BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

原始研究

Soulbound 代幣：醫療資料儲存中的隱私感知與分散式驗證機制的推動者

Biagio Boi, PhD , 學生; Franco Cirillo, PhD , 學生; Marco De Santis, PhD , 學生; and Christian Esposito, PhD

薩勒諾大學電腦科學系，義大利 Fisciano，通訊作者：Franco Cirillo，電子郵件：

fracirillo@unisa.it

DOI: https://doi.org/10.30953/bhty.v7.334

關鍵字：認證、區塊鏈、醫療保健、醫療記錄、SBT、自治身份、Soulbound Token、SSI

摘要

背景：醫療照護領域的數位化面臨重大的挑戰，因為資料的多樣化及其在不同醫院的分佈。此外，由於醫療照護相關資料必須遵守「一般資料保護條例」(GDPR) 及類似資料保護法的法律義務，因此安全性是主要的考量。為了增強資料互通性，已實施了健康等級七 (Health Level Seven, HL7) 等標準化工作。然而，驗證仍然是一個具有重大挑戰的關鍵問題。

目的：本研究旨在透過引進新穎的分散式認證架構，改善並強化認證程序。此外，本研究還提出了分散式資料管理的新方法，這對於有效處理敏感的醫療資料至關重要。

方法：所提出的架構採用以使用者為中心的方法，並利用自主身份（SSI）。在醫療領域中，它引進了一種新的不可偽造標記 (NFT) 種類，稱為靈魂標記 (SBT)，這將有助於不同醫院之間的用戶認證，有效地創建了一個互聯機構聯盟。

結果：實施建議的架構後，可顯著縮短多間醫院的驗證時間。SBT 的使用可確保安全且無縫的使用者驗證，進而提升整體系統的互通性與資料安全性。分散式方法也降低了與集中式驗證伺服器相關的風險。

結論：本研究利用 SSI 和 SBT，成功地為醫療照護領域提出了新穎的分散式驗證架構。此方法可加速驗證程序，並提升資料安全性及醫院間的互通性。未來的研究應該探討此架構的可擴充性及其在其他需要嚴格資料安全措施的領域中的應用。

簡明摘要

本研究針對數位醫療的挑戰，特別是資料的多樣化、分發與驗證。它介紹了一個分散式認證系統，使用自治身份和一種新型的不可偽造的代幣（稱為靈魂代幣）。此系統可連結醫院、縮短驗證時間、增強資料安全性，並改善系統互通性。透過分散認證，可降低與集中式伺服器相關的風險。這項研究結果顯示，這種創新方法可以造福醫療照護業，也可能造福其他有嚴格資料安全性需求的產業，但仍建議對可擴充性和更廣泛的應用進行進一步研究。

提交日期：2024 年 7 月 2 日；接受日期：2024 年 8 月 9 日；發表日期：2024 年 8 月 9 日：2024 年 8 月 9 日；發表：2024 年 8 月 31 日

改善資料管理、營運效率和病患照護，都有賴於醫療照護產業的數位化。然而，這個轉變有幾個主要的障礙，特別是在驗證和資料相容性方面。醫療照護資料通常分散在數個系統和組織中，[1]每個系統和組織使用不同的標準和技術來管理病患資料。這種分散性使得在不同系統之間進行整合變得困難，並導致資料呈現的差異。標準資料格式的缺失增加了資料交換的難度，也增加了出錯和效率低下的風險。由於許多系統並非總是能很好地合作，使用者在存取健康記錄時可能會遇到困難。這種混亂會影響照護協調的有效性，並可能導致錯誤或延遲病患照護。

傳統的醫療照護驗證方法通常依賴集中式伺服器來儲存及驗證使用者憑證。這些集中式系統有幾項困難，例如

- 單點故障：用於驗證的集中式伺服器容易發生故障。如果伺服器發生故障或損壞，整個網路都可能受到影響，使得不同機構的員工都無法存取病患資料。
- 擴充性問題：隨著醫療照護網路的發展與使用者群的增加，集中式系統可能無法滿足需求，進而造成效能瓶頸。
- 網路安全相關風險：集中式伺服器經常是網路攻擊的焦點。如果對這些系統的攻擊成功，重要的病患資料可能會在大規模的資料外洩中被洩露。

依賴集中式驗證系統可能會導致嚴重的安全漏洞，損害醫療照護資料管理的整體效能與安全性。在資料分散於不同機構的分散環境中，這種漏洞會更加嚴重。健康保險可攜性與責任法案 (Health Insurance Portability and Accountability Act, HIPAA) 和一般資料保護規範 (General Data Pro-tection Regulation, GDPR) 等嚴格的法律適用於醫療照護資料。為了保護病患隱私並確保合規，這些法規對資料存取和管理實施嚴格的控制。傳統的驗證方法往往無法在使用者便利性與安全性之間取得折衷。複雜的認證標準可能會導致更多的管理工作，並可能導致不符合規定的情況。對於傳統系統而言，要保證只有授權人員才能存取重要資訊，同時又能維持完美的使用者體驗是相當困難的。體驗。

