BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

ORIGINELLE FORSCHUNG

Seelengebundene Token: Ermöglichung eines datenschutzgerechten und dezentralen Authentifizierungsmechanismus in der medizinischen Datenspeicherung

Biagio Boi, PhD , Student; Franco Cirillo, PhD , Student; Marco De Santis, PhD , Student; und Christian Esposito, PhD

Fakultät für Informatik, Universität Salerno, Fisciano, Italien Korrespondierender Autor: Franco Cirillo,

E-Mail: fracirillo@unisa.it

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

Schlüsselwörter: Authentifizierung, Blockchain, Gesundheitswesen, Krankenakte, SBT, Self-Sovereign Identity, Soulbound Token, SSI

Zusammenfassung

Kontext: Die Digitalisierung des Gesundheitswesens steht vor großen Herausforderungen aufgrund der vielfältigen Darstellung von Daten und deren Verteilung über verschiedene Krankenhäuser. Darüber hinaus ist die Sicherheit ein zentrales Anliegen, da gesundheitsbezogene Daten den rechtlichen Verpflichtungen der General Data Protection Regulation (GDPR) und ähnlichen Datenschutzgesetzen unterliegen. Standardisierungsbemühungen wie Health Level Seven (HL7) wurden implementiert, um die Interoperabilität von Daten zu verbessern. Die Authentifizierung ist jedoch nach wie vor ein kritisches Thema mit erheblichen Herausforderungen.
Ziel: Diese Forschung zielt darauf ab, den Authentifizierungsprozess zu verbessern und zu stärken, indem eine neuartige Architektur für die dezentralisierte Authentifizierung eingeführt wird. Darüber hinaus wird ein neuer Ansatz zur dezentralen Datenverwaltung vorgeschlagen, der für den effizienten Umgang mit sensiblen medizinischen Daten entscheidend ist.
Die Methodik: Die vorgeschlagene Architektur verfolgt einen nutzerzentrierten Ansatz, der auf der selbstsouveränen Identität (SSI) beruht. Sie führt einen neuen, nicht-fungiblen Token-Typ (NFT) ein, der im medizinischen Kontext als Soulbound Token (SBT) bezeichnet wird und die Benutzerauthentifizierung über verschiedene Krankenhäuser hinweg erleichtert, wodurch eine Föderation miteinander verbundener Einrichtungen entsteht.
Ergebnisse: Die Implementierung der vorgeschlagenen Architektur führte zu einer erheblichen Verkürzung der Authentifizierungszeit über mehrere Krankenhäuser hinweg. Durch den Einsatz von SBT wurde eine sichere und nahtlose Benutzerauthentifizierung gewährleistet, wodurch die Interoperabilität des Gesamtsystems und die Datensicherheit verbessert wurden. Der dezentrale Ansatz minderte auch die Risiken, die mit zentralisierten Authentifizierungsservern verbunden sind.
Schlussfolgerung: In dieser Studie wird erfolgreich eine neuartige dezentrale Authentifizierungsarchitektur für den Gesundheitsbereich vorgestellt, die SSI und SBTs nutzt. Dieser Ansatz beschleunigt den Authentifizierungsprozess und verbessert die Datensicherheit und Interoperabilität zwischen Krankenhäusern. Zukünftige Forschungsarbeiten sollten die Skalierbarkeit dieser Architektur und ihre Anwendung in anderen Bereichen, die strenge Datensicherheitsmaßnahmen erfordern, untersuchen.

Zusammenfassung im Klartext

Diese Forschungsarbeit befasst sich mit den Herausforderungen im digitalen Gesundheitswesen, insbesondere mit der Datenvielfalt, -verteilung und -authentifizierung. Es wird ein dezentralisiertes Authentifizierungssystem eingeführt, das Self-Sovereign Identity und eine neue Art von nicht-fungiblen Token, so genannte Soulbound Tokens, verwendet. Dieses System vernetzt Krankenhäuser, verkürzt die Authentifizierungszeiten, erhöht die Datensicherheit und verbessert die Interoperabilität der Systeme. Durch die Dezentralisierung der Authentifizierung werden die mit zentralisierten Servern verbundenen Risiken gemildert. Die Ergebnisse dieser Studie deuten darauf hin, dass dieser innovative Ansatz für das Gesundheitswesen und möglicherweise auch für andere Branchen mit strengen Anforderungen an die Datensicherheit von Nutzen sein könnte, auch wenn weitere Forschungen zur Skalierbarkeit und breiteren Anwendung empfohlen werden.

Eingereicht: 2. Juli 2024; Angenommen: August 9, 2024; Veröffentlicht: August 31, 2024

Die Verbesserung der Datenverwaltung, der betrieblichen Effizienz und der Patientenversorgung hängt davon ab, dass die Gesundheitsbranche digital wird. Diesem Wandel stehen jedoch mehrere große Hindernisse entgegen, vor allem in Bezug auf Authentifizierung und Datenkompatibilität. Die Daten des Gesundheitswesens sind oft über mehrere Systeme und Organisationen verstreut[1], die jeweils unterschiedliche Standards und Technologien für die Verwaltung von Patientendaten verwenden. Diese Fragmentierung erschwert die Integration zwischen verschiedenen Systemen und führt zu Diskrepanzen bei der Datenübermittlung. Das Fehlen eines Standarddatenformats erschwert den Datenaustausch und erhöht das Risiko von Fehlern und Ineffizienzen. Da viele Systeme nicht immer gut zusammenarbeiten, könnte es für die Nutzer schwierig sein, auf ihre Gesundheitsakten zuzugreifen. Dieses Durcheinander beeinträchtigt die Wirksamkeit der Pflegekoordinierung und könnte dazu führen, dass Fehler oder Verzögerungen bei der Patientenversorgung.

Herkömmliche Authentifizierungsmethoden im Gesundheitswesen sind in der Regel von zentralen Servern abhängig, auf denen die Anmeldedaten der Benutzer gespeichert und überprüft werden. Diese zentralisierten Systeme haben mehrere Probleme, wie z. B.:

- Einzelner Fehlerpunkt: Zentralisierte Server, die für die Authentifizierung verwendet werden, sind anfällig für Störungen. Bei einem Ausfall oder einer Beschädigung des Servers kann das gesamte Netzwerk betroffen sein, so dass Mitarbeiter verschiedener Einrichtungen nicht mehr auf Patientendaten zugreifen können.
- Probleme mit der Skalierbarkeit: Wenn sich die Netze im Gesundheitswesen weiterentwickeln und die Zahl der Nutzer steigt, können die zentralisierten Systeme möglicherweise nicht mit der Nachfrage Schritt halten, was zu Leistungsengpässen führen kann.
- Cybersicherheitsbezogene Risiken: Zentralisierte Server stehen häufig im Mittelpunkt von Cyberangriffen. Wenn ein Angriff auf diese Systeme erfolgreich ist, können wichtige Patientendaten durch massive Datenverletzungen gefährdet werden.

