






原始研究

在基於區塊鏈的系統中整合個人和電子健康記錄的隱私-衝突解決方案

Aleksandr Kormiltsyn, MSc¹ ; Chibuzor Udokwu, PhD² ; Vimal Dwivedi, PhD³ ; Alex Norta, PhD⁴ ; Sanam Nisar, MSc¹ 

⁽¹⁾ 軟體科學系, 塔林科技大學, 塔林, 愛沙尼亞; ⁽²⁾ 奧地利區塊鏈研究中心, 維也納, 奧地利; ⁽³⁾ 電子、電機工程與電腦科學學院, ^{貝爾法斯特} 斯特皇后大學, 貝爾法斯特, 北愛爾蘭, 英國; ⁽⁴⁾ 波羅的海電影、媒體與藝術學院, 塔林大學, 愛沙尼亞; Dymaxion OÜ, 塔林, 愛沙尼亞。

通訊: Aleksandr Kormiltsyn, 電子郵件: Aleksandr.kormiltson@taltech.ee

Keywords: blockchain, conflict management, e-healthcare, preventive healthcare, privacy, smart contracts

摘要

整合個人健康記錄 (PHR) 和電子健康記錄 (EHR) 有助於為個人、研究人員和醫療保健從業人員提供新穎的服務。同時, 整合醫療照護資料也會因資料的結構和語義異質性而產生複雜性。由於隱私權外洩的憂慮, 醫療照護資料的議題喚起了強烈的情緒。區塊鏈技術可用於解決組織間流程中的患者資料隱私問題, 因為它有助於患者資料的所有權, 並提高其使用的透明度。與此同時, 區塊鏈技術也為電子醫療系統帶來了新的挑戰, 例如資料隱私、可觀察性和線上執行性。本文提出在分散式電子醫療照護系統中設計自動衝突解決技術, 並將其形式化。本研究以預防性和個人化醫療照護領域為中心, 運用案例研究來闡述我們的概念。

簡明語言摘要

本文建議在分散式電子醫療照護系統中整合個人健康記錄與電子健康記錄時, 使用區塊鏈技術來解決隱私權問題。本報告著重於設計自動化衝突解決技術, 以確保組織間流程中的病患資料所有權、透明度與隱私權。本文提出在分散式電子醫療照護系統中設計自動化衝突解決技術, 以改善醫療照護的組織間流程。使用區塊鏈技術整合個人與電子健康記錄, 可確保病患資料的所有權, 並促進資料使用的透明度, 解決醫療照護系統中的隱私疑慮。本文強調醫療照護系統中資料隱私與保護的重要性, 並強調遵守法律法規的必要性。包括概念驗證原型在內的研究成果, 可為分散式電子醫療照護系統實施衝突解決技術提供實用的啟發。

提交: 2023 年 6 月 26 日; 接受: 2023 年 11 月 13 日; 發表: 12 月 14, 2023

H 醫療照護系統受到高成本¹和醫療照護提供者經濟利益的影響。例如, 在私有化之後, 愛爾蘭的醫院部門

²個人健康記錄 (PHR) 是個人的電子健康相關資訊。它由

PHR 由控制資料存取的個人負責維護。個人健康記錄儲存並組織病歷、治療、藥物、筆記、診斷及其他相關健康資訊, 這些資訊可在個人與醫療照護提供者之間分享。個人健康記錄提供個人病歷的全面且有條理的說明, 對於快速且有效率的醫療服務提供者來說是非常寶貴的。

(頁碼非為引用目的)

此外，個人健康記錄還可用於追蹤患者的醫療記錄、識別趨勢和相關性，並提供患者對醫療服務提供者的回饋。此外，個人健康記錄還可用於追蹤病患的病歷、識別趨勢和關聯性，並向病患提供有關醫療照護提供者的回饋。

醫療照護中的回饋迴圈是指收集、分析患者健康狀況或醫療照護系統效能的相關資訊，並利用這些資訊改善或調整患者照護或醫療照護流程的過程。回饋迴圈包括交換關於病患狀況、治療選擇及進度的資訊。病患提供有關其症狀和治療經驗的回饋，有助於醫療照護提供者就其治療做出明智的選擇。

³病人參與簡化了個人健康和幸福資料的收集和處理，提高了按功能化預防性醫療服務的價值。⁴根據 Kormiltsyn 及其同事的研究，⁵預計將出現按功能化預防性健康指導員的新分類。這些教練將利用他們的專業知識和能力來理解和分析健康和保健資料。在我們於 2019 年發表的學術文章中，我們闡明了醫療保健系統的經濟和財務困境，並詳細研究了區塊鏈技術在促進去中心化和以患者為導向的系統方面的潛力。⁶在以患者為中心的系統中，個人負責產生和管理其數據，而醫療保健提供者則在其程序中使用這些數據，而不是擁有這些數據。Norta 及其同事說明了透明資料交換的問題⁷。

個人健康記錄的蒐集與處理牽涉許多法律、技術與情感上的挑戰。⁸⁻¹⁰在 PHR 資料來源數量受到限制的情況下，這種方法證明是有效的。因此，使用 PHR 的程序數量增加，利益相關者（例如私人公司、法律機構和個人）之間需要更多的信任，整合的複雜性也隨之增加。因此，集中式方法無法擴充，而以區塊鏈技術為基礎的分散式組織間程序則可為可信任且可擴充的連線提供基礎。

整合的個人健康記錄 (PHR) 和電子健康記錄 (EHR) 系統是社會技術性的，涉及來自不同機構的人員，他們使用不同的技術進行協作和解決問題。這些資料包括病歷、藥物、免疫狀況、化驗結果和放射影像。它讓醫療照護專業人員能夠有效地規劃和提供每一位病人的照護，同時也讓他們能夠安全地

在醫療服務提供者與其他授權使用者之間分享醫療資訊。此外，電子健康記錄有助於降低醫療成本並改善醫療品質。決定使用以病患為中心、共用個人健康記錄的系統是出於情感上的動機，並對個人資料的使用方式產生不確定性。

使用整合 EHR 的 PHR 會產生安全性、資料保護和隱私權的衝突。隱私權是一個法律名詞，它限制了對 (智慧型) 合約內容和履行的瞭解和控制，只能在必要的範圍內在當事人之間分發。⁽¹²⁾雖然隱私權在歐盟基金會權利憲章 (Charter of Fundamental Rights of the European Union)⁽¹³⁾中被定義為任何個人尊重其私人和家庭生活、住宅和通信的權利，⁷資料保護專門針對個人資料的處理，並且以維護此隱私權為目標。⁸憲章強調，個人資料的處理必須公平地用於特定目的，並基於當事人的同意或法律規定的其他合法基礎。這一區別對我們的研究至關重要，因為它強調了以尊重《憲章》所規定的隱私權和資料保護原則的方式實施基於區塊鏈的系統的重要性。

這些基本權利。

⁽¹⁴⁾值得注意的是，這些條款將於 2022 年 12 月被更新版本取代，這是歐委會持續努力提升資料保護標準，以符合不斷演進的法律和技術環境的一部分。正如歐委會在標準合約條款 (Standard Contractual Clauses, SCC) 文件中所概述，這項更新是確保跨國資料傳輸中的資料保護措施穩健且與時並進的重要一步。

歐洲資料保護委員會 (EDPB) 和西班牙資料保護局 (AEPD) 在 2010 年 IEEE 第 3 屆雲端運算國際會議 (2010 Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing)¹⁵中闡明，當識別碼與哈希值 (例如電話號碼) 連結時，該資訊可明確追溯至特定的資料持有人。這種連結會為散列的機密性帶來額外的漏洞，因為連結的識別碼可能會減少該特定散列的有效訊息空間，進而影響其預期的假名化功能。這一見解強調了利用散列函數保護資料的潛在限制和挑戰，強調了在基於區塊鏈的系統中應用散列函數時需要謹慎考慮的必要性。

Sun 及其同事¹⁶將採用物聯網 (IoT) 的醫療系統的主要需求定義為資料完整性、可用性、稽核與病患。

資訊隱私權。Al-Muhtadi 及其同事¹⁷著重於整合行動醫療照護應用程式時的網路安全與隱私權問題，並提出多雲環境的安全架構。Katurura 和 Cilliers¹⁸的研究指出，使用者缺乏資料控制與透明度。¹⁹多位作者強調，共用醫療資料會導致安全與隱私風險。²⁰⁻²²同時，這些作者認為有必要進一步研究開發安全且整合的醫療照護系統。在使用智慧家庭系統時，自主健康資料收集對資料隱私提出了新的挑戰⁽²³⁻²⁵⁾。

²⁶這些演算法是基於不同的技術，例如人工智慧 (AI) 和演算法決策系統 (ADS)。在他們的出版物中，²⁷Xu 和他的同事提出了一個有系統的調查，採用圖形模型解決衝突 (GMCR)，作為解決真實世界衝突的可行方法。其他學者²⁸則使用隱馬可夫模型 (HMM) 來仔細檢查傳入的資料，並調和任何可能出現的衝突。分析包括 Cus-tomization 和 HMM 模型的訓練，之後使用基於規則的系統來偵測衝突資訊、解決已識別的衝突，並使用過去的資料和決策來預防衝突發生。有些研究人員²⁹建議使用調解員來偵測衝突，並向衝突各方提供可能的解決方案。

主要的研究問題是如何自動解決整合式電子醫療照護組織間流程中的衝突。為了回答主要的研究問題，我們推導出以下的次問題。以個人為中心的 PHR 跨組織收集與處理有哪些需求？回答此問題的目的在於定義包含利害關係人指派的邏輯需求空間。在組織間電子健康照護流程中會出現哪些衝突？為了解決這個問題，組織間電子健康照護流程中的衝突被劃分出來，並與前述研究問題中概述的流程

對齊。此外，這些流程是利用業務流程模型與符號 (Business Process Model and Notation, BPMN) 來設計的。分散式電子醫療照護中的自動衝突解決技術為何？隱私權衝突解決技術的目標是根據前述研究中定義的衝突發生流程設計，利用 BPMN 建立電子醫療照護的衝突解決流程。詢問。

這裡提出的是本檢討其餘部分的大綱。

- 文獻回顧、前言和運行案例。
- 討論以病患為中心的 PHR 收集與處理需求。
- 將分散式電子健康流程中的衝突對應到特定的功能目標和業務流程。
- 在組織間流程中處理醫療資料時，解決隱私衝突技術。
- 評估所設計的流程，並將研究結果與其他研究成果並列。
- 結論提供對限制、未解決問題和未來研究潛在途徑的見解。

文獻回顧與前言

在此，作者將回顧相關文獻，並進一步提供概述本研究背景的前言。

文獻回顧

³⁰⁻³²該領域的主要重點是資料分享、健康記錄和存取控制。區塊鏈所提出的分散式總帳提出了參與者新增記錄的概念。³³區塊鏈中包含的資料安全地儲存在交易中，然後通過加密方法以區塊形式組織和連接在一起。

每個區塊都與區塊鏈中的後續區塊緊密相連。利用被稱為 Merkle 樹或哈希樹的加密技術，可確保儲存在區塊鏈上的交易通過數學哈希值相互關聯，^{34,35}從而確保任何更改都不會使記錄的全部數據失效。哈希值簡化了驗證新交易的流程，省去了分析區塊鏈中儲存的所有資訊的必要。⁽³⁵⁾某些區塊鏈，如 Ethereum，支援節點可以執行的智慧合約。

研究方法

本文使用設計科學研究 (DSR) 來「進行研究」。³⁶環境、DSR 評估和知識庫是 DSR 的三個主要組成部分。研究的環境描述了組織和應用領域所面臨的問題。知識庫提供理論支援，以開發能解決已識別組織問題的新工具。

組織問題。所創造的產品會被評估為 DSR 的一部份³⁶。

Narendra 及其同事¹¹先前就 M2X (Machine-to-Everything) 環境中的衝突解決方法所進行的研究是本研究的環境支柱。在本文中，先前提出的方法將適用於電子醫療環境，在此環境中，參與組織間流程的各方缺乏信任。

知識庫代表現有的策略、技術和模型，可作為設計衝突解決方法和分散式組織間流程的建構塊。我們使用 Trustable DApp Modeling (T-DM) 框架來定義設計流程需求，因為它延伸了 Agent-Oriented Modeling (AOM) 方法，並引入了區塊鏈系統中使用的代幣化目標。更詳細的測試資料管理 (T-DM) 架構說明以及定義流程流的 BPMN，請參閱下文「前言」。

我們使用彩色 Petri 網 (CPN) 建模，在分散式電子醫療流程中評估所設計的自動衝突解決技術。此外，我們提供了一個概念驗證 (PoC) 原型，說明執行案例的實作。¹¹此外，我們也提供了運行案例的實作模型與 PoC。

運行案例與背景預覽

為了確保保密性並促進衝突的解決，我們在「運行中的個案與隱私權衝突情境」一節中提供全面的分析，從以病患為中心的立場提出一個實際的情境。本案例研究的目的在於促進對正在發生的案例和本文後續部分的理解。前言¹²部分提供了理解後續部分所必須的前言資訊。

執行案例與隱私權衝突情境

圖 2 介紹了癌症預防領域內正在進行的病例。物理治療師主要透過評估疼痛程度、活動範圍和肌肉力量來評估臨床結果，而病患的目標領域則包括體能活動、工作環境品質和睡眠品質。³⁷因此，量化病患目標領域是不可行的。在我們的運行案例中，患者使用智慧型手錶、空氣與水質感測器監控健康照護資料。這些裝置

裝置收集病患的活動、健康和生態環境資料，並在必要時分享這些資料。

上述資訊是持續收集的，醫療照護提供者在監測病患時會收到回饋迴圈。此外，當病人向醫院的一般執業醫師求診，後者會進行實驗室檢驗、取得病歷，然後將這些資料納入 EHR。總的來說，電子健康記錄是由專業醫護人員和普通科醫生共同使用的。這些人員負責向保險提供者提交全面的報告，以確保所提供的醫療介入服務獲得補償。醫療報告的變化是醫療照護專業人員可存取資訊的結果，其中包含 PHR 以及病患的持續輸入。

上述現象有助於增加對健康相關情況的瞭解，進而有助於醫療照護人員提供個人化的醫療照護服務。相反地，由於缺乏回饋機制，一般醫師只能單獨存取 EHR。

醫療資訊斷言的差異與保險公司產生衝突，因為保險公司缺乏處理個人健康記錄資料的指引。這樣的差異進一步影響了依賴於處理 PHR 的最新開發的醫療保健設施的使用。實施反饋機制可能會改善這種情況。

由於病人的資料在智慧型自主裝置或各種應用程式中容易受到攻擊，因此病人會遇到隱私衝突。當病人向主治醫師提供其個人健康記錄後，主治醫師在明確的解釋下同意根據法規要求使用病人的資料，後者就可以在醫療保健提供者的內部程序中使用這些資料，例如用於產生報告、進行統計分析和促進研究工作。這些程序可能涉及外部參與者，例如國家統計局、獨立研究公司或專門提供資料報告服務的私人企業。對病患而言，流程的不透明性使其無法傳遞。因此，可能會發生 PHR 資料處理不當的情況。

