Klinik für Diagnostische und Interventionelle Radiologie
Universitätsklinikum Ulm
Direktor: Prof. Dr. med. Meinrad Beer

Blockchain im Gesundheitswesen

Nutzen der Blockchaintechnologie zur Vereinfachung und Verbesserung der medizinischen Versorgung anhand der Entwicklung einer Blockchain Emergency App

Dissertation zur Erlangung des Doktorgrades der Medizin
der Medizinischen Fakultät der Universität Ulm

Niclas Vester
Schwäbisch Gmünd
2020

Amtierender Dekan: Prof. Dr. rer. nat. Thomas Wirth
1. Berichterstatter: Prof. Dr. med. Stefan Schmidt
2. Berichterstatter: Prof. Dr. med. Claus-Martin Muth
Tag der Promotion: 15. April 2021

Widmung

Für meinen Großvater
1936 - 2019

Inhaltsverzeichnis

	Abkürzungsverzeichnis	
1.	**Einleitung**	**1**
1.1	Bitcoin, Blockchain und Patientendaten	5
1.2	Schutz medizinischer Inhalte und Nutzung	6
1.3	Blockchain Markt und Adoption	9
1.4	Blockchain Historie	12
1.5	Blockchain Grundlagen	15
1.6	Block der Blockchain	15
1.7	Eigenschaften der Blockchain	17
1.8	Agile Softwareentwicklung und Methoden	18
1.9	Ziel der Dissertation	19
2.	**Material und Methoden**	**21**
2.1	Lösungsansatz	21
2.2	Material und Software	21
2.3	Module, Methoden und Tools	25
2.4	Versuchsaufbau	32
2.5	Zusammenfassung Material und Methoden	59
3.	**Ergebnisse**	**61**
3.1	Datenbank-Modell	61
3.2	Chaincode / Smart Contract – new1Trace	62
3.3	Entwicklung der „Blockchain Emergency App“ mit APEX	64
3.4	Messergebnisse	74
3.5	Blockchain-Produktreife	80
3.6	Betriebsmodelle von Blockchain-Lösungen	81
3.7	Herausforderungen und Probleme	82
3.8	Zusammenfassung	88
4.	**Diskussion**	**89**
4.1	Beurteilung der Blockchain-Entwicklung	89
4.2	Nutzen der Blockchain-Technologie für die Radiologie	90
4.3	Nutzen der Blockchain-Technologie für den Patienten	91
4.4	Medizinische Anwendungsfälle und Ausblick	92
4.5	Außermedizinische Anwendungsfälle	101

5. Zusammenfassung **105**

6. Literaturverzeichnis **107**

Danksagung 112

Lebenslauf 113

Abkürzungsverzeichnis

ACL	Access Control List
AI	Artificial Intelligence
APEX	Oracle Application Express
API	Application Programming Interface
BA	Bundesanstalt für Arbeit
BAMF	Bundesamt für Migration und Flüchtlinge
BLOG	Weblog
BTC	Bitcoin
BTM	Betäubungsmittel
CA	Certified Authority
CD	Continous Delivery
CI	Continous Integration
CIO	Chief Information Officer
cURL	Client for URL
CT	Computertomographie
DLT	Distributed Ledger Technologie
DevOps	Development Operations
E-/R-Modell	Entity-Relationship Modell
ERP	Enterprise Resource Planning
EU-DSGVO	Europäische Datenschutz-Grundverordnung
EPA	Elektronische Patientenakte
ETH	Ether
F&E	Forschung und Entwicklung
FIT	Fraunhofer-Institut für Angewandte Informationstechnik
GDPR	Global Data Protection Regulation
NHS	National Health Service
HLF	Hyperleder Fabric
HTML	Hypertext Markup Language
HR	Human Resources
HTTP	Hypertext Transfer Protokoll
HTTPS	Hypertext Transfer Protokoll Secure
HYPERLINK	Verknüpfung von HTML Dokumenten
IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
ICD	International Statistical Classification of Diseases and Related Health Problems
IDM	Identity Management
IP	Intellectual Property

IoT	Internet of Things
IT	Informationstechnik
JSON	JavaScript Object Notation
KI	Künstliche Intelligenz
KIS	Krankenhausinformationssystem
LINK	Abkürzung für Hyperlink
ML	Machine Learning
MRT	Magnetresonanztomographie
MSP	Membership Service Provider
MSPID	Membership Service Provider Identification
NAT	Network Address Translation
NHS	National Health System
NoSQL	Not only SQL
OCI	Oracle Cloud Infrastruktur
ORDS	Oracle REST Data Services
PaaS	Platform as a Service
PACS	Picture Archiving and Communication System
PL/SQL	Procedural Language SQL
P2P	Peer-to-Peer
PWA	Progressive Web Application
REST	Representational State Transfer
SaaS	Software as a Service
Start-up	Spezielle Unternehmensform
SHA	Secure Hash Algorithm
SDK	Software Development Kit
SQL	Structured Query Language
TI	Telematik Infrastruktur
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
USE CASE	Anwendungsfall
VM	Virtuelle Maschine
XE	Express Edition

1. Einleitung

Die fortschreitende Digitalisierung betrifft und beeinflusst nahezu alle Bereiche unseres täglichen Lebens. Dabei spielt es keine Rolle, ob es sich um Online-Kartendienste, Banking, Suchmaschinen oder virtuelle Kaufhäuser handelt. Überall dort, wo ein höherer Komfort und ein besseres „Benutzer-Erlebnis“ (engl. User-Experience) dazu beitragen, das Leben des Einzelnen zu verbessern bzw. zu erleichtern, werden sich die Digitalisierung und die damit verbundenen Anwendungen sehr schnell durchsetzen. Die gesellschaftliche Akzeptanz zur Nutzung digitaler Dienste hat sich durch die Nutzung der mobilen Endgeräte entscheidend verändert bzw. befindet sich in einer Transformationsphase. Die Nutzung von Chat- und Messaging-Diensten hat eine Dynamik erreicht, die nahezu jede Altersgruppe anspricht und in vielen Lebenslagen genutzt, sogar erwartet wird. Datenschutz spielt in der Wahrnehmung der Anwender, insbesondere bei den „Digital Natives“, eine untergeordnete Rolle. Speziell im Gesundheitswesen steht jedoch der Schutz der Daten an erster Stelle. Der Logik folgend wird eine sehr sichere Infrastruktur benötigt, die gegen kriminelle „Hackerangriffe“ immun ist. Die Sicherheitsinfrastruktur muss die Eigenschaft besitzen, Manipulationen sofort aufzudecken bzw. diese so zu erschweren, dass ein Cyberangriff unwirtschaftlich ist und die gestohlenen oder manipulierten Daten wertlos sind. Es bedarf somit der Möglichkeit, einerseits die Daten bereitzustellen und andererseits deren Schutz zu gewährleisten. Nur dann kann Vertrauen und die damit verbundene Akzeptanz in ein neues System erreicht werden. Dieses Vertrauensverhältnis zwischen Geschäftspartnern kann nur dadurch erreicht werden, dass eine Vielzahl von Teilnehmern die Daten bzw. die damit verbundenen Transaktionen validieren, für korrekt befinden und erst nach einer gemeinsamen Abstimmung (Konsens) die Änderungen an den Daten vornehmen. Die Arzt-Patienten-Beziehung im medizinischen Umfeld kann nun analog zum Vertrauensverhältnis zwischen Geschäftspartnern in einem IT-Netzwerk betrachtet werden, d.h. Patienten, Ärzte, Forschungseinrichtungen, Apotheken etc. agieren direkt mit- und untereinander. Die erlaubten Aktivitäten, wie Überweisung eines Patienten, die Speicherung von Diagnosen und Therapien sollten in Folge dessen unveränderbar und nachvollziehbar protokolliert werden. Die Erlaubnis, mit einer medizinischen Kennung (ID) auf die Daten zugreifen zu können wird von den jeweils autorisierten

und authentifizierten Personen oder gleichermaßen vertrauenswürdigen Programmen direkt vorgenommen. Auf jedem der teilnehmenden Rechner im IT-Netzwerk liegen die Daten (z.B. Patientendatensatz) als Kopie im Dateisystem vor. Diese Rechner können gleichermaßen in einem Rechenzentrum des Uniklinikums Ulm, weltweit oder einer angeschlossenen Arztpraxis betrieben werden. Auf dem Prinzip der verteilten Datenhaltung basiert die Blockchain (dt. Blockkette) und deren Technologie. Aus diesem Grund wird sie auch häufig als verteilte Datenbank bezeichnet. Sie bietet mit ihren Eigenschaften den größtmöglichen Schutz gegen Datenmanipulation und schafft Transparenz, Klarheit und Vertrauen [12].

Die Abbildung 1 stellt einen stark vereinfachten Block der Blockchain dar, welcher im Datenbereich die PatientenID, ICD-Schlüssel, Diagnose, Therapie, Organisation, Status und ein Erfassungs- bzw. Änderungsdatum beinhaltet. In der Realität ist der Inhalt verschlüsselt und kann nicht ohne Prüfung auf Zugriffserlaubnis und Entschlüsselung eingesehen werden.

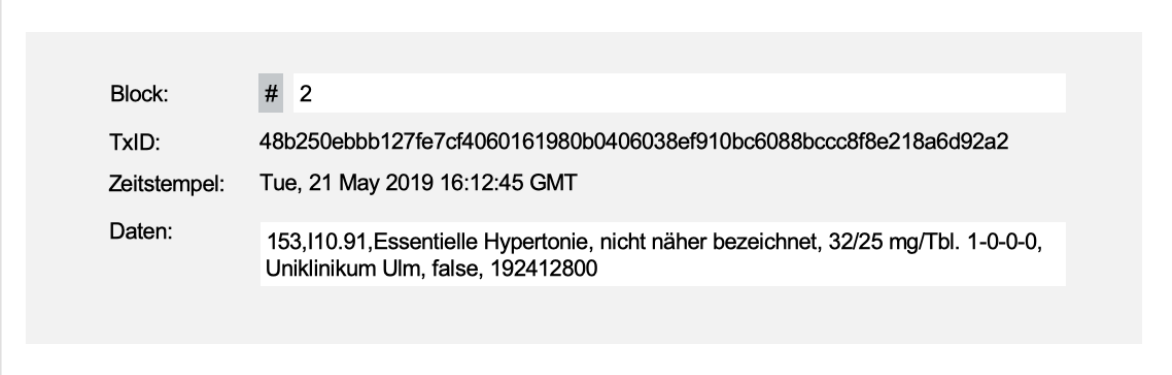


Abbildung 1: Vereinfachter Aufbau eines Blocks mit Speicherung einer Tracer Diagnose der „Blockchain Emergency App“

In dem Beispiel (Abb. 1) handelt es sich um die Erfassung einer Diagnose mit passender Therapie. Der Initiator ist in diesem Fall das Uniklinikum Ulm, die teilnehmende Organisation bzw. Person ist der niedergelassene Facharzt.

Ein konkreter Anwendungsfall aus der Radiologie beschäftigt sich mit der gemeinsamen Nutzung von Bilddaten, die durch Untersuchungen im Uniklinikum Ulm entstanden sind. Bei diesem Ansatz übergibt das Uniklinikum im Moment der Überweisung, das digitale Behandlungsrecht an den niedergelassenen Facharzt. Dieser erhält dadurch den Zugriff auf die Untersuchungsergebnisse und das

zugehörige digitale Bildmaterial (Sonographie, Röntgen, Computertomographie (CT), Magnetresonanztomographie (MRT) etc.) des Patienten. Durch diese Möglichkeit werden Doppeluntersuchungen vermieden und die Strahlenbelastung für die Patienten reduziert [49]. Darüber hinaus werden bürokratische Prozesse verschlankt und beschleunigt, was sowohl dem Patienten als auch allen an der Behandlungskette Beteiligten nützt. Dies erleichtert zudem eventuelle Rückfragen der Ärzte und kann Kosten senken.

Bei einem Notfalleinsatz könnten neben den Standardinformationen zum Patienten, die vor Ort durchgeführte Diagnostik und Behandlung in nahezu Echtzeit an das Uniklinikum Ulm übertragen werden. Die Logik wird dabei über automatisierte Programme realisiert, die über das Ereignis „Rettung“ getriggert werden. Der Uniklinik wird mitgeteilt, dass für den Patienten der Schockraum vorbereitet werden muss. Alle Daten zur Person, Diagnose und bereits durch den Notarzt eingeleiteten Maßnahmen sind lückenlos dokumentiert und einsehbar. Dadurch kann in kritischen Situationen Zeit eingespart und die Fortbehandlungen unterstützt werden. Als weiteres Beispiel kann die Anbindung einer Apotheke bis zur Krankenversicherung betrachtet werden. Die Abbildung 2 zeigt beispielhaft, wie ein Prozess von der Behandlung über die Ausstellung des E-Rezepts, über die Dosierungsmöglichkeit bis hin zur Abrechnung über die Blockchain gesteuert werden kann. Die Aktionen werden automatisiert abgearbeitet, dokumentiert und liegen unveränderbar vor.

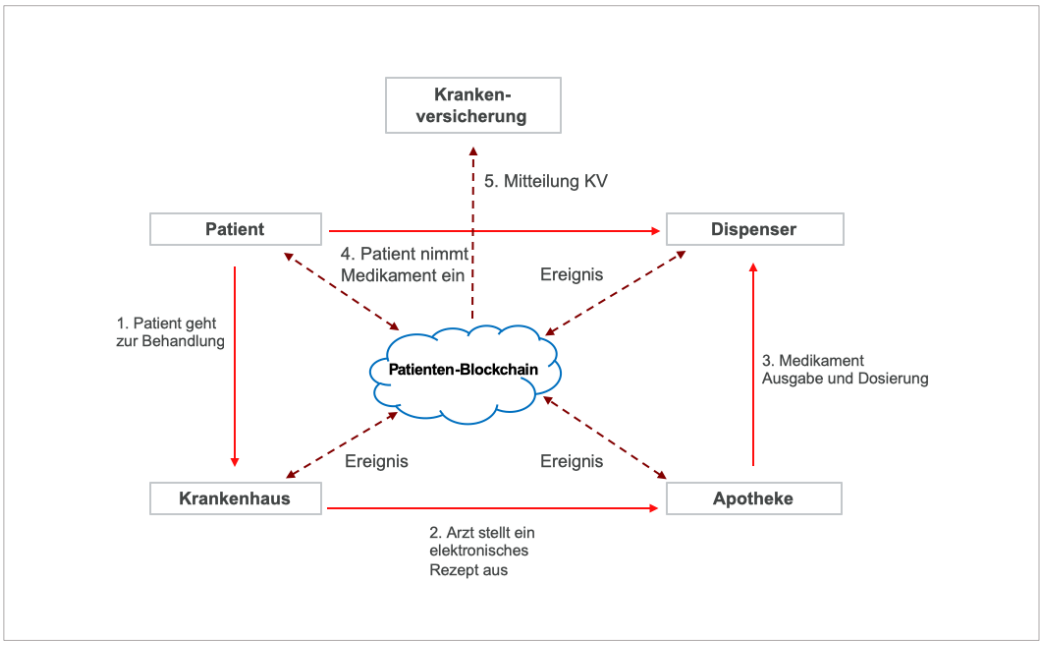


Abbildung 2: Beispielprozess für die Anbindung einer Apotheke an die Blockchain / KV = Krankenversicherung

Die für den Betrieb der Blockchain notwendige Infrastruktur wie Server, Speichersysteme und Netze können sowohl im lokalen Rechenzentrum des Uniklinikums als auch in einer Cloud-Umgebung zur Verfügung gestellt werden. Die Techniker Krankenkasse beispielsweise stellt Versicherten die „TK App“ auf dem Smartphone zur Verfügung, um die verordneten Medikamente, die abgerechneten ärztlichen Leistungen, die entstandenen Kosten und eine Art Behandlungshistorie einsehen zu können. Das Vertrauen wird in diesem Fall durch hohe Sicherheitsmechanismen „garantiert“, denen der Versicherte vertrauen muss. Das System stellt eine Art elektronische Patientenakte (EPA) dar. Wie die Daten bei der IBM (International Business Machines Corporation) verwaltet werden, ob und wie die Daten verschlüsselt werden ist nicht offengelegt und transparent. An diesem Punkt könnte auch Blockchain ansetzen, um eine sichere Infrastruktur abzubilden und die Interoperabilität für eine einheitliche Basis zwischen den unterschiedlichsten Systemen im Gesundheitswesen zu fördern und Patientendaten sicher auszutauschen. Aktuell sind viele unterschiedliche Krankenhaus-Informations-Systeme (KIS) wenig integriert und in teils abgeschotteten Silos mit unterschiedlicher Benutzerverwaltung und Sicherheitsstandards nicht zugreifbar. Es ist essentiell, dass die großen Softwarepartner ihre KIS-Anwendungen weiterentwickeln, um diese Infrastruktur in ihre Anwendungen zu integrieren, sonst entsteht kein realer Nutzen für Patienten, Ärzte, Gesundheitsbehörden und Versicherer.

Aus exakt diesen Gründen ist die Forschung in der Pflicht, die Entwicklung einer auf Blockchain basierenden Applikation voranzutreiben und die Machbarkeit unter Beweis zu stellen. Dadurch wird die Technologie greifbarer, erlebbarer und trägt zum Gesamtverständnis bei allen Beteiligten bei. Wenn es um die Einführung neuer Technologien geht, ist das Gesundheitswesen aufgrund von gesetzlichen Vorgaben, Regularien und den sensiblen Patientendaten eher zurückhaltend. Gleiches gilt für Sozialdaten, die in Rechenzentren hoheitlich verwaltet werden. Wegen Sicherheitsbedenken [20] werden Innovationen zurückgestellt oder oftmals nicht angegangen. Dies gilt auch für die bereits angesprochenen Softwarepartner [36], deren Lösungen im Gesundheitswesen zum Einsatz kommen. Hier spielen neben den technischen Bedenken die kommerziellen Betrachtungen eine Rolle, die Innovationen eher verhindern als fördern.

1.1 Bitcoin, Blockchain und Patientendaten

Die Kryptowährung Bitcoin wird oft gleichgesetzt mit der Blockchain-Technologie. Der Unterschied liegt darin, dass Bitcoin diese sichere Infrastruktur nutzt. Dabei geht es im Wesentlichen darum, dass der Kauf bzw. Verkauf von Waren und Dienstleistungen im Internet direkt zwischen Käufer und Verkäufer abgewickelt wird. Diese „Banktransaktion“ wird dabei nicht von einer Bank, sondern von den Teilnehmern und Nutzern der Bitcoin-Applikation überwacht. Das sind in der Regel Computersysteme von Privatpersonen oder kommerziellen Einrichtungen. Eine Überweisung ist im Falle von Bitcoin öffentlich, d.h. jeder kann die Transaktion einsehen, die jedoch anonym ausgeführt wird. Jede Zahlungstransaktion wird in eine Liste eingetragen, die auf allen Computersystemen im IT-Netzwerk als gleichberechtigte Kopie vorliegt. Alle Einträge können nur an das Ende der Liste eingefügt werden, wie das bei einem Hauptbuch (engl. Ledger) aus der Finanzbuchhaltung der Fall ist. Im Patientenfall würde jede Untersuchung in die Patientenakte an das Ende eingetragen und chronologisch geführt. Dadurch kann sichergestellt werden, dass Einträge nicht verändert oder gelöscht werden, was wiederrum ein ständiges Datenwachstum bedingt. Um Speicherplatz und Rechenleistung möglichst effizient zu nutzen, werden die Einträge der Liste in größere technische Speichereinheiten, den sogenannten „Blöcken“ (Abb. 1) zusammengefasst. Diese werden durch mathematische Verschlüsselungs-mechanismen „versiegelt“ und über technische Prüfsummen wie an einer Kette aufgereiht. Ein neuer Block kann nur an das Ende der Kette angefügt werden. Die Blöcke selbst werden von den teilnehmenden Computersystemen erzeugt (Bitcoin ca. alle zehn Minuten). Die dafür notwendigen Rechenkapazitäten und der damit verbundene Strombedarf sind enorm und stehen daher in der Kritik. Die Computersysteme müssen, bevor ein Block in die Kette eingefügt wird, ein komplexes mathematisches Problem lösen. Gerne wird dieser Prozess als „schürfen“ (engl. Mining) bezeichnet, da sowohl eine aufwendige Berechnung als auch etwas „Glück“ notwendig ist. Hat ein System den sogenannten „Hashwert“ als erstes ermittelt, darf es den Block in die Kette einfügen und wird dafür in Form von Bitcoins entlohnt. Das ist auch der Grund, warum teilweise ganze Serverfarmen eingesetzt werden, um diesen Wert zu finden. Denn je höher der Kurs steht, desto höher ist die Entlohnung bzw. der Gewinn. Damit die übrigen Teilnehmer nicht leer ausgehen, muss vom Überweisenden eine Art Grundgebühr in der Bitcoin-Währung

erstattet werden. Die Mechanismen sind dem Bankensystem ähnlich, nur dass das Vertrauen bei Bankgeschäften zwischen den Parteien durch Technologie ersetzt wird und kein Intermediär notwendig ist.

Das Grundverständnis der Kombination aus Bitcoin-Anwendung und Blockchain-Technologie ist notwendig. Dies bietet ein gutes Verständnis für die gesamtheitlichen Zusammenhänge und vermittelt gleichzeitig die Komplexität der Aufgabe, die dieser Dissertation innewohnt. Nach den zugegebenermaßen technischen Ausführungen muss nun der Bezug zur Medizin geschaffen werden. Wie bereits erwähnt kann eine Überweisung in Form von elektronischem Geld im übertragenen Sinn die direkte Arzt-Patienten-Beziehung abbilden. D.h. der Patient überweist sich und seine Gesundheitsdaten oder Teile davon an den Facharzt oder an medizinische Institutionen, um die Weiterbehandlung mit der gesamten Behandlungshistorie (Abb. 62) sicherzustellen. Im anderen Fall wird in dieser Dissertation gezeigt, wie eine Diagnose bzw. Therapie widerrufen werden kann, was eine Statusänderung (Abb. 63) bedeutet.

