






ORIGINALE FORSCHUNG

Lösung von Datenschutzkonflikten bei der Integration von persönlichen und elektronischen Gesundheitsdaten in Blockchain-basierten Systemen

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

¹Department of Software Science, Tallinn University of Technology, Tallinn, Estland; ²Austrian Blockchain Centre Research, Wien, Österreich;

³School of Electronics, Electrical Engineering and Computer Science, Queens University Belfast, Belfast, Nordirland, Vereinigtes Königreich;

⁴Baltic Film, Media and Arts School, Tallinn University, Estland; Dymaxion OÜ, Tallinn, Estland

Korrespondenz: Aleksandr Kormiltsyn, E-Mail: Aleksandr.kormiltsyn@taltech.ee

Stichworte: Blockchain, Konfliktmanagement, E-Healthcare, Gesundheitsvorsorge, Datenschutz, Smart Contracts

Zusammenfassung

Die Integration von persönlichen Gesundheitsdaten (PHR) und elektronischen Gesundheitsdaten (EHR) erleichtert die Bereitstellung neuartiger Dienste für Einzelpersonen, Forscher und Fachkräfte im Gesundheitswesen. Gleichzeitig führt die Integration von Gesundheitsdaten zu komplexen Problemen, die sich aus der strukturellen und semantischen Heterogenität der Daten ergeben. Das Thema Gesundheitsdaten weckt starke Emotionen aufgrund der Sorge um Datenschutzverletzungen. Die Blockchain-Technologie wird eingesetzt, um das Problem des Datenschutzes von Patientendaten in organisationsübergreifenden Prozessen anzugehen, da sie das Eigentum an Patientendaten erleichtert und die Transparenz ihrer Nutzung fördert. Gleichzeitig schafft die Blockchain-Technologie neue Herausforderungen für E-Healthcare-Systeme wie Datenschutz, Beobachtbarkeit und Online-Durchsetzbarkeit. Dieser Artikel schlägt die Entwicklung und Formalisierung automatischer Konfliktlösungstechniken in dezentralen E-Healthcare-Systemen vor. Die vorliegende Studie erläutert unsere Konzepte anhand einer laufenden Fallstudie, die sich auf die Bereiche der präventiven und personalisierten Gesundheitsversorgung konzentriert.

Klartext-Zusammenfassung

In diesem Papier wird vorgeschlagen, die Blockchain-Technologie für Datenschutzbelange bei der Integration persönlicher Gesundheitsdaten und elektronischer Gesundheitsdaten in dezentralisierten E-Healthcare-Systemen einzusetzen. Dieser Bericht konzentriert sich auf die Entwicklung automatischer Konfliktlösungstechniken, um das Eigentum an Patientendaten, Transparenz und Datenschutz in organisationsübergreifenden Prozessen zu gewährleisten. In diesem Beitrag wird vorgeschlagen, automatische Konfliktlösungstechniken in dezentralisierten E-Healthcare-Systemen zu entwickeln, die die interorganisationalen Prozesse im Gesundheitswesen verbessern können. Der Einsatz der Blockchain-Technologie zur Integration persönlicher und elektronischer Gesundheitsdaten kann das Eigentum an den Patientendaten sicherstellen und die Transparenz bei der Datennutzung fördern, wodurch Bedenken hinsichtlich des Datenschutzes in Gesundheitssystemen ausgeräumt werden. In diesem Papier wird die Bedeutung des Datenschutzes in Gesundheitssystemen hervorgehoben und auf die Notwendigkeit der Einhaltung von Gesetzen und Vorschriften hingewiesen. Die Forschungsergebnisse, einschließlich des Proof-of-Concept-Prototyps, können praktische Einblicke in die Implementierung von Konfliktlösungstechniken in dezentralisierten E-Healthcare-Systemen liefern.

Eingereicht: 26. Juni 2023; Angenommen: November 13, 2023; Veröffentlicht: Dezember 14, 2023

Hie Gesundheitssysteme leiden unter hohen Kosten¹ und den wirtschaftlichen Interessen der Gesundheitsdienstleister. Nach der Privatisierung hat sich beispielsweise der irische Krankenhaussektor

nach der Privatisierung einen Anstieg der Patientenbetten in privaten, gewinnorientierten Krankenhäusern, während die Zahl der Betten in gemeinnützigen Krankenhäusern zurückging.² Eine persönliche Gesundheitsakte (Personal Health Record, PHR) ist die elektronische Gesundheitsinformation einer Person. Sie wird verwaltet und

von der Person verwaltet, die den Zugriff auf die Daten kontrolliert. Die PHR speichert und organisiert die Krankengeschichte, Behandlungen, Medikamente, Notizen, Diagnosen und andere relevante Gesundheitsinformationen, die zwischen der Person und ihren Gesundheitsdienstleistern ausgetauscht werden können. Die PHR bieten einen umfassenden und organisierten Überblick über die Krankengeschichte einer Person, was von unschätzbarem Wert für die schnelle und

effiziente Diagnose, verbesserte Sicherheit und Qualität der Versorgung. Darüber hinaus können PHRs dazu verwendet werden, den medizinischen Werdegang eines Patienten zu verfolgen, Trends und Korrelationen zu erkennen und dem Patienten Feedback über seine Gesundheitsdienstleister zu geben.

Eine Rückkopplungsschleife im Gesundheitswesen bezieht sich auf einen Prozess, bei dem Informationen über den Gesundheitszustand eines Patienten oder die Leistung eines Gesundheitssystems gesammelt, analysiert und verwendet werden, um Verbesserungen oder Anpassungen an der Patientenversorgung oder den Prozessen im Gesundheitswesen vorzunehmen. Eine Feedbackschleife beinhaltet den Austausch von Informationen über den Zustand eines Patienten, seine Behandlungsmöglichkeiten und seinen Fortschritt. Die Patienten geben Rückmeldungen zu ihren Symptomen und Behandlungserfahrungen, was den Gesundheitsdienstleistern hilft, fundierte Entscheidungen bezüglich ihrer Behandlung zu treffen.

Die Forschung definiert den Wert von PHR als Verbesserung der Kommunikation zwischen einem Patienten und einem Arzt, was zu einer Patientenaufklärung führt, die zu einer Änderung des Lebensstils führt.³ Das Engagement der Patienten vereinfacht die Erfassung und Verarbeitung von persönlichen Gesundheits- und Wohlbefindensdaten, was den Wert von präventiven Gesundheitsdiensten erhöht.⁴ Laut Kormiltsyn und Kollegen⁵ ist zu erwarten, dass eine neue Klassifizierung von präventiven Gesundheitscoaches entstehen wird. Diese Coaches werden ihr Fachwissen und ihre Fähigkeiten beim Verstehen und Analysieren von Gesundheits- und Wellnessdaten einsetzen. In unserem 2019 veröffentlichten wissenschaftlichen Artikel beleuchten wir die wirtschaftlichen und finanziellen Probleme des Gesundheitssystems und untersuchen das Potenzial der Blockchain-Technologie, um dezentralisierte und patientenorientierte Systeme zu ermöglichen.⁶ In einem patientenzentrierten System ist der Einzelne dafür verantwortlich, seine Daten zu generieren und zu verwalten, während Gesundheitsdienstleister diese Daten in ihren Verfahren verwenden, anstatt sie zu besitzen. Das Problem des transparenten Datenaustauschs wird von Norta und Kollegen erläutert.⁷

Die Erhebung und Verarbeitung von PHR bringt viele rechtliche, technische und emotionale Herausforderungen mit sich. Wissenschaftler konzentrieren sich auf die technischen und sicherheitstechnischen Voraussetzungen von PHR-Systemen, wenn die Daten zentral verwaltet werden.⁸⁻¹⁰ Diese Methodik erweist sich als effektiv, wenn die Anzahl der PHR-Datenquellen begrenzt ist. So steigt die Anzahl der Prozesse, die PHR verwenden, und der Bedarf an mehr Vertrauen zwischen den Beteiligten wie Privatunternehmen, Rechtsinstitutionen und Einzelpersonen sowie die Komplexität der Integration nehmen zu. Daher ist ein zentralisierter Ansatz nicht skalierbar, während dezentralisierte interorganisationale Prozesse auf der Grundlage der Blockchain-Technologie eine Grundlage für vertrauenswürdige und skalierbare Verbindungen bieten.

Ein integriertes PHR- und EHR-System ist ein soziotechnisches System, an dem Menschen aus verschiedenen Organisationen beteiligt sind, die unterschiedliche Technologien für die Zusammenarbeit und Problemlösung nutzen.¹¹ Ein EHR-System besteht aus Patientendaten, die von Angehörigen der Gesundheitsberufe erstellt und digital gespeichert werden. Zu diesen Daten gehören die Krankengeschichte, Medikamente, der Impfstatus, Labortestergebnisse und radiologische Bilder. Sie ermöglicht es den Angehörigen der Gesundheitsberufe, die Patientenversorgung effektiv zu planen und individuell zu gestalten, und bietet ihnen gleichzeitig die Möglichkeit, ihre Daten sicher zu speichern.

den Austausch medizinischer Informationen zwischen Gesundheitsdienstleistern und anderen autorisierten Nutzern. Darüber hinaus können EHR dazu beitragen, die Kosten im Gesundheitswesen zu senken und die Qualität der Versorgung zu verbessern. Die Entscheidung für ein patientenzentriertes System, das die persönlichen Daten weitergibt, ist emotional motiviert und schafft ein Gefühl der Unsicherheit über die Art und Weise, wie persönliche Daten verwendet werden.

Die Verwendung von EHR-integrierten PHR führt zu Konflikten in den Bereichen Sicherheit, Datenschutz und Privatsphäre. Datenschutz ist ein Rechtsbegriff, der die Kenntnis und Kontrolle über den Inhalt und die Erfüllung eines (intelligenten) Vertrags einschränkt, der nur im erforderlichen Umfang zwischen den Parteien ausgetauscht werden sollte.¹² Während der Schutz der Privatsphäre gemäß der Definition in der Charta der Grundrechte der Europäischen Union¹³ das Recht jeder Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz ist,⁷ bezieht sich der Datenschutz speziell auf die Verarbeitung personenbezogener Daten und ist auf die Wahrung dieser Privatsphäre ausgerichtet.⁸ In der Charta wird betont, dass personenbezogene Daten nach Treu und Glauben für festgelegte Zwecke und auf der Grundlage der Einwilligung der betroffenen Person oder einer anderen gesetzlich geregelten legitimen Grundlage verarbeitet werden müssen. Diese Unterscheidung ist für unsere Forschung von entscheidender Bedeutung, da sie unterstreicht, wie wichtig es ist, Blockchain-basierte Systeme so zu implementieren, dass sowohl die Rechte auf Privatsphäre als auch die Datenschutzgrundsätze gemäß der Charta gewahrt bleiben.

diese Grundrechte.

Der von der Europäischen Kommission (EK) definierte Standard schlägt Vertragsklauseln der Europäischen Union vor, die von der EU im Juni 2021 genehmigt wurden.¹⁴ Es ist wichtig anzumerken, dass diese Klauseln im Dezember 2022 durch aktualisierte Versionen ersetzt werden sollen, als Teil der laufenden Bemühungen der EK, die Datenschutzstandards im Einklang mit der sich entwickelnden rechtlichen und technologischen Landschaft zu verbessern. Wie in den Standardvertragsklauseln (SCC) der Europäischen Kommission dargelegt, ist diese Aktualisierung ein wichtiger Schritt, um robuste und aktuelle Datenschutzmaßnahmen bei grenzüberschreitenden Datenübertragungen zu gewährleisten.

In den Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing¹⁵ weisen der Europäische Datenschutzausschuss (EDPB) und die spanische Datenschutzbehörde (AEPD) darauf hin, dass bei der Verknüpfung von Identifikatoren mit einem Hash, z. B. einer Telefonnummer, die Informationen eindeutig auf einen bestimmten Dateninhaber zurückgeführt werden können. Diese Verknüpfung stellt eine zusätzliche Schwachstelle für die Vertraulichkeit des Hash dar, da der verknüpfte Identifikator den effektiven Nachrichtenraum für diesen bestimmten Hash verringern kann, wodurch die beabsichtigte Pseudonymisierungsfunktion beeinträchtigt wird. Diese Erkenntnis verdeutlicht die potenziellen Einschränkungen und Herausforderungen bei der Verwendung von Hash-Funktionen für den Datenschutz und unterstreicht die Notwendigkeit einer sorgfältigen Prüfung ihrer Anwendung in Blockchain-basierten Systemen.

Sun und Kollegen¹⁶ definieren die wichtigsten Anforderungen an medizinische Systeme, die das Internet der Dinge (IoT) nutzen, als Datenintegrität, Benutzerfreundlichkeit, Auditing und Patientenschutz.

Datenschutz. Al-Muhtadi und Kollegen¹⁷ konzentrieren sich auf Fragen der Cybersicherheit und des Datenschutzes bei der Integration von mobilen Gesundheitsanwendungen und schlagen eine sichere Architektur für Multi-Cloud-Umgebungen vor. In einer Studie von Katurura und Cilliers¹⁸ wird festgestellt, dass es den Nutzern an Datenkontrolle und Transparenz mangelt. Darüber hinaus haben Forscher einen Mangel an Wissen über Sicherheits- und Datenschutzrisiken im Zusammenhang mit persönlichen Daten für tragbare Geräte festgestellt.¹⁹ Mehrere Autoren haben hervorgehoben, dass die gemeinsame Nutzung medizinischer Daten zu Sicherheits- und Datenschutzrisiken führt.²⁰⁻²² Gleichzeitig machen die Autoren geltend, dass weitere Untersuchungen zur Entwicklung sicherer und integrierter Gesundheitssysteme erforderlich sind. Die autonome Erhebung von Gesundheitsdaten stellt neue Herausforderungen für den Datenschutz beim Einsatz von Smart-Home-Systemen dar.²³⁻²⁵

Salehi und Giacalone haben die Verwendung gleichwertiger Algorithmen zur Lösung ziviler Konflikte vorgeschlagen.²⁶ Diese Algorithmen beruhen auf verschiedenen Technologien wie künstlicher Intelligenz (KI) und algorithmischen Entscheidungssystemen (ADS). In ihrer Veröffentlichung²⁷ stellen Xu und Kollegen eine systematische Untersuchung vor, bei der das Graph Model for Conflict Resolution (GMCR) als praktikabler Ansatz zur Lösung von Konflikten in der realen Welt verwendet wurde. Andere Wissenschaftler²⁸ verwenden Hidden Markov Models (HMM), um die eingehenden Daten zu untersuchen und eventuell auftretende Konflikte zu lösen. Die Analyse umfasst die Simulation und das Training der HMM-Modelle, die später mit einem regelbasierten System verwendet werden, um widersprüchliche Informationen zu erkennen, die identifizierten Konflikte zu lösen und frühere Daten und Entscheidungen zu nutzen, um Konflikte zu vermeiden, bevor sie auftreten. Einige Forscher²⁹ schlagen den Einsatz eines Mediators vor, der Konflikte aufdeckt und den Konfliktparteien eine mögliche Lösung anbietet.

Die Hauptforschungsfrage ist, wie Konflikte in integrierten interorganisatorischen Prozessen der elektronischen Gesundheitsversorgung automatisch gelöst werden können. Zur Beantwortung der Hauptfragestellung leiten wir die folgenden Teilfragen ab. Was sind die Anforderungen an eine individuumszentrierte interorganisationale Erfassung und Verarbeitung von PHR? Die Beantwortung dieser Frage zielt darauf ab, den logischen Anforderungsraum zu definieren, der die Zuordnungen der Stakeholder beinhaltet. Welche Konflikte entstehen in inter-organisationalen eHealthcare-Prozessen? Zur Beantwortung dieser Frage werden die Konflikte innerhalb der interorganisationalen E-Healthcare-Prozesse herausgearbeitet und mit den in der vorangegangenen Forschungsfrage skizzierten Prozessen abgeglichen. Darüber hinaus werden diese Prozesse unter Verwendung der Business Process Model and Notation (BPMN) entwickelt. Welche automatischen Konfliktlösungstechniken gibt es in der dezentralen elektronischen Gesundheitsfürsorge? Das Ziel der Technik zur Lösung von Datenschutzkonflikten besteht darin, einen Konfliktlösungsprozess für die elektronische Gesundheitsfürsorge unter Verwendung von BPMN zu erstellen, der auf dem Prozessdesign basiert, in dem Konflikte auftreten, wie in der vorangegangenen Forschungsfrage definiert.

Untersuchung.

Im Folgenden wird ein Überblick über den weiteren Verlauf dieser Untersuchung gegeben.

- Eine Literaturübersicht, Vorbemerkungen und ein laufender Fall.
- Diskussion der Anforderungen an eine patientenzentrierte PHR-Erfassung und -Verarbeitung.
- Darstellung von Konflikten im dezentralen E-Health-Prozess durch Zuordnung zu spezifischen funktionalen Zielen und Geschäftsprozessen.
- Erörterung der Techniken zur Lösung von Datenschutzkonflikten bei der Verarbeitung medizinischer Daten in interorganisationalen Prozessen.
- Bewertung des entwickelten Prozesses und Gegenüberstellung der Ergebnisse mit denen anderer Forschungsbemühungen.
- Schlussfolgerung mit Einblicken in die Grenzen, ungelöste Probleme und mögliche Wege für zukünftige Forschung.

Literaturübersicht und Vorbemerkungen

Hier geben die Autoren einen Überblick über die einschlägige Literatur und stellen die Vorarbeiten vor, die den Hintergrund für diese Untersuchung bilden.

Literaturübersicht

Die Forschung zur Blockchain-Technologie im Gesundheitswesen hat stetig zugenommen.³⁰⁻³² Die Hauptschwerpunkte in diesem Bereich sind die gemeinsame Nutzung von Daten, Gesundheitsakten und die Zugangskontrolle. Ein verteiltes Hauptbuch, wie es von einer Blockchain vorgeschlagen wird, stellt das Konzept dar, dass Teilnehmer neue Datensätze hinzufügen. Die in einer Blockchain gespeicherten Informationen sind unveränderlich, was durch Kryptografie gewährleistet wird.³³ Die in der Blockchain enthaltenen Daten werden sicher in Transaktionen gespeichert, die dann durch kryptografische Methoden in Blöcken organisiert und miteinander verbunden werden.

Jeder Block ist eng mit dem nachfolgenden Block in der Kette verbunden. Durch die Verwendung der als Merkle-Baum oder Hash-Baum bezeichneten kryptografischen Technik wird sichergestellt, dass die in einer Blockchain gespeicherten Transaktionen durch mathematische Hashes korreliert werden,^{34,35} wodurch gewährleistet wird, dass keine Veränderung die Gesamtheit der gespeicherten Daten ungültig machen kann. Hashes rationalisieren den Prozess der Validierung neuer Transaktionen und machen eine Analyse aller in einer Blockchain gespeicherten Informationen überflüssig.³⁵ Einige Blockchains, wie z. B. Ethereum, unterstützen intelligente Verträge, die von den Knoten ausgeführt werden können.

Forschungsmethodik

In dieser Arbeit wird die Design-Science-Forschung (DSR) zur "Durchführung der Forschung" verwendet. Die DSR bietet einen Rahmen für die Entwicklung und Bewertung neuer Artefakte.³⁶ Die Umgebung, die DSR-Bewertung und die Wissensbasis sind die drei Hauptkomponenten der DSR. Das Forschungsumfeld beschreibt die Probleme, mit denen Organisationen und Anwendungsbereiche konfrontiert sind. Die Wissensbasis bietet theoretische Unterstützung für die Entwicklung neuer Artefakte, die die identifizierten

organisatorische Probleme lösen. Das erstellte Artefakt wird im Rahmen der DSR evaluiert.³⁶

Frühere Forschungsarbeiten von Narendra und Kollegen¹¹ über den Konfliktlösungsansatz in der M2X-Umgebung (Machine-to-Everything) dienen als Grundlage für diese Studie. In diesem Artikel wird der zuvor vorgeschlagene Ansatz an eine E-Health-Umgebung angepasst, in der es den an den inter-organisationalen Prozessen beteiligten Parteien an Vertrauen fehlt.

Die Wissensbasis stellt bestehende Strategien, Techniken und Modelle dar, die als Bausteine für die Gestaltung der Konfliktlösungsmethoden und des dezentralen interorganisationalen Prozessablaufs dienen. Wir verwenden das Trustable DApp Modeling (T-DM) Framework für die Definition von Design-Prozess-Anforderungen, da es den Agent-Oriented Modeling (AOM) Ansatz erweitert und tokenisierte Ziele einführt, die in Blockchain-Systemen verwendet werden. Für eine detailliertere Beschreibung des Testdatenmanagement-Frameworks (T-DM) und der BPMN zur Definition von Prozessabläufen verweisen wir den Leser auf den Abschnitt "Vorarbeiten" weiter unten.