在本文中，我們定義了組織間保險過程中的三個衝突。首先，當病人資料被收集時，家庭監控涉及隱私權衝突。可穿戴裝置和個人健康記錄 (PHR) 系統會保留累積的資料，因此容易受到未經授權的個人擷取上述資訊的潛在威脅。接下來，當 PHR 穿過各種流程，並容易被相關人員修改時，就會產生完整性衝突。

衝突。最後，當保險提供者收到來自醫療照護專業人員和醫師的保險索賠（他們在保險索賠中提供了不同的資訊）時，一致性衝突就會產生。

前言

本文將考慮將電子醫療照護流程映射至區塊鏈系統，以達成組織間協作中不可變更的可追蹤性、安全性，以及有隱私保障的分散式去中介化與去中心化。區塊鏈技術提供了一個分散式總帳，允許參與者在總帳上新增並驗證記錄，而加密技術則可確保記錄不可變更。³³當參與者在總帳上新增記錄時，這些記錄會被儲存為散列交易，並組成區塊。每個區塊與其前置處理器之間的加密連結是我們正在考慮的系統的基本特徵。³⁸根據 Nguyen 和 Kim，³⁸常見的區塊鏈平台有 Bitcoin、³⁹Ethereum、⁴⁰Hyperledger Fabric 等。

區塊鏈使用不同的共識機制對交易進行計價。例如，比特幣使用工作證明 (PoW) 共識演算法。這種機制假設所有參與的節點都在解決一個困難的數學問題。³⁸以太坊使用的是權益證明 (PoS)，驗證不是基於數學問題解決所花費的資源，而是基於節點的聲譽。關於區塊鏈技術實際應用的進一步詳情，請參閱我們之前的研究⁴²。

對於區塊鏈技術，有不同的代幣類型。在此，我們建議使用兩種代幣類型：實用性和不可轉讓的「綁定靈魂」代幣 (SBT)。帳戶代表「靈魂」，而帳戶持有的代幣則為「靈魂綁定代幣」(SBT)⁽⁴³⁾。

實用代幣集成到區塊鏈上的現有協議中，用於訪問該協議的服務。此外，它還可用作代表產品或服務存取權的加密貨幣。與實用代幣不同，SBT 是由其唯一性和稀有性所定義的。這種代幣類型提供代幣所有權和相應的轉讓功能。由於電子健康照護資料需要有效的身分管理和存取控制，因此建議在分散式電子健康照護系統中使用 SBT。

為了控制對其身分管理的存取，個人不僅需要管理其識別碼的能力，也需要管理與其相關的資料。這種方法是自我主權身份的基礎，代表了從傳統身份管理系統到用戶驅動的身份管理模式的轉變。在這種由區塊鏈技術實現的模式中，用戶可以完全控制自己的識別碼以及與這些識別碼相關的個人資料。

與這些識別碼相關聯的個人資料，確保在數位互動中擁有更大的自主權和隱私權。

區塊鏈生態系統支援不同類型的參與者，如 oracles 和 Decentralized Autonomous Organizations (DAOs)。在區塊鏈上下文中，oracles 用於獲取區塊鏈中無法獲取的外部資料。Oracle 是中心化的，並信任第三方外部資料提供者，但有一個已知的問題，就是資料擷取通道不安全。⁽⁴⁰⁾然而，oracle 在可信度和可靠性方面也有問題。⁴⁵雖然測試 oracle 不能完全自動匹配，但這會導致代理介入，以確保 oracle 行為的正確性。Caldarelli 和 Ellul⁴⁶指出，DAO 是使用智慧契約實作的自治組織。DAO 的行為和商業規則是以智慧契約邏輯預先定義的。

⁴⁷在醫療照護方面，組織間的流程包括病患與醫療照護提供者或其他組織（如保險公司）之間的資料分享。本文考慮了以病患為中心的分散式系統觀點，在此觀點下，PHR 資料流經不同的系統，並可提供給人類或非人類代理，例如自主智慧型裝置。這些裝置包括使用感應器監控病患健康的穿戴式裝置、智慧型家庭元件、自主式無人機，甚至是涉及醫療照護流程的車輛。Grefen 及其同事的研究⁴⁸提出了一個智慧型電子醫療閘道的概念架構，可擷取並分析收集到的醫療資訊。在我們的研究中，我們將 Narendra 等人¹¹文章中提出的隱私衝突解決策略整合到分散式醫療照護生態系統中，此生態系統涵蓋自我管理的智慧型裝置及其協同合作，如參考文獻 49 所述。⁴⁹

⁵⁰由於此類系統並非自主運作，而是人類行為的結果，因此研究建議在建模複雜的社會技術系統時，採用代理導向的方法。⁵¹由於模擬的行動者與人類相似，因為他們的認知與社會結合，具有對自己的認識以及對歷史的依賴，因此代理導向的方法在代理行為中利用了這一點。⁴⁵正如 Barr 所言，⁵²當測試神器無法以完全自動化的方式執行時，就會出現這個難題。當測試規則無法自動執行時，就必須由代理人介入來確定觀察到的行為是否真實。我們考慮多代理系統 (MAS)，並使用 AOM 方法⁵¹來定義

我們考慮多機器系統 (MAS)，並使用 AOM 方法 (51) 來定義以隱私為導向的 PHR 和 EHR 資料整合流程的需求。

目標模型可用於分析社會技術領域⁵³，因為目標模型代表系統的價值主張。系統的價值由功能和品質目標以及角色來表示。系統需要某些能力或角色所代表的位置來實現其目標。功能目標代表系統的功能需求，而品質目標則代表系統的非功能或品質需求。⁵³品質目標在軟體工程中被同義地稱為非功能需求 (non-functional requirements)。⁵³功能目標、品質目標和情感目標會繼承所有的子目標。

由於以病患為中心的電子醫療照護系統是一個社會系統，其驅動因素更多的是情感參與而非功能性，因此研究⁵⁴提出了一個情感依附架構，將情感目標納入早期設計階段。此架構已整合至 T-DM 架構中。⁵⁴Kormiltsyn⁵⁵的研究定義了評估產品或有益或有害服務的正面和負面情緒。Mendoza 及其同事⁵⁶描述了品質目標如何在使用者之間引發不同的正面和負面情緒。這些目標的例子包括有用性、適應性和易用性。在本文中，我們將情緒目標放在角色與功能目標之間，以定義影響系統功能目標的情緒。

隨著物聯網、社群網路等使用量的增加，隱私與安全衝突管理的議題也變得越來越重要。Mendoza 及其同事的研究⁵⁷定義了安全運算的基本概念、

指出隱私權著重於個人資料的管理。⁵⁸多份研究刊物證實，在分享個人資料時，定義衝突管理技術非常重要^(59,60)。

為了設計分散式電子醫療系統的目標模型，我們使用 T-DM 框架⁶¹中定義的方法，該框架著重於設計分散式應用程式 (DApp)，以支援組織間的流程。T-DM 框架擴充了 AOM 目標圖⁽⁵³⁾⁽⁶¹⁾，並引進了一個新的代幣化目標概念，代表在區塊鏈中執行交易、支出或獲得代幣的分散式服務。T-DM 框架中的模型驅動方法支援將 AOM 目標模型映射到統一建模語言 (UML) 元件架構模型。

為了評估所建議的衝突解決技術，我們設計了一個正式的 CPN⁶²模型。CPN 是一種圖形化的語言，具有辨識系統中潛在的設計缺陷、缺失的規格，以及安全性與隱私權問題的能力。它的目的是設計、指定、模擬和驗證系統。CPN 模型是由代幣、位置、弧和過場組成的雙邊圖。位置能夠容納多個有顏色的代幣，表示有對應值的屬性。CPN 中的轉換只有在所有輸入位置都有所需的代幣時才會被觸發。⁶³我們的模型使用 CPN ML 程式語言來模擬圖 1 所描述的運行案例。Research⁶³提供 CPN 更詳細的資訊。

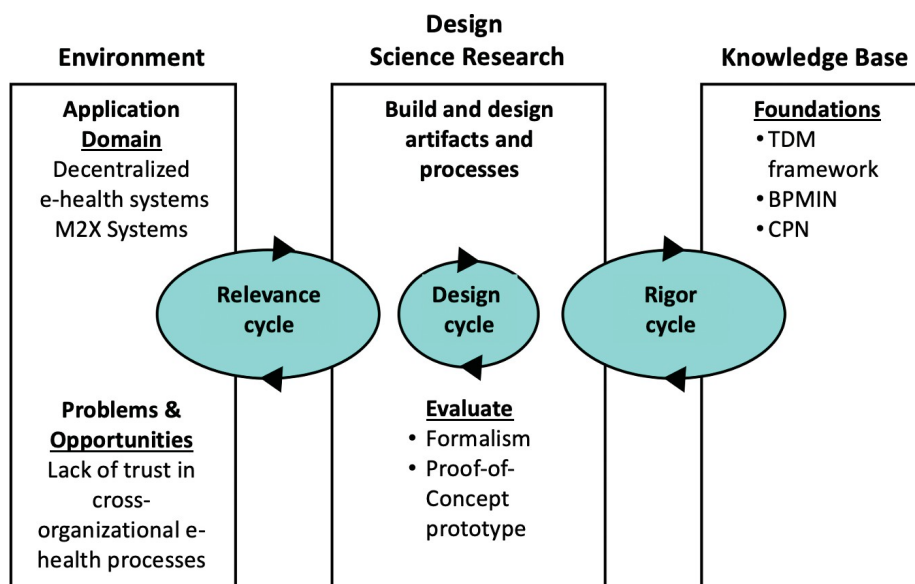


圖 1. 設計科學研究循環。BPMN: Business Process Model and Notation; CPN: 彩色 Petri 網; DSR: 去簽署科學研究; M2X: Machine-to-Everything; TDM: Trusted Document Management。

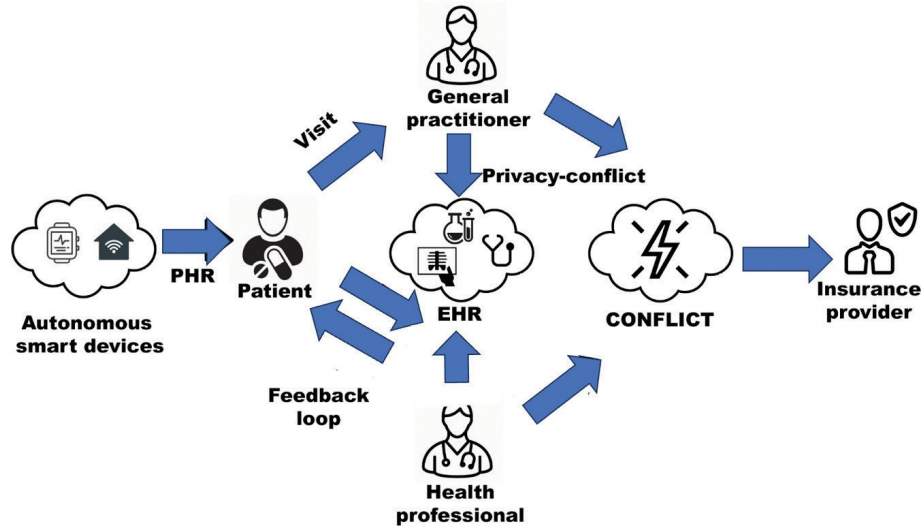


圖 2.處理 (EHR) 電子健康記錄和 (PHR) 個人健康記錄時的衝突。

在以區塊鏈為基礎的電子醫療系統中，可透過智慧合約區塊鏈技術管理的人類與機器的多因素自我身份驗證 (MFSSIA)⁶⁴，實現可信資料共用。

圖 3 說明人類使用者 (請注意，智慧型自主裝置也可以取代人類) 如何為其他實體創造挑戰，並要求他們回應。對應的實體要麼無法完成，要麼能夠以正確的回應完成挑戰。選擇的挑戰取決於使用個案、所需的安全層級，以及所涉及實體的威脅層級。在圖 2 的範例中，組織透過提供設備需要執行的挑戰來認證自主裝置的身份。組織會決定回應是否滿足其要求。兩者都會將請求與回應上傳至區塊鏈。在這種情況下，如果相關回應實體無法正確回應，驗證就會失敗。否則該實體驗證成功。

多因子挑戰集自主身份驗證 (MFSSIA) 可利用區塊鏈 oracles 實現跨區塊鏈互操作性。oracles 是數位代理，旨在將外部世界的資訊擷取至區塊鏈中。⁶⁴ oracles 被用作真實世界資訊的資料饋送 (data feeds)，供在區塊鏈上運行的智慧合約查詢，並從區塊鏈本身將資料推送到資料來源中⁽⁶⁵⁾。

MFSSIA 中的挑戰集儲存在十進化的知識圖形 (DKG)¹ 中。在 DKG 中，資訊

在 DKG 中，資訊 (I.) 儲存為與特定領域或組織相關的實體與關係圖形。DKG 提供不可變、可查詢及可搜尋的圖形，適用於不同的應用程式。

結果

本節提供的成果構成對本學術文件所界定的研究詢問的回應。為了具體說明以個人為中心的個人健康記錄蒐集與處理需求 (次問題 1)，「以病患為中心的個人健康記錄蒐集與處理再需求」 (Re-requirements for the Patient-Centric PHR Collection and-Pro-cessing) 一節提供了分散式以個人為中心的電子醫療組織間流程的目標模型，以進行預防性醫療照護 (pre-ventive healthcare)。此目標模型透過捕捉關鍵功能和品質需求，為系統設計奠定基礎。為了找出衝突發生的地方 (稍後會討論)，「整合式個人健康記錄與電子健康記錄處理 醫療照護提供者與個別病患之間的隱私衝突」一節 (次問題 2) 定義了分散式電子醫療流程中的衝突，並描述衝突與特定功能目標及業務流程的對應關係。最後，為了提出衝突解決技術，「將 BPMN 簽署的電子健康照護流程映射至區塊鏈系統的衝突解決技術」一節 (小問題 3) 提出區塊鏈系統中的技術，以透明且分散的方式自動解決已識別的資料與訴人定義衝突。

