BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

技術簡介與簡短報告

我的整體資料分享：WEB3 資料分享應用程式：從金融擴展到隱私保護的分散式多維資料分享，以加強全球醫療保健

Sathya Krishnasamy，碩士

ChainAim, Newington, Connecticut, USA DOI:

https://doi.org/10.30953/bhty.v7.341

通訊作者：Sathya Krishnasamy，電子郵件： sathya.krishnasamy@chainaim.com

Keywords: access control, blockchain, distributed ledger, healthcare, privacy, threshold cryptography

摘要

WEB3 網路架構、分散式帳本和分散式人工智慧技術代表著資料處理、儲存和分享方式的轉變。這些創新技術有望解決與傳統集中式系統和自我保管錢包相關的基本漏洞，從而顯著提升消費者的資料隱私權。在主要由第三方操作的傳統系統中，資料外洩事件比較常見，由於集中儲存和過度資料移動（有時是不必要的），導致嚴重的資料外洩。醫療保健資料外洩在全球日益受到關注。由於勒索軟件對病人護理和隱私的影響，幾家醫院面臨停業。WEB3 電子錢包是全球金融包容性的重要組成部分，尤其是在發展中國家。它們促進了包容性，降低了成本，並通過自我保管賦予個人權力。儘管這些錢包需要重大改進，但其使用量正在穩步上升。根據 Statista 在 2023 年的一份報告，全球加密貨幣用戶群預計將在 2025 年達到 5 億以上，其中新興市場將有大幅增長。本文介紹了一個超越加密貨幣和金融的概念，進入日常真實世界的使用案例，這些案例需要組合存取一個人的整體資料，包括財務和健康記錄、基因組資料、進階指令等，這些資料需要隱私保護，並透過分散式識別碼和不可偽造的代幣徽章來識別特定的接收者，並與特定的行動者分享，以確定他們在 WEB3 生態系統中的角色。作者於 2024 年 4 月在 ETHBoston 提出此概念，利用底層臨界加密技術的原始實作獲得好評，並將其強化為全球醫療保健的概念性整體資料分享應用程式，如本文所述。

收到：收稿日期：2024 年 8 月 1 日；接受日期：2024 年 8 月 25 日；發表日期：2024 年 8 月 25 日：2024 年 8 月 25 日；發表：2024 年 8 月 31 日

WEB3 是一系列新興技術的集合。它包括分佈式分類帳、自我主權識別 (ID) 和人工智能 (AI)、並推廣資料和資產所有權的概念。WEB3 為傳統銀行系統提供了一種去中心化的替代方案。[1]WEB3 技術為沒有銀行服務和銀行服務不足的人群提供了金融服務，[2]降低了交易成本，並賦權個人通過自我保管的 WEB3 錢包實現以消費者為中介的資料共享。此外，Web 3.0 的資料分享原則符合現代資料隱私法，加強了使用者對個人資訊的控制。這些創新承諾透過解決與傳統集中式系統相關的一些基本漏洞，顯著改善消費者資料隱私權。

傳統系統中的資料外洩事件較為常見，由於集中式儲存漏洞和過多的資料移動（有時是不必要的），導致大量資料外洩。WEB3 技術提升消費者資料隱私權的潛力，是邁向更安全未來的一步。醫療保健資料外洩是全球日益關注的問題。數家醫院因勒索軟體而面臨營運停頓，影響病患照護與隱私[3]。

自我保管的資料主權和控制 關於 WEB3 電子錢包，自我保管是指透過自己持有私人金鑰來管理自己的數位資產，而不依賴可能濫用金鑰的第三方中介。自我保管基本上符合資料隱私原則，因為它強調個人對個人資料的控制。聯邦一般資料保護法規中的許多條款都定義了個人資料、資料最小化、合法性和安全第一的設計，以符合風險和通知的要求。同樣地，加州消費者隱私權法案的條文也涵蓋了個人資 料 的定義、知情權、選擇退出、刪除及不歧視異議等條文。特別是對於健康保險可攜性與責任法案 (Health Insurance Portability and Accountability Act) 的遵從，其主要規則是隱私權 - 確保任何承保實體和業務夥伴保護消費者資料、安全性 (規定管理、實體和技術保障措施) 和通知 - 任何資料外洩。這些法規規定，個人擁有其資料的所有權，必須向其資料使用者提供明確的同意，並收集所需的小型資訊，在特定期間內保留作特定用途，且資料的存取權限、使用和撤銷動作完全可稽核。自我保管可減少對第三方服務供應商的依賴，有可能減少系統不夠安全的資料處理不當或外洩事件。

