BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE
TECHNISCHE KURZDARSTELLUNGEN & KURZBERICHTE

My Holistic Data Share: Eine WEB3-Datenfreigabe-Anwendung: Ausweitung über das Finanzwesen hinaus auf den datenschutzgeschützten dezentralen Austausch mehrdimensionaler Daten zur Verbesserung der globalen Gesundheitsversorgung

Sathya Krishnasamy, MS

ChainAim, Newington, Connecticut, USA DOI:

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

Korrespondierender Autor: Sathya Krishnasamy, E-Mail: sathya.krishnasamy@chainaim.com

Schlüsselwörter: Zugriffskontrolle, Blockchain, Distributed Ledger, Gesundheitswesen, Datenschutz, Schwellenwertkryptographie

Zusammenfassung

Die WEB3-Technologien für Netzwerkarchitekturen, verteilte Ledger und dezentralisierte künstliche Intelligenz stellen einen grundlegenden Wandel in der Art und Weise dar, wie Daten gehandhabt, gespeichert und weitergegeben werden. Diese Innovationen versprechen, die Datenschutzrechte der Verbraucher erheblich zu stärken, indem sie die grundlegenden Schwachstellen herkömmlicher zentralisierter Systeme und selbstverwahrender Geldbörsen beseitigen. Bei herkömmlichen Systemen, die hauptsächlich von Dritten betrieben werden, kommt es häufiger zu Datenschutzverletzungen, die aufgrund der zentralisierten Speicherung und der übermäßigen, manchmal unnötigen Datenverschiebung zu erheblichen Datenlecks führen. Datenschutzverletzungen im Gesundheitswesen sind weltweit ein wachsendes Problem. Mehrere Krankenhäuser mussten aufgrund der Auswirkungen von Ransomware auf die Patientenversorgung und den Datenschutz ihren Betrieb einstellen. WEB3 Geldbörsen sind eine wichtige Komponente, die sich zu einer bedeutenden Kraft für die globale finanzielle Eingliederung entwickelt, insbesondere in Entwicklungsländern. Sie fördern die Integration, senken die Kosten und geben dem Einzelnen die Möglichkeit, sich selbst zu verwahren. Obwohl diese Wallets noch stark verbesserungsbedürftig sind, nimmt ihre Nutzung stetig zu. Laut einem Bericht von Statista aus dem Jahr 2023 wird erwartet, dass die Zahl der Nutzer von Kryptowährungen bis 2025 weltweit auf über 500 Millionen ansteigt, mit einem erheblichen Wachstum in den Schwellenländern. In diesem Beitrag wird ein Konzept vorgestellt, das über Kryptowährungen und Finanzen hinausgeht und sich auf alltägliche, reale Anwendungsfälle bezieht, bei denen ein kombinatorischer Zugriff auf die ganzheitlichen Daten einer Person erforderlich ist, darunter Finanz- und Gesundheitsdaten, Genomdaten, Patientenverfügungen usw., die durch dezentrale Identifikatoren und nicht fungible Token-Badges, die bestimmte Empfänger identifizieren, geschützt und mit bestimmten Akteuren geteilt werden müssen, die aufgrund ihrer Rolle im WEB3-Ökosystem identifiziert werden. Der Autor stellte das Konzept im April 2024 an der ETHBoston vor, erhielt Auszeichnungen für eine primäre Implementierung unter Verwendung der zugrundeliegenden Schwellenwertkryptografie-Technologien und erweiterte es zu einer konzeptionellen, ganzheitlichen Datenfreigabeanwendung für das globale Gesundheitswesen, wie sie in diesem Papier vorgestellt wird.

Eingegangen: August 1, 2024; Angenommen: August 25, 2024; Veröffentlicht: 31. August 2024

WEB3 ist eine Sammlung von aufkommenden Technologien. Sie umfasst verteilte Ledger, autonome Identifikationen (IDs) und künstliche Intelligenz (AI), und fördert Konzepte für das Eigentum an Daten und Vermögenswerten. WEB3 bietet eine dezentralisierte Alternative zu herkömmlichen Bankensystemen.[1] WEB3-Technologien ermöglichen den Zugang zu Finanzdienstleistungen für Menschen, die keine oder nur wenige Banken haben.[2] Sie senken die Transaktionskosten und ermöglichen es dem Einzelnen, durch selbstverwaltete WEB3-Wallets Daten mit anderen zu teilen. Darüber hinaus stehen die Grundsätze der gemeinsamen Datennutzung im Web 3.0 im Einklang mit modernen Datenschutzgesetzen, was die Kontrolle der Nutzer über ihre persönlichen Daten verbessert. Diese Innovationen versprechen die Rechte der Verbraucher auf Datenschutz deutlich zu verbessern, indem einige grundlegende Schwachstellen herkömmlicher zentralisierter Systeme beseitigt werden.

Bei herkömmlichen Systemen kommt es häufiger zu Datenschutzverletzungen, die aufgrund von Schwachstellen in der zentralen Speicherung und übermäßiger, manchmal unnötiger Datenbewegung zu erheblichen Datenlecks führen. Das Potenzial der WEB3-Technologien zur Stärkung der Datenschutzrechte der Verbraucher ist ein Schritt in eine sicherere Zukunft. Datenschutzverletzungen im Gesundheitswesen sind weltweit ein wachsendes Problem. Mehrere Krankenhäuser mussten ihren Betrieb aufgrund von Ransomware einstellen, was sich auf die Patientenversorgung und den Datenschutz auswirkte.[3]