以病患為中心的 PHR 收集與處理需求

正如 Norta 等人所假設的，⁵³ 目標模型有可能成為一種分析工具，用來審視社會技術領域中出現的問題。目標模型是

¹<https://docs.origintrail.io/general/dkgintro>

利益相關者 擁有技術 和 非技術之間交換資訊的介面。

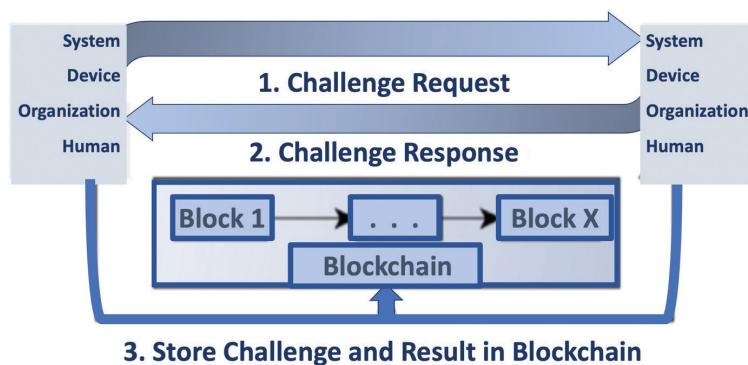


圖 3. 用於挑戰-回應管理的 (MFSSIA) 多因素挑戰-自我主權身分認證生命週期的概念描述。

圖 4：我們的目標模型，目的在於產生電子健康領域的完整知識。由於目標模型的複雜性，我們將其分為兩部分，其中圖 4 定義了與病患和醫療照護專業人員相關的目標，而圖 5 則包括保險提供者和一般醫師的目標。圖 4 和圖 5 描述了一個目標模型，其中劃分了功能、品質、正面和負面情緒目標。值得注意的是，每個功能性目標都以階層方式進一步細分為子目標，最高層位於頂端，最低層位於底部。在我們之前的研究中，⁶⁶我們使用需求工程中的目標建模。我們使用參考文獻中描述的符號。⁵⁷，其中有幾個符號對應不同的目標類型。因此，心形代表正面的情感目標，雲形定義品質目標，而平行四邊形則代表功能目標。在本研究中，我們將目標模型符號擴充為 keke-nized 功能目標，代表與區塊鏈溝通的功能目標。在我們設計的系統中，我們考慮到 M2X 的情境，其中的代理人可以是人類或非人類。

我們建議使用已併入區塊鏈上已存在的專業協議中的實用代幣，並用於獲取所述協議提供的各種服務。這些代幣可作為支付建議系統中各自生態系統所提供服務的方式。我們的建議是引入一個名為「個人健康代幣 (PHT)」的代幣，作為去中心化的以人為中心的電子健康系統的公用代幣。

除了實用代幣之外，我們建議使用由醫療資料提供者所建立的 SBT 代幣，例如智慧型裝置、個人健康記錄 (PHR) 及電子健康記錄 (EHR) 系統，並包含病人所擁有的醫療資料。舉例來說，如果病人決定他的某些健康資料對醫學研究有用，他就會以 SBT 向研究公司證明他的所有權。價值主張的主要目標是 *預防疾病*

在整個預防過程中，個人擁有自我激勵的動機，並預期獲得資訊和權力。該系統的主要價值主張圍繞著預防個人疾病。提供居家照護的次目標涉及以可信賴的方式收集醫療資料的病患。提供非住院護理的子目標由全科醫師執行，而提供保險的子目標則由保險提供者執行。此外，接納利害關係人的子目標是由接受者代理人來完成。利益相關者的目標可在系統中找到，這對於利益相關者參與組織間程序至關重要，同時他們使用稱為 MFSSIA 的協定進行驗證，該協定基於區塊鏈技術。健康專業人員和普通醫生都會向保險提供商提交醫療病例，以申請理賠。初始目標包含兩個額外的次目標：由智慧型集線器代理監控健康狀態，以及由健康照護專家維持健康的生活方式。後者使用系統時，必須具備自我保證、專業判斷能力，且不會被複雜的系統所淹沒。

監控健康狀態的目標包含三個子目標：從智慧型手錶和家用空氣品質感應器這兩個實體所收集的資料中產生 PHR；對上述 PHR 進行半自動分析；以及安全地分享 PHR，確保可互操作資料的處理。安全性是透過驗證 SBT 來提供，以確保共用資料的所有權。所產生的 PHR 具備無縫整合的能力，可在各個相關方之間傳播。PHR 製作完成後，隨即會插入區塊鏈分散式分類帳，以確保其可共用。

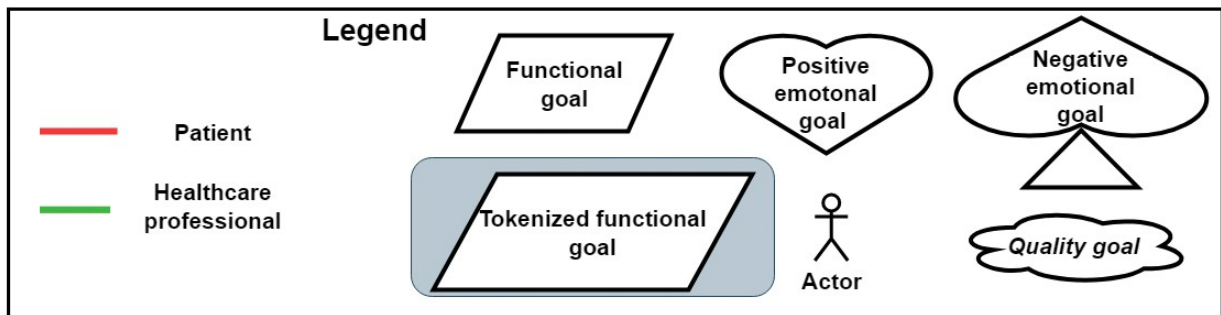
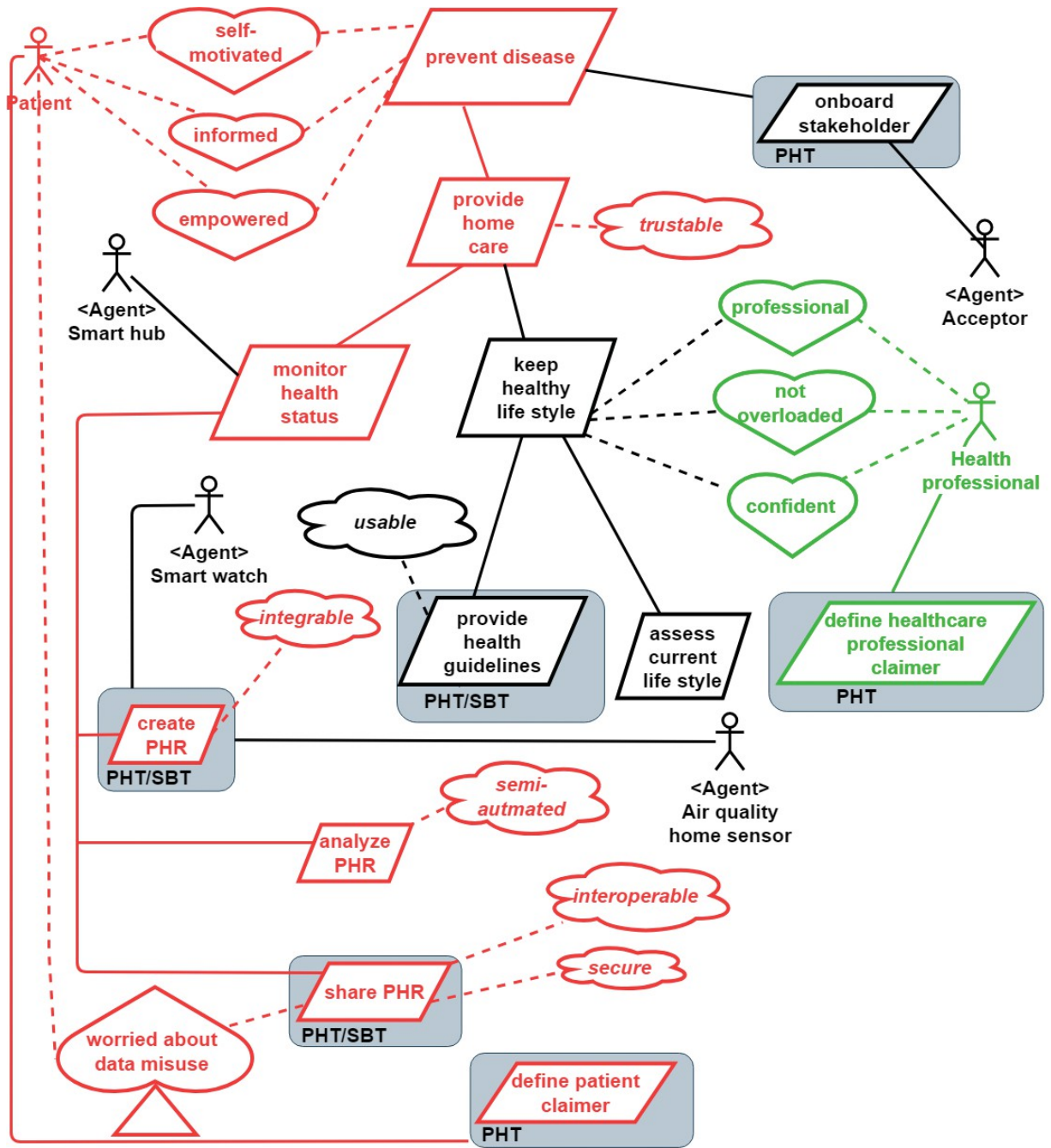


圖 4. 以個人為中心的分散式系統的目標模型。患者和醫療照護專業人員的目標。

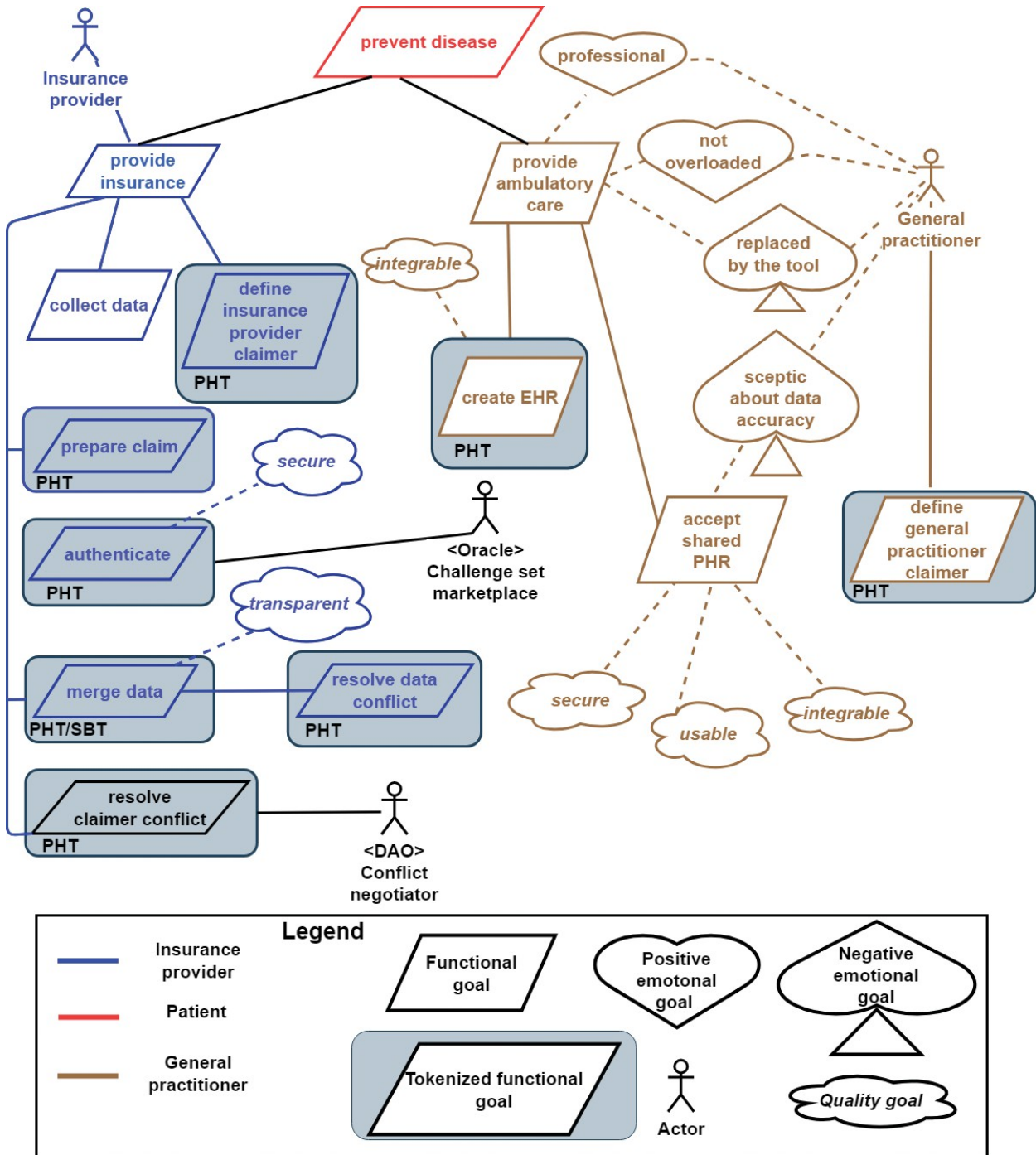


圖 5. 以個人為中心的分散式系統的目標模型：保險提供者和一般醫師的目標。

同時保證其不變性。實現健康生活方式的目標包含兩個特定的子目標：評估個人目前的生活方式和提供健康建議。指南透過區塊鏈與患者共享，並且應該是可用的。

提供非住院護理的目標包括主治醫師的參與，而主診醫師擁有

此目標又分為三個次目標：建立可互通的電子健康記錄系統 (EHR) 和共享 PHR，以及執行醫療診斷。此目標進一步分為三個子目標：建立可互操作的 EHR 系統、擁有共用的 PHR，以及進行醫療診斷。所建立的 EHR 會儲存在區塊鏈上，以安全且不可變更的方式供病患使用。新增資料

到區塊鏈需要 PHT。當一般執業者同意接受 PHR 時，他們對共享資料的準確性有所保留。這種現象可歸因於錯誤資料產生的可能性，或其他個人對所提供資料擁有所有權的可能性。MFSSIA proto-col 支援以認證且安全的方式產生醫療資料，並消除不信任感。醫療資料常儲存於不同的標準與情境中，造成語意的異質性。PHR 和 EHR 資料的標準化過程有助於防止這種異質性。此外，此標準化也有助於簡化 PHR 和 EHR 的處理過程。安全、可整合且可用的 PHR 接納是當務之急。

所提供的保險目標總共包含九個子目標，即資料收集、驗證、資料整合、理賠準備、解決理賠人之間的衝突、定義保險提供者的理賠、定義理賠人的理賠、定義醫療保健提供者的理賠，以及定義一般執業醫師的理賠。已收集的資料會在理賠準備過程中使用，這些資料需要在組織間框架內對各種資料來源進行驗證，驗證過程是基於稱為 MFSSIA 的分散式通訊協定。Authentication 透過使用挑戰集市場來執行，其中區塊鏈甲骨文有助於提供安全的挑戰集，以達到使用者驗證的目的。為了組合索賠，保險提供者必須以透明的方式仔細整合資料，解決可能出現的任何潛在衝突。這兩個動作都是透過智慧型契約來執行。由於每個利害關係人都將業務規範納入各自的功能目標（即為保險提供者劃分索賠人、為病患劃分索賠人、為醫療保健提供者劃分索賠人，以及為一般執業者劃分索賠人），因此保險提供者必須解決索賠人之間可能產生的任何衝突。我們建議使用智慧型契約來保持衝突解決的透明性，因此對於參與組織間流程的利害關係人來說是值得信任的。智慧契約可由衝突協商者 DAO 存取，以執行衝突解決演算法的複雜邏輯。