醫療照護資料網路的複雜性隨著使用者數量的增加而增加，現有的驗證解決方案可能無法跟上。[2]一些傳統的系統是以缺乏彈性的基礎架構為基礎，因此很難因應醫療照護產業或技術的改變而修改。當醫療照護系統發展並納入新技術時，舊有的驗證技術可能會變得過時或需要昂貴的修改費用。這種缺乏彈性和可擴充性的情況可能會使產業更難發展和適應新的問題。

本研究旨在透過提出新穎的分散式驗證架構，解決醫療保健領域的驗證挑戰。所提出的解決方案利用自我主權身份 (SSI)，這是一種以使用者為中心的方法，能夠賦予個人對其數位身份的控制權。此外，該架構還引進了一種新型的不可偽造標記 (NFT)，稱為靈魂標記 (SBT)。SBT 是一種特定類型的不可轉讓代幣，以安全且可驗證的方式代表區塊鏈上的個人憑證和成就。

與傳統的可替代代幣或可轉讓 NFT 不同，SBT 綁定於特定個人，無法轉讓或交易給另一方。SBTs 的起源在於需要一種可靠的方法來數位化地呈現和驗證個人的屬性和憑證，例如學位、專業認證和會員記錄。隨著人類驗證在從教育到專業網路等各個領域的重要性與日俱增，這種需求也變得更加迫切。靈魂綁定」一詞隱喻了這個概念，即這些代幣與個人的「靈魂」有著固有的聯繫，也就是他們個人獨特的身份，並且不能被分離或交換。透過實施這種分散式方法，我們的目標是建立一個醫療照護機構聯盟網路，強化資料安全性與互通性，同時大幅縮短驗證時間。為了補充這個分散式認證架構，我們建議整合 Solid 資料管理系統 (一種安全、分散式交換公共與私人資料的媒介)，它提供了一個強大的分散式資料儲存與管理架構。透過使用 Solid，患者可將其個人健康資料儲存於個人線上資料庫（Pods）中，並由患者完全控制。這可確保患者有權授予或撤銷對其健康資訊的存取權，從而促進信任並提高隱私權[3]。

在本報告中，我們將詳細介紹建議架構背後的方法，包括 SSI 與 SBT 的整合，並介紹我們的實作結果。我們展示了此方法如何降低與集中式驗證伺服器相關的風險，並改善醫療照護資料管理系統的整體效率與安全性。

引用：區塊鏈在醫療保健的今天2024，7：334 - https://doi.org/10.30953/bhty.v7.334

醫療照護資料管理系統的整體效率與安全性。最後，我們討論此架構對更廣泛的醫療照護產業的潛在影響，並建議未來的研究方向。

背景

在數位憑證管理領域中，區塊鏈技術與加密通訊協定的整合已帶來顯著的進步。一個突出的發展是使用 SBT 來發行和管理數位存取憑證。

本節將探討此領域的各種當代方法與創新，並強調每種方法的優點與限制，尤其著重於隱私權、不可否認性與法規遵循。

參考文獻 4 所提出的數位憑證管理系統，利用加強版的 SBT（Rejectionable soul-bound token，RejSBT），引進了一種創新的方法。4 引進了一種創新的方法，利用 SBT 的增強版，稱為可拒絕的靈魂綁定代用幣 (RejSBT)。此系統在發行時嵌入條款與條件，並確保使用者接受時不會拒絕接收，從而增強了傳統憑證的功能。RejSBTs 可保證接收和來源證明的不可抵賴性，這是法律和安全目的的一個重要方面。然而，目前的通訊協定缺乏加密措施，因為它主要是處理非敏感的數位存取憑證。未來的整合必須符合 GDPR 法規，才能解決潛在的隱私疑慮。

另一個值得注意的方法是在數位認證系統中，特別是在 Web3 和 metaverse 環境中，整合 decen-tralized identifiers (DID) 與 SBT。Kim 和 Ryou (2023)[5]提出的方案利用 DID 透過智慧契約進行使用者驗證，並發行 SBT 進行無縫整合。為了加強隱私權，驗證機關的服務供應商使用零知識證明 (ZKP) 系統，確保在驗證過程中重要的使用者資訊不被洩露。這種方法允許在沒有使用者直接參與的情況下產生加密證明，從而增加使用者的對話。此外，統一的錢包同時管理 DID 認證和 SBT，簡化了認證管理。