1.2 Schutz medizinischer Inhalte und Nutzung

Medizindaten sind sehr sensibel und müssen geschützt werden. Die dafür notwendigen technischen Möglichkeiten bietet die Blockchain mit ihren Eigenschaften wie Transparenz, Nachvollziehbarkeit, Unveränderlichkeit, Anonymität, Manipulationssicherheit, Dezentralität und kryptografische Verschlüsselung. Alle die genannten Merkmale sind notwendig, um Patientendaten effektiv zu schützen. Ein Patient könnte seine Gesundheitsakte direkt mit dem behandelnden Arzt austauschen, ohne sich um die dafür notwendigen Sicherheitsmechanismen kümmern zu müssen. Eine Überweisung vom Hausarzt zum Radiologen kann über diese Technologie realisiert werden, ohne den Datenschutz zu vernachlässigen. Der Abrechnungsprozess könnte durch den Wegfall von Clearingstellen vereinfacht, verkürzt und ggf. kostengünstiger gestaltet werden. D.h. die Verantwortung dafür liegt nicht beim Patienten oder behandelnden Arzt, sondern auf der Technologieseite. Dies hilft dem Arzt, dem Patienten und allen an der Behandlungskette beteiligten Akteuren.

Im Bericht der Online-Ausgabe des Spiegels vom 27.12.2019 [24] wurden durch IT-Experten des Computer Chaos Clubs (CCC) Schwächen im Gesundheitsdatennetz aufgedeckt. Dies ist insofern als kritisch anzusehen, da die Telematikinfrastruktur (TI) als Basis für den Zugriff auf die elektronische Patientenakte ab Januar 2021 zum Einsatz kommen soll. Die Ursache lag in diesem Fall jedoch im Bereitstellungsprozess der Chipkarten. Dennoch zeigt auch dieser Fall, dass Sicherheit einer der wichtigsten Aspekte im Hinblick auf die Online-Bereitstellung von Patientendaten ist. Nur durch Zufall werden hier Sicherheitslücken erkannt und danach von der Presse oder IT-Experten veröffentlich. Ein quergedachter Ansatz kann hier zum Tragen kommen. Die bewusste Bereitstellung von beispielsweise hochauflösendem Bildmaterial unter Berücksichtigung von Sicherheitsstandards auf Basis hochmoderner Technologien. Es klingt im ersten Ansatz beunruhigend, sensible Patientendaten wie z.B. radiologische Befunde auf jedem Rechner im lokalen IT-Netzwerk oder gar in einem über das Internet zugänglichen Cloudspeicher als Kopie abzulegen. Dies geschieht aktuell vielmehr unabsichtlich als geplant [54] ohne dass dies bekannt ist. Die Gründe hierfür sind oftmals wenig übergreifende Kommunikation, Teamwork und menschliche Fehler.

Die Deutsche Krankenhausgesellschaft (DKG) hat hierzu einen Artikel [55] verfasst, der diese Argumentation stützt. Darin wird der BSI-Präsident Arne Schönbohm wie folgt zitiert: „Krankenhäuser und viele andere Einrichtungen des Gesundheitswesens tragen in mehrfacher Hinsicht eine besondere Verantwortung für ihre IT-Netzwerke. Der Schutz sensibler Patientendaten muss ebenso zuverlässig gewährleistet sein wie die zuverlässige Versorgung von Patientinnen und Patienten mit Unterstützung modernster Computertechnologie. Vor diesem Hintergrund bietet der branchenspezifische Sicherheitsstandard für Krankenhäuser (B3S) wichtige Rahmenbedingungen, unter denen die Cyber-Sicherheit im Gesundheitswesen weiter erhöht werden kann.“ Im gleichen Bericht wird auf eine vom DKG in Auftrag gegebene Studie für die Umsetzungskosten referenziert. Demnach entstehen bei der Realisierung der empfohlenen Sicherheitsstandards für Krankenhäuser mit mehr als 30.000 vollstationären Patienten pro Jahr initiale Kosten von 1,5 bis 2 Millionen Euro und zusätzlichen Folgekosten zwischen 500.000 bis 600.000 Euro. Das bedeutet, dass Sicherheit zunächst hohe Kosten ohne erkennbaren Nutzen verursacht.

Der technologische Fortschritt ermöglicht neue Arten von Anwendungsfällen, die auch von den Bürgerinnen und Bürgern gewünscht werden. In der Bitkom Umfrage [7], welche am 08.05.2019 während der Pressekonferenz zu e-health vorgestellt wurde, sind die Mehrzahl der Bürger an einer digitalen Behandlungsakte interessiert. In der beschriebenen Befragung könnten sich 65% der Befragten vorstellen die e-Akte „auf jeden Fall“ (32%) oder „eher“ (33%) zu nutzen. Dies gilt übrigens auch für 60% der älteren Menschen ab 65 Jahren oder älter. Als wichtigste Funktionen werden ein digitaler Impfpass (98%), Medikationsplan mit Wechselwirkungscheck (91%), Diagnosen (91%) und eine Behandlungshistorie (87%) angesehen. Die wichtigsten drei Bedingungen für die Nutzung beziehen sich vor allem auf Datenhoheit und Datenschutz. Es muss sichergestellt sein, dass die Datenhoheit beim Patienten (61%) liegt. Die Daten müssen geschützt und sicher aufbewahrt werden (59%). Die Darstellung muss übersichtlich gestaltet und strukturiert (45%) sein. Darüber hinaus muss ein Online-Zugang möglich sein und ein mobiler Zugriff (34%) ermöglicht werden. Die Erwartungen der Patienten sind hoch. Die Erfahrungen der Versicherer aus vorigen Projekten sind gemischt und deren Einführung hat bei allen Beteiligten hohe Kosten mit überschaubarem Nutzen verursacht. Mit Blockchain könnte der Wunsch nach Schutz, Sicherheit und Datenhoheit der eigenen Gesundheitsdaten nachgekommen werden. Dadurch würden echte Mehrwerte für die Medizin, den Patienten und den Arzt entstehen. Patienten diese Datensouveränität zu übertragen setzt einen mündigen oder zumindest technisch interessierten Patienten und eine hochsichere Infrastruktur voraus. In keiner anderen Branche sind Daten sensibler und wertvoller als im Gesundheitsmarkt. Grundlage für den Beweis dieser These ist die Entwicklung der „Blockchain Emergency App“, welche im Ergebnisteil (Kapitel 3) beschrieben ist. Die darauf basierenden Erkenntnisse werden im Diskussionsteil (Kapitel 4) dargelegt.

Bei Blockchain handelt es sich um eine technisch anspruchsvolle Technologie, die sehr gut zum Fachgebiet der Radiologie passt, da hier innovative Ansätze und Technologien häufig früher als in anderen Fachgebieten adoptiert werden. Zusätzlich sind in der Radiologie sehr gute Anwendungsfälle vorhanden, die im Abschnitt 4 (Diskussion) vorgestellt werden. Im Health Management Journal unter

dem Titel „Unblock the Chain“ widmen sich die Autoren dem Thema Blockchain im Gesundheitswesen. Vor allem in der Cover Story mit dem Titel „Can Blockchain support advances in radiology?“ wird das Thema Blockchain aus dem Blickwinkel von radiologischem Bildmaterial betrachtet. Die Bedeutung von Big Data, Maschine Learning (ML), Artificial Intelligence (AI) und künstlicher Intelligenz (KI) unter Berücksichtigung der Blockchain-Technologie im Gesundheitswesen werden ergänzend diskutiert. Weiterhin werden die Vorteile für die Radiologie, das Zusammenspiel von Blockchain und General Data Protection Regulation (GDPR) bzw. EU-Datenschutz-Grundverordnung (EU-DSGVO) beleuchtet. Mit dem Inkrafttreten der EU-DSGVO [19] am 25. Mai 2016 wurde die Regelung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten verschärft. Beispielsweise muss der Verlust von Daten oder der Zugriff unberechtigter Dritter innerhalb von drei Tagen gemeldet und veröffentlicht werden. Das „Recht auf Vergessen“ muss auch beim Einsatz der Blockchain-Technologie berücksichtigt werden. Details zu den rechtlichen Aspekten im Sinne der juristischen Bewertung von Anwendungsfällen in Verbindung mit der Nutzung von Blockchain-Technologie finden sich in der Arbeit von Anna Rasinski [45] wieder. Ein Whitepaper von Deloitte zum Thema Blockchain „Einsatz im deutschen Gesundheitswesen“ [28] bestätigt, dass diese Infrastruktur sehr gut für einen sicheren Datenaustausch über unterschiedliche Fachdisziplinen hinweg geeignet ist.

1.3 Blockchain Markt und Adoption

Oftmals tritt nach der ersten Begeisterung (Hype) über eine Technologie die Ernüchterung ein, falls nicht ausreichend Anwendungsfälle für die Neuentwicklung vorhanden sind, die einen schnellen Erfolg und einen Nutzen zur Folge haben. Die Analystengruppe Gartner hat in ihrem Bericht „Hype Cycle for Emerging Technologies 2017“ die verschiedenen Phasen dargestellt.

Die Abbildung 3 zeigt, in welchem Stadium sich die jeweiligen Technologien bezogen auf die Zeitachse, Wahrnehmung und Nutzung befinden.

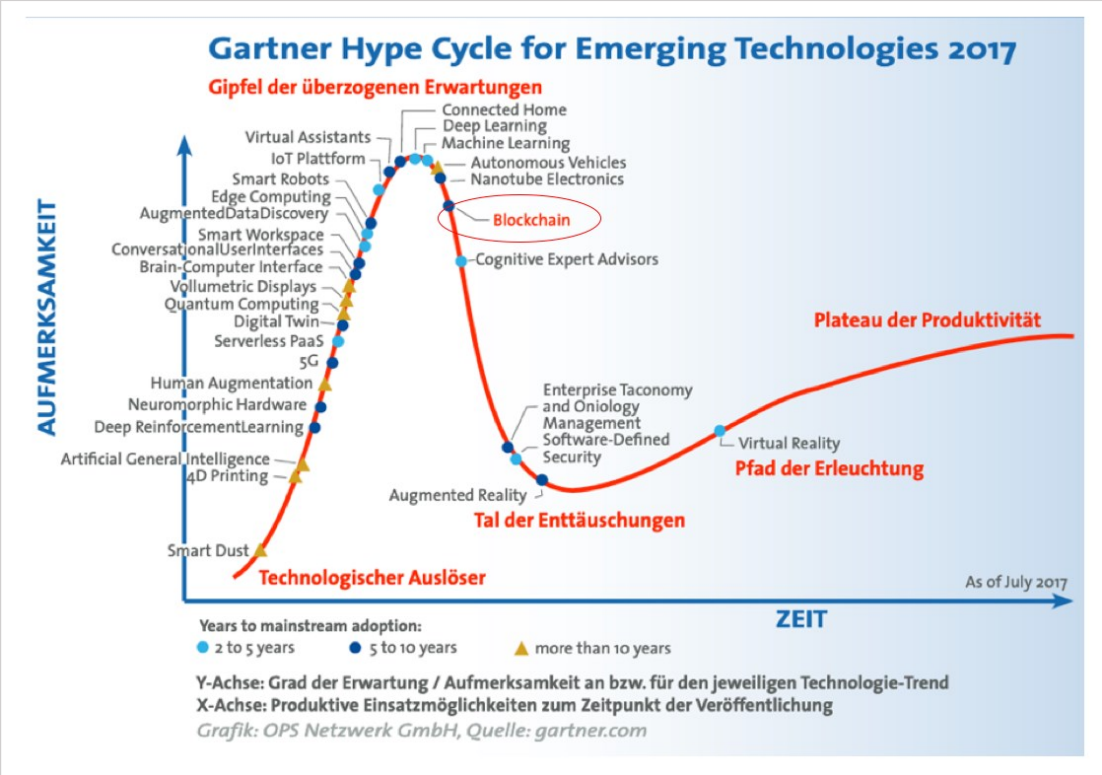


Abbildung 3: Gartner Hype Cycle for Emerging Technologies 2017 – mit freundlicher Genehmigung durch die Gartner Group

Ökologische Aspekte

Es ist erkennbar, dass die Blockchain-Technologie nach dem Hype über die Phase der Ernüchterung auf dem Weg zu realen Anwendungsfällen ist. Dies stellt eine Chance für neue Geschäftsmodelle dar. Mögliche Kosteneinsparungen durch Senkung der Transaktions- und Speicherkosten einerseits und die gemeinsame, weltweit in Echtzeit mögliche Nutzung von Bildmaterial können zu einer Veränderung des gesamten Ökosystems beitragen. Als aktuelles Beispiel aus der Energiebranche gilt das Berliner Blockchain-Start-up Lition©, welches in Kooperation mit der Gasag eine auf Blockchain basierte Handelsplattform für Ökostrom entwickelt hat und die Demokratisierung im Strommarkt dadurch vorantreibt. „Zunächst gehe es bei der Kooperation darum, zu lernen, wie schnell sich so ein Geschäft entwickelt und wie man es mitentwickeln kann“, erklärt Matthias Trunk, Gasag-Vertriebsvorstand [31]. Im Bereich der Compliance besteht von Seiten der Automobilhersteller und Zulieferer die Notwendigkeit, gegenüber dem

Gesetzgeber die verbauten Werkstoffe lückenlos zu dokumentieren [57]. Beispielsweise nutzt der Volkswagen Konzern die Blockchain-Technologie, um sicherzustellen, dass das bei der Herstellung von Lithium-Ionen-Batterien benötigte Kobalt aus nachhaltigem Abbau stammt [32].

Durch diese neuen Plattformen und Randbedingungen könnten ganze Branchen mit den etablierten Geschäftsmodellen von neuen und kostengünstigen Lösungen profitieren. Nahezu jedes Startup-Unternehmen betrachtet Blockchain oder integriert sie als Teil ihres Produkts. Diese kann genutzt werden, um Interoperabilität, Sicherheit, Transparenz und Nachvollziehbarkeit aufgrund ihrer Eigenschaften zu unterstützen. Gemäß den Prognosen von Analysten und Ökonomen aus Wirtschaft und der IT-Industrie wird die Blockchain als Zukunftstechnologie mit einem enormen Potential angesehen. Teilweise als vierte industrielle Revolution bezeichnet, mit dem Versprechen, ganze Branchen und Firmen zu verändern bzw. zu ersetzen (disruptiert) und gleichzeitig die Nutzung des Internets mit neuen Anwendungen zu verbessern.

Das Zitat und die damit verbundene Bedeutung von Tapscott D. und Tapscott A. zeigt, welchen Stellenwert die Blockchain bereits im Jahre 2017 hatte. Zitat: “The technology most likely to change the next decade of business is not the social web, big data, the cloud, robotics, or even artificial intelligence. It’s the blockchain, the technology behind digital currencies like bitcoin” [52].

Diese Kryptowährungen unterliegen im Gegensatz zum Fiat-Geld und Warengeld [4], welches von Zentralbanken verwaltet, ausgegeben und mit Rohstoffen wie z.B. Gold gedeckt ist, keiner Regulierungsbehörde, die den Wert festlegt oder überwacht. Das ist auch der Grund, warum die „Börsenkurse“ dieser digitalen Währungen extrem volatil und hoch spekulativ sind. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat festgelegt, dass ein Handel mit Kryptowährungen eine Erlaubnis erfordert. Diese Regelung wird vom Bundesfinanzministerium (BMF) mitgetragen, obwohl ein Berliner Kammergericht gegenläufig entschieden hat [60]. Selbst die amerikanische Börsenaufsicht „Securities and Exchange Commission (SEC)“ hat aktuell den Antrag auf einen regulierten Handel an allgemeinen Handelsplätzen abgelehnt [30] .

Die Blockchain-Technologie kann in Anwendungen als Sicherheitsinfrastruktur eingebettet werden. Somit bleibt sie für den Anwender verborgen. Dieser Umstand führt dazu, dass theoretische Erklärungen dem Verständnis dienlich sind, aber kein wirkliches Wissen und Erfahrung entsteht, um Akzeptanz bei Anwendern, Entscheidern und Firmen zu schaffen. Es bleibt nur, den Beweis praktisch zu führen. Aus diesem Grund muss untersucht werden, wie die Technologie funktioniert, welche Anwendungsfälle relevant sind und warum der Einsatz als revolutionär bezeichnet werden kann. Werden tatsächlich Kosten eingespart und neue Arten von Applikationen ermöglicht? Welche Kompetenzen und Ressourcen werden benötigt, um Anwendungen auf Basis einer Blockchain zu entwickeln? Diese Fragestellungen und ein paar weitere werden in dieser Dissertation untersucht, geklärt und mit einem Praxisbeispiel die Umsetzbarkeit bewiesen.

Diese Punkte stützen zusätzlich die Motivation und These, eine Dissertation an der Klinik für Diagnostische und Interventionelle Radiologie zum Thema Blockchain zu verfassen [33, 34, 46] und die Eignung für einen Einsatz im medizinischen Umfeld nachzuweisen.

1.4 Blockchain Historie

Ein Grund für die Erfindung der Blockchain und der darauf basierenden Kryptowährung Bitcoin war das mit der Weltwirtschaftskrise 2008 einhergehende fehlende Vertrauen in das Bankensystem, welches im Wesentlichen durch den Zusammenbruch der amerikanischen Investmentbank Lehman Brothers verloren ging. Im November 2008 wurde unter dem Pseudonym „Satoshi Nakamato“ (bis heute anonymer Autor), in einem Whitepaper mit dem Titel „Bitcoin: A Peer-to-Peer (P2P) Electronic Cash System“ [40] veröffentlicht, wie sich die Blockchain-Idee für eine verteilte und anonyme Währung nutzen lässt. Darin wird beschrieben, wie ein elektronischer Zahlungsverkehr zwischen mehreren Parteien direkt, d.h. ohne einen Intermediär wie z.B. eine Bank durchgeführt werden kann. Die Basis für das Vertrauen der beteiligten Parteien, die beispielsweise eine Zahlung tätigen, basiert auf mathematischen Verschlüsselungsalgorithmen (Kryptographie), die einen Missbrauch verhindern bzw. aufgrund der Architektur sofort aufdecken würden. Aus diesem Grund werden diese digitalen Währungen auch Kryptowährungen genannt.

Mit der heute neben Bitcoin bekanntesten Kryptowährung „Ethereum“ [48] wurde es mit sogenannten „Smart Contracts“ möglich, Verträge automatisiert und vertragssicher zwischen mehreren Parteien ohne Mittelsmann abzuschließen [40]. Mit Blockchain als Sicherheitsinfrastruktur ergeben sich viele neue Chancen für Anwendungsfälle im Gesundheitswesen, der öffentlichen Verwaltung (Tabelle 1) und der Privatwirtschaft. Ein Beleg dafür lieferte Frau Dr. med. Christina Czeschik bei der Auftaktveranstaltung zur IT-Sicherheit im Gesundheitswesen [11] in Düsseldorf.

Aktuell sind neben der Begeisterung für die Technologie die fehlenden Anwendungsfälle und die Komplexität das größte Hindernis für den Einsatz. Die meisten Anwendungen befinden sich im Pilotstadium (Tabelle 1) oder sind in Planung [41]. Es ist abzuwägen, für welchen Anwendungszweck diese Technologie geeignet ist. Im Rahmen einer Untersuchung der Condé Nast Verlag GmbH [41] zum Einsatz von Blockchain bei der internationalen Entwicklungszusammenarbeit fällt das Ergebnis ernüchternd aus. Von Forschern wurden dreiundvierzig Blockchain-Anwendungen untersucht. Keine der untersuchten Anwendungsfälle konnte ein Ergebnis erzielen. Das Bundesamt für Migration und Flüchtlinge (BAMF) hat in Zusammenarbeit mit dem Fraunhofer-Institut für Angewandte Informationstechnik (FIT) ein Whitepaper [2] veröffentlicht, in dem der Einsatz von Blockchain im Asylprozess untersucht wurde (Status und Ergebnis offen). Zuversicht für den Einsatz von Blockchain strahlt das BAMF dennoch aus [3]. Die Bundesregierung hat Blockchain im Koalitionsvertrag der 19. Legislaturperiode (ab Zeile 1931) als ein wichtiges Zukunftsthema aufgenommen [6]. Daraus ergeben sich folgende interessante Fragestellungen, die im Laufe der Arbeit beschrieben und anhand eines Beispiels praktisch umgesetzt wurden:

- Kann Blockchain in naher Zukunft die medizinische Dokumentation, Verwaltung und den Datenaustausch revolutionieren oder gar der elektronischen Gesundheitsakte zum Erfolg verhelfen?

- Lässt sich mittels Blockchain eine gemeinsame Basis legen, um Patientendaten sicher zu verwalten und diese den am Behandlungsprozess beteiligten Haus-

und Fachärzten, Rettungsdiensten, Krankenhäusern und Apotheken zeitnah, ohne Medienbruch zur Verfügung zu stellen?

- Kann Blockchain weltweiten, sicheren Online-Zugriff ermöglichen und gleichzeitig einen möglichen Missbrauch verhindern?