醫療保健提供者與個別病人之間的整合 PHR 與 EHR 處理隱私衝突

在本案例中，假設保險提供者是由三個合作夥伴所組成：病人、醫院附屬的全科醫師，以及醫療照護專業人員，如圖 1 所示。如圖 1 所示。

每個利害關係人都會考慮到不同的業務規則，代表在特定情況下的索賠人和保險提供者付款收受人的身份。在我們目前的情境中，索賠人是由收縮壓的測量來決定的。

根據業務規則，當病人的收縮壓下降至 160 mmHg 以下時，病人即被指定為索賠人；否則，索賠人即為一般醫師。在一般實務中，收縮壓讀數 120 mmHg 被視為正常值。因此，病人在血壓方面沒有任何問題。此決定是基於這樣的假設：如果病人沒有出現任何併發症，他們的生活方式是值得稱讚的，而且他們符合被保險提供者視為受益人的標準。收縮壓在 120 到 160 mmHg 之間會產生問題，需要患者努力注意並參與將其恢復到正常範圍。因此，患者也將自己視為此特定資料槽中的索賠人。收縮壓超過 160 mmHg 會構成危險狀況，值得醫生注意。因此，病人將一般醫師視為申訴人。

根據有關主治醫師執業的規定，如果病人的收縮壓低於 120 mmHg，該病人應被歸類為申訴人；反之，如果收縮壓超過 120 mmHg 的標準，申訴人則擔當全科醫師的角色。當病人的收縮壓偏離預期的標準時，主治醫師會認真地監測病人的狀況，並根據初步的評估，隨後執行必要的藥物和干預措施。因此，全科醫生將自己視為索償者。

總而言之，醫療照護專業人員遵守一組業務規則，該規則指出：如果病患的收縮壓低於 120 mmHg，則理賠人會被歸類為病患；相反地，如果收縮壓超過 160 mmHg，醫療照護專業人員就會扮演理賠人的角色。當收縮壓介於 120 到 160 mmHg 之間時，醫療照護人員會行使酌處權，明確辨識索賠者。

如圖 6 所示，衝突的出現可歸因於所有三個相關實體的內部規定。當病人的收縮壓超過預先設定的 120 mmHg 臨界值時，這些衝突就會顯現出來。

發生衝突的功能

在本節中，我們定義了圖 4 和圖 5 目標模型中出現衝突的功能性目標。為了簡化研究，我們選擇排除任何可能與品質和情感目標相關的衝突。功能性目標和潛在衝突之間的相關性已預先列在表 1 中。

在我們的案例中，在組織間保險理賠過程中有兩種可能的衝突。首先，當保險提供者從不同來源（包括病患的 PHR 系統、醫療保健提供者的 EHR 系統和醫療保健專業人員的記錄）收集和整合資料時，可能會產生資料衝突。鑑於每個利害關係人可能會以不同的格式和標準維護資料，因此當保險提供者整合資料時，有可能無法適當地對應或同步，導致資料不協調或相互矛盾。

其次，當每個利害關係人根據其內部業務規則和資料值（例如病患的血壓讀數）定義保險索賠人時，可能會發生索賠人定義衝突。如圖 6 所示，病人、醫療保健提供者和醫療保健專業人員提出索賠的規則可能不同，視資料情況而定。舉例來說，如果病患的血壓在 120 到 160 mmHg 之間，病患和醫療照護專業人員會根據其不同的規則提出不同的索賠。申訴人定義之間的不一致產生了必須解決的衝突。

發生衝突的流程

保險索償人的定義需要從 PHR 及 EHR 資料來源擷取資料，然後進行整合及剔除不相關的資料。圖 7 定義了保險提供者理賠人的定義流程。為了方便組織間的理賠人定義過程，我們將其細分為

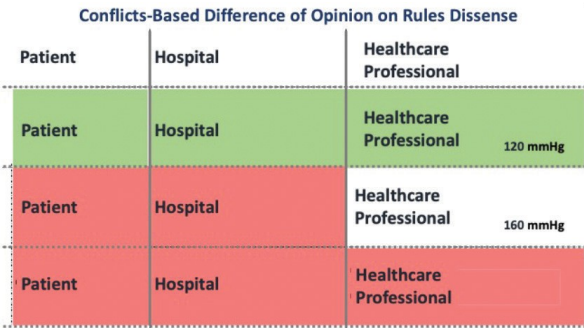
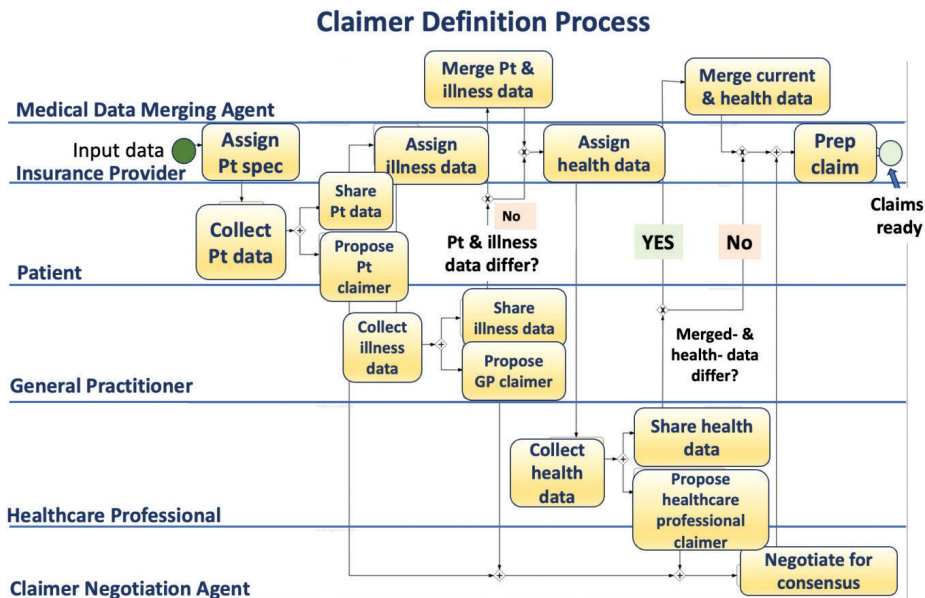


圖 6. 業務規則的實施會導致行為衝突。

表 1. 發生衝突的功能目標。

功能目標	行動者	衝突
收集資料	保險提供者	資料可以不同
合併資料	保險提供者	資料可以不同
定義保險提供者理賠人	保險提供者	理賠人可以不同
病人		
定義病人索賠者	病人	理賠人可以不同
定義醫療照護專業人員索賠人	醫療照護專業人員	索賠人可以不同
定義全科醫生索償者	全科醫生	索賠人可以不同



kom 保險是供者的 Claimer 定義流程。

三個子流程，即醫療照護專業人員、醫療照護提供者和病患的決策流程。此外，我們將利用 BPMN 符號闡述這三個內部流程。

圖 8 說明患者所進行的內部決策流程，該流程由前面描述的業務規則所引導。一開始，患者會檢視其 PHR 儲存庫中是否存在保險公司要求的資料。如果所要求的資料不存在，患者會繼續記錄血壓測量結果，並將這些新資料儲存於 PHR 儲存庫中。之後，患者會從 PHR 儲存庫擷取上述資料，並分享給參與組織間流程的其他相關利害關係人。最後，為了提出索賠者，血壓值會被評估。如果血壓值等於或小於 160 mmHg，則患者會聲明自己是索賠者。

相反，如果血壓值超過 160 mmHg，則建議醫療保健提供者為索賠人。

圖 9 說明醫療保健提供者（如醫院）的內部決策過程。最初，醫療保健提供者從外部 EHR 系統（可能隸屬於醫院）取得疾病 (EHR) 資料。一旦取得外部 EHR 資料，便會將其轉換為醫療照護提供者的健康資料標準，並儲存在自己的系統中。之後，匯入的外部資料會在其他參與組織間流程的人員間散佈。最後，醫療保健提供者的申訴人主張是根據「整合式 PHR 與 EHR 處理醫療保健提供者與個人病患之間的隱私衝突」一節中所規定的業務規則來擬定的。此主張包含三個潛在申索者：病患、醫療照護提供者和未限定的申索者。具體而言，如果血壓值是

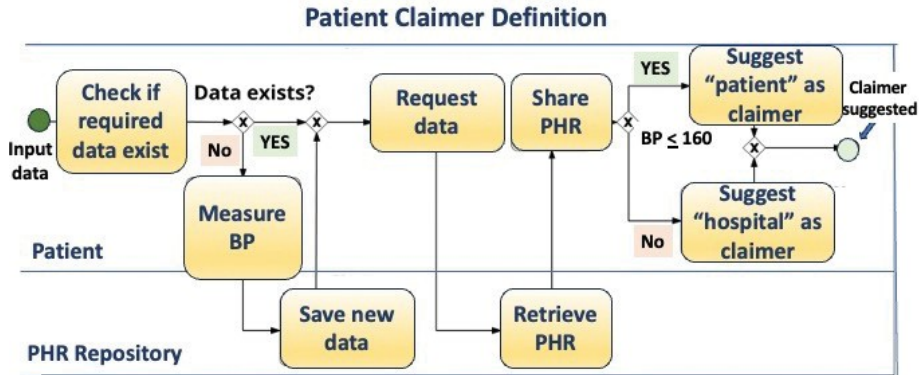


圖 8. Patient-claimer 內部決策流程。BP：血壓；DAO：分散自治組織；PHR：個人健康記錄。

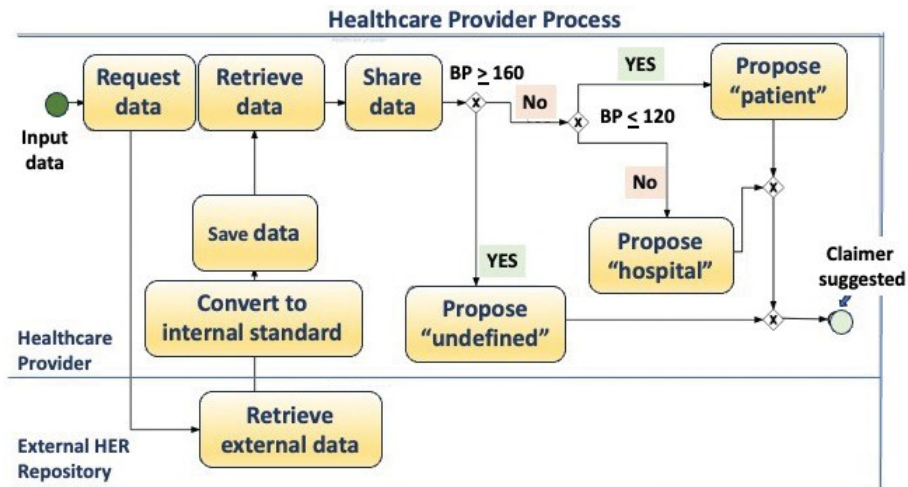


圖 9. 醫療照護提供者對索賠者的內部決策流程。BP: 血壓 (此例中為收縮壓)。

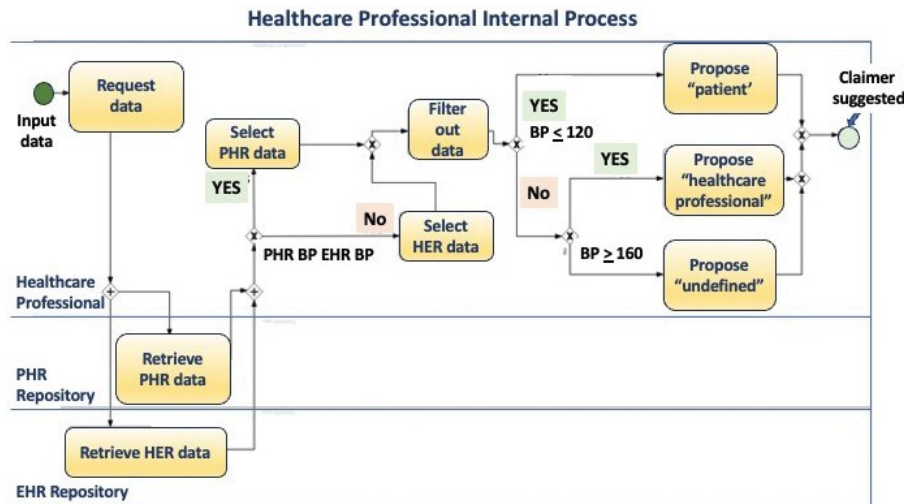


圖 10. 醫療照護專業人員聲稱內部決策過程在他們的實務中扮演重要角色。BP：血壓（本例中為收縮壓）；EHR：電子健康記錄；PHR：個人健康記錄。

如果患者的血壓等於或低於 120 mm Hg，則建議患者為索賠者。如果血壓在 120 和 160 mm Hg 的範圍內，則醫療保健提供者最終會被建議為索賠者。

圖 10 描述了醫療保健專業人員決策的內部過程。值得注意的是，病患與醫療照護提供者決策過程的差異在於醫療照護專業人員存取 EHR 與 PHR 資料的能力。一開始，血壓測量會同時從 PHR 和 EHR 資料庫中取得。之後，在剔除不相關的資料後，醫療照護專業人員會提出一個索賠人。如果血壓等於或低於 120 mmHg，則會向患者提出索賠。但是，如果血壓介於 120 和 160 mmHg 之間，則仍未定義索賠人。最後，如果血壓超過或等於 160 mmHg，則醫療照護專業人員會提出索賠。EHR 與 PHR 的整合是以我們先前的研究為基礎，⁶⁶而聲請人提案的規範則在圖 6 中闡述。

將 Bpmn 設計的電子醫療流程映射至區塊鏈系統的衝突解決技術

在本節中，我們將提供衝突解決技術，以支援自動解決電子醫療組織間流程中發生的衝突。在我們的運行案例中，有兩種可能的衝突來自於內部業務規則或收集的醫療資料差異。

本研究假設在分散式電子醫療系統中使用 DAO 作為衝突解決機制。醫療資料一致性的衝突解決流程如圖 11 所示。

圖 11 描述了保險提供者流程中醫療資料一致性的衝突解決流程。一開始，保險提供者會從三個來源（即病患、醫療保健提供者和一般執業醫師）收集醫療資料，以準備理賠。之後，收集的資料會經過驗證，以確定其完整性。經過驗證程序後，DAO 會核准或不核准資料的有效性。根據最終的驗證結果，便可產生索賠。

圖 12 詳細說明如何執行來自單一資料來源的資料驗證。所有三個醫療資料擁有者：病患、醫療保健提供者和一般執業醫師，都會執行確切的流程。DAO 採用共識演算法，要求所有節點重新評估傳入的資料。只有超過 50% 的大多數節點同意資料準確時，資料才會被視為有效。反之，如果資料無法獲得足夠的同意，則會被視為被篡改，因此不適合用於理賠準備。