Die Abhängigkeit von zentralisierten Authentifizierungssystemen kann zu schwerwiegenden Sicherheitsmängeln führen, die die Effizienz und Sicherheit der Datenverwaltung im Gesundheitswesen insgesamt beeinträchtigen. Diese Schwachstelle wird in einer dezentralisierten Umgebung, in der die Daten über verschiedene Einrichtungen verteilt sind, noch verschärft. Für Daten im Gesundheitswesen gelten strenge Gesetze wie der Health Insurance Portability and Accountability Act (HIPAA) und die General Data Protection Regulation (GDPR). Um die Privatsphäre der Patienten zu schützen und die Einhaltung der Vorschriften zu gewährleisten, sehen diese Vorschriften strenge Kontrollen des Datenzugriffs und der Datenverwaltung vor. Herkömmliche Authentifizierungsmethoden schaffen häufig keinen Kompromiss zwischen Benutzerfreundlichkeit und Sicherheit. Komplizierte Authentifizierungsstandards können zu erhöhtem Verwaltungsaufwand und möglicher Nichteinhaltung von Vorschriften führen. Bei herkömmlichen Systemen ist es schwierig zu gewährleisten, dass nur befugtes Personal auf wichtige Informationen zugreift und gleichzeitig ein nahtloses Benutzererlebnis gewahrt bleibt. Erfahrung.

Die Komplexität der Datennetze im Gesundheitswesen nimmt mit der Zahl der Benutzer zu, und die bestehenden Authentifizierungslösungen können damit möglicherweise nicht Schritt halten.[2]Mehrere herkömmliche Systeme basieren auf unflexiblen Infrastrukturen, die es schwierig machen, sie an Veränderungen in der Gesundheitsbranche oder in der Technologie anzupassen. Es ist möglich, dass alte Authentifizierungstechniken veraltet sind oder kostspielige Änderungen erfordern, wenn sich die Gesundheitssysteme weiterentwickeln und neue Technologien einbeziehen. Dieser Mangel an Flexibilität und Skalierbarkeit kann es der Branche erschweren, sich weiterzuentwickeln und an neue Probleme anzupassen.

Diese Forschungsarbeit zielt darauf ab, die Authentifizierungsherausforderungen im Gesundheitssektor zu bewältigen, indem eine neuartige dezentrale Authentifizierungsarchitektur vorgeschlagen wird. Die vorgeschlagene Lösung nutzt die selbstsouveräne Identität (SSI), einen nutzerzentrierten Ansatz, der dem Einzelnen die Kontrolle über seine digitalen Identitäten gibt. Darüber hinaus führt die Architektur eine neue Art von nicht-fungiblen Token (NFT) ein, die als soulbound token (SBT) bekannt sind. Die SBTs sind eine spezielle Art von nicht übertragbaren Token, die eingeführt wurden, um persönliche Referenzen und Errungenschaften auf der Blockchain auf sichere und überprüfbare Weise darzustellen.

Im Gegensatz zu herkömmlichen fungiblen Token oder übertragbaren NFTs sind SBTs an eine bestimmte Person gebunden und können nicht an eine andere Partei übertragen oder gehandelt werden. Der Ursprung von SBTs liegt in der Notwendigkeit einer zuverlässigen Methode zur digitalen Darstellung und Überprüfung von persönlichen Attributen und Zeugnissen wie akademischen Abschlüssen, beruflichen Zertifizierungen und Mitgliedschaftsnachweisen. Dieser Bedarf wird immer dringender, da die Verifizierung von Personen in verschiedenen Bereichen, von der Bildung bis hin zu beruflichen Netzwerken und darüber hinaus, an Bedeutung gewinnt. Der Begriff "soulbound" steht metaphorisch für die Idee, dass diese Token von Natur aus mit der "Seele" des Einzelnen, d. h. seiner persönlichen und einzigartigen Identität, verbunden sind und nicht losgelöst oder ausgetauscht werden sollen. Durch die Umsetzung dieses dezentralen Ansatzes wollen wir ein föderiertes Netzwerk von Gesundheitseinrichtungen schaffen, das die Datensicherheit und Interoperabilität erhöht und gleichzeitig die Authentifizierungszeiten erheblich verkürzt. Zur Ergänzung dieser dezentralisierten Authentifizierungsarchitektur schlagen wir die Integration eines Solid-Datenverwaltungssystems (ein Medium für den sicheren, dezentralisierten Austausch öffentlicher und privater Daten) vor, das einen robusten Rahmen für die dezentralisierte Datenspeicherung und -verwaltung bietet. Durch den Einsatz von Solid können Patienten ihre persönlichen Gesundheitsdaten in persönlichen Online-Datenspeichern (Pods) speichern, die sie vollständig kontrollieren. Dadurch wird sichergestellt, dass die Patienten die Befugnis haben, den Zugriff auf ihre Gesundheitsdaten zu gewähren oder zu widerrufen, was das Vertrauen fördert und die Privatsphäre stärkt.[3]

In diesem Bericht erläutern wir die Methodik hinter der vorgeschlagenen Architektur, einschließlich der Integration von SSI und SBTs, und präsentieren die Ergebnisse unserer Implementierung. Wir zeigen, wie dieser Ansatz die mit zentralisierten Authentifizierungsservern verbundenen Risiken mindert und die

Zitat: Blockchain im Gesundheitswesen heute 2024, **7**: 334 - https://doi.org/10.30953/bhty.v7.334

die Gesamteffizienz und Sicherheit des Datenmanagementsystems im Gesundheitswesen verbessert. Abschließend erörtern wir die potenziellen Auswirkungen dieser Architektur auf das Gesundheitswesen im Allgemeinen und zeigen Wege für künftige Forschungen auf.

Hintergrund

Im Bereich der Verwaltung digitaler Anmeldeinformationen hat die Integration von Blockchain-Technologie und kryptografischen Protokollen zu erheblichen Fortschritten geführt. Eine herausragende Entwicklung ist die Verwendung von SBTs für die Ausstellung und Verwaltung von digitalen Zugangsberechtigungen.

In diesem Abschnitt werden verschiedene aktuelle Ansätze und Innovationen in diesem Bereich untersucht, wobei die Stärken und Grenzen jedes Ansatzes hervorgehoben werden, mit besonderem Augenmerk auf Datenschutz, Nichtabstreitbarkeit und Einhaltung gesetzlicher Vorschriften.