在隱私權保護憑證系統的背景下，結合選擇性揭露機制的 SBT 的使用正受到越來越多的關注。其中一個架構[6]建議以加密格式在星際檔案系統 (IPFS) 上儲存的 NFT 來發行憑證。儘管這個系統賦予使用者對其憑證資訊的完全控制權，但驗證程序並未採用 ZKPs，這可能會限制其隱私保證。一種先進的私人身份驗證方法[7]涉及零知識 SBT，它結合了 SBT 與 ZKPs。此協定使用身份持有人的私人/公開金鑰來加密儲存在 SBT 中的資料。然後再使用 ZKP 進行驗證，以確保資料未被篡改，且身份持有人符合特定要求，而不會洩露任何個人資訊。此方法有效地平衡了隱私權與安全性，使其成為身份驗證的強大解決方案。

元世界為數位身分管理帶來了獨特的挑戰和機會。其中一項實作[8]主要是在 Decentraland（一個以瀏覽器為基礎的 3D 虛擬世界平台）中使用 Ethereum 智慧合約和 ZKPs 來提供年齡限制的存取權限。這種方法允許使用者在不透露真實身份的情況下，證明他們有資格進行某些活動，例如進入虛擬電影院。它充分利用了現有的法律框架，如 eIDAS（電子身份識別）和 W3C 可驗證憑證，展示了區塊鏈技術在確保符合法律標準的同時，在維護隱私方面的實際應用。

SBT 的一個實用案例是 COVID-19 疫苗接種的認證。此建議的系統[9]採用分散式應用程式，SBT 以不可轉讓和可撤銷代幣的形式發行，確保符合疫苗接種記錄不可轉讓的特性。雖然此方法解決了疫苗接種認證的管理問題，但並沒有明確處理隱私權和機密性的問題，這也是未來需要改善的地方。

此外，資料去中心化的概念已超越憑證管理的範疇，在各行各業都有更廣泛的應用。除了安全性之外，一個重大的挑戰是在區塊鏈網路中儲存大型檔案，因為傳統的區塊鏈缺乏儲存醫療影像等大型檔案的能力。整合分散式儲存解決方案，例如 IPFS 和 Solid Pods（個人資料儲存，提供存取、更新和分享資料的地方），可以徹底改變整個網路的資料管理和分享。例如，IPFS 在分散式檔案系統中提供對等網路來儲存和共用資料，提高資料可用性並降低中央故障點的風險。針對 IPFS 上的資料儲存提出的安全模型[10] 利用 Shamir's Secret Sharing (SSS) 在儲存前加密資料，以 Ethereum 實作，並運作在需要高計算能力的工作證明共識演算法上。

IPFS 的另一個挑戰是它只提供資料的切細值，使得搜尋相關病患記錄的工作變得複雜。為了解決這個問題，參考文獻中提出了一種基於星際名稱系統的區塊鏈。11 中提出了一種基於星際名稱系統的區塊鏈，它透過提供名稱而非切細值來方便資料搜尋，從而縮短搜尋時間。因此，區塊鏈系統可用於儲存、分享、使用和操作病患資料。另一個解決方案是使用 Solid pod 來儲存醫療照護資料。範例

*表 1.*憑證管理解決方案的比較分析

來源	主要功能	優勢	限制	隱私權	不可抵賴性	符合法規
Pericàs-Gornals. 等人 (2024)[4]	強化 SBT 與 T&C，確保接收的不可抵賴性	法律與安全保證、接收與來源的不可抵賴性	缺乏加密措施，主要用於非敏感憑證	低	高	需要與未來的 GDPR 看齊
Kim 等人 (2023)[5]	用於使用者驗證的 DID、用於隱私的 ZKP、統一錢包	使用 ZKP 增強隱私，無縫整合	實施的複雜性	高	中等	符合法律標準
Reddy 和 Kushwaha (2023)[6]	NFT 儲存於 IPFS，加密格式	使用者可控制憑證資訊	缺乏 ZKP，隱私權保證有限	低	中	需要加強隱私權
Cabot-Nadal 等人 (2023)[7]	結合 SBT 與 ZKP，使用私人/公開金鑰加密	有效平衡隱私性與安全性	高複雜度	高複雜度	高	與隱私權法規高度一致
Zichichi 等人 (2023)[8]	Ethereum 智慧型契約、ZKPs、eIDAS、W3C VCs	在 metaverse 中的實際應用，可維護隱私與合規性	特定於年齡限制存取	高	中	嚴格遵守法律標準
Lunesu 等人 (2023)[9])	SBT 是不可轉讓和撤銷的代幣	解決管理問題	缺乏對隱私權和機密性的重視	低	中度	需要加強隱私權
Naz 等人 (2019)[10]	用於儲存的 IPFS、用於加密的 SSS、PoW 共識	增強資料可用性、減少故障中心點	高運算能力，搜尋困難	高	中	潛力強大，但需要針對醫療保健進行優化
Saharan 和 Prasad (2020)[11]	使用名稱而非雜湊值促進資料搜尋	縮短搜尋時間、加強資料分享與使用	實施複雜度	中	中等	與資料管理標準高度一致
提案。	使用 SBT、私有區塊鏈（Hyperledger Besu）、PoA 共識（QBFT）、隱私感知規則（Chainlink）實現去中心化自動化	全面的框架、可擴充性、利用私有智慧合約增強安全性	私有區塊鏈	高	高	強調合規性，私有區塊鏈確保隱私性