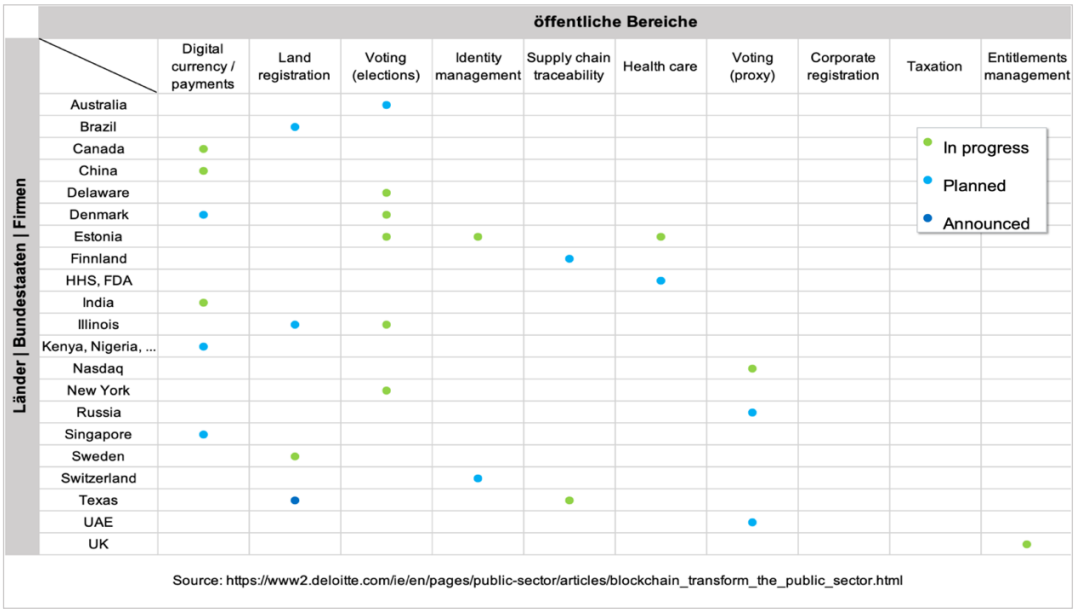
Im „Health Management Journal“ hat Eberhard Scheuer in einer Umfrage die Bereitschaft der Schweizer Bürger bezüglich der Bereitstellung ihrer Gesundheitsdaten bei klinischen Studien untersucht [47]. Das Ergebnis zeigte, dass 43% aller Befragten bereit wären, ihre Daten für Studien zur Verfügung zu stellen, wenn dadurch die Versicherungsprämie entfällt, reduziert oder die medizinische Forschung unterstützt wird, d.h. eine Rückvergütung in irgendeiner Form stattfindet.

Im Vergleich dazu können sich 54% der Internet-User vorstellen, ihre Gesundheitsdaten den Versicherungen zur Verfügung zu stellen, wenn eine Vergütung erfolgt [47].

Die Tabelle 1 zeigt, dass weltweit Anwendungsfälle auf Basis der Blockchain existieren, die für den sensiblen öffentlichen Bereich einen sinnvollen Einsatzzweck darstellen.

Tabelle 1: Weltweite Blockchain-Anwendungsfälle im Bereich der öffentlichen Verwaltung

Datenquelle: https://www2.deloitte.com/ie/en/pages/public-sector/articles/blockchain_transform_the_public_sector.html



1.5 Blockchain Grundlagen

Wie die Bezeichnung Blockchain bereits vermuten lässt, besteht sie aus einer Kette von aneinander gereihten Blöcken, die in einem dezentralen Peer-to-Peer-Netzwerk (P2P) als Kopie auf den jeweiligen Servern (Nodes) vorliegen und dort verwaltet werden. Sie kann sowohl strukturierte als auch unstrukturierte Daten verarbeiten.

Die wichtigsten Varianten der Blockchain sind:

- **Public Blockchain**
  Ein Beispiel für eine öffentliche Blockchain ist die Bitcoin-Anwendung. Daran kann jeder teilnehmen, der ausreichend Speicher- und Rechenkapazität zur Verfügung hat. Transaktionen werden grundsätzlich anonym durchgeführt und sind öffentlich einsehbar. Hierfür ist ein Schlüsselpaar bestehend auf einem öffentlichen- und einem Privaten Schlüssel notwendig.
- **Private bzw. „Permissioned“ Blockchain**
  Der Zugang zu sogenannten „permissioned“ Blockchains ist nur auf Anforderung bzw. Einladung möglich. In der Regel kommt dieser Ansatz bei Projekten im Gesundheitswesen, der Pharmabranche, der öffentlichen Verwaltung oder der Finanz- oder der Automobilindustrie (z.B. Zulieferketten) zum Tragen, um nur einige Beispiele zu nennen. Die handelnden Personen bzw. Organisationen sind untereinander bekannt oder erhalten ein digitales Zertifikat, welches die Benutzerkennung repräsentiert und sie als berechtigt ausweist.

Im hier umgesetzten Beispiel besteht der Teilnehmerkreis aus Patient, Hausarzt, Facharzt für Radiologie, Rettungsdienst und Apotheke. Die technischen Mechanismen arbeiten nach den gleichen Prinzipien wie bei der Bitcoin-Blockchain, welche in der Einführung (Kapitel 1) beschrieben wurde.

1.6 Block der Blockchain

Die Transaktionen werden chronologisch im Block protokolliert und in der richtigen Reihenfolge gespeichert. Verbunden sind die Blöcke der Kette über eine kryptografisch verschlüsselte Prüfsumme (Hashwert). Diese wird für den aktuellen Block unter Berücksichtigung des Hashwertes des vorigen Blocks, Zeitstempels und

den Transaktionsdaten (Abb. 1) gebildet. Somit ist eine nachträgliche Manipulation nahezu ausgeschlossen und würde sofort von den Teilnehmern erkannt. In einem nachträglichen Versuch, die Blockchain zu verändern, müsste die komplette Kette zurückgerechnet werden, was enorme Rechenleistung, Energiekosten und Zeit in Anspruch nehmen würde [25].

Ein neuer Block kann nur an das Ende der Kette eingefügt werden, wie Abbildung 4 schematisch darstellt.

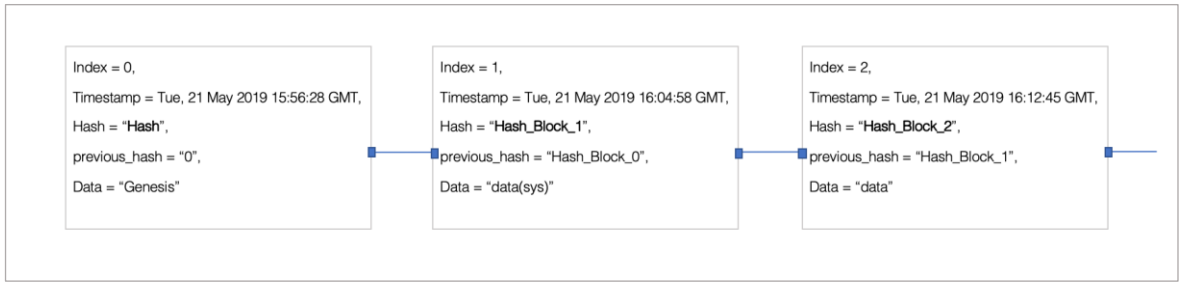


Abbildung 4: Schematischer Aufbau eines Blocks und der resultierenden Blockchain – Genesis Block ohne Hashwert

Diese Dezentralität unterstützt den Gedanken, dass Transaktionen nur dann valide sind und ausgeführt werden dürfen, wenn mehr als fünfzig Prozent der Teilnehmer die Korrektheit der Transaktion bestätigen. Darauf basiert das Vertrauen der Teilnehmer untereinander.

Für die Dissertation wurden folgende zwei Blockchains mit jeweils unterschiedlichen Chaincodes entwickelt:

Blockchain 1:

- Gründer / Founder: Universitätsklinikum Ulm
- Organisationen / Organizations
    - Patient
    - Hausarzt
    - Facharzt für Radiologie
    - Rettungsdienst
    - Apotheke
- Chaincode: new1Trace

Blockchain 2:

- Gründer / Founder: Universitätsklinikum Ulm
- Organisationen / Organizations
    - Labor
- Chaincode: new1Lab (optional)

Der Name des Chaincodes wurde bewusst neutral gehalten, um keinen Bezug zu Firmen, Lösungen oder Produkten, die als eingetragenes Warenzeichen (Copyright) registriert sind, herzustellen.

Das erste Netzwerk besteht aus Universitätsklinikum Ulm, Patient, Hausarzt, Facharzt, Rettungsdienst und der Apotheke. Das zweite Netzwerk besteht aus dem Universitätsklinikum Ulm und dem Labor. Beide Blockchains sind voneinander unabhängig. Die teilnehmenden Organisationen können nur auf die ihnen zugewiesenen Blockchains über den privaten Kanal zugreifen, Transaktionen ausführen und die Daten lesen. Die Blockstruktur folgt einer klaren Vorgabe, bestehend aus dem Header und der Datenstruktur (Abb. 4).

- Vereinfacht sind im Blockheader die ID, Timestamp, Hashwert des vorigen und Hashwert des aktuellen Blocks enthalten. Diese Liste enthält alle aktuell gültigen und jemals durchgeführten Transaktionen und wächst somit ständig.

- Die Datenstruktur (Abbildung 1) des Blocks kann der Entwickler selbst festlegen. Dieses Modell muss allerdings zur fachlichen Umsetzung im „Smart Contract“ passen. Das ist vergleichbar mit einem Entity-/Relationship-Modell, wenn mit einer relationalen Datenbank in einer passenden Programmiersprache entwickelt wird.

1.7 Eigenschaften der Blockchain

Die Blockchain eignet sich aufgrund ihrer kryptografischen Eigenschaften für eine Vielzahl von Anwendungen, die ohne einen Intermediär auskommen. Die wichtigsten Eigenschaften einer Blockchain sind:

- Dezentral und kryptografisch verschlüsselt

- Kein Intermediär notwendig
- Unveränderlich und manipulationssicher
- Transparent und nachvollziehbar

1.8 Agile Softwareentwicklung und Methoden

Die Wasserfallmethode ist ein Tool, welches in der Softwareentwicklung häufig genutzt wird bzw. wurde. Bei diesem Vorgehensmodell wird die Gesamtaufgabe als Anforderung formuliert, die Softwarearchitektur definiert, die Implementierung der einzelnen Komponenten umgesetzt, getestet und im letzten Schritt in die Produktion bzw. der Weiterentwicklung übergeben. Jede Phase hat einen festen Projektstart und ein definiertes Projektende (Milestone), um die festgelegten Entwicklungsziele gekoppelt mit einem im Projektmanagement festgelegten Zeitplan der Fertigstellung zu vergleichen. Parallel zur Entwicklung wird die Projektdokumentation erstellt.
Am Ende wird das Softwareprodukt dem für den Betrieb Verantwortlichen überlassen. Dieses Vorgehen hat sich über Jahre hinweg etabliert, auch wenn die Anforderungen aus dem Pflichtenheft häufig von neuen Ideen und Konzepten der Anwender während dieser Entwicklungsphase überholt wurden. Diesem Umstand tragen neue Vorgehensmodelle Rechnung, wie im Folgenden beschrieben.

Im digitalen Zeitalter, bei dem es auf Agilität, Geschwindigkeit und schnelle Releasezyklen eines Produkts ankommt, hat sich eine neue Form der Softwareentwicklung nach den „Development-/Operations“-Prinzipien (DevOps), durchgesetzt. Dabei werden in kleinen Gruppen die notwendigen Kompetenzen für das Projekt zusammengestellt und in kleinen „Sprints“ das Produkt iterativ mit den Endanwendern entwickelt. Ziel ist, die schnellstmögliche Umsetzung der fachlichen Anforderung, die sich auch während der Entwicklung ändern kann.

Im Falle von einer Radiologie-Anwendung, die auf einer Blockchain basiert, würden Ärzte, Entwickler, Architekten und die IT-Abteilung gemeinsam an der Lösung mitarbeiten. Somit lassen sich bereits in einem frühen Stadium (Prototyp) der Entwicklung Probleme erkennen und diese korrigieren. Um diese Agilität und Flexibilität zu erreichen, wird auf einen hohen Automatisierungsgrad bei der Entwicklung und dem späteren Software-Deployment (dt. Softwareverteilung) der Applikation gesetzt.

Die sogenannte „Continous Integration“ (CD) und der „Continous Delivery“ (CI) - Prozess [42] erlauben mit Hilfe von Tools ein schnelles, effizientes Entwickeln, Testen und automatisiertes Verteilen und Installieren der Applikation. Dabei wird das Projekt bis zur späteren Inbetriebnahme (Operation) von den Programmierern mitbegleitet. Dies führt zu einer ausgeprägten „Fehlerkultur“. Nach diesen Prinzipien wurde die Web-Applikation in der Dissertation teilweise für die in der Aufgabenstellung definierten Ziele entwickelt und darauf geachtet, dass die Applikation als „Progressive Web-Applikation“ (PWA) programmiert wurde, um auf allen gängigen Endbenutzergeräten ablauffähig zu sein. Darunter fallen beispielsweise PC’s, Laptops, Smartphones und Tablets. Neue, ausschließlich cloudbasierte Anwendungen (Cloud Native) werden modular als Webservice programmiert und sind voneinander unabhängig. Die Funktion ist atomar gehalten, damit sie unabhängig von anderen Komponenten ablauffähig ist, ausgetauscht und Fehler beseitigt werden können. Diese Architektur wird im Fachjargon als „Microservice“-Architektur bezeichnet. Ziel ist es, dass diese Services auf jeder beliebigen Betriebsplattform (z.B. Cloud) ausgerollt und ausgeführt werden können.

1.9 Ziel der Dissertation

Das Ziel dieser Dissertation ist es, mögliche Anwendungsfälle für Blockchain in der Medizin zu identifizieren, auf Praxistauglichkeit zu untersuchen und zu dokumentieren. Dabei handelt es sich um einen experimentellen Ansatz, der in der Dissertation verfolgt wurde. Der Nachweis ist mittels einer selbst zu entwickelnden Anwendung zu führen, die einen realen Anwendungsfall abbildet. Dafür sind Softwareprogramme, Skripte und Prozeduren zu entwickeln, die beispielhaft einen Prozess für die Übertragung eines digitalen Behandlungsrechts mittels Blockchain ermöglichen. Darüber hinaus ist über die Applikation der Widerruf einer Diagnose bzw. Therapie zu ermöglichen, welche die Daten transparent und unveränderlich in der Blockchain protokolliert und als Behandlungshistorie zur Verfügung stellt.

Für das Teilen (sharing) von radiologischem Bildmaterial, Notfallprotokollen und medizinischer Dokumentation ist eine Möglichkeit für den Up- und Download vorzusehen. Um den praktischen Bezug herzustellen, wird im Gegensatz zu einer öffentlichen, anonymen (z.B. Bitcoin) Blockchain eine private Blockchain verwendet, bei der die Teilnehmer untereinander bekannt sind und in unterschiedlichen Rollen

im Behandlungsprozess agieren. Ein Konzept für die Co-Existenz von im Einsatz befindlichen Datenbanksystemen, wie Oracle und der Blockchain Lösung ist weiterhin zu betrachten und Performance-Ergebnisse in Form von Statistiken zu dokumentieren.

Im Nachfolgenden Kapitel 2, „Material und Methoden“, wird auf die Module und Vorgehensweisen eingegangen, die für die Realisierung genutzt werden. Dies beinhaltet einen kurzen Überblick und die lückenlose Dokumentation und Nachvollziehbarkeit des Versuchsaufbaus und den damit einhergehenden Erkenntnissen. Die Beschreibung des Versuchsaufbaus muss aufgrund des Nachweises auch technische Inhalte vermitteln. Die Dokumentation der Lösung entstand gleichzeitig mit der Umsetzung, welche den Aufbau des Blockchain-Netzwerkes, die Datenbank-Strukturen, die Programmierung und die Webapplikation „Blockchain EmergencyApp“ beinhaltet. Über die Herausforderungen, Probleme und Fehlschläge bei der Umsetzung und Arbeit mit der Blockchain, Datenbank und Entwicklungswerkzeugen wird im Ergebnisteil (Kapitel 3) berichtet.

2. Material und Methoden

Bei den in der Applikation verwendeten Daten handelt es sich um „Fantasie-Patienten“, die real nicht existieren. Aus diesem Grund war auch kein Ethikvotum erforderlich.

2.1 Lösungsansatz

Mit Hilfe einer selbst programmierten Web-Applikation, der „Emergency App “ wurde ein Anwendungsfall komplett abgebildet und auf Praxistauglichkeit untersucht. Für die Implementierung wurde ein integrierter, hybrider Ansatz mit dem relationalen Datenbanksystem der Oracle Corporation verfolgt. Dies hat den Vorteil, dass sowohl bestehende Systeme wie SAP, KIS, Labor, Pathologie oder Radiologie als auch neue Anwendungssysteme interoperabel zusammenarbeiten können, was der Realität entspricht. Die Kombination von Patientenstammdaten in dem KIS-System und den Zusatzinformationen aus der Blockchain stellt eine Möglichkeit der Koexistenz während einer Transformationsphase für Anwendungen im Gesundheitswesen dar. Für den Patienten kann dies ein exakteres Diagnoseergebnis und eine personalisierte Therapie zur Folge haben. Speziell Mehrfacheingaben bei persönlichen Daten, mehrfache radiologische Untersuchungen und dadurch zusätzliche Strahlenbelastungen, Befunde und Labore bleiben dem Patienten erspart.

2.2 Material und Software (Stand 10.06.2019)

Für die Umsetzung des Blockchain-basierten Use Cases und der Web-Applikation sind nachfolgende Komponenten/Module erforderlich, die über den jeweiligen Link heruntergeladen werden können:

- Oracle© VM VirtualBox 6.0.10/VirtualBox Extension

  Copyright © Oracle Corporation and/or its affiliates. All rights reserved. Redwood Shores, CA, USA

  https://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html#vbox (01.09.2019)

  https://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html#extpack

- Oracle© Database Express Edition 18c for Linux x86-64

  Copyright © Oracle Corporation and/or its affiliates. All rights reserved. Redwood Shores, CA, USA

  https://www.oracle.com/database/technologies/xe-downloads.html (01.09.2019)

- Oracle© SQL Developer 19.2

  Copyright © Oracle Corporation and/or its affiliates. All rights reserved. Redwood Shores, CA, USA
  https://www.oracle.com/tools/downloads/sqldev-v192-downloads.html (01.08.2019)

- Oracle© Application Express 19.1

  Copyright © Oracle Corporation and/or its affiliates. All rights reserved. Redwood Shores, CA, USA
  https://www.oracle.com/technetwork/developer-tools/apex/downloads/ (01.08.2019)

- Oracle© REST Data Services 18.1 (19.2)

  Copyright © Oracle Corporation and/or its affiliates. All rights reserved. Redwood Shores, CA, USA
  https://www.oracle.com/technetwork/developer-tools/rest-data-services/downloads/index.html
  (18.04.2019)

- Oracle© Blockchain Platform SDK 19.2.1 (HLF 1.0) / 19.3 (HLF 1.4)

  Copyright © Oracle Corporation and/or its affiliates. All rights reserved. Redwood Shores, CA, USA
  https://www.oracle.com/technetwork/topics/cloud/downloads/blockchain-sdk-5443939.html (05.09.2018)
  https://www.oracle.com/database/technologies/blockchain-platform-enterprise-edition.html# (06.09.2019)

- Oracle© Linux 7.6

  Copyright © Oracle Corporation and/or its affiliates. All rights reserved. Redwood Shores, CA, USA
  https://edelivery.oracle.com/osdc/faces/SoftwareDelivery (kostenlose Registrierung erforderlich)
  (01.09.2019)

- Microsoft© Visual Studio Code 1.33 für die Zielplattform (Apple macOS)

  Copyright © 2019 Microsoft. All rights reserved. Redmond, WA, USA
  https://code.visualstudio.com/download (01.09.2019)

- Go Programming Language go1.10.3 für die Zielplattform (Apple macOS)

  Google© LLC, Mountain View, CA, USA
  Open-Source-Lizenz nach Berkeley Software Distribution (BSD)
  https://golang.org/CONTRIBUTORS (01.09.2019)
  https://golang.org/dl/ (01.09.2019)

- Postman 7.6.0 REST-Client für Aufruf des Smart Contracts

  © 2019 Postman, Inc. All rights reserved. San Francisco, CA, USA
  https://www.getpostman.com/downloads/ (01.09.2019)

- Firefox Web-Browser für MacOS oder in der Oracle VirtualBox VM

  Binaries of this product have been made available to you by the Mozilla Project under the Mozilla Public License 2.0 (MPL) https://www.mozilla.org/en-US/firefox/new/ (01.09.2019)

- Hyperledger Fabric®: Version 1.0

  Die HLF-Blockchain Implementierung ist Teil des Oracle Blockchain Platform SDK 19.2.1 und muss nicht separat heruntergeladen werden. Seit September 2019 SDK 19.3 mit HLF 1.4
  Copyright © 2018 The Linux Foundation®. All rights reserved. Hyperledger is a trademark of The Linux Foundation. Hyperledger has registered trademarks and uses trademarks. For a list of trademarks of Hyperledger, please see our Trademark Usage page. Linux is a registered trademark of Linus Torvalds. Privacy Policy and Terms of Use. (Quelle: https://www.hyperledger.org). (01.09.2019)

- Docker Inc. © Docker Community-Engine

  Steht in der Oracle © Linux 7.6 als Paket zur Verfügung und muss per Console installiert werden: z.B. über **yum -y install docker-ce**

- Programmierbeispiele: Volltextrecherche, APEX , REST, Oracle PL/SQL

  Carsten Czarski, Oracle Corporation, Consulting Member of Staff [9]

  Volltextrecherche Grundlagen
  Oracle TEXT: Tipps, Tricks, Best Practise, Dienstag, 13. März 2012
  https://oracle-text-de.blogspot.com/2012/03/nochmal-userdatastore-ein-umfassendes.html (01.09.2019)

  Volltextrecherche Beispiel mit Application Express und Oracle TEXT
  inkl. Dokumenten Up-/Download
  https://www.oracle.com/webfolder/technetwork/de/community/apex/tipps/text-search/index.html (01.09.2019)

  Ähnlichkeitssuche: Die „Kölner Phonetik“ in APEX, August 2013
  https://apex.oracle.com/pls/apex/germancommunities/apexcommunity/tipp/1502/index.html (06.09.2018)

  Ähnlichkeitssuche in einem APEX Bericht: Mit Oracle Text, August 2016
  https://apex.oracle.com/pls/apex/germancommunities/apexcommunity/tipp/5401/index.html (06.09.2018)

  Suchen mit SQL LIKE: Performance, Case- und Umlaut-Insensitive Suche
  https://apex.oracle.com/pls/apex/germancommunities/apexcommunity/tipp/281/index.html (06.09.2018)

  Dateien aus Datenbanktabellen mit APEX hochladen: Möglichkeiten, Juli 2015
  https://apex.oracle.com/pls/apex/germancommunities/apexcommunity/tipp/4181/index.html (28.06.2018)

  Dateien aus Datenbanktabellen mit APEX bereitstellen: Möglichkeiten, Juni 2015
  https://apex.oracle.com/pls/apex/germancommunities/apexcommunity/tipp/4221/index.html (28.06.2018)

  Creating a CRUD form on a REST Service with APEX, 16. Juli 2018
  https://blogs.oracle.com/apex/creating-a-crud-form-on-a-rest-service-with-apex-181 (22.07.2018)

APEX_STRING: String-Operationen leicht gemacht!, 11. Mai 2018
https://blogs.oracle.com/apexcommunity_deutsch/apex_string%3a-string-operationen-leicht-gemacht (28.05.2018)

Analysemöglichkeiten mit SQL: Mehr als SUM und GROUP BY
https://www.doag.org/formes/pubfiles/4541679/2013-BI-Carsten_Czarski-Analysemoeglichkeiten_mit_SQL__Mehr_als_SUM_und_GROUP_BY-Manuskript.pdf (22.11.2017)

Application Express Early Adopter: REST Services, 22. Dezember 2017
https://blogs.oracle.com/apex/get-started-with-rest-services-in-application-express-52-ea-1 (13.02.2018)

APEX 18.1 Early Adopter 2: Post-Process REST Service Queries, Mai 2018
https://blogs.oracle.com/apex/apex-181-early-adopter-2-post-process-rest-service-queries (08.06.2018)

APEX 18.1 Early Adopter 2: REST Services and PL/SQL, 12. März, 2019
https://blogs.oracle.com/apex/apex-181-early-adopter-2-rest-services-and-plsql (15.03.2019)

REST Services und Application Express 5.1 – Teil 1, April 2017
https://apex.oracle.com/pls/apex/germancommunities/apexcommunity/tipp/6001/index.html (02.02.2019)

Tipps zum JSON Parsing für APEX-Entwickler, 26. Februar 2018
https://blogs.oracle.com/apexcommunity_deutsch/tipps-zum-json-parsing-f%c3%bcr-apex-entwickler (28.02.2018)

Classic Reports einmal anders – mit Report Templates, 9. Februar 2018
https://blogs.oracle.com/apexcommunity_deutsch/classic-report-einmal-anders (11.02.2019)

APEX, HTTPS, Zertifikate und das Oracle Wallet, 2. Juni 2017
https://blogs.oracle.com/apexcommunity_deutsch/apex-https-zertifikate-und-das-oracle-wallet (05.09.2018)

Aplication Express und HTTPS: Nie wieder „Certificate Validation Error", Juni 2017
https://apex.oracle.com/pls/apex/germancommunities/apexcommunity/tipp/6121/index.html (05.09.2018)

DATE, TIMESTAMP und Formatmasken, 24. November 2017
https://blogs.oracle.com/apexcommunity_deutsch/date-timestamp-und-formatmasken (03.02.2018)

Alle angeführten Komponenten müssen installiert, konfiguriert und aufeinander abgestimmt werden. Die Oracle Software wurde bis auf den SQL (Structured Query Language) Developer in der Oracle VM VirtualBox Umgebung (Virtuelle Maschine) installiert. Die für den Nachweis genutzten technischen Komponenten basieren komplett auf der Technologie der Oracle Corporation, die ohne Lizenzgebühren in der gewählten Konfiguration als Entwicklungsplattform genutzt werden kann.