Das System zur Verwaltung digitaler Berechtigungsnachweise, das in Ref. 4 führt einen innovativen Ansatz ein, indem es eine verbesserte Version von SBTs nutzt, die als "rejectable soul-bound tokens" (RejSBTs) bezeichnet werden. Dieses System verbessert die herkömmlichen Merkmale von Berechtigungsnachweisen, indem es bei der Ausstellung Bedingungen einbettet und bei der Annahme durch die Benutzer die Nichtabstreitbarkeit des Empfangs gewährleistet. Die RejSBTs garantieren die Nichtabstreitbarkeit von Empfangs- und Herkunftsnachweisen, ein kritischer Aspekt für rechtliche und Sicherheitszwecke. Dem derzeitigen Protokoll fehlt es jedoch an Verschlüsselungsmaßnahmen, da es in erster Linie nicht-sensible digitale Zugangsberechtigungen verarbeitet. Es ist von entscheidender Bedeutung, dass künftige Integrationen mit den GDPR-Vorschriften übereinstimmen, um potenzielle Datenschutzbedenken auszuräumen.

Ein weiterer bemerkenswerter Ansatz ist die Integration von dezentralisierten Identifikatoren (DIDs) mit SBTs in digitalen Authentifizierungssystemen, insbesondere im Web3- und Metaverse-Umfeld. Dieses von Kim und Ryou (2023)[5]vorgeschlagene System nutzt DIDs für die Benutzerverifizierung über Smart Contracts und gibt SBTs für eine nahtlose Integration aus. Um den Datenschutz zu verbessern, verwenden die Dienstleister der Verifizierungsbehörden Zero-Knowledge-Proof-Systeme (ZKP), die sicherstellen, dass kritische Nutzerinformationen während des Verifizierungsprozesses nicht offengelegt werden. Diese Methode erhöht die Vertraulichkeit für den Benutzer, da sie die Erstellung kryptografischer Beweise ohne direkte Beteiligung des Benutzers ermöglicht. Darüber hinaus verwaltet eine einheitliche Brieftasche sowohl DID-Berechtigungsnachweise als auch SBTs und vereinfacht so die Verwaltung der Berechtigungsnachweise.

Im Zusammenhang mit datenschutzfreundlichen Berechtigungsnachweissystemen gewinnt die Verwendung von SBTs in Kombination mit selektiven Offenlegungsmechanismen zunehmend an Bedeutung. In einem Rahmen[6]wird vorgeschlagen, Berechtigungsnachweise als NFTs auszugeben, die im Interplanetary File System (IPFS) in einem verschlüsselten Format gespeichert werden. Obwohl dieses System den Nutzern die vollständige Kontrolle über ihre Ausweisdaten gibt, verwendet der Verifizierungsprozess keine ZKPs, was seine Datenschutzgarantien möglicherweise einschränkt. Eine fortschrittliche Methode zur privaten Identitätsüberprüfung[7]beinhaltet SBTs mit Null-Wissen, die SBTs mit ZKPs kombinieren. Dieses Protokoll verwendet den privaten/öffentlichen Schlüssel des Identitätsinhabers öffentlichen Schlüssels des Identitätsinhabers zur Verschlüsselung der in einer SBT gespeicherten Daten. Zur Überprüfung wird dann eine ZKP verwendet, die sicherstellt, dass die Daten nicht verändert wurden und dass der Identitätsinhaber bestimmte Anforderungen erfüllt, ohne persönliche Informationen preiszugeben. Dieser Ansatz stellt ein wirksames Gleichgewicht zwischen Datenschutz und Sicherheit her und ist damit eine robuste Lösung für die Identitätsüberprüfung.

Das Metaversum bietet einzigartige Herausforderungen und Möglichkeiten für das digitale Identitätsmanagement. Eine Implementierung[8]konzentriert sich auf die Bereitstellung von altersbeschränktem Zugang in Decentraland (einer browserbasierten Plattform für virtuelle 3D-Welten) unter Verwendung von Ethereum-Smart Contracts und ZKPs. Diese Methode ermöglicht es Nutzern, ihre Berechtigung für bestimmte Aktivitäten, wie z. B. den Zugang zu einem virtuellen Kino, nachzuweisen, ohne ihre reale Identität preiszugeben. Sie nutzt bestehende rechtliche Rahmenbedingungen wie eIDAS (elektronische Identifizierung) und W3C Verifiable Credentials und demonstriert die praktische Anwendung der Blockchain-Technologie zur Wahrung der Vertraulichkeit bei gleichzeitiger Einhaltung rechtlicher Standards.

Ein praktischer Anwendungsfall für SBTs ist die Zertifizierung von COVID-19-Impfungen. Dieses vorgeschlagene System[9]verwendet eine dezentrale Anwendung, bei der SBTs als nicht übertragbare und widerrufbare Token ausgegeben werden, um sicherzustellen, dass sie mit der nicht übertragbaren Natur von Impfunterlagen übereinstimmen. Dieser Ansatz befasst sich zwar mit den administrativen Aspekten der Impfbescheinigung, geht aber nicht explizit auf den Datenschutz und die Vertraulichkeit ein, was einen Bereich für künftige Verbesserungen aufzeigt.

Darüber hinaus geht das Konzept der Datendezentralisierung über die Verwaltung von Berechtigungsnachweisen hinaus und bietet breitere Anwendungsmöglichkeiten in verschiedenen Sektoren. Eine große Herausforderung, abgesehen von der Sicherheit, ist die Speicherung großer Dateien im Blockchain-Netzwerk, da herkömmliche Blockchains nicht die Kapazität haben, umfangreiche Dateien wie medizinische Bilder zu speichern. Die Integration dezentraler Speicherlösungen wie IPFS und Solid Pods (persönliche Datenspeicher, die einen Ort für den Zugriff, die Aktualisierung und die gemeinsame Nutzung von Daten bieten) kann die Datenverwaltung und die gemeinsame Nutzung in Netzwerken revolutionieren. IPFS beispielsweise bietet ein Peer-to-Peer-Netzwerk für die Speicherung und gemeinsame Nutzung von Daten in einem verteilten Dateisystem, wodurch die Datenverfügbarkeit erhöht und das Risiko zentraler Fehlerpunkte gemindert wird. Ein für die Datenspeicherung auf IPFS[10]vorgeschlagenes Sicherheitsmodell verwendet Shamirs Secret Sharing (SSS) zur Verschlüsselung von Daten vor der Speicherung, das in Ethereum implementiert ist und auf einem Proof-of-Work-Konsensalgorithmus beruht, der eine hohe Rechenleistung erfordert.