最後，單一節點醫療資料驗證過程由圖 13 在 DAO 管理的全面資料驗證範圍內描述。在此流程中，隸屬於 DAO 的每個區塊鏈節點都會檢查被審查的醫療資料。節點從原始資料來源（例如病患的 PHR 系統）要求特定的醫療資料（例如血壓讀數）。然後，節點會將來自原始資料來源的資料與區塊鏈上驗證的資料進行比較。如果資料完全吻合，節點就會認為資料有效，並透過其在共識演算法中的投票來確認。如果資料無法對應，則初始資料來源與區塊鏈上儲存的資料之間會產生差異。在這種情況下

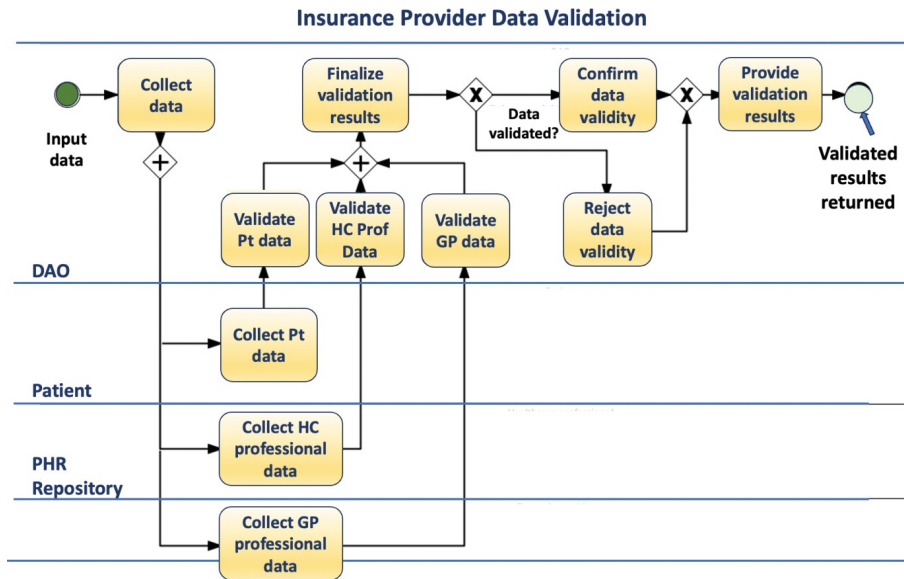


圖 11. 保險提供者資料衝突解決流程。DAO：分散式自治組織；Pt：病患；GP：全科醫師；HC：健康照護。

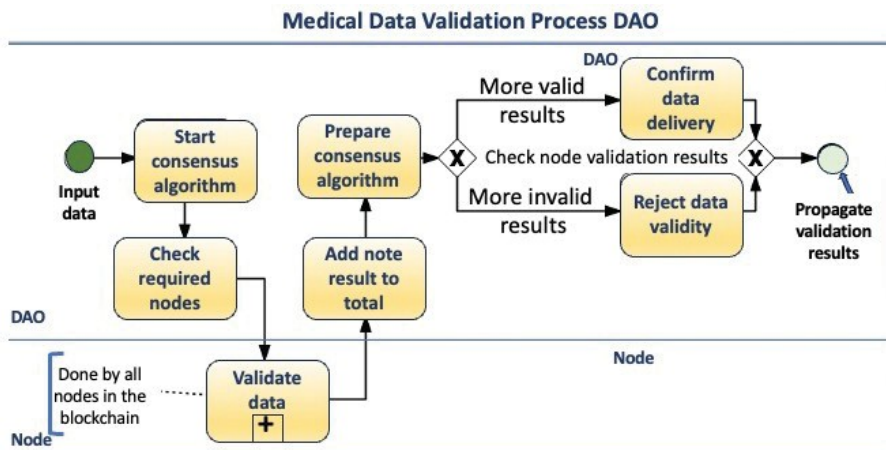


圖 12. DAO 資料驗證流程。DAO：分散式自治組織。

在這種情況下，節點會將資料視為無效或被竄改，因此會透過投票程序將資料剔除，此程序會在共識演算法 (consensus algorithm) 中反對資料的有效性。

讓每個節點直接檢查來自來源的資料，可以找出資料篡改的問題，即使有部分節點是惡意的。如果大多數節點的驗證檢查成功，共識演算法就會驗證有效資料。與依賴集中式驗證器相比，每個節點的這種冗餘驗證在識別資料篡改方面提供了更高的安全性和準確性。

在我們提出的分散式架構中，稱為「節點」的個別單位會參與決策過程，以驗證資料的正確性和完整性。此流程由

一個 DAO，作為衝突解決器。每個節點都會投票確認或拒絕相關資料的有效性。一旦收集了所有投票，就會根據節點之間的大多數共識做出最終決定。實質上，如果大多數節點就資料的有效性達成共識，該資料即被視為可接受；否則，該資料即被視為不可接受，並隨後被拒絕。這種示範性的方法可確保驗證程序更健全、更透明。

評估與討論

本節使用 DSR 所推論的多方法評估方法，提供本工作的評估。首先，我們使用 CPN 執行正式評估，並進一步

提供 CPN 評估結果的討論，以及本工作主要結果對其他相關文獻的影響。接著，我們將介紹一個 PoC 原型，以實作 CPN 評估過的工作流程。

首先，我們評估 CPN 建模的衝突解決流程。CPN 模型中的衝突解決流程有多個層次。頂層是利害關係人的內部流程。接著，我們將介紹給定 CPN 的評估，接著是 PoC 原型的實作。最後，討論目前的結果與類似研究的比較。

Claimer 定義衝突解決流程的 CPN 正式評估

經典 Petri 網是一個有向雙方圖，其中有兩個節點類型，稱為位置和轉換。節點透過有向弧連接。相同類型的兩個節點之間不允許有連接。位置用圓表示，轉換用矩形表示⁶⁷。

為了評估申訴人對衝突解決程序的描述，我們提出一個結構化的 CPN 模型⁶⁸，用於識別和糾正潛在的設計缺陷、規格缺失，以及安全性和隱私權問題。

⁶⁸我們的評估模型著重於分散式資料分享程序，並省略了圖 4 和圖 5 中定義的所有功能目標。

這些目標與衝突發生和恢復有關。CPN 模型涵蓋的目標為

- 提出保險索賠人
- 收集資料
- 分享 PHR
- 解決資料衝突
- 解決索賠人衝突。

我們使用 eSourcing 框架的形式化⁶⁹，其中包含工作流程網路 (WF-nets)。因此，利害關係人內部流程的 CPN 模型是有範圍的，所以控制流程類似於 eSourcing formalization。WF-net 定義了單獨個案的動態行為。

⁷⁰Research⁷¹將 WF 網描述為一個 Petri 網，它有一個三元組 $N = (P, T, F)$ ，其中 P 和 T 是兩個不相交的有限集合，分別稱為地方 (圓 可視化) 和 轉換 (矩形表示它們)。
 $F \subseteq (P \times T) \cup (T \times P)$ 是 N 中的流程關係集。
 集合 F 是 N 的子集。

$P \times T$ 表示集合 P 和 T 的笛卡兒積。笛卡兒積由所有可能的有序對組成，其中第一個元素來自集合 P ，第二個元素來自集合 T 。

圖 14 描述了 WF 網，它有一個唯一的起始位置和一個唯一的終止位置，起始位置有一個標記 (所有其他位置為空)。所有節點都從起點引導到終點，當制定完成時，只有一個標記位於唯一的終點，其他地方都是空的。¹¹應該注意的是，WF 網指定了單一案例的動態行為。

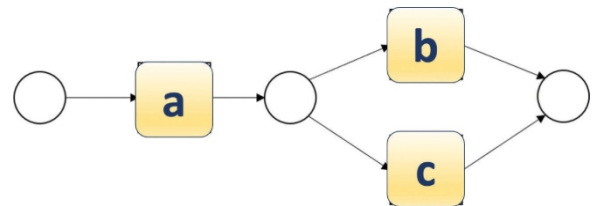


圖 14. 工作流程網範例⁷²

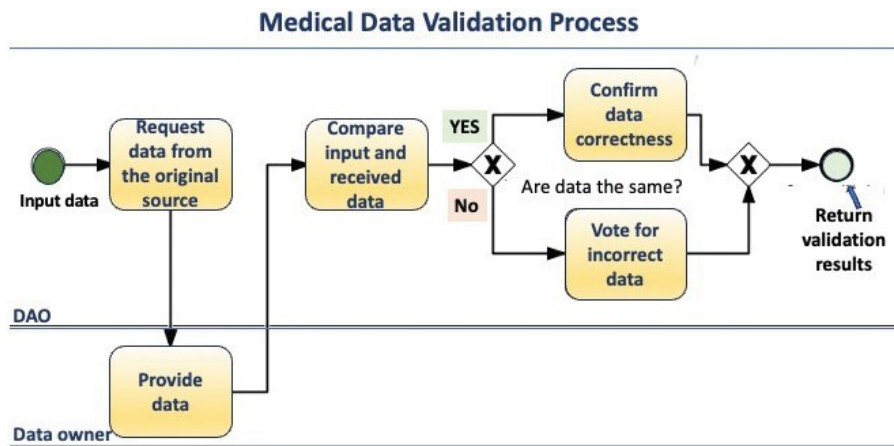


圖 13. 節點資料驗證流程。DAO: 分散式自治組織。

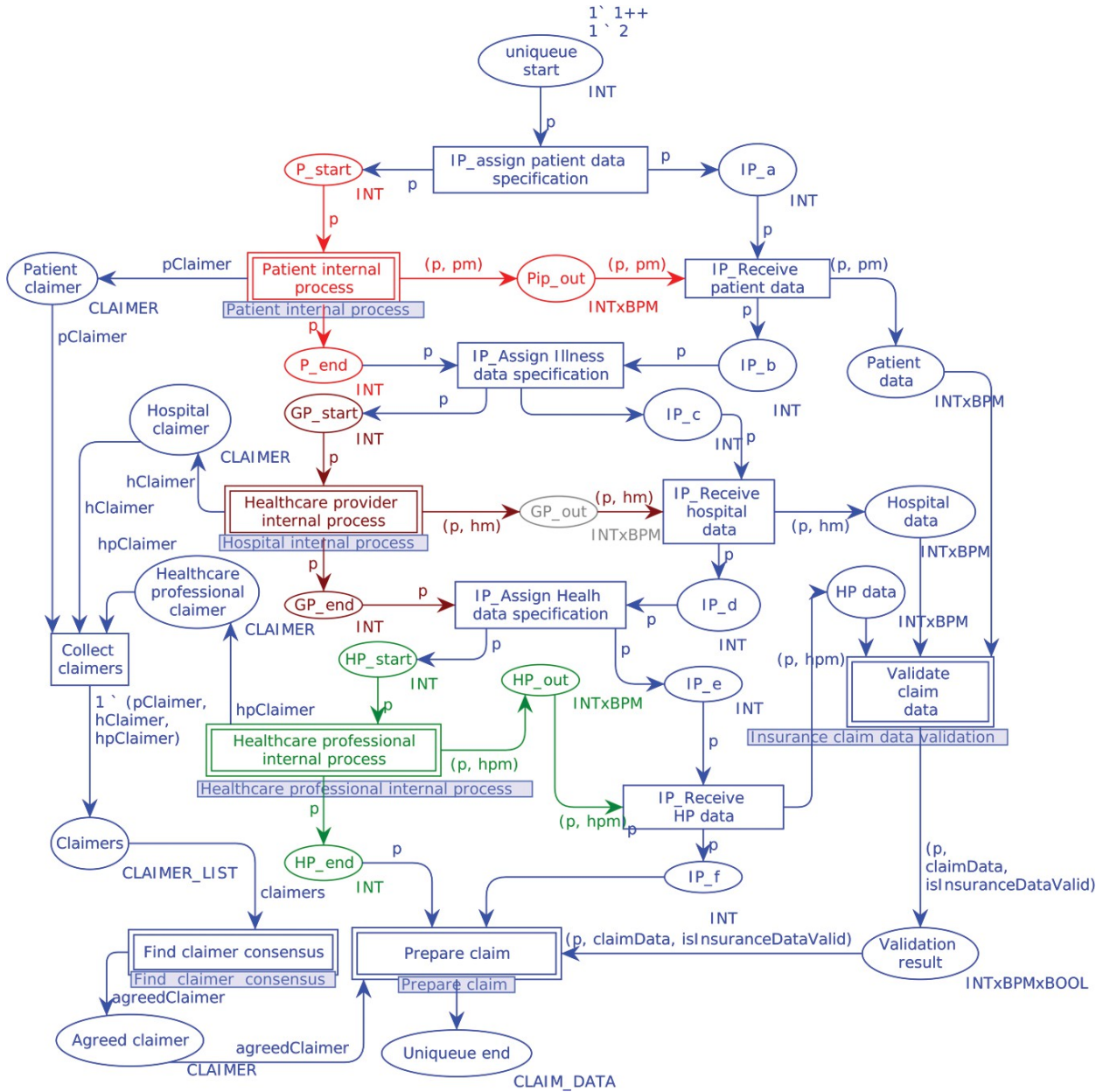


圖 15. CPN 模型的外部層定義了組織間流程。CPN：彩色 Petri 網。

是孤立的。這表示每一項工作都是針對一個特定的案例（也稱為工作流程實例）來執行的⁶⁷。

形式化的頂層設定

圖 15 說明了提出包含多個組織實體的索賠所涉及的程序層面。為了組合醫療索賠，保險提供者從不同來源取得醫療照護資料，例如病患記錄、醫療照護提供者系統，以及醫療照護專家使用的系統。資料收集及索賠人定義內部程序涉及與利害關係人分散式系統的互動。

系統互動。我們對內部流程使用不同的顏色，以便更直觀地顯示組織間流程。病患的內部流程以紅色顯示，醫療照護專業人員以褐色顯示，而醫療照護專業人員則以綠色顯示。

我們的 CPN 模型是以本文前面定義的 BPMN 流程為基礎。整個保險專業人員理賠員定義流程源自於圖 10。定義封裝內部理賠人定義業務邏輯流程的 CPN 層是以 BPMN 流程為基礎。在評估 CPN 模型時，將內部理賠人定義流程模型化可讓衝突發生和模擬成為可能。BPMN 圖表與 CPN 模

型的病人、醫護專業人員和醫護人員層間的映射、

BPMN 圖表與 CPN 模型層之間的對應關係如表 2 所示。

索賠準備流程從獨一無二的起始地點開始，兩個標記描述獨立的流程識別碼。當為每個地點提供流程識別符時，模型設計可支援多個平行的流程執行。保險提供者執行的所有轉換都以藍色標記，並以前綴 IP_ 開始。隨後，啟動 IP_assign 患者資料規格轉換，從而開始患者的內部流程。患者的內部流程有兩個輸出 - 血壓測量和索賠建議。醫療照護提供者和醫療照護專業人員都有相同的工作流程。理賠人定義是基於圖 6 所描述的內部規則。

