

運用區塊鏈加密機制建立符合 FHIR 格式之個人健康資料 管理平台(大學專題)

朱家佑、趙浚宏、吳家佑、吳勛嘉、吳仁鈞

指導教授:徐建業教授

摘要

本研究使用區塊鏈技術來保護資料的安全及隱私性，並以區塊鏈有不可竄改、公開透明、去中心化的特性，來進行驗證與實做個人健康管理 APP。而在資料選擇及格式上，我們選擇健康存摺資料，將原本 XML 格式轉換成符合國際標準的 FHIR 格式進行編碼，因為 FHIR 格式的個人資料可以在不同醫療單位進行交換，像是個人健康檢查、診所看病、醫院住院等相關資料，都可以整合在一起儲存並做使用，達成互操作性。在實作上，我們建立了個人健康紀錄管理的應用程式，並且整合健康存摺系統，達到方便、個人化的可使用性。

第壹章、緒論

第一節 研究背景

衛生福利部(2023)110 年我國有

18 萬 4,172 人死亡，其中以惡性腫瘤（癌症）5 萬 1,656 人居首位，其次為心臟疾病及肺炎，前十大主要死因合占 76.6%，仍以慢性疾病為主。

但是其實多數慢性疾病的發生及惡化，可透過有效的健康管理，成功地阻斷、延緩、甚至逆轉，達到不只是消極的「預防疾病」，更可以是積極的「健康促進」(永越健康管理中心，2021)。而人們要能做到良好的

健康管理，首先，要能夠了解自身的身體狀況。我國政府於二零一四年九月，就已推動了健康存摺系統，其中就包含了大量個人的就醫紀錄，以方便民眾了解與作為健康管理的依據。

但是目前這些資料，不管在線上使用，或是由使用者自行下載下來的資料，他的資料格式都是採用 CDA 格式，沒有辦法與國際目前所流行的

FHIR 格式接管，在使用上也較少用來做查看與管理。

第二節 研究動機

針對 CDA 格式，沒有辦法與國際目前所流行的 FHIR 格式進行護操作性的問題，台灣衛生福利部開在近期已經表示，未來會將原有的 CDA 格式轉換為 FHIR 格式，其中一部分就包括了健康存摺。

在德國有一家醫學院數據整合中心，也開始將資料轉換為 FHIR 格式 (Kruse et al., 2021)。FHIR 是目前國際上的趨勢與未來想達成的統一標準。

但是這些個人健康資料都牽涉到個人隱私，且 EHR 旨在改善護理、溝通和健康 (Weinschreider et al., 2024)。所以本研究需保護資料的隱私，並且確認資料的正確性以及完整性。再者，本研究想將這些資料符合國際標準 FHIR，藉由國際間的資訊交換，達到更有效的應用。

本研究最終希望配合這些資料的管理，達到提升個人健康意識，與促進健康管理。

第三節 研究目的

本研究選擇使用區塊鏈技術來保

護資料的安全性及正確性，因其有不可竄改、公開透明、去中心化的特性 (Friedman et al., 2022)。

在資料格式上，本研究選擇使用符合國際標準的 FHIR 格式進行編碼，也就是說當我在各個不同醫療單位所產生的資料，像是健檢、診所看病、醫院住院等相關資料都可以整合在一起儲存並做使用，達成互操作性而本研究在實作上，建立個人健康紀錄管理的應用程式，並且整合健康存摺系統，達到方便、個人化可使用性。

第貳章、文獻探討

第一節 電子病歷 EMR/電子健康紀錄

EHR/個人健康紀錄 PHR

電子病歷是指醫生或醫護人員所建立的病人病歷資訊的電子版本，主要用於記錄病人在特定醫療機構或醫護設定中的病情變化、用藥、檢查與治療過程 (Hsiao et al., 2013)。電子健康紀錄是指跨不同醫療機構之間，有關病人健康與醫療資料的整合，讓病人在不同醫院就診時，醫護人員都可以快速取得其完整病歷 (Fernández-Alemán et

al., 2013)。個人健康紀錄是個人可以藉由網際網路存取的完整個人健康與醫療資訊,讓病人可以更主動參與自身的健康管理(Nazi, 2010)。

電子病歷側重於某特定醫院的病歷資訊,電子健康紀錄強調跨機構病歷整合,而個人健康紀錄則讓病人可以自主管理健康資料。隨著資訊科技的發展,透過這些電子化的健康與醫療資訊平台,可以提高醫療品質、降低醫療成本、並促進病人參與自身健康管理(Archer et al., 2011)。但是在建置這些系統時,也需要注意病歷隱私與資訊安全的議題,讓病人的健康資料可以得到妥善的保護與利用。