Eine weitere Herausforderung bei IPFS besteht darin, dass es nur einen Hash der Daten liefert, was die Suche nach verwandten Patientendatensätzen erschwert. Um dieses Problem zu lösen, wurde in Ref. 11 vorgeschlagen, die die Suche nach Daten erleichtert, indem sie einen Namen anstelle eines Hashes liefert und so die Suchzeit verkürzt. Blockchain-Systeme werden daher für die Speicherung, gemeinsame Nutzung, Verwendung und Manipulation von Patientendaten verwendet. Eine weitere Lösung ist die Verwendung von Solid Pods zur Speicherung von Gesundheitsdaten. Beispiele für

Tabelle 1. Vergleichende Analyse von Lösungen zur Verwaltung von Anmeldeinformationen

Quelle	Wesentliche Merkmale	Stärken	Beschränkungen	Datenschutz	Unverfälschbarkeit	Einhaltung gesetzlicher Vorschriften
Pericàs-Gornals. et al. (2024)[4]	Verbesserte SBTs mit AGBs, die die Nichtabstreitbarkeit des Empfangs gewährleisten	Rechts- und Sicherheitsgarantie, Nichtabstreitbarkeit des Empfangs und der Herkunft	Fehlende Verschlüsselungsmaßnahmen, vor allem für nicht-sensible Anmeldedaten	Niedrig	Hoch	Benötigt zukünftige GDPR-Anpassung
Kim et al. (2023)[5]	DIDs zur Nutzerverifizierung, ZKP für Datenschutz, einheitliche Brieftasche	Verbesserter Datenschutz mit ZKP, nahtlose Integration	Komplexität der Implementierung	Hoch	Mittel	Angleichung an rechtliche Standards
Reddy und Kushwaha (2023)[6]	NFTs auf IPFS gespeichert, verschlüsseltes Format	Benutzerkontrolle über Anmeldeinformationen	Fehlen von ZKP, begrenzte Datenschutzgarantien	Gering	Mittel	Verbesserungen des Datenschutzes erforderlich
Cabot-Nadal et al. (2023)[7]	Kombiniert SBTs mit ZKP, verwendet private/öffentliche Schlüssel zur Verschlüsselung	Ausgewogenes Verhältnis zwischen Privatsphäre und Sicherheit	Hohe Komplexität	Hoch	Hoch	Starke Übereinstimmung mit Datenschutzbestimmungen
Zichichi et al. (2023)[8]	Ethereum Smart Contracts, ZKPs, eIDAS, W3C VCs	Praktische Anwendung im Metaverse, Wahrung der Privatsphäre und Einhaltung der Vorschriften	Speziell für altersbeschränkten Zugang	Hoch	Mittel	Starke Übereinstimmung mit rechtlichen Standards
Lunesu et al. (2023)[9]	SBTs als nicht übertragbare und widerrufbare Token	Behandelt administrative Aspekte	Mangelnder Fokus auf Datenschutz und Vertraulichkeit	Gering	Mittel	Benötigt Verbesserungen für den Datenschutz
Naz et al. (2019)[10]	IPFS für Speicherung, SSS für Verschlüsselung, PoW-Konsens	Verbesserte Datenverfügbarkeit, mildert zentrale Fehlerpunkte	Hohe Rechenleistung, Suchschwierigkeiten	Hoch	Mittel	Starkes Potenzial, muss aber für das Gesundheitswesen optimiert werden
Saharan und Prasad (2020)[11]	Erleichtert die Datensuche mit Namen anstelle von Hashes	Reduziert die Suchzeit, verbessert den Datenaustausch und die Nutzung	Komplexität der Implementierung	Mittel	Mittel	Starke Angleichung an Datenverwaltungsstandards
Prop.	Dezentralisierte Authentifizierung mit SBTs, privater Blockchain (Hyperledger Besu), PoA-Konsens (QBFT), datenschutzfreundliche Orakel (Chainlink)	Umfassendes Framework, skalierbar, erhöhte Sicherheit mit privaten Smart Contracts	Private Blockchain	Hoch	Hoch	Starker Fokus auf Compliance, private Blockchain gewährleistet Datenschutz

DID: dezentralisierte Identifikatoren; eIDAS: elektronische Identifizierung, Authentifizierung und Vertrauensdienste; GDPR: General Data Protection Regulation; IPFS: InterPlanetary File System; NFTs: non-fungible tokens; PoA: Proof of Authority; PoW: Proof of Work; QBFT: Quorum Byzantine Fault Tolerant; SBTs: 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.

Ihre Verwendung und Techniken zur Optimierung einer Suche sind veröffentlicht worden.[12,13]

Tabelle 1 zeigt, dass unsere Lösung die bestehenden Methoden übertrifft, da sie ein umfassendes und skalierbares Rahmenwerk bietet, das Datenschutz, Sicherheit und die Einhaltung gesetzlicher Vorschriften in Einklang bringt. Sie nutzt eine dezentrale Authentifizierung mit SBTs, einer privaten Blockchain und datenschutzfreundlichen Orakeln, die einen hohen Datenschutz und eine hohe Sicherheit gewährleisten. Im Gegensatz zu anderen Ansätzen werden wichtige Einschränkungen wie fehlende Verschlüsselung, Komplexität und Anwendungsbeschränkungen behoben, was es zu einer überlegenen und robusteren Option macht.

Vorgeschlagenes System

Die Fortschritte bei den Systemen zur Verwaltung digitaler Anmeldeinformationen unter Verwendung von SBTs zeigen, dass es erhebliche Fortschritte bei der Verbesserung des Datenschutzes, der Sicherheit und der Benutzerfreundlichkeit gibt. Jeder Ansatz hat jedoch seine Stärken und Grenzen, insbesondere in Bezug auf die Wahrung der Privatsphäre und die Einhaltung von Vorschriften. Zukünftige Entwicklungen müssen sich auf die Integration von robusten Verschlüsselungsmaßnahmen, umfassenden Datenschutzmaßnahmen und die Einhaltung gesetzlicher Standards konzentrieren, um das Potenzial dieser innovativen Systeme für die Verwaltung digitaler Ausweise voll auszuschöpfen.

Der aktuelle Stand der Technik zeigt einen erheblichen Mangel an Interoperabilität zwischen den im Gesundheitswesen erzeugten Daten. Durch die Nutzung von Standards wie HL7 ist es möglich, interoperable Lösungen für verschiedene Krankenhäuser zu entwickeln. Die bestehenden Datenspeichermethoden, die überwiegend auf zentralisierten Servern beruhen, müssen jedoch sorgfältig neu konzipiert werden. Dazu gehört auch eine Überarbeitung der Mechanismen für den Datenzugriff.