當前錢包的限制

目前的錢包持有加密原生資產，例如加密貨幣和不可偽造代幣 (NFT)，主要用於金融應用程式和服務，在某種程度上也用於儲存數位收藏品。這些使用案例將收藏品儲存在分散式儲存中，如 InterPlanetary File System (IPFS)，並在錢包和元資料中對其進行指針。然而，由於相同的概念同樣適用於在財務記錄之上管理其他形式個人資訊的存取，因此許多使用個案都是可能的。這些包括健康記錄、基因組記錄、進階指令等等，不同形式的資料可能需要由在社會環境中扮演特定角色的人來查看，這些都是比較符合邏輯的用途。

自我保管要求個人對於處理自己的私密金鑰有一定的知識和經驗。此外，錢包的使用者體驗仍不太容易上手，需要一定的技術熟練度和一系列非瑣碎的步驟。有些用戶可能需要技術支援來管理他們的金鑰，也可能需要依賴第三方。根據保管人的安全能力和完整性，這可能會導致風險，包括身份盜用、資金損失、隱私外洩等等。

這開啟了對分散式協定的需求，分散式協定比集中式保管人更具彈性，而資料盲目協定層級的分散式，可透過加密使用者資訊，以及使用分散式且由加密機制管理的關鍵管理系統，增加資料管理的彈性，這些關鍵管理系統可根據特定時段的細粒角色，重新組合存取資料的憑證。閥值加密技術是嘗試實現這種分散性的關鍵技術。

臨界值加密技術

臨界值加密法是一種加密方案，其中加密金鑰被分成多份，分發給不同的對象。要執行解密或簽章等加密作業，必須結合預先定義的份數（臨界值）。舉例來說，如果金鑰被分成 10 份，而臨界值設定為 6，則任何 6 份都可以用來重建金鑰，但少於 6 份則無法提供金鑰的相關資訊。每一份都會有特定的保管人，他們只知道金鑰的一部分，而不是整個金鑰。

臨界值加密技術的優點

臨界值加密技術的優點包括增強安全性、冗餘性和可靠性，以及多方授權。

增強安全性

透過在多方之間分配金鑰共用，thresh-old 加密技術可確保沒有任何單一實體可完全存取敏感資訊。此方法可降低未經授權存取的風險，並為重要記錄的管理提供額外的安全層級。實際上，這表示即使惡意行為者入侵了一個共用空間，他們也無法存取敏感資料，或在未取得所需的最低共用空間數目的情況下執行作業。任何個人都無權獨立洩露資料，大幅降低資料外洩和內部威脅的可能性。

備援與可靠性

臨界值加密技術允許在某些金鑰份額遺失或損毀的情況下進行操作，只要臨界值的份額數保持不變即可。這可確保重要記錄在面臨技術問題或安全漏洞時仍可存取且安全無虞。

多方授權

臨界值加密技術有助於確保在沒有多方共識的情況下，資料不會被篡改。這有助於安全協作，允許研究人員分享和分析資料，而不會將資料全部暴露給任何單一參與者。這在

引用：Blockchain in Healthcare Today 2024, 7: 341 - https://doi.org/10.30953/bhty.v7.341

這在臨床試驗和研究調查中尤其重要，因為資料完整性對於得出有效結論和確保病患安全至關重要。在涉及多方利害關係人的情境中，例如遺產規劃或預先指示，臨界值加密技術可實現安全的多方授權。這可確保與敏感記錄相關的決策或行動需要多方授權者的共識，進而提升安全性與完整性。