DID：分散式識別碼；eIDAS：電子識別、驗證和信任服務；GDPR：一般資料保護條例；IPFS：InterPlanetary File System；NFT：不可流通代幣；PoA：PoA：權力證明；PoW：工作證明；QBFT：QBFT：QBFT：Quorum Byzantine Fault Tolerant；SBT：soulbound tokens；SSI：Self-Sovereign Identity；SSS：Shamir's Secret Sharing；T&C：terms and conditions；VCs：verifiable credentials W3C：World Wide Web Consortium；ZKP：zero-knowledge proof。

[12,13]。

根據表 1，我們的解決方案提供了平衡隱私、安全性和法規遵循的全面且可擴充的架構，因此優於現有的方法。它使用 SBT 的分散式驗證、私人區塊鏈和感知隱私的口令，確保高度隱私和強大的安全性。與其他方法不同的是，它解決了缺乏加密、複雜性和應用程式限制等關鍵限制，使其成為更優越、更穩健的選擇。

建議的系統

使用 SBT 的數位憑證管理系統的進展說明了在強化隱私、安全性和使用者便利性方面的重大進展。然而，每種方法都有其優點和限制，尤其是在隱私權保護和法規遵循方面。和法規遵循方面。未來的發展必須著重於整合強大的加密措施、全面的隱私權保護，以及遵守法規標準，以充分發揮這些創新系統在數位憑證管理上的潛力。

目前最先進的技術強調醫療照護領域內產生的資料之間嚴重缺乏互操作性。利用 HL7 等標準，開發跨醫院的互操作解決方案是可行的。然而，現有的資料儲存方法主要依賴集中式伺服器，需要仔細重新設計。這包括重新檢視資料存取的機制。