Datensouveränität und -kontrolle mit Self-Custody Im Zusammenhang mit WEB3-Wallets bezieht sich Self-Custody auf die Verwaltung des eigenen digitalen Vermögens, indem man seine privaten Schlüssel bei sich selbst aufbewahrt, ohne sich auf Drittanbieter zu verlassen, die die Schlüssel missbrauchen könnten. Die Selbstverwahrung stimmt grundsätzlich mit den Grundsätzen des Datenschutzes überein, da sie die individuelle Kontrolle über persönliche Daten betont. In vielen Artikeln der allgemeinen Datenschutzverordnung der Europäischen Union werden die Begriffe personenbezogene Daten, Datenminimierung, Rechtmäßigkeit und ein dem Risiko und den Meldungen angemessenes Sicherheitskonzept definiert. In ähnlicher Weise enthalten die Abschnitte des kalifornischen Gesetzes zum Schutz der Privatsphäre von Verbrauchern Bestimmungen zur Definition personenbezogener Daten, zum Recht auf Kenntnisnahme, zum Opt-out, zur Löschung und zur Nichtdiskriminierung bei Widerspruch. Speziell für die Einhaltung des Health Insurance Portability and Accountability Act (Gesetz über die Übertragbarkeit von Krankenversicherungen und die Rechenschaftspflicht) sind die wichtigsten Vorschriften der Datenschutz (der sicherstellt, dass alle betroffenen Einrichtungen und Geschäftspartner die Verbraucherdaten schützen), die Sicherheit (die administrative, physische und technische Schutzmaßnahmen vorschreibt) und die Benachrichtigung bei Verstößen. Diese Vorschriften sehen vor, dass Einzelpersonen Eigentümer ihrer Daten sind, dass sie den Nutzern ihrer Daten ihre ausdrückliche Zustimmung erteilen müssen und dass die benötigten Informationen für einen bestimmten Zeitraum und für bestimmte Verwendungszwecke aufbewahrt werden, wobei die Zugriffsrechte, die Verwendung und der Widerruf der Daten vollständig nachvollziehbar sind. Die Selbstverwahrung verringert die Abhängigkeit von Drittanbietern, was zu einer Verringerung von Datenmissbrauch oder Datenschutzverletzungen führen kann, wenn die Systeme nicht sicher genug sind.

Einschränkungen der aktuellen Wallets

Derzeitige Wallets speichern kryptonative Vermögenswerte wie Kryptowährungen und nicht-fungible Token (NFTs) vorwiegend für Finanzanwendungen und -dienste und bis zu einem gewissen Grad auch für die Speicherung digitaler Sammlerstücke. In diesen Anwendungsfällen werden Sammlerstücke in einem dezentralisierten Speicher wie dem InterPlanetary File System (IPFS) gespeichert und haben einen Zeiger darauf in der Wallet und den Metadaten. Es sind jedoch viele Anwendungsfälle denkbar, da dieselben Konzepte auch für die Verwaltung des Zugangs zu anderen Formen personenbezogener Informationen zusätzlich zu den Finanzdaten gelten können. Dazu gehören u. a. Gesundheitsdaten, Genomdaten und Patientenverfügungen, bei denen verschiedene Formen von Daten von Personen eingesehen werden müssen, die bestimmte Rollen im sozialen Kontext spielen, was eine logischere Verwendung darstellt.

Die Selbstverwahrung setzt voraus, dass der Einzelne mit seinen privaten Schlüsseln gut umgehen kann und versiert ist. Außerdem ist die Wallet immer noch nicht sehr benutzerfreundlich und erfordert ein gewisses Maß an technischem Verständnis und eine Reihe nicht trivialer Schritte, die zu befolgen sind. Einige Nutzer benötigen möglicherweise technische Unterstützung bei der Verwaltung ihrer Schlüssel und müssen sich an Dritte wenden. Je nach den Sicherheitsfähigkeiten und der Integrität der Verwahrer kann dies zu Risiken wie Identitätsdiebstahl, Verlust von Geldern, Verletzung der Privatsphäre und anderen führen.

Daraus ergibt sich die Notwendigkeit dezentralisierter Protokolle, die widerstandsfähiger sind als zentralisierte Verwahrer, und einer datenblinden Dezentralisierung auf Protokollebene, die die Widerstandsfähigkeit der Datenverwaltung erhöht, indem sie die Informationen der Nutzer verschlüsselt und kritische Verwaltungssysteme einsetzt, die dezentralisiert sind und von kryptografischen Mechanismen verwaltet werden, die die Anmeldeinformationen für den Zugriff auf die Daten auf der Grundlage granularer Rollen für bestimmte Zeiträume wieder zusammensetzen können. Eine Schlüsseltechnologie, mit der diese Dezentralisierung erreicht werden soll, ist die Schwellenwertkryptografie.

Schwellenwert-Kryptographie

Die Schwellenwertkryptographie ist ein kryptographisches Verfahren, bei dem ein kryptographischer Schlüssel in mehrere Anteile aufgeteilt wird, die auf verschiedene Parteien verteilt werden. Eine vordefinierte Anzahl dieser Anteile (die Schwelle) muss kombiniert werden, um kryptografische Operationen wie Entschlüsselung oder Signierung durchzuführen. Wenn ein Schlüssel beispielsweise in 10 Anteile aufgeteilt ist und der Schwellenwert auf 6 festgelegt ist, können alle 6 Anteile zur Rekonstruktion des Schlüssels verwendet werden, aber weniger als 6 Anteile liefern keine Informationen über den Schlüssel. Jeder Anteil befindet sich bei einem bestimmten Verwahrer, und dieser kennt nur einen Teil des Schlüssels, nicht den gesamten Schlüssel.

Vorteile der Schwellenwertkryptographie

Zu den Vorteilen der Schwellenwertkryptografie gehören erhöhte Sicherheit, Redundanz und Zuverlässigkeit sowie die Autorisierung durch mehrere Parteien.

Erhöhte Sicherheit

Durch die Verteilung von Schlüsselanteilen auf mehrere Parteien stellt die thresh-old-Kryptographie sicher, dass keine einzelne Einheit vollständigen Zugang zu sensiblen Informationen hat. Dieser Ansatz mindert das Risiko eines unbefugten Zugriffs und bietet eine zusätzliche Sicherheitsebene für die Verwaltung wichtiger Datensätze. In der Praxis bedeutet dies, dass selbst wenn ein böswilliger Akteur eine Freigabe kompromittiert, er nicht auf die sensiblen Daten zugreifen oder Operationen durchführen kann, ohne die erforderliche Mindestanzahl von Freigaben zu erhalten. Keine einzelne Person hat die Möglichkeit, die Daten unabhängig voneinander zu kompromittieren, was die Wahrscheinlichkeit von Datenschutzverletzungen und Insider-Bedrohungen drastisch reduziert.