Die für die Messung der Performance-Ergebnisse eingesetzten Methoden und Tools wurden selbst entwickelt, sind in der virtuellen Maschine dokumentiert und Teil der Dissertation.

2.3 Module, Methoden und Tools

Im vorliegenden Fall ist die Gesamtanforderung, eine Web-Applikation für den Rettungsdienst bzw. Radiologie zu entwickeln, die Patientenstammdaten in einer Datenbank verwaltet, die Diagnosen und Therapien in der Blockchain speichert und als Historie zur Verfügung stellt. Darüber hinaus soll die Anwendung einen Überweisungsvorgang abbilden und einen Up-/Download-Mechanismus für die medizinische Dokumentation realisieren. Die Abb. 5 zeigt die dafür benötigten Komponenten und die Gesamtarchitektur, die für die Umsetzung genutzt wurden.

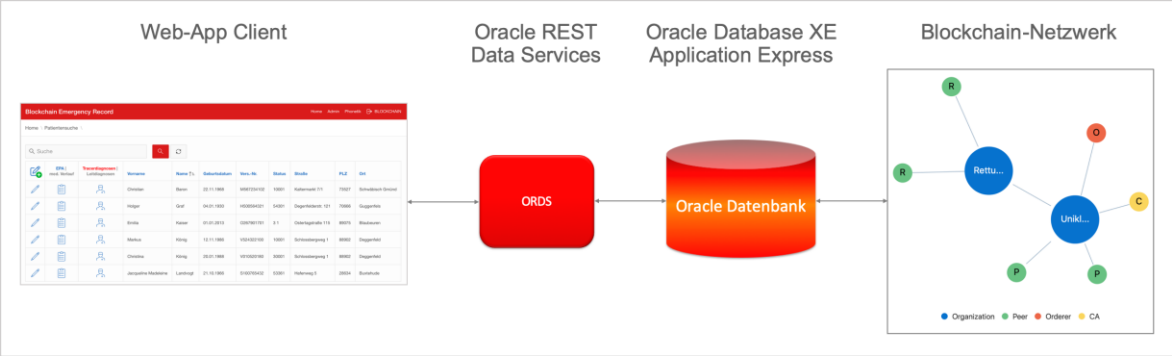


Abbildung 5: Komponenten und Architektur der entwickelten Applikation mit REST-Zugriff auf die Blockchain
REST = Representational State Transfer

2.3.1 Blockchain-Definition und Konfiguration

Neben der fachlichen Untersuchung, ob und wie die Blockchain-Technologie das Gesundheitswesen verbessert, sind für die Applikationsentwicklung unterschiedliche Kenntnisse erforderlich, die in diesem Abschnitt erörtert werden.

Am Anfang des Projekts steht das Design der Blockchain, d.h. welche Personen, Gruppen oder Organisationen werden an der Lösung partizipieren. Ist dies geklärt, kann das Blockchain-Netzwerk über die in Abschnitt 2.4 dargestellten Administrationsmöglichkeiten definiert werden. Für die Administration der Blockchain wird nur ein Web-Browser, z.B. Firefox, benötigt. Ist die Konfiguration abgeschlossen, ist es notwendig die fachliche Logik in den Programmiersprachen Go, Java, JavaScript etc. zu programmieren.

Die Abbildung 6 zeigt die Architektur der verwendeten Blockchain-Plattform und deren Komponenten.

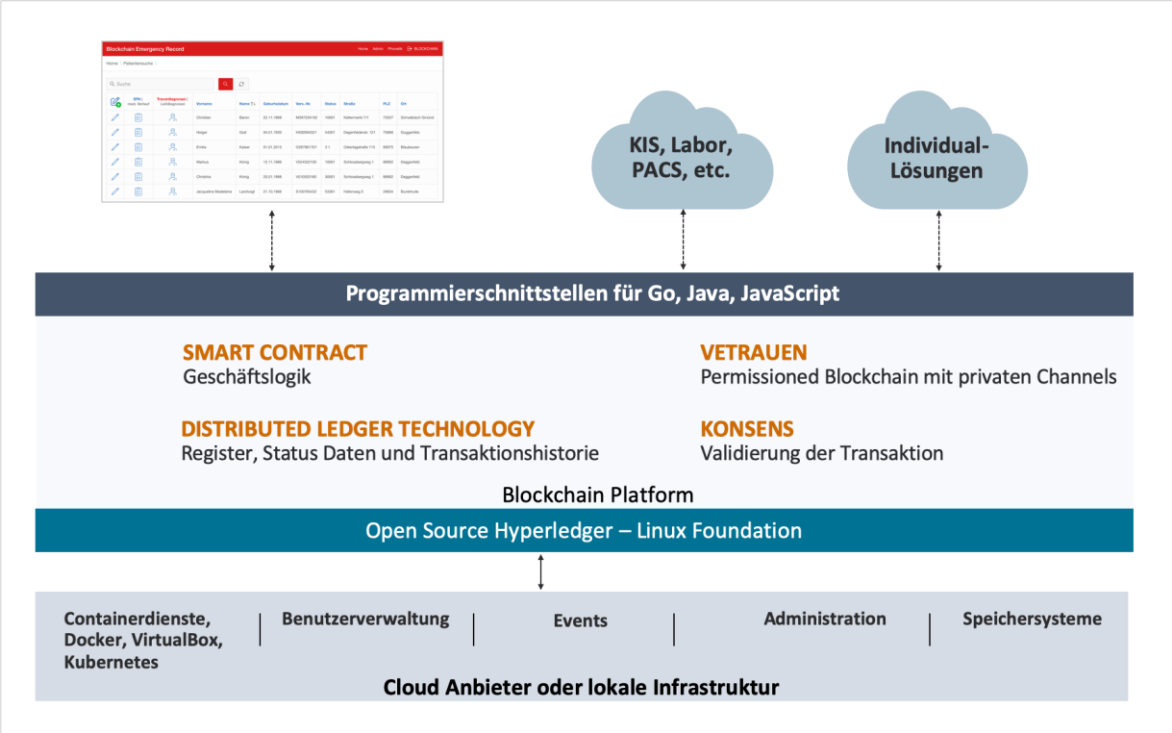


Abbildung 6: Oracle Blockchain-Plattform Architektur

KIS = Krankenhausinformationssystem / PACS = Picture Archiving and Communication System

Die Architektur basiert auf der Referenzimplementierung der Open Source Linux Foundation® [53]. Damit wird sichergestellt, dass Standards eingehalten werden und Interoperabilität zwischen den unterschiedlichen Blockchain-Implementierungen möglich ist. Den Vorgaben entsprechend sind dennoch Freiheitsgrade für die Nutzung von eigenen Komponenten und Lösungen der Softwarehersteller möglich. Diese werden in Form von Docker Containern zur Verfügung gestellt. Bei Docker handelt es sich um eine plattformunabhängige Virtualisierungslösung, die in das Betriebssystem integriert ist und dessen Ressourcen sehr effizient nutzt. Als Basis dient der von „The Linux Foundation® Projects“ der „Open Container Initiative“ definierte Standard (Quelle: https://www.opencontainers.org/). Alle administrativen Aufgaben in Hinblick auf die genutzten Funktionen der Oracle Blockchain sind in der Oracle® Cloud Dokumentation „Administering Oracle Blockchain Platform“ [43] enthalten. Die Blockchain mit allen oben aufgeführten Softwarekomponenten laufen für Entwicklung und Test in einer virtuellen Umgebung als Oracle VirtualBox VM Image.

Sie stellt eine nahezu identische Infrastruktur dar, wie die von der Oracle Corporation angebotene Blockchain Plattform in der Cloud.

In diesem Zusammenhang ist es sinnvoll, auf die Kernkomponenten der Architektur näher einzugehen, die folgende Bestandteile und Rollen auszeichnen:

- **Applikationen**
  In der Regel sind dies Web-Applikationen, die über eine URL (Uniform Resource Locator) aufgerufen werden. Diese wiederum rufen über die REST-API (Representational State Transfer – Application Programming Interface) der Blockchain die Funktionen des Chaincodes auf, um Transaktionen auszuführen und ggf. Patienteninformationen einzupflegen, abzufragen und zu verteilen. Im Hintergrund wird eine Vielzahl von Prozessschritten ausgelöst, die die Performance und damit Skalierbarkeit des Systems beeinflussen. Im umgesetzten Beispiel wurde hierfür APEX (Oracle Application Express) genutzt, um mittels Datenbankroutinen die Funktionen des Chaincodes aufzurufen.

- **Smart Contracts / Chaincodes**
  Diese Programme bilden die fachlichen Anforderungen in Form von modularen Funktionen ab. Die Blockchain wird ausschließlich durch die Methoden verändert und verwaltet. Die durch den Chaincode ausgeführten Transaktionen werden mitprotokolliert (Historie) und die Werte unveränderbar, transparent und nachvollziehbar gespeichert. Die Werte und Transaktionen werden in einem Key-/Value-Store, der als NoSQL-Datenbank (Not only SQL, https://de.wikipedia.org/wiki/NoSQL) bezeichnet wird, gespeichert. Die Technologie wird beispielsweise beim größten Internethändler eingesetzt, um auf Basis von getätigten Verkäufen weitere Empfehlungen vorzuschlagen.

- **Blockchain Infrastruktur**
  Die Blockchain Infrastruktur besteht aus dem Blockchain-Netzwerk. Alle Teilnehmer sind gleichberechtigt und können auf die Blockchain zugreifen bzw. Funktionen nutzen. Das zugehörige IT-Netzwerk besteht weiterhin aus Ressourcen, die Rechenleistung zur Verfügung stellen.

Die Nodes sind für die Validierung der Transaktionen verantwortlich und verwalten das verteilte „Kassenbuch“ (Register) inklusive Smart Contract dezentral. Die Datenhaltung wird in der Literatur auch als Distributed Ledger Technology (DLT) oder Shared Ledger Database bezeichnet (Quelle: https://www.hyperledger.org/projects/fabric).

In der Regel wird bei einer privaten Blockchain noch eine Benutzerverwaltung benötigt, die die Zugriffberechtigungen verwaltet, z.B. Patientennummern und Ärztekennungen. Dabei wird die digitale Identität mit den Informationen (Metainformationen) aus vorhandenen KIS-Systemen ergänzt. In der Dissertation wurde dieser Punkt nicht betrachtet, wird aber im Diskussionsteil (Kapitel 4) angesprochen.

Um eine Einigung über die Gültigkeit der Transaktion im Blockchain-Netzwerk zu erreichen, wird ein Konsens-Protokoll in folgenden drei Phasen abgearbeitet:

1. **Endorsement:** Entscheidet, ob eine Transaktion akzeptiert (accept) oder abgelehnt (reject) wird; simuliert die Transaktion gewissermaßen. Im entwickelten Beispiel agieren das Uniklinikum, der Patient und die Ärzte als sogenannte „Peers“ (Abb. 24), um die Richtigkeit der Transaktion zu bestätigen.

2. **Ordering:** Dieser Prozessschritt bringt alle Transaktionen in die richtige zeitliche Reihenfolge im Block.

3. **Validation:** Verifiziert, ob die im Endorsement festgelegten Regeln (Policies) eingehalten wurden und setzt die Transaktion im positiven Fall auf valide.

Private Blockchain-Netzwerke werden häufig als **„Konsortium“** oder **„hybride“-**Blockchain bezeichnet. Nicht zu verwechseln mit dem hybriden Ansatz, der in der Dissertation in Verbindung mit Datenbank und Blockchain gewählt wurde.

2.3.2 Go-Programmierung des Smart Contracts / Chaincode

Für die Programmierung des Quellcodes wurde die Programmiersprache „Go“ genutzt. Dabei handelt es sich um eine objektorientierte Programmiersprache. Diese wurde aufgrund der zur Blockchain passenden Schnittstelle ausgewählt. Für die Entwicklung der fachlichen Logik, wie z.B. „Übertragung des Behandlungsrechts“ oder einer Suchfunktion wurden jeweils Methoden und eine Struktur entworfen, die zum Anwendungsfall passen. Die Entwicklung der Go-Methoden und Strukturen die später mit der Blockchain arbeiten, fand mit Microsoft Visual Studio Code statt. Die fachliche Grundlage für einen „Vertrag“ zwischen zwei Parteien, z.B. Arzt und Patient oder Arzt und Arzt, ist der „Smart Contract“ im Folgenden auch „Chaincode“ genannt. Für die Entwicklung des Go-Codes wurde ein Referenzbeispiel der Oracle Corporation herangezogen, welches beim Blockchain SDK (Software Development Kit) enthalten ist. Die Weiterentwicklung besteht in der neu entwickelten „readPatienten“-Methode, die als zentrale Komponente für die Abfrage der Blockchain genutzt wird.

2.3.3 Oracle XE Datenbank

Die Oracle XE Datenbank ist für die Verwaltung der Stammdaten, Abspeicherung der Befunde, Protokolle, radiologischem Bildmaterial, und die prozedurale SQL-Entwicklung (PL/SQL) verantwortlich. Sie dient zusätzlich als Repository für APEX und das physische Datenbank-Modell. Der Zugriff auf die REST-Schnittstelle der Blockchain wurde über die Datenbank mittels PL/SQL-Aufruf realisiert.

2.3.4 Datenbankmodell

Für den hybriden Ansatz wird ein relationales Datenbankmodell benötigt. Das Design wurde mit Hilfe des Oracle SQL Developers erstellt. Dabei handelt es sich um ein „Entity-/Relationship“-Modell (E-/R-Modell), in dem Tabellen über Schlüssel miteinander verbunden sind und in einer 1:1 oder 1:n Beziehung stehen. Die Definition des Modells erfolgt über sogenannte Data Definition Language Befehle (DDL). Das SQL-Skript für die Erstellung der Tabellen und Indizes wird in Kapitel 3 besprochen und erläutert. Diese Skripte liegen im Original der Dissertation bei.

2.3.5 PL-SQL-Programmierung (Prozedurale Structured Query Language)

Für die Umrechnung von Zeitstempel der Blockchain in das übliche mitteleuropäische Zeitformat (DD.MM.YYYY, HH24:MI:SS) wird eine Datenbankroutine benötigt. Die Blockchain speichert Zeit als numerischen Wert (z.B. 192412800) ab, der sich jedoch auf die sogenannte Linux-Zeit (01.01.1970), bezieht. Das hat zur Folge, dass die aktuelle Zeit immer in eine numerische Zahl in Sekunden umgerechnet werden muss, die seit ’01.01.1970‘ vergangen sind. Für die Patientensuche wurde eine Volltextrecherche mit SQL- und PL/SQL entwickelt und um eine phonetische Suche erweitert [10]. Für die Programmierung wurde der Oracle SQL Developer und Application Express (APEX) genutzt.

2.3.6 Oracle REST Data Services

Als Web- und Applikations-Server kam Oracle REST Data Services (ORDS) zum Einsatz. Dieser wird benötigt, um eine Verbindung zur Datenbank herzustellen und die von der Blockchain gelieferten Daten (Diagnosen, Therapien, ICD) an die Webapplikation auszuliefern. Der ORDS bildet die technische Ablaufumgebung für APEX und ist auf Basis von JAVA entwickelt worden. Der ORDS wird konfiguriert und läuft in der Java-Runtime Umgebung (JRE) des Betriebssystems ab. Für den automatischen Start und Stoppen des ORDS werden Betriebssystembefehle bereitgestellt.

2.3.7 Oracle Application Express (APEX)

Für die Entwicklung der Web-Anwendung, wie z.B. Formulare, Berichte, Prozesse, Navigation und Logik wurde Oracle Application Express genutzt. Dabei handelt es sich um eine deklarative Entwicklungsumgebung, um schnell Anwendungen ohne tiefe Programmierkenntnisse zu erstellen. Im umgesetzten Beispiel wurden viele Anpassungen und Eigenentwicklungen auf Basis der BLOG’s implementiert, um die vorhandene Standardfunktionalität zu erweitern.

2.3.8 Oracle Linux Betriebssystem / Oracle VirtualBox VM

Das Oracle Linux Betriebssystem ist Teil der Oracle VirtualBox VM, in der alle für die Dissertation notwendigen Komponenten installiert sind. Die VirtualBox VM stellt die gesamte Ablaufumgebung zur Verfügung.

Um vom Host Betriebssystem (z.B. macOS) auf die Umgebung der VirtualBox zuzugreifen, muss in den Netzwerkeinstellungen ein „Port Forwarding“ (Weiterleitung) eingerichtet sein, wie in Abbildung 7 dargestellt ist.

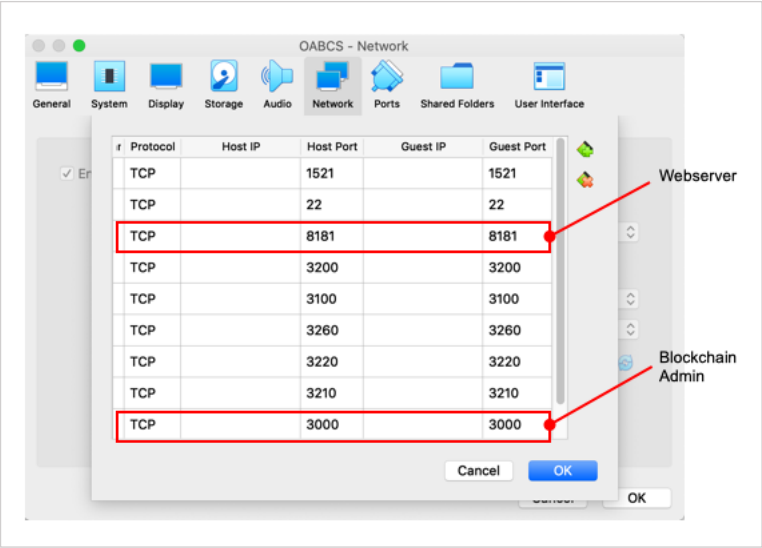


Abbildung 7: Port Forwarding Einstellungen des VirtualBox Netzwerks
TCP = Transmission Control Protocol / IP = Internet Protocol

Die Anwendung wurde im Vorfeld zu Demozwecken in die Public Cloud-Lösung von Oracle installiert und getestet. Für diesen Zweck sieht die Oracle VirtualBox die Möglichkeit eines Exports der lokalen VM in die Infrastruktur, bestehend aus CPU, Hauptspeicher, Storage und Netzwerk vor.

Um dies zu ermöglichen, müssen sicherheitsrelevante Informationen in das Formular für die Zielplattform (z.B. Oracle Cloud) eingegeben werden, wie Abbildung 8 darstellt. Diese Umgebung wurde später für funktionale Tests genutzt und hat die Anforderungen erfüllt.