閾值加密技術的限制與挑戰

複雜性、可用性和可擴充性是限制和挑戰。

複雜性

分割密碼金鑰和管理共享需要精密的通訊協定。要正確執行這些協定，並確保在各種安全攻擊下的彈性，是一項挑戰。

可用性

重新建構金鑰需要多方的積極參與，如果各方在地理上分散或可用性不一致，效率可能會很低。

擴充性

當參與者和共享的數量增加時，複雜性、通訊和可用性的開銷也會增加，這可能會造成擴充性的問題。

臨界值加密技術的具體實作可以根據加密金鑰的分發方式和資料檢索的存取控制配置方式而有所不同。重新組合金鑰份額和門檻的機制也是可設定的。在 Decen-tralised 運作模式中，協定實作可將金鑰分片分散至驗證器節點。

MyHolisticDataShare 與全球醫療照護的可能性

MyHolisticDataShare 是一個 WEB3 資料分享應用程式，可解決各種限制，並引入更新的概念來組織和儲存使用者資料類型，從財務資料和數位收藏品擴展至現實世界的資產，例如醫療記錄。這些進階指令可透過擴充安全資料分享的加密基本原則來管理。對於這些記錄的存取，可以個別提供並計量給社會情境中的特定方及其角色，也可以是特定接收者或角色的資產組合。

MyHolisticDataShare 是 SocialSecureShare 應用程式的修正與強化版，最初由作者於 2024 年 4 月在 ETHBoston 提出，並贏得隱私權與社區投票的最佳專案。MyHolisticDataShare 是一個技術原型。

MyHolisticDataShare 是一個技術原型，針對消費者與此類資料的接收者，結合消費者導向資料分享的多個層面，以及其對醫療照護的影響，並結合定期與緊急狀況下的健康資料，以及健康與財務的努力，例如照護的社會決定因素。

這些新興的隱私權保護技術，例如臨界值加密技術和存取控制，顯示了促進以消費者為中介的資料分享的可能性，同時藉由減少單點失敗、細粒化和可組合的存取控制來增強隱私權，以及制衡實體也可參與節點以提高可視性的可能性。

MyHolisiticDataShare 技術設計 MyHolisticDataShare 使用加密隱私基本原則和分散式機制 (例如用於隱私保護分散式儲存中加密資料的解密存取的臨界值加密**技術**)，其基礎為可識別獨特項目的代幣 NFT。NFT 是獨一無二的代幣，只代表一件事，並可用於代表特定的徽章。通訊協定和應用程式的管理者可以指派這些徽章。

[4]這些 NFT 對應到與個人或角色相關的特定身份徽章，根據持有這些存取徽章的錢包的分散身份驗證，提供存取用戶資料的權限。

臨界值網路提供一整套分散式臨界值加密服務，以增加使用者隱私和許可區塊鏈的主權（圖 1）。閾值加密技術透過在獨立節點網路中分散作業來保護資料，提高安全性和可用性，並減少對可信賴方的依賴。Threshold 網路使用服務 TACo 通訊協定進行存取控制。資料擁有者可以加密他們的有效負載 (可以有多個部分)，並可以將它們儲存在離線位置。根據需要，這些儲存元件也可以用於分散式儲存。在本範例中，資料擁有者將已加密的資料儲存在 IPFS（一種流行的分散式儲存解決方案）中。

TACo 將共同秘密 - 解密金鑰 - 分成*多份*，並將其分發給授權和抵押的節點操作者 (即臨界值網路中的利害關係人)。持有金鑰股份的操作者中，必須有最低數目的操作者 (*臨界值*) 在線，並積極參與部分解密。這些部分解密隨後會在請求者的用戶端結合，以重新建構原始明文資料。每個資料有效負載都附有條件，可以細緻地限制存取。資料擁有者可以定義一系列的存取條件，這些條件可以有存取控制檢查，例如：「該資料是否已被存取」、「該資料是否已被存取」、「該資料是否已被存取」。