當執行所有三個內部流程時，會觸發收集申索者的轉換，其中有三個輸入定義了每個利害關係人提出的申索者。尋找索賠者共識轉換會處理所有三個提出的索賠者，並根據共識演算法選擇其中一個。

在準備索賠之前，另一個程序會與索賠人定義 - 收集的血壓測量驗證同時進行。此程序驗證資料的潛在妥協，並隨後解決資料分歧時可能產生的任何差異。在共識演算法與索賠人及血壓測量結果達成一致後，即進行準備索賠轉換。

組織間利害關係人處理整合 EHR 與 PHR 的內部工作流程

為了描繪不同利害關係人的工作流程，我們採用替代轉換，這些替代轉換包含詳細說明與轉換連結的活動的子網路。與轉換連結的子網路通常在學術論述中表示為子頁。使用 CPN 形式主義，可以無限擴展子頁的層級排列，從而方便表達不同複雜程度的系統描述⁷³。

(73)為了強化協作情境，我們利用 CPN 的模擬功能進一步強化協作情境。此外，我們也將衝突情況納入量化模擬模型中。為了組織整體 CPN 模型，²我們將其分為多個子頁，如表 3 所示。

圖 16 是 CPN 工具的截圖，顯示設計模型內子頁面的層級排列。這些子頁面為

²<https://goo.by/JOQJ8>

表 2. 內部申索者定義流程從 BPMN 圖表到 CPN 模型層的內部索賠者定義流程對應。

BPMN 流程	CPN 層
病人-申領者內部決策流程 (圖 8)	病人內部流程
醫療照護提供者申領者內部決策流程 (圖 9)	醫療照護提供者內部流程
醫療照護專業人員聲請者內部決策流程 (圖 10)	醫療照護專業人員內部流程

BPMN: 業務流程模型與符號; CPN: 彩色 Petri 網。

作為可重複使用的元件，有助於提高複雜模型的可理解性。在此架構中，主要頁面 (稱為「外部」) 的角色是界定準備保險理賠的組織間協議。不同利害關係人的內部程序，即病患內部程序、醫院內部程序及醫療照護專業人員內部程序，則包含在不同的子頁面中。衝突的解決是在流程的較高層次上進行，特別是在專門用於保險理賠資料驗證和在理賠人之間達成共識的子頁中。

CPN 模型評估

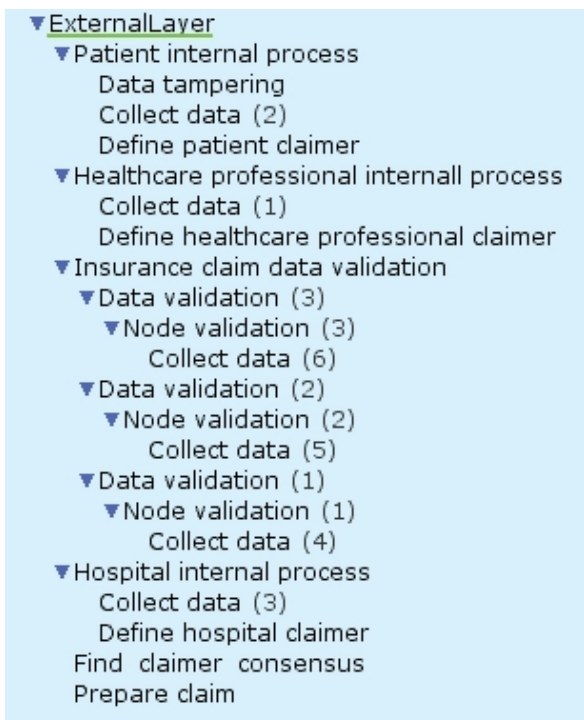
我們使用兩種不同的方法來評估我們的模型。首先，我們在 CPN Tools 中透過模擬來評估原始模型，確保所有初始代幣都導向模型的唯一最終狀態。鑑於所提供 CPN 模型的複雜性，我們針對每個子頁面個別進行狀態空間分析。如果頁面包含任何子頁面，我們會模仿其輸出。此模仿包括以產生常數資料的單一元素取代子頁面的實際執行。如此一來，我們就能保持主頁面流程的完整性，同時降低狀態空間分析的複雜度。預設值是根據子頁面的潛在結果來建立的。在整個狀態空間分析過程中，我們以有向圖表來計算和呈現 CPN 模型的所有可達狀態和狀態變化。圖表將狀態顯示為節點，將發生的事件顯示為弧。狀態空間分析的主要目標是描述系統的行為，並檢查是否有死鎖、給定的狀態是否永遠可達，以及給定的服務是否永遠可提供。

關於狀態空間的報告提供了原點屬性和有效性屬性的說明。前者與特定的原點標記 (home marking) 有關，該標記可從任何可達標記 (reachable marking) 存取。在我們的情境中，每個與子頁面相關的進程最終都會達到它的最終狀態。另一方面，活躍性屬性界定了沒有活動結合元素的標記。沒有活動的標記既可以是死標記，也可以是活標記。

表 3. CPN 模型層級結構中的子頁面。

子頁面	意義
病人內部流程	病人資料收集及索賠者定義流程
醫院內部流程	全科醫師資料收集與申報人定義流程
醫療照護專業人員內部流程	醫療照護專業人員資料收集與申報人定義流程
資料篡改	資料收集過程中發生的資料篡改程序
收集資料	資料收集過程
定義病人申領者	定義病人申報者的流程
定義醫療照護專業人員聲稱者	醫療照護專業人員索賠者定義流程
定義醫院索賠人	醫院理賠人定義過程
保險理賠資料驗證	驗證從不同利益相關者收集的所有資料的流程
資料驗證	由多個節點驗證血壓測量的流程
節點驗證	由單一節點執行的血壓量測驗證流程
尋找索賠者共識	最終申索人共識程序

CPN: 彩色 Petri 網。



。這些過渡

圖 16. CPN 模型頁層結構。CPN: 彩色 Petri 網。

和原點標記同時出現，因為任何標記都可以透過零長度的瑣碎出現序列從自身存取。在此之後，狀態空間報告會描繪出活躍的轉換。在學術層面，當一個轉換可以從任何可達到的標記中，找出包含這個轉換的出現序列，這個轉換就被認為是活的。狀態空間報告提供無效轉換的說明。如果轉換不是啟用就是無法達成，就會被歸類為非活動轉換

74。

所有分析狀態空間的報告都是基於 CPN 模型中的每個子頁面，如後面提供的對應表格所示。狀態空間分析報告的原始檔案可在線上取得。

根據表 4 所示的結果，很明顯在資料收集過程中存在固有的循環。資料儲存庫包含各種流程的相關資訊，而資料收集流程會持續擷取資料，直到找到與進行中的流程相關的資訊為止。在我們的流程中，所有的子頁面都不包含任何死活轉換，表示沒有未使用的元件。值得注意的是，所有子頁面的狀態都與 home 和 dead 標記的狀態一致。

*運行案例的概念驗證原型實作*本研究將介紹參考文獻中開發的電子健康資料分享流程⁷⁵的原型實作。76.在我們的特定情況下，我們建議在保險提供者系統中使用 Polygon⁷⁷智慧契約 (SC)。同時，Ethereum SCs 也被推薦用於病人、醫院和醫療保健專業人員系統。Polygon 網路建立在高吞吐量的區塊鏈架構上，每個檢查點選擇一組區塊生產者來達成共識。區塊的驗證透過 PoS 層進行，PoS 層也會定期以區塊製造者提供的證明更新 Ethereum 主網路。為了增強可擴展性，並使不同的區塊鏈系統之間能夠互通，我們採用了 Polkadot，⁷⁸它促進了專門區塊鏈之間安全且無信任的通訊。

³<https://goo.by/QaISC>

表 4. CPN 模型子頁面的狀態空間分析結果。

子頁面	迴圈	原點標記	死標記	死轉換	活轉換
病人內部流程	無	是	是	是	無
醫療照護專業人員內部流程	無	是	是	是	無
醫院內部流程	是	是	是	是	無
定義病人申領者	無	是	是	是	無
定義醫療照護專業人員聲請人	無	是	是	是	無
定義醫院索賠人	是	是	是	是	無
尋找申索人共識	是	是	有	是	無
收集資料	是	是	是	是	無
資料篡改	無	無	有	無	無
資料驗證	無	是	是	是	無
節點驗證	無	有	有	無	無
外部層	無	有	有	無	無
準備索賠	無	是	是	是	無

CPN: 彩色 Petri 網。

在 Polkadot 基礎層促成的分散式網路環境中，使用者可行使對其資料的權限。此原型包含三個基於區塊鏈的主要元素。具體來說，它包含兩個不同的應用程式，用於輸入醫療記錄，即病人和醫生的記錄。此外，它還包含一個應用程式，用來執行涉及保險提供者的組織間程序，以及一個 DAO 智慧合約，用來在發生衝突時進行資料比較，並提供可靠的資料。正在考慮的 PoC 原型著重於病人和醫生輸入血壓測量值的情況。

圖 17 展示病人應用程式介面的截圖，明確顯示血壓測量的輸入。此應用程式與 Metamask 電子錢包整合，可透過智慧契約分享輸入的資料。值得注意的是，此應用程式結合了在 Ethereum Blockchain 上部署智慧型契約。

圖 18 直觀呈現了收集資料時發生的衝突。所描述的情境舉例說明病人記錄的血壓值與醫生記錄的血壓值之間的差異。在這種情況下，資料會傳送到 DAO，由 DAO 負責驗證資料並解決任何潛在的衝突。

組織間的流程是透過 Polkadot parachain 來實作的，它可以進行跨區塊鏈通訊。⁷⁹ 保險提供者的應用程式以 Substrate 後端本地節點的方式執行。

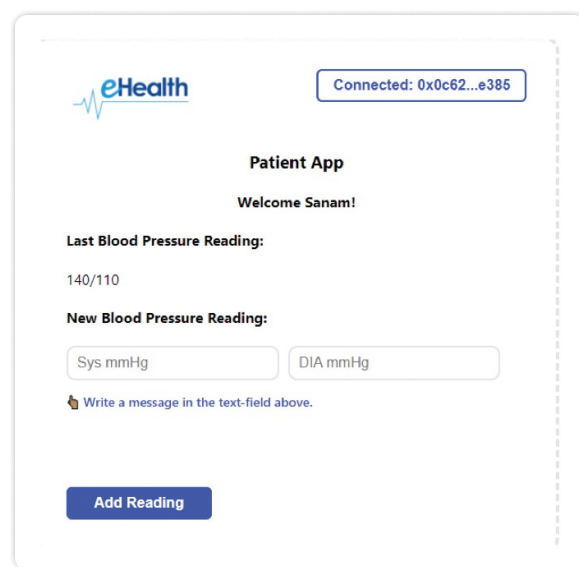


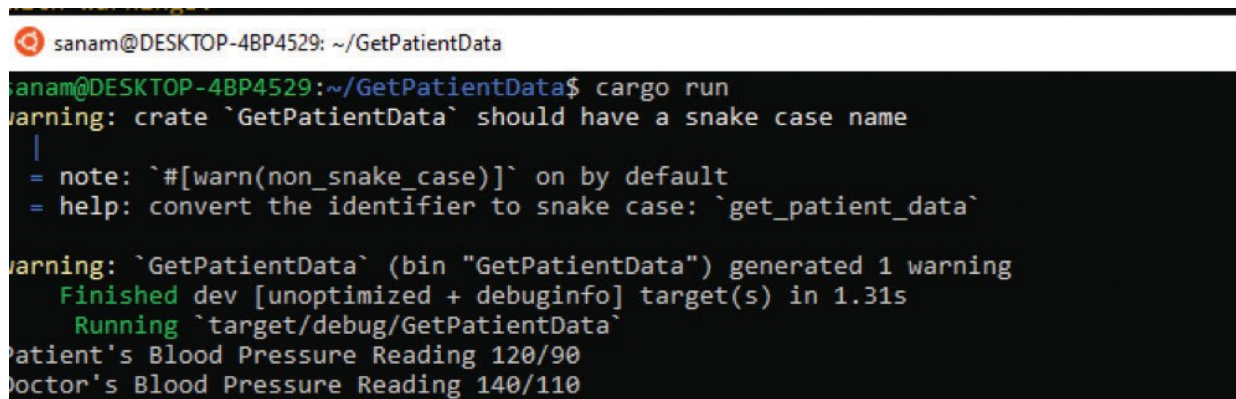
圖 17. 病人應用程式的截圖。

類似作品的研究意涵討論

本研究提出，區塊鏈能夠在沒有單一信任點的情況下透明地自動解決衝突。此外，區塊鏈與智慧契約技術可支援個人化的電子醫療服務，包括多個利害關係人，同時確保個人對醫療資料的所有權。M2X 經濟的興起以及組織間流程中的非人為代理需要基於多因素挑戰集機制的新驗證方法。這種方法可以在利益相關者之間缺乏信任的情況下，實現新的組織間流程。CPN 的評估顯示，以分散式電子醫療保險為例，這樣的流程是可行的。不過，我們仍沒有實際

經驗證明這是可行的。

基於區塊鏈的系統中記錄的隱私衝突解決。



```

sanam@DESKTOP-4BP4529: ~/GetPatientData
sanam@DESKTOP-4BP4529:~/GetPatientData$ cargo run
warning: crate `GetPatientData` should have a snake case name
|
| = note: `#[warn(non_snake_case)]` on by default
| = help: convert the identifier to snake case: `get_patient_data`
|
warning: `GetPatientData` (bin "GetPatientData") generated 1 warning
    Finished dev [unoptimized + debuginfo] target(s) in 1.31s
    Running `target/debug/GetPatientData`
Patient's Blood Pressure Reading 120/90
Doctor's Blood Pressure Reading 140/110

```

圖 18. 保險提供者的資料收集截圖。

本論文提出了體外可行性證明。在分散式電子醫療中自主解決衝突的可能性，可讓個人的健康資料以可信任且透明的方式在不同產業中得到有價值的使用。最後，PoC 原型的實作顯示，運行中的案例可以在目前最先進的分散式技術中實作。

我們的研究是基於 Narendra 和同事的工作，¹¹其中作者提出根據衝突的類型，以協商的方式解決衝突。本研究提供虛擬企業 (VE) 中團結自主參與者的架構，該架構提出分層結構，呈現不同的商業邏輯內容。研究顯示衝突發生在企業間、外部層。我們的論文將文獻 11 中定義的方法應用於電子醫療領域。11 中定義的方法。醫療保健用例證實衝突發生在組織間協作層，因為不同的利害關係人可能擁有彼此不同的電子健康資料。此外，每個利害關係人的商業決策也可能與其他利害關係人不同，因為所有參與者都有自己的內部流程。

Stahnke 及其同事⁸⁰指出，區塊鏈技術能夠強制執行組織間的工作流程。為了建立組織間流程中所有利益相關者都能接受的可靠工作流程，有必要使用 CPN 設計和驗證這些工作流程，然後再將其轉換為智慧合約。在使用 CPN 驗證組織間流程的同時，必須承認與法律相關的智慧契約需求以及必要的支援。