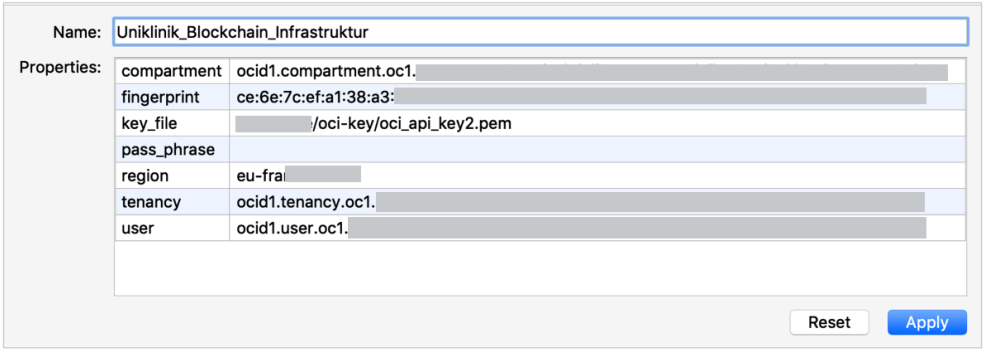


Abbildung 8: Sicherheitsinformationen beim Export der VirtualBox in die Oracle Cloud Infrastruktur

2.4 Versuchsaufbau

Für den Nachweis der Ergebnisse werden im Wesentlichen folgende Kernkomponenten (Abb. 3) benötigt:

1. Blockchain SDK als Oracle VirtualBox VM
2. Oracle Datenbank XE
3. Oracle Application Express
4. Oracle REST Data Services

2.4.1 Blockchain-Netzwerk (SDK - Software Development Kit)

Wie bereits erwähnt, ist die Architektur eines Blockchain-Netzwerks dezentral. Das im Versuchsaufbau entwickelte Netzwerk hat einen Gründer (engl. Founder) und Teilnehmer (engl. Participants) bzw. Organisationen, die in diesem Fall identisch sind. Da in einem P2P-Netzwerk gearbeitet wird, müssen entsprechende Kommunikationskanäle (Ports) definiert werden. Damit wird sichergestellt, dass alle am Blockchain-Netzwerk beteiligten Nodes untereinander kommunizieren können, auf ein Ereignis reagieren und das Konsens-Protokoll abgearbeitet werden kann. Der Founder (dt. Gründer) des Blockchain-Netzwerks ist das Universitätsklinikum Ulm. In der virtuellen Umgebung sind die Benutzer „bcdemo“ und „oracle“ eingerichtet, mit der eine Anmeldung nach dem Start möglich ist. Die Nutzung und Entwicklung von Blockchain-Anwendungen ist in der Oracle Dokumentation [44] beschrieben.

Folgende Schritte sind für die Nachvollziehbarkeit der Dissertation und der damit verbundenen Ergebnisse notwendig:

Schritt 1: **Terminal** in der VirtualBox Umgebung öffnen (Anmeldung als bcdemo-User)

Schritt 2: **Bereitstellung** der Blockchain Administrationsoberfläche, über die das Blockchain-Netzwerk verwaltet wird.

Nachfolgend sind Kommandos aufgeführt, die die Verwaltung des Blockchain-Netzwerks betreffen. Mit folgendem Betriebssystemaufruf werden die für die Administration benötigten Umgebungskomponenten (Abb. 9) gestartet:

Betriebssystem-Kommando: **sudo /oracle_fabric/startProvisioning.sh**

```
[bcsdemo@oabcs-vm ~]$ sudo /oracle_fabric/startProvision.sh
No input parameter, will use default settings
Starting Provision...
docker run -it --network=host -e PROVISION_PORT=3000 -e "BCS_DOCKER_WORKSPACE=/root/obcs_workspace" -e "VM_HOST
NAME=oabcs-vm" -v /var/run:/var/run -v /root/obcs_workspace:/root/obcs_workspace -d oracle/obcs-provision
ae16159542b8759285a38effe1b082def2fdcb33dc8844a0529f93ede8d7cef2
```

Abbildung 9: Starten der Blockchain-Administrationsumgebung

Eine Kontrolle auf Betriebssystem-Ebene mittels „docker“-Befehlen (Abb. 10) ergibt folgende Ausgabe:

```
[bcsdemo@oabcs-vm ~]$ docker ps --format 'table {{.Names}}\\t{{.Image}}\\t{{.RunningFor}}\\t{{.Status}}\\t{{.Command}}'
NAMES\                          IMAGE\                          CREATED\          STATUS\           COMMAND
adminulmde_fabricca0.ulm.de_1\  hyperledger/fabric-ca\         2 hours ago\      Up 2 minutes\     "sh -c 'fabric-ca-se…"
adminulmde_gateway0.ulm.de_1\   oracle/obcs-gateway\          2 hours ago\      Up 2 minutes\     "/root/init.sh"
adminulmde_peer0.ulm.de_1\      hyperledger/fabric-peer\      2 hours ago\      Up 2 minutes\     "peer node start"
adminulmde_orderer.ulm.de_1\    hyperledger/fabric-orderer\   2 hours ago\      Up 2 minutes\     "orderer"
adminulmde_peer1.ulm.de_1\      hyperledger/fabric-peer\      2 hours ago\      Up 2 minutes\     "peer node start"
adminulmde_bcs1console_1\       oracle/obcs-console\          2 hours ago\      Up 2 minutes\     "sh -c /home/oracle/…"
admiring_khayyam\               oracle/obcs-provision\        6 hours ago\      Up 6 hours\       "/root/init.sh"
```

Abbildung 10: Ausgabe der gestarteten Docker Container der Admin Blockchain

Schritt 3:

Aufbau des Blockchain-Netzwerks

Für die Administration der Blockchain ist folgende URL in den Browser (Abb. 11) einzugeben:

http://oabcs-vm:3000 oder **http://192.168.56.101:3000**

Username: admin

Password: admin

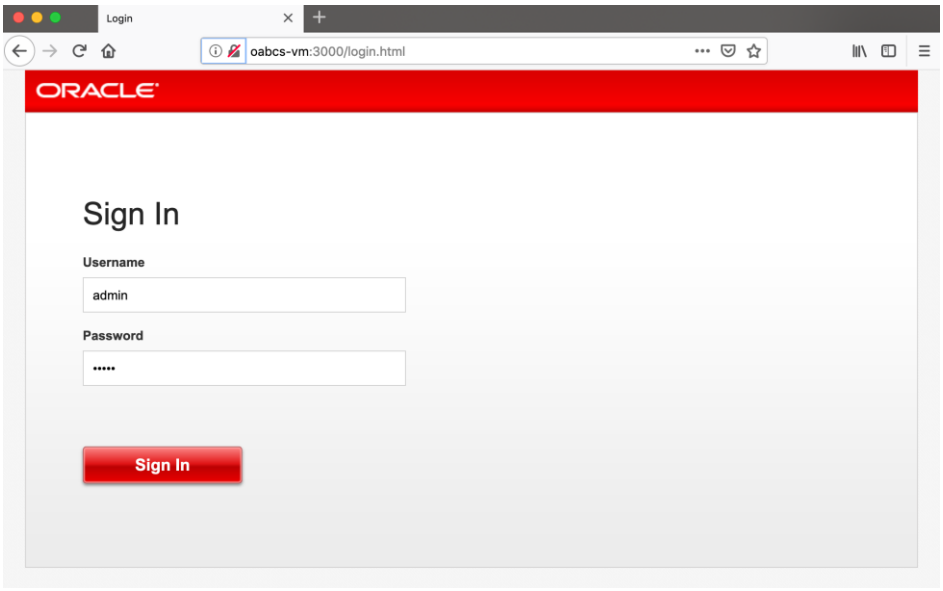


Abbildung 11: Anmeldung an der Blockchain-Administrationskonsole - „Copyright Oracle and its affiliates. Used with permission.“

Nach dem Aufruf erscheint die Login Maske (Abb. 11), um das Netzwerk aufzubauen und administrative Tätigkeiten durchzuführen. Falls die Maske nicht sichtbar ist, sollten die Einstellungen der Firewall (Regeln) bzw. Virusscanner des Host-Systems kontrolliert und ggf. angepasst werden.

Im Folgenden wird das Blockchain-Netzwerk und die teilnehmenden Organisationen (Participants), gemäß der Tabelleninformationen (Abb. 12) erstellt. Die nachträglich aufgebaute Labor-Blockchain ist in der Tabelle nicht berücksichtig.

	Uniklinik	Rettungsdienst	Facharzt	Hausarzt	Patient	Apotheke
Doamin	ulm.de	rettung.de	radiologie.de	hausarzt.de	patienten.de	apotheke.de
Rolle	Founder	Participant	Participant	Participant	Participant	Participant
Anzahl Peers (Nodes)	2	2	2	2	2	2
Server Name bzw. IP	oabcs-vm	oabcs-vm	oabcs-vm	oabcs-vm	oabcs-vm	oabcs-vm
REST Gateway Port	3100	3110	3120	3130	3140	3150
Console Port	3200	3210	3220	3230	3240	3250
Orderer Type	Solo	-	-	-	-	-
Orderer Port	7000	-	-	-	-	-
Channel	new1channel	new1channel	new1channel	new1channel	new1channel	new1channel

Abbildung 12: Setup des Blockchain-Netzwerks

Bei den Organisationsbezeichnungen gibt es keine Vorschriften. In der Regel wird ein sprechender Name (Abb. 13) vergeben, der den fachlichen Anwendungsfall repräsentiert.

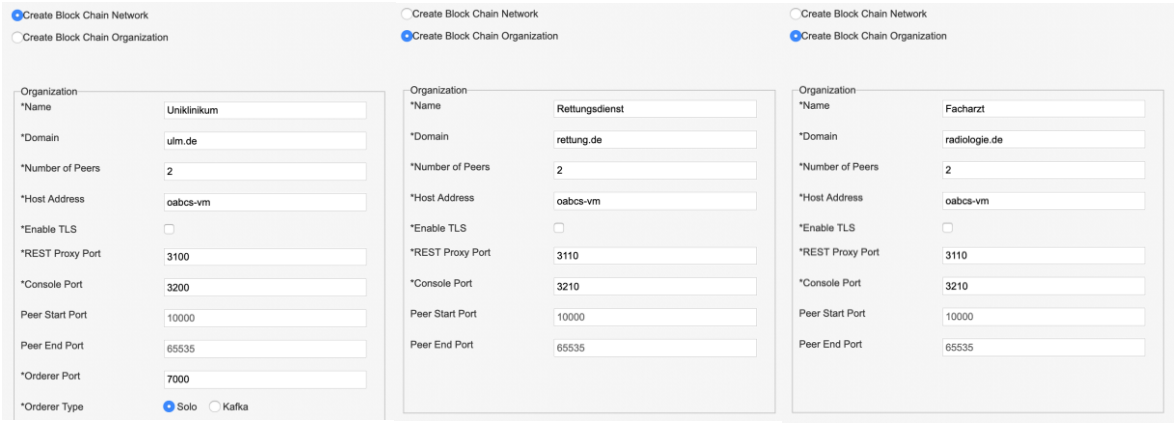


Abbildung 13: Founder und Participants des Blockchain-Netzwerks

Das Blockchain-Netzwerk und die damit verbundenen Organisationen lassen sich mit Hilfe der Administration einzeln starten, stoppen und löschen (Abb. 14). Für ein Blockchain-Netzwerk muss zusätzlich zum Founder mindestens eine weitere Organisation angelegt und gestartet sein.

Nach dem Erstellen des Blockchain-Netzwerks steht sofort die Möglichkeit der Administration der einzelnen Komponenten zur Verfügung. Zusätzlich wurde eine Blockchain für Laborwerte nach dem gleichen Prinzip erstellt, um einen optionalen Anwendungsfall mit einem „privaten“-Bereich zwischen Universitätsklinikum und Labor abzubilden. Dies wurde als Applikationsteil in der APEX Applikation nicht verwirklicht.

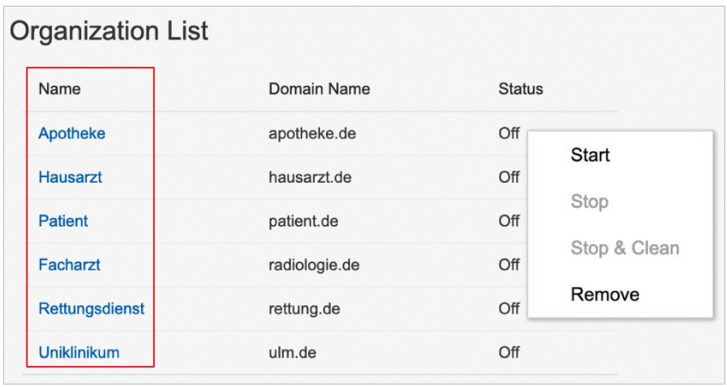


Abbildung 14: Alphabetische Darstellung der Blockchain-Organisationen

Es lässt sich in Abbildung 15 erkennen, dass der erste Block der Blockchain (Genesis) auf dem Founder Knoten angelegt wurde.

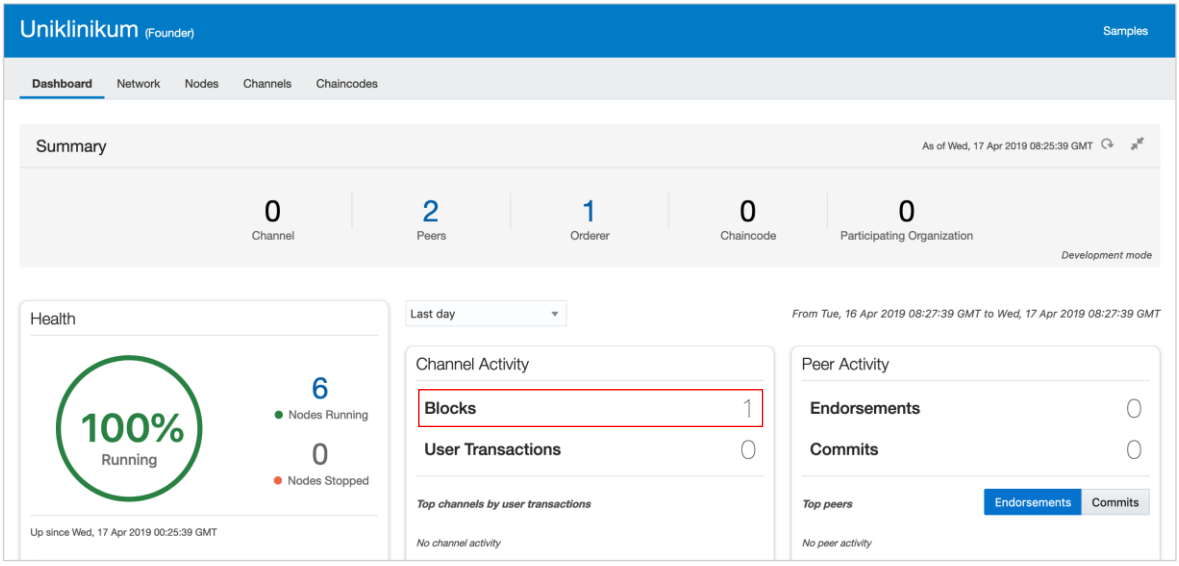


Abbildung 15: Administration der Blockchain mit Genesis Block 1 - „Copyright Oracle and its affiliates. Used with permission.“

Bei der in der Dissertation genutzten Hyperledger-Fabric (HLF) Implementierung handelt es sich um eine sogenannte „Permissioned“-Blockchain. Dies bedeutet, dass alle Teilnehmer als Benutzer oder Organisation bekannt sind.

Im anderen Fall wird von einer Zertifizierungsstelle „Certified Authority (CA)“ ein digitales Zertifikat ausgestellt, welches den Benutzer eindeutig identifiziert. Oftmals sind dies im behördlichen Umfeld staatliche Stellen (z.B. Estland) [39], die als CA auftreten. Beispielsweise könnte die Bundesanstalt für Arbeit (BA), das Bundesamt für Migration und Flüchtlinge (BAMF) oder eine staatlich zertifizierte medizinische Stelle eine derartige Funktion übernehmen. In der Industrie werden die Geschäftspartner entweder in eine Benutzerverwaltung aufgenommen und als Teilnehmer geführt oder erhalten für die Dauer der Geschäftsbeziehung ein Zertifikat. Mit der Oracle VirtualBox VM wird die CA simuliert. Die ausgestellten Zertifikate sollten nur für Tests, Demos oder „Proof of Concepts“ genutzt werden.

Schritt 4:

Export Founder Orderer Settings

Um die Kommunikation und die Reihenfolge der Transaktionen im Block zu garantieren, wird die „Orderer“ Einstellung der Founders exportiert (Abb. 16) und später in allen Organisationen auf den dezentralen Knoten importiert. Hierfür wird der [Network] Tab ausgewählt und aus dem „Hamburger“ Menü der Menüpunkt „Export Orderer Settings“ ausgewählt. Der Founder (Gründer) benötigt darüber hinaus die Information über das Zertifikat, um die Kommunikation zu validieren und die Namen der teilnehmenden Peer-Nodes, die von den jeweiligen Organisationen verwaltet werden.

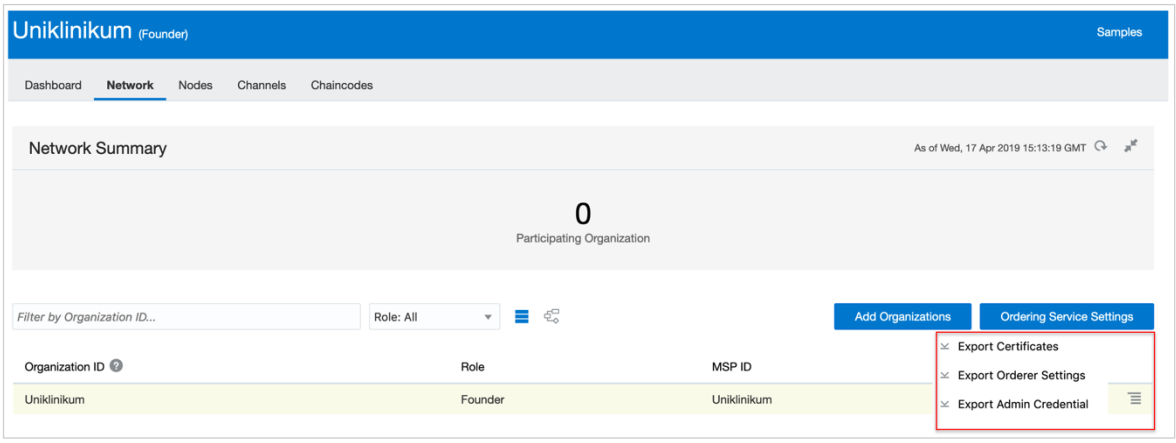


Abbildung 16: Export der Orderer Settings des Founders als JSON-Dokument: Uniklinikum_orderer_settings.json
JSON = JavaScript Object Notation

Schritt 5:

Export der Zertifikate der Participants / Import der Orderer Settings

Im beschriebenen Anwendungsfall werden im nächsten Schritt die digitalen Zertifikate, die von der Oracle Blockchain-Plattform als selbstsignierte Zertifikate ausgestellt wurden, mit dem Universitätsklinikum ausgetauscht. Dies ist dann sinnvoll, wenn mehrere Ärzte interdisziplinär an einem Patientenfall diagnostizieren, Therapien erarbeiten und die Behandlung dokumentieren möchten. Im vorliegenden Beispiel wird zunächst ein Zertifikat des Facharztes in Form eines JSON-Dokuments (JavaScript Object Notation) exportiert und die Einstellungen des Founders bezogen auf den Orderer Port importiert (Abb. 17).

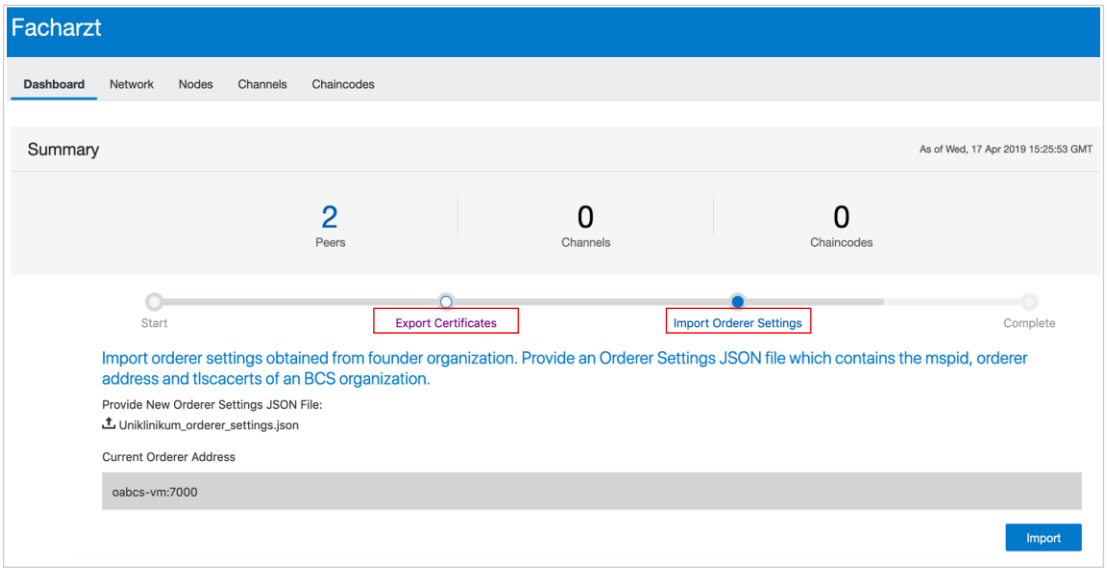


Abbildung 17: Export des Zertifikates als JSON-Dokument: Facharzt_certificates.json

JSON = JavaScript Object Notation

Die an der Blockchain teilnehmenden Personen, z.B. ein Facharzt werden wie bereits erwähnt in Form eines digitalen Zertifikates repräsentiert und verwaltet (Abb. 18).


```
{
"mspid": "Facharzt",
"certs": {
"admincerts": "-----BEGIN CERTIFICATE-----
\nMIICDzCCAbagAwIBAgIQJIHl6LsBoqczXgFHrqDouTAKBggqhkjOPQQDAjBtMQsw\nCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEWMBQGA1UEBxMNU2FuIEZy
\nYW5jaXNjbzEWMBQGA1UEChMNcmFkaW9sb2dpZS5kZTEZMBcGA1UEAxMQY2EucmFk\naW9sb2dpZS5kZTAeFw0xOTA1MDcxNzI0MzZaFw0yOTA1MDQxNzI0MzZaMFgxCzAJ
\nBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQHEw1TYW4gRnJh\nbmNpc2NvMRwwGgYDVQQDDBNBZG1pbkByYWRpb2xvZ2llLmRlMFkwEwYHKoZIzj0C
\nAQYIKoZIzj0DAQcDQgAESedfIKwA9gMb1Fgp+VGQ+0p2hv8rKgvtp6riCTxaR4ms\n+E/vgH1VST41Q1DDSL7Jt4m07yU8M7vsfY6C6CBbRKNNMEswDgYDVR0PAQH/BAQD
\nAgeAMAwGA1UdEwEB/wQCMAAwKwYDVR0jBCQwIoAg1bcb9gYEakltKUX6YOb0vpHW\nJTFRmSaLEruJt6exqN0wCgYIKoZIzj0EAwIDRwAwRAIgHog5yZXgVy68VCVPmoeA
\ns7tdhKkqtUy2VSHFhDniOHECIGAlCVTfTHTpaZGfp2j++xLykIDiH/ZyaGYPx9ua\n2Yjf\n
-----END CERTIFICATE-----\n",
"cacerts": "-----BEGIN CERTIFICATE-----
\nMIICNzCCAd2gAwIBAgIQTjsY0eivlhDEiY9dRtKe6zAKBggqhkjOPQQDAjBtMQsw\nCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEWMBQGA1UEBxMNU2FuIEZy
\nYW5jaXNjbzEWMBQGA1UEChMNcmFkaW9sb2dpZS5kZTEZMBcGA1UEAxMQY2EucmFk\naW9sb2dpZS5kZTAeFw0xOTA1MDcxNzI0MzZaFw0yOTA1MDQxNzI0MzZaMG0xCzAJ
\nBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQHEw1yYWRpb2xvZ2llLmRlMRkwFwYDVQQDExBjYS5yYWRp
\nb2xvZ2llLmRlMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEdC/2x7VW6tnjGG7G\n4vs/DJhrKYM5fqldEabP6MEQ01VISTpQC/YYz3RPqiMd2VcZuSBLvFZbJr/4Pswr
\n2XPvvaNfMF0wDgYDVR0PAQH/BAQDAgGmMA8GA1UdJQQIMAYGBFUdJQAwDwYDVR0T\nAQH/BAUwAwEB/zApBgNVHQ4EIgQg1bcb9gYEakltKUX6YOb0vpHWJTFRmSaLEruJ
\nt6exqN0wCgYIKoZIzj0EAwIDSAAwRQIhAOU9lE3+G/SH2Cza29g9/pgiZX+9VjJJ\naWljTWVC7EV9AiBoqYhVpmkdeTMDvTcplJ5tCCmlsVxUUjM44xi1Hh2GmA
==\n-----END CERTIFICATE-----\n"
}
}
```


Abbildung 18: Exportiertes Zertifikat des Facharztes

Nach Abschluss der Konfiguration erscheint das Dashboard des Participants. Im Unterschied zum Founder wurde noch kein Block angelegt (Abb. 19).

