡與 eSIM 之比較

	傳統 SIM	eSIM
實體空間	實體卡，有卡槽	無實體卡，無卡槽
儲存問題	發生遺失或損壞時，SIM 卡所儲存內容無法復得	無須擔心卡片損壞導致儲存內容遺失
驗證性	一般用戶**無法辨識**來電或來訊號碼的**真實性**	一般用戶**無法辨識**來電或來訊號碼的**真實性**
保密性	SIM Cloning 可複製 SIM 卡資料	容易被攔截 OTA 來竊取資訊
便利性	新舊客戶皆需至實體門市辦理	新舊客戶皆需至實體門市或網路辦理

在本文的第一小節，我們介紹目前 SIM 卡與 eSIM 的現況，也描述了研究動機與解決方案。第二小節將介紹有關通訊的發展與應用。第三小節則介紹我們提出來的 SIM 架構與功能應用。最後，第四小節針對本研究進行總結。

貳、背景及相關研究

2.1 傳統 SIM 卡

傳統 SIM 卡是由 CPU、ROM、RAM、EEPROM 和 I/O 電路組成的微處理器的晶片卡[16]，不宜在高於 80℃或低於－20℃的環境下工作，且卡片受到折損也可能會導致資料錯亂或喪失。該卡是以 GSM 作為行動電話通訊的基礎，一卡一營運商的模式，根據規範來執行或者拒絕指令；隨著手機越輕薄，SIM 卡面積也隨之縮減，從最初的 1FF 原卡到現在最盛行的 4FF 標準的 Nano-SIM 卡，為手機擁擠的內部讓出不少空間。SIM 卡儲存的資料主要分為以下四類：

- 固定存放的資料
- 暫時存放的有關網路的資料
- 相關的業務代碼
- 用戶自己存入的資料

第一類-固定存放的資料，由 SIM 卡製造商寫入，主要包括國際行動用戶辨識碼 (IMSI)、IMSI 認證演算法、鑒權密鑰 (Ki) 與 Ki 加密演算法等等；第二類-暫時存放的有關網路的數據，如位置區域識別碼 (LAI)、臨時行動簽約用戶標識 (TMSI) 等；第三類-相關的業務代碼，如個人識別碼 (PIN)、解鎖碼 (PUK)、計費費率等；第四類-電話簿、簡訊等，是手機用戶自行輸入的電話號碼，或是收發的簡訊等用戶相關資料。

在文獻[14]提到，對 GSM 用戶進行身份鑒權，透過使用質詢-響應機制的用戶身份

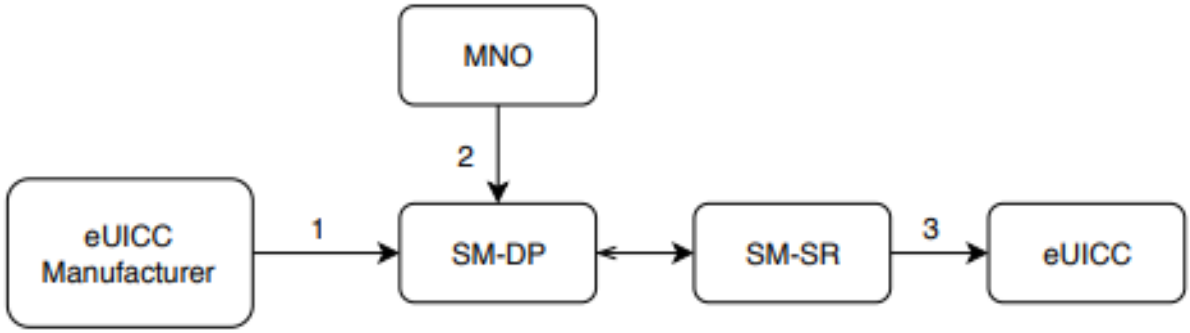
進行認證，會產生一個 128bit 的隨機數 RAND，發送至 SIM 卡接收端，根據 SIM 卡中的密鑰 Ki 和個人用戶的認證密鑰的認證演算法(A3)，對接收到的 RAND 計算出 32bit 有簽名的響應(SRES)，並將結果發回網路端；而網路端在鑒權中心查明該用戶的密鑰 Ki，用同樣的 RAND 和演算法 A3 計算出 SRES，並與收到的 SRES 進行比較，如果兩者 SRES 一致，則鑒權通過，判斷該用戶為合法使用者，若兩者相異，反之。每張 SIM 卡都會設置一個 PIN 碼，只有當用戶輸入正確的密碼後，手機才能進入正常使用狀態，若連續三次 PIN 碼都輸入錯誤，手機便會將 SIM 卡鎖住，要解鎖，就必須使用 PUK 碼來解鎖。