Die entwickelten automatischen Konfliktlösungstechniken werden in dezentralen e-Healthcare-Prozessen mit Colored Petri Nets (CPN) Modellierung evaluiert. Zusätzlich stellen wir einen Proof-of-Concept (PoC)-Typ zur Verfügung, der die Implementierung des laufenden Falls illustriert. Der Bewertungsansatz ähnelt dem, der in früheren Forschungsarbeiten verwendet wurde.¹¹ Darüber hinaus stellen wir die Implementierung des modellierten laufenden Falls mit dem PoC bereit.

Der laufende Fall und der Hintergrund Vorbemerkungen

Um die Vertraulichkeit zu gewährleisten und die Konfliktlösung zu erleichtern, bieten wir im Abschnitt "Laufender Fall und Konfliktszenario zum Schutz der Privatsphäre" eine umfassende Analyse an, die ein praktisches Szenario aus der Sicht des Patienten darstellt. Die vorliegende Fallstudie soll das Verständnis des laufenden Falles und der nachfolgenden Abschnitte dieses Papiers erleichtern. Der Abschnitt "Vorbemerkungen" bietet die notwendigen einleitenden Informationen, die für das Verständnis der nachfolgenden Abschnitte unerlässlich sind.

Laufender Fall und Konfliktszenario zum Datenschutz

Abbildung 2 zeigt eine Beschreibung des laufenden Falles im Bereich der Krebsprävention. Während Physiotherapeuten in erster Linie die klinischen Ergebnisse bewerten, indem sie den Schmerzgrad, den Bewegungsumfang und die Muskelkraft beurteilen, bestehen die Zielbereiche der Patienten aus körperlicher Aktivität, der Qualität der Arbeitsumgebung und der Schlafqualität. Die beobachtete Diskrepanz lässt sich erklären, wenn man bedenkt, wie kompliziert der Vergleich von Einzelpersonen mit Hilfe der Patient Specific Functional Scale ist.³⁷ Folglich ist es nicht möglich, die Bereiche der Patientenziele zu quantifizieren. In unserem Fall werden die Gesundheitsdaten vom Patienten mit einer Smartwatch und Sensoren für die Luft- und Wasserqualität überwacht. Diese

Geräte sammeln Aktivitäts-, Gesundheits- und ökologische Umweltdaten der Patienten und teilen sie bei Bedarf.

Die oben genannten Informationen werden kontinuierlich gesammelt, wobei der Gesundheitsdienstleister während der Patientüberwachung eine Feedbackschleife erhält. Wenn der Patient einen Allgemeinmediziner in einem Krankenhaus aufsucht, führt dieser Labortests durch, erhebt die Krankengeschichte und gibt diese Daten anschließend in das EHR ein. Zusammenfassend lässt sich sagen, dass das EHR sowohl von Angehörigen der Gesundheitsberufe als auch von Allgemeinmedizinern gemeinsam genutzt wird. Diese Personen sind dafür verantwortlich, umfassende Berichte an die Versicherungsträger zu übermitteln, um die Kostenerstattung für die erbrachten medizinischen Leistungen sicherzustellen. Die medizinischen Berichte variieren in Abhängigkeit von den Informationen, die den Angehörigen der Gesundheitsberufe zur Verfügung stehen und die die PHR zusammen mit den kontinuierlichen Eingaben des Patienten umfassen.

Das oben beschriebene Phänomen dient dazu, das Verständnis für gesundheitsbezogene Umstände zu verbessern, was wiederum die Erbringung von personalisierten Gesundheitsdienstleistungen durch den Arzt erleichtert. Im Gegensatz dazu kann der Allgemeinmediziner nur auf die elektronische Patientenakte zugreifen, da es keinen Feedback-Mechanismus gibt.

Die Diskrepanz bei der Geltendmachung medizinischer Informationen steht im Widerspruch zur Versicherungsgesellschaft, die über keine Richtlinien für die Verarbeitung von PHR-Daten verfügt. Diese Diskrepanz erschwert zudem die Nutzung neu entwickelter Gesundheitseinrichtungen, die auf der Verarbeitung von PHR-Daten basieren. Es ist plausibel, dass die Implementierung eines Feedback-Mechanismus die Situation verbessern könnte.

Der Patient stößt auf Datenschutzkonflikte aufgrund der Anfälligkeit seiner Daten in intelligenten autonomen Geräten oder verschiedenen Anwendungen, was zu Datenschutzkonflikten führt. Wenn der Patient seine PHR dem Hausarzt zur Verfügung stellt, nachdem dieser sich mit einer ausdrücklichen Erklärung zur Verwendung der Patientendaten im Rahmen der gesetzlichen Bestimmungen bereit erklärt hat, kann dieser sie im Rahmen der internen Verfahren des Gesundheitsdienstleisters verwenden, z. B. zur Erstellung von Berichten, zur Durchführung statistischer Analysen und zur Erleichterung von Forschungsbemühungen. An diesen Verfahren können externe Teilnehmer wie das Nationale Statistikamt, unabhängige Forschungsunternehmen oder auf Datenberichterstattung spezialisierte Privatunternehmen beteiligt sein. Die Undurchsichtigkeit der Verfahren für den Patienten macht sie intransparent. Infolgedessen besteht die Möglichkeit, dass mit den PHR-Daten falsch umgegangen wird.

In diesem Artikel definieren wir drei Konflikte während des interorganisatorischen Versicherungsprozesses. Erstens ist das Home-Monitoring mit Datenschutzkonflikten verbunden, wenn Patientendaten gesammelt werden. Wearable Devices und PHR-Systeme, die die gesammelten Daten speichern, sind anfällig für die Möglichkeit, dass Unbefugte diese Informationen abgreifen. Als Nächstes entsteht ein Integritätskonflikt, wenn PHR verschiedene Prozesse durchlaufen und von den beteiligten Parteien verändert werden können.

beteiligten Parteien. Schließlich entsteht ein Konsistenzkonflikt, wenn der Versicherungsanbieter sowohl von der medizinischen Fachkraft als auch vom Arzt Anträge erhält und diese unterschiedliche Informationen im Versicherungsantrag angeben.

Vorbemerkungen

Dieser Artikel befasst sich mit Prozessen des elektronischen Gesundheitswesens, die auf Blockchain-Systemen abgebildet werden, um unveränderliche Rückverfolgbarkeit, Sicherheit und Datenschutz zu erreichen, die eine verteilte Disintermediation und Dezentralisierung bei der Zusammenarbeit zwischen Organisationen gewährleisten. Die Blockchain-Technologie bietet ein verteiltes Hauptbuch, das es den Teilnehmern ermöglicht, Datensätze zu einem Hauptbuch hinzuzufügen und zu überprüfen, wobei die Kryptographie sicherstellt, dass die Datensätze unveränderlich sind.³³ Wenn Teilnehmer Datensätze zum Hauptbuch hinzufügen, werden sie als Hash-Transaktionen gespeichert und in Blöcken gruppiert. Die kryptografische Verknüpfung zwischen jedem Block und seinem Vorgänger ist ein grundlegendes Merkmal des betrachteten Systems. Intelligente Verträge sind ausführbare Programme, die auf der Blockchain ausgeführt und gespeichert werden.³⁸ Laut Nguyen und Kim³⁸ sind die gängigen Blockchain-Plattformen Bitcoin,³⁹ Ethereum,⁴⁰ Hyperledger Fabric,⁴¹ usw.

Blockchains verwenden verschiedene Konsensmechanismen, um Transaktionen zu validieren. Bitcoin beispielsweise verwendet einen Proof-of-Work (PoW)-Konsensalgorithmus. Dieser Mechanismus geht davon aus, dass alle teilnehmenden Knoten ein schwieriges mathematisches Problem lösen. Er belohnt den ersten Knoten mit der Anzahl der Token, indem er ihm erlaubt, den nächsten Block hinzuzufügen.³⁸ Ethereum verwendet einen Proof-of-Stake (PoS), bei dem die Validierung nicht auf den für die Lösung eines mathematischen Problems aufgewendeten Ressourcen, sondern auf der Reputation eines Knotens beruht. Wir verweisen auf unsere frühere Forschung⁴² für weitere Einzelheiten über die praktische Nutzung der Blockchain-Technologie.

Für die Blockchain-Technologie gibt es verschiedene Token-Typen. Hier schlagen wir die Verwendung von zwei Token-Typen vor: nutzbare und nicht übertragbare "soul bound" Token (SBT). Das Konto stellt die "Seele" dar, und die von den Konten gehaltenen Token werden als "Soulbound Tokens" (SBTs) bezeichnet.⁴³

Der Utility Token wird in ein bestehendes Protokoll auf der Blockchain integriert und für den Zugriff auf die Dienste dieses Protokolls verwendet. Darüber hinaus wird er als Kryptowährung verwendet, die den Zugang zu einem Produkt oder einer Dienstleistung darstellt. Im Gegensatz zu Utility-Tokens sind SBTs durch ihre Einzigartigkeit und Seltenheit definiert. Dieser Token-Typ bietet Token-Eigentum und entsprechende Transferfunktionen. Die Verwendung von SBTs im dezentralen E-Healthcare-System wird vorgeschlagen, da eine wirksame Verwaltung der Identität und Zugangskontrolle für E-Healthcare-Daten erforderlich ist.

Um den Zugang zu ihrem Identitätsmanagement zu kontrollieren, müssen Einzelpersonen in der Lage sein, nicht nur ihre Identifikatoren, sondern auch die mit ihnen verbundenen Daten zu verwalten. Dieser Ansatz ist von grundlegender Bedeutung für die selbstverwaltete Identität und stellt eine Abkehr von herkömmlichen Identitätsmanagementsystemen hin zu einem nutzergesteuerten Identitätsverwaltungsmodell dar. In einem solchen Modell, das durch die Blockchain-Technologie ermöglicht wird, haben die Nutzer die volle Kontrolle über ihre Identifikatoren und die damit verbundenen persönlichen Daten.

Daten, die mit diesen Identifikatoren verknüpft sind, was eine größere Autonomie und Privatsphäre bei digitalen Interaktionen gewährleistet.⁴⁴

Das Blockchain-Ökosystem unterstützt verschiedene Arten von Teilnehmern, z. B. Orakel und dezentrale autonome Organisationen (DAOs). Im Blockchain-Kontext werden Orakel verwendet, um externe Daten abzurufen, die in der Blockchain nicht zur Verfügung stehen. Orakel sind zentralisiert und vertrauen dem externen Datenanbieter, aber es gibt ein bekanntes Problem mit ungesicherten Datenabrufkanälen.⁴⁰ Allerdings gibt es bei Orakeln Probleme mit der Vertrauenswürdigkeit und Zuverlässigkeit.⁴⁵ Da Testorakel nicht vollständig automatisiert werden können, muss der Agent eingreifen, um die Korrektheit des Verhaltens des Orakels sicherzustellen. Caldarelli und Ellul⁴⁶ erklären, dass eine DAO eine autonome Organisation ist, die mit intelligenten Verträgen implementiert ist. Das Verhalten und die Geschäftsregeln der DAO sind durch eine intelligente Vertragslogik vordefiniert.

Das daraus abgeleitete E-Healthcare-System wird in einer inter- oder organisationsübergreifenden Zusammenarbeit eingesetzt, die auf einem dynamischen Outsourcing von Dienstleistungen basiert, das in elektronischen Verträgen festgelegt ist.⁴⁷ Im Gesundheitswesen umfassen interorganisatorische Prozesse den Austausch von Daten zwischen Patienten und Gesundheitsdienstleistern oder anderen Organisationen wie Versicherungsgesellschaften. In diesem Papier wird eine patientenzentrierte, dezentrale Systemperspektive betrachtet, bei der PHR-Daten durch verschiedene Systeme fließen und menschlichen und nicht-menschlichen Agenten wie autonomen intelligenten Geräten zur Verfügung stehen. Zu solchen Geräten gehören Wearables, die den Gesundheitszustand des Patienten mit Sensoren überwachen, Smart-Home-Komponenten, autonome Drohnen oder sogar Fahrzeuge, die in Gesundheitsprozesse eingebunden sind. Die Forschung von Grefen und Kollegen⁴⁸ stellt einen konzeptionellen Rahmen für ein intelligentes E-Health-Gateway vor, das die gesammelten medizinischen Informationen erfasst und analysiert. In unserer Untersuchung integrieren wir die in dem Artikel von Narendra et al.¹¹ vorgeschlagene Strategie zur Lösung von Datenschutzkonflikten in ein dezentralisiertes Ökosystem für das Gesundheitswesen, das selbstverwaltete intelligente Geräte und deren Zusammenarbeit umfasst, wie in Ref. 49.

In soziotechnischen Systemen steht die Erfüllung gesellschaftlicher Funktionen im Mittelpunkt.⁵⁰ Da solche Systeme nicht autonom funktionieren, sondern das Ergebnis menschlichen Handelns sind, schlägt die Forschung bei der Modellierung komplexer soziotechnischer Systeme einen agentenorientierten Ansatz vor.⁵¹ Da simulierte Akteure aufgrund ihrer kognitiven und sozialen Bindung mit dem Wissen über sich selbst und der Abhängigkeit von ihrer Geschichte dem Menschen ähnlich sind, nutzt ein agentenorientierter Ansatz dies im Verhalten der Agenten. Im Bereich von Blockchain und Smart Contracts geht es beim Orakelproblem vor allem um die Vertrauenswürdigkeit und Zuverlässigkeit von Orakeln.⁴⁵ Wie Barr behauptet,⁵² entsteht dieses Problem, wenn Testorakel nicht in der Lage sind, vollautomatisch zu arbeiten. Wenn die Orakel nicht automatisiert sind, muss ein Agent eingreifen, um die Richtigkeit des beobachteten Verhaltens zu überprüfen. Wir betrachten Multi-Agenten-Systeme (MAS) und verwenden einen AOM-Ansatz⁵¹, um die Anforderungen zu definieren

des datenschutzorientierten PHR- und EHR-Datenintegrationsprozesses.

Die Zielmodellierung wird zur Analyse soziotechnischer Bereiche⁵³ verwendet, da Zielmodelle das Wertversprechen eines Systems darstellen. Der Wert des Systems wird durch funktionale und qualitative Ziele und Rollen dargestellt. Das System benötigt eine bestimmte Kapazität oder eine Position, die durch eine Rolle dargestellt wird, um seine Ziele zu erreichen. Ein funktionales Ziel stellt die funktionale Anforderung des Systems dar, und ein Qualitätsziel stellt die nichtfunktionale oder qualitative Anforderung eines Systems dar.⁵³ Qualitätsziele werden in der Softwaretechnik synonym als nichtfunktionale Anforderungen bezeichnet.⁵³ Die funktionalen, qualitativen und emotionalen Ziele werden an alle ihre Unterziele vererbt.

Da es sich bei einem patientenzentrierten elektronischen Gesundheitsfürsorgesystem um ein soziales System handelt, das mehr durch emotionales Engagement als durch Funktionalität bestimmt wird, wird in der Forschung⁵⁴ ein Emotional Attachment Framework vorgeschlagen, das emotionale Ziele bereits in der frühen Entwurfsphase berücksichtigt. Dieser Rahmen ist in den T-DM-Rahmen integriert. Es wird um emotionale Ziele erweitert, die die Gefühle der Benutzer in Bezug auf negative Emotionen repräsentieren, wie z. B. Misstrauen und fehlendes Eigentum an privaten und vertraulichen Daten.⁵⁴ Die Forschung von Kormiltsyn⁵⁵ definiert positive und negative Emotionen bei der Bewertung eines Produkts oder einer nützlichen oder schädlichen Dienstleistung. Mendoza und Kollegen⁵⁶ beschreiben, wie Qualitätsziele unterschiedliche positive und negative Emotionen bei den Nutzern auslösen. Beispiele für solche Ziele sind Nützlichkeit, Anpassungsfähigkeit und Benutzerfreundlichkeit. In dieser Arbeit platzieren wir die emotionalen Ziele zwischen einer Rolle und einem funktionalen Ziel, um Emotionen zu definieren, die die funktionalen Ziele des Systems beeinflussen.

Das Thema Datenschutz- und Sicherheitskonfliktmanagement gewinnt mit der zunehmenden Nutzung von IoT, sozialen Netzwerken usw. an Bedeutung. In einer Studie von Mendoza und Kollegen⁵⁷ werden die grundlegenden Konzepte der sicheren Datenverarbeitung definiert,

Sie besagen, dass sich der Datenschutz auf die Verwaltung der Daten einer Person konzentriert. Sicherheitsmaßnahmen werden zum Schutz vor unbefugtem Zugriff implementiert, wobei der Schwerpunkt auf der Sicherung von Daten gegen verschiedene Formen von Angriffen und der Verhinderung von Datendiebstahl liegt.⁵⁸ Mehrere Forschungspublikationen bestätigen die Bedeutung der Definition von Konfliktmanagementtechniken beim Austausch persönlicher Daten.^{59,60}

Um ein Zielmodell für das dezentrale E-Health-System zu entwerfen, verwenden wir den im T-DM-Rahmenwerk⁶¹ definierten Ansatz, der sich auf die Entwicklung dezentraler Anwendungen (DApps) zur Unterstützung interorganisatorischer Prozesse konzentriert. Der T-DM-Rahmen erweitert die AOM-Zieldiagramme^(53, 61) und führt ein neues Konzept von tokenisierten Zielen ein, die die dezentralen Dienste darstellen, die Transaktionen in der Blockchain durchführen und Token ausgeben oder gewinnen. Der modellgesteuerte Ansatz im T-DM-Rahmen unterstützt die Abbildung von AOM-Zielmodellen auf das Komponentenarchitekturmodell der Unified Modeling Language (UML).

Um die vorgeschlagene Konfliktlösungstechnik zu bewerten, haben wir ein formales CPN⁶²-Modell entwickelt. CPN, eine grafisch orientierte Sprache, ist in der Lage, potenzielle Entwurfsfehler, fehlende Spezifikationen sowie Sicherheits- und Datenschutzprobleme in Systemen zu erkennen. Sie dient dem Zweck, Systeme zu entwerfen, zu spezifizieren, zu simulieren und zu verifizieren. Ein CPN-Modell ist ein zweiseitiger Graph mit Token, Stellen, Bögen und Übergängen. Stellen können mehrere farbige Token enthalten, die Attribute mit entsprechenden Werten anzeigen. Die Übergänge in CPN werden nur ausgelöst, wenn alle Eingabestellen die erforderlichen Token enthalten. Schließlich erzeugen die Übergänge bedingungsabhängige Token in den Ausgabestellen.⁶³ Unser Modell verwendet die CPN ML-Programmiersprache, um den in Abbildung 1 beschriebenen Fall zu simulieren. Ausführlichere Informationen über CPN finden Sie in der Forschung⁶³.

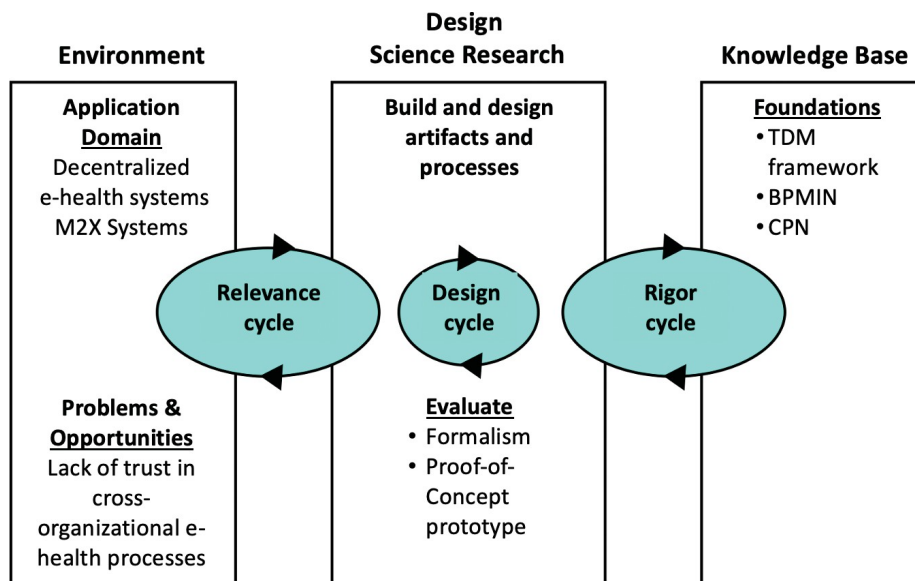


Abb. 1. Design Science Forschungszyklen. BPMN: Geschäftsprozessmodell und Notation; CPN: Colored Petri Nets; DSR: de-sign-science research; M2X: Machine-to-Everything; TDM: Trusted Document Management.