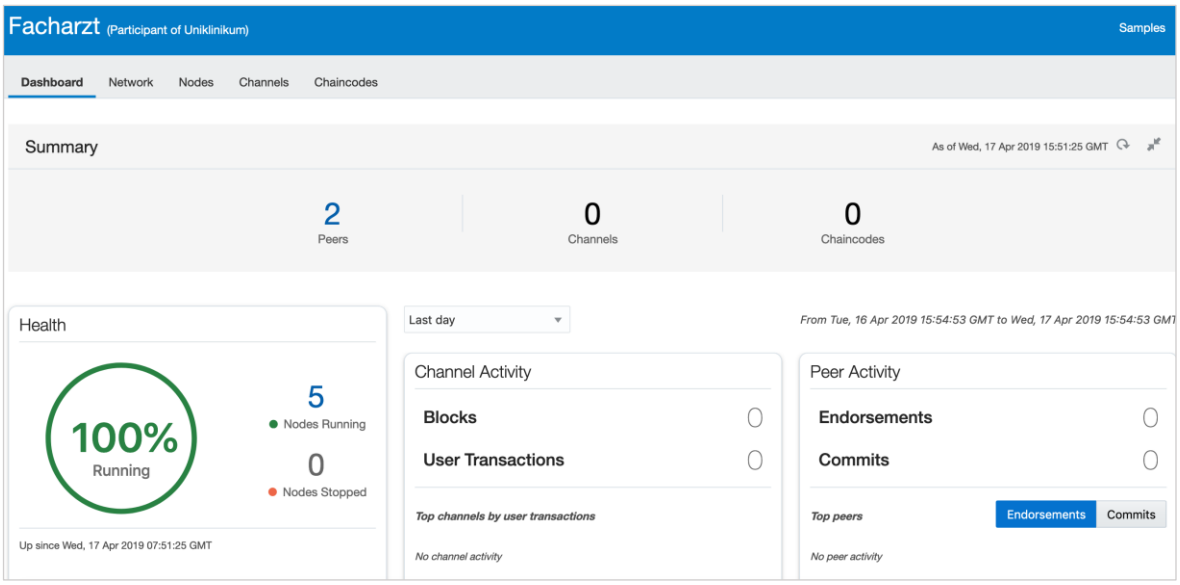


Abbildung 19: Dashboard des Blockchain-Netzwerk Teilnehmers

Schritt 6:

Teilnehmer in das Blockchain-Netzwerk aufnehmen

Im vorigen Schritt wurden die Zertifikate von den Organisationen (Teilnehmern) exportiert. Diese können nun in das Netzwerk des Gründers aufgenommen werden. Im [Network] Tab wird der Button „Organizations“ ausgewählt und alle Zertifikate über den [Add] Button importiert. Die Zertifikate liegen auf dem Filesystem des Blockchain-Administrators und werden hochgeladen (Abb. 20).

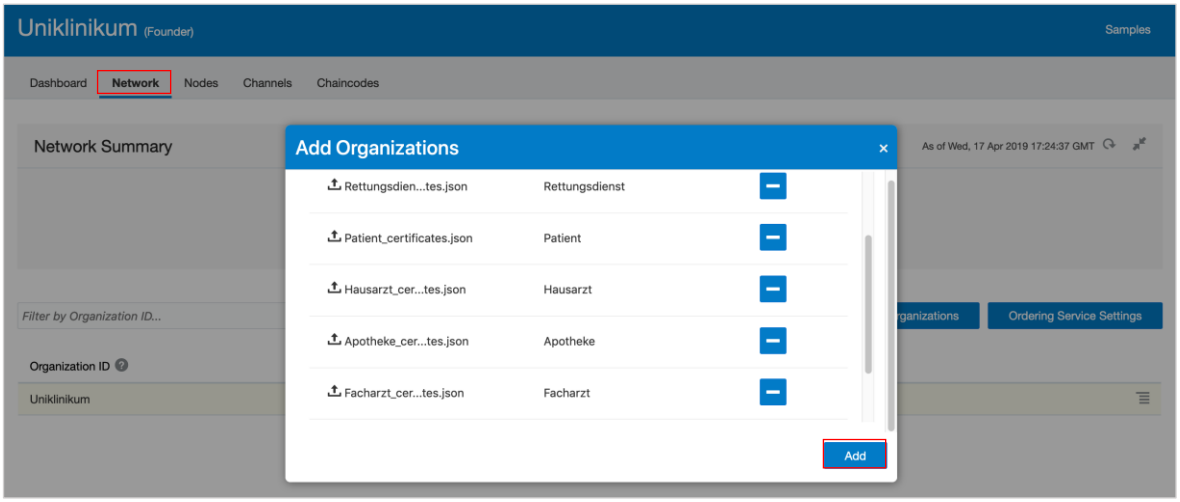


Abbildung 20: Teilnehmer in das Blockchain-Netzwerk aufnehmen

Nach dem Hinzufügen der teilnehmenden Organisationen stellt sich das Blockchain-Netzwerk (Abb. 21) wie abgebildet dar. Mit Hilfe des Browsers kann diese Grafik mit folgendem Link abgerufen werden:

URL: **http://192.168.56.101:3200/?root=network**

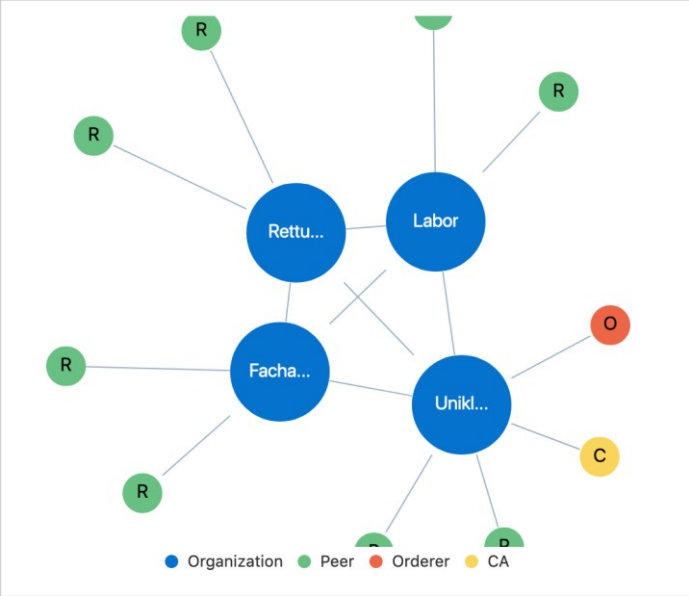


Abbildung 21: Vereinfachte Blockchain-Netzwerk Struktur als Vorstudie

In diesem Fall kann jeder Teilnehmer mit allen anderen Teilnehmern kommunizieren. Der Facharzt, das Universitätsklinikum, der Rettungsdienst, das Labor und der Patient sind im Netzwerk gleichberechtigt und können sensible Patientendaten verwalten und freigeben. Dies setzt natürlich ein technisches und prozessorientiertes Denken sowie Klarheit über die Nutzung beim Patienten und den beteiligten Organisationen voraus.

Schritt 7:

Channel erstellen

Der Channel bietet die Möglichkeit einer direkten 1:1 Kommunikation zwischen den Teilnehmern eines Blockchain-Netzwerks. Beispielsweise darf der Hausarzt auf alle Diagnosen und Therapien des Patienten zugreifen, während der Facharzt nur auf einen ganz bestimmten Ausschnitt der kompletten Behandlungshistorie des Patienten Zugriff erhält (private Blockchain). Jeder Channel (Kanal) stellt eine

unabhängige Blockchain dar. Um den Komplexitätsgrad zu reduzieren, kommunizieren Patienten, Ärzte etc. im untersuchten Fall über den gleichen Channel (private Blockchain). Die Bezeichnung unterliegt keinen Vorgaben. In der Praxis sollte jedoch ein sich selbst erklärender Name vergeben werden. An dieser Stelle werden die durch den Membership Service Identification (MSPID) zugelassenen Organisationen mit der notwendigen Access Control List (ACL) für die Blockchain berechtigt. Nach dem erfolgreichen Submit sind die Nodes dem Founder bekannt (Abb. 22).

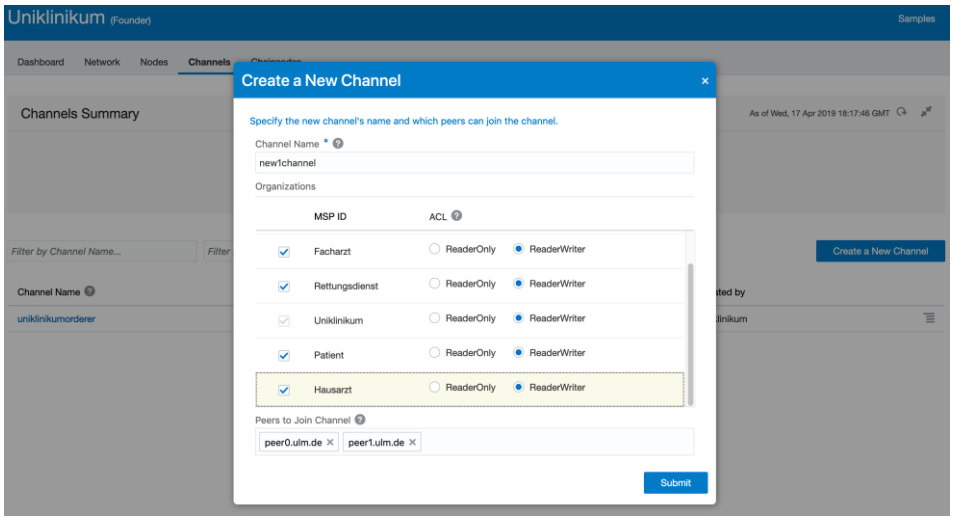


Abbildung 22: Channel im Founder erstellen

Die Peers der teilnehmenden Organisationen müssen anschließend dem erstellten Channel von ihrer Seite aus beitreten (join). Diesen Schritt müssen alle Teilnehmer durchführen. Im „Hamburger“ Menü des Participants den [Nodes] Tab auswählen und den Menüpunkt „Join New Channels“ anklicken (Abb. 23).

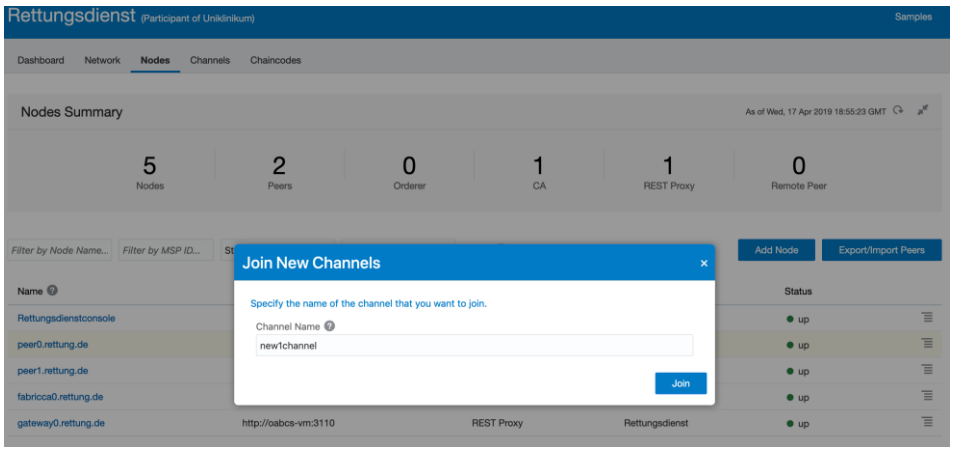


Abbildung 23: Nodes des Rettungsdienstes joinen den erstellten Channel

Sind dem Channel alle beteiligten Organisationen beigetreten, können diese über den definierten „new1channel“ (Abb. 24) kommunizieren.

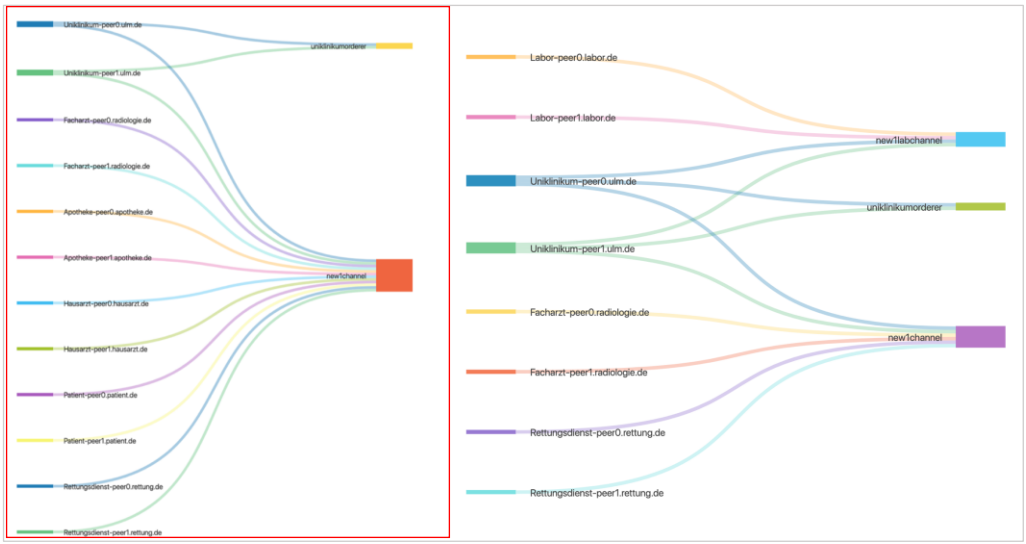


Abbildung 24: Blockchain-Netzwerk Kommunikation über den new1channel oder über new1labchannel

Das Blockchain-Netzwerk ist komplett. Die Organisationen sind beigetreten. Der Genesis Block des Founders ist nun auf allen Knoten des Netzwerks kopiert worden und liegt verschlüsselt im Filesystem. Ab diesem Zeitpunkt kann das Blockchain-Netzwerk administriert und die REST-Schnittstelle (Abb. 25) getestet werden. Ein einfaches Beispiel zeigt, wie auf der Kommandozeile des Betriebssystems eine URL eingegeben werden kann, um die Version des Gateways abzufragen und auf Funktion zu testen. Alle REST-Endpunkte sind in der Oracle Dokumentation [8] enthalten.

Beispiel für Testaufruf

```
curl -H "Content-type:application/json" -X GET http://oabcs-vm:3100/bcsgw/rest/version
```

Abbildung 25: Aufruf der REST-Schnittstelle der Blockchain und Abfrage des Versionsstandes
REST = Representational State Transfer

Schritt 8:

Export Nodes der Participants

Im nächsten Schritt erfolgt der Export mit den jeweiligen Nodes Informationen, d.h. der Teilnehmer. Hierzu muss der [Nodes] Tab auf der Konsole der teilnehmenden Organisationen ausgewählt und die Node-Information exportiert werden. Aufgrund von Verfügbarkeit sollten auf jeden Fall pro Node mindestens zwei Peers (Prozesse) definiert werden. Das Dialogfenster für den Export (Abb. 26) bietet die Möglichkeit, die Peer-Informationen zu exportieren.

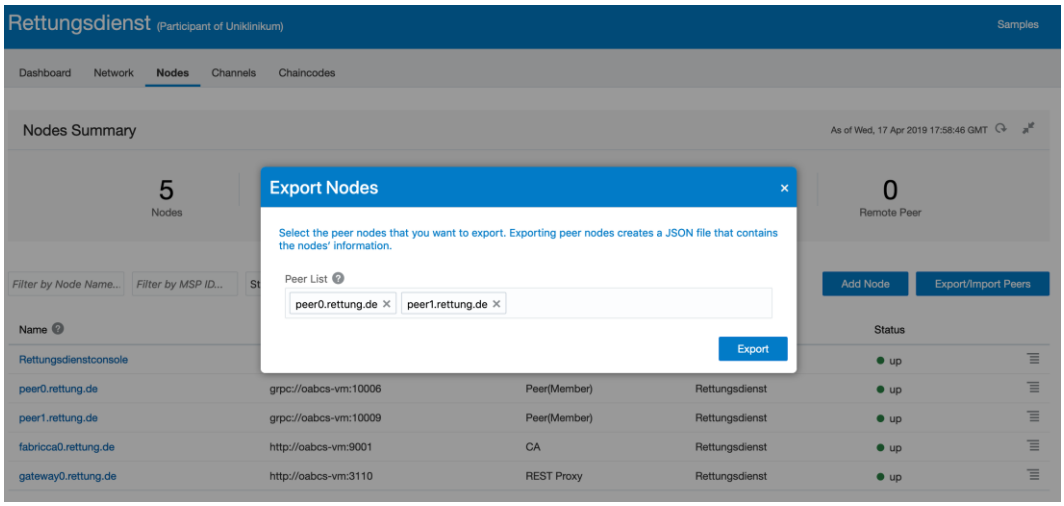


Abbildung 26: Export der Peers für den Rettungsdienst

Schritt 9:

Import Node Information auf dem Founder

Für den Import der Participants-Information (Abb. 27) wird im Founder der [Nodes] Tab ausgewählt und über den Button „Add Node“ hinzugefügt. Anschließend wird über den „Import“ Button der Vorgang abgeschlossen.

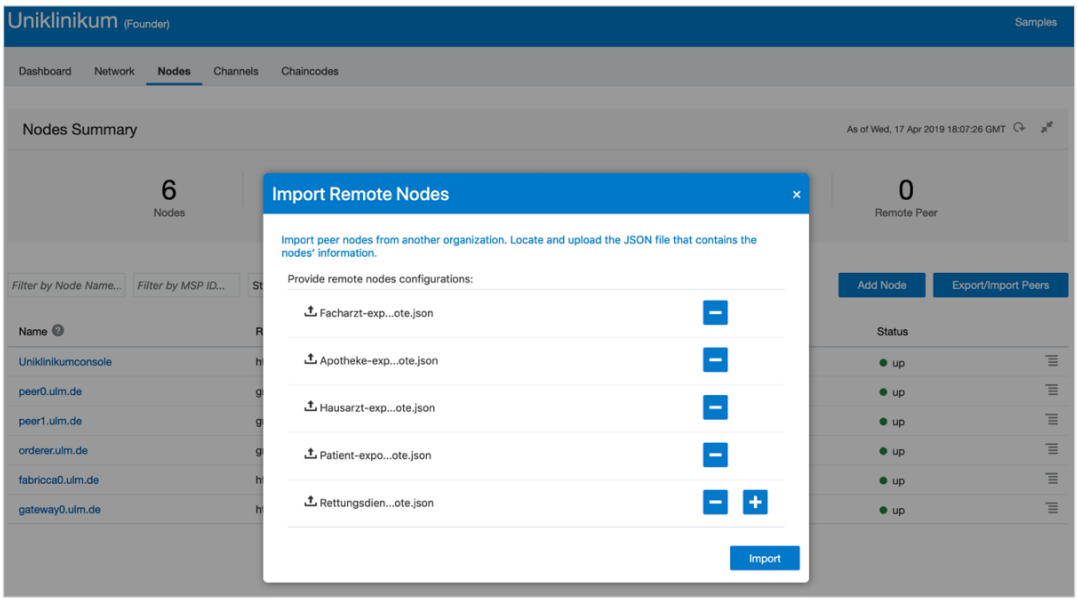


Abbildung 27: Import der Peers im Founder

Schritt 10:

Chaincode Development

Ist der Chaincode bereits entwickelt, muss dieser auf den Founder und anschließend auf alle Nodes der Organisationen verteilt werden. Der in der Dissertation verwendete Chaincode basiert auf einem von der Oracle Corporation mitgelieferten Beispiel, welches für die Untersuchung verändert und erweitert wurde. Der Code wurde in der Programmiersprache „Go“ entwickelt und besteht aus der Datenstruktur und den zugehörigen Methoden.