2.2 eSIM

eSIM 嚴格來說並不是真正的虛擬 SIM 卡，而是將 SIM 卡直接嵌入到行動設備上而無需卡槽，進而大幅縮減手機的使用空間，加上嵌入至電路板以後，將不再受限於環境，可達到耐氧化、耐高溫等相關需求，eSIM 是基於 OTA (Over-the-Air Technology) 即空中下載技術[19]，透過電信網路 (GSM 或 CDMA) 的空中接口對 SIM 卡數據及應用進行遠程管理的技術，下載的方式分 3 種：簡訊/瀏覽器/PUSH 方式，空中接口可以採用 WAP、GPRS、CDMA1X 以及廣為普及的短訊 (SMS) 技術，因此用戶便可以靈活切換運營商，做到換號不換卡的多重運用。

eSIM 的基本結構如圖 1 所示[3][4]，其中 eUICC 為嵌入式通用積體電路卡 (UICC)，即 E-SIM，Mobile Network Operator (MNO) 是行動網路營運商，而 Subscription Manager - Data Preparation (SM-DP) 則是負責儲存、管理電信設定檔，最後 Subscription Manager Data – Preparation (SM-SR) 配置、管理 eSIM 晶片的資訊，SM-DP 可與其他 SM-SR 實現資料切換。其運作流程如下：

1. SM-DP 從 EUM 獲取 eUICC 所需的工具以及服務
2. MNO 也會提供相關資料給 SM-DP，例如 OTA 傳輸方式
3. 隨後 SM-SR 再透過 OTA(Over The Air)技術與 eUICC 通訊



- eUICC：嵌入式的用戶識別模組(SIM)及機器辨識模組(MIM)
- SM-DP：Subscription Manager – Data Preparation
- MNO：Mobile network operator
- SM-SR：Subscription Manager –Secure Routing

圖 1：eSIM 的基本結構

2.3 區塊鏈

區塊鏈的架構與想法最早可以追溯回 1991 年，由 Haber、Stuart 和 W. Scott Stornetta 所發表的論文[5]，他們提出一個利用電腦運算為數位文件切實地標記時間，來達到資料不能被追溯或篡改的解決方案；而真正讓此技術受到注目的契機，是一個名為中本聰 (Satoshi Nakamoto) 於 2008 年在網路上發布了一份名為”Bitcoin: A peer-to-peer electronic cash system”的文章[12]，透過文章，可以知道區塊鏈具有以下幾點特性：

- 去中心化
- 安全性
- 每筆交易皆為公開
- 不可被竄改
- 每個節點的帳本內容都一樣

簡單來說，區塊鏈就是個建立在 P2P (Peer to Peer) 網路架構的分散式帳本系統，每一個區塊包含了前一個區塊的加密雜湊函數值、相應時間戳記以及交易資料，其中雜湊函數擁有不容易找到相同函數值，這樣的設計使得區塊內容具有難以篡改的特性；為了強調區塊鏈的共享性，所以每個節點都擁有一本帳本，記載了大家的交易紀錄，由於每個人帳本內容都要一致，因此可以不必依賴中間的信賴機構來替雙方對帳，進而達到去中心化；又因為前述所說幾個特性，若攻擊者偽裝自己是區塊鏈上的某一個節點，企圖利用此散播惡意程式或是攻擊，在區塊鏈上，每個節點都需要經過驗證，不管是要竄改資料或是成為惡意節點，至少要得到超過 51%節點的認可，所以攻擊者想藉此破壞區塊鏈，是很難達到的，因此區塊鏈對資料的儲存相對安全。