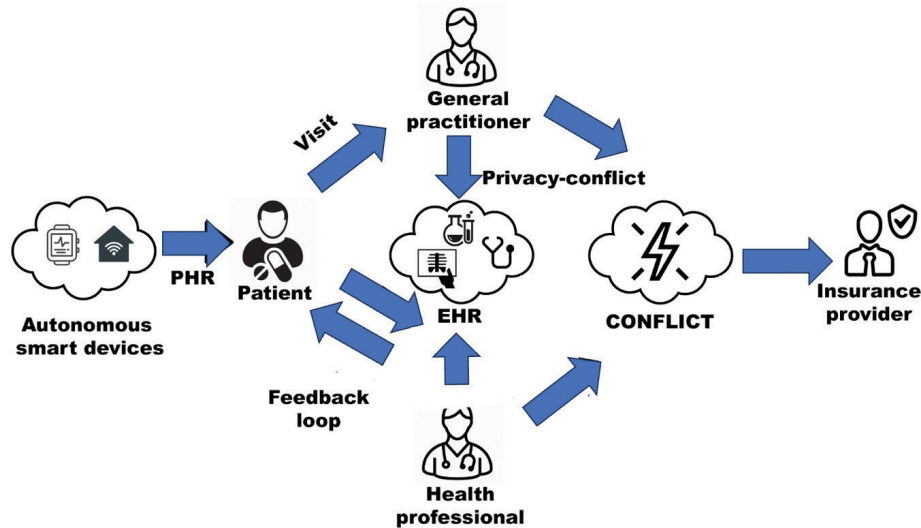


Abb. 2. Konflikte bei der Verarbeitung von (EHRs) Electronic Health Records und (PHRs) Personal Health Records.

In einem Blockchain-basierten E-Health-System kann die vertrauenswürdige gemeinsame Nutzung von Daten durch die Multi-Faktor-Authentifizierung (MFSSIA)⁶⁴ für Menschen und Maschinen ermöglicht werden, die mit Smart-Contract-Blockchain-Technologien verwaltet wird.

Abbildung 3 veranschaulicht, wie menschliche Nutzer (wobei zu beachten ist, dass intelligente autonome Geräte auch anstelle von Menschen eingesetzt werden können) Aufgaben für andere Entitäten erstellen und diese auffordern, zu antworten. Entweder scheidet die entsprechende Entität oder sie kann die Herausforderungen mit korrekten Antworten abschließen. Die gewählte Herausforderung hängt vom Anwendungsfall, der erforderlichen Sicherheitsstufe und der Bedrohungsstufe der beteiligten Einheiten ab. In dem Beispiel in Abbildung 2 authentifiziert die Organisation ein autonomes Gerät, indem sie ihm Aufgaben stellt, die es zur Bestätigung seiner Identität erfüllen muss. Die Organisation entscheidet, ob die Antwort ihrer Anfrage entspricht. Beide laden die Anfrage und die Antwort in die Blockchain hoch. In diesem Fall schlägt die Authentifizierung fehl, wenn die antwortende Einheit nicht korrekt antwortet. Andernfalls, wird die Entität erfolgreich authentifiziert.

Die Multi-Factor-Challenge-Set-Self-Sovereign-Identity-Authentifizierung (MFSSIA) ermöglicht blockchain-übergreifende Interoperabilität durch den Einsatz von Blockchain-Orakeln. Die Orakel sind digitale Agenten, die darauf abzielen, Informationen aus der Außenwelt in eine Blockchain zu holen. Daten aus verschiedenen Quellen (Blutdruckmessgeräte, PHR, EHR usw.) werden dann als Transaktionsdaten in die Blockchain eingespeist.⁶⁴ Orakel werden als Datenfeeds für Informationen aus der realen Welt verwendet, die von Smart Contracts, die auf Blockchains laufen, abgefragt werden, und indem sie Daten von der Blockchain selbst in Datenquellen einspeisen.⁶⁵

Die Challenge-Sets in MFSSIA werden in einem dezentralen Wissensgraphen (DKG³) gespeichert. Im DKG werden die Informationen

als Graph von Entitäten und Beziehungen gespeichert, die für eine bestimmte Domäne oder Organisation relevant sind. Der DKG bietet unveränderliche, abfragbare und durchsuchbare Graphen, die in verschiedenen Anwendungen verwendet werden können.

Ergebnisse

Der vorliegende Abschnitt liefert die Ergebnisse, die die Antworten auf die in diesem wissenschaftlichen Dokument formulierten Forschungsfragen darstellen. Zur Spezifizierung der Anforderungen an die personenzentrierte PHR-Erfassung und -Verarbeitung (Teilfrage 1) liefert der Abschnitt "Anforderungen an die patientenzentrierte PHR-Erfassung und -Verarbeitung" das Zielmodell für den dezentralen, personenzentrierten, organisationsübergreifenden E-Health-Prozess für die präventive Gesundheitsversorgung. Dieses Zielmodell bildet die Grundlage für den Systementwurf, indem es die wichtigsten funktionalen und qualitativen Anforderungen festhält. Zur Identifizierung von Konflikten (die später erörtert werden) werden im Abschnitt "Integrierte PHR- und EHR-Verarbeitung - Datenschutzkonflikte zwischen Gesundheitsdienstleistern und einzelnen Patienten" (Unterfrage 2) Konflikte im dezentralen E-Health-Prozess definiert und die Zuordnung von Konflikten zu spezifischen funktionalen Zielen und Geschäftsprozessen beschrieben. Zur Darstellung der Konfliktlösungstechniken werden schließlich im Abschnitt "The Conflict-Resolution Techniques When Mapping the BPMN-Designed e-Healthcare Process to a Blockchain System" (Teilfrage 3) Techniken im Blockchain-System vorgeschlagen, um die identifizierten Daten- und Antragstellerdefinitions konflikte transparent und dezentral automatisiert zu lösen.

Anforderungen an die patientenzentrierte PHR-Erhebung und -Verarbeitung

Wie Norta et al.⁵³ darlegen, kann ein Zielmodell als Analyseinstrument für die Untersuchung von Problemen dienen, die in einem soziotechnischen Bereich auftreten. Die Zielmodelle dienen als Schnittstelle für den Informationsaustausch zwischen den Beteiligten technischen und nicht-technischen

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

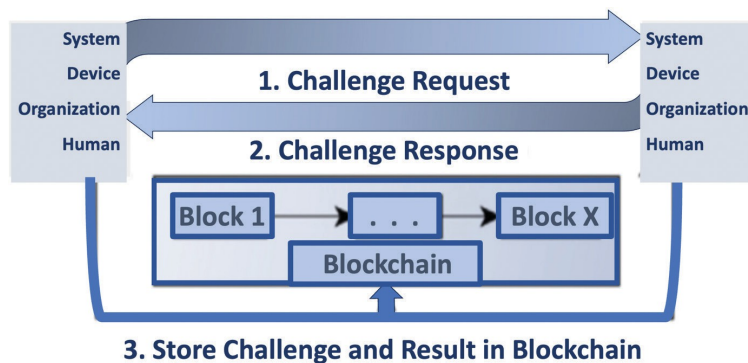


Abb. 3. Konzeptuelle Darstellung des (MFSSIA) Multi-Factor Challenge-Set Self-Sovereign Identity Authentication Lifecycle für Challenge-Response Management.

Hintergründe mit dem Ziel, umfassendes Wissen über den E-Health-Bereich zu generieren. Aufgrund der Komplexität des Zielmodells haben wir es in zwei Teile aufgeteilt, wobei in Abbildung 4 Ziele in Bezug auf den Patienten und das medizinische Fachpersonal und in Abbildung 5 Ziele in Bezug auf den Versicherungsträger und den Allgemeinmediziner definiert sind. Die Abbildungen 4 und 5 zeigen ein Zielmodell, in dem funktionale, qualitative, positive und negative emotionale Ziele beschrieben werden. Es ist wichtig zu beachten, dass jedes funktionale Ziel hierarchisch in Unterziele unterteilt ist, wobei die höchste Ebene an der Spitze und die niedrigste Ebene am unteren Ende angeordnet ist. In unserer früheren Forschung⁶⁶ haben wir die Zielmodellierung im Requirements Engineering eingesetzt. Wir verwenden die Notation, die in Ref. 57 beschriebene Notation, bei der mehrere Symbole verschiedenen Zieltypen entsprechen. So steht die Herzform für positive emotionale Ziele, die Wolkenform für Qualitätsziele und ein Parallelogramm für funktionale Ziele. In dieser Forschungsarbeit erweitern wir die Zielmodellnotation um die tokenisierten funktionalen Ziele, die die funktionalen Ziele darstellen, die mit einer Blockchain kommunizieren. In unserem entworfenen System betrachten wir den M2X-Kontext, in dem Agenten sowohl menschlich als auch nicht-menschlich sein können.

Wir schlagen vor, ein Utility-Token zu verwenden, das in ein bereits bestehendes Protokoll auf der Blockchain integriert ist und für den Zugang zu den verschiedenen von diesem Protokoll angebotenen Diensten verwendet wird. Diese Token dienen als Zahlungsmittel für die Dienstleistungen, die innerhalb ihres jeweiligen Ökosystems im vorgeschlagenen System angeboten werden. Unser Vorschlag ist die Einführung eines Tokens mit dem Namen "Personal Health Token (PHT)" als Utility Token für das dezentralisierte, personenzentrierte E-Health-System.

Zusätzlich zum Utility Token schlagen wir die Verwendung von SBT-Tokens vor, die von Anbietern medizinischer Daten wie Smart Devices, PHR- und EHR-Systemen erstellt werden und die medizinischen Daten enthalten, die dem Patienten gehören. Wenn ein Patient beispielsweise beschließt, dass einige seiner Gesundheitsdaten für die medizinische Forschung nützlich sind, weist er seine Eigentümerschaft mit SBT gegenüber dem Forschungsunternehmen nach. Das Hauptziel des Wertversprechens ist die *Prävention von Krankheiten*

in Verbindung mit einem Individuum, das über selbstmotivierte Anreize verfügt und davon ausgeht, dass es während des gesamten Präventionsprozesses informiert und befähigt wird. Das Hauptwertversprechen des Systems liegt in der Prävention von Krankheiten beim Einzelnen. Das Teilziel der häuslichen Pflege beinhaltet einen Patienten, der seine medizinischen Daten vertrauensvoll erfasst. Das Teilziel der ambulanten Versorgung wird vom Hausarzt ausgeführt, während das Teilziel der Versicherung von einem Versicherungsanbieter ausgeführt wird. Das Teilziel des Onboarding von Stakeholdern wird von einem Akzeptanzagenten ausgeführt. Das Ziel des Akteurs, das im System zu finden ist, ist für die Akteure entscheidend, um sich am interorganisationalen Prozess zu beteiligen, während sie die Verifizierung mithilfe eines Protokolls namens MFSSIA vornehmen, das auf der Blockchain-Technologie basiert.⁶⁴ Das Onboarding umfasst die Verwendung von PHT-Tokens für den Zugriff auf Authentifizierungsdienste. Sowohl ein Mediziner als auch ein Allgemeinmediziner reichen medizinische Fälle beim Versicherungsanbieter ein, um Ansprüche zu beantragen. Das ursprüngliche Ziel umfasst zwei weitere Teilziele: die Überwachung des Gesundheitszustands durch den Smart-Hub-Agenten und die Aufrechterhaltung eines gesunden Lebensstils durch einen Gesundheitsspezialisten. Letzterer setzt das System ein, sofern er über Selbstvertrauen und die Fähigkeit verfügt, fachkundige Urteile zu fällen, und nicht von der Komplexität des Systems überfordert ist.

Das Ziel der Überwachung des Gesundheitszustands umfasst drei Teilziele: die Erstellung einer PHR aus den von zwei Einheiten, nämlich einer Smartwatch und einem Luftqualitätssensor zu Hause, gesammelten Daten; die halbautomatische Analyse der PHR; und die sichere gemeinsame Nutzung der PHR, die die Verarbeitung interoperabler Informationen gewährleistet. Die Sicherheit wird durch die Validierung von SBT gewährleistet, um das Eigentum an den gemeinsam genutzten Daten sicherzustellen. Die erstellten PHR können nahtlos integriert werden, was ihre Weitergabe an verschiedene Beteiligte ermöglicht. Nach der Erstellung wird die PHR in das über die Blockchain verteilte Hauptbuch eingefügt, wodurch sichergestellt wird, dass sie gemeinsam genutzt werden kann.

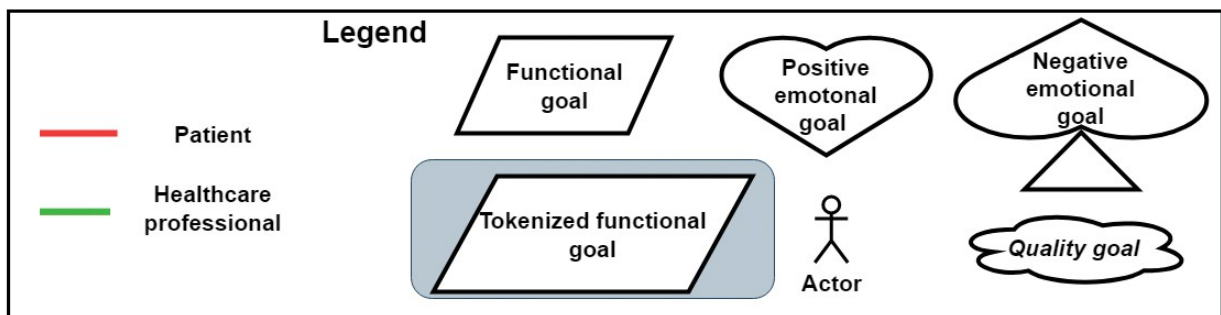
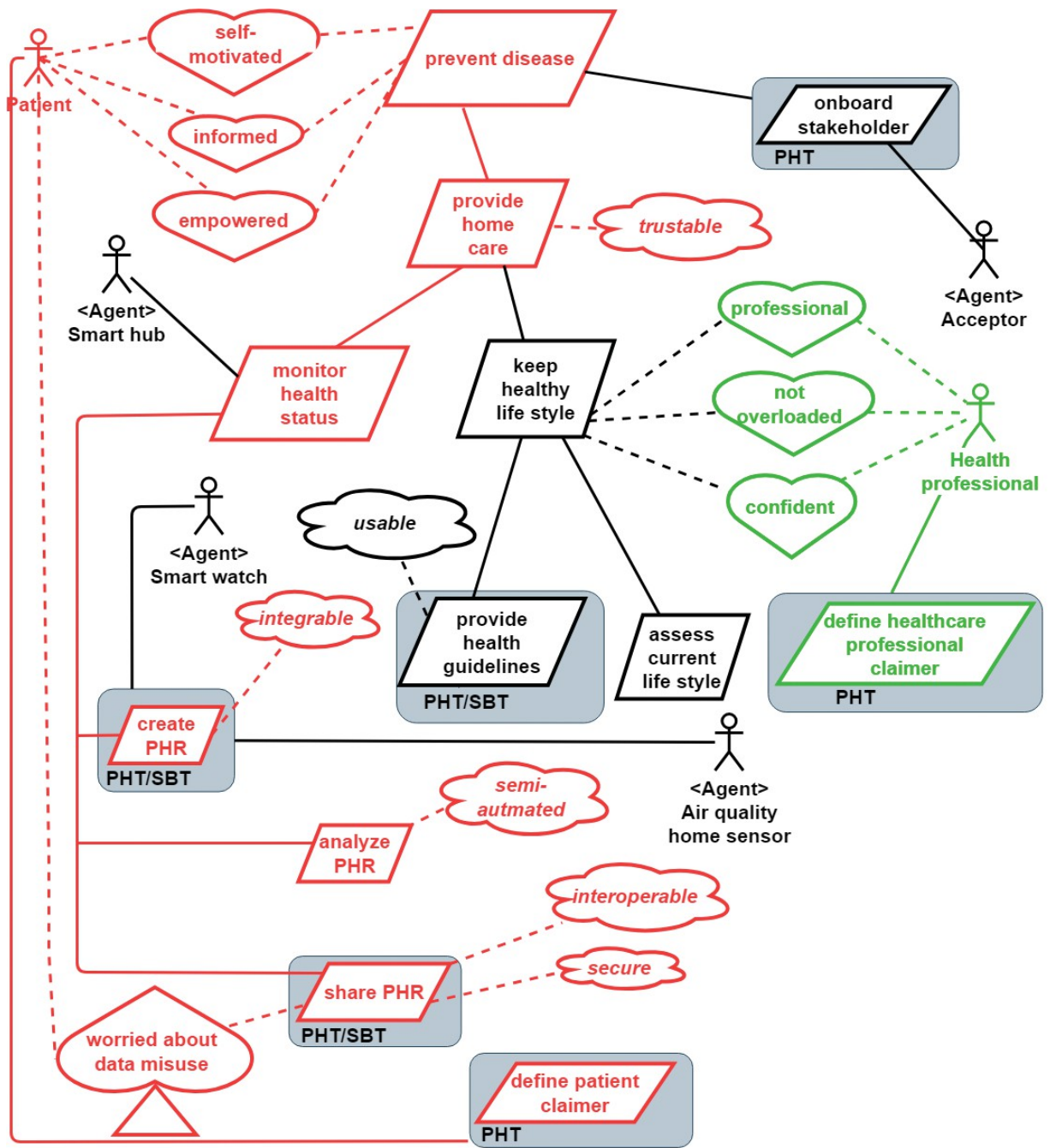


Abb. 4. Das Zielmodell für ein dezentrales, individuumzentriertes System. Ziele des Patienten und des medizinischen Personals.

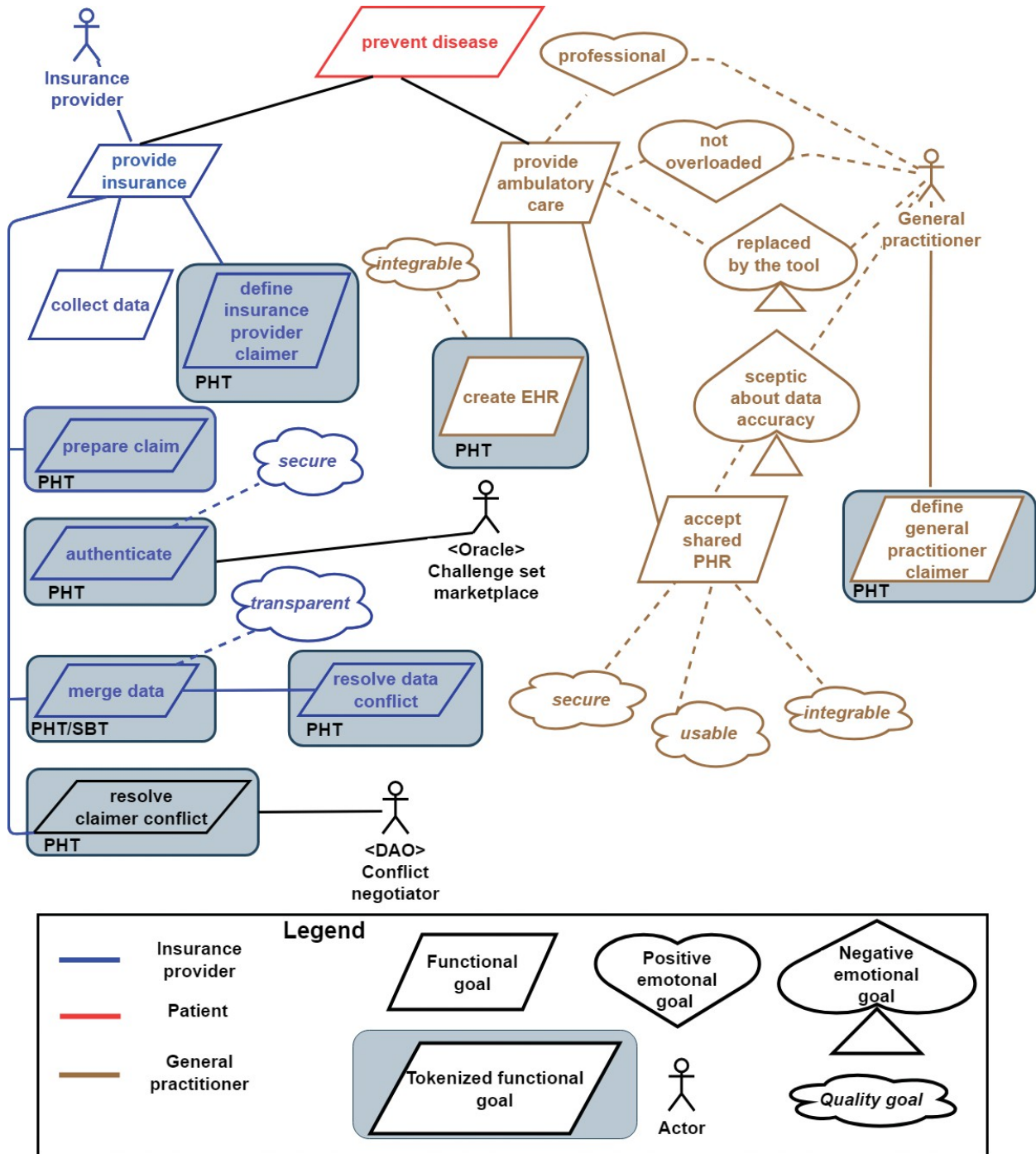


Abb. 5. Das Zielmodell für ein dezentrales, individualszentriertes System: Ziele des Versicherers und des Hausarztes.

mit anderen Akteuren und garantiert gleichzeitig seine Unveränderlichkeit. Das Ziel, einen gesunden Lebensstil zu erreichen, umfasst zwei spezifische Unterziele: die Bewertung des derzeitigen Lebensstils und das Anbieten von Gesundheitsempfehlungen. Leitlinien werden über die Blockchain mit dem Patienten geteilt und sollen nutzbar sein.