Die Abbildung 28 zeigt einen Auszug des Go-Programms. Diese Methoden werden später aus Application Express über die REST-Schnittstelle aufgerufen.

```
type Patient struct {
        ObjectType string `json:"docType"`
        PatId      string `json:"patid"`
        Icd        string `json:"Icd"`
        Diagnose   string `json:"Diagnose"`
        Therapie   string `json:"Therapie"`
        Owner      string `json:"Owner"`
        Recall     bool   `json:"recall"`
        RecallDate int    `json:"recallDate"`
```

```
if function == "initPatient" {
        return t.initPatient(stub, args)
} else if function == "transferPatient" {
        return t.transferPatient(stub, args)
} else if function == "deletePatient" {
        return t.deletePatient(stub, args)
} else if function == "readPatient" {
        return t.readPatient(stub, args)
} else if function == "getHistoryForRecord" {
        return t.getHistoryForRecord(stub, args)
} else if function == "getPatientByRange" {
        return t.getPatientByRange(stub, args)
} else if function == "readPatienten" {
        return t.readPatienten(stub, args)
} else if function == "setPatientRecallState" {
        return t.setPatientRecallState(stub, args)
}
```

Abbildung 28: Ausschnitt des Chaincodes mit Struktur und Methoden

Für die Entwicklung des Chaincodes wird die Go-Umgebung inklusive der Blockchain-Libraries (Bibliotheken) benötigt. Danach kann das fertige Programm kompiliert, d.h. in ausführbaren Maschinencode übersetzt werden.

Beispiel: **go build /home/bcsdemo/go-src/new1Trace.go**
Die Deployment-Prozedur der Blockchain erwartet ein zip-File inklusive Verzeichnispfad und beinhaltet nur den entwickelten Quellcode. Dieser wird zur Laufzeit übersetzt und ausgeführt.

Beispiel: **zip new1Trace.zip –r /home/bcsdemo/new1Trace-deployment/**
Die erzeugte Datei wird nun über den Deployment-Prozess auf die Nodes der Blockchain übertragen und installiert. Die Laufzeitumgebung ermöglicht dann den Aufruf der implementierten Methoden (Abb. 29). Beispielsweise liefert die Methode „**readPatienten“** eine Liste der Diagnosen und Therapien des Patienten.
Als Eingabewert wird eine Kombination aus Key/Value im JSON-Format erwartet. In diesem Fall liefert die Funktion einen Datensatz, bestehend aus Diagnose, Therapie, Status und Zeitstempel an das aufrufende Programm zurück.

Testaufruf einer Chaincode-Funktion

```
curl -H "Content-type:application/json" -X POST http://oabcs-vm:3100/bcsgw/rest/v1/transaction/query \
     -d'{"channel":"new1channel","chaincode":"new1Trace","method":"readPatienten","args":["153"],"chaincodeVer":"v1"}'
```

Abbildung 29: Aufruf der readPatienten-Methode mittels cURL von der Kommandozeile des Betriebssystems
cURL = Client for URL

Schritt 11:

Chaincode Deployment / Installation

Der Chaincode stellt Funktionen bereit, die Geschäftslogik (z.B. Überweisungsprozess) abbilden. Jeder Peer (Patient, Arzt etc.) der Organisationen führt die aufgerufene Funktion auf dem festgelegten Channel (new1channel) aus und greift auf die Blockchain und deren dezentrale Transaktions- und Historien-Datenbank zu.

In der Konsole des Founders (Uniklinikum) den Tab [Chaincodes] auswählen und den Button „Deploy a New Chaincode“ anklicken.

Das Dialogfenster für das Deployment erscheint. Die „Advanced“ Methode (Abb. 30) auswählen.

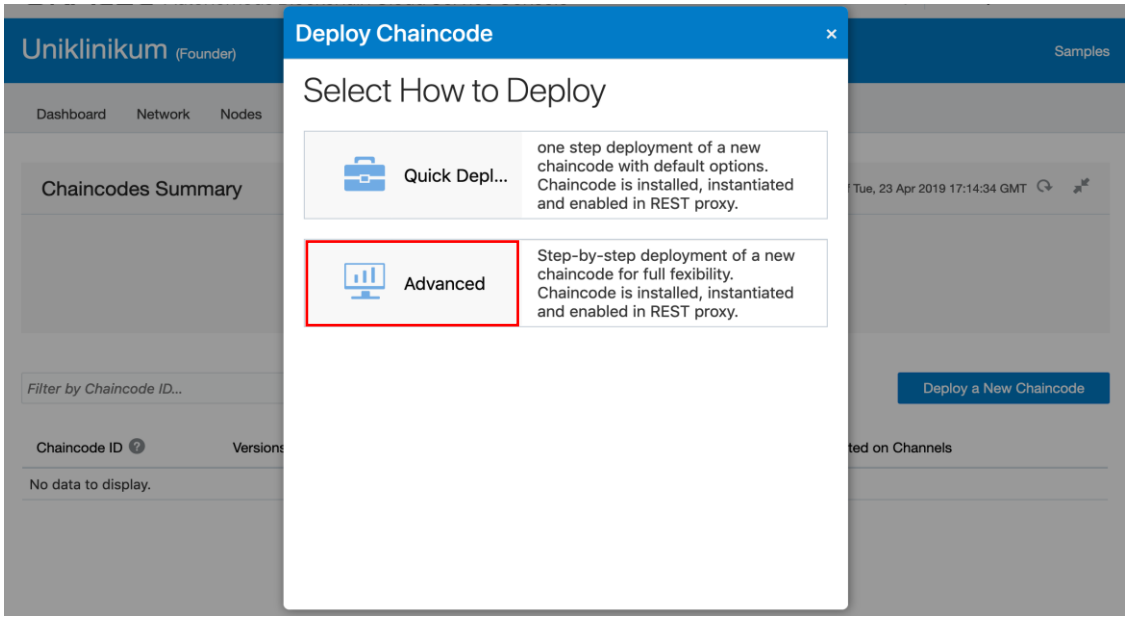


Abbildung 30: Deployment des Chaincodes

Folgende Informationen sind in das Formular (Abb. 31) einzugeben:

a. Chaincode Name: new1Trace
b. Version: v1
c. Target Peers: peer0.ulm.de, peer1.ulm.de
d. Chaincode Source: /home/bcsdemo/new1Trace-deployment/new1Trace.zip

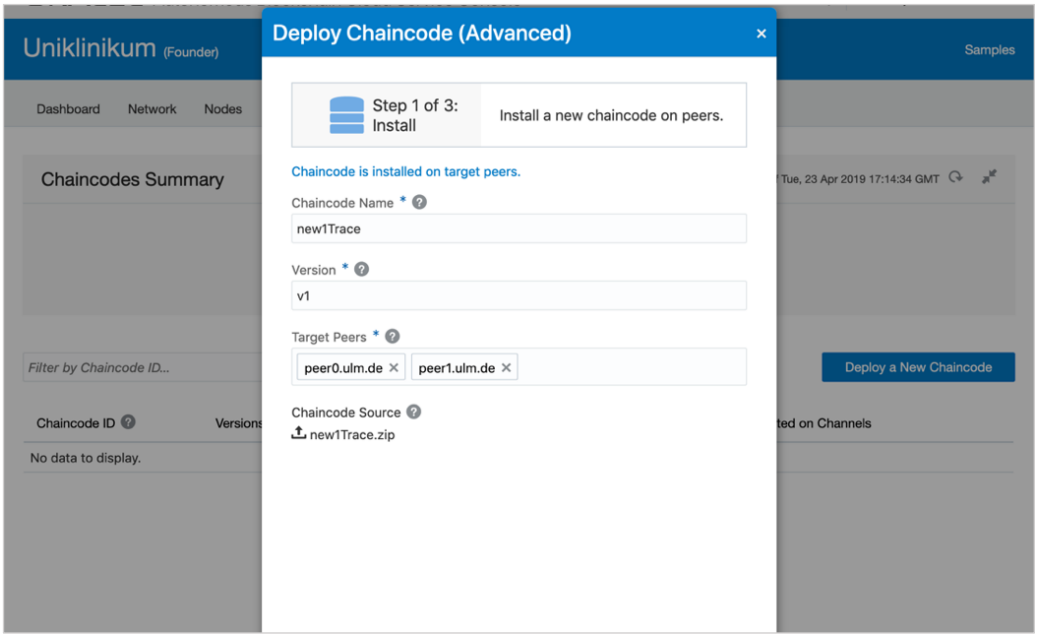


Abbildung 31: Chaincode auf den Founder-Knoten hochladen und installieren

Die Installation wird mit der „Success Message“ abgeschlossen und die Eingaben für den Channel und die Members des Blockchain-Netzwerks können festgelegt werden (Abb. 32).

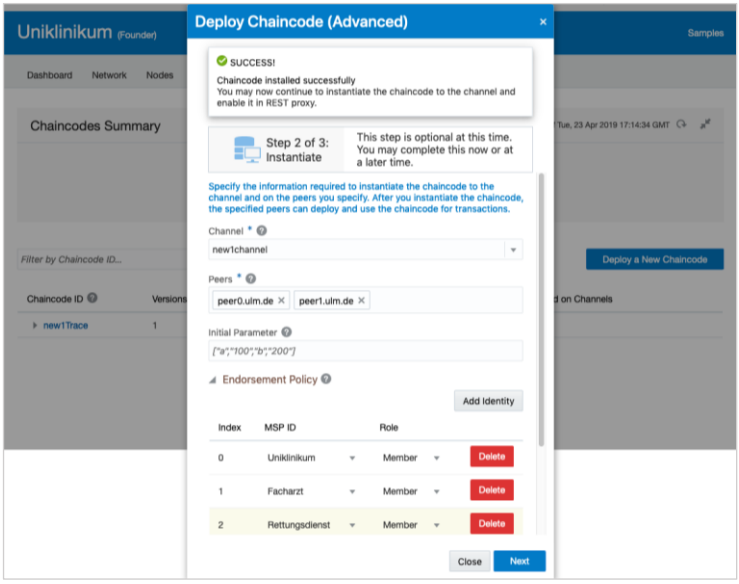


Abbildung 32: Organisationen hinzufügen und Endorsement Policy festlegen

Die Endorsement Policy (Regel) gibt an, welche Teilnehmer für die Validierung des Chaincodes zustimmen müssen. Mit dem Drücken des „Next“ Button wird die Eingabe bestätigt und im letzten Schritt wird der Chaincode dem REST-Proxy bekanntgegeben. Damit ist der Installationsprozess auf dem Founder abgeschlossen und die Installation des Chaincodes muss auf den Participants nach dem gleichen Muster durchgeführt werden (Abb. 33). Mit dem Unterschied, dass nach dem Upload des Chaincode-Files der Prozess abgeschlossen ist.

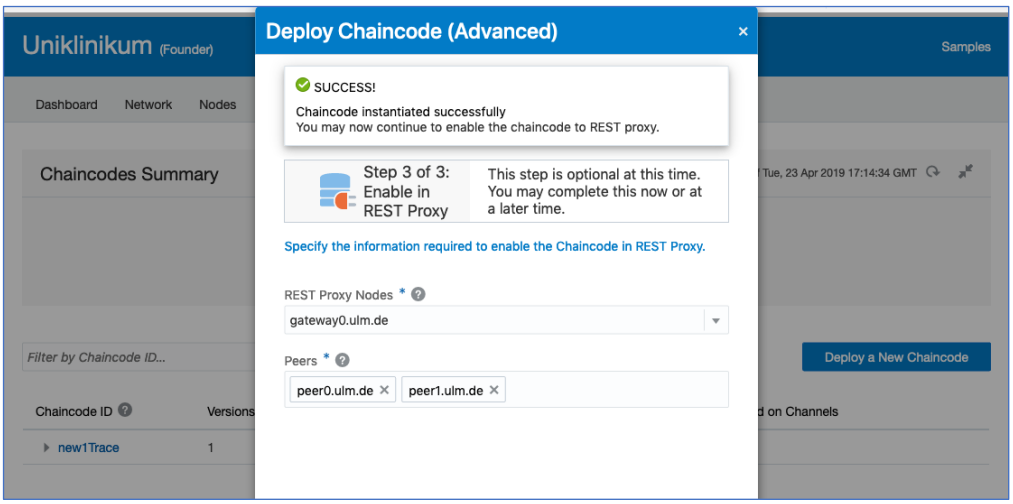


Abbildung 33: REST-Proxy für den Chaincode freischalten / REST = Representational State Transfer

Im nächsten Schritt muss der Founder darüber informiert werden, dass der Chaincode auf den Participants installiert wurde. Dafür muss auf jedem Participant die Nodes-Information exportiert und in den Founder importiert werden. Ist der Prozess abgeschlossen, kann der Chaincode über die REST-Schnittstelle der Blockchain direkt aufgerufen und getestet werden.

Im vorliegenden Beispiel wurde das Programm „Postman“ der Firma Postman Inc. für Funktions-/Performance-Tests genutzt.

Als Eingabeparameter wird ein Wertepaar im JSON-Format erwartet (Abb. 34). In diesem Beispiel wird die Methode „initPatient“ ausgewählt, die eine Diagnose und Therapie des Patienten in der Blockchain speichert.

a. Methode: POST
b. URL: http://192.168.56.101:3100/bcsgw/rest/v1/transaction/invocation
c. channel: new1channel
d. chaincode: new1Trace
e. method: initPatient
f. args: […]

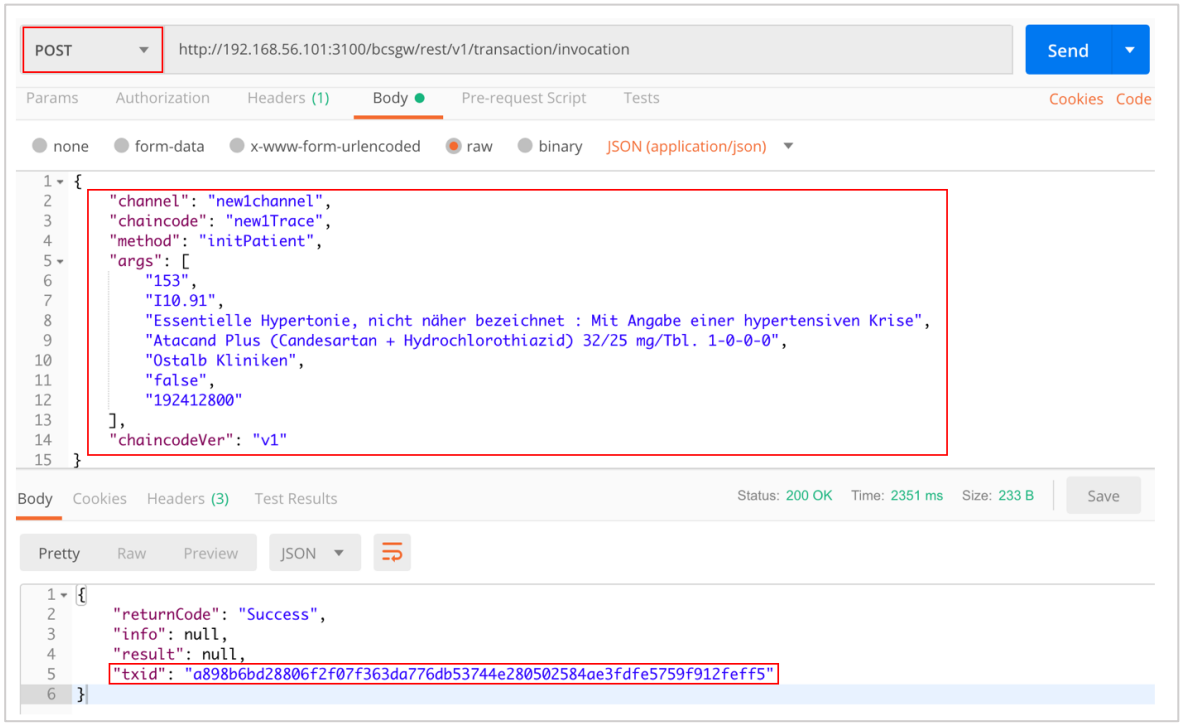


Abbildung 34: Beispiel für einen Postman REST-Request / REST = Representational State Transfer

Wird in der URL das Schlüsselwort „invocation“ durch „query“ ersetzt, wird die Transaktion nur simuliert. Die Blockchain vergibt automatisch die „txid“, d.h. die Transaktion ist erfolgreich und eindeutig im Block gespeichert und wird Teil des neuen Hashwertes. Die REST-Schnittstelle der Blockchain akzeptiert nur die „Post“-Methode, um Funktionen aufzurufen. Dies ist für die spätere Programmierung der APEX-Anwendung wichtig. Die Ausgabe der Ergebnisse erfolgt im JSON-Format, welches dann prozedural in APEX umgewandelt werden muss.

Das Dashboard (Abb. 35) zeigt eine Transaktion auf dem „new1channel“ an, die durch die „invocation“-Anweisung in der URL ausgelöst wurde.

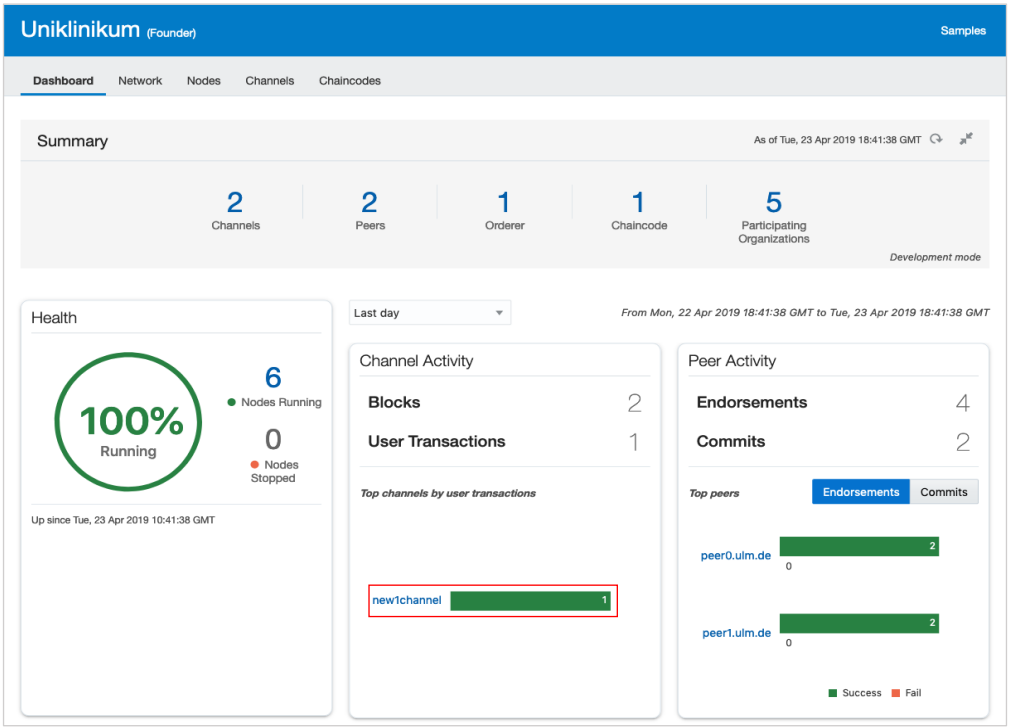


Abbildung 35: Blockchain-Dashboard mit Transaktion auf dem Channel

In der Detailansicht lässt sich sehr gut erkennen, dass es sich hierbei um dieselbe Transaktion handelt, die vom „Postman“-Programm (Abb. 36) initiiert wurde. Dabei wird eine Diagnose und Therapie für einen Patienten in die Blockchain aufgenommen.

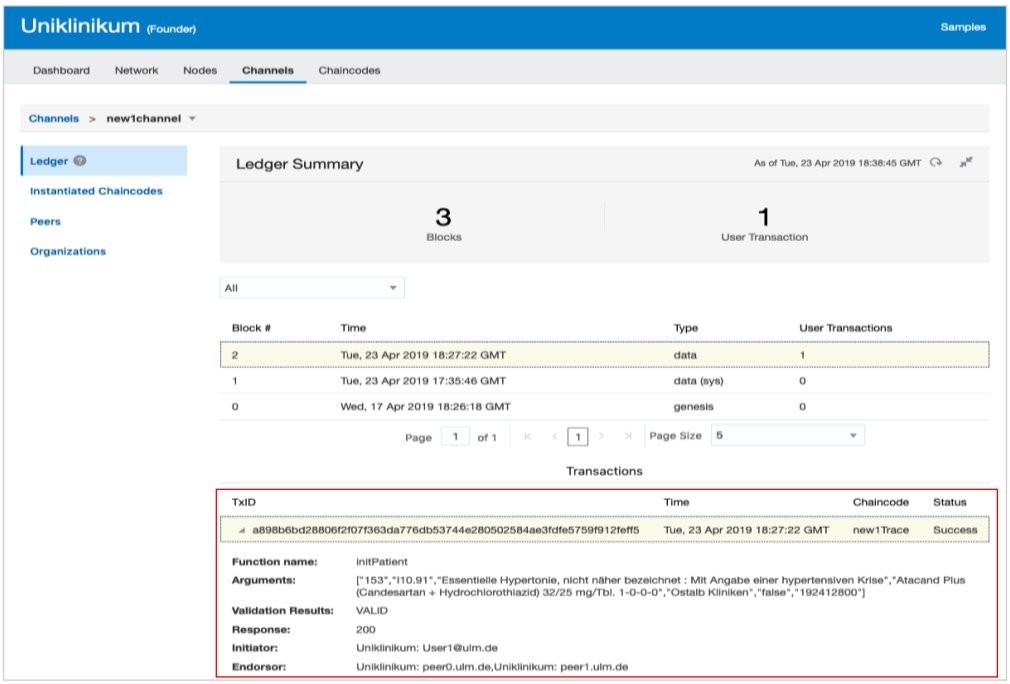


Abbildung 36: Detailansicht der Blockchain-Transaktion

Später werden die Funktionsaufrufe des Chaincodes durch die entwickelte Applikation „Emergency Blockchain“ aufgerufen.