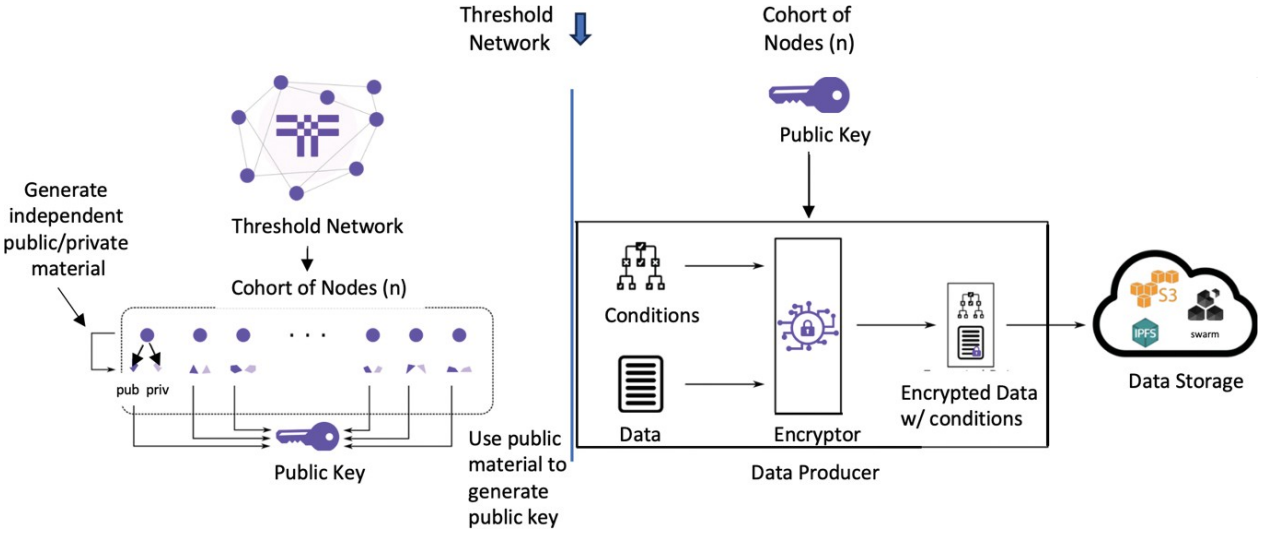

*圖 1.*門檻加密技術的門 檻 網路實作截圖。來源：https://docs.threshold.network/ applications/threshold-access-control/key-concepts。來源： application/threshold-access-control/key-concept：作者版權所有，2024 年。

請求者擁有代表緊急醫療人員徽章的特定 NFT？「或」.....幫助病人的社工？"也可以將它們與其他元素結合，例如：「請求者是否要求在資料擁有者給予存取權限的時間內進行存取？

請求者通過簽署交易證明其與條件滿足的關聯 - 他們接收臨界數解密股份的權利 - 該交易驗證了他們對特定 WEB3 電子錢包的所有權（在本例中，Polygon Test Network Amoy 上的 MetaMask 電子錢包）。該錢包會被檢查是否符合特定條件（例如，擁有 NFT 以存取資料資產）。

MyHolisticDataShare 旨在由不同類型的記錄組成，如圖 2 所示，消費者可將其儲存於 IPFS 等分散式儲存基礎架構中，並由元資料定義 URI。

實作是在 Polygon 區塊鏈海淘測試網，MetaMask 錢包存取透過 NFT 徽章儲存存取控制。

使用者可彈性儲存不同類型的記錄，包括財務、健康、基因組與進階指令。

財務記錄

這些記錄可能包括傳統的財務帳戶、加密帳戶、銀行對帳單、信用狀等等，使用者可以安全地儲存這些記錄，並決定分享給使用者認為有必要分享的特定收件人，以達到特定的財務相關目的。

健康記錄

這些記錄可能包括基本健康記錄，包括實驗室報告、診斷、診斷影像以及使用者認為有必要為特定健康相關目的而分享的約會。

引用：Blockchain in Healthcare Today 2024, 7: 341 - https://doi.org/10.30953/bhty.v7.341