Das Ziel der ambulanten Versorgung umfasst die Einbindung eines Hausarztes, der über

Befürchtungen, durch Technologie ersetzt zu werden, und die Notwendigkeit, ein Gefühl der Professionalität zu bewahren, ohne eine übermäßige Arbeitsbelastung zu erfahren. Dieses Ziel ist in drei Unterziele unterteilt: die Einrichtung eines interoperablen EHR-Systems, die Einführung einer gemeinsamen PHR und die Verwaltung der medizinischen Diagnose. Die erstellte EHR wird auf einer Blockchain gespeichert, um für den Patienten auf sichere und unveränderliche Weise verfügbar zu sein. Hinzufügen von Daten

zur Blockchain erfordert PHT. Wenn ein Allgemeinmediziner zustimmt, PHR zu akzeptieren, hat er Vorbehalte hinsichtlich der Genauigkeit der gemeinsam genutzten Daten. Dieses Phänomen lässt sich auf das Potenzial für eine fehlerhafte Datengenerierung oder die Wahrscheinlichkeit zurückführen, dass eine andere Person das Eigentum an den bereitgestellten Daten beansprucht. Das MFSSIA-Protokoll unterstützt den authentifizierten und sicheren Weg zur Erzeugung medizinischer Daten und beseitigt das Misstrauen. Medizinische Daten werden häufig in verschiedenen Standards und Kontexten gespeichert, was zu semantischer Heterogenität führt. Der Prozess der Standardisierung von PHR- und EHR-Daten trägt dazu bei, diese Heterogenität zu vermeiden. Darüber hinaus vereinfacht diese Standardisierung die Verarbeitung von PHR- und EHR-Daten. Die sichere, integrierbare und nutzbare Akzeptanz von PHR ist zwingend erforderlich.

Das vorgesehene Versicherungsziel umfasst insgesamt neun Unterziele, nämlich die Datenerfassung, die Überprüfung, die Datenkonsolidierung, die Schadensvorbereitung, die Beilegung von Konflikten zwischen Antragstellern, die Definition des Anspruchs des Versicherers, die Definition des Anspruchs des Antragstellers, die Definition des Anspruchs des Gesundheitsdienstleisters und die Definition des Anspruchs des Hausarztes. Die gesammelten Daten werden bei der Antragsstellung verwendet und erfordern eine Authentifizierung der verschiedenen Datenquellen innerhalb des interorganisatorischen Rahmens, der auf dem dezentralen Protokoll MFSSIA basiert. Die Authentifizierung erfolgt durch die Nutzung des Challenge-Set-Marktplatzes, wobei das Blockchain-Orakel die Bereitstellung sicherer Challenge-Sets für die Benutzerauthentifizierung ermöglicht. Um einen Anspruch zusammenzustellen, muss der Versicherungsanbieter die Daten sorgfältig und transparent integrieren und mögliche Konflikte lösen. Beide Aktionen werden mit Smart Contracts durchgeführt. Da jeder einzelne Stakeholder Geschäftsregeln in seine jeweiligen funktionalen Ziele einbezieht (nämlich die Abgrenzung des Anspruchsberechtigten für Versicherungsanbieter, die Abgrenzung des Anspruchsberechtigten für Patienten, die Abgrenzung des Anspruchsberechtigten für Gesundheitsdienstleister und die Abgrenzung des Anspruchsberechtigten für Allgemeinmediziner), ist es für den Versicherungsanbieter unerlässlich, alle Konflikte zu lösen, die zwischen den Anspruchsberechtigten entstehen können. Wir schlagen die Verwendung von Smart Contracts vor, um die Konfliktlösung für die an den interorganisatorischen Prozessen beteiligten Akteure transparent und damit vertrauenswürdig zu machen. Der Zugriff auf die Smart Contracts erfolgt durch den Konfliktvermittler DAO, der die komplexe Logik der Konfliktlösungsalgorithmen implementiert.

Integrierte PHR- und EHR-Verarbeitung - Datenschutzkonflikte zwischen Gesundheitsdienstleistern und einzelnen Patienten

Im vorliegenden Fall wird davon ausgegangen, dass der Versicherungsanbieter aus drei Partnern besteht: einem Patienten, einem an ein Krankenhaus angeschlossenen Allgemeinmediziner und einem Angehörigen der Gesundheitsberufe, wie in Abbildung 1 dargestellt. Unterschiedliche Geschäfts

Für jeden Akteur werden unterschiedliche Geschäftsregeln berücksichtigt, die die Identität des Antragstellers und des Empfängers von Zahlungen des Versicherungsträgers unter bestimmten Umständen darstellen. Der Antragsteller in unserem Szenario wird durch die Messung des systolischen Blutdrucks bestimmt.

Eine Geschäftsregel besagt, dass der Patient als Antragsteller gilt, wenn sein systolischer Blutdruck unter 160 mmHg fällt; andernfalls ist der Antragsteller ein Allgemeinmediziner. In der gängigen Praxis wird ein systolischer Blutdruckwert von 120 mmHg als Normwert angesehen. Der Patient hat also keine Probleme mit dem Blutdruck. Die Entscheidung beruht auf der Annahme, dass der Patient, wenn er keine Komplikationen hat, eine lobenswerte Lebensweise an den Tag legt und die Kriterien erfüllt, um für den Versicherungsträger als Begünstigter in Frage zu kommen. Ein systolischer Blutdruck von 120 bis 160 mmHg ist problematisch und erfordert die Aufmerksamkeit und das Engagement des Patienten, um ihn wieder in den Normalbereich zu bringen. Folglich sieht sich der Patient auch als Antragsteller in diesem speziellen Datenbereich. Ein systolischer Blutdruck von mehr als 160 mmHg stellt eine gefährliche Situation dar und erfordert die Aufmerksamkeit eines Arztes. Folglich sieht der Patient den Hausarzt als Antragsteller an.

In der Verordnung über die Ausübung der Tätigkeit eines Hausarztes ist festgelegt, dass ein Patient, dessen systolischer Blutdruck unter 120 mmHg liegt, als Antragsteller eingestuft wird; überschreitet der systolische Blutdruck die Norm von 120 mmHg, übernimmt der Antragsteller die Rolle eines Allgemeinmediziners. In den Fällen, in denen der systolische Blutdruck des Patienten von der erwarteten Norm abweicht, überwacht der Hausarzt gewissenhaft den Zustand des Patienten und verabreicht anschließend die erforderlichen Medikamente und Interventionen entsprechend den vorläufigen Bewertungen. Infolgedessen sieht sich der Allgemeinmediziner als Antragsteller.

Abschließend hält sich die medizinische Fachkraft an eine Reihe von Geschäftsregeln, die Folgendes besagen: Liegt der systolische Blutdruck des Patienten unter 120 mmHg, wird der Antragsteller als Patient eingestuft; übersteigt der systolische Blutdruck dagegen 160 mmHg, übernimmt die medizinische Fachkraft die Rolle des Antragstellers. In Situationen, in denen der systolische Blutdruck zwischen 120 und 160 mmHg liegt, liegt es im Ermessen des medizinischen Personals, den Antragsteller ausdrücklich zu identifizieren.

Das Auftreten von Konflikten kann auf die internen Regelungen aller drei beteiligten Stellen zurückgeführt werden, wie in Abbildung 6 veranschaulicht. Diese Konflikte werden deutlich, wenn der systolische Blutdruck eines Patienten den vorgegebenen Schwellenwert von 120 mmHg überschreitet.

Funktionen, bei denen es zu Konflikten kommt

In diesem Abschnitt definieren wir die im Zielmodell in Abbildung 4 und Abbildung 5 dargestellten funktionalen Ziele, bei denen Konflikte auftreten. Um die Untersuchung zu vereinfachen, haben wir uns dafür entschieden, alle Konflikte, die im Zusammenhang mit qualitativen und emotionalen Zielen auftreten können, auszuschließen. Die Korrelation zwischen funktionalen Zielen und potenziellen Konflikten ist in Tabelle 1 dargestellt.

In unserem Fall werden zwei mögliche Konflikte während des interorganisationalen Versicherungsantragsprozesses betrachtet. Zunächst kann ein Datenkonflikt entstehen, wenn ein Versicherungsanbieter Daten aus verschiedenen Quellen sammelt und konsolidiert, darunter das PHR-System des Patienten, das EHR-System des Gesundheitsdienstleisters und die Aufzeichnungen der medizinischen Fachkräfte. Da jeder Beteiligte die Daten in unterschiedlichen Formaten und Standards verwaltet, besteht die Möglichkeit, dass die zusammengeführten Daten bei der Integration durch den Versicherungsträger nicht richtig übereinstimmen oder synchronisiert werden, was zu inkongruenten oder widersprüchlichen Daten führt.

Conflicts-Based Difference of Opinion on Rules Dissense

Patient	Hospital	Healthcare Professional
Patient	Hospital	Healthcare Professional 120 mmHg
Patient	Hospital	Healthcare Professional 160 mmHg
Patient	Hospital	Healthcare Professional

Abb. 6. Es hat sich gezeigt, dass die Umsetzung von Geschäftsregeln zu Konflikten im Verhalten führen kann.

Zweitens kann ein Konflikt bei der Definition des Antragstellers entstehen, wenn jeder Beteiligte den Versicherungsantragsteller auf der Grundlage seiner internen Geschäftsregeln und des Datenwerts, z. B. des Blutdruckwerts des Patienten, definiert. Wie in Abbildung 6 veranschaulicht, können die Regeln für das Vorschlagen eines Leistungsanspruchs durch den Patienten, den Leistungserbringer und das medizinische Fachpersonal je nach den Datenbedingungen unterschiedlich sein. Wenn beispielsweise der Blutdruck des Patienten zwischen 120 und 160 mmHg liegt, werden der Patient und der Leistungserbringer aufgrund ihrer unterschiedlichen Regeln verschiedene Antragsteller vorschlagen. Die Inkongruenz zwischen der Definition des Antragstellers führt zu einem Konflikt, der gelöst werden muss.

Prozesse, bei denen es zu Konflikten kommt

Die Definition eines Antragstellers für eine Versicherung beinhaltet den Abruf von Daten aus PHR- und EHR-Datenquellen, gefolgt von deren Integration und der Eliminierung irrelevanter Daten. Der Prozess zur Definition eines Antragstellers für einen Versicherungsträger ist in Abbildung 7 dargestellt. Zur Erleichterung des organisationsübergreifenden Prozesses der Antragstellerdefinition haben wir ihn unterteilt in

Tabelle 1. Funktionale Ziele, bei denen Konflikte auftreten.

Funktionales Ziel	Akteur	Konflikt
Daten sammeln	Versicherungsträger	Daten können unterschiedlich sein
Daten zusammenführen	Versicherungsträger	Daten können unterschiedlich sein
Kostenträger Antragsteller definieren	Kostenträger	Anspruchsteller kann unterschiedlich sein
Patientenantragsteller definieren	Patient	Antragsteller kann unterschiedlich sein
Antragsteller für Angehörige der Gesundheitsberufe definieren	Fachkraft im Gesundheitswesen	Antragsteller kann unterschiedlich sein
Definieren Sie Hausarzt-Antragsteller	Allgemeinmediziner	Antragsteller kann unterschiedlich sein

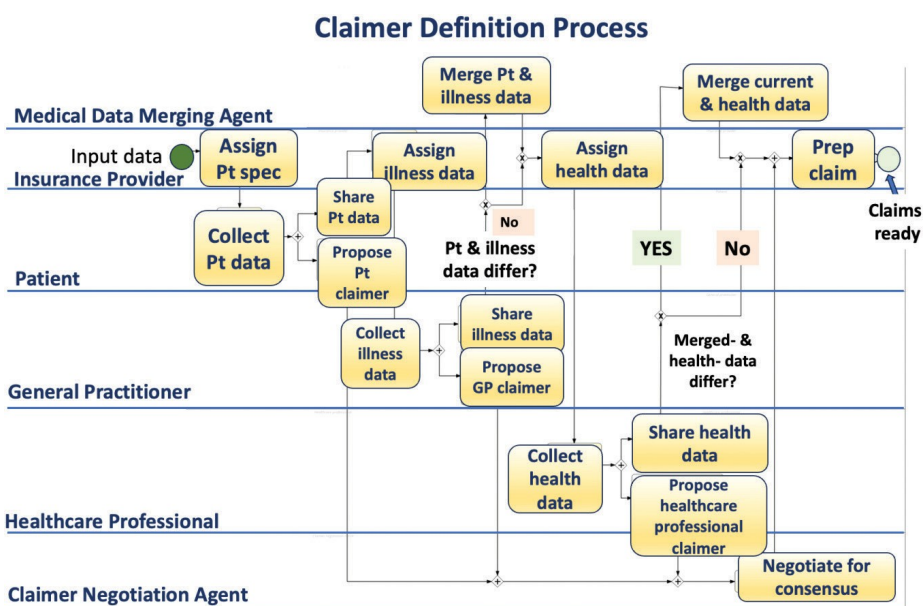


Abb. 7. Prozess zur Definition des Antragstellers für den Versicherungsträger.

drei Teilprozesse, nämlich den Entscheidungsprozess für Angehörige der Gesundheitsberufe, Gesundheitsdienstleister und Patienten. Zusätzlich werden wir diese drei internen Prozesse unter Verwendung der BPMN-Notation erläutern.

Abbildung 8 veranschaulicht den internen Entscheidungsprozess des Patienten, der sich an den zuvor beschriebenen Geschäftsregeln orientiert. Zu Beginn prüft der Patient, ob die von der Versicherungsgesellschaft angeforderten Daten in seinem PHR-Repository vorhanden sind. Falls die angeforderten Daten nicht vorhanden sind, nimmt der Patient die Blutdruckmessungen vor und speichert diese neuen Daten anschließend im PHR-Repository. Anschließend ruft der Patient die genannten Daten aus dem PHR-Repository ab und gibt sie an andere relevante Akteure weiter, die am interorganisatorischen Prozess beteiligt sind. Um den Antragsteller vorzuschlagen, wird schließlich der Blutdruckwert ermittelt. Wenn der Blutdruckwert gleich oder kleiner als 160 mmHg ist, macht der Patient sich selbst als Antragsteller geltend.

Umgekehrt wird bei einem Blutdruckwert von über 160 mmHg der Gesundheitsdienstleister als Antragsteller vorgeschlagen.

Abbildung 9 veranschaulicht den internen Entscheidungsfindungsprozess des Gesundheitsdienstleisters, z. B. eines Krankenhauses. Zunächst erwirbt der Gesundheitsdienstleister die Krankheitsdaten (EHR) von externen EHR-Systemen, die mit einem Krankenhaus verbunden sein können. Sobald die externen EHR-Daten vorliegen, werden sie in den Gesundheitsdatenstandard des Gesundheitsdienstleisters transformiert und im eigenen System gespeichert. Anschließend werden die importierten externen Daten an die anderen Teilnehmer des interorganisationalen Prozesses weitergegeben. Schließlich wird der Antrag des Gesundheitsdienstleisters auf der Grundlage der Geschäftsregeln formuliert, die im Abschnitt "Integrierte PHR- und EHR-Verarbeitung - Datenschutzkonflikte zwischen Gesundheitsdienstleistern und einzelnen Patienten" beschrieben sind. Dieser Vorschlag umfasst drei potenzielle Antragsteller: den Patienten, den Gesundheitsdienstleister und einen nicht näher definierten Antragsteller. Insbesondere, wenn der Blutdruckwert

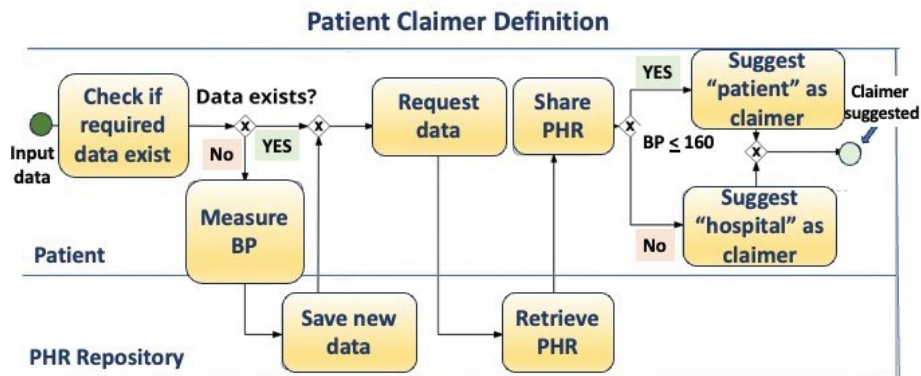


Abb. 8. Interner Entscheidungsprozess des Patienten-Claimers. BP: Blutdruck; DAO: Dezentrale Autonome Organisationen; PHR: Persönliche Gesundheitsakte.

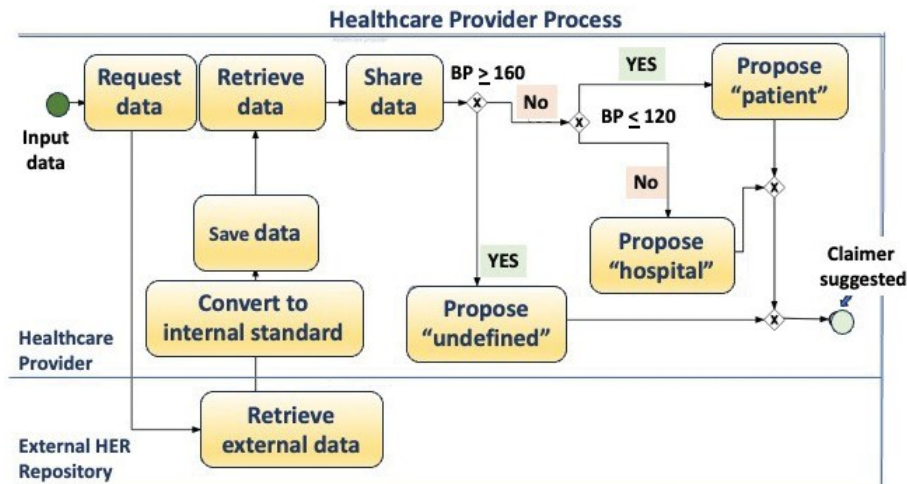


Abb. 9. Der interne Entscheidungsprozess von Gesundheitsdienstleistern in Bezug auf Antragsteller. BP: Blutdruck (in diesem Fall systolischer Blutdruck).

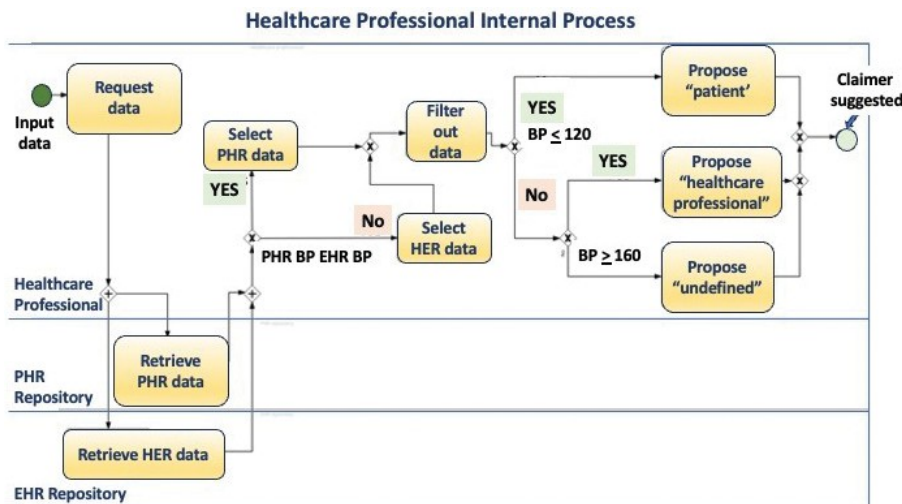


Abb. 10. Die Angehörigen der Gesundheitsberufe geben an, dass der interne Entscheidungsprozess in ihrer Praxis eine entscheidende Rolle spielt. BP: Blutdruck (hier: systolischer Blutdruck); EHR: elektronische Gesundheitsakte; PHR: persönliche Gesundheitsakte.