2.4 智能合約

智能合約 Smart Contract 這個概念第一次出現是在 1994 年，由 Nick Szabo 提出來的[13]，所謂的合約就是雙方皆同意的一套規則，為了闡釋智能合約的概念，他舉了自動販賣機當例子，當我們把硬幣投入自動販賣機後，當我們給足夠金額，自動販賣機便會給我們所選的商品，廠商將規則(買賣合約)制定好並放入自動販賣機中，而負責實現這份合約的就是自動販賣機，但自動販賣機也有可能遭受駭客入侵，或是廠商惡意竄改合約規則，只收錢而不給商品，因此智能合約主要設計的目的在於確保合約的執行，且避免惡意行為以及有不可預見的情況，最大程度地減少對受信任第三方的依賴，從而降低交易成本。

隨著區塊鏈的出現[1][2][7][19][8]，將可避免諸如此類的事情發生，當智能合約部署在區塊鏈後，就無法被修改，這避免了合約被竄改的風險，且每筆交易在區塊鏈上都是公開的，所以合約參與者都可以審查合約代碼是否有問題，且佈署於區塊鏈上的智能合約，便無人可以阻止，可以有效執行。

參、區塊鏈 SIM 架構概述

在本小節中，我們將介紹區塊鏈 SIM 架構，解釋如何讓 SIM 的相關功能在區塊鏈中實現，並利用此架構解決前述所說之困境，使得通訊更具安全性。依據文獻[4] [16][17]，不管是傳統 SIM 卡還是 eSIM 都具有三個主要功能：

- SIM 卡中存有自己的保密演算法及密鑰
- 用戶身份鑒權
- 儲存用戶相關資料

而後我們也會敘述如何將我們所設計的架構，利用區塊鏈特性，與此三個主要功能對應。本文第一及第二小節，提及 SIM 卡與 eSIM 所面臨的問題，傳統 SIM 卡必須具有卡槽，且一卡代表一電信業者，雖說這部分在 eSIM 得到了解決方案，且比傳統 SIM 卡更具安全性，但是 eSIM 的傳輸方式也帶來另一安全性隱憂，因此我們提出區塊鏈式的 SIM 來解決相關問題，我們將沿用 eSIM 無卡槽的概念，透過區塊鏈註冊方式來配置我們的區塊鏈 SIM，考量到隱私性問題，針對行動用戶，我們將讓使用者自行選擇資料是否加密或者公開，由於區塊鏈不可竄改特性，最後再把資料存放於區塊鏈之中，確保安全性，如圖 2。

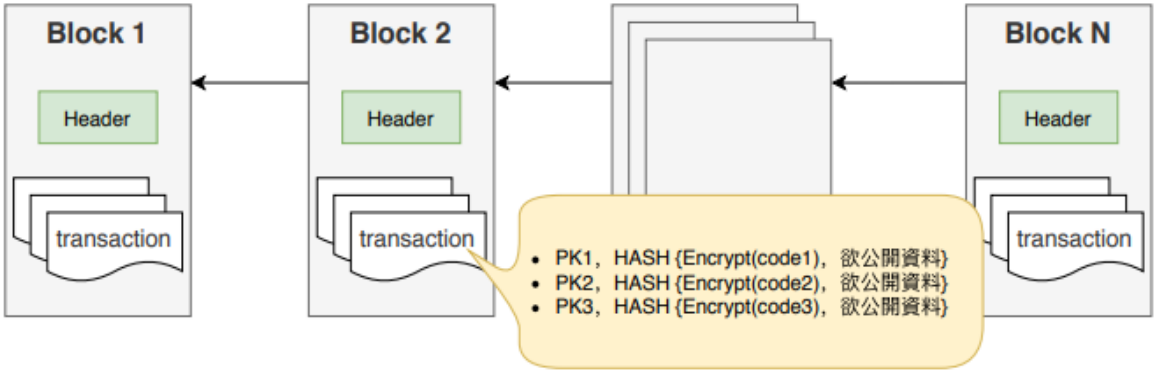


圖 2：區塊鏈 SIM 區塊圖

3.1 區塊鏈 SIM 架構

在我們所提議的區塊鏈架構中，如圖 3，電信業者或是營運商 (Telecom) 會佈署一份智能合約，將其註冊流程、驗證方法與通訊方案等相關規則撰寫於其中，使用者將根據其功能需求，對智能合約發起交易，當交易被判定為合法時才會被廣播於區塊鏈網路中。而圖 4 我們展示了幾個主要子組件：