Die vorgeschlagene Architektur zielt darauf ab, einen umfassenden Rahmen für die dezentrale Verwaltung der Authentifizierung zu schaffen und gleichzeitig die im vorangegangenen Abschnitt beschriebenen dezentralen Datenlösungen zu berücksichtigen.

Zitat: Blockchain im Gesundheitswesen heute 2024, **7**: 334 - https://doi.org/10.30953/bhty.v7.334

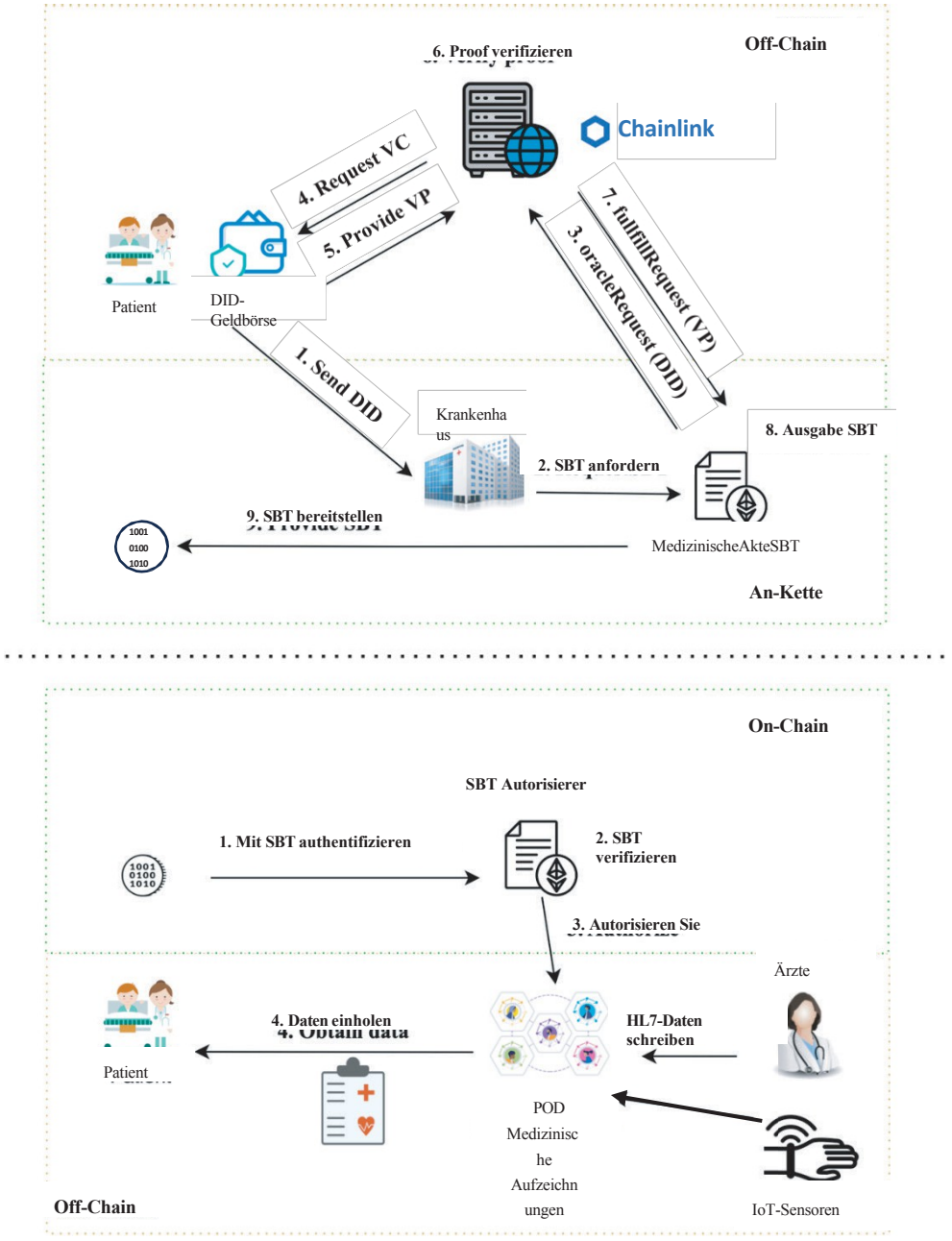

Abb. 1. Systemmodell: Einschreibungsphase (obere Abbildung) und Authentifizierung (untere Abbildung). HL7: Health Level Seven; IoT: Internet der Dinge; Pods: persönliche Online-Datenspeicher; SBT: soulbound token.

Ziel ist es, diesen Ansatz zu validieren, indem Einblicke in die mittlere Antwortzeit und eine gründliche Sicherheitsbewertung des Protokolls gegeben werden.

Einführung

Die Verwendung von DID ist im medizinischen Bereich aufgrund der komplexen Interaktion nicht direkt anwendbar. Darüber hinaus stellt die Authentifizierung mit SSI bei dezentralen Anwendungen eine große Herausforderung dar, da eine Signaturprüfung der Anmeldeinformationen erforderlich ist, die nicht auf der Kette durchgeführt werden kann, ohne dass Benutzerdaten offengelegt werden. Diese Probleme werden noch kritischer, wenn öffentliche Blockchains wie Ethereum verwendet werden.

Unsere Architektur zielt darauf ab, alle Vorteile von SSI zu bieten und gleichzeitig einen neuartigen, auf NFTs basierenden Authentifizierungsmechanismus einzubauen, insbesondere eine Erweiterung, die als Soulbound Tokens (SBTs) bekannt ist. SBTs wurden entwickelt, um Token an ihren Besitzer zu binden und so die Vorteile von NFTs zu nutzen.

Um unser System zu analysieren, unterteilen wir es in zwei Hauptphasen: die Registrierungsphase, die in Abbildung 1 oben dargestellt ist, und die Authentifizierungsphase, die in Abbildung 2 unten gezeigt wird.

unten in Abbildung 1. Bevor wir diese Phasen genauer analysieren, müssen wir einige technische Aspekte unserer Architektur klären.

Aus diesem Grund haben wir einen hybriden Ansatz gewählt, bei dem die Identität außerhalb der Blockchain verifiziert wird und dann ein SBT über eine private Blockchain wie Hyperledger Besu freigegeben wird. Der Bedarf an einer privaten Blockchain ergibt sich aus der Notwendigkeit, die Privatsphäre eines Nutzers bei der Durchführung von On-Chain-Transaktionen zu gewährleisten.