Wenn der systolische Blutdruck 120 mm Hg oder weniger beträgt, wird der Patient als Antragsteller vorgeschlagen. Fällt der Blutdruck in den Bereich zwischen 120 und 160 mm Hg, wird letztlich der Gesundheitsdienstleister als Antragsteller vorgeschlagen.

Abbildung 10 zeigt den internen Prozess der Entscheidungsfindung im Bereich der Angehörigen der Gesundheitsberufe. Die Diskrepanz zwischen den Entscheidungsprozessen von Patienten und Gesundheitsdienstleistern liegt vor allem in der Fähigkeit der Gesundheitsfachkräfte, sowohl auf EHR- als auch auf PHR-Daten zuzugreifen. Zunächst werden die Blutdruckmessungen gleichzeitig aus den Datenbanken der Patientenakten und der elektronischen Patientenakten entnommen. Nach der Eliminierung von Fremddaten schlägt die medizinische Fachkraft dann einen Antragsteller vor. Liegt der Blutdruck bei oder unter 120 mmHg, wird dem Patienten ein Antrag vorgelegt. Liegt der Blutdruck jedoch zwischen 120 und 160 mmHg, bleibt der Antragsteller unbestimmt. Liegt der Blutdruck über oder gleich 160 mmHg, stellt sich die medizinische Fachkraft selbst als Antragsteller vor. Die Integration von EHR und PHR basiert auf unserer früheren Forschung⁶⁶, während die Regelungen für den Antragstellervorschlag in Abbildung 6 erläutert werden.

Die Konfliktlösungstechniken bei der Abbildung des von Bpmn entworfenen E-Healthcare-Prozesses auf ein Blockchain-System

In diesem Abschnitt stellen wir die Konfliktlösungstechniken vor, die die automatische Lösung von Konflikten unterstützen, die in den interorganisatorischen Prozessen des elektronischen Gesundheitswesens auftreten. In unserem Beispielfall ergeben sich zwei mögliche Konflikte aus internen Geschäftsregeln oder Unterschieden bei den gesammelten medizinischen Daten.

In dieser Studie wird der Einsatz einer DAO als Konfliktlösungsmechanismus in dezentralen E-Health-Systemen vorgeschlagen. Der Konfliktlösungsprozess für medizinische Daten

Konsistenz der medizinischen Daten im Prozess des Versicherungsträgers ist in Abbildung 11 dargestellt. Zunächst sammelt der Versicherungsträger medizinische Daten aus drei Quellen, nämlich von Patienten, Gesundheitsdienstleistern und Hausärzten, um einen Antrag zu erstellen. Anschließend werden die gesammelten Daten einer Validierung unterzogen, um ihre Integrität zu prüfen. Im Anschluss an den Validierungsprozess genehmigt die DAO die Gültigkeit der Daten oder lehnt sie ab. Auf der Grundlage des endgültigen Validierungsergebnisses kann ein Antrag erstellt werden.

In Abbildung 12 wird näher erläutert, wie die Datenvalidierung aus einer einzelnen Datenquelle durchgeführt wird. Der exakte Prozess wird für alle drei Eigentümer der medizinischen Daten durchgeführt: Patient, Gesundheitsdienstleister und Allgemeinmediziner. Die DAO verwendet einen Konsensalgorithmus, der alle Knoten dazu veranlasst, die eingehenden Daten neu zu bewerten. Die Daten werden nur dann als gültig erachtet, wenn eine Mehrheit von mehr als 50 % der Knoten übereinstimmt, dass sie korrekt sind. Erreichen die Daten hingegen keine ausreichende Zustimmung, werden sie als manipuliert betrachtet und können folglich nicht für die Erstellung von Anträgen verwendet werden.

Schließlich wird der Prozess der Validierung medizinischer Daten für einen einzelnen Knoten in Abbildung 13 im Kontext der umfassenden Datenvalidierung durch die DAO dargestellt. Im Rahmen dieses Prozesses nimmt jeder Blockchain-Knoten, der mit der DAO verbunden ist, eine Prüfung der zu prüfenden medizinischen Daten vor. Der Knoten fordert bestimmte medizinische Daten, wie z. B. einen Blutdruckmesswert, von der ursprünglichen Datenquelle, z. B. dem PHR-System des Patienten, an. Der Knoten vergleicht dann die Daten von der Quelle mit den Daten, die auf der Blockchain validiert werden. Wenn die Daten genau übereinstimmen, betrachtet der Knoten sie als gültig und bestätigt dies durch seine Stimme im Konsensalgorithmus. Stimmen die Daten nicht überein, entsteht eine Diskrepanz zwischen der ursprünglichen Datenquelle und den in der Blockchain gespeicherten Daten. Unter solchen

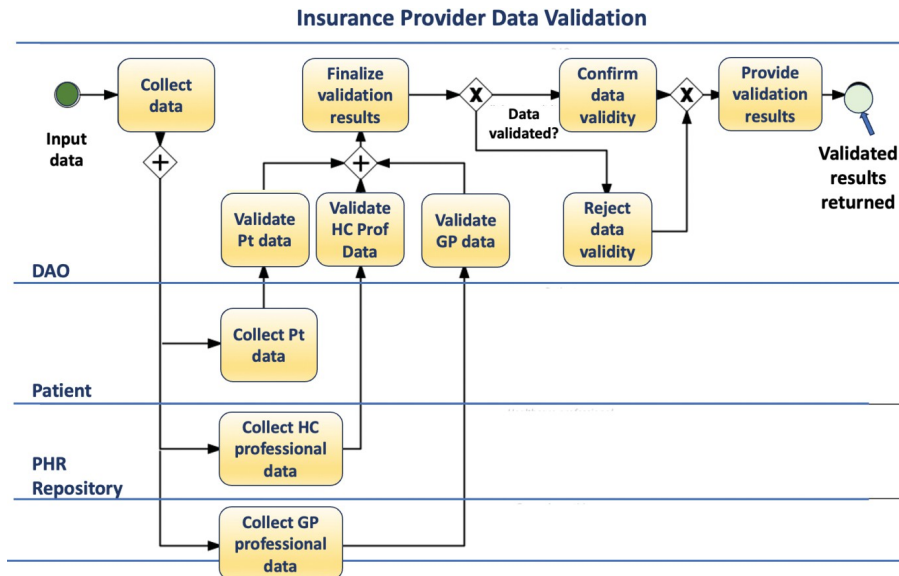


Abb. 11. Prozess zur Lösung von Datenkonflikten bei Versicherungsanbietern. DAO: Dezentrale Autonome Organisationen; Pt: Patient; GP: Allgemeinmediziner; HC: Gesundheitswesen.

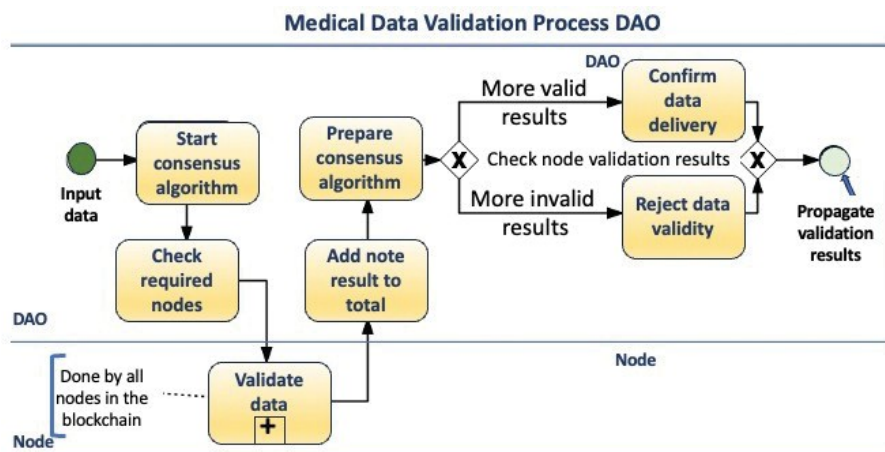


Abb. 12. DAO-Datenvalidierungsprozess. DAO: Dezentralisierte autonome Organisationen.

Unter bestimmten Umständen hält der Knoten die Daten entweder für ungültig oder manipuliert und verwirft sie folglich durch einen Abstimmungsprozess, der sich gegen ihre Gültigkeit innerhalb des Konsensalgorithmus richtet.

Dadurch, dass jeder Knoten die Daten direkt von der Quelle aus überprüft, können Probleme mit Datenmanipulationen erkannt werden, selbst wenn eine Teilmenge der Knoten böswillig ist. Der Konsensalgorithmus verifiziert gültige Daten, wenn die Validierungsprüfungen der meisten Knoten erfolgreich sind. Diese redundante Überprüfung durch jeden Knoten bietet eine größere Sicherheit und Genauigkeit bei der Erkennung von Datenmanipulationen als ein zentraler Überprüfer.

In der von uns vorgeschlagenen dezentralen Architektur nehmen die einzelnen Einheiten, die als "Knoten" bezeichnet werden, an einem Entscheidungsprozess teil, um die Richtigkeit und Integrität der Daten zu überprüfen. Ein solcher Prozess wird gesteuert durch

eine DAO, die als Konfliktlöser dient. Jeder Knoten gibt eine Stimme ab, um die Gültigkeit der fraglichen Daten entweder zu bestätigen oder abzulehnen. Sobald alle Stimmen gesammelt sind, wird eine endgültige Entscheidung auf der Grundlage des Mehrheitskonsenses der Knoten getroffen. Wenn die Mehrheit der Knoten einen Konsens über die Gültigkeit der Daten erzielt, werden diese als akzeptabel angesehen, andernfalls werden sie als inakzeptabel eingestuft und abgelehnt. Dieser demo-kratische Ansatz gewährleistet einen robusteren und transparenteren Validierungsprozess.

Bewertung und Diskussion

In diesem Abschnitt wird die Evaluierung dieser Arbeit unter Verwendung des Multi-Methoden-Evaluierungsansatzes, den DSR zugrunde legt, dargelegt. Zunächst führen wir eine formale Evaluierung mit CPN und weiteren

die Diskussion der CPN-Evaluierungsergebnisse und die Implikationen der Hauptergebnisse dieser Arbeit mit anderer verwandter Literatur. Anschließend stellen wir einen PoC-Prototyp vor, der den vom CPN evaluierten Arbeitsablauf implementiert.

Zunächst bewerten wir den Konfliktlösungsprozess mit der CPN-Modellierung. Der Konfliktlösungsprozess im CPN-Modell hat mehrere Ebenen. Die oberste Ebene sind die internen Prozesse der Beteiligten. Dann wird die Bewertung des gegebenen CPN vorgestellt, gefolgt von der PoC-Prototyp-Implementierung. Abschließend werden die aktuellen Ergebnisse mit ähnlichen Forschungsarbeiten verglichen und diskutiert.

Formale Bewertung des CPN für den Konfliktlösungsprozess bei der Definition von Ansprüchen

Das klassische Petri-Netz ist ein gerichteter zweiseitiger Graph mit zwei Knotentypen, den Stellen und den Übergängen. Die Knoten sind über gerichtete Bögen miteinander verbunden. Verbindungen zwischen zwei Knoten desselben Typs sind nicht erlaubt. Stellen werden durch Kreise und Übergänge durch Rechtecke dargestellt.⁶⁷

Um die Charakterisierung des Konfliktlösungsprozesses durch den Antragsteller zu bewerten, schlagen wir ein strukturiertes CPN-Modell⁶⁸ zur Identifizierung und Behebung potenzieller Designmängel, fehlender Spezifikationen sowie von Sicherheits- und Datenschutzproblemen vor.

Die vollständige Beschreibung des CPN-Modells ist im technischen Bericht zu finden.⁶⁸ Unser Bewertungsmodell konzentriert sich auf einen dezentralen Datenaustauschprozess und lässt alle in Abbildung 4 und Abbildung 5 definierten funktionalen Ziele aus.

Diese Ziele beziehen sich auf das Auftreten von Konflikten und deren Beilegung. Die vom CPN-Modell abgedeckten Ziele sind:

- Antragsteller für die Versicherung vorschlagen
- Daten sammeln
- PHR teilen
- Datenkonflikt auflösen
- Lösen des Konflikts mit dem Antragsteller.

Wir verwenden die Formalisierung des eSourcing-Frameworks,⁶⁹ in dem Workflow-Netze (WF-Netze) enthalten sind. Auf diese Weise werden die CPN-Modelle für die internen Prozesse der Beteiligten in einer Reihe angeordnet, so dass der Kontrollfluss der eSourcing-Formalisierung ähnelt. Das WF-Netz definiert das dynamische Verhalten eines einzelnen Falles in Isolation.

WF-Netze sind eine Formalisierung zur Beschreibung von Prozessmodellen in parallelen und verteilten Systemen.⁷⁰ Die Forschung⁷¹ beschreibt ein WF-Netz als ein Petri-Netz mit einem 3-Tupel $N = (P, T, F)$, wobei P und T zwei disjunkte und endliche Mengen sind, die jeweils Orte (Kreise visualisieren sie) und Übergänge (Rechtecke stellen sie dar) genannt werden.

giles stellen s i e dar), und $F \subseteq (P \times T) \cup (T \times P)$ ist eine Menge von Flussrelationen in N . Die Menge F ist eine Teilmenge von die Vereinigung des kartesischen Produkts von P und T mit dem kartesischen Produkt von T und P . $P \times T$ steht für das kartesische Produkt der Mengen P und T . Das kartesische Produkt besteht aus allen möglichen geordneten Paaren, bei denen das erste Element aus der Menge P und das zweite Element aus der Menge T stammt.

Abbildung 14 zeigt ein WF-Netz mit einer eindeutigen Start- und einer eindeutigen Endstelle und einem Token an der Startstelle (alle anderen Stellen sind leer). Alle Knoten führen von der Start- zur Endstelle, so dass sich nach Abschluss des Enactments nur ein Token an der eindeutigen Endstelle befindet und alle anderen Stellen leer sind.¹¹ Es ist zu beachten, dass ein WF-Netz das dynamische Verhalten eines einzelnen Falls spezifiziert

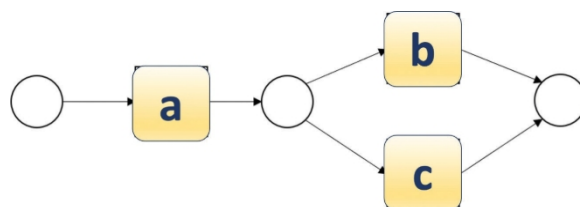


Abb. 14. Beispiel für ein Workflow-Netz.⁷²

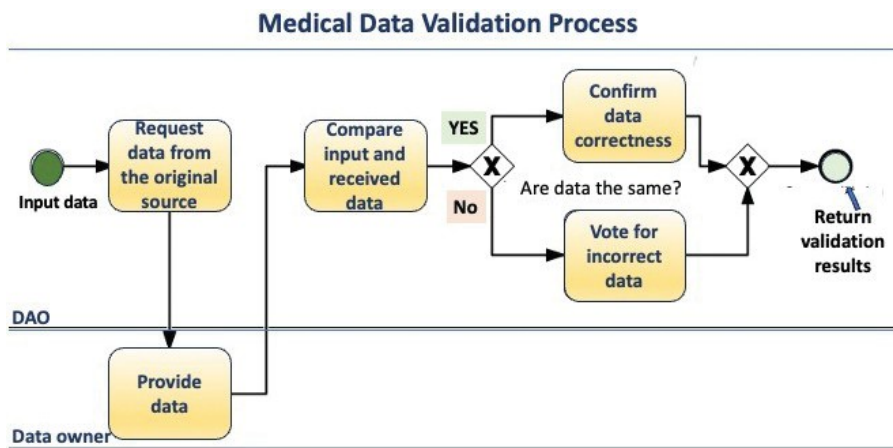


Abb. 13. Prozess der Validierung von Knotendaten. DAO: Dezentralisierte autonome Organisationen.

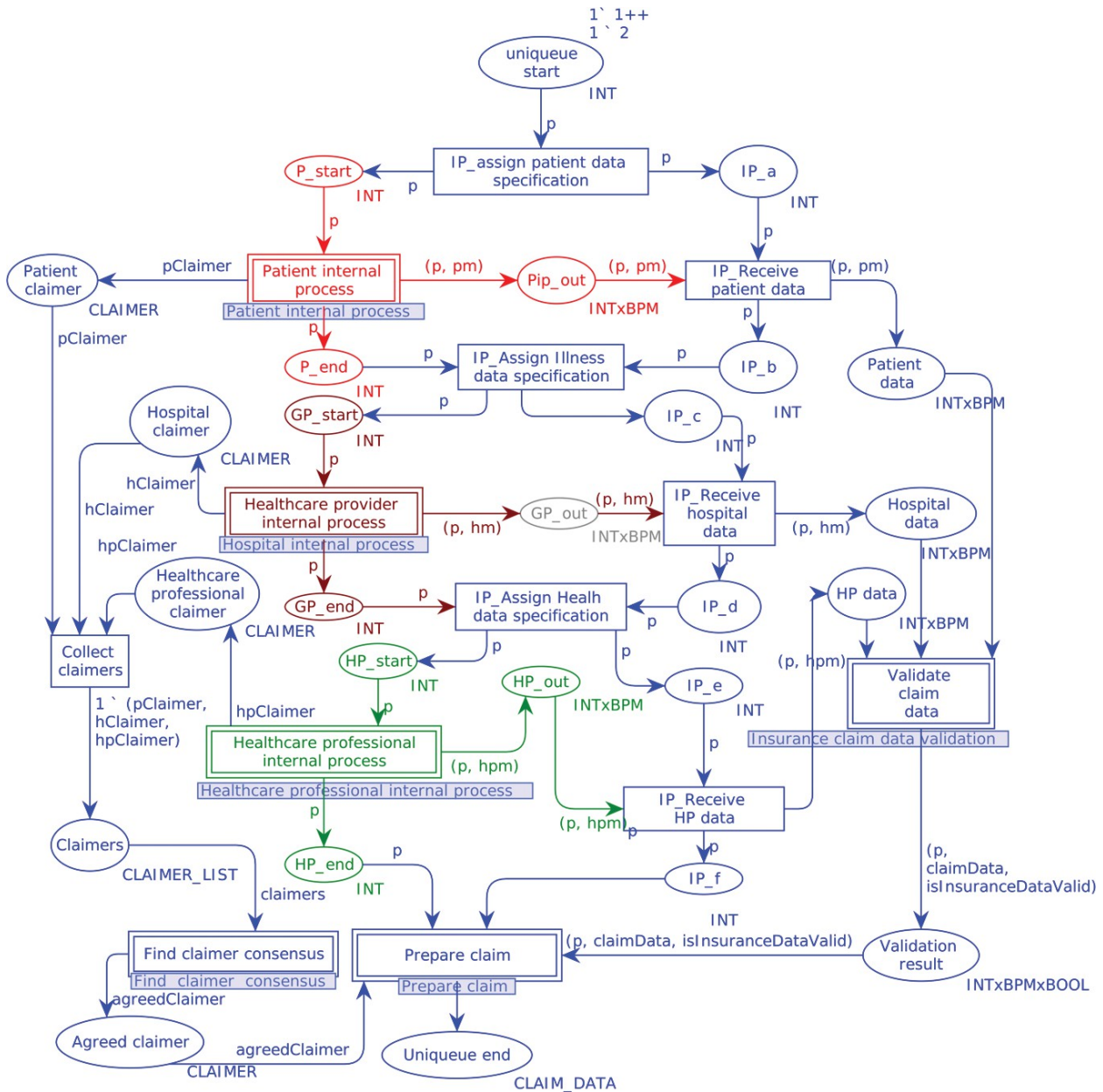


Abb. 15. Die externe Schicht des CPN-Modells definiert den interorganisatorischen Prozess. CPN: Farbige Petri-Netze.

in Isolation. Das bedeutet, dass jeder Arbeitsschritt für einen bestimmten Fall ausgeführt wird, der auch als Workflow-Instanz bezeichnet wird.⁶⁷

Formalisierte Einrichtung auf oberster Ebene

Abbildung 15 veranschaulicht die verfahrenstechnischen Aspekte bei der Formulierung eines Anspruchs, der mehrere Organisationseinheiten umfasst. Um einen medizinischen Anspruch zusammenzustellen, beschafft der Versicherungsträger Gesundheitsdaten aus verschiedenen Quellen, wie z. B. aus Patientenakten, Systemen von Gesundheitsdienstleistern und Systemen, die von Fachärzten genutzt werden. Die internen Prozesse der Datenerfassung und Falldefinition beinhalten die Interaktion mit den dezentralen Systemen der Beteiligten.