建議的架構旨在提供一個完整的架構，以分散的方式管理驗證，同時也考慮前一節所討論的分散資料解決方案。

引用：區塊鏈在醫療保健的今天2024，7：334 - https://doi.org/10.30953/bhty.v7.334

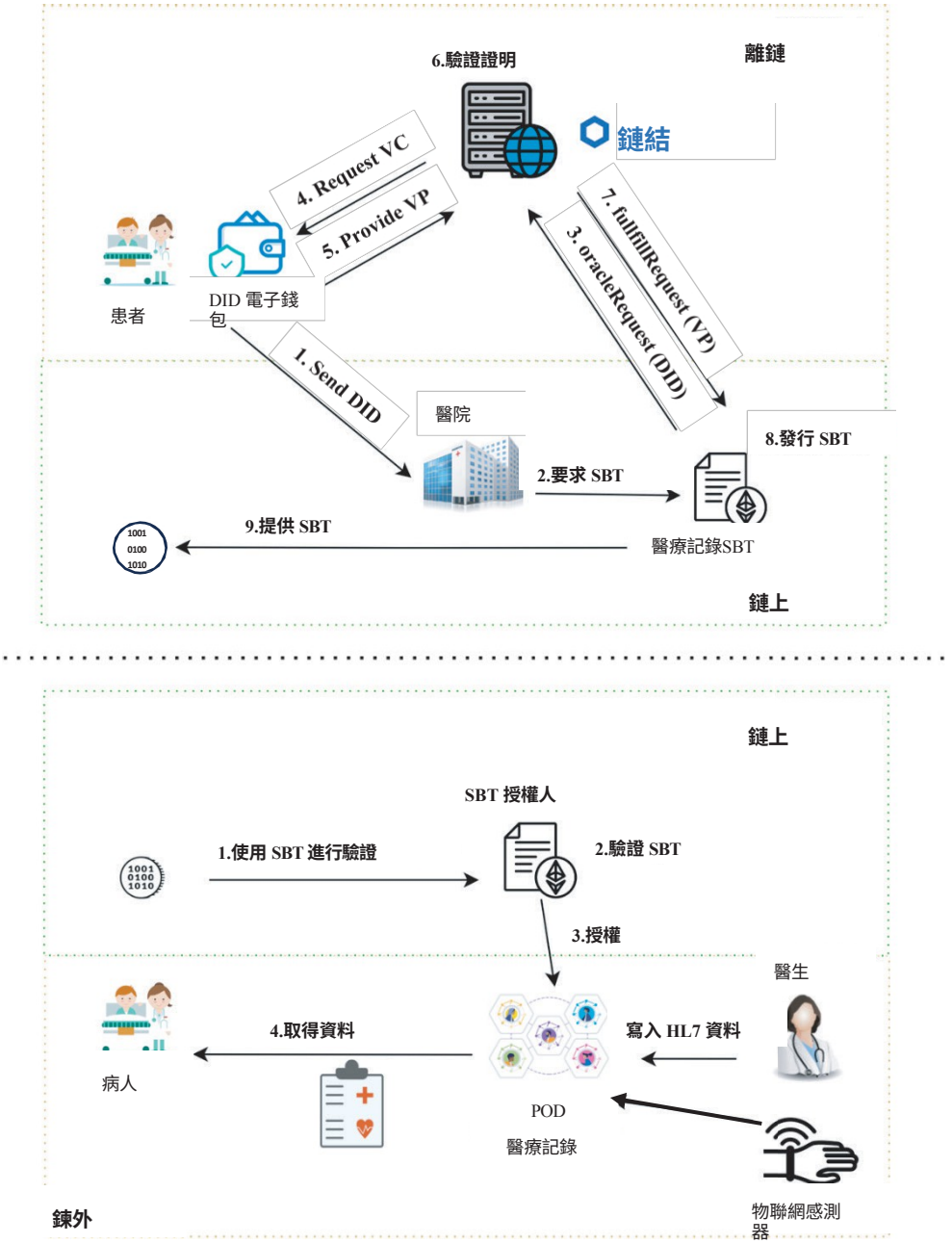

圖 1. 系統模型：註冊階段（上圖）和驗證（下圖）。HL7：Health Level Seven；IoT：物聯網；Pods：個人線上資料儲存；SBT：soulbound token。

目的是透過深入瞭解平均回應時間以及對通訊協定進行徹底的安全性評估，來驗證此方法。

簡介

由於複雜的互動關係，在醫療領域使用 DID 並非直接適用的選擇。此外，由於需要對憑證進行簽名驗證，因此在分散式應用程式中使用 SSI 進行驗證會面臨重大挑戰，而簽名驗證無法在不洩露使用者資料的情況下在鏈上執行。

在使用公共區塊鏈 (例如 Ethereum) 時，這些問題變得更加重要。

我們的架構旨在提供 SSI 的所有優點，同時整合基於 NFT 的新型驗證機制，特別是稱為 Soulbound Tokens (SBT) 的擴展。SBT 旨在將代幣與其擁有者綁定，從而充分利用 NFT 帶來的好處。

為了分析我們的系統，我們將它分為兩個主要階段：註冊階段，如圖 1 最上方所示，以及驗證階段，如圖 2 最下方所

引用：區塊鏈在醫療保健的今天2024，7：334 - https://doi.org/10.30953/bhty.v7.334

圖 1 的底部。在深入分析這些階段之前，有必要釐清與我們的架構相關的一些技術層面。

憑證驗證對於鏈上來說是複雜的；因此，我們採用了一種混合方法，即先在鏈外驗證身份，然後再使用私有區塊鏈 (如 Hyperledger Besu) 發佈 SBT。私有區塊鏈的需求來自於在執行鏈上交易時保證使用者隱私的需要。

法定人數與權限證明

該架構已部署在使用 Hyperledger Besu 的私有區塊鏈上，由四個節點組成，作為實驗性專案的一部分。這個設定很容易擴充，因為我們只使用區塊鏈來釋放 SBT。在採用的權限證明 (PoA) 共識機制中，驗證者（即授權挖掘區塊的節點）由區塊鏈擁有者預先授權。

每個區塊都由其中一個預先授權的節點進行驗證。Hyperledger Besu 支援多種 PoA 方案，包括 QBFT、IBFT 2.0 (Istanbul Byzantine Fault Tol-erance) 和 Clique。就我們的專案而言，我們選擇 QBFT 是因為它能夠確保交易的隱私，這對於實現基於 Chainlink 基礎架構的隱私感知甲骨文非常重要。這些交易是安全的，而且只有相關方能存取。PoA 的可擴展性是非常有利的，因為它可以支援網路的成長而不會有顯著的效能問題。由於驗證者是可信賴的實體，因此安全性和信任度都得到了增強，降低了惡意活動的風險，並確保 SBT 簽發的可信度。我們在 PoA 中選擇 QBFT 方案是因為它的交易隱私功能，這對於我們使用 Chain-link 基礎架構的隱私感知 Oracle 來說非常重要。總體而言，PoA 的效率、可擴充性、安全性和隱私權使其成為我們部署 SBT 的理想選擇。

註冊

需要註冊階段是因為在系統內建立及時的使用者驗證程序非常複雜。基於 DID 的驗證需要驗證憑證，並由持有者產生可驗證的證明，這可能會產生開銷。此外，這些程序無法如前所述應用於公共區塊鏈。