Park 及其同事的研究⁸¹建議將企業資源規劃 (ERP) 系統納入業務流程模擬模型，以便在 CPN 設計的模擬流程中使用真實生活資料。Park 和 van der Aalst⁸¹的目標是要克服 ERP 系統的複雜性，方法是實施一個框架，將 ERP 系統整合到模擬流程中。然而，我們

由於電子健康資料的敏感性，我們避免在模擬中引入現實生活中的元件。此外，我們假設參與組織間電子健康流程的利害關係人及其內部系統數量不限。因此，個別系統的整合不會產生任何額外的價值。

在他們的工作中，Jadav 及其同事⁸²著重於使用 AI 來發現可穿戴式攻擊，並與公共區塊鏈分享醫療照護資料。作者建議使用區塊鏈技術來實現資料的不可變性。在我們的研究中，我們也指出區塊鏈技術可實現電子健康資料的不可篡改性，但我們並未專注於使用人工智能來發現資料篡改。不過，本文所提出的組織間流程設計仍允許整合非人類參與者，例如 AI 代理。

Kim 和 Kim⁸³提出的 DeepBlockShield 框架旨在利用區塊鏈技術解決醫療資料洩漏問題。相應的解決方案建議將資料儲存在區塊鏈上，同時提供特殊代理人存取。在我們的研究中，我們假設醫療資料不僅可以儲存在區塊鏈上，並提出 MFSSIA 架構，以建立不同利害關係人在分享電子健康資料時的安全協作。

Abbas 及其同事⁸⁴最近的一項研究提出了一個可穿戴裝置資料安全分享與存取的框架，利用區塊鏈技術來確保互連節點之間的資料傳輸安全與管理。作者從準確度、精確率、平均信任值及回應時間等方面評估其研究成果的有效性。在我們的研究中，我們採用了正式的 CPN 工具來評估設計流程，並確保沒有設計問題。此外，我們所設計的流程除了著重解決安全性問題之外，也著重於解決資料處理上的衝突。

本文主要針對 區塊鏈 在醫療保健 資料管理 的技術層面進行探討，特別是在整合個人與電子病歷資料

方面。

基於區塊鏈的系統中記錄的隱私衝突解決。

管理，特別是在整合個人和 EHR 方面。鑑於此技術方向，本研究不直接涉及人類受試者，也不收集種族或人種為相關因素的資料。

在這種情況下，研究的重點在於技術開發而非人類主體，因此收集種族或民族資料並不適用。我們的研究更關心醫療照護資料整合的系統與技術挑戰及解決方案，而非終端使用者的人口特徵。然而，在更廣泛的部署環境中，這些因素會影響醫療照護技術的實施及其社會影響。

結論

在本文中，我們利用區塊鏈技術研究分散式電子醫療保健系統中的自動衝突解決機制。後者可實現自主且透明的組織間流程以及可信賴的衝突解決機制，而無需涉及中央機關。我們所提出的方法是基於數個科學方法，例如 DSR、CPN 建模，以及框架，例如 T-DM、eSourcing 和 MFSSIA。我們使用 T-DM 來定義基於區塊鏈的系統需求，為系統的架構設計、定義鏈上交易集的代幣經濟以及動態協議開發奠定基礎。此外，我們將 T-DM 定義的功能目標與 BPMN 流程的衝突點對應。最後，我們使用 CPN 評估我們的研究成果，因為 CPN 驗證了 T-DM 在執行流程中定義的衝突解決概念。我們的評估包括運行案例的 PoC 原型實作。透過 CPN 與原型的 PoC 評估，我們確保研究成果可以用於即時流程中。

我們建議在處理個人電子健康資料並將其對應到組織間流程時，使用 DAO 作為衝突自動解決程式。自動解決衝突的要求是由分散環境中的多個利害關係人建立 PHR 和 EHR 資料。這些利害關係人應加入 MFSSIA 並經過認證，以同意 DAO 使用的電子健康資料共用和使用衝突解決技術。來自不同來源的電子健康資料應在使用前合併。在定義電子健康資料蒐集與處理的需求後，我們提出兩種衝突-內部業務規則與資料差異衝突。最後，我們提出在資料差異衝突的情況下，分散式系統會由多個節點重新檢查資料，然後決定哪些資料是正確的。

我們的研究有幾個固有的限制。首先，我們需要在組織間資料分享流程的背景下，全面評估整合式 MFSSIA。此外，本研究

此外，本研究並未徹底界定實施電子醫療系統所面臨的特定挑戰。此外，代幣經濟的概念涉及內容製造者與貢獻價值的服務使用者分享社群收入，這已超出本文的研究範圍。因此，代幣經濟和交易成本的問題不在我們的研究範圍內。

保護使用者資料隱私是最重要的，否則會有法律上的影響。然而，本研究並未探討與使用者資料隱私保護相關的法律層面。因此，建議技術的接受與實施，將取決於國家的法律管轄權以及醫院是否遵守相關法律法規。

我們致力於 MFSSIA 的電子醫療特定挑戰設定規則。在實作 PoC 原型之後，我們計劃與醫療照護提供者合作，以真實的使用案例來測試我們的研究成果。此外，未來的工作還包括解決與社會行政環境的異質性相關的挑戰。在建議的設計中，我們以不可變的智慧型契約定義權利人之間的協議。未來的工作是以電子醫療智慧契約生命週期的發展來克服這項挑戰，讓現實生活中的協議變更為智慧契約所定義的協議。

最後，電子健康照護資料的互通性是電子健康照護最大的挑戰之一。使用共通標準，例如 SNOMED CT、HL7、LOINC 等，可以解決這個問題。與此同時，由於我們認為組織間的流程具有彈性，可支援無限數量的利害關係人，因此存在與資料隱私和互操作性相關的挑戰。我們假設 M2X 情境中的人類與非人類參與者都必須透過 MFSSIA 架構進行驗證，才能存取這些流程。由於 MFS-SIA 使用挑戰集和回應式身分驗證，因此支援的電子健康資料標準可成為未來開發的挑戰集的一部分。未來的工作還包括採用可在不同組織間流程階段使用的 AI 代理，例如 MFSSIA 驗證、電子健康資料收集和衝突解決，還有更多工作有待進行。

經費聲明

無資金。

財務及非財務關係與活動

Norta 博士是 BHTY 編輯委員會成員，無其他公開資訊。

貢獻者

所有作者對本文皆有貢獻。Aleksandr Kormilt-syn 撰寫文章並進行研究。Alex Norta 監督了文章並提供了反饋意見。Chibuzor Udokwu 和 Vimal Dwivedi 編輯了本文並提供了反饋意見。Sanam Nisar 開發了概念驗證原型。

參考文獻

- Susskind RE, Susskind D. The future of the professions: how technology will transform the work of human experts. 牛津大學出版社; 2015 年。
- Mercille J. 1980 年以來愛爾蘭醫院部門的私有化。J Public Health.2018; 40:863-70. <https://doi.org/10.1093/pubmed/fty027>
- Archer N, Fevrier-Thomas U, Lokker C, McKibbin KA, Straus SE. 個人健康記錄：廣泛評論。J Am Med Inform Assoc. 2011;18:515-22. <https://doi.org/10.1136/amiainl-2011-000105>
- Leviton B, Getz K, Eisenstein EL, Goldberg M, Harker M, Hes-terlee S, et al. Assessing the financial value of patient engagement: a quantitative approach from CTTI's Patient Groups and Clinical Trials project. Ther Innov Regul Sci. 2018;52:220-9. <https://doi.org/10.1177/2168479017716715>
- Dimitrov DV. 醫療物聯網和醫療大數據。Healthc Inform Res. 2016;22:156-63. <https://doi.org/10.4258/hir.2016.22.3.156>
- Kormiltsyn A, Udokwu C, Karu K, Thangalimodzi K, Norta A. 使用智慧契約改善醫療照護流程。In: Pro-ceedings of the international conference on business information systems. Springer, 2019; pp.
- Norta A, Hawthorne D, Engel SL. 具有所有權與貨幣化能力的隱私保護 da-ta 交換錢包。In: Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN). IEEE, 2018; pp.
- Eccher C, Piras EM, Stenico M. TreC - a REST-based Regional PHR. User Centred Networked Health Care A. Moen et al. (Eds.) IOS Press, 2011. <https://doi.org/10.3233/978-1-60750-806-9-108>
- Urbauer P, Sauer mann S, Frohner M, Forjan M, Pohn B, Mense A. IHE/Continua 元件對 PHR 系統的適用性：從經驗中學習。Comput Biol Med. 2015;59:186-93. <https://doi.org/10.1016/j.combiomed.2013.12.003>
- 張瑞，劉立。醫療應用雲的安全模型與需求。In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing. IEEE, 2010; pp.
- Narendra NC, Norta A, Mahunnah M, Ma L, Maggi FM. 虛擬企業協作的健全衝突管理與解決方案。2016;10:233-51. <https://doi.org/10.1007/s11761-015-0183-0>
- Szabo N. Smart contracts: Building blocks for digital markets. EXTROPY J Transhumanist Thought. 1996;18:2.
- 歐盟。歐盟基本權利憲章 [Internet]. Europa.eu; 2012 [cited 2023 Jun 15]. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT>
- Standard Contractual Clauses (SCC) [Internet]. 歐洲委員會-European Commission。 [cited 2023 Jun 15]. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
- 哈希函數作為個人資料偽化技術簡介。European Data Protection Supervisor [Inter-net]. 2023 [cited 2023 Nov 15]. Available from: https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en
- Sun W, Cai Z, Li Y, Liu F, Fang S, Wang G. Security and Privacy in the Medical Internet of Things: a review. Secur Commun Netw. 2018;2018:5978636. <https://doi.org/10.1155/2018/5978636>
- Al-Muhtadi J, Shahzad B, Saleem K, Jameel W, Orgun MA. 在多雲環境中運作的社會整合醫療保健應用程式的網路安全與隱私權問題。 <https://doi.org/10.1177/1460458217706184>
- Katurura M, Cilliers L. A review of the implementation of elec-tronic health record systems on the African continent. In: Pro-ceedings of the African Computer and Information System & Technology Conference. 2017; pp.
- Cilliers L. Wearable devices in healthcare: privacy and information security issues. Health Inf Manag J. 2019; 49(2-3):150-6. <https://doi.org/10.1177/1833358319851684>
- Luo E, Bhuiyan MZA, Wang G, Rahman MA, Wu J, Atiqz-zaman M. Privacy protector: Privacy-protected patient data collection in IoT-based healthcare systems. IEEE Commun Mag. 2018;56:163-8. <https://doi.org/10.1109/MCOM.2018.1700364>
- Hussein AF, ArunKumar N, Ramirez-Gonzalez G, Abdulhay E, Tavares JMR, de Albuquerque VHC. 基於遺傳演算法和離散小波轉換形式支援的醫療記錄管理和安全區塊鏈系統。 Cogn Syst Res. 2018;52:1-11. <https://doi.org/10.1016/j.cogsys.2018.05.004>
- Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. Fhir-chain: Application blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J. 2018;16:267-78. <https://doi.org/10.1016/j.csbj.2018.07.004>
- Azorin-Lopez J, Fuster-Guillo A, Saval-Calvo M, Bradley D. Home technologies, smart systems and eHealth. In: 機電未來。 Springer, 2016; pp.
- Dittmar A, Meffre R, De Oliveira F, Gehin C, Delhomme G. Wearable medical devices using textile and flexible technologies for ambulatory monitoring. In: 2005 IEEE 醫學與生物工程第 27 屆年會論文。 IEEE, 2006; pp.
- Sebestyen G, Hangan A, Oniga S, Gál Z. 物聯網背景下的電子健康解決方案。 In: 2014 IEEE 自動化、品質與測試、機器人國際會議論文集。 IEEE, 2014, pp.
- Salehi S, Giacalone M. Conflict resolution with equitable algorithms: a tool to establish a European common ground of available rights. In: F. Romeo, S. Martuccelli & M. Giacalone (Eds.). The European common ground of available rights.那不勒斯: Edizionale Scientifica; 2009, p.111.
- Xu H, Hipel KW, Kilgour DM, Fang L. 使用圖形模型解決衝突：競爭與合作中的策略互動。 Springer, 2018.
- Neyens G. 自主系統的衝突處理。 In: Pro-ceedings of the 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W). IEEE, 2017; pp.
- Priya KF, Patil NN. 解決線上社群網路中維護隱私權政策的隱私權衝突。 Int J Comput Eng Technol. 2019;10:94-101. <https://doi.org/10.34218/IJCET.10.3.2019.011>
- Hölbl M, Kompara M, Kamišalić, A, Nemeč Zlatolas L. A systematic review of the use of blockchain in healthcare. 對稱。 2018;10:470. <https://doi.org/10.3390/sym10100470>