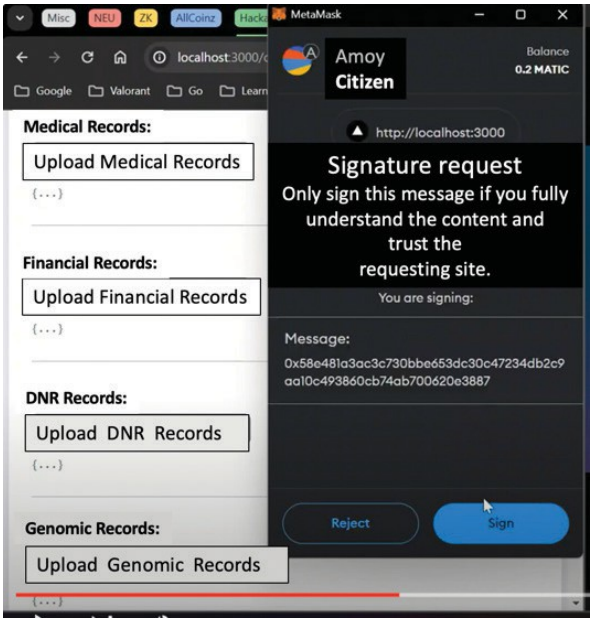

*圖 2.*使用者記錄加密的截圖。來源：作者版權所有，2024 年。

基因組記錄

這些可能包括特定粒度、高度專業化和個人資訊，例如使用者可與特定研究人員和有興趣的臨床醫師分享的基因組記錄。

預先指示

這些可能包括特定的健康代理資訊，例如「不急救」(DNR)偏好等，對醫療照護人員和急救技術人員而言非常重要。

圖 2 顯示在社群環境中，資料擁有者和市民在儲存他們想要加密的不同資料有效載荷到分散式儲存空間時簽署交易的流程截圖。圖 3 顯示資料負載與分散式儲存位置詳細資訊的截圖，並顯示確認回饋訊息。

MyHolisticDataShare 接收者徽章

區塊鏈網路參與者會獲得由管理資料自治組織管理的特定 NFT 徽章，該組織會註冊分散式 ID。舉例來說，網路中的分散式身分識別碼 (DID) 可以被指派一個主治醫師徽章，而另一個 DID 則可以被指派一個緊急醫療技術員 (EMT) 工作者徽章，代表資料需求的特定社會背景。

社會資料情境徽章及其配置可在註冊表中使用，註冊表會向使用者指出哪些徽章可以存取哪種資料。例如，在預設配置中，急救人員可能可以存取醫療記錄和 DNR 記錄，但無法存取財務記錄。基因組研究員可能擁有一個徽章，以顯示他對特定類型的基因組資料的興趣。組合存取也可以細緻地控制。例如，社會工作者可以存取健康與財務記錄，以協助規劃協調健康的社會決定因素。圖 4 顯示不同類型的徽章，以 NFT 形式儲存於資料接收者錢包中。當