Redundanz und Verlässlichkeit

Die Schwellenwertkryptografie ermöglicht den Betrieb auch dann, wenn einige Schlüsselanteile verloren gehen oder gefährdet sind, solange die Schwellenzahl der Anteile intakt bleibt. Dadurch wird gewährleistet, dass wichtige Datensätze auch bei technischen Problemen oder Sicherheitsverletzungen zugänglich und sicher bleiben.

Autorisierung durch mehrere Parteien

Mit Hilfe der Schwellenwertkryptografie kann sichergestellt werden, dass Daten nicht ohne die Zustimmung mehrerer Parteien manipuliert werden können. Dies erleichtert die sichere Zusammenarbeit, da Forscher Daten gemeinsam nutzen und analysieren können, ohne dass sie in ihrer Gesamtheit einem einzelnen Teilnehmer offengelegt werden. Dies ist besonders

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 341 - https://doi.org/10.30953/bhty.v7.341

Dies ist besonders wichtig bei klinischen Versuchen und Forschungsstudien, bei denen die Integrität der Daten für die Ableitung gültiger Schlussfolgerungen und die Gewährleistung der Patientensicherheit unerlässlich ist. In Szenarien, an denen mehrere Beteiligte beteiligt sind, z. B. bei der Nachlassplanung oder bei Patientenverfügungen, ermöglicht die Schwellenwertkryptografie eine sichere Autorisierung durch mehrere Parteien. Dadurch wird sichergestellt, dass Entscheidungen oder Maßnahmen im Zusammenhang mit sensiblen Daten den Konsens mehrerer autorisierter Parteien erfordern, was die Sicherheit und Integrität erhöht.

Einschränkungen und Herausforderungen der Schwellenwertkryptografie

Komplexität, Verfügbarkeit und Skalierbarkeit sind Einschränkungen und Herausforderungen.

Komplexität

Die Aufteilung des kryptografischen Schlüssels und die Verwaltung von Freigaben erfordern anspruchsvolle Protokolle. Die korrekte Implementierung dieser Protokolle und die Gewährleistung der Widerstandsfähigkeit bei verschiedenen Sicherheitsangriffen ist eine Herausforderung.

Verfügbarkeit

Die Rekonstruktion des Schlüssels erfordert die aktive Beteiligung mehrerer Parteien, was ineffizient sein kann, wenn die Parteien geografisch verstreut sind oder eine uneinheitliche Verfügbarkeit aufweisen.

Skalierbarkeit

Mit zunehmender Anzahl von Teilnehmern und Anteilen steigt die Komplexität, der Kommunikations- und Verfügbarkeitsaufwand, was zu Skalierbarkeitsproblemen führen kann.

Die spezifische Implementierung der Schwellenwertkryptografie kann variieren, je nachdem, wie die Verteilung der kryptografischen Schlüssel erfolgt und wie die Zugriffskontrolle für den Datenabruf konfiguriert ist. Der Mechanismus zur Wiederzusammensetzung der Schlüsselanteile und der Schwellenwerte ist ebenfalls konfigurierbar. In einem dezentralisierten Betriebsmodus kann die Protokollimplementierung die Schlüsselanteile über die Validierungsknoten hinweg dezentralisieren.

MyHolisticDataShare und Möglichkeiten im globalen Gesundheitswesen

MyHolisticDataShare ist eine WEB3-Datenfreigabeanwendung, die sich mit den Beschränkungen befasst und neuere Konzepte für die Organisation und Speicherung von Benutzerdaten einführt, die über Finanzdaten und digitale Sammlerstücke hinausgehen und reale Werte wie medizinische Aufzeichnungen umfassen. Diese fortschrittlichen Richtlinien können durch die Erweiterung der kryptographischen Grundregeln für die sichere gemeinsame Nutzung von Daten verwaltet werden. Der Zugang zu diesen Aufzeichnungen kann individuell für bestimmte Parteien und ihre Rollen im sozialen Kontext bereitgestellt und bemessen werden, oder er kann eine Kombination von Werten für einen bestimmten Empfänger oder eine Rolle sein.

MyHolisticDataShare ist eine überarbeitete und erweiterte Adaption der SocialSecureShare-Anwendung, die ursprünglich vom Autor im April 2024 an der ETHBoston entwickelt wurde und den Preis für das beste Projekt für Privatsphäre und Gemeinschaft gewann. MyHolisticDataShare ist ein technischer Prototyp für Verbraucher und Empfänger solcher Daten, der viele Aspekte der verbrauchergesteuerten Datenfreigabe und deren Auswirkungen auf die Gesundheitsversorgung und die Verknüpfung von Daten mit der Gesundheit in regulären und Notfall-Settings sowie der Gesundheit und den Finanzen für Bemühungen wie die sozialen Determinanten der Pflege kombiniert.

Diese aufkommenden Technologien zum Schutz der Privatsphäre, wie die Schwellenwertkryptographie und die Zugangskontrolle, zeigen Möglichkeiten zur Förderung des verbrauchervermittelten Datenaustauschs auf und ermöglichen gleichzeitig einen verbesserten Schutz der Privatsphäre durch die Verringerung einzelner Fehlerquellen, eine granulare und zusammensetzbare Zugangskontrolle und die Möglichkeit von Kontrollinstanzen, die ebenfalls als Knotenpunkte teilnehmen, um eine bessere Sichtbarkeit zu erhalten.

Technischer Aufbau von MyHolisticDataShare

MyHolisticDataShare verwendet kryptografische Datenschutz-Primäre und dezentrale Mechanismen - wie die Schwellenwertkryptografie zum Schutz der Privatsphäre beim Entschlüsselungszugriff auf verschlüsselte Daten, die in einem dezentralen Speicher abgelegt sind - auf der Grundlage von NFTs, die Token zur Identifizierung eindeutiger Elemente sind. Die NFTs sind einzigartige Token, die eine Sache und nur eine Sache repräsentieren und zur Darstellung eines bestimmten Ausweises verwendet werden können. Die Verwaltung des Protokolls und der Anwendung kann diese Ausweise zuweisen.