Quorum und Autoritätsnachweis

Die Architektur wurde im Rahmen eines Versuchsprojekts auf einer privaten Blockchain mit Hyperledger Besu eingesetzt, die aus vier Knoten besteht. Dieser Aufbau ist leicht skalierbar, da wir die Blockchain nur zur Freigabe von SBT verwenden. Beim eingesetzten Proof of Authority (PoA)-Konsensverfahren werden die Validierer, d. h. die zum Mining von Blöcken berechtigten Knoten, vom Blockchain-Eigentümer vorab autorisiert.

Jeder Block wird von einem dieser vorautorisierten Knotenpunkte validiert. Hyperledger Besu unterstützt verschiedene PoA-Schemata, darunter QBFT, IBFT 2.0 (Istanbul Byzantine Fault Tol-erance) und Clique. Für die Zwecke unseres Projekts haben wir uns für QBFT entschieden, da es die Vertraulichkeit von Transaktionen gewährleisten kann, was für die Implementierung eines vertrauenswürdigen Orakels auf der Grundlage der Chainlink-Infrastruktur unerlässlich ist. Diese Transaktionen sind gesichert und nur für die beteiligten Parteien zugänglich. Die Skalierbarkeit von PoA ist vorteilhaft, da sie das Wachstum des Netzes ohne nennenswerte Leistungsprobleme unterstützt. Die Sicherheit und das Vertrauen werden erhöht, da die Validierer vertrauenswürdige Instanzen sind, die das Risiko böswilliger Aktivitäten verringern und eine glaubwürdige Ausstellung von SBTs gewährleisten. Wir haben das QBFT-Schema innerhalb von PoA wegen seiner Transaktionsdatenschutzfunktionen ausgewählt, die für unser datenschutzbewusstes Orakel mit der Chain-Link-Infrastruktur von entscheidender Bedeutung sind. Insgesamt ist PoA aufgrund seiner Effizienz, Skalierbarkeit, Sicherheit und Privatsphäre die ideale Wahl für unsere SBT-Implementierung.

Einschreibung

Die Notwendigkeit einer Registrierungsphase ergibt sich aus der Komplexität der Schaffung eines zeitnahen Verfahrens zur Authentifizierung von Benutzern innerhalb des Systems. Die Authentifizierung auf der Grundlage von DIDs erfordert die Überprüfung von Berechtigungsnachweisen und die Generierung von überprüfbaren Beweisen durch den Inhaber, was zu einem Mehraufwand führen kann. Außerdem können diese Verfahren nicht auf eine öffentliche Blockchain angewendet werden, wie zuvor beschrieben.

In unserem Vorschlag umfasst die erste Phase neun Schritte, um dem Nutzer einen SBT zu liefern. In dieser Phase teilt der Nutzer die SSI-Anmeldeinformationen mit und erhält eine SBT. Das Verfahren beginnt damit, dass der Inhaber eine SBT-Freigabe vom Krankenhaus anfordert. Während dieser Anfrage teilt der Inhaber seine DID_Hmit, die in unserem Fall eine *did:eth* (dezentralisierte eth (dezentralisierter Bezeichner:Etherium) ist, um die Kompatibilität mit der Ethereum-Blockchain zu gewährleisten. Eine solche DID_Hwird mit einem $DIDDocument_H$durch die Verwendung von den zuvor registrierten Smart Contract. Das Krankenhaus leitet die Anfrage an den Smart Contract MedicalRecordSBT weiter, der die gleiche DID_Henthält, die zuvor auf der Besu-Blockchain bereitgestellt wurde. Die Funktion requestSBT leitet diese Anfrage dann an die Chainlink-Infrastruktur weiter, die die Off-Chain-Kommunikation mit dem externen Server übernimmt. Wie in Abbildung 1 dargestellt, folgen die Anfragen während der Schritte 4, 5 und 6 dem klassischen SSI-Vertrauensdreieck-Ansatz, bei dem der Verifizierer, der in diesem Fall der ChainLink-Knoten ist, eine Anfrage an den Off-Chain-Server sendet, der eine VPR generiert. Die Benutzer erstellen eine überprüfbare Präsentation, die mit dieser VPR verbunden ist, und übermitteln sie an den Off-Chain-Server, der die Überprüfung der Anmeldedaten vornimmt. Sobald die Gültigkeit der übermittelten Anmeldeinformationen bestätigt ist, wird ein Rückruf auf die MedicalRecordSBT ausgeführt, wodurch die endgültige SBT an den Benutzer freigegeben wird. Diese SBT kann nun vom Benutzer verwendet werden um sich auf krankenhausvertrauenswürdigen Plattformen zu authentifizieren.

Authentifizierung

Zu Beginn der Authentifizierung verfügt der Patient bereits über ein SBT, das seine Identität innerhalb des Krankenhauses darstellt. Dieses Token wird verwendet, um den Benutzer zu authentifizieren und auf die auf dem POD gespeicherten persönlichen Daten zuzugreifen. Das gesamte Verfahren wird über den intelligenten Vertrag *SBTAuthorizer* verwaltet, der Verweise auf den ausgestellten SBT enthält und in der Lage ist, den Authentifizierungsprozess durchzuführen. Dieser intelligente Vertrag enthält auch Metadaten zu widerrufenen Token und Rollen innerhalb des Systems, so dass das Krankenhaus den Zugang widerrufen kann, wenn ein Benutzer den Besitz seiner Brieftasche verliert.

Ähnlich wie die Patienten werden auch die Geräte des Internets der Dinge (IoT) und die Ärzte auf die Datenräume zugreifen, indem sie einen dezentralen Ansatz verwenden. Wie in Ref. 14 und in Ref. 15 beschrieben, können sowohl Ärzte als auch IoT-Geräte diese Art der Authentifizierung mithilfe von SSI durchführen. Insbesondere die Ärzte verwalten die Authentifizierung durch die Verwendung des HSM als Mechanismus zur Verringerung des Zeitaufwands für die Authentifizierung, während die IoT-Geräte physische Merkmale wie den statischen Direktzugriffsspeicher (SRAM) oder das Elektrokardiogramm nutzen können, um einen privaten Schlüssel zu erstellen, der bei der Generierung der SSI-Brieftasche verwendet wird. Schließlich trennt die vorgeschlagene Architektur den Authentifizierungsprozess von der Datenspeicherung.