在我們的提案中，第一階段包含九個步驟，將 SBT 傳送給使用者。在此階段中，使用者分享 SSI 認證並接收 SBT。程序開始於持有人向醫院要求釋放 SBT。在此請求中，持有者將其 DID_H傳送給醫院，在我們的案例中，DID_H是一個 *did:eth*（decen-tralized identifier:*以太坊*）。
tralized identifier:以太坊）方法識別符，以確保
與以太坊區塊鏈的相容性。這樣的 DID_H與 $DIDDocument_H$相關聯，透過使用
的智能合約。醫院將該請求轉發給包含相同 DID_H的 MedicalRecordSBT 智能合約，該 DID_H以前部署在 Besu 區塊鏈上。功能 requestSBT 然後將此請求轉發給 Chainlink 基礎設施，由其處理與外部服務器的鏈外通 訊。如圖 1 所示，在步驟 4、5 和 6 中，請求遵循經典的 SSI 信任三角形方法，其中驗證器（在本例中為 ChainLink 節點）向鏈外伺服器發送請求，由其生成 VPR。使用者產生與該 VPR 相連的可驗證簡報，並將簡報傳送至離鏈伺服器，由離鏈伺服器執行憑證驗 證。一旦確認傳輸憑證的有效性，就會在 MedicalRecordSBT 上執行回呼，將最終的 SBT 釋放給使用者。使用者現在可以使用此 SBT 在醫院信任的平台上驗證自己。

認證

在認證開始時，病人已經擁有一個在醫院內代表其身份的 SBT。這個標記用於認證使用者和存取儲存在 POD 上的個人資料。整個程序透過 *SBTAuthorizer* 智慧型契約進行管理，該契約包含對已發行 SBT 的參照，並能夠執行驗證程序。此智慧型契約也包含與系統內已撤銷的代幣和角色相關的元資料，允許醫院在使用者失去錢包所有權時撤銷存取權。

與病人類似，物聯網 (IoT) 裝置和醫生也會使用分散式方法存取資料空間。如參考文獻14 和參考文獻15 中所述，醫生和 IoT 裝置都可以使用 SSI 實現此類認證。特別是，醫生會透過使用 HSM 管理驗證，作為減少驗證所需時間的機制，而 IoT 裝置則可利用靜態隨機存取記憶體 (SRAM) 或心電圖等物理特性，以建立 SSI 錢包產生時使用的私密金鑰。最後，建議的架構可將認證程序與資料儲存分離。

分散式資料儲存

所建議的方法還包括一個新穎的分散式資料儲存系統，與所建議的分散式認證機制完全相容。Solid 是一個相對較新的架構，透過授權使用者對應用程式所產生的資料負責，符合以使用者為中心的資料儲存範例。在這個特定的使用案例中，這涉及到由 IoT 裝置和醫生進行的分析所產生的醫療資料。Solid 利用知識圖表技術，提供結構良好的資料儲存方法。

*表 2.*部署建議架構的成本

作業	所需氣體	成本 ($)	花費
部署			
• TokenLink.(constructor)	1467527 瓦斯	11.87	權限
• 經營者(建設者)	4184013 瓦斯	33.83	權限
• EthereumDIDRegistry.	574518 氣體	1.55	權限
• NationalHealthServiceDIDRegistry.	1168361 氣體	9.45	權限
• MedicalRecordSBT.	5159457 瓦斯	41.72	權限
註冊			
• EthereumDIDRegistry.updateDIDDocument(string,bytes)	742188 瓦斯	6.00	醫院
• NationalHealthServiceDIDRegistry.authorizeDID(string,string)	58569 氣體	0.47	醫院
• MedicalRecordSBT.requestSBT(string)	164520 氣體	1.33	醫院
SBT 造幣			
• MedicalRecordSBT.fulfillRequest(string)	2594670 瓦斯	20.98	鏈結節點

DID：分散式識別碼/身分；SBT：靈魂代幣。

此表示法完全符合醫療領域的當代資料表示機制，例如 HL7，它提供了一個記錄完備的本體學。此方法可透過促進分散式資料儲存，讓使用者可以管理由 IoT 裝置產生的資料，而無需複製到外部伺服器上，進而提升 GDPR 的合規性。

結果

為了評估建議架構的品質，我們主要著重於部署解決方案的成本，即執行智慧契約的費用。為了評估我們的建議，我們在一台 iMac 3.3 GHz Intel Core i5 6 核心配備 16 GB 2667 MHz DDR4 的機器上，部署了一個配備 QBFT consen-sus 的 Hyper-ledger Besu Docker 映像檔。