MyHolisiticDataShare basiert auf der dezentralen Implementierung von Schwellenwertkryptographie unter Verwendung des Threshold-Protokolls und des Threshold-Access-Control-Protokolls (TACo).[4]Diese NFTs werden bestimmten Identitätsausweisen zugeordnet, die Personen oder Rollen zugeordnet sind, die auf der Grundlage der dezentralen Identitätsüberprüfung der Geldbörsen, die diese Zugangsausweise besitzen, Zugang zu den Daten des Kunden erhalten.

Das Threshold-Netzwerk bietet eine ganze Reihe dezentraler Threshold-Kryptographie-Dienste, um die Privatsphäre und Souveränität der Nutzer in Permission Blockchains zu erhöhen (Abbildung 1). Die Schwellenwertkryptografie schützt Daten durch die Verteilung von Operationen auf ein Netzwerk unabhängiger Knoten, erhöht die Sicherheit und Verfügbarkeit und verringert die Abhängigkeit von vertrauenswürdigen Parteien. Das Threshold-Netzwerk verwendet das TACo-Protokoll für die Zugriffskontrolle. Der Dateneigentümer kann seine Nutzdaten, die aus mehreren Abschnitten bestehen können, verschlüsseln und sie an Offline-Speicherorten speichern. Je nach Bedarf können diese Speicherelemente auch in dezentraler Speicherung verwendet werden. In diesem Beispiel speichert der Dateneigentümer die verschlüsselten Daten im IPFS, einer beliebten dezentralen Speicherlösung.

Die TACo teilt ein gemeinsames Geheimnis - einen Entschlüsselungsschlüssel - in mehrere *Anteile* auf und verteilt diese unter den autorisierten und besicherten Knotenbetreibern (d. h. den Akteuren im Schwellenwertnetz). Eine Mindestanzahl - ein *Schwellenwert* - der Betreiber, die über die Schlüsselanteile verfügen, muss online sein und aktiv an Teilentschlüsselungen teilnehmen. Diese werden anschließend auf dem Client des Anfragenden kombiniert, um die ursprünglichen Klartextdaten wieder zu rekonstruieren. Jede Daten-Nutzlast ist an Bedingungen geknüpft, die den Zugang granular einschränken können. Der Dateneigentümer kann eine Reihe von Zugriffsbedingungen definieren, die Zugriffskontrollprüfungen enthalten können, wie z. B. "Ist die

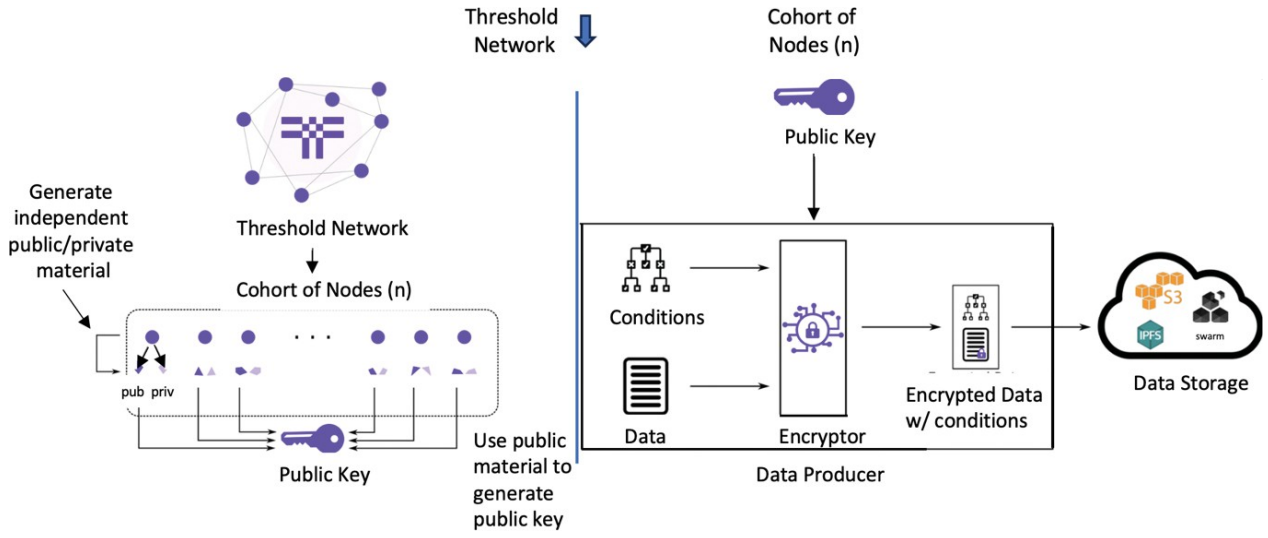

Abb. 1. Screenshots der Schwellenwert-Netzwerk-Implementierung der Schwellenwert-Kryptografie. Quelle: https://docs.threshold.network/applications/threshold-access-control/key-concepts.
Quelle: Copyright des Autors, 2024.

Besitzt der Antragsteller eine bestimmte NFT, die einen Ausweis eines Rettungssanitäters darstellt?" oder "...ein Sozialarbeiter, der Patienten hilft?". Sie können auch mit anderen Elementen kombiniert werden, wie z. B. "Bittet der Anfragende um Zugang während einer Zeit, für die der Dateneigentümer Zugang gewährt?"

Die Antragsteller beweisen, dass sie die Bedingung - ihr Recht auf eine bestimmte Anzahl von Entschlüsselungsanteilen - erfüllen, indem sie eine Transaktion unterzeichnen, die ihren Besitz einer bestimmten WEB3-Brieftasche (in diesem Fall die MetaMask-Brieftasche im Polygon-Testnetz Amoy) bestätigt. Diese Wallet wird daraufhin überprüft, ob die spezifische Bedingung erfüllt ist (z. B. der Besitz einer NFT, um auf die Datenbestände zugreifen zu können).