- User Client：使用者節點
- Smart Contract：智能合約，將依使用者其需求進行處裡
- Worker Client：驗證其發出的交易 (Tran.) 的節點
- Blockchain Network：區塊鏈網路

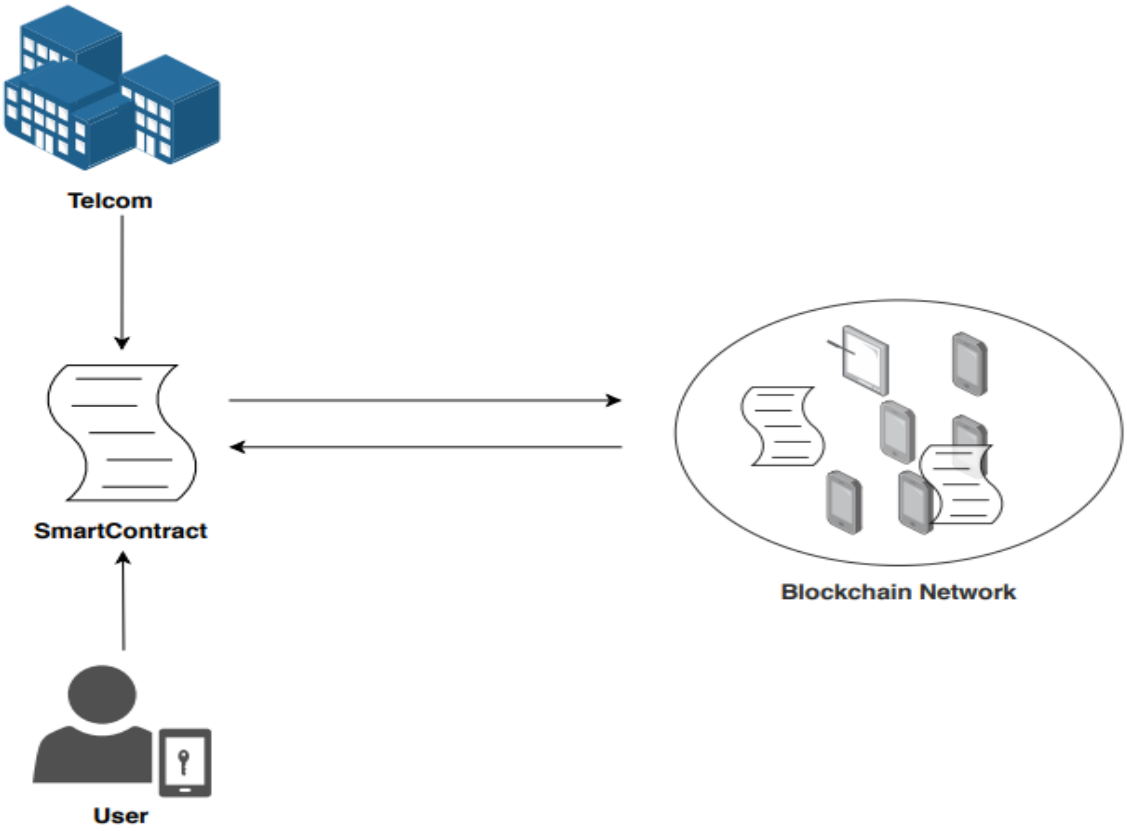


圖 3：區塊鏈 SIM 概觀

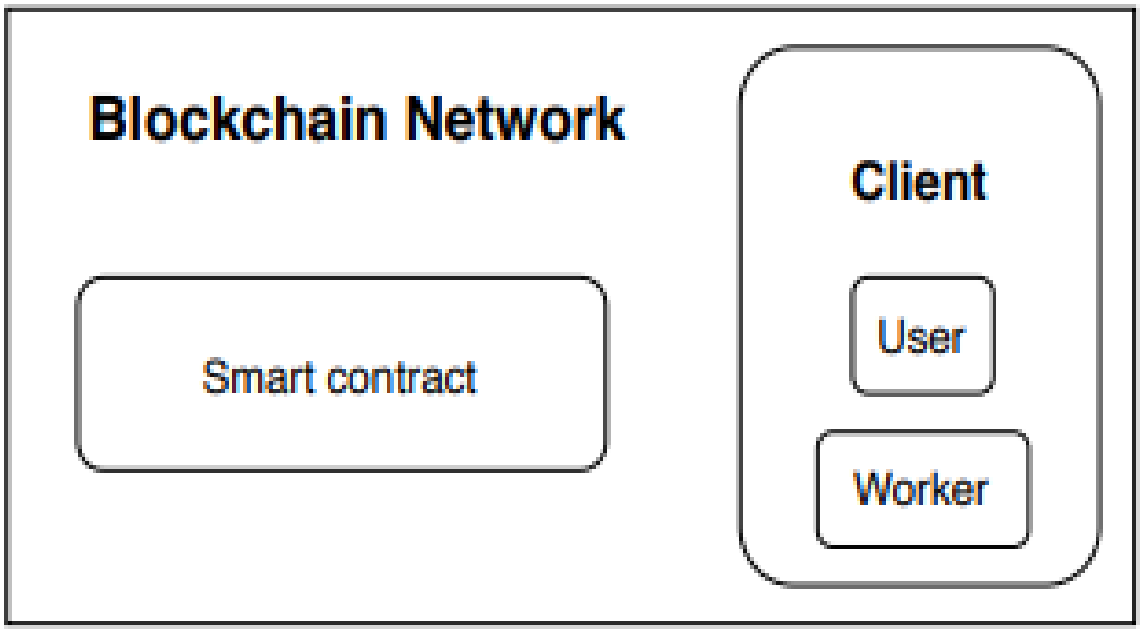


圖 4：區塊鏈 SIM 基本架構

3.2 功能

首先我們將介紹加密的方法，作為 SIM 卡中保有自己的保密演算法及密鑰的對應，其次解釋用戶身份鑒權的功能如何在此架構中實現，最後再敘述我們如何儲存用戶的相關數據。

3.2.1 加密算法及密鑰

使用者申請或是註冊區塊鏈 SIM 的程式 Program，以下簡稱 P，用來取代 eSIM 透過 OTA 傳輸的配置文件，在 P 中我們把產生區塊鏈 SIM 的所需配置的資料放在其中，例如電信業者資料、IMSI、公開金鑰密碼系統、雜湊加密法等相關演算法與數據。

公開金鑰密碼系統又稱為非對稱式 RSA 加密演算法，於 1978 年美國麻省理工學院三位教授 Rivest、Shamir 及 Adleman (RSA) 所提出，會產生一對金鑰，在區塊鏈中，所有節點都保有一對金鑰，其中公開金鑰 (Public Key，PK) 可被廣為流傳，而私密金鑰 (Private key) 必須妥善保存，RSA 加密演算法，使用對方的公開金鑰 (Public Key) 將明文加密，而 RSA 解密演算法，則是必須使用自己的私密金鑰 (Private Key) 才能將密文解出。為使資料更具安全性，我們採用了 SHA (Security Hash Algorithm) 雜湊函式，利用雜湊函數特性，將信息加以雜湊成為一串固定的字串，最後再把其自字串以私密金鑰加密，所得內容即為該信息的數位簽章，可作為自己證明是信息的來源，若原始內容相同則結果相同，反之，加上此函數無法透過結果反推原始資料，因此透過公私鑰與雜湊函數的方法，可用於信息加密解密以及驗證身分[5]。

3.2.2 用戶身份鑒權

我們取代了傳統 SIM 卡與 eSIM 的用戶身分鑒權方式，利用區塊鏈特性，當使用者發起交易時，皆需要對身分做驗證才可使得交易完成，我們以用戶申請區塊鏈 SIM 的流程作為範例介紹，如圖 5，步驟如下：

1. 使用者註冊時，將會輸入一組專屬自己的密碼，然後對 Smart Contract 發出請求交易。
2. Smart Contract 接收到以後，根據請求信息會回傳程式 P 參數。
3. 程式 P 執行以後會為使用者產生一區塊鏈 SIM 與一組唯一密鑰對，然後對 Smart Contract 發起註冊交易。
4. 運用區塊鏈特性，Worker 驗證交易。
5. 驗證成功後，便將資料佈署於區塊鏈，並廣播出去。