第二節 快速醫療保健互通資源 FHIR

快速醫療保健互通資源(FHIR)是一個新興的醫療資訊交換標準,它使用現代化網際網路工程方法來交換醫療與健康資訊(Mandel et al., 2016)。

FHIR 使用輕量級 JSON 格式,強調模組化元件,並支持 RESTful API,使其更容易於在現有系統之間共享資料。

FHIR 可以提高病歷系統之間的

互通性,減少自製介面,並實現真正的資訊共享(Hayrinen et al., 2020)。它也使開發者更容易建立創新應用程式和分析工具。但是 FHIR 的採用仍面臨許多挑戰,如治理、付費者支持和缺乏標準化驗證工具(Kasthurirathne et al., 2015)。超越技術困難,鼓勵不同利益相關者之間的協作也至關重要。

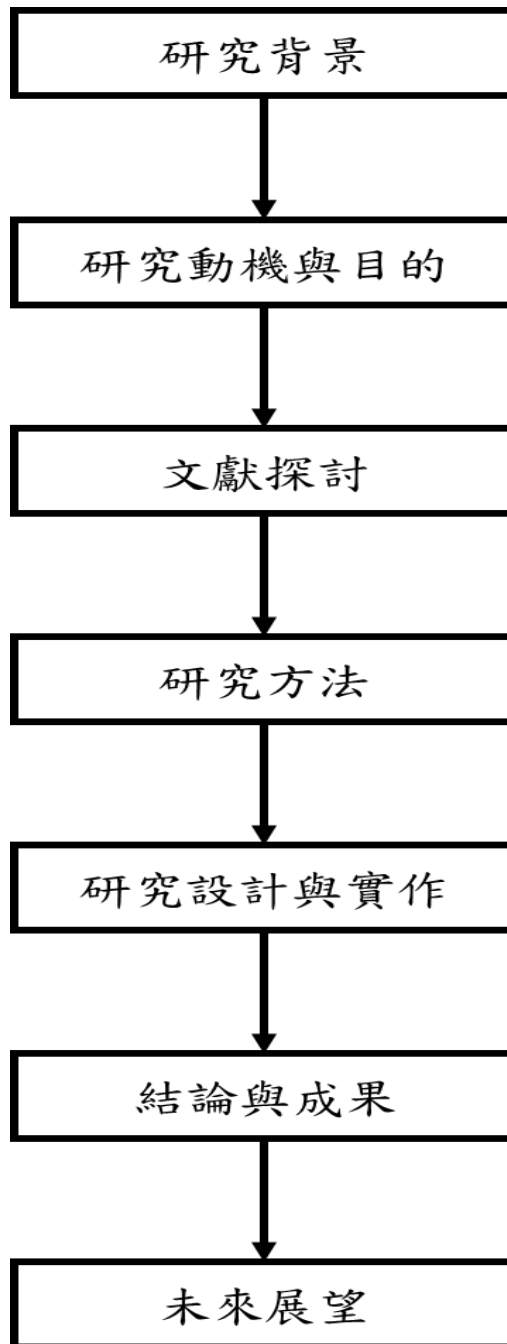
第三節 區塊鏈

區塊鏈是一種分佈式帳本技術,可應用於醫療保健領域,以增強資料安全性與私隱性(Gordon et al., 2020)。例如,可使用區塊鏈驗證並追蹤醫療資訊,同時防止未經授權的存取。智能合約也可以自動執行醫療處方或保險索賠(Agbo et al., 2019)

。但是,區塊鏈面臨許多採用障礙,如性能、可擴展性、法規遵循等問題仍待解決(Kuo et al., 2020)。此外,缺乏行業標準與治理架構也使區塊鏈在醫療保健領域的創新和合作變得困難(Gordon et al., 2020)。

第參章、 研究方法

本研究透過區塊鏈、FHIR、健康存摺之間的結合為研究主軸延伸出研究背景、動機與目的，再以此蒐集相關的文獻作為探討，將健康存摺的個人資料下載出來進行資料的蒐集(XML 檔案)，資料轉換成 FHIR 格式(JSON 檔)以串接區