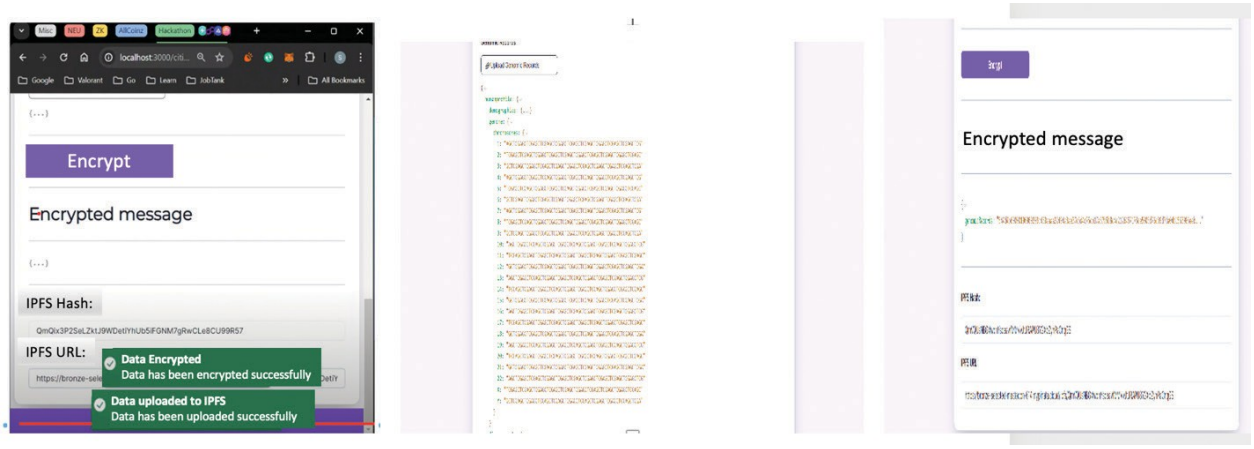

圖 3. 根據合成樣本資料成功加密的內容。來源：作者版權所有，2024。

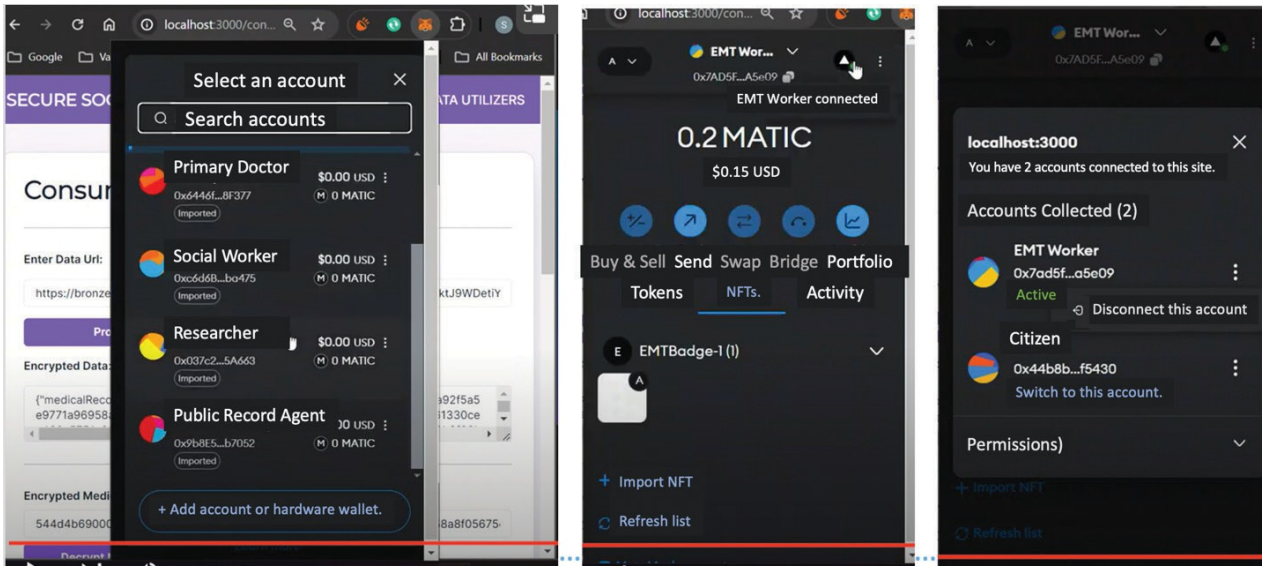

圖 4. 以分配給分散式 ID 的 NFT 為模型的不同徽章。EMT：緊急醫療技術員；ID：識別；NFT：不可偽造的代幣。資料來源：作者版權所有，2024 年。

引用：Blockchain in Healthcare Today 2024, 7: 341 - https://doi.org/10.30953/bhty.v7.341

資料接收者嘗試存取資料擁有者的加密資料時，會根據所定義的存取控制，檢查這些 NFT 徽章是否存在，以允許或拒絕存取。

解密結果與資料可用性

根據網路的分散式法定人數設定和 NFT 定義，使用者可以簽署交易以加密交易，使其可供持有特定資料需求的特定 DIDs 解密，這些特定 DIDs 模擬為獨特的 NFT 定義。這些也可以建模，而解密通訊協定會檢查特定的解密時間。徽章和通訊協定定義將提供解密存取權。其他資料則無法存取。圖 5 顯示在解密過程中檢查特定 NFT 徽章、驗證並執行解密權且解密成功的情況。範例包括指定研究人員合法存取基因組記錄，或 EMT 醫護人員存取 DNR 資料。圖 6 描述沒有所需 NFT 徽章的人無法解密資料的情況。例如，沒有社會工作者 NFT 徽章的人無法存取所有者的健康與財務摘要記錄資料。

在現實世界的環境中，此協定與應用程式背後的管理將涉及簽發徽章的離線驗證，可能涉及健康系統與社會組織的組合，以定義授權存取的角色與存取標準。舉例來說，具有特定存取控制的指定社工 (可能擔任照護協調或社區照護的角色) 可以存取醫療和財務記錄，以便根據病患的社會經濟地位為其尋找整體照護，其中的照護可能不只包括醫療照護，還包括尋找住房、交通和其他證明其需求的功能。