MyHolisticDataShare ist so konzipiert, dass es aus verschiedenen Arten von Datensätzen besteht, wie in Abbildung 2 dargestellt, die ein Verbraucher in einer dezentralen Speicherinfrastruktur wie dem IPFS speichern könnte, wobei die Metadaten den URI definieren.

Die Implementierung erfolgt im Polygon-Blockchain-Amoy-Testnetz, wobei der MetaMask-Wallet-Zugang die Zugangskontrolle über NFT-Badges speichert.

Die Nutzer können flexibel verschiedene Arten von Datensätzen speichern, darunter Finanz-, Gesundheits- und Genomdaten sowie erweiterte Richtlinien.

Finanzielle Aufzeichnungen

Dazu gehören herkömmliche Finanzkonten, Krypto-Konten, Kontoauszüge, Kreditbriefe usw., die der Nutzer sicher aufbewahren und für bestimmte Empfänger freigeben kann, die er für bestimmte finanzbezogene Zwecke für notwendig hält.

Gesundheitsdaten

Dazu gehören grundlegende Gesundheitsdaten wie Laborberichte, Diagnosen, diagnostische Bilder und Termine, deren Weitergabe der Nutzer für bestimmte gesundheitsbezogene Zwecke für erforderlich hält.

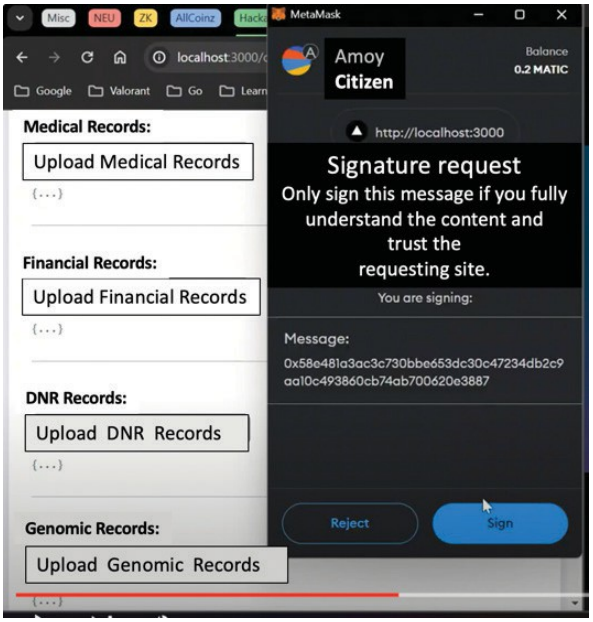

Abb. 2. Screenshot einer verschlüsselten Benutzerakte.
Quelle: Copyright des Autors, 2024.

Genomische Datensätze

Diese können bestimmte granulare, hochspezialisierte und persönliche Informationen enthalten, wie z. B. genomische Aufzeichnungen, die der Nutzer mit bestimmten Forschern und Klinikern von Interesse teilen kann.

Erweiterte Verfügungen

Diese können spezifische Informationen über Gesundheitsvollmachten enthalten, wie z. B. "Do Not Resuscitate" (DNR), die für medizinisches Personal und Notfalltechniker wichtig sind.

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 341 - https://doi.org/10.30953/bhty.v7.341

Abbildung 2 zeigt einen Screenshot des Prozesses, bei dem der Dateneigentümer und ein Bürger in einem sozialen Umfeld die Transaktion unterzeichnen, wenn sie die verschiedenen zu verschlüsselnden Daten in einem dezentralisierten Speicher speichern wollen. Abbildung 3 zeigt einen Screenshot der Daten-Nutzlast und der Details des dezentralen Speicherortes, sowie die Rückmeldungen zur Bestätigung.

MyHolisticDataShare-Empfängerausweise

Die Teilnehmer des Blockchain-Netzwerks erhalten spezifische NFT-Abzeichen, die von einer regierenden, datenautonomen Organisation verwaltet werden, die die dezentralen Kennungen registriert. So kann z. B. einem dezentralen Identifikator (DID) im Netzwerk ein primärer Arztausweis zugewiesen werden, während einem anderen DID ein Notarztausweis zugewiesen werden kann. zugewiesen werden, was den spezifischen sozialen Kontext für den Datenbedarf darstellt.

Die Ausweise für den Sozialdatenkontext und ihre Konfigurationen werden in einem Register zur Verfügung gestellt, das dem Benutzer anzeigt, welche Ausweise auf welche Art von Daten zugreifen können. In der Standardkonfiguration hat ein Rettungssanitäter beispielsweise Zugriff auf Krankenakten und Patientenverfügungen, nicht aber auf Finanzdaten. Ein Genomforscher könnte einen Ausweis besitzen, der sein Interesse an einer bestimmten Art von Genomdaten verdeutlicht, über die er verfügt. Der kombinatorische Zugang könnte auch granular gesteuert werden. So könnte beispielsweise ein Sozialarbeiter Zugang zu Gesundheits- und Finanzdaten haben, um bei der Planung der Koordinierungshilfe für soziale Gesundheitsfaktoren zu helfen. Abbildung 4 zeigt die verschiedenen Arten von Ausweisen, die als NFTs in den Geldbörsen der Datenempfänger gespeichert werden sollen. Wenn die