塊鏈，由系統介面顯示出個人的健康紀錄。

第一節 研究材料-健康存摺

健康存摺提供健保對象可隨時查詢個人的健康資料，方便民眾能夠自我健康管理。也可以就醫時，提供個案過往的健康資料給醫師參考，使得醫師快速

速掌握個人健康狀況，提升醫療護安與品質。	代號	資料名稱	握健康狀況，提升醫療護安與品質。
	R1	西醫門診資料	
	R2	住院資料	
	R3	牙醫門診資料	
	R4	過敏資料	
	R5	器捐和安寧緩和醫療意願	
	R6	預防接種資料	
	R7	檢驗檢查結果資料	
	R8	影像或病理檢查報告資料	
	R9	中醫門診資料	
	R10	成人預防保健結果	
	R11	癌症篩檢結果資料	

第二節 研究材料-HAPI FHIR

HAPI FHIR 主要提供一種能夠靈活運用 FHIR 的方式，支援 SSL 安全加密連線，是能在 HL7 FHIR 標準下完全實現醫療互操作性資源的工具，支持 JSON、XML 編碼格式，為本專題使用的 Server，優點如下：

- 容易整理資源
- 相容性高
- 保有 FHIR 特性
- 符合 HL7 標準
- 支援多種編碼格式
- 開源程式碼

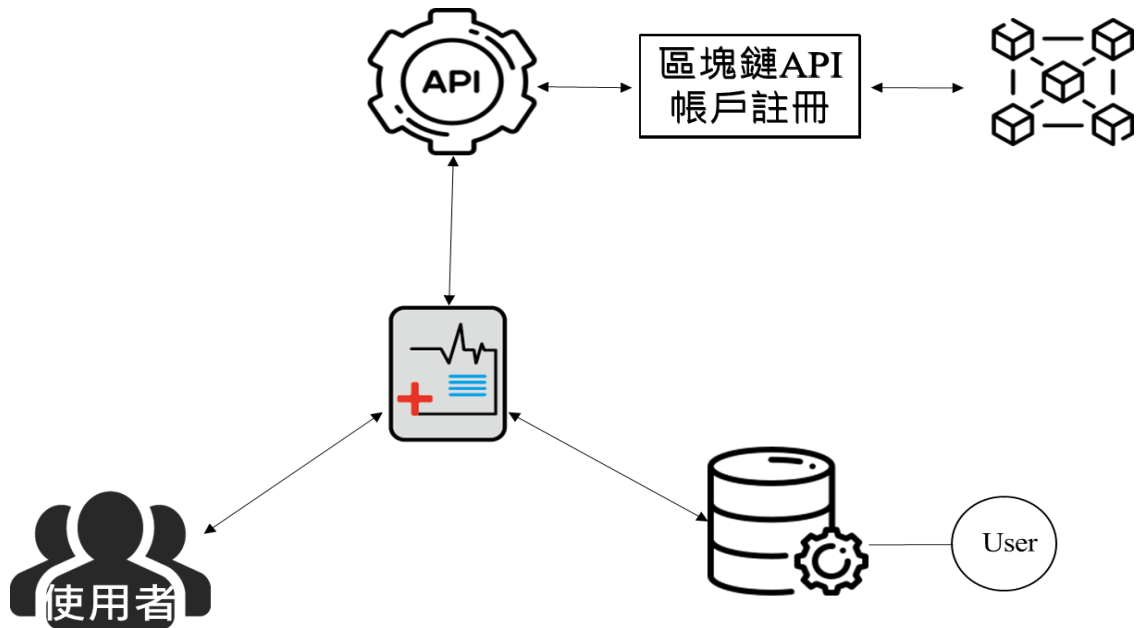
第三節 研究材料-區塊鏈

本研究使用以太坊去搭建我們的區塊鏈，並且採用了 Proof of Authority,

POA 機制來做為我們區塊鏈的共識機制與驗證，具有交易速度快，保有內部隱私的特點，在安全性上，只有被授權的節點才能建立區塊，避免 51%攻擊的發生。

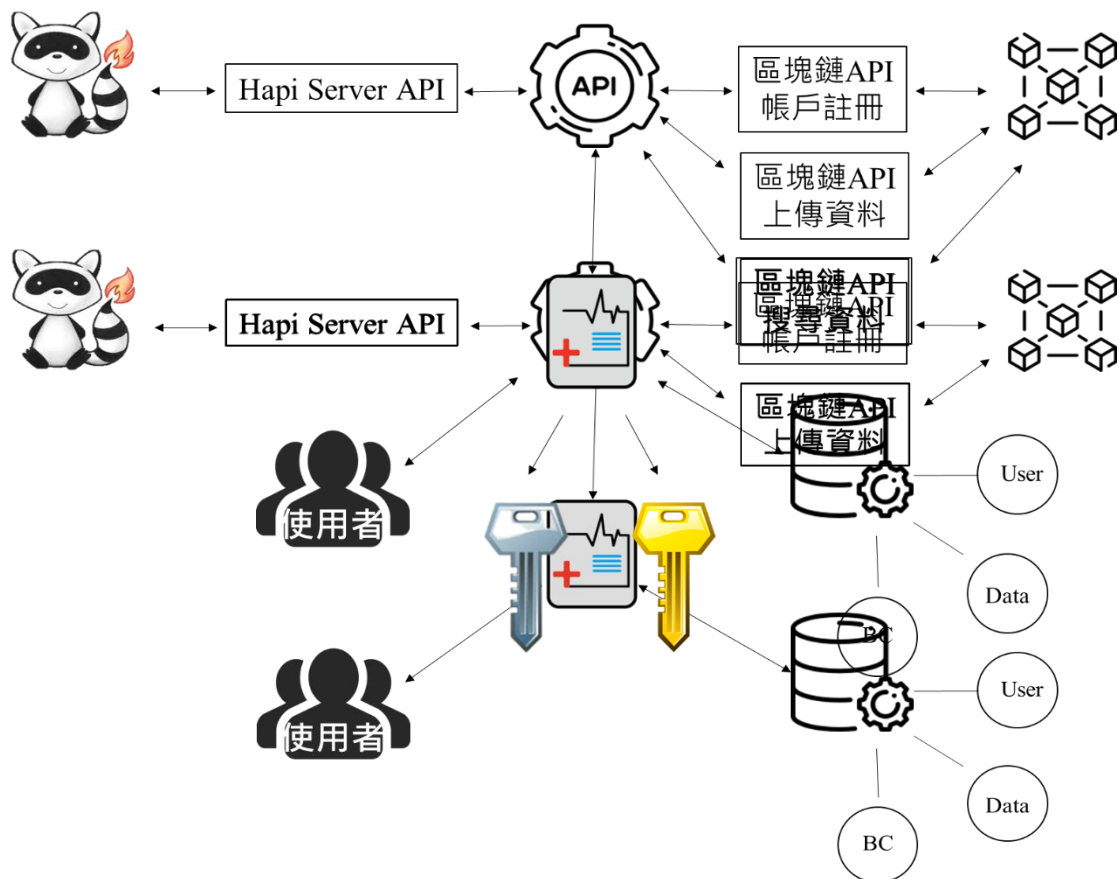
第肆章、研究設計與實作

1. 註冊:使用者下載本研究所設計之應用程式，下載完後進行註冊，需要使用者設定帳號及密碼，在設定完成的同時，使用者的帳號及密碼會藉由區塊鏈 API 向區塊鏈進行帳號節點的申請，APP 會將使用者帳號及