31. Agbo CC, Mahmoud QH, Eklund JM. 區塊鏈技術在醫療保健中的應用：系統性評論。In: Proceedings of the health-care. 多學科數位出版研究所, 2019; Vol. p.56.
32. McGhin T, Choo KKR, Liu CZ, He D. Blockchain in health-care applications: research challenges and opportunities. *J Netw Comput Appl.* 2019;135:62-75. <https://doi.org/10.1016/j.jnca.2019.02.027>
33. Swan M. Blockchain: blueprint for a new economy. O'Reilly Media, Inc; 2015.
34. Buterin V. A next generation smart contract & decentralized application platform. 白皮書。Ethereum Foundation; 2013.
35. Becker G. 梅克尔签名方案、梅克尔树及其密码分析。Ruhr-University Bochum, Tech.Rep; 2008.
36. Hevner A, Chatterjee S. Information Systems Design Science Research. 資訊系統整合系列。2010; pp.
37. Westaway MD, Stratford PW, Binkley JM. 患者特定功能量表：在頸部功能障礙患者中的使用驗證。 *J Orthop Sports Phys Ther.* 1998; 27:331-8. <https://doi.org/10.2519/jospt.1998.27.5.331>
38. Nguyen GT, Kim K. 區塊鏈中使用的共識演算法調查。 *J Inf Process Syst.* 2018;14:101-28.
39. Bitcoin-Open source P2P money [Internet]. bitcoin.org.[cited 2023 Jun 15]. 網址: <https://bitcoin.org>
40. 首頁|Ethereum [Internet]. Ethereum.org.2019 [於 2023 年 6 月 15 日引用]。網址: <https://www.ethereum.org>
41. Hyperledger Fabric-Hyperledger [Internet].Hyperledger; 2017 [cited 2023 Jun 15].Available from: <https://www.hyperledger.org/projects/fabric>
42. Udokwu C, Kormiltsyn A, Thangalimodzi K, Norta A. The state of the art for blockchain-enabled smart-contract applications in the organization.In : Proceedings of the 2018 Ivannikov Ispras Open Conference (ISPRAS).IEEE, 2018; pp.
43. Weyl EG, Ohlhaber P, Buterin V. Decentralized Society：尋找 Web3 的靈魂。 Available at SSRN 4105763 2022.
44. 專題報告 [網際網路]. 網址 : https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf
45. Damjan M. The interface between blockchain and the real world.In : *Ragion pratica.* 2018; pp.
46. Caldarelli G, Ellul J. The blockchain oracle problem in decentralized finance-a multivocal approach. *Appl Sci.* 2021; 11:7572. <https://doi.org/10.3390/app11167572>
47. Liu L, Zhou S, Huang H, Zheng Z. From technology to society: an overview of blockchain-based DAO. *IEEE Open J Comput Soc.* 2021.
48. Grefen P, Aberer K, Hoffner Y, Ludwig H. CrossFlow: 動態虛擬企業中的跨組織工作流程管理. *Comput Syst Sci Eng.*
49. Rahmani AM, Thanigaivelan NK, Gia TN, Granados J, Negash B, Liljeberg P, et al. Smart e-health gateway: Bring intelligence to Internet-of-things based ubiquitous health-care systems.In : Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC).IEEE, 2015; pp.
50. Leiding B, (sup) Dieter Hogrefe, Clemens HC, Norta A. The M2X economy-business interactions, transactions and collaborations among autonomous smart devices. 博士論文, Georg-August-Universitaet Goettingen, 2019.
51. Shiang CW, Meyer JJ, Taveter K. Agent-oriented methodology for designing cognitive agents for serious games. *Engineering multi-agent systems.* 2016; p. 39.
52. Barr ET, Harman M, McMinn P, Shahbaz M, Yoo S. The oracle problem in software testing: a survey. *IEEE Trans Softw Eng.* 2014; 41:507-25. <https://doi.org/10.1109/TSE.2014.2372785>
53. Norta A, Mahunnah M, Tenso T, Taveter K, Narendra NC. 以代理為導向的大型社會-技術-服務-裝置-生態系統設計方法。In: IEEE, 2014; pp.IEEE, 2014; pp.
54. Sherkat M, Mendoza A, Miller T, Burrows R. Emotional attachment framework for people-oriented software. ArXiv pre-print arXiv:1803.08171 2018.
55. Kormiltsyn A. A systematic approach to define requirements and engineer the ontology for semantically merging data sets for personal-centric healthcare systems. 2018.
56. Sherkat M. 軟體工程中的情感主義。博士論文, 2019.
57. Mendoza A, Miller T, Pedell S, Sterling L, et al. The role of users' emotions and associated quality goals on appropriation of systems: two case studies.In: 第 24 屆澳大利亞資訊系統會議論文集。2013.
58. Avizienis A, Laprie JC, Randell B, Landwehr C. 可靠與安全運算的基本概念與分類。 *IEEE Trans Dependable Secure Comput.* <https://doi.org/10.1109/TDSC.2004.2>
59. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big Healthcare Data: preserving security and privacy. *J Big Data.* 2018;5:1. <https://doi.org/10.1186/s40537-017-0110-7>
60. Fulpagare Priya K, Patil NN. 用於保護社交媒體隱私的衝突檢測技術。 2018.
61. Udokwu C, Norta A. Deriving and formalizing requirements of decentralized applications for inter-organizational collaborations on blockchain. 2021;46:8397-8414. <https://doi.org/10.1007/s13369-020-05245-4>
62. Jensen K, Kristensen LM. 彩色 Petri 網：並發系統的建模與驗證。 Springer Science & Business Media, 2009.
63. Mahunnah M, Norta A, Ma L, Taveter K. Heuristics for de-signing and evaluating socio-technical agent-oriented behaviour models with coloured petri nets.In : Proceedings of the Computer Software and Applications Conference Workshops (COMP-SACW), 2014 IEEE 38th International. IEEE, 2014; pp.
64. Norta A, Kormiltsyn A, Udokwu C, Dwivedi V, Aroh S, Ni-kolajev I. A blockchain implementation for configurable multi-factor challenge-set self-sovereign identity authentication.In: Ezzat SK, Saleh YN, Abdel-Hamid AA (Eds.). *Blockchain Oracles: state-of-the-art and research directions.* IEEE Access; 2022.
65. Riley L. Universal DLT interoperability is now a practical reality. Hyperledger Foundation Blog [Internet]. 2021 [於 2023 年 10 月 7 日引用]。 Available from: <https://www.hyperledger.org/blog/2021/05/10/universal-dlt-interoperability-is-now-a-practical-reality>
66. Kormiltsyn A, Norta A. Dynamically integrating electronic-with personal health records for ad-hoc healthcare quality improvements.In: 數位轉型與全球社會國際研討會論文集。 Springer, 2017; pp.385-99.
67. Norta AH. 探索動態組織間業務流程協作 [網際網路]。 2007 [2023 年 10 月 7 日引用]。 Available from: <https://research.tue.nl/files/2003544/200710444.pdf>
68. Kormiltsyn A, Norta A. Formal evaluation of privacy-conflict resolution for integrating personal-and electronic health records in blockchain-based systems. 技術報告。 2022.

69. Norta A, Eshuis R. 和諧化業務流程協作的規範與驗證. *Inf Syst Front.*2010;12:457–79. <https://doi.org/10.1007/s10796-009-9164-1>
70. 趙 F, 向 D, 劉 G, 江 C. 測量 WF 網系統行為一致性程度的新方法. *IEEE Trans Comput Soc Syst.*<https://doi.org/10.1109/tcss.2021.3099475>
71. Weidlich M. Behavioural profiles: a relational approach to behaviour consistency. 博士論文, 波茨坦大學; 2011 年。
72. 工作流程網路-ML 維基 [網際網路]。[cited 2023 Jul 11]. Available from: http://mlwiki.org/index.php/Workflow_Nets
73. Gehlot V, Sloane E, Thalassinidis AE. 個人健康技術：基於 CPN 的協調鄰里照護環境 (hubs) 與個人照護裝置生態系統建模. 2019.
74. Jensen K, Kristensen LM, Wells L. Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. *2007*;9:213-54. <https://doi.org/10.1007/s10009-007-0038-x>
75. sanamisarmalik. sanamisarmalik/hprivacyconflictresolutionbyblockchain [Internet]. GitHub. 2022 [cited 2023 Sep 25]. Available from: <https://github.com/sanamisarmalik/hprivacyconflictresolutionbyblockchain>
76. Nisar S. Defining blockchain-based techniques for privacy conflict-resolution in cross-organizational processes for e-health systems. 碩士論文, University of Tartu, Faculty of Science and Technology Institute of Computer Science; 2022.
77. 大量採用的區塊鏈 [網際網路]。[cited 2023 Jun 15]. 網址：<https://polygon.technology>
78. Polkadot: Web3 Interoperability | Decentralized blockchain [Internet]. Polkadot Network. [cited 2023 Oct 4]. 網址：<https://www.polkadot.network/>
79. Substrate And Polkadot | Substrate_ [Internet]. substrate.io. [cited 2023 Jun 15]. Available from: <https://substrate.io/vision/substrate-and-polkadot/>
80. Stahnke S, Shumaiev K, Cuellar J, Kasinathan P. Enforcing a crossorganizational workflow: an experience report. In: Proceedings of the Enterprise, Business-Process and Information Systems Modeling: 21st International Conference, BPMDS 2020, 25th International Conference, EMMSAD 2020, Held at CAiSE 2020, Grenoble, France, June 8-9, 2020, Proceedings 21. Springer, 2020; pp.85-98.
81. Park G, van der Aalst WM. Towards reliable business process simulation: a framework to integrate ERP systems. In Proceedings of the Enterprise, Business-Process and Information Systems Modeling: 22nd International Conference, BPMDS 2021, and 26th International Conference, EMMSAD 2021, Held at CAiSE 2021, Melbourne, VIC, Australia, June 28-29, 2021, Proceedings. Springer, 2021; pp.
82. Jadav D, Jadav NK, Gupta R, Tanwar S, Alfarraj O, Tolba A, et al. A trustworthy healthcare management framework using amalgamation of AI and blockchain network. *數學*。 2023;11:637. <https://doi.org/10.3390/math11030637>
83. Kim J, Kim M. DeepBlockShield: blockchain agent-based secured clinical data management model from the deep web environment. *Mathematics.* 2021;9:1069. <https://doi.org/10.3390/math9091069>
84. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Al-mansour FM. 用於健康資訊分析的區塊鏈輔助安全資料管理框架。

版權所有： 本文為開放存取文章，依據創用 CC BY-NC 4.0 授權條款發佈，該授權條款允許他人非商業性地散佈、改編、增強本作品，並以不同條款授權其衍生作品，但必須適當引用原作，且使用為非商業性。請參閱：<http://creativecommons.org/licenses/by-nc/4.0>。

附錄

3 元組 N: Antuple 是數字的有限序列或有序列表，或更廣泛而言，數學物件，稱為**元組中的元素**。3 元組稱為三元組 (或三元組)。數字 n 可以是任何非負整數。

面向代理建模 (AOM): 用於組織和資訊系統的建模，提供流程的意向性描述，作為行動者之間的關係網路。因此，它們捕捉並表示目標、依存關係、意向、信念、替代方案等。

演算決策系統 (ADS): 將決策與執行委託給機器。

雙方圖: 一種圖形，其頂點可分為兩個互不相連的集合，使得所有的邊都能將一個集合中的頂點連接至另一個集合中的頂點。

業務流程模型與符號 (BPMN): 用於在業務流程模型中指定業務流程的圖形表示法。

彩色 Petri 網 (CPN)⁶⁹模型: Petri 網的數學概念的向後相容延伸。

彩色 Petri 網 (CPN): 擴充了一般 Petri 網的詞彙，並增加了使其適用於大型系統建模的功能。

版權所有: 這是一篇依據創用 CC BY-NC 4.0 授權條款散佈的開放存取文章，該授權條款允許他人非商業性地散佈、改編和增強本作品，並授權其衍生作品使用不同條款，但必須適當引用原作，且使用目的為非商業性。請參閱：<http://creativecommons.org/licenses/by-nc/4.0>。

分散式自治組織 (DAO): 由於沒有中央機關，所有成員都參與決策的實體。

歐盟基本權利憲章第 7 條: 根據《歐盟基本權利憲章》的定義，¹³第 7 條是任何個人尊重其私人 and 家庭生活、住宅和通信的權利。

DeepBlockShield: 實現臨床資料安全分享的模型。它採用雙向使用者驗證和非同步資訊提供方法，以加強臨床資料的安全性。

設計科學研究循環: 包括六個步驟的流程：發現問題與動機、解決方案的目標、設計與開發、評估與溝通。

設計科學研究 (DSR): 研究發明一種新的有目的的藝術品，以解決一般類型的問題，並評估其對解決該類型問題的效用。

電子健康 (EHR): 由醫療照護專業人員建立並以數位方式儲存的病患資料。

企業資源規劃 (ERP): 組織用來管理日常活動和簡化業務流程的一種軟體。ERP 系統將不同部門的各種功能，例如財務、人力資源、採購、製造、供應鏈管理等，整合到單一的統一平台。

Ethereum 主網: 主要的公共 Ethereum 生產區塊鏈，實際價值的交易發生在分散式帳簿上。Ethereum 使用權益證明 (PoS)，其驗證並非基於解決數學問題所花費的資源，而是基於節點的聲譽。

歐洲資料保護委員會 (EDPB): 具有法人地位的歐盟獨立機構，其目的是確保《一般資料保護條例》的一致應用，並促進歐盟資料保護機構之間的合作。

解決衝突的圖形模型 (GMCR): 在競爭環境中，用於策略管理的靈活工具。

Health Level Seven International (HL7): 一種臨床結果報告標準，目前在世界各地的醫療保健系統中無處不在。

隱马尔可夫模型 (HMM): 序列模型。也就是說，給定一連串的輸入，例如字詞，HMM 會計算一連串相同長度的輸出。HMM 模型是一個圖形，其中節點是標籤和邊緣的概率分布，提供從一個節點轉換到另一個節點的概率。

物聯網 (IoT): 連接裝置的集體網路，以及促進裝置與雲端之間以及裝置本身之間通訊的技術。

邏輯觀察識別名稱與代碼 (LOINC®): 對於實驗室檢驗單與檢驗結果非常重要的臨床術語，也是美國聯邦政府用於臨床健康資訊電子交換系統的一套指定標準之一。

Merkle 樹或散列樹: 確保儲存在區塊鏈上的交易透過數學切細值相互關聯。

Metamask 皮夾: 用於與 Ethereum 區塊鏈互動的軟體加密貨幣錢包。

多重代理系統 (MAS): 由多個互動的智慧型代理人所組成的電腦化系統。多代理系統可以解決單獨代理或單體系統難以或無法解決的問題。

多因素挑戰集自主身份驗證 (MFSSIA): 利用區塊鏈oracle，實現跨區塊鏈互操作性。

Parachains: 連接至 Polkadot 或 Kusama 中繼鏈的區塊鏈。它們是特定於應用程式的資料結構，使用中繼鏈來驗證交易，中繼鏈是一個底層結構，支援所有連接的區塊鏈之間的安全通訊，也稱為 Parachains。

個人健康記錄 (PHR): 個人的電子健康相關資訊。

個人健康代幣 (PHT): 以個人為中心的分散式電子健康系統的實用代幣。

Polkadot: 可實現任何類型的資料或資產的跨區塊鏈轉讓，而不僅僅是代幣。連接至 Polkadot 可讓您有能力與 Polkadot 網路中的各種區塊鏈互通。

概念驗證 (PoC): 也稱為原理證明，是實現某種方法或想法，以證明其可行性，或是原則上的證明，目的在於驗證某些概念或理論具有實用潛力。概念驗證通常規模較小，可能完整，也可能不完整。

工作證明 (PoW) 共識演算法: 一種分散式的共識機制，需要網路成員付出努力來解決一個加密的十六進位數字。工作證明 (Proof of work) 也稱為挖礦 (Mining)，指的是因所做的工作而獲得報酬。

SNOMED CT 或 SNOMED: 有系統地組織的電腦可處理的醫學術語集合，提供臨床文件和報告中使用的代碼、術語、同義詞和定義。

軟體開發生命週期 (SDLC): 具有成本效益和時間效率的流程，開發團隊使用此流程去簽署和建立高品質的軟體。SDLC 的目標是透過前瞻性的規劃，將專案風險降至最低，使軟體在生產期間及之後都能符合客戶的期望。

"Soulbound" 代幣 (SBT): 一種只能由特定地址擁有和轉讓的代幣。這意味著一旦 Soulbound 代幣被創建並分配給一個地址，它就不能被任何其他地址轉讓或擁有。

西班牙資料保護局 (AEPD): 西班牙政府的一個獨立機構，負責監督個人資料保護法律規定的遵守情況。

標準合約條款 (SCC): 由歐委會所制定的文件；此項更新是確保跨國資料傳輸過程中，資料保護措施健全且與時並進的重要一步。

測試資料管理 (TDM): 在整個軟體開發生命週期 (SDLC) 中，為現代團隊提供受控資料存取的流程。

實用性和不可轉讓的「靈界」代幣 (SBT): 也稱為「不可轉讓代幣」，是一種無法轉讓或出售到其他錢包中的 NFT。這些類型的代幣通常用於代表憑證、從屬關係、成就或會員資格。

WF-nets: 用於描述並行和分散式系統中流程模型的形式化。