Dezentralisierte Datenspeicherung

Der vorgeschlagene Ansatz umfasst auch ein neuartiges dezentralisiertes Datenspeichersystem, das vollständig mit dem vorgeschlagenen dezentralen Authentifizierungsmechanismus kompatibel ist. Solid, ein relativ neues Framework, entspricht dem Paradigma der nutzerzentrierten Datenspeicherung, indem es den Nutzern die Möglichkeit gibt, die Verantwortung für die von Anwendungen erzeugten Daten zu übernehmen. In diesem speziellen Anwendungsfall betrifft dies die medizinischen Daten, die sowohl von IoT-Geräten als auch von ärztlichen Analysen erzeugt werden. Solid bietet eine gut strukturierte Methode zur Speicherung von Daten unter Verwendung der Wissensgraphen-Technologie.

Zitat: Blockchain im Gesundheitswesen heute 2024, **7**: 334 - https://doi.org/10.30953/bhty.v7.334

Tabelle 2. Kosten für den Einsatz der vorgeschlagenen Architektur

Betrieb	Benötigtes Gas	Kosten ($)	Ausgegeben durch
Bereitstellung			
• TokenLink.(Konstrukteur)	1467527 Gas	11.87	Behörde
• Betreiber (Errichter)	4184013 Gas	33.83	Autorität
• EthereumDIDRegistry.(Konstrukteur)	574518 Gas	1.55	Behörde
• NationalHealthServiceDIDRegistry.(Konstrukteur)	1168361 Gas	9.45	Behörde
• MedicalRecordSBT.(Konstrukteur)	5159457 Gas	41.72	Behörde
Immatrikulation			
• EthereumDIDRegistry.updateDIDDocument(string,bytes)	742188 Gas	6.00	Krankenhaus
• NationalHealthServiceDIDRegistry.authorizeDID(Zeichenfolge,Zeichenfolge)	58569 Gas	0.47	Krankenhaus
• MedicalRecordSBT.requestSBT(string)	164520 Gas	1.33	Krankenhaus
SBT-Prägung			
• KrankenakteSBT.fulfillRequest(string)	2594670 Gas	20.98	Chainlink-Knoten

DID: dezentralisierte Identifikatoren/Identität; SBT: Soulbound Token.

Diese Darstellung ist vollständig konform mit den aktuellen Datenrepräsentationsmechanismen im medizinischen Bereich, wie HL7, das eine gut dokumentierte Ontologie bietet. Dieser Ansatz verbessert die Konformität mit der Datenschutz-Grundverordnung (GDPR), indem er eine dezentrale Datenspeicherung fördert, bei der die Nutzer die von IoT-Geräten erzeugten Daten verwalten können, ohne sie auf externe Server kopieren zu müssen.

Ergebnisse

Um die Qualität der vorgeschlagenen Architektur zu bewerten, konzentrieren wir uns hauptsächlich auf die Kosten für die Bereitstellung der Lösung in Form von Gebühren für die Ausführung eines Smart Contracts. Für die Bewertung unseres Vorschlags haben wir ein Hyper-Ledger-Besu-Docker-Image mit QBFT-Konsens auf einem iMac 3,3 GHz Intel Core i5 mit 6 Kernen und 16 GB 2667 MHz DDR4 eingesetzt.

Um unsere Lösungen zu implementieren, haben wir fünf intelligente Verträge eingesetzt:

1. **LinkToken.sol:** Verantwortlich für die Bezahlung von Chainlink-Anfragen. Ursprünglich mit 1.000.000 LINK ausgestattet.
2. **Operator.sol:** Verantwortlich für den Betrieb mit dem Chainlink-Knoten, der alle Anfragen weiterleitet.
3. **EthereumDIDRegistry.sol:** Verantwortlich für die Verwaltung der DIDs-Architektur.
4. **NationalHealthServiceDIDRegistry.sol:** Verantwortlich für die Verwaltung der Rollen innerhalb des gesamten Rahmens.
5. **MedicalRecordSBT.sol:** Enthält die SBT-Definition und den Vorgang für das Minting der SBT.

Wie in Tabelle 2 dargestellt, ist der Einsatz von Smart Contracts zusammen mit dem SBT-Minting der teuerste Vorgang, der zur Erzeugung und Freigabe der SBT für den Nutzer erforderlich ist. Operative Anfragen sind erforderlich, um die gesamte Umgebung einzurichten und sich auf die Zuordnung der erstellten DID zu die interne Registrierung, die die Rollen enthält. Die Kostenschätzung gibt Aufschluss über die Komplexität der mit dem intelligenten Vertrag verbundenen Vorgänge, aber die Kosten hängen von mehreren Faktoren ab, wie z. B. der Belegung des Netzwerks und den erforderlichen Gebühren. Durch die Annahme von Kosten in Höhe von 3 gwei pro benötigtem Gas, was den normalen Kosten der Ethereum-Blockchain entspricht, ist es möglich, eine Schätzung der Gesamtkosten für die verschiedenen Operationen vorzunehmen.

Die Bereitstellungsphase wird nur einmal bei der Einführung des Systems durchgeführt, während die Registrierung und die SBT-Minting-Operationen für jeden neuen Patienten, der dem System angehört, durchgeführt werden. Die Gesamtkosten von weniger als 30 $ pro neuem Benutzer im System sind angesichts der Vorteile des vorgeschlagenen Ansatzes angemessen.

Für das Authentifizierungsverfahren, das nur aus dem Auslesen von Daten aus der Blockchain besteht, fallen keine Kosten an, ohne dass eine zusätzliche Gebühr verlangt wird.

Die Gesamtzeit für das Anmeldeverfahren beträgt etwa 16,03 s im Durchschnitt; der größte Teil entfällt auf die Verifizierung von Ausweisen (12,54 s). Das ist die Hauptmotivation, die uns dazu veranlasst hat, zu einem vollständig dezentralen und ketteninternen Ansatz überzugehen. Mit unserem Vorschlag ist es nun möglich, sich mit dem SBT zu authentifizieren, indem nur das Vorhandensein des SBT auf dem MedicalRecordSBT Smart Contract überprüft wird.

Mit der aktuellen Forschung haben wir versucht, die für die Authentifizierung benötigte Gesamtzeit zu reduzieren, indem wir eine On-Chain-Verifizierungsmethode bereitgestellt haben, wobei die Privatsphäre der Knoten und alle von SSI eingeführten Vorteile erhalten bleiben. Der durch die vorgeschlagene Architektur verursachte Overhead ist relativ gering, da die Anmeldephase nur einmal für jeden Benutzer ausgeführt wird und die Authentifizierungsphase auf einen einzigen Aufruf des Smart Contracts reduziert wird. Außerdem basiert das System ausschließlich auf der Blockchain und dem asymmetrischen Mechanismus hinter der Blockchain. SBTs erhöhen die Sicherheit durch den Einsatz einer kryptografischen Brieftasche, in der der private Schlüssel in Verbindung mit dem öffentlichen Schlüssel gespeichert wird.