其中步驟 2 的程式 P 參數，裡面包含了電信業者資料、IMSI 生成法與公私鑰等產生區塊鏈 SIM 的相關資料，而步驟 3 程式 P 則必需透過使用者解密才可以啟動，隨後

便將產生的資訊，其 $<ID_U, Address_U, Pk_U, SIM_U, Other_U>$傳送給 Smart Contract 做後續處理。

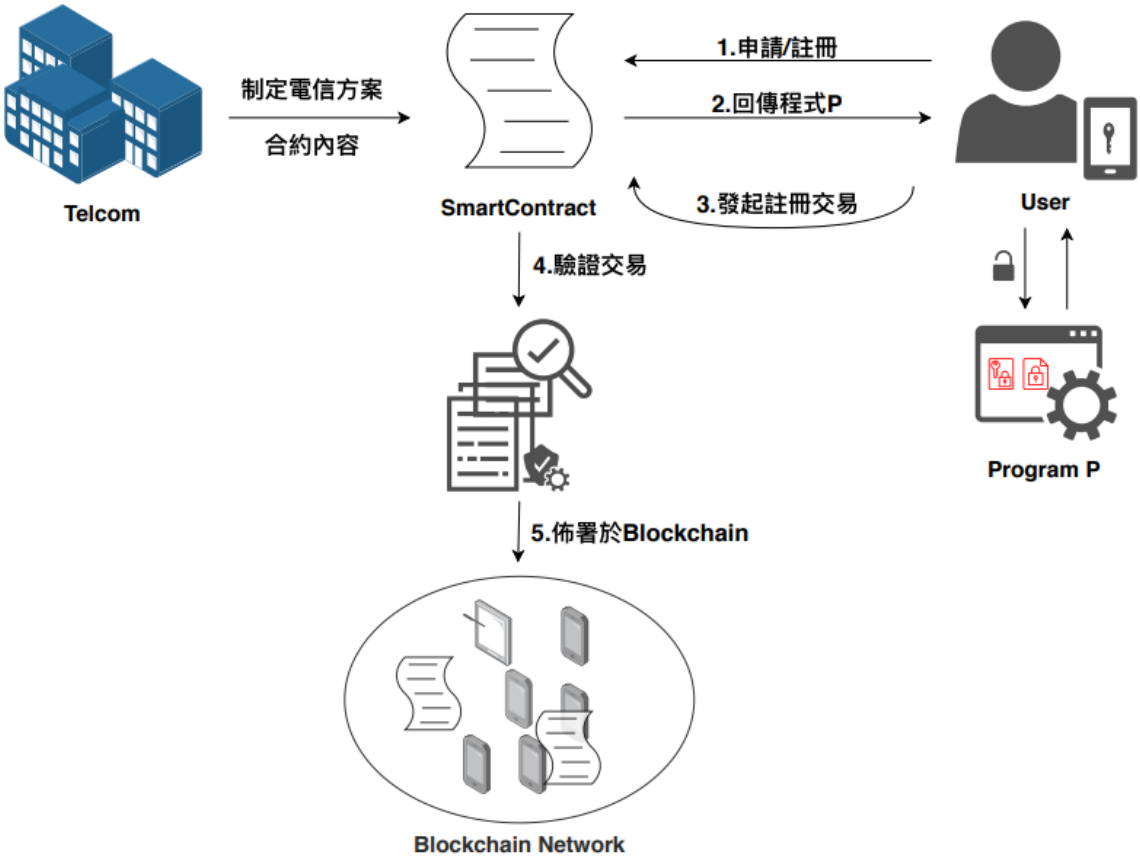


圖 5：區塊鏈 SIM 申請/註冊流程

3.2.3 儲存用戶的相關資料

在用戶儲存資料方面，我們一樣保有傳統 SIM 卡與 eSIM 功能，將可以儲存電話簿、訊息等相關用戶自己的資料。下面我們以用戶儲存資料作為範例介紹，如圖 6，步驟如下：

1. 使用者將把欲隱匿的信息先行加密，並對此密文作數位簽名。
2. 對 Smart Contract 發起交易
3. 運用區塊鏈特性，Worker 驗證交易。
4. 驗證成功後，便將資料佈署於區塊鏈，並廣播出去。