為了實現我們的解決方案，我們部署了五個智慧型契約：

1. **LinkToken.sol：**負責支付 Chainlink 請求。最初部署了 1.000.000 LINK。
2. **Operator.sol：**負責操作 Chainlink 節點，轉發所有請求。
3. **EthereumDIDRegistry.sol：**負責管理 DIDs 架構。
4. **NationalHealthServiceDIDRegistry.sol：**負責管理整個架構內的角色。
5. **MedicalRecordSBT.sol：**包含 SBT 定義與鑄造 SBT 的作業。

如表 2 所示，智能合約部署是最昂貴的操作，加上 SBT 造币，需要生成并向用户发布 SBT。操作請求需要設定整個環境，並參考已建立的 DID 對應到包含角色的內部註冊表。包含角色的內部註冊表。氣體估算提供了有關智慧契約所涉及的作業複雜性的洞察力，但成本將取決於多種因素，例如網路佔用率、所需費用等。假設每個 gas 所需的成本為 3 gwei，這與 Ethereum 區塊鏈的一般成本相符，因此可以估算出不同作業的總成本。

部署階段只會在系統採用時執行一次，而註冊和 SBT 造幣作業則會針對屬於系統的每位新病患執行。對於建議方法的優點而言，系統中每位新使用者的總成本低於 30 美元是合理的。

認證程序不需要任何費用，只需要從區塊鏈中讀取資料，不需要任何額外費用。

註冊程序的整體時間約為

平均為 16.03 秒；其中最大的部分用於驗證憑證 (12.54 秒)。這就是促使我們轉向完全分散式鏈上方式的主要動機。有了我們的提案，現在就可以使用 SBT 進行驗證，而且只需檢查 MedicalRecordSBT 智慧合約上是否有 SBT 即可。

透過目前的研究，我們嘗試在保留節點隱私和 SSI 引入的所有優勢的同時，透過提供鏈上驗證方法來縮短驗證所需的整體時間。考慮到每個使用者只需執行一次註冊階段，且認證階段只需呼叫一次智慧契約，因此建議架構所引入的開銷相對較低。此外，該系統嚴格地基於區塊鏈和區塊鏈背後的sym-metric 機制。SBT 藉由加密錢包來增加安全性，錢包會儲存與公開金鑰相關的私人金鑰。

引用：區塊鏈在醫療保健的今天2024，7：334 - https://doi.org/10.30953/bhty.v7.334

結論

未來，我們計畫將提供者存取整合到真實世界的情境中，以加強我們對建議方法的評估。透過整合提供者存取，我們將能夠模擬更複雜、多利害關係人的環境，從 而更全面地評估我們的方法在實務中的有效性。這將讓我們更了解真實世界對醫療資料安全性與隱私權的影響。例如，在糖尿病用例中，提供者存取將可讓醫療照護專業人員直接與儲存在 Solid Pods 中的病患資料互動，同時也可對分散式機器學習模型有所貢獻，並從中獲益。這個新增的提供者互動層對於驗證我們的架構在各種醫療用例中的可擴展性和實用性至關重要。

經費來源

本工作部分由 EU-NGEU 資助的 NRRP MUR 計畫下的專案 SERICS (PE00000014) 以及義大利衛生部資助的創新健康生態系統 (PNC)-National Recovery and Resilience Plan (NRRP) 計畫下的專案「DHEAL-COM-社區醫學的數位健康解決方案」所支持。

利益衝突

作者無此報告。

貢獻者

Boi 先生對系統概念化、系統評估及撰寫貢獻良多。Cirillo 先生對系統的概念化、技術狀況和整篇論文的撰寫做出了貢獻。De Santis 先生對系統的概念化和論文的撰寫貢獻良多。Esposito 博士參與了系統的概念化和每篇論文草稿的審閱。

所有作者均已核准該手稿，並同意將其投稿至 Blockchain in Healthcare Today。

資料可用性聲明 (DAS)、資料分享、可重複性和資料庫。

聯絡作者。

生成文本或相關技術的應用

本文編寫過程中未使用人工智慧及相關技術。

鳴謝

本工作部分由 EU-NGEU 資助的 NRRP MUR 計畫下的專案 SERICS (PE00000014) 以及 EU-NGEU 資助的專案 SERICS (PE00000014) 所支持。