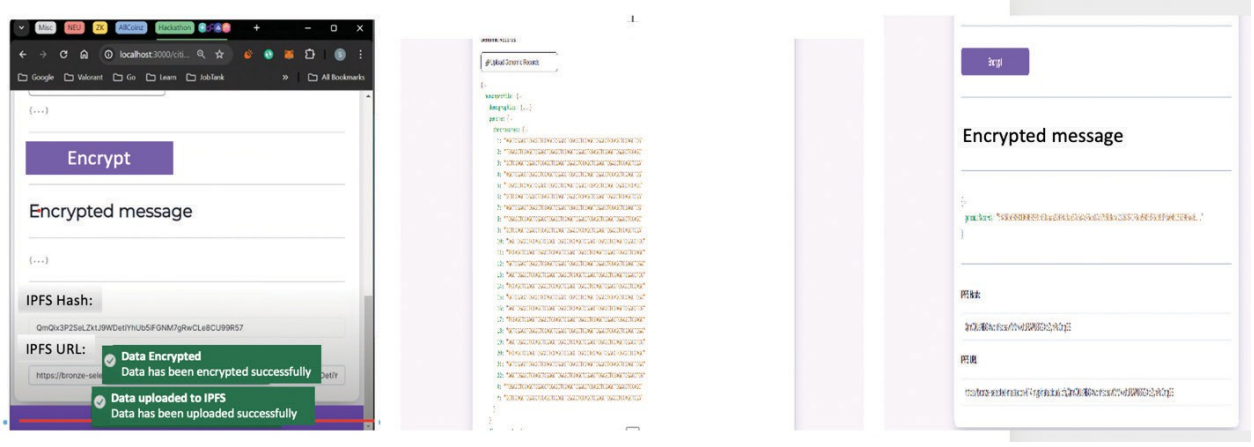

Abb. 3. Erfolgreich verschlüsselter Inhalt auf der Grundlage synthetischer Beispieldaten. Quelle: Copyright des Autors, 2024.

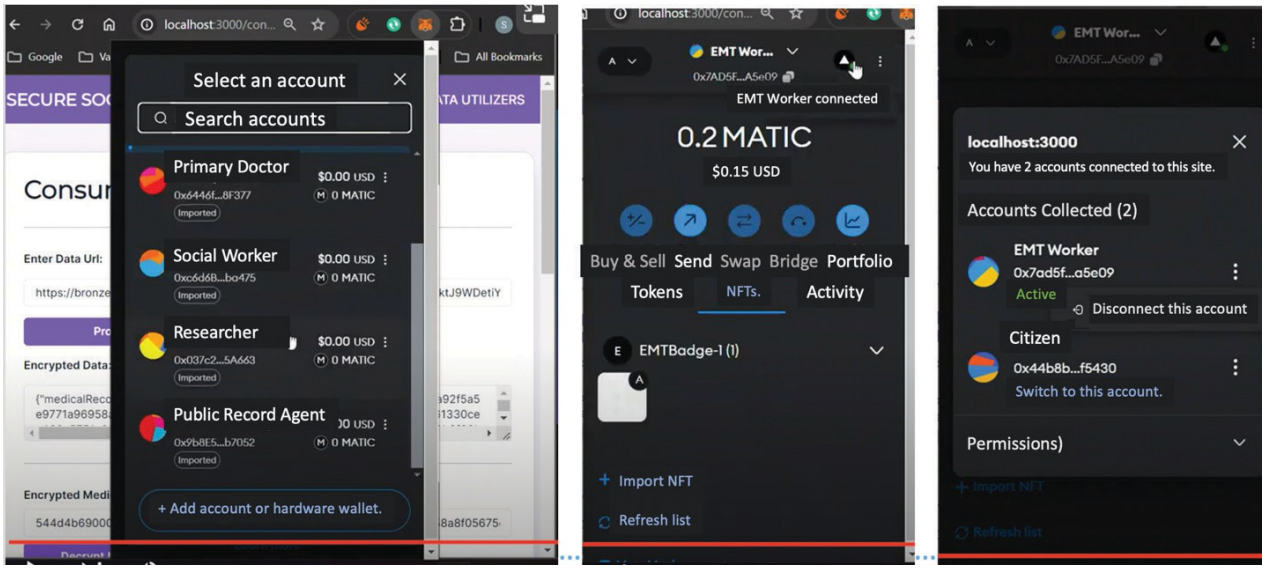

Abb. 4. Verschiedene unterschiedliche Abzeichen, modelliert als NFTs, die dezentralen IDs zugewiesen sind. EMT: Emergency Medical Technician; ID: Identifikation; NFTs: Nicht-fungible Token.
Quelle: Copyright by the author, 2024.

Wenn ein Datenempfänger versucht, auf die verschlüsselten Daten des Dateneigentümers zuzugreifen, wird auf der Grundlage der festgelegten Zugangskontrollen das Vorhandensein dieser NFT-Badges überprüft, um den Zugang zu erlauben oder zu verweigern.

Entschlüsselungsergebnisse und Datenverfügbarkeit

Auf der Grundlage der Quorum-Konfigurationen für die Dezentralisierung des Netzes und der NFT-Definitionen kann der Nutzer seine Transaktionen signieren, um sie zu verschlüsseln, so dass sie für bestimmte DIDs mit spezifischen Datenanforderungen, die als eindeutige NFT-Definitionen modelliert sind, zur Entschlüsselung zur Verfügung stehen. Diese können ebenfalls modelliert werden, und das entschlüsselte Protokoll wird einen bestimmten Zeitpunkt für die Entschlüsselung abwarten. Der Ausweis und die Protokolldefinitionen würden den Zugang zur Entschlüsselung ermöglichen. Der Zugriff auf alle anderen Daten ist nicht möglich. Abbildung 5 zeigt die Situation, in der während der Entschlüsselung nach einem bestimmten NFT-Badge gesucht wird, das Recht zur Entschlüsselung überprüft und ausgeführt wird und die Entschlüsselung erfolgreich ist. Beispiele hierfür sind der rechtmäßige Zugang zu genomischen Aufzeichnungen für einen ausgewiesenen Forscher oder eine medizinische Fachkraft mit Zugang zu DNR-Daten. In Abbildung 6 ist eine Situation dargestellt, in der jemand, der nicht über den erforderlichen NFT-Ausweis verfügt, die Daten nicht entschlüsseln kann. Zum Beispiel hat jemand, der keinen NFT-Ausweis für Sozialarbeiter b e s i t z t , keinen Zugang zu den die Gesundheits- und Finanzdaten der Eigentümer.