其中步驟 1，使用者可以依據自己的需求，對欲隱匿的信息加密，是利用原有的密鑰操作，隨後再與其他數據一起傳送給 Smart Contract，經過 Hash，每筆交易都會有使用者的數位簽章，而步驟 3 再做驗證的時候，會根據使用者的公鑰來檢驗此信息的來源是否合法或屬實，若交易判斷為合法才會繼續往下進行，將資料寫入區塊鏈裡，且每個

區塊都含有上一個區塊的 Hash 值，使其竄改成本提高，當有一個區塊無法被驗證，交易的不真實性就會曝光，因此可以確保資料的完整性與一致性。

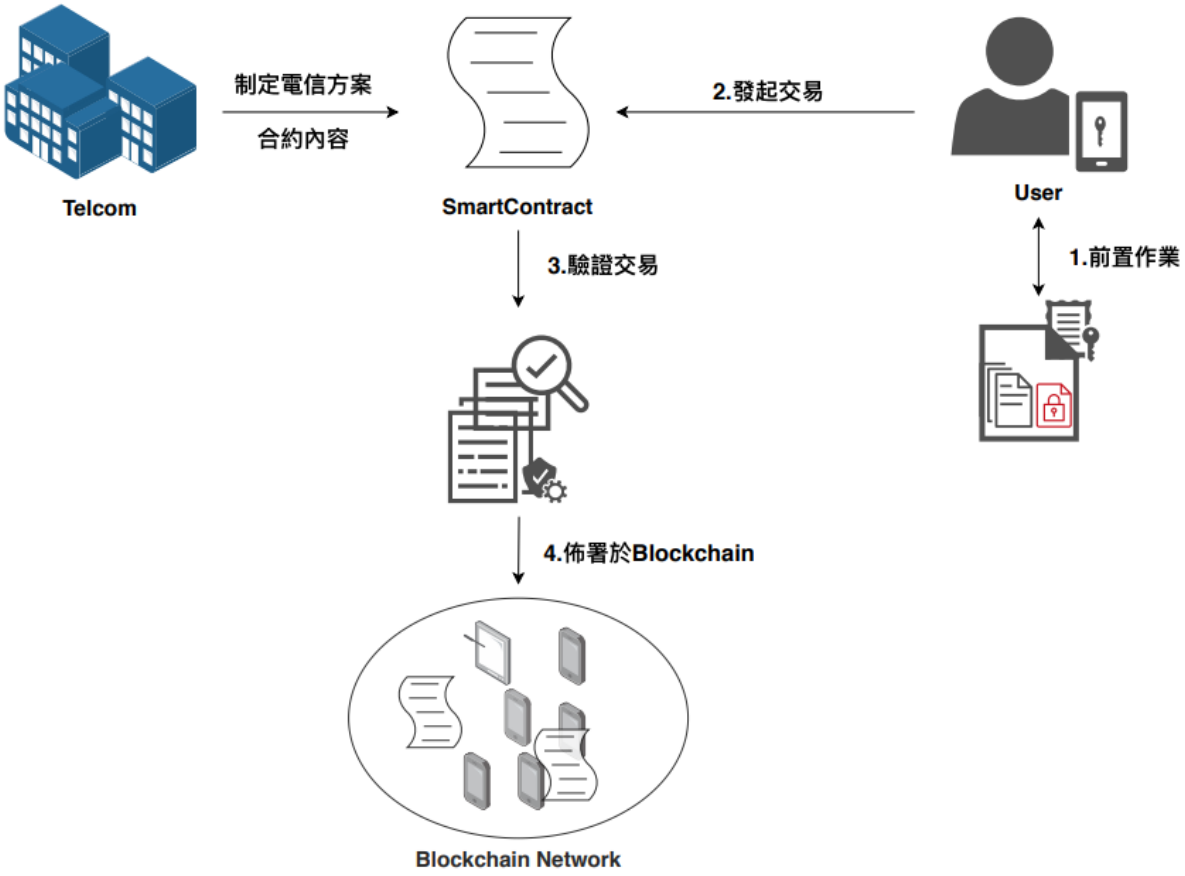


圖 6：區塊鏈 SIM 儲存流程

肆、結論

本研究提出了一種以區塊鏈技術為基礎的 SIM 架構，這個架構利用區塊鏈去中心化特性，解決了傳統 SIM 卡與 eSIM 集中式儲存的問題。透過線上區塊鏈註冊系統，每個節點都必須是合法的，因此可以過濾偽號碼，進而發起交易，然而每筆交易都需要經過驗證，當驗證通過後才可以將其資料佈署於區塊鏈中，且每筆交易內容，用戶可以根據自己的需求，加密欲隱匿的數據，唯有透過自己的私鑰解密才可看到其真正的資料，這將使得用戶在操作區塊鏈 SIM 上更具有安全性以及隱匿性。在區塊鏈中，所記載的交易紀錄是不可以隨意竄改的，不管是要竄改資料或是成為惡意節點，至少要得到超過 51%節點的認可，由於每個節點都擁有一本帳本，因此可以防止惡意攻擊的破壞，確保資料儲存的完整性。未來，我們將進一步透過實作的方式來驗證區塊鏈 SIM 架構的可行性。

[誌謝]

本研究由科計部計畫 MOST 110-2221-E-197-002 補助支持，特此誌謝。

參考文獻

[1] Ali Dorri, Marco Steger, Salil S. Kanhere and Raja Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy", IEEE Commun. Mag., vol. 55, no. 12, pp. 119-25, Dec. 2017.

[2] Byzantium Version, "Ethereum: a secure decentralised generalised transaction ledger", 2020, [online] Available: https://ethereum.github.- io /yellowpaper/paper.pdf.

[3] GSMA Embedded SIM Specification, [online] Available: https://www.gsma.com/esim/esim/esim -specification/.

[4] GSMA Embedded SIM Specification Remote SIM Provisioning for M2M, 2014, [online] Available: https://www.gsma.com/iot/wp-content-/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated.pdf.

[5] S. Haber and W. S. Stornetta, "How to time-stamp a digital document", J. Cryptol., vol. 3, pp. 99-111, 1991.

[6] [online] Available: https://github.com/ethereum-/wiki/wiki/Design-Rationale.

[7] [online] Available: https://ethereum.org/en/white- paper/.

[8] [online] Available: https://ithelp.ithome.com.tw/articles/10201781.

[9] [online] Available: https://ithome.com.tw/news/- 133042.