隨著無權限區塊鏈的成熟，我們看到消費者端採用無權限區塊鏈的趨勢越來越大，通過不同實體和個人的自我監護錢包和參與基於 WEB3 的社交應用程式來衡量。如果這些活動經過仔細規劃，並有足夠的制衡措施，包括一些在公共/混合區塊鏈上運行的監管節點，那麼也可以利用這些活動來採用以消費者為中介的健康資料隱私權，這種情況正在慢慢開始發生。

閾值加密技術並非其他隱私權保護技術的競爭者，而是其他技術的補充，例如完全同態加密和多方運算。在這些情況下，閾值系統仍可增加另一層安全性，其中加密內容可在存取時受到控制。

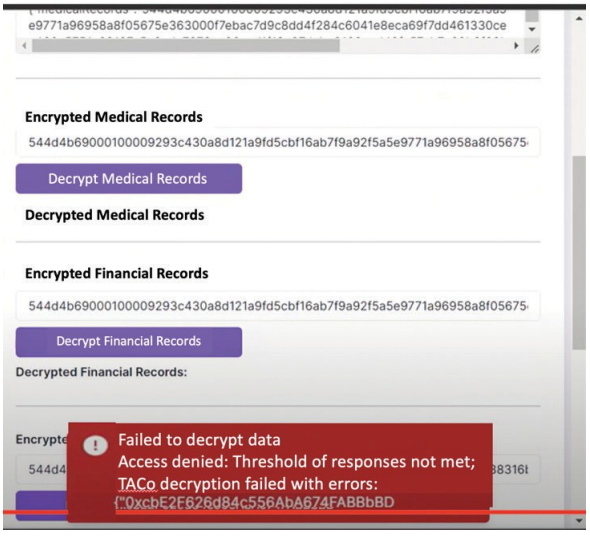

圖 6. 基於粒度存取控制的拒絕存取截圖。TACo：閾值存取控制。

資料來源：作者版權所有，2024 年。

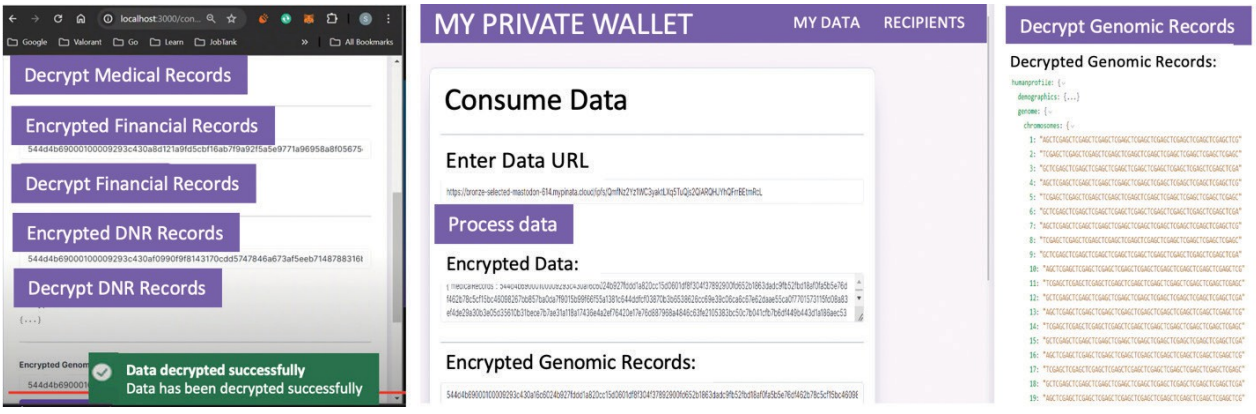

圖 5. 合法存取樣本合成資料的加密與解密範例。URL：統一資源定位器。來源：作者版權所有，2024 年。

請求系統從分散式端點存取資料，或在加密資料上執行計算。在這些情況下，存取控制系統的「防彈性」可能變得更加重要。在另一篇當代論文中，作者討論了零知識證明和機器學習的出現，這也是非常互補的，透過為驗證者提出證明，可以將資料分享減到最少。這種保護隱私的整體資料分享也可以解決另一個問題，那就是跨組織和跨領域的資料外洩。舉例來說，當資料外洩發生在零售業或銀行業時，可能會妨礙健康記錄的存取，因為某些個人資訊會外洩，並為惡意使用者提供更多資料。然而，有了這種整體性的資料分享，以及細粒度和可組合的存取，消費者就能對其資料有更多的控制權，並能更有效地因應逆境。