In der Praxis wird die diesem Protokoll und der Anwendung zugrunde liegende Verwaltung eine Offline-Verifizierung für die Ausstellung der Ausweise beinhalten, möglicherweise unter Einbeziehung einer Kombination aus Gesundheitssystemen und sozialen Organisationen, die die Rollen und Zugangskriterien für die Zugangsberechtigung festlegen. So kann zum Beispiel ein ausgewiesener Sozialarbeiter mit spezifischen Zugangskontrollen, der vielleicht in der Pflegekoordination oder in der Gemeindepflege tätig ist, sowohl auf die medizinischen als auch auf die finanziellen Daten zugreifen, um eine ganzheitliche Betreuung für diesen Patienten auf der Grundlage seiner sozioökonomischen Stellung zu finden, wobei die Betreuung nicht nur die medizinische Versorgung, sondern auch die Suche nach einer Wohnung, einem Transportmittel und anderen Funktionen umfassen könnte, die seinen Bedarf belegen.

Mit zunehmender Reife der zustimmungsfreien Blockchains sehen wir einen zunehmenden Trend bei den Verbrauchern zur Annahme von zustimmungsfreien Blockchains, gemessen an selbstverwalteten Wallets und der Teilnahme an WEB3-basierten sozialen Anwendungen von verschiedenen Unternehmen und Einzelpersonen. Diese Aktivitäten können auch für die Annahme von Gesundheitsdaten durch die Verbraucher genutzt werden, wenn sie sorgfältig geplant werden, mit angemessenen Kontrollen und Abwägungen, einschließlich einiger regulatorischer Knoten, die auf öffentlichen/hybriden Blockchains betrieben werden, was langsam beginnt.

Die Schwellenwertkryptografie ist kein Konkurrent für andere Techniken zum Schutz der Privatsphäre, sondern ergänzt andere Techniken wie die vollständig homomorphe Verschlüsselung und das Multi-Party-Computing. In diesen Fällen können Schwellenwertsysteme noch eine weitere Sicherheitsebene hinzufügen, in der der Zugriff auf den verschlüsselten Inhalt kontrolliert werden kann, wenn die

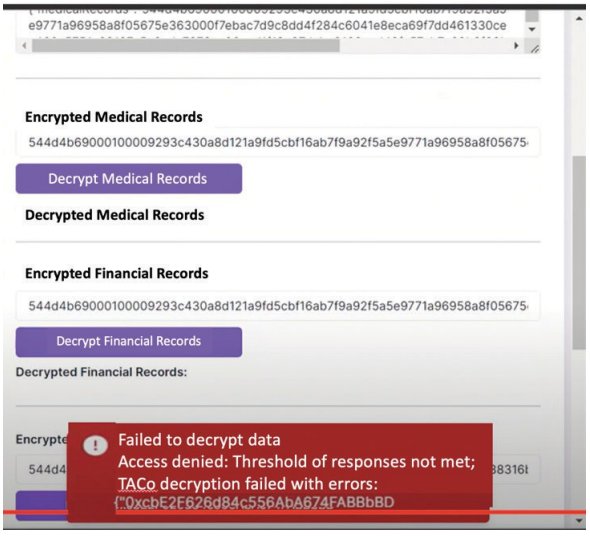

Abb. 6. Screenshot des verweigerten Zugriffs basierend auf der granularen Zugriffskontrolle. TACo: Threshold Access Control. Quelle: Copyright des Autors, 2024.

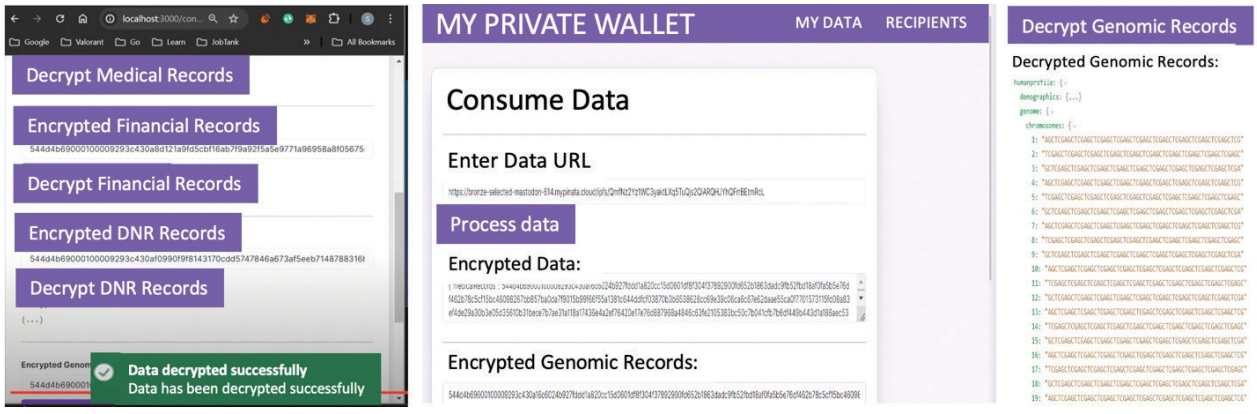

Abb. 5. Beispiel für die Ver- und Entschlüsselung von synthetischen Beispieldaten mit rechtmäßigem Zugriff. URL: Uniform Resource Locator. Quelle: Copyright des Autors, 2024.

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 341 - https://doi.org/10.30953/bhty.v7.341

das anfordernde System auf Daten von verteilten Endpunkten zugreift oder Berechnungen mit den verschlüsselten Daten durchführt. In diesen Kontexten könnte es sogar noch wichtiger werden, dass die Zugangskontrollsysteme "kugelsicher" sind. In einem anderen aktuellen Beitrag erörtert der Autor das Aufkommen von Zero-Knowledge-Beweisen und maschinellem Lernen, die ebenfalls sehr komplementär sind und bei denen der Datenaustausch durch die Vorlage von Beweisen für die Überprüfer minimiert werden kann. Die gemeinsame Nutzung von Daten unter Wahrung des Schutzes der Privatsphäre könnte auch ein weiteres Problem angehen, nämlich organisations- und bereichsübergreifende Datenverletzungen. Wenn es beispielsweise im Einzelhandel oder im Bankensektor zu Datenschutzverletzungen kommt, könnte dies den Zugang zu Gesundheitsdaten gefährden, da einige persönliche Informationen durchsickern und böswilligen Nutzern mehr Möglichkeiten bieten. Mit einer solchen ganzheitlichen Datenfreigabe und einem granularen und kompatiblen Zugang könnten die Verbraucher jedoch mehr Kontrolle über ihre Daten haben und in der Lage sein, viel besser auf Angriffe zu reagieren.