Systemen. Wir verwenden verschiedene Farben für interne Prozesse, um einen interorganisatorischen Prozess besser zu visualisieren. Der interne Prozess des Patienten wird in rot dargestellt, der des Leistungserbringers in braun und der der medizinischen Fachkraft in grün.

Unser CPN-Modell basiert auf den BPMN-Prozessen, die weiter oben in diesem Artikel definiert wurden. Der gesamte Prozess der Antragstellerdefinition des Versicherungsanbieters ist von Abbildung 10 abgeleitet. Die CPN-Schichten, die die Prozesse definieren, die die interne Geschäftslogik der Antragstellerdefinition kapseln, basieren auf den BPMN-Prozessen. Die Modellierung der internen Schadenregulierungsprozesse ermöglicht das Auftreten von Konflikten und die Simulation bei der Evaluierung des CPN-Modells. Die Abbildung zwischen BPMN-Diagrammen und CPN-Modellebenen der Patienten-

Fachkräften und Leistungserbringern ist in Tabelle 2 dargestellt.

Der Prozess der Antragserstellung beginnt an einem eindeutigen Startort mit zwei Token, die unabhängige Prozessbezeichner beschreiben. Das Modelldesign unterstützt mehrere parallele Prozessausführungen, wenn für jeden Ort Prozesskennungen angegeben werden. Alle vom Versicherungsträger durchgeführten Übergänge sind blau gekennzeichnet und beginnen mit dem Präfix IP_. Anschließend wird der Übergang IP_Zuweisung von Patientendaten eingeleitet, wodurch der interne Prozess des Patienten beginnt. Der interne Prozess des Patienten hat zwei Ausgänge: die Blutdruckmessung und den Antrag des Antragstellers. Der gleiche Arbeitsablauf gilt sowohl für Leistungserbringer als auch für Angehörige der Heilberufe. Die Definition des Antragstellers basiert auf den in Abbildung 6 beschriebenen internen Regeln.

Wenn alle drei internen Prozesse ausgeführt werden, wird der Übergang Antragsteller sammeln mit drei Eingaben ausgelöst, die den von jedem Beteiligten vorgeschlagenen Antragsteller definieren. Der Übergang Antragsteller-Konsens finden verarbeitet alle drei vorgeschlagenen Antragsteller und wählt einen auf der Grundlage des Konsensalgorithmus aus.

Bevor ein Antrag erstellt werden kann, läuft parallel zur Antragstellerdefinition ein weiterer Prozess ab: die Validierung der erfassten Blutdruckmessungen. Dieser Prozess prüft die potenzielle Kompromissfähigkeit der Daten und löst anschließend alle Diskrepanzen, die im Falle von Datenabweichungen auftreten können. Wenn die Konsensalgorithmen mit dem Antragsteller und den Blutdruckmessungen übereinstimmen, erfolgt die Überleitung des vorbereiteten Antrags.

Interorganisationale Arbeitsabläufe der Beteiligten bei der Verarbeitung integrierter EHRs und PHRs

Um die Arbeitsabläufe der verschiedenen Akteure darzustellen, verwenden wir Substitutionenübergänge, die Teilnetze beinhalten, die die mit einem Übergang verbundenen Aktivitäten näher erläutern. Das Teilnetz, das mit einem Übergang verknüpft ist, wird im akademischen Diskurs üblicherweise als Unterseite bezeichnet. Die Verwendung des CPN-Formalismus ermöglicht die hierarchische Anordnung von Unterseiten in einem unbestimmten Ausmaß und erleichtert so die Darstellung von Systembeschreibungen auf verschiedenen Ebenen der Komplexität.⁷³

Um das kollaborative Szenario zu verbessern, erweitern wir es um eine Simulation, die CPN verwendet. Zusätzlich integrieren wir das Konfliktszenario in das quantitativ simulierbare Modell. Um das gesamte CPN-Modell zu organisieren,⁷⁴ unterteilen wir es in mehrere Unterseiten, wie in Tabelle 3 dargestellt.

Abbildung 16 zeigt einen Screenshot aus den CPN-Tools, der die hierarchische Anordnung der Unterseiten innerhalb des Entwurfsmodells darstellt. Diese Unterseiten, die der

⁷³<https://goo.by/JOQJ8>

Tabelle 2. Interne Claimer-Definitionsprozessabbildung von BPMN Diagrammen auf CPN-Modellschichten.

BPMN-Prozess	CPN-Schicht
Patienteninterner Entscheidungsprozess des Antragstellers (Abbildung 8)	Interner Prozess des Patienten
Interner Entscheidungsprozess Leistungserbringer - Antragsteller (Abbildung 9)	Interner Prozess des Leistungserbringers im Gesundheitswesen
Interner Entscheidungsprozess des Antragstellers aus dem Gesundheitswesen (Abbildung 10)	Interner Prozess für medizinische Fachkräfte

BPMN: Geschäftsprozessmodell und Notation; CPN: Farbige Petri-Netze.

als wiederverwendbare Komponenten tragen dazu bei, das komplizierte Modell verständlicher zu machen. Innerhalb dieses Rahmens übernimmt die Hauptseite, die als "Extern" bezeichnet wird, die Rolle, das interorganisatorische Protokoll für die Vorbereitung eines Versicherungsfalls zu beschreiben. Die internen Verfahren der verschiedenen Beteiligten, d. h. der interne Prozess des Patienten, der interne Prozess des Krankenhauses und der interne Prozess des medizinischen Fachpersonals, sind auf separaten Unterseiten zusammengefasst. Die Konfliktlösung erfolgt auf einer höheren Ebene des Prozesses, nämlich auf den Unterseiten, die der Validierung der Versicherungsdaten und der Erzielung eines Konsenses zwischen den Antragstellern gewidmet sind.

Bewertung des CPN-Modells

Wir bewerten unser Modell mit zwei verschiedenen Ansätzen. Zunächst bewerten wir das ursprüngliche Modell durch Simulation in den CPN Tools, wobei wir sicherstellen, dass alle anfänglichen Token zu einem eindeutigen Endzustand des Modells führen. Angesichts der Komplexität des bereitgestellten CPN-Modells führen wir eine Zustandsraumanalyse für jede einzelne Unterseite durch. Wenn die Seite eine der Unterseiten enthält, imitieren wir deren Ausgabe. Bei dieser Imitation wird die tatsächliche Ausführung der Unterseite durch ein einzelnes Element ersetzt, das konstante Daten erzeugt. Auf diese Weise wird die Integrität des Ablaufs der Hauptseite beibehalten und gleichzeitig die Komplexität der Zustandsraumanalyse verringert. Die vorgegebenen Werte werden auf der Grundlage der möglichen Ergebnisse der Unterseite festgelegt. Während der gesamten Zustandsraumanalyse werden alle erreichbaren Zustände und Zustandsänderungen des CPN-Modells in Form eines gerichteten Graphen berechnet und dargestellt. Der Graph stellt Zustände als Knoten und auftretende Ereignisse als Bögen dar. Das Hauptziel der Zustandsraumanalyse besteht darin, das Verhalten des Systems zu beschreiben und zu überprüfen, dass es keine Deadlocks gibt, dass ein bestimmter Zustand immer erreichbar ist und dass ein bestimmter Dienst immer geliefert wird.⁷¹

In dem Bericht über den Zustandsraum werden sowohl die Heimat- als auch die Liveness-Eigenschaften erläutert. Erstere beziehen sich auf eine bestimmte Heimatmarkierung, die von jeder erreichbaren Markierung aus zugänglich ist. In unserem Szenario wird jeder Prozess, der mit einer Unterseite verbunden ist, letztendlich seinen Endzustand erreichen. Auf der anderen Seite beschreiben die Liveness-Eigenschaften Markierungen ohne aktive Bindungselemente. Eine Markierung ohne Aktivität kann sowohl eine tote Markierung sein

Tabelle 3. Unterseiten in der Hierarchie des CPN-Modells.

Unterseite	Bedeutung
Patienteninterner Prozess	Patientendatenerfassungs- und Antragstellerdefinitionsprozesse
Krankenhausinterner Prozess	Hausärztliche Datenerfassungs- und Antragstellerdefinitionsprozesse
Interner Prozess für Angehörige der Gesundheitsberufe	Datenerfassungs- und Antragstellerdefinitionsprozesse für Angehörige der Gesundheitsberufe
Datenverfälschung	Datenmanipulationsprozess, der während der Datenerfassung stattfindet
Sammeln von Daten	Prozess der Datenerfassung
Definition des Patientenantragstellers	Prozess der Definition des Patientenantragstellers
Definition des Antragstellers für medizinisches Fachpersonal	Prozess zur Definition von medizinischen Fachkräften als Antragsteller
Definieren von Krankenhausantragstellern	Prozess zur Definition von Krankenhausantragstellern
Validierung der Daten von Versicherungsansprüchen	Prozess der Validierung aller gesammelten Daten von verschiedenen Beteiligten
Datenvalidierung	Prozess der Validierung der Blutdruckmessung durch mehrere Knotenpunkte
Knotenpunkt-Validierung	Prozess der Validierung der Blutdruckmessung durch einen einzelnen Knotenpunkt
Konsens der Antragsteller finden	Endgültiger Antragsteller-Konsensprozess

CPN: Farbige Petri-Netze.

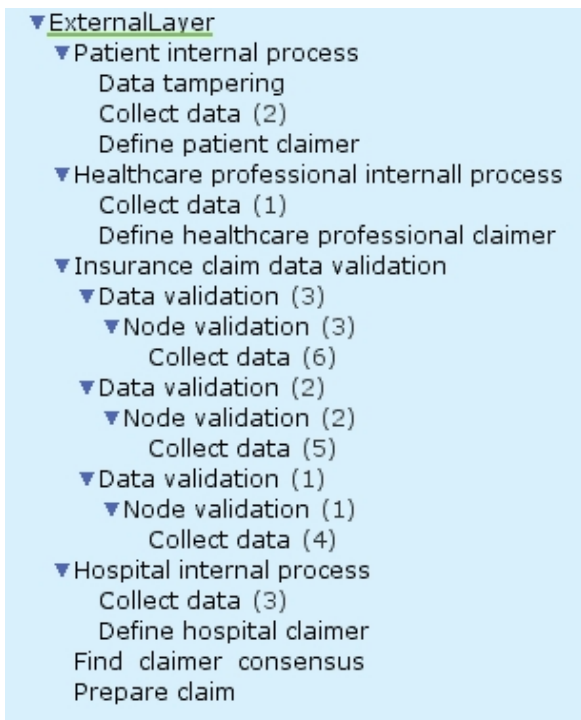


Abb. 16. Hierarchie der CPN-Modellseite. CPN: Farbige Petri-Netze.

und eine Heimatmarkierung gleichzeitig, da jede Markierung von sich aus über eine triviale Ereignisfolge der Länge Null erreicht werden kann. Im Anschluss daran werden im Zustandsraumbericht die lebenden Übergänge beschrieben. In einem akademischen Kontext gilt ein Übergang als live, wenn es dauerhaft möglich ist, eine Folge von Ereignissen zu identifizieren, die den Übergang von jeder erreichbaren Markierung aus einschließen. Der Zustandsraumbericht enthält eine Darstellung inaktiver Übergänge. Ein Übergang wird als inaktiv eingestuft, wenn er entweder aktiviert oder unerreichbar ist. Diese Übergänge

die Funktionalität eines Modells zu beschreiben, das niemals ausgeführt werden kann.⁷⁴

Alle Berichte, in denen der Zustandsraum analysiert wird, basieren auf jeder Unterseite des vorgestellten CPN-Modells, wie in den entsprechenden Tabellen weiter unten angegeben. Die vollständigen Dateien des Berichts über die Zustandsraumanalyse können online abgerufen werden.³

Aus den in Tabelle 4 dargestellten Ergebnissen geht hervor, dass dem Prozess der Datenerhebung Schleifen inhärent sind. Der Datenspeicher enthält Informationen über verschiedene Prozesse, und der Datenerfassungsprozess fährt fort, Daten abzurufen, bis er Informationen findet, die mit dem laufenden Prozess verbunden sind. Alle Unterseiten in unserem Prozess enthalten keine toten und lebenden Übergänge, was darauf hindeutet, dass es keine ungenutzten Komponenten gibt. Bemerkenswert ist, dass der Zustand aller Unterseiten mit dem der Home- und Dead-Markierungen übereinstimmt.

Proof-of-Concept-Prototyp-Implementierung für den laufenden Fall In dieser Studie wird die Implementierung eines Prototyps für den Prozess des elektronischen Austauschs von Gesundheitsdaten⁷⁵ vorgestellt, der im Rahmen von Ref. 76. In unserem spezifischen Kontext schlagen wir die Verwendung von Polygon⁷⁷ Smart Contracts (SCs) für das System der Versicherungsanbieter vor. Gleichzeitig werden Ethereum SCs für die Systeme von Patienten, Krankenhäusern und Gesundheitsfachkräften empfohlen. Das Polygon-Netzwerk basiert auf einer Blockchain-Architektur mit hohem Durchsatz, bei der jeder Kontrollpunkt eine Gruppe von Blockproduzenten auswählt, um einen Konsens zu erreichen. Die Validierung der Blöcke erfolgt über eine PoS-Schicht, die auch das Ethereum-Mainnet regelmäßig mit den von den Blockproduzenten bereitgestellten Beweisen aktualisiert. Um die Skalierbarkeit zu verbessern und die Interoperabilität zwischen verschiedenen Blockchain-basierten Systemen zu ermöglichen, setzen wir Polkadot⁷⁸ ein, das eine sichere und vertrauensfreie Kommunikation zwischen spezialisierten Blockchains ermöglicht.

³<https://goo.by/QaISC>

Tabelle 4. Ergebnisse der Zustandsraumanalyse für die Unterseiten des CPN-Modells.

Unterseite	Schleifen	Home Markierung	Tote Markierung	Tote Übergänge	Lebendige Übergänge
Patienteninterner Prozess	Nein	Ja	Ja	Nein	Nein
Internes Verfahren für Angehörige der Gesundheitsberufe	Nein	Ja	Ja	Nein	Nein
Krankenhausinterner Prozess	Nein	Ja	Ja	Nein	Nein
Patientenantragsteller definieren	Nein	Ja	Ja	Nein	Nein
Antragsteller aus dem Gesundheitswesen definieren	Nein	Ja	Ja	Nein	Nein
Krankenhausantragsteller definieren	Nein	Ja	Ja	Nein	Nein
Konsens der Antragsteller finden	Nein	Ja	Ja	Nein	Nein
Daten sammeln	Ja	Ja	Ja	Nein	Nein
Datenverfälschung	Nein	Nein	Ja	Nein	Nein
Datenüberprüfung	Nein	Ja	Ja	Nein	Nein
Knoten-Validierung	Nein	Ja	Ja	Nein	Nein
Externe Schicht	Nein	Ja	Ja	Nein	Nein
Anspruch vorbereiten	Nein	Ja	Ja	Nein	Nein

CPN: Farbige Petri-Netze.

In der dezentralen Webumgebung, die durch die Polkadot-Grundschrift ermöglicht wird, üben die Nutzer die Autorität über ihre Daten aus. Dieser Prototyp umfasst drei primäre blockchainbasierte Elemente. Insbesondere umfasst er zwei verschiedene Anwendungen für die Eingabe von medizinischen Daten, nämlich die des Patienten und des Arztes. Darüber hinaus enthält er eine Anwendung, die das interorganisatorische Verfahren mit dem Versicherungsträger durchführt, sowie einen DAO-Smart-Contract, der im Falle von Konflikten einen Datenabgleich vornimmt und zuverlässige Daten liefert. Der betrachtete PoC-Prototyp konzentriert sich auf das Szenario, in dem der Patient und der Arzt die Blutdruckwerte eingeben.

Abbildung 17 zeigt einen Screenshot der Benutzeroberfläche der Patientenapplikation, die explizit die Eingabe von Blutdruckmessungen zeigt. Diese Anwendung ist in die Metamask-Brieftasche integriert und ermöglicht die gemeinsame Nutzung der eingegebenen Daten über einen intelligenten Vertrag. Insbesondere beinhaltet die Anwendung die Bereitstellung eines Smart Contracts auf der Ethereum-Blockchain.

Abbildung 18 stellt einen Konflikt dar, der bei der Datenerfassung auftritt. Das dargestellte Szenario zeigt eine Diskrepanz zwischen den vom Patienten aufgezeichneten Blutdruckwerten und den vom Arzt dokumentierten Werten. In diesem Fall werden die Daten an eine DAO weitergeleitet, die die Aufgabe übernimmt, die Daten zu validieren und eventuelle Konflikte zu lösen.

Der interorganisationale Prozess wird mit der Polkadot-Parachain implementiert, die eine blockchain-übergreifende Kommunikation ermöglicht. Wir implementieren ein anwendungsspezifisches Blockchain-basiertes Modul mit dem Substrate-Framework.⁷⁹ Die Anwendung des Versicherungsanbieters läuft als lokaler Backend-Knoten von Substrate.

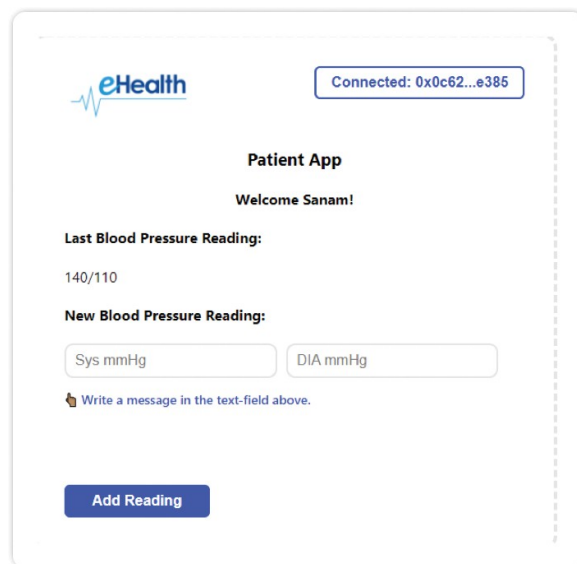


Abb. 17. Screenshot der Anwendung eines Patienten.

Erörterung von Forschungsimplicationen für ähnliche Arbeiten

In dieser Forschungsarbeit wird vorgeschlagen, dass Blockchain eine autonome Konfliktlösung auf transparente Weise ohne einen einzigen Vertrauenspunkt ermöglicht. Außerdem unterstützen Blockchain- und Smart-Contract-Technologien personalisierte E-Health-Dienste, die mehrere Akteure einbeziehen und gleichzeitig das Eigentum des Einzelnen an den Gesundheitsdaten sicherstellen. Das Aufkommen der M2X-Wirtschaft und nicht-menschlicher Agenten in den interorganisationalen Prozessen erfordert neue Authentifizierungsmethoden, die auf dem Multifaktor-Challenge-Set-Mechanismus basieren. Ein solcher Ansatz ermöglicht neue interorganisatorische Prozesse in Situationen, in denen es an Vertrauen zwischen den Beteiligten mangelt. Die Evaluierung mit CPN zeigt, dass ein solcher Prozess am Beispiel einer dezentralen E-Krankenversicherung machbar sein kann. Dennoch haben wir keinen empirischen in vivo Beweis dafür, dass dies möglich ist.

```

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

```

Abb. 18. Bildschirmfoto der Datenerfassung durch den Versicherer.

möglich; stattdessen erbringt diese Arbeit den in vitro Machbarkeitsnachweis. Die Möglichkeit der autonomen Konfliktlösung im dezentralen E-Health ermöglicht die wertvolle Nutzung der Gesundheitsdaten einer Person über verschiedene Branchen hinweg auf eine vertrauenswürdige und transparente Weise. Schließlich zeigt die Implementierung des PoC-Prototyps, dass der laufende Fall mit den derzeit modernsten dezentralen Technologien implementiert werden kann.

Unsere Forschung basiert auf der Arbeit von Narendra und Kollegen,¹¹ in der die Autoren eine Konfliktlösung mit Verhandlungen je nach Konflikttyp vorschlagen. Diese Studie bietet einen Rahmen für autonome Teilnehmer, die sich in virtuellen Unternehmen (VE) zusammenschließen, und schlägt eine mehrschichtige Struktur vor, die verschiedene Geschäftslogik-Kontexte darstellt. Die Forschung zeigt, dass Konflikte auf der interorganisationalen, externen Ebene auftreten. In unserem Beitrag wird der Ansatz aus Ref. 11 definierte Ansatz auf die e-Health-Domäne. Der Anwendungsfall des Gesundheitswesens bestätigt, dass Konflikte in der interorganisationalen Kollaborationsschicht auftreten, da verschiedene Interessengruppen über voneinander abweichende E-Health-Daten verfügen können. Außerdem können sich die Geschäftsentscheidungen der einzelnen Beteiligten von denen der anderen unterscheiden, da alle Beteiligten ihre eigenen internen Prozesse haben.