以及由義大利衛生部資助的創新健康生態系統 (PNC) - 國家復甦與恢復計劃 (NRRP) 項目下的「DHEAL-COM-社區醫學中的數位健康解決方案」專案。

參考文獻

1. Reegu F, Abas H, Jabbari A, Akmam R, Uddin M, Wu CM, Chen CL, Khalaf O. Interoperability Requirements for Block-chain-Enabled Electronic Health Records in Healthcare：系統回顧與公開研究挑戰。安全與通訊網路 2022; 2022(1):9227343. https://doi.org/10.1155/2022/9227343
2. Gupta D, Mazumdar N, Nag A, Singh J. Secure Data authentication and access control protocol for industrial health-care system.環境智慧與人性化運算期刊 2023; 14(5):4853-4864. https://doi.org/10.1007/ s12652-022-04370-2
3. Esposito C、Horne R、Robaldo L、Buelens B、Goesaert E. 評估固態通訊協定的安全性與保密義務。https://doi. org/10.3390/info14070411
4. Pericàs-Gornals R, Mut-Puigserver M, Payeras-Capellá MM, Cabot-Nadal MÁ, Ramis-Bibiloni J. Digital credentials man-agement system using rejectable soulbound tokens.Ann Tele-commun [Internet].2024 Apr 23 [cited 2024 Jun 19]; Available from: https://link.springer.com/10.1007/s12243-024-01032-6
5. 數位憑證管理系統使用可拒絕的灵魂绑定令牌。數學.2023 Oct 22;11(20):4387. https:// doi.org/10.3390/math11204387
6. Reddy S, Kushwaha DS.使用靈魂標記的隱私保護憑證發行與驗證系統框架。Sumathi AC, Yuvaraj N, Ghazali NH, editors. ITM Web Conf.ITM Web Conf.
7. Cabot-Nadal MÀ, Playford B, Payeras-Capellà MM, Gerske S, Mut-Puigserver M, Pericàs-Gornals R. Private Identity-Related Attribute Verification Protocol Using SoulBound Tokens and Zero-Knowledge Proofs.In: 2023 7th Cyber Security in Net-working Conference (CSNet) [Internet].Montreal, QC, Canada：IEEE; 2023 [cited 2024 Jun 19]. p. 153-6.Available from: https:// ieeexplore.ieee.org/document/10339754/
8. Zichichi M, Bomprezzi C, Sorrentino G, Palmirani M.在 Metaverse 中保護數位身分：Decentraland 中電影院的存取案例。In：語言理論發展國際會議。2023.https://ceur-ws.org/Vol-3460/papers/DLT_2023_paper_13. pdf
9. Lunesu MI, Tonelli R, Pinna A, Sansoni S. Soulbound Token for Covid-19 Vaccination Certification.In: 2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops) [Internet].Atlanta, GA, USA: IEEE; 2023 [cited 2024 Jun 19]. p.
10. Naz M, Al-zahrani FA, Khalid R, Javaid N, Qamar AM, Afzal MK, et al. A Secure Data Sharing Platform Using Block-chain and Interplanetary File System. 永續性。2019 10;11(24):7054. https://doi.org/10.3390/su11247054
11. Saharan R, Prasad R. Blockchain Technology for Healthcare Data.智慧系統與運算的進展。2020 2;671-7. https://doi.org/10.1007/978-981-15-6014-9_81
12. Ghayvat H, Zuhair M, Shukla N, Kumar N. Healthcare-CT: Solid PoD and Blockchain-Enabled Cyber Twin Approach.

醫療保健 5.0 生態系統。IEEE 物聯網期刊。2024 Feb 15;11(4):6119-30. https://doi.org/10.1109/JIOT.2023.3312448

13. Ragab M, Savateev Y, Oliver H, Tiropanis T, Poulovassilis A, Chapman A, et al. Unlocking the Potential of Health Data with Decentralised Search in Personal Health Datastores.2024 年 5 月 13 日。
14. Barbareschi M, Boi B, Cirillo F, De Santis M, Esposito C. CSe-curing the Internet of Medical Things using PUF-based SSI Authentication.In Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024) 2024.
15. Boi B, Esposito C. Securing the Internet of Medical Things with ECG-based PUF encryption.IET Cyber-Physical Systems：理論與應用 2024 。

附錄：縮寫詞定義

DID：分散式識別碼/身分 did:eth：分散式識別碼

：以太坊

$DIDDocument_H$: 數位身分文件 (持有人) DID_H: 數位身分 (持有人)

eIDAS：電子識別、驗證和信任服務。

和信任服務。

GDPR：一般資料保護條例

HIPAA：健康保險可攜性與責任法案

HL7：健康等級七

HSM：硬體安全模組

IBFT：伊斯坦堡拜占庭容錯 IoT：物聯網

IPFS：跨專屬檔案系統 NFT：不可偽造

的令牌

PoA：權限證明

Pod：個人線上資料儲存 PoW：工作證

明

QBFT：Quorum Byzantine Fault Tolerant

RejSBTs：可拒絕靈魂邊界令牌 SBT：靈魂邊

界令牌

SRAM：靜態隨機存取記憶體 SSI：自我主權身

份

SSS：沙密爾秘密分享 T&C：條款

與條件 VC：可驗證憑證

VPR：可驗證的呈現請求 W3C：萬維網

聯盟 ZKP：零知識證明