Eine wichtige Verbesserung, die in WEB3 erforderlich ist, ist die Benutzerfreundlichkeit für die Verbraucher, da es für die Benutzer schwierig ist, den Überblick über die Schritte und die unheimlichen Adressen zu behalten. In diesem Projekt wurde bereits versucht, das UI/UX (User Interface Design/User Experience Design) sehr nahe an einer Web 2-Webseite zu halten, zumindest was die Verwaltung der Daten betrifft. Es verwendet eine verbraucherorientierte Konzeption um JSON (JavaScript Object Notation) Datenstrukturen, Standards und einfache Bildschirme. In den folgenden Iterationen wird untersucht, wie die Datendefinitionen auch in einer Browsererweiterung enthalten sein können, und es werden fortgeschrittene Mechanismen zur Abstraktion von Konten und zur Vereinfachung von Identitäten verwendet, um die Benutzerfreundlichkeit zu erhöhen.

Schlussfolgerungen und zukünftige Arbeiten

MyHolisticDataShare hat eine neue Erweiterung der WEB3-Technologien demonstriert, die auf dezentraler Datenfreigabe und Schwellenwertkryptographie zur Dezentralisierung des Entschlüsselungszugriffs auf nicht zentralisierte Quorum- und konfigurierbare Schwellenwertdefinitionen beruht. Dies ist noch ein einführendes Konzept, und die endgültige Version der Implementierung wird von den Definitionen des regulatorischen Kontexts, dem Governance-Design der dezentralen autonomen Organisation sowie der Reife und den erfolgreichen DID-Governance-Prozessen in einem sozialen Kontext abhängen.

Alle Versuche, Blockchains im Mainstream-Bereich zu testen, müssen sorgfältig geplant werden und hängen von spezifischen Blockchains ab, einschließlich bestimmter öffentlicher/privater/hybrider Architekturen. Dieser konzeptionelle Prototyp zeigt alternative Wege auf, wie die WEB3-Technologien potenzielle Lösungen für chronische Probleme in zentralisierten Systemen mit dem Datenschutz und der gemeinsamen Nutzung von Daten bieten, vor allem die Verringerung von Single-Point-of-Trust-Fehlern und eine granulare und komponierbare Zugangskontrolle.

Der Autor beabsichtigt, diese Anwendung zu einer Browser-Erweiterung für Geldbörsen auszubauen, wenn die Landschaft reift, insbesondere wenn es darum geht, wie Geldbörsen und WEB3-Datenfreigabeanwendungen und ihre Verantwortlichkeiten genauer definiert werden. Ergänzende Technologien wie Zero-Knowledge-Systeme und vollständig homomorphe Verschlüsselungen können dieses Konzept erweitern, um verbesserte, datenschutzfreundliche Designs für den vom Verbraucher initiierten und nachgewiesenen Datenaustausch zu schaffen. Die Bemühungen des Autors bei ChainAim zielen darauf ab, Beziehungen zu Standardisierungsorganisationen und Technologiestiftungen aufzubauen, um den Bedarf an Skalierbarkeit und Governance für die Förderung eines solchen Datenaustauschs zu ermitteln.

Finanzierung

Keine.

Interessenkonflikte

Keine.

Mitwirkende

Sathya Krishnasamy ist der Präsident und Leiter von ChainAim Technologies. Er verfügt über 25 Jahre Erfahrung im Bereich Managed Care bei führenden US-Gesundheitsunternehmen, darunter Aetna und Anthem. Er konzentriert sich auf aufkommende Technologien, einschließlich künstlicher Intelligenz/Maschinenlernsysteme und Dis-Tributed-Ledger-Technologien. Darüber hinaus ist er als Berater bei zahlreichen Bemühungen der Branche im Bereich der Zusammenarbeit zwischen Kostenträgern und Leistungserbringern, bei Standardisierungsorganisationen und bei Bestrebungen wie Account Aggregators in Indien tätig, die die Bereiche Fintech, Gesundheitswesen und Skills voranbringen. Derzeit ist er Präsident und Geschäftsführer von ChainAim, das technische Strategieberatung sowie Anwendungs- und Entwicklungsdienstleistungen anbietet.

Sathya Krishnasamy war an der Forschung, Konzeption und Gesamtimplementierung beteiligt.

Datenverfügbarkeitserklärung (DAS), gemeinsame Nutzung von Daten, Reproduzierbarkeit und Datenarchive

Keine Daten-Repositorien.

Anwendung von KI-generiertem Text oder verwandter Technologie

Keine.

Danksagungen

Pankhuri Gupta, Masterstudentin in Software-Engineering an der Northeastern University in Boston, Massachusetts, USA, half dem Auftraggeber bei der Gestaltung und Implementierung der Benutzeroberfläche. Sie kann unter gupta@pankh@ northeastern.edu erreicht werden.

Referenzen

1. Buterin V. Ethereum whitepaper [Internet]. ethereum.org; 2014 [zitiert 2024 Aug 01]. Verfügbar unter: https://ethereum.org/en/ whitepaper/
2. WEB3 und finanzielle Eingliederung: Überbrückung der Kluft [Internet]. www.linkedin.com. [zitiert am 2024 Aug 01]. Verfügbar unter: https://

www.linkedin.com/pulse/WEB3- finanzielle-einbindung-ueberbrueckung-der-kluft-liveplexplatform-ojazc/

3. U.S. Department of Health & Human Services [Internet]. HHS. gov.; 2019 [zitiert 2024 Aug 01]. Verfügbar unter: https://www.hhs.gov
4. Threshold Access Control (TACo). Threshold.network; 2024 [zitiert 2024 Aug 15]. Verfügbar unter: https://docs.threshold.network/applications/threshold-access-control

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 341 - https://doi.org/10.30953/bhty.v7.341