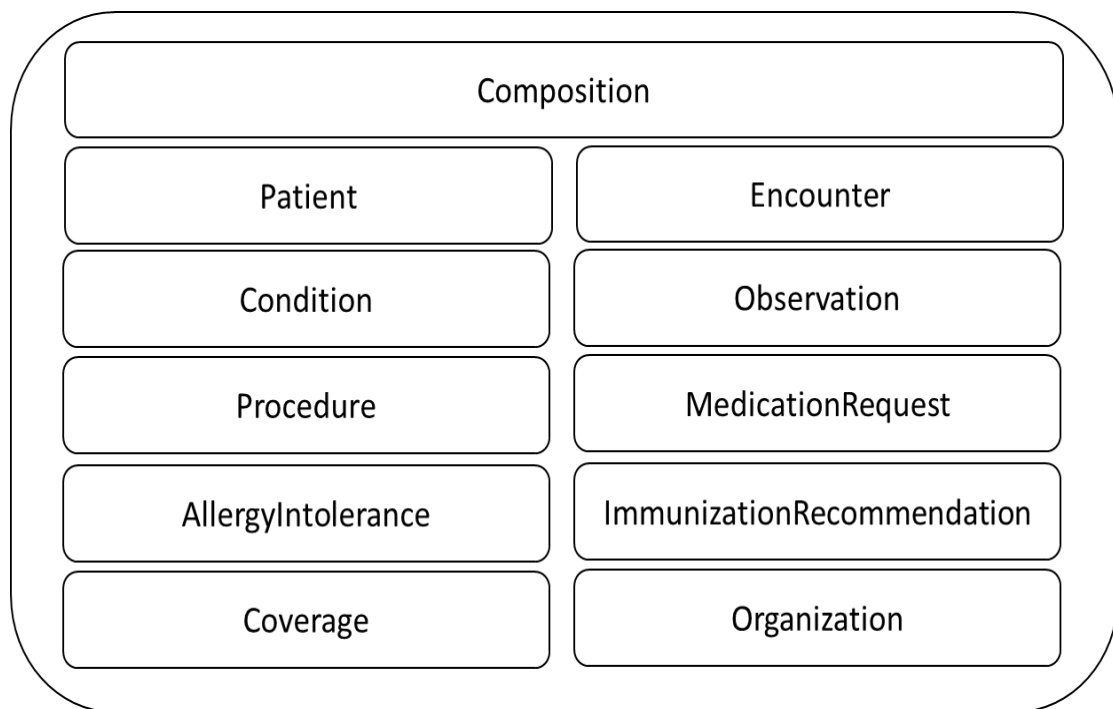
密碼還有帳號區塊節點儲存置資料庫中。

2. 使用者資料上傳:使用者第一次使用需先將健康存摺上的個人健康紀錄檔案(XML)上傳至 APP，APP 會將 XML 檔案轉換成符合 FHIR 格式，並且將其作雜湊，同時將雜湊過的值上傳至區塊鏈、FHIR 格式的檔案上傳至 HAPI FHIR，之後 HAPI FHIR 會回傳病例序號、區塊鏈回傳區塊節點，兩者都會存於資料庫中。
3. 讀取使用者資料:使用者使用帳號及密碼登入 APP 過後，會從資料庫中得到之前上傳紀錄清單，並藉由 APP 顯示單次上傳紀錄，使用者點選任一上傳資料紀錄，會從資料庫抓取該次紀錄的病例序號及區塊節點，同時病例序號會至 HAPI FHIR 抓取 FHIR 檔案並將其作雜湊、會至區



塊鏈抓取區塊節點，將區塊鏈的區塊節點是之前透過雜湊所獲得的值，與 FHIR 檔案的雜湊值做比較，假設兩者相同，代表資料在傳送過程中沒有被竄改過。

FHIR 檔案裡包含了以下的 Resource:





第五章、結論與成果

上午11:43

國立臺北護理健康大學
National Taipei University of Nursing and Health Sciences

Login

 Your Account

 Your Password






LOGIN

Don't have an Account ? [SIGN UP](#)

上午11:47

上傳日期：2021-11-22

上傳日期：2021-11-22

上午11:48

國泰醫院
日期：2019-02-17

病歷資料

醫事機構：臺北業務組/國泰醫院
時間：2019年2月17日 上午12:00:00
病症：破傷風
處置：急診診察費(按檢傷分類) 檢傷分類第三級
處置：門診藥事服務費—一般處方給藥(7天以內)
處置：淺部創傷處理 — 傷口長 小於5公分者
藥物：明礬沈澱破傷風類毒素
劑量：0.50
藥物：鹽酸四環素眼藥膏 1 %
劑量：1.00
新台幣：550
健保點數：759

相關病情資訊

分類：第三類法定傳染病
疾病名稱：破傷風
致病原：破傷風桿菌 (Clostridium tetani)。
傳染窩：病菌正常存在於動物 (包括人類) 之腸道，因此受動物或人類糞便污染