[10] [online] Available: https://www. ithome.com.tw -/news/ 133327.

[11] Mumin Cebe, Enes Erdin, Kemal Akkaya, Hidayet Aksu and Selcuk Uluagac, "Block4-Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles", IEEE Commun. Mag., vol. 56, no. 10, pp. 50-57, Oct. 2018.

[12] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, [online] Available: https://bit- coin.org/bitcoin.pdf.

[13] Nick Szabo, "Smart contracts: Building blocks for digital markets", EX-TROPY: The Journal of Transhumanist Thought, no. 16, 1996.

[14] Ozer Aydemir and Ali Aydin Selcuk, "A Strong User Authentication Protocol for GSM", 14th IEEE International Workshop on Enabling Technologies Infrastructure for Collaborative Enterprise (WETICE'05) Linkopings University Sweden, 2005.

[15] Rui Yuan, Yu-Bin Xia, Hai-Bo Chen, Bin-Yu Zang and Jan Xie, "ShadowEth: Private Smart Contract on Public Blockchain", Journal of Computer Science and Technology,

vol. 33, no. 3, pp. 542-556, 2018.

[16] Sheng He, "SIM Card Security" in Seminar Work, Temmuz:Ruhr-University of Bochum, 2007.

[17] Vesselkov A, H?mm?inen H, Ik?l?inen P, "Value networks of embedded SIM-based remote subscription management", Conf. of Telecommunication, Media and Internet Techno-Economics (CTTE), 2015.

[18] Yongle Chen, Xiaojian Wang, Yuli Yang and Hong Li, "Location-Aware Wi-Fi Authentication Scheme Using Smart Contract", Sensors (Basel), vol. 20, no. 4, Feb. 2020.

[19] Yuanyu Zhang, Shoji Kasahara, Yulong Shen, Xiaohong Jiang and Jianxiong Wan, "Smart Contract-Based Access Control for the Internet of Things", IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594-1605, Apr. 2019.

[20] [online] Available: http://www.twcloud.org.tw/-files/file_pool/1/0j123554536798487144/台灣雲協-物聯網 eSIM 技術與應用白皮書.pdf.