Stahnke und Kollegen⁸⁰ stellen fest, dass die Blockchain-Technologie die Durchsetzung von interorganisationalen Arbeitsabläufen ermöglicht. Um zuverlässige Arbeitsabläufe zu schaffen, die für alle an interorganisationalen Prozessen beteiligten Akteure akzeptabel sind, müssen diese Arbeitsabläufe mithilfe von CPN entworfen und validiert werden, bevor sie in intelligente Verträge umgewandelt werden. Während CPN zur Validierung von interorganisationalen Prozessen eingesetzt wird, ist es wichtig, den Bedarf an rechtlich relevanten Smart Contracts und der notwendigen Unterstützung zu erkennen.

In einer Studie von Park und Kollegen⁸¹ wird vorgeschlagen, Enterprise Resource Planning (ERP)-Systeme in das Geschäftsprozess-Simulationsmodell einzubinden, um reale Daten in dem mit CPN entworfenen Simulationsprozess zu nutzen. Park und van der Aalst⁸¹ zielen darauf ab, die Komplexität von ERP-Systemen durch die Implementierung eines Rahmens zu überwinden, der es ermöglicht, sie in die Simulationsprozesse zu integrieren. Wir jedoch

weichen von diesem Ansatz ab, da wir aufgrund der sensiblen Natur von E-Health-Daten keine realen Komponenten in die Simulation einbringen. Zudem gehen wir von einer unbegrenzten Anzahl von Akteuren und deren internen Systemen aus, die an interorganisationalen eHealth-Prozessen teilnehmen. Folglich bringt die Integration einzelner Systeme keinen zusätzlichen Nutzen.

In ihrer Arbeit konzentrierten sich Jadav und Kollegen⁸² auf den Einsatz von KI zur Entdeckung von Angriffen auf Wearables und zur gemeinsamen Nutzung von Gesundheitsdaten mit einer öffentlichen Blockchain. Die Autoren schlagen die Verwendung der Blockchain-Technologie für die Unveränderbarkeit der Daten vor. In unserer Forschung stellen wir ebenfalls fest, dass die Blockchain-Technologie die Unveränderbarkeit von E-Health-Daten ermöglicht, aber wir konzentrieren uns nicht auf den Einsatz von KI zur Aufdeckung von Datenmanipulationen. Das in diesem Papier vorgeschlagene interorganisatorische Prozessdesign ermöglicht jedoch die Integration nicht-menschlicher Akteure wie KI-Agenten.

Das von Kim und Kim⁸³ vorgeschlagene DeepBlockShield-System zielt darauf ab, Probleme mit dem Verlust medizinischer Daten mithilfe der Blockchain-Technologie zu lösen. Die entsprechende Lösung sieht vor, Daten auf einer Blockchain zu speichern und gleichzeitig speziellen Agenten Zugang zu gewähren. In unserer Forschung gehen wir davon aus, dass medizinische Daten nicht nur auf einer Blockchain gespeichert werden können, und schlagen das MFSSIA-Framework vor, um eine sichere Zusammenarbeit zwischen verschiedenen Akteuren bei der gemeinsamen Nutzung von E-Health-Daten zu ermöglichen.

In einer neueren Studie von Abbas und Kollegen⁸⁴ wurde ein Rahmen für den sicheren Austausch und Zugriff auf Daten von tragbaren Geräten vorgeschlagen, der die Blockchain-Technologie nutzt, um die Sicherheit der Datenübertragung und die Verwaltung zwischen miteinander verbundenen Knoten zu gewährleisten. Die Autoren haben die Wirksamkeit ihrer Forschungsergebnisse in Bezug auf Genauigkeit, Präzisionsverhältnis, durchschnittlichen Vertrauenswert und Reaktionszeit bewertet. In unserer Forschung haben wir die formalen CPN-Tools eingesetzt, um den Entwurfsprozess zu bewerten und sicherzustellen, dass keine Entwurfsprobleme auftreten. Darüber hinaus legt unser Entwurfsprozess den Schwerpunkt auf die Lösung von Datenverarbeitungskonflikten und die Berücksichtigung von Sicherheitsaspekten.

Dieser Artikel konzentriert sich in erster Linie auf die technischen Aspekte der Blockchain-Implementierung im Gesundheitswesen Datenmanagement, insbesondere bei der Integration von persönlichen und

Verwaltung, insbesondere bei der Integration von persönlichen und elektronischen Patientenakten. Angesichts dieser technischen Ausrichtung bezieht diese Studie keine menschlichen Probanden direkt mit ein und sammelt auch keine Daten, bei denen Ethnie oder Ethnizität relevante Faktoren wären.

In Fällen wie diesen, in denen sich die Forschung auf die Entwicklung von Technologien und nicht auf menschliche Subjekte konzentriert, ist die Erhebung von Daten zur Ethnie oder zur Volkszugehörigkeit nicht sinnvoll. Unsere Studie befasst sich eher mit den systemischen und technologischen Herausforderungen und Lösungen bei der Integration von Gesundheitsdaten als mit den demografischen Merkmalen der Endnutzer. Im breiteren Einsatzkontext beeinflussen solche Faktoren jedoch die Implementierung von Gesundheitstechnologie und ihre gesellschaftlichen Auswirkungen.

Schlussfolgerungen

In diesem Beitrag untersuchen wir die automatische Konfliktlösung in dezentralen E-Healthcare-Systemen mit Blockchain-Technologie. Letztere ermöglicht autonome und transparente interorganisatorische Prozesse und einen vertrauenswürdigen Konfliktlösungsmechanismus, ohne eine zentrale Behörde einzubeziehen. Der von uns vorgeschlagene Ansatz basiert auf mehreren wissenschaftlichen Methoden, wie DSR, CPN-Modellierung und Frameworks, wie T-DM, eSourcing und MFSSIA. Wir verwenden T-DM für eine Blockchain-basierte Systemanforderungsdefinition, um die Grundlage für den Entwurf der Systemarchitektur, die Token-Ökonomie, die die On-Chain-Transaktionsätze definiert, und die dynamische Protokollentwicklung zu schaffen. Außerdem ordnen wir die in T-DM definierten funktionalen Ziele, bei denen Konflikte auftreten, den BPMN-Prozessbeschreibungen zu. Schließlich evaluieren wir unsere Forschungsergebnisse mit CPN, da es die mit T-DM definierten Konfliktlösungskonzepte im laufenden Prozess validiert. Unsere Evaluierung umfasst eine PoC-Prototyp-Implementierung des laufenden Prozesses. Mit der PoC-Evaluierung des CPN und des Prototyps stellen wir sicher, dass die Forschungsergebnisse in Echtzeitprozessen eingesetzt werden können.

Wir schlagen vor, eine DAO als automatischen Konfliktlöser bei der Verarbeitung und Abbildung von persönlichen E-Health-Daten in interorganisatorischen Prozessen einzusetzen. Voraussetzung für die automatische Konfliktlösung ist die Erstellung von PHR- und EHR-Daten durch mehrere Akteure in einer dezentralen Umgebung. Diese Akteure müssen in das MFSSIA eingebunden und authentifiziert werden, um sich auf die von einer DAO verwendeten Techniken zur gemeinsamen Nutzung von elektronischen Gesundheitsdaten und zur Lösung von Nutzungskonflikten zu einigen. Die elektronischen Gesundheitsdaten aus unterschiedlichen Quellen müssen vor ihrer Verwendung zusammengeführt werden. Nach der Definition der Anforderungen an die Erhebung und Verarbeitung von elektronischen Gesundheitsdaten schlagen wir zwei Arten von Konflikten vor - interne Geschäftsregeln und Konflikte bei Datendifferenzen. Schließlich schlagen wir vor, dass das dezentralisierte System im Falle eines Datenunterschiedskonflikts die Daten von mehreren Knotenpunkten erneut überprüft und dann entscheidet, welche Daten korrekt sind.

Unsere Forschung ist mit einigen Einschränkungen verbunden. Erstens müssen wir die integrierte MFSSIA im Kontext von Prozessen der gemeinsamen Nutzung von Daten zwischen Organisationen umfassend bewerten. Außerdem hat diese Studie

die spezifischen Herausforderungen bei der Implementierung von E-Health-Systemen nicht genau definiert. Darüber hinaus geht das Konzept der Token-Ökonomie, das die Aufteilung des Gemeinschaftseinkommens zwischen den Produzenten von Inhalten und den Nutzern von Diensten, die einen Wertbeitrag leisten, beinhaltet, über den Rahmen dieser Arbeit hinaus. Folglich werden die Aspekte der Token-Wirtschaft und der Transaktionskosten in unserer Forschung nicht behandelt.

Die Wahrung der Privatsphäre der Nutzer ist von größter Bedeutung, da ein Versäumnis rechtliche Folgen haben kann. Diese Studie befasst sich jedoch nicht mit den rechtlichen Aspekten des Schutzes der Privatsphäre bei Nutzerdaten. Daher hängen die Akzeptanz und Umsetzung der vorgeschlagenen Techniken von der Rechtsprechung des jeweiligen Landes und der Einhaltung der einschlägigen Gesetze und Vorschriften durch das Krankenhaus ab.

Wir arbeiten an den E-Health-spezifischen Challenge-Set-Regeln für MFSSIA. Nach der Implementierung eines PoC-Prototyps planen wir die Zusammenarbeit mit Gesundheitsdienstleistern, um unsere Forschungsergebnisse mit realen Anwendungsfällen zu testen. Zukünftige Arbeiten beziehen sich auch auf die Lösung der Herausforderungen, die mit der Heterogenität des sozioadministrativen Umfelds verbunden sind. In dem vorgeschlagenen Entwurf definieren wir Vereinbarungen zwischen den Beteiligten mit unveränderlichen intelligenten Verträgen. Die künftige Arbeit bezieht sich auf die Überwindung dieser Herausforderung durch die Entwicklung eines Lebenszyklus für intelligente Verträge im Bereich der elektronischen Gesundheitsfürsorge, der die Übernahme von Änderungen in realen Vereinbarungen in die durch intelligente Verträge definierten Vereinbarungen ermöglicht.

Schließlich ist die Interoperabilität von Daten der elektronischen Gesundheitsfürsorge eine der größten Herausforderungen im Bereich der elektronischen Gesundheitsfürsorge. Die Verwendung gemeinsamer Standards, wie SNOMED CT, HL7, LOINC usw., soll dieses Problem lösen. Da wir davon ausgehen, dass der interorganisatorische Prozess flexibel ist und eine unbegrenzte Anzahl von Akteuren unterstützt, ergeben sich gleichzeitig Herausforderungen in Bezug auf Datenschutz und Interoperabilität. Wir gehen davon aus, dass sich sowohl menschliche als auch nicht-menschliche Teilnehmer im M2X-Kontext gegenüber dem MFSSIA-Framework authentifizieren müssen, um auf solche Prozesse zugreifen zu können. Da MFSSIA Challenge-Sets und eine auf Antworten basierende Identitätsauthentifizierung verwendet, können die unterstützten E-Health-Datenstandards ein Teil der Challenge-Sets sein, die in Zukunft entwickelt werden. Zukünftige Arbeiten umfassen auch die Einführung von KI-Agenten, die in verschiedenen interorganisatorischen Prozessphasen eingesetzt werden können, z. B. bei der MFSSIA-Authentifizierung, der Erhebung von E-Health-Daten und der Konfliktlösung.

Finanzierung

Keine Finanzierung.

Finanzielle und nichtfinanzielle Beziehungen und Aktivitäten

Dr. Norta ist Mitglied des BHTY-Redaktionsausschusses - es sind keine weiteren Offenlegungen zu melden.

Mitwirkende

Alle Autoren haben zu diesem Artikel beigetragen. Aleksandr Kormiltsyn schrieb den Artikel und führte Recherchen durch. Alex Norta betreute den Artikel und gab Feedback. Chibuzor Udokwu und Vimal Dwivedi bearbeiteten den Artikel und gaben Feedback. Sanam Nisar entwickelte einen Proof-of-Concept-Prototyp.

Referenzen

- Susskind RE, Susskind D. The future of the professions: how technology will transform the work of human experts. Oxford University Press; 2015.
- Mercille J. Privatisierung im irischen Krankenhausesektor seit 1980. *J Public Health*. 2018;40:863-70. <https://doi.org/10.1093/pubmed/fty027>
- Archer N, Fevrier-Thomas U, Lokker C, McKibbin KA, Straus SE. Personal health records: a scoping review. *J Am Med Inform Assoc*. 2011;18:515-22. <https://doi.org/10.1136/amiajnl-2011-000105>
- Leviton B, Getz K, Eisenstein EL, Goldberg M, Harker M, Hes-lerlee S, et al. Assessing the financial value of patient engagement: a quantitative approach from CTTI's Patient Groups and Clinical Trials project. *Ther Innov Regul Sci*. 2018;52:220-9. <https://doi.org/10.1177/2168479017716715>
- Dimitrov DV. Medizinisches Internet der Dinge und Big Data im Gesundheitswesen. *Health Inform Res*. 2016;22:156-63. <https://doi.org/10.4258/hir.2016.22.3.156>
- Kormiltsyn A, Udokwu C, Karu K, Thangalimodzi K, Norta A. Verbesserung von Gesundheitsprozessen mit intelligenten Verträgen. In: Proceedings of the international conference on business information systems. Springer, 2019; pp. 500-13.
- Norta A, Hawthorne D, Engel SL. A privacy-protecting data-exchange wallet with ownership-and monetization capabilities. In: Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN). IEEE, 2018; pp. 1-8.
- Eccher C, Piras EM, Stenico M. TreC - a REST-based Regional PHR. User Centred Networked Health Care A. Moen et al. (Eds.) IOS Press, 2011. <https://doi.org/10.3233/978-1-60750-806-9-108>
- Urbauer P, Sauer mann S, Frohner M, Forjan M, Pohn B, Mense A. Anwendbarkeit von IHE/Continua-Komponenten für PHR-Systeme: Lernen aus Erfahrungen. *Comput Biol Med*. 2015;59:186-93. <https://doi.org/10.1016/j.combiomed.2013.12.003>
- Zhang R, Liu L. Sicherheitsmodelle und -anforderungen für Anwendungscloids im Gesundheitswesen. In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing. IEEE, 2010; S. 268-75.
- Narendra NC, Norta A, Mahunnah M, Ma L, Maggi FM. Sound conflict management and resolution for virtual-enterprise collaborations. *Serv Oriented Comput Appl*. 2016;10:233-51. <https://doi.org/10.1007/s11761-015-0183-0>
- Szabo N. Smart contracts: building blocks for digital markets. *EXTROPY J Transhumanist Thought*. 1996;18:2.
- European Union. Charta der Grundrechte der Europäischen Union [Internet]. Europa.eu; 2012 [zitiert 2023 Jun 15]. Verfügbar unter: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT>
- Standardvertragsklauseln (SCC) [Internet]. Europäische Kommission-Europäische Kommission. [zitiert 2023 Jun 15]. Verfügbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de
- Einführung in die Hash-Funktion als Pseudonymisierungsverfahren für personenbezogene Daten. Europäischer Datenschutzbeauftragter [Internet]. edps.europa.eu. 2023 [zitiert 2023 Nov 15]. Verfügbar unter: https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_de
- Sun W, Cai Z, Li Y, Liu F, Fang S, Wang G. Security and privacy in the medical internet of things: a review. *Secur Commun Netw*. 2018;2018:5978636. <https://doi.org/10.1155/2018/5978636>
- Al-Muhtadi J, Shahzad B, Saleem K, Jameel W, Orgun MA. Fragen der Cybersicherheit und des Datenschutzes für sozial integrierte mobile Gesundheitsanwendungen, die in einer Multi-Cloud-Umgebung betrieben werden. *Health Inform J*. 2019;25:315-29. <https://doi.org/10.1177/1460458217706184>
- Katurura M, Cilliers L. Ein Überblick über die Einführung elektronischer Patientendatenysteme auf dem afrikanischen Kontinent. In: Pro-ceedings of the African Computer and Information System & Technology Conference. 2017; pp. 10-11.
- Cilliers L. Wearable devices in healthcare: privacy and information security issues. *Health Inf Manag J*. 2019;49(2-3):150-6. <https://doi.org/10.1177/1833358319851684>
- Luo E, Bhuiyan MZA, Wang G, Rahman MA, Wu J, Atiqz-zaman M. Privacyprotector: privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Commun Mag*. 2018;56:163-8. <https://doi.org/10.1109/MCOM.2018.1700364>
- Hussein AF, ArunKumar N, Ramirez-Gonzalez G, Abdulhay E, Tavares JMR, de Albuquerque VHC. Ein auf einer Blockchain basierendes System zur Verwaltung und Sicherung medizinischer Aufzeichnungen, unterstützt durch einen genetischen Algorithmus und eine diskrete Wavelet-Transformationsform. *Cogn Syst Res*. 2018;52:1-11. <https://doi.org/10.1016/j.cogsys.2018.05.004>
- Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. Fhir-chain: applying blockchain to securely and scalably share clinical data. *Comput Struct Biotechnol J*. 2018;16:267-78. <https://doi.org/10.1016/j.csbj.2018.07.004>
- Azorin-Lopez J, Fuster-Guillo A, Saval-Calvo M, Bradley D. Home technologies, smart systems and eHealth. In: Mecha-tronic futures. Springer, 2016; S. 179-200.
- Dittmar A, Meffre R, De Oliveira F, Gehin C, Delhomme G. Wearable medical devices using textile and flexible technologies for ambulatory monitoring. In: Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference. IEEE, 2006; S. 7161-4.
- Sebestyen G, Hangan A, Oniga S, Gál Z. eHealth-Lösungen im Kontext des Internets der Dinge. In: Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics. IEEE, 2014, S. 1-6.
- Salehi S, Giacalone M. Conflict resolution with equitable algorithms: a tool to establish a European common ground of available rights. In: F. Romeo, S. Martuccelli & M. Giacalone (Eds.). Die europäische gemeinsame Grundlage verfügbarer Rechte. Napoli: Edi-toriale Scientifica; 2009, S.111.
- Xu H, Hipel KW, Kilgour DM, Fang L. Conflict resolution using the graph model: strategic interactions in competition and cooperation. Springer, 2018.
- Neyens G. Konfliktbehandlung für autonome Systeme. In: Pro-ceedings of the 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W). IEEE, 2017; pp. 369-70.
- Priya KF, Patil NN. Resolving privacy conflict for maintaining privacy policies in online social networks. *Int J Com-put Eng Technol*. 2019;10:94-101. <https://doi.org/10.34218/IJCET.10.3.2019.011>
- Hölbl M, Kompara M, Kamišalić, A, Nemeč Zlatolas L. A systematic review of the use of blockchain in healthcare. *Symmetry*. 2018;10:470. <https://doi.org/10.3390/sym10100470>