WEB3 需要改進的一個主要方面是消費者的易用性，因為對用戶來說，記住步驟和不可思議的地址是很有挑戰性的。這項工作已嘗試讓 UI/UX（使用者介面設計/使用者體驗設計）非常接近 Web 2 網頁，至少在管理資料方面是如此。它使用 JSON（JavaScript Object Notation，JavaScript 物件符號）資料結構、標準和簡單畫面的消費者可用性導向概念。在接下來的迭代中，將努力研究如何在瀏覽器擴充中使用資料定義，並使用先進的帳戶抽象和身份簡化機制來增加可用性。

結論與未來工作

MyHolisticDataShare 已經展示了 WEB3 技術的新延伸，其基礎是分散式資料分享和臨界值加密技術，用於分散非集中式法定人數和可配置臨界值定義的解密存取。這仍是一個介紹性的概念，最終版本的實作將取決於監管情境定義、分散式自治組織的治理設計，以及社會情境中成熟且成功的 DID 治理程序。

在主流環境中試用區塊鏈的任何嘗試都必須仔細規劃，並取決於特定的區塊鏈，包括特定的公共/私有/混合架構。本概念原型展示了 WEB3 技術開啟解決集中式系統中長期面臨的資料隱私和共享問題的潛在解決方案，主要是減少單點信任失效以及粒度和可組合的存取控制。

作者打算隨著技術的成熟，特別是圍繞著錢包和 WEB3 資料共享應用程式的方式，將此應用程式擴展為瀏覽器擴展錢包應用程式。

及其責任的定義。零知識系統（Zero-Knowledge Sys-tems）和完全同態加密（fully homomorphic encryptions）等輔助技術可增強這一概念，從而為消費者發起的和經證明的資料共享創建增強的隱私保護設計。作者在 ChainAim 所做的努力是繼續與標準組織和技術基金會建立關係，以辨識推進此類資料分享的可擴展性需求和管理需求。

經費來源

無。

利益衝突

無。

貢獻者

Sathya Krishnasamy 是 ChainAim Technologies 的總裁兼負責人。他擁有 25 年的工作背景，曾在美國領先的醫療保健公司 (包括 Aetna 和 Anthem) 擔任管理性醫療付費者設定工作，累積了豐富的經驗。他專注於新興技術，包括人工智慧/機器學習系統和分散式帳本技術。他也擔任許多產業的顧問，包括付款人與提供者的合作、標準組織，以及在印度推動金融科技、醫療保健和技能產業的 Account Aggregators 等工作。他目前是 ChainAim 的總裁兼負責人，提供技術策略諮詢、應用與開發服務。

Sathya Krishnasamy 對研究、構思和整體實作貢獻良多。

資料可用性聲明 (DAS)、資料分享、可重複性及資料庫

沒有資料庫。

應用人工智能產生的文字或相關技術

無。

鳴謝

Pankhuri Gupta 是美國馬薩諸塞州波士頓東北大學 (Northeastern University) 軟體工程碩士學生，協助校長進行使用者介面設計與實作。她的聯絡方式是 gupta@pankh@northeastern.edu。

參考文獻

1. Buterin V. Ethereum whitepaper [Internet]. Ethereum.org; 2014 [cited 2024 Aug 01].Available from: https://ethereum.org/en/ whitepaper/
2. WEB3 與金融包容性：縮小差距 [網際網路]。www.linkedin.com。[cited 2024 Aug 01].Available from: https://

引用：Blockchain in Healthcare Today 2024, 7: 341 - https://doi.org/10.30953/bhty.v7.341

www.linkedin.com/pulse/WEB3- financial- inclusion- bridging-gap-liveplexplatform-ojazc/

3. 美國衛生與人類服務部 [網際網路]。gov.; 2019 [cited 2024 Aug 01].Available from: https://www.hhs.gov
4. 閾值存取控制 (TACo)。Threshold.network; 2024 [cited 2024 Aug 15].Available from: https://docs.threshold.network/applications/threshold-access-control