Schlussfolgerung

Für die Zukunft planen wir, unsere Bewertung der vorgeschlagenen Methoden zu verbessern, indem wir den Zugang zu Anbietern in reale Szenarien integrieren. Durch die Einbeziehung des Provider-Zugriffs werden wir in der Lage sein, komplexere Umgebungen mit mehreren Interessengruppen zu simulieren, was eine umfassendere Bewertung der Effektivität unseres Ansatzes in der Praxis ermöglichen wird. So können wir die Auswirkungen auf die Sicherheit und den Schutz medizinischer Daten in der Praxis besser verstehen. In einem Diabetes-Anwendungsfall würde der Zugriff des Anbieters es den medizinischen Fachkräften beispielsweise ermöglichen, direkt mit den in Solid Pods gespeicherten Patientendaten zu interagieren und gleichzeitig einen Beitrag zu einem verteilten maschinellen Lernmodell zu leisten und davon zu profitieren. Diese zusätzliche Ebene der Interaktion mit den Leistungserbringern ist entscheidend für die Validierung der Skalierbarkeit und Praktikabilität unserer Architektur in verschiedenen medizinischen Anwendungsfällen.

Finanzierung

Diese Arbeit wurde teilweise durch das Projekt SERICS (PE00000014) im Rahmen des von der EU-NGEU finanzierten NRRP MUR-Programms und durch das Projekt "DHEAL-COM-Digital Health Solutions in Community Medicine" im Rahmen des vom italienischen Gesundheitsministerium finanzierten Innovative Health Ecosystem (PNC)-National Recovery and Resilience Plan (NRRP) Programms unterstützt.

Interessenkonflikte

Die Autoren haben keine Interessenkonflikte angegeben.

Mitwirkende

Herr Boi trug zur Konzeption des Systems, zur Bewertung des Systems und zum Verfassen der Studie bei. Herr Cirillo trug zur Konzeption des Systems, zum Stand der Technik und zum Verfassen des gesamten Artikels bei. Herr De Santis trug zur Konzeption des Systems und zum Verfassen der Arbeit bei. Dr. Esposito trug zur Konzeptualisierung des Systems und zur Überprüfung der einzelnen Entwürfe bei.

Alle Autoren haben das Manuskript genehmigt und sind mit der Veröffentlichung in Blockchain in Healthcare Today einverstanden.

Datenverfügbarkeitserklärung (DAS), gemeinsame Nutzung von Daten, Reproduzierbarkeit und Datenrepositorien.

Kontaktieren Sie den Autor.

Anwendung von generiertem Text oder verwandter Technologie

Künstliche Intelligenz und verwandte Technologien wurden bei der Erstellung dieses Artikels nicht verwendet.

Danksagungen

Diese Arbeit wurde teilweise durch das Projekt SERICS (PE00000014) im Rahmen des NRRP MUR-Programms unterstützt, das von der EU-NGEU und durch das Projekt "DHEAL-COM-Digital Health Solutions in Community Medicine" im Rahmen des Programms Innovative Health Ecosystem (PNC)-National Recovery and Resilience Plan (NRRP), das vom italienischen Gesundheitsministerium finanziert wird.

Referenzen

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: A Sys-tematic Review and Open Research Challenges. Security and Communication Networks 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. Journal of Ambient Intelligence and Humanized Computing 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. Assessing the solid protocol in relation to security and pri-vacy obligations. Information 2023; 14(7):411. 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-management system using rejectable soulbound tokens. Ann Tele-commun [Internet]. 2024 Apr 23 [cited 2024 Jun 19]; Verfügbar unter: https://link.springer.com/10.1007/s12243-024-01032-6
5. Kim G, Ryou J. Digitales Authentifizierungssystem in Avatar mit DID und SBT. Mathematics. 2023 Oct 22;11(20):4387. https://doi.org/10.3390/math11204387
6. Reddy S, Kushwaha DS. Framework for privacy preserving cre-dential issuance and verification system using soulbound token. Sumathi AC, Yuvaraj N, Ghazali NH, editors. ITM Web Conf. 2023;56:06002.
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 [zitiert 2024 Jun 19]. p. 153-6. Verfügbar unter: https:// ieeexplore.ieee.org/document/10339754/
8. Zichichi M, Bomprezzi C, Sorrentino G, Palmirani M. Schutz der digitalen Identität im Metaverse: der Fall des Zugangs zu einem Kino in Dezentraland. In: Internationale Konferenz über Entwicklungen in der Sprachtheorie. 2023. Verfügbar unter: 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 [zitiert 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. Sustainability. 2019 10;11(24):7054. https://doi.org/10.3390/su11247054
11. Saharan R, Prasad R. Blockchain Technology for Healthcare Data. Advances in intelligent systems and computing. 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

für Ökosysteme des Gesundheitswesens 5.0. IEEE internet of things jour-nal. 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 Mai 13.
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: Theory & Applications 2024.

Anhang: Definierte Akronyme

DID: dezentralisierte Identifikatoren/Identität did:eth: dezentralisierter Identifikator:Etherium
DIDDocument$_H$: digitales Identitätsdokument (Inhaber) DID$_H$: digitale Identität (Inhaber)
eIDAS: elektronische Identifizierung, Authentifizierung und Vertrauensdienste.
GDPR: Allgemeine Datenschutzverordnung
HIPAA: Health Insurance Portability and Accountability Act (Gesetz zur Übertragbarkeit und Rechenschaftspflicht von Krankenversicherungen)
HL7: Gesundheitsstufe Sieben
HSM: Hardware-Sicherheitsmodul
IBFT: Istanbul-Byzantine-Fehlertoleranz IoT: Internet der Dinge
IPFS: InterPlanetary File System NFT: nicht-fungibles Token
PoA: Beweis der Autorität;
Pod: persönlicher Online-Datenspeicher
PoW: Proof of Work
QBFT: Quorum Byzantine Fault Tolerant RejSBTs: zurückweisbare seelengebundene Token SBT: seelengebundener Token
SRAM: Static Random Access Memory (statischer Direktzugriffsspeicher) SSI: Selbstsouveräne Identität
SSS: Shamir's Secret Sharing T&C: Allgemeine Geschäftsbedingungen
VCs: Verifiable Credentials
VPR: Überprüfbare Präsentationsanforderung
W3C: World Wide Web Consortium ZKP: Null-Kenntnis-Beweis