31. Agbo CC, Mahmoud QH, Eklund JM. Blockchain-Technologie im Gesundheitswesen: eine systematische Übersichtsarbeit. In: Proceedings of the health-care. Multidisciplinary Digital Publishing Institute, 2019; Vol. 7, p. 56.
32. McGhin T, Choo KKR, Liu CZ, He D. Blockchain in health-care applications: research challenges and opportunities. *J Netw Comput Appl.* 2019;135:62-75. <https://doi.org/10.1016/j.jnca.2019.02.027>
33. Swan M. Blockchain: Blaupause für eine neue Wirtschaft. O'Reilly Media, Inc; 2015.
34. Buterin V. Ein intelligenter Vertrag der nächsten Generation und eine dezentrale Anwendungsplattform. Whitepaper. Ethereum Foundation; 2013.
35. Becker G. Merkle-Signaturverfahren, Merkle-Bäume und ihre Kryptoanalyse. Ruhr-Universität Bochum, Tech. Rep; 2008.
36. Hevner A, Chatterjee S. Design Science Research in Information Systems. Integrierte Reihe in der Wirtschaftsinformatik. 2010; S. 9-22.
37. Westaway MD, Stratford PW, Binkley JM. Die patientenspezifische Funktionsskala: Validierung ihrer Verwendung bei Personen mit Nackenfunktionsstörungen. *J Orthop Sports Phys Ther.* 1998;27:331-8. <https://doi.org/10.2519/jospt.1998.27.5.331>
38. Nguyen GT, Kim K. A survey about consensus algorithms used in blockchain. *J Inf Process Syst.* 2018;14:101-28.
39. Bitcoin-Open Source P2P Geld [Internet]. bitcoin.org. [cited 2023 Jun 15]. Verfügbar unter: <https://bitcoin.org>.
40. Home| Ethereum [Internet]. ethereum.org. 2019 [zitiert 2023 Jun 15]. Verfügbar unter: <https://www.ethereum.org>.
41. Hyperledger Fabric-Hyperledger [Internet]. Hyperledger; 2017 [zitiert 2023 Jun 15]. Verfügbar unter: <https://www.hyperledger.org/projects/fabric>
42. Udokwu C, Kormiltsyn A, Thangalimodzi K, Norta A. The state of the art for blockchain-enabled smart-contract applications in the organization. In: Proceedings of the 2018 Ivannikov Ispras Open Conference (ISPRAS). IEEE, 2018; pp. 137-44.
43. Weyl EG, Ohlhaber P, Buterin V. Decentralized society: Finding Web3's soul. Verfügbar unter SSRN 4105763 2022.
44. Thematic Report[Internet]. Verfügbar unter: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf
45. Damjan M. Die Schnittstelle zwischen Blockchain und der realen Welt. In: *Ragion pratica.* 2018; pp. 379-406.
46. Caldarelli G, Ellul J. The blockchain oracle problem in decentralized finance-a multivocal approach. *Appl Sci.* 2021;11:7572. <https://doi.org/10.3390/app11167572>
47. Liu L, Zhou S, Huang H, Zheng Z. From technology to society: an overview of blockchain-based DAO. *IEEE Open J Comput Soc.* 2021.
48. Grefen P, Aberer K, Hoffner Y, Ludwig H. CrossFlow: cross-organizational workflow management in dynamic virtual enterprises. *Comput Syst Sci Eng.* 2000;1:277-90.
49. Rahmani AM, Thanigaivelan NK, Gia TN, Granados J, Negash B, Liljeberg P, et al. Smart e-health gateway: bringing intelligence to internet-of-things based ubiquitous health-care systems. In: Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). IEEE, 2015; pp. 826-34.
50. Leiding B, (sup) Dieter Hogrefe, Clemens HC, Norta A. The M2X economy-business interactions, transactions and col-laborations among autonomous smart devices. PhD thesis, Georg-August-Universitaet Goettingen, 2019.
51. Shiang CW, Meyer JJ, Taveter K. Agent-oriented methodology for designing cognitive agents for serious games. *Engineering Multi-Agent Systems.* 2016; p. 39.
52. Barr ET, Harman M, McMin P, Shahbaz M, Yoo S. The oracle problem in software testing: a survey. *IEEE Trans Softw Eng.* 2014;41:507-25. <https://doi.org/10.1109/TSE.2014.2372785>
53. Norta A, Mahunnah M, Tenso T, Taveter K, Narendra NC. Eine agentenorientierte Methode zur Gestaltung großer sozio-technischer Service-Ökosysteme. In: Proceedings of the 2014 IEEE World Con-gress on Services. IEEE, 2014; pp. 242-9.
54. Sherkat M, Mendoza A, Miller T, Burrows R. Emotional at-tachment framework for people-oriented software. arXiv pre-print arXiv:1803.08171 2018.
55. Kormiltsyn A. A systematic approach to define requirements and engineer the ontology for semantically merging data sets for personal-centric healthcare systems. 2018.
56. Sherkat M. Emotionalism in software engineering. PhD thesis, 2019.
57. Mendoza A, Miller T, Pedell S, Sterling L, et al. Die Rolle der Emotionen der Nutzer und der damit verbundenen Qualitätsziele bei der Aneignung von Systemen: zwei Fallstudien. In: Proceedings of the 24th Austral-asian Conference on Information Systems. 2013.
58. Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans Dependable Secure Comput.* 2004;1:11-33. <https://doi.org/10.1109/TDSC.2004.2>
59. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. *J Big Data.* 2018;5:1. <https://doi.org/10.1186/s40537-017-0110-7>
60. Fulpagare Priya K, Patil NN. Conflict detection techniques for preserving privacy in social media. 2018.
61. Udokwu C, Norta A. Deriving and formalizing requirements of decentralized applications for inter-organizational collabora-tions on blockchain. *Arab J Sci Eng.* 2021;46:8397-8414. <https://doi.org/10.1007/s13369-020-05245-4>
62. Jensen K, Kristensen LM. Coloured Petri Nets: Modelling and validation of concurrent systems. Springer Science & Business Media, 2009.
63. Mahunnah M, Norta A, Ma L, Taveter K. Heuristics for de-signing and evaluating socio-technical agent-oriented behaviour models with coloured petri nets. In: Proceedings of the Computer Software and Applications Conference Workshops (COMP-SACW), 2014 IEEE 38th International. IEEE, 2014; pp. 438-43.
64. Norta A, Kormiltsyn A, Udokwu C, Dwivedi V, Aroh S, Ni-kolajev I. A blockchain implementation for configurable multi-factor challenge-set self-sovereign identity authentication. In: Ezzat SK, Saleh YN, Abdel-Hamid AA (Eds.). *Blockchain Ora-cles: state of the art and research directions.* IEEE Access; 2022.
65. Riley L. Universelle DLT-Interoperabilität ist jetzt eine praktische Realität. Hyperledger Foundation Blog [Internet]. 2021 [zitiert 2023 Oct 7]. Verfügbar unter: <https://www.hyperledger.org/blog/2021/05/10/universal-dlt-interoperability-is-now-a-practical-reality>
66. Kormiltsyn A, Norta A. Dynamically integrating electron-ic-with personal health records for ad-hoc healthcare quality improvements. In: Proceedings of the International Conference on Digital Transformation and Global Society. Springer, 2017; pp. 385-99.
67. Norta AH. Exploring dynamic inter-organizational business pro-cess collaboration [Internet]. 2007 [cited 2023 Oct 7]. Verfügbar unter: <https://research.tue.nl/files/2003544/200710444.pdf>
68. Kormiltsyn A, Norta A. Formal evaluation of privacy-conflict resolution for integrating personal and electronic health records in blockchain-based systems. Technical report. 2022.

69. Norta A, Eshuis R. Specification and verification of harmonized business-process collaborations. *Inf Syst Front.* 2010;12:457–79. <https://doi.org/10.1007/s10796-009-9164-1>
70. Zhao F, Xiang D, Liu G, Jiang C. A new method for measuring the behavioral consistency degree of WF-net systems. *IEEE Trans Comput Soc Syst.* 2021;9:480-93. <https://doi.org/10.1109/TCSS.2021.3099475>
71. Weidlich M. Behavioural profiles: a relational approach to behaviour consistency. Dissertation, Universität Potsdam; 2011.
72. Workflow Nets-ML Wiki [Internet]. mlwiki.org. [zitiert 2023 Jul 11]. Verfügbar unter: http://mlwiki.org/index.php/Workflow_Nets.
73. Gehlot V, Sloane E, Thalassinidis AE. Persönliche Gesundheitstechnologie: CPN based modeling of coordinated neighborhood care environments (hubs) and personal care device ecosystems. 2019.
74. Jensen K, Kristensen LM, Wells L. Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. *Int J Softw Tools Technol Transf.* 2007;9:213-54. <https://doi.org/10.1007/s10009-007-0038-x>
75. sanamisarmalik. [sanamisarmalik/hprivacyconflictresolutionbyblockchain](https://github.com/sanamisarmalik/hprivacyconflictresolutionbyblockchain) [Internet]. GitHub. 2022 [cited 2023 Sep 25]. Verfügbar unter: <https://github.com/sanamisarmalik/hprivacyconflictresolutionbyblockchain>
76. Nisar S. Defining blockchain-based techniques for privacy conflict-resolution in cross-organizational processes for e-health systems. Masterarbeit, Universität Tartu, Fakultät für Wissenschaft und Technologie, Institut für Informatik; 2022.
77. Blockchains für die Massen-anwendung [Internet]. polygon.technology. [zitiert 2023 Jun 15]. Verfügbar unter: <https://polygon.technology>
78. Polkadot: Web3 Interoperabilität | Dezentralisierte Blockchain [Internet]. Polkadot Network. [zitiert 2023 Okt 4]. Verfügbar unter: <https://www.polkadot.network/>
79. Substrate und Polkadot | Substrate_ [Internet]. substrate.io. [zitiert 2023 Jun 15]. Verfügbar unter: <https://substrate.io/vision/substrate-and-polkadot/>
80. Stahnke S, Shumaiev K, Cuellar J, Kasinathan P. Enforcing a cross-organizational workflow: an experience report. In: *Proceedings of the Enterprise, Business-Process and Information Systems Modeling: 21st International Conference, BPMDS 2020, 25th International Conference, EMMSAD 2020, Held at CAiSE 2020, Grenoble, France, June 8-9, 2020, Proceedings 21*. Springer, 2020; pp. 85-98.
81. Park G, van der Aalst WM. Towards reliable business process simulation: a framework to integrate ERP systems. In *Proceedings of the Enterprise, Business-Process and Information Systems Modeling: 22nd International Conference, BPMDS 2021, and 26th International Conference, EMMSAD 2021, Held at CAiSE 2021, Melbourne, VIC, Australia, June 28-29, 2021, Proceedings*. Springer, 2021; S. 112-27.
82. Jadav D, Jadav NK, Gupta R, Tanwar S, Alfarraj O, Tolba A, et al. A trustworthy healthcare management framework using amalgamation of AI and blockchain network. *Mathematics.* 2023;11:637. <https://doi.org/10.3390/math11030637>
83. Kim J, Kim M. DeepBlockShield: Blockchain-Agent-basiertes gesichertes klinisches Datenmanagementmodell aus der Deep-Web-Umgebung. *Mathematics.* 2021;9:1069. <https://doi.org/10.3390/math9091069>
84. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Al-mansour FM. Blockchain-unterstütztes gesichertes Datenmanagement-Framework für die Analyse von Gesundheitsinformationen.

Copyright Ownership: Dies ist ein Open-Access-Artikel, der in Übereinstimmung mit der Creative Commons Attribution Non-Commercial (CC BY-NC 4.0)-Lizenz verbreitet wird, die es anderen erlaubt, dieses Werk nicht-kommerziell zu verbreiten, anzupassen, zu verbessern und ihre abgeleiteten Werke unter anderen Bedingungen zu lizenzieren, vorausgesetzt, das Originalwerk wird ordnungsgemäß zitiert und die Nutzung ist nicht-kommerziell. Siehe: <http://creativecommons.org/licenses/by-nc/4.0>.

Anhang

3-Tupel N: Ein Tupel ist eine endliche Folge oder geordnete Liste von Zahlen oder, allgemeiner, von mathematischen Objekten, die als Elemente des **Tupels** bezeichnet werden. Ein 3er-Tupel wird als Tripel (oder Triple) bezeichnet. Die Zahl n kann eine beliebige nichtnegative ganze Zahl sein.

Agentenorientierte Modellierung (AOM): Wird in der Organisations- und Informationssystemmodellierung verwendet, um absichtliche Beschreibungen von Prozessen als ein Netzwerk von Beziehungen zwischen Akteuren bereitzustellen. Als solche erfassen und repräsentieren sie Ziele, Abhängigkeiten, Absichten, Überzeugungen, Alternativen, usw.

Algorithmische Entscheidungssysteme (ADS): Die Delegation der Entscheidungsfindung und -umsetzung an Maschinen.

Zweiteiliger Graph: Ein Graph, dessen Eckpunkte in zwei disjunkte Mengen unterteilt werden können, so dass alle Kanten einen Eckpunkt in einer Menge mit einem Eckpunkt in einer anderen Menge verbinden.

Geschäftsprozessmodell und -notation (BPMN): Eine grafische Darstellung zur Spezifizierung von Geschäftsprozessen in einem Geschäftsprozessmodell.

Colored Petri Net (CPN)⁶⁹Modell: Rückwärtskompatible Erweiterung des mathematischen Konzepts der Petri-Netze.

Farbige Petri-Netze (CPNs): Erweitern das Vokabular gewöhnlicher Petri-Netze und fügen Merkmale hinzu, die sie für die Modellierung großer Systeme geeignet machen.

Urheberrecht: Dies ist ein Open-Access-Artikel, der in Übereinstimmung mit der Creative Commons Attribution Non-Commercial (CC BY-NC 4.0)-Lizenz verbreitet wird, die es anderen erlaubt, dieses Werk nicht-kommerziell zu verbreiten, anzupassen und zu verbessern und ihre abgeleiteten Werke zu anderen Bedingungen zu lizenzieren, vorausgesetzt, das Originalwerk wird ordnungsgemäß zitiert und die Nutzung ist nicht-kommerziell. Siehe: <http://creativecommons.org/licenses/by-nc/4.0>.

Dezentralisierte autonome Organisationen (DAOs): Eine Organisation, in der alle Mitglieder an der Entscheidungsfindung beteiligt sind, da es keine zentrale Behörde gibt.

Artikel 7 der Charta der Grundrechte der Europäischen Union: Gemäß der Definition in der Charta der Grundrechte der Europäischen Union¹³ ist Artikel 7 das Recht jeder Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

DeepBlockShield: Ein Modell, das die sichere gemeinsame Nutzung klinischer Daten implementiert. Es verwendet eine zweiseitige Benutzerüberprüfung und eine asynchrone Informationsbereitstellungsmethode, um die Sicherheit klinischer Daten zu verbessern.

Design Science Forschungszyklen: Ein Prozess, der sechs Schritte umfasst: Problemerkennung und Motivation, Lösungsziele, Design und Entwicklung, Bewertung und Kommunikation.

Designwissenschaftliche Forschung (DSR): Forschung, bei der ein neues zweckmäßiges Artefakt erfunden wird, um eine allgemeine Art von Problem anzugehen, und dessen Nutzen für die Lösung von Problemen dieser Art bewertet wird.

Elektronische Gesundheitsdaten (EHR): Daten eines Patienten, die von Angehörigen der Gesundheitsberufe erstellt und digital gespeichert werden.

Enterprise Resource Planning (ERP): Eine Art von Software, die Unternehmen zur Verwaltung ihrer täglichen Aktivitäten und zur Rationalisierung von Geschäftsprozessen einsetzen. ERP-Systeme integrieren verschiedene Funktionen aus unterschiedlichen Abteilungen wie Finanzen, Personalwesen, Beschaffung, Fertigung, Lieferkettenmanagement usw. in eine einzige, einheitliche Plattform.

Ethereum-Hauptnetz: Die primäre öffentliche Ethereum-Produktionsblockchain, auf der Transaktionen mit tatsächlichem Wert auf dem verteilten Ledger stattfinden. Ethereum verwendet ein Proof-of-Stake-Verfahren (PoS), bei dem die Validierung nicht auf den für die Lösung mathematischer Probleme aufgewendeten Ressourcen, sondern auf dem Ruf eines Knotens basiert.

Europäischer Datenschutzausschuss (EDPB): Unabhängiges Gremium der Europäischen Union mit eigener Rechtspersönlichkeit, dessen Aufgabe es ist, die einheitliche Anwendung der Allgemeinen Datenschutzverordnung sicherzustellen und die Zusammenarbeit zwischen den Datenschutzbehörden in der EU zu fördern.

Graphisches Modell zur Konfliktlösung (GMCR): Ein flexibles Instrument für den Einsatz im strategischen Management in einem wettbewerbsorientierten Umfeld.

Health Level Seven International (HL7): Ein Standard für die Meldung klinischer Ergebnisse, der heute in Gesundheitssystemen auf der ganzen Welt allgegenwärtig ist.

Versteckte Markov-Modelle (HMM): Sequenzmodelle. Das heißt, dass ein HMM bei einer Folge von Eingaben, wie z. B. Wörtern, eine Folge von Ausgaben derselben Länge berechnet. Ein HMM-Modell ist ein Graph, bei dem die Knoten Wahrscheinlichkeitsverteilungen über Etiketten und Kanten sind, die die Wahrscheinlichkeit des Übergangs von einem Knoten zum anderen angeben.

Internet der Dinge (IoT): Das kollektive Netzwerk verbundener Geräte und die Technologie, die die Kommunikation zwischen Geräten und der Cloud sowie zwischen den Geräten selbst erleichtert.

Logical Observation Identifiers Names and Codes (LOINC®): Klinische Terminologie, die für Labortestbestellungen und -ergebnisse wichtig ist und zu einer Reihe von Standards gehört, die in Systemen der US-Bundesregierung für den elektronischen Austausch von klinischen Gesundheitsinformationen verwendet werden.

Merkle-Baum oder Hash-Baum: Stellt sicher, dass die in einer Blockchain gespeicherten Transaktionen durch mathematische Hashes korreliert werden.

Metamask-Geldbörse: Software-Wallet für Kryptowährungen, die zur Interaktion mit der Ethereum-Blockchain verwendet wird.

Multi-Agenten-Systeme (MAS): Ein computergestütztes System, das aus mehreren interagierenden intelligenten Agenten besteht. Multiagentensysteme können Probleme lösen, die für einen einzelnen Agenten oder ein monolithisches System schwierig oder unmöglich zu lösen sind.

MFSSIA (Multifactor challenge-set self-sovereign identity authentication): Ermöglicht Blockchain-übergreifende Interoperabilität durch die Verwendung von Blockchain-Orakeln.

Parachains: Blockchains, die mit der Relay Chain von Polkadot oder Kusama verbunden sind. Dabei handelt es sich um anwendungsspezifische Datenstrukturen, die Transaktionen unter Verwendung der Relay-Chain validieren, einer zugrunde liegenden Struktur, die die sichere Kommunikation zwischen allen angeschlossenen Blockchains unterstützt, auch bekannt als Parachains.

Persönliche Gesundheitsakte (PHR): Elektronische gesundheitsbezogene Informationen einer Person.

Personal Health Token (PHT): Ein Utility Token für das dezentralisierte, personenzentrierte E-Health-System.

Polkadot: Ermöglicht blockkettenübergreifende Übertragungen jeglicher Art von Daten oder Vermögenswerten, nicht nur von Token. Die Anbindung an Polkadot ermöglicht die Interoperabilität mit einer Vielzahl von Blockchains im Polkadot-Netzwerk.

Konzeptnachweis (Proof of Concept, PoC): Auch bekannt als Proof of Principle (Grundsatzbeweis). Es handelt sich um die Umsetzung einer bestimmten Methode oder Idee, um ihre Durchführbarkeit zu demonstrieren, oder um eine prinzipielle Demonstration mit dem Ziel, zu überprüfen, ob ein Konzept oder eine Theorie praktisches Potenzial hat. Ein Proof of Concept ist in der Regel klein und kann vollständig oder unvollständig sein.

Proof-of-Work (PoW) Konsensalgorithmus: Ein dezentraler Konsensmechanismus, bei dem die Mitglieder des Netzwerks Anstrengungen unternehmen müssen, um eine verschlüsselte Hexadezimalzahl zu lösen. Proof-of-Work wird auch als Mining bezeichnet und bezieht sich auf den Erhalt einer Belohnung für geleistete Arbeit.

SNOMED CT oder SNOMED: Eine systematisch organisierte, computerverarbeitbare Sammlung medizinischer Begriffe mit Codes, Begriffen, Synonymen und Definitionen, die in der klinischen Dokumentation und Berichterstattung verwendet werden.

Lebenszyklus der Softwareentwicklung (SDLC): Der kosteneffiziente und zeitsparende Prozess, den Entwicklungsteams für die Entwicklung und Erstellung hochwertiger Software verwenden. Ziel des SDLC ist es, die Projektrisiken durch vorausschauende Planung zu minimieren, damit die Software die Kundenerwartungen während der Produktion und darüber hinaus erfüllt.

"Seelengebundene" Token (SBT): Eine Art von Token, die nur von einer bestimmten Adresse besessen und übertragen werden kann. Das bedeutet, dass ein "Soulbound"-Token, sobald er erstellt und einer Adresse zugewiesen wurde, nicht mehr von einer anderen Adresse übertragen oder besessen werden kann.

Spanische Datenschutzbehörde (AEPD): Eine unabhängige Behörde der spanischen Regierung, die die Einhaltung der gesetzlichen Bestimmungen zum Schutz personenbezogener Daten überwacht.

Standardvertragsklauseln (SCC): Dokumentation der Europäischen Kommission; diese Aktualisierung ist ein wichtiger Schritt zur Gewährleistung robuster und aktueller Datenschutzmaßnahmen bei grenzüberschreitenden Datenübertragungen.

Testdatenmanagement (TDM): Der Prozess zur Bereitstellung eines kontrollierten Datenzugriffs für moderne Teams während des gesamten Lebenszyklus der Softwareentwicklung (SDLC).

Utility- und nicht übertragbare "soulbound" Token (SBT): Auch als "nicht übertragbare Token" bezeichnet, handelt es sich um eine Art von NFT, die nicht auf eine andere Geldbörse übertragen oder verkauft werden können. Diese Art von Token wird häufig verwendet, um Referenzen, Zugehörigkeiten, Leistungen oder Mitgliedschaften zu repräsentieren.

WF-Netze: Eine Formalisierung zur Beschreibung von Prozessmodellen in parallelen und verteilten Systemen.