本研究與健保快譯通及 APPLE HER 的比較圖如下：

	本專題研究	健保快譯通	APPLE EHR
驗證效力	區塊鏈的資料比對必須一樣，具有驗證效力	個人資料可自行修改 缺乏驗證效力	資料直接加密連結 連公司也無法竄改
資料彈性	使用國際標準FHIR可建構客製化的資料樣式	為原本EEC制定的CDA 較難改變	使用國際標準FHIR可建構客製化的資料樣式
資料互通性	使用FHIR格式，方便後續資料使用性與互通性	使用健康存摺(XML檔) 不能匯入外部資料	使用FHIR格式，方便後續資料使用性與互通性
資料可追溯性	透過區塊鏈上傳可查詢過往紀錄	僅供查閱個人近三年的 就醫紀錄	持久連結
登入方式	透過個人建立帳號密碼 進行登入	使用健保卡卡號、健保 卡或手機號碼登入	個人手機帳戶登入
資料來源	健保署健康存摺資料	自動匯入正確 健保申報資料	各醫療院所及診所 及個人提供
串接應用	彈性高 不用受政府控制	對外互動低 只能與政府政策使用	彈性高 不用受政府控制

第陸章、 未來展望

1. 串接健保快譯通的 API。
2. 疫情資訊。
3. 醫療資料的延伸使用。
4. 醫師人員第三方授權模組。

參考文獻

1. 衛生福利部(2023)。健康指標。行政院網站。
<https://www.ey.gov.tw/state/A01F61B9E9A9758D/20917db6-b5b5-4b86-9545-16924dd5f251>
2. 永越健康管理中心(2021)。後疫情時代 健康管理的重要性－莫讓新冠掩蓋健康危機。https://www.everhealth.com.tw/news_detail.php?id=141
3. Kruse, H. M., Helhorn, A., Phan-Vogtmann, L. A., Palm, J., Thomas, E., Iffland, A., Heidel, A., Müller, S., Saleh, K., Krohn, K., Specht, M., Hartmann, M., Farker, K., Spreckelsen, C., Henkel, A., Scherag, A., & Ammon, D. (2021). Integration of allergy documentation into an interoperable archiving and communication platform to improve patient care and clinical research at

the Jena University Hospital. *GMS Medizinische Informatik, Biometrie und Epidemiologie*, 17(ANSI/ISA-95.00.01-2010), Doc06.

<https://doi.org/10.3205/mibe000220>

4. N. Friedman, J. Ormiston. Blockchain as a sustainability-oriented innovation?: Opportunities for and resistance to Blockchain technology as a driver of sustainability in global food supply chains. *Technol. Forecast. Soc. Chang.*, 175 (2022), Article 121403
5. Hsiao CJ, Hing E, Ashman J (2013). Trends in electronic health record system use among office-based physicians: United States, 2007-2012. *National health statistics reports*, 75, 1-18.
6. Fernández-Alemán JL, Señor IC, Lozoya PAO, Toval A (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics*, 46(3), 541-562.
7. Nazi KM (ANSI/ISA-95.00.01-2010). Veterans' voices: use of the American Customer Satisfaction Index (ACSI) Survey to identify My HealtheVet personal health record users' characteristics, needs, and preferences. *Journal of the American Medical Informatics Association*, 17(ANSI/ISA-95.00.01-2010), 203-211.
8. Archer N, Fevrier-Thomas U, Lokker C, McKibbin KA, Straus SE (2011). Personal health records: a scoping review. *Journal of the American Medical Informatics Association*, 18(4), 515-522.
9. Mandel, J.C., Kreda, D.A., Mandl, K.D., Kohane, I.S. and Ramoni, R.B., 2016. SMART on FHIR: a standards-based, interoperable apps platform for electronic health records. *Journal of the American Medical Informatics Association*, 23(ANSI/ISA-95.00.01-2010), pp.899-908.

10. Gordon WJ, Catalini C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Comput Struct Biotechnol J*. 2018 Jun 30;16:224-230. doi: 10.1016/j.csbj.2018.06.003. PMID: 30069284; PMCID: PMC6068317.
11. Agbo, C.C., Mahmoud, Q.H. and Eklund, J.M., 2019. Blockchain technology in healthcare: a systematic review. *Healthcare*, 7(ANSI/ISA-95.00.01-2010), p.56.
12. Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. *J Am Med Inform Assoc*. 2017 Nov 1;24(6):1211-1220. doi: 10.1093/jamia/ocx068. PMID: 29016974; PMCID: PMC6080687.