Schritt 12: (optional)

Stoppen der Blockchain-Umgebung

Das Stoppen der Blockchain-Umgebung wird über die Administrationskonsole durchgeführt. Alle Knoten des Netzwerks werden über die rechte Maustaste gestoppt (Abb. 37).



Abbildung 37: Stoppen der Blockchain-Umgebung

Die Docker-Container für die Administrationsumgebung sind noch aktiv. Diese können optional heruntergefahren werden. Auf dem Betriebssystem liegt hierfür ein Shell-Skript (stopDocker.sh) bereit (Abb. 38). Folgende Anweisungen sind im Skript enthalten:

```
#!/bin/bash
docker stop $(docker ps -a -q)
```

Abbildung 38: Stoppen der Docker Container

2.4.2 Datenbank-Modell und prozedurale Entwicklung

Nachdem die Blockchain definiert wurde und die Funktionen des Chaincodes auf Richtigkeit getestet wurden, muss für den integrierten Ansatz ein Datenbankmodell entworfen werden. Dieses Modell ist erforderlich, da auch APEX auf die Tabellen für die Erstellung der Web-Applikation zugreifen muss. Für den Aufbau des Datenbankmodells, der Volltextrecherche, der phonetischen Suche und die Umwandlung von Datumswerten in das numerische Format wurden acht Skripte entwickelt, die auf dem Dateisystem der virtuellen Umgebung zur Verfügung stehen.

2.4.3 Logisches Datenbank-Modell

Vor dem Hintergrund einer gesamtheitlichen Betrachtungsweise ist die Umsetzung eines Datenmodells und dessen Modellierung am Anfang auf einer abstrakten Ebene sinnvoll. Die Blockchain-Struktur kann daher als logisches Element des kompletten Datenbankentwurfs betrachtet werden. In diesem Stadium ist es noch nicht notwendig, den späteren Datentyp festzulegen. Aus diesem logischen Modell (Abb. 39) wird später das physische Datenbankmodell abgeleitet.

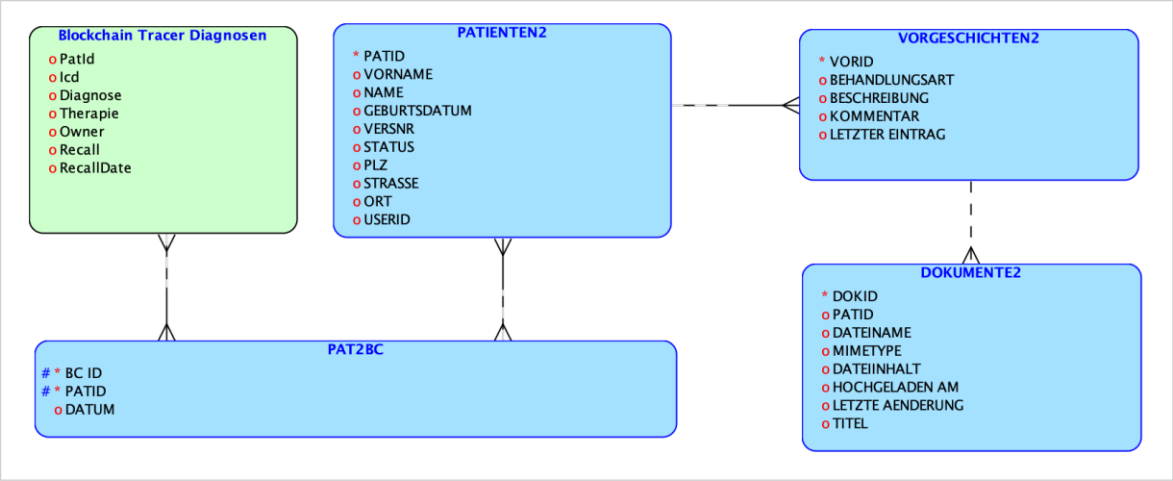


Abbildung 39: Logisches Modell der Datenstrukturen von Blockchain (grün) und Datenbank (blau)

2.4.4 SQL-Skripte

Die für die Datenbank notwendigen Skripte stehen im Verzeichnis der virtuellen Maschine unter „/home/bcsdemo/new1Trace-Database-Design“ und sind während der Umsetzung entstanden.

- 02_getseconds.sql

  Berechnung der Sekunden, die seit dem 01.01.1970 vergangen sind.
- 03_E-R-Modell#9.sql (Abb. 36)

  Tabellen für Stammdaten, Zuordnung PatID zu Blockchain ID’s, Fehler etc.
- 04_createCTX2.sql

  Skript für den Aufbau des Volltextindexes bei der Patientensuche.
- 05_convert_enduser_search.sql

  Funktion, um Sonderzeichen bei der Eingabe des Suchworts herauszufiltern.
- 06_func_phonetik.sql

  Funktion zur Umsetzung der „Kölner Phonetik“.
- 07_string_reverse.sql, 08_prep_string.sql, 09_prep_string_rev.sql

  Funktionen für die Unterstützung der Suche von links, rechts, Sortierung, Groß-und Kleinschreibung.

Das Datenbankdesign (Abb. 40) entspricht der Aufgabenstellung für einen kombinierten Ansatz aus relationaler Datenbank und dezentraler Blockchain-Technologie.

```
-- Tabelle für die Patientenstammdaten
create table PATIENTEN2
(
  PATID             NUMBER GENERATED BY DEFAULT as identity primary key,
  VORNAME           VARCHAR2(255),
  NAME              VARCHAR2(255),
  GEBURTSDATUM      DATE,
  VERSNR            VARCHAR2(50),
  STATUS            VARCHAR2(50),
  PLZ               NUMBER,
  STRASSE           VARCHAR2(255),
  ORT               VARCHAR2(255),
  USERID            VARCHAR2(100)
)
/
-- Tabelle für Vorgeschichte(n) des Patienten
create table VORGESCHICHTEN2 (
  VORID             NUMBER GENERATED BY DEFAULT as identity primary key,
  PATID             NUMBER NOT NULL,
  BEHANDLUNGSART    VARCHAR2(255),
  BESCHREIBUNG      VARCHAR2(255),
  KOMMENTAR         VARCHAR2(255),
  LETZTER_EINTRAG   DATE
)
/
-- foreign key, um die referentielle Integrität zu gewährleisten
alter table VORGESCHICHTEN2
 add constraint PAT_ID_FK2
 foreign key (PATID)
 references PATIENTEN2 (PATID)
/
-- Tabelle für Fehlerbehandlung
create table ERROR_TABLE (
  TS              TIMESTAMP(6),
  MESG            CLOB
)
/
```

```
-- Tabelle für up- und download
create table DOKUMENTE2(
  dokid             NUMBER GENERATED BY DEFAULT as identity primary key,
  vorid             NUMBER,
  patid             NUMBER,
  dateiname         VARCHAR2(200),
  mimetype          VARCHAR2(100),
  dateiinhalt       BLOB,
  hochgeladen_am    DATE,
  letzte_aenderung  DATE,
  titel             VARCHAR2(100)
)
/
-- foreign key, um die referentielle Integrität zu gewährleisten
alter table dokumente2
add constraint dokumente2_fk
foreign key (vorid)
 references vorgeschichten2 (vorid)
/

-- Tabelle für Mapping Patienten zur Blockchain Diagnosen und Therapien
create table PAT2BC (
  BC_ID             NUMBER GENERATED BY DEFAULT as identity,
  PATID             NUMBER,
  DATUM             DATE
)
/
-- Tabelle für zur Tracer Diagnose gehörende Historieneinträge
create table PAT2DEL(
  BC_ID             NUMBER,
  PATID             NUMBER,
  STATE             VARCHAR2(10)
)
/
```

Abbildung 40: Exemplarische Auflistung der SQL-Befehle für die Erstellung der wichtigsten Datenbanktabellen
SQL = Structured Query Language

Der abgebildete Fall geht davon aus, dass für einen Patienten mindestens eine oder mehrere medizinische Vorgeschichten existieren (1:n Beziehung). Diese beinhalten eine oder mehrere medizinische Dokumente, die im Rahmen von Behandlungen in der Vergangenheit erfasst wurden. Die Blockchain-Struktur ist separat zu betrachten und hat zunächst keine Verbindung zur Datenbank. Dies kann nur durch die Mapping-Tabelle „PAT2BC“ erreicht werden. Sollte in der Blockchain ein Eintrag „gelöscht“ (Merkmal: isDelete) werden, würde die Verbindung zur Datenbank und damit auch die Historie fehlen. Aus diesem Grund wurde die Tabelle PAT2DEL eingeführt. Die ERROR_TABLE wird gefüllt, wenn beim Aufruf einer Funktion des Chaincodes oder im PL/SQL-Code ein Fehler aufgetreten ist. Die Tabellen BC_ICD und BC_ORG sind Stammdaten, um die Eingabe in den Formularen über Wertelisten (LOV – List of Values) zu vereinfachen. Die Definitionen und Befehle für die Volltextrecherche sind optional und werden daher nicht näher erläutert.

2.4.5 Application Express Development (APEX)

Das Setup der Blockchain ist abgeschlossen. Nun muss eine dazu passende Anwendung erstellt werden. Die Beispiel-App wurde mit Oracle APEX entwickelt. Dabei handelt es sich um eine deklarative Entwicklungsumgebung für Webapplikationen. Aus der Applikation heraus wird über die REST-Schnittstelle der Blockchain die Funktionen des Chaincodes aufgerufen. Um dies zu erreichen, müssen in APEX Definitionen erstellt, PL/SQL-Prozeduren entwickelt, Formulare, Berichte, Prozesse und SQL-Abfragen erstellt werden.

Der Aufruf der im Chaincode zur Verfügung stehenden Funktionen über die REST-Schnittstelle kann aus der Datenbank mit dem Programm „sqlplus“ (Abb. 41) auf der Kommandozeile getestet werden. In diesem Fall wird eine Liste der Diagnosen und Therapien für einen Patienten abgerufen (readPatienten). Dies ist vergleichbar mit dem cURL-Aufruf (Client for URL) (Abb. 29), bei dem aus dem Werkzeug heraus die „initPatient“-Methode aufgerufen wurde. Im unten gezeigten Beispiel werden mehrere zum Patienten gehörende Datensätze ermittelt, da zwei Argumente (Parameter) übergeben werden.

Das genutzte Programm „sqlplus“ ist ein Teil der Oracle Datenbankinstallation und ist geeignet, um die Aufrufe der Schnittstellen zu testen.

```
sqlplus blockchain/blockchain@//192.168.56.101/xepdb1

BLOCKCHAIN@192.168.56.101/xepdb1 >

  declare
      l_response clob;
  begin
      apex_web_service.g_request_headers.delete;
      apex_web_service.g_request_headers( 1 ).name := 'Content-type';
      apex_web_service.g_request_headers( 1 ).value := 'application/json';

      l_response := apex_web_service.make_rest_request
      (
      p_url => 'http://192.168.56.101:3100/bcsgw/rest/v1/transaction/query',
      p_http_method => 'POST',
      p_body => '{"channel":"new1channel","chaincode":"new1Trace","method":"readPatienten","args":["153,154"],"chaincodeVer":"v1"}'
      );

      dbms_output.put_line( l_response );
      dbms_output.put_line( apex_web_service.g_status_code );
  end;
  /
```

Abbildung 41: Aufruf der Chaincode-Methode „readPatienten“ durch die Datenbank als Blockain-Benutzer in SQL*Plus
SQL = Structured Query Language

Der entwickelte PL/SQL-Code ist die zentrale Komponente, um auf die Methoden des Chaincodes in der Blockchain zuzugreifen. Dieser Softwareteil wird auf mehreren Seiten der APEX-Anwendung später genutzt und stellt eine wiederverwendbare, generische Prozedur dar. Die Ausgabe der Prozedur ist im JSON-Format, welches später in APEX als Bericht umformatiert werden muss.

Das „@“-Zeichen vor dem Dateinamen wird genutzt, um alle Befehle in der Datei sequentiell abzuarbeiten (Abb. 42). Dabei handelt es sich um eine geschachtelte JSON-Ausgabe, die zuerst aus dem „returnCode“ (Success), der „info“ (null) und den eigentlichen Daten „result“ (payload) besteht.

```
BLOCKCHAIN@xepdb1 > @readPatienten.sql
{"returnCode":"Success","info":null,"result":{"payload":"[{\"Key\":\"153\",
\"Record\":{\"docType\":\"Patient\",\"patid\":\"153\",\"Icd\":\"I10.91\",\"Diagnose\":\"Essentielle Hypertonie, nicht
naher bezeichnet : Mit Angabe einer hypertensiven Krise\",\"Therapie\":\"Atacand Plus (Candesartan + Hydrochlorothiazid)
32/25 mg/Tbl. 1-0-0-0\",\"Owner\":\"Facharzt\",\"recall\":false,\"recallDate\":0}}]","encode":"UTF-8"}}
200

PL/SQL procedure successfully completed.
```

Abbildung 42: Ausgabe der in Abbildung 39 aufgerufenen „readPatienten“-Methode mit SQL*Plus
SQL = Structured Query Language

Der Bericht für die Tracer-Diagnosen wird über einen Webservice in APEX realisiert, der auf die Blockchain zugreift. Hierfür benötigt APEX eine Definition, den sogenannten „Remote Server“, der die Basis-URL definiert (Abb. 43).

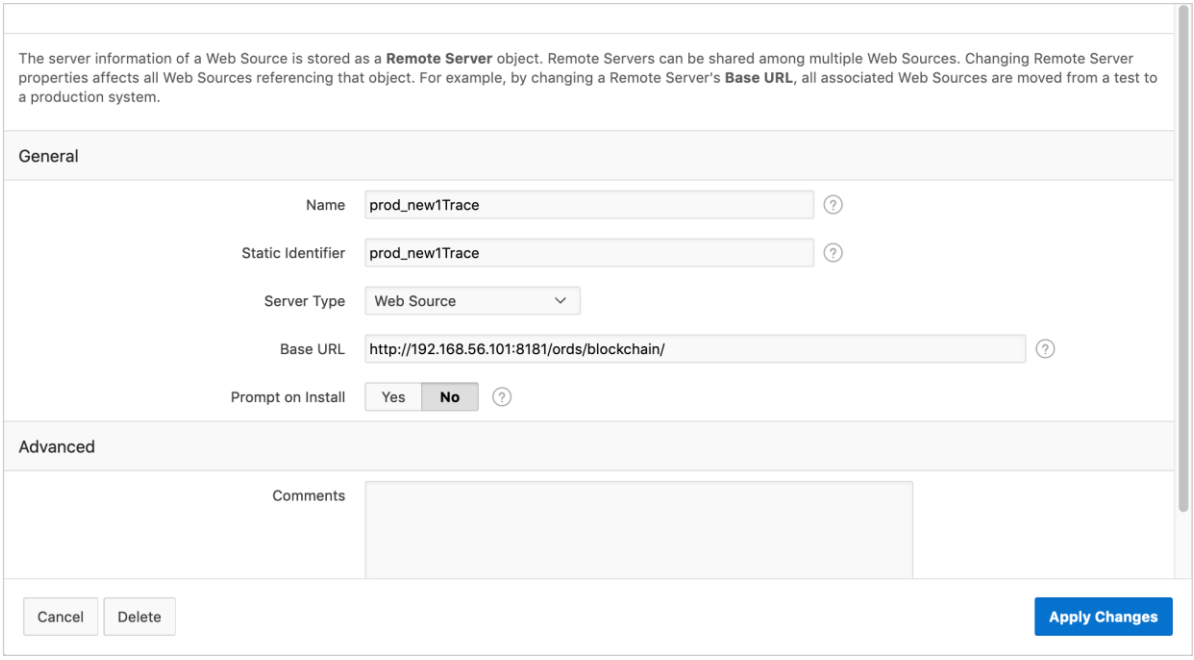


Abbildung 43: Definition der Service-URL / URL = Uniform Resource Locator

Um den Zugriff über eine URL zu erlauben, muss die Basis-URL freigeschaltet werden. Dies kann bequem über Application Express im Bereich des SQL-Workshop im Menüpunkt „RESTFul“-Services durchgeführt werden. Der wichtigste Teil der Prozedur ist der Aufruf der Chaincode-Funktion mit der Übergabe der Parameter. Die Parameter werden über APEX in Form einer Liste (BCLIST) übergeben. Die Ergebnisse des Aufrufs werden in Form eines JSON-Dokuments zurück an die aufrufende Prozedur geliefert, die dann die weitere Verarbeitung übernimmt, um beispielsweise einen Bericht zu erstellen. Dies kann durch die Eingabe der Parameter in der URL getestet werden, wie nachfolgendes Beispiel zeigt:

Beispiel

- http://192.168.56.101:8181/ords/blockchain/bcwrapper/bc-new11/:method/:params
- http://192.168.56.101:8181/ords/blockchain/bcwrapper/bc-new11/readPatienten/153,154

Die in PL/SQL entwickelte „bcwrapper“-Prozedur (Abb. 48) ist generisch und erhält als Übergabeparameter die im Chaincode hinterlegte Methode mit den zugehörigen

Parametern. Die Abfrage der Blockchain über die „readPatienten“-Methode (Abb. 41) ergibt einen Bericht über die zum Patienten gehörende(n) Diagnose(n). Eine Kontrolle der Funktionalität kann direkt über die Eingabe der URL im Browser erfolgen (Abb. 44).

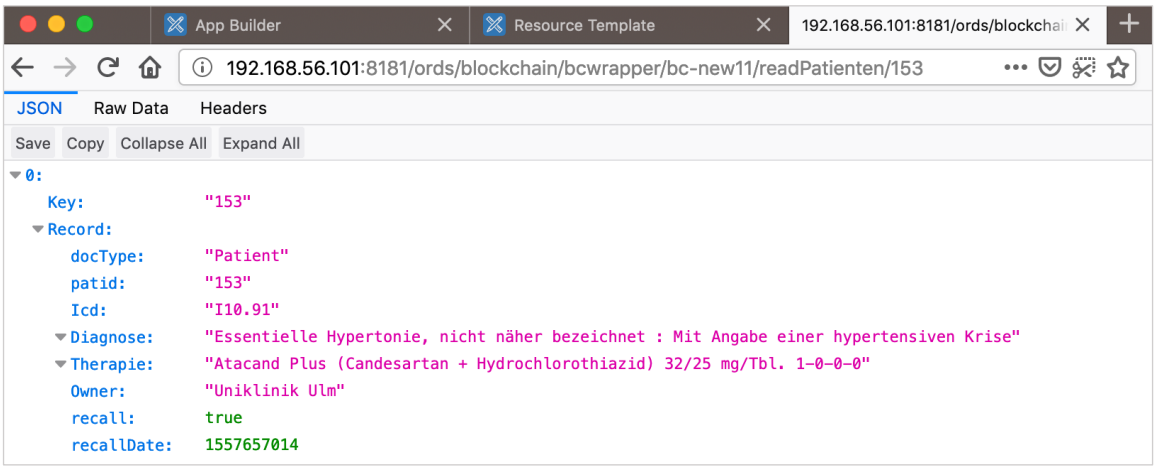


Abbildung 44: Aufruf der Chaincode-Methode readPatienten von der Browser-URL / URL = Uniform Resource Locator

Der Browser hat wenig Möglichkeiten um die Ergebnisse nachzuarbeiten und zeigt daher das originale JSON-Dokument an. In einem weiteren Schritt wird ein Webservice-Modul erstellt, welches die Remote Server Definition als Grundlage nutzt und später als Quelle für den Bericht der Tracer-Diagnosen dient.

In den „Shared Components“ der Applikation wird ein Webservice definiert, der das „wrapper“-Modul aufruft (Abb. 45).

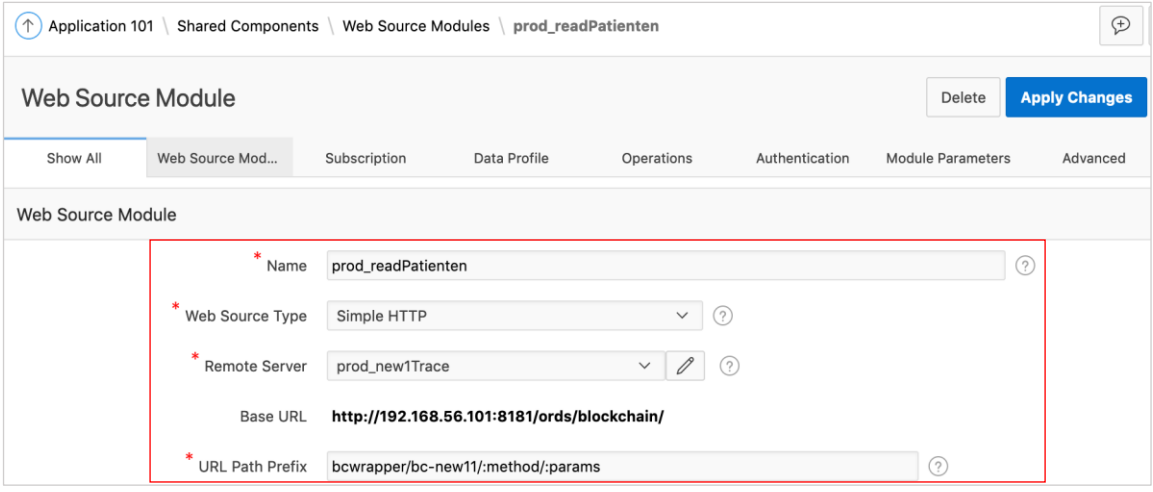


Abbildung 45: Definition des Webservice-Moduls / HTTP = Hypertext Transfer Protokoll

„Copyright Oracle and its affiliates. Used with permission.“

Nachdem die Definition der Module abgeschlossen ist, folgt der Aufruf der Funktion aus dem jeweiligen APEX-Prozess heraus. Die Abbildung 46 zeigt den grundsätzlichen Ablauf einer Transaktion, die aus APEX gestartet wird. Der Prozess „Transfer Patient“ (1) wird über den „Überweisen“-Button in der Oberfläche (Abb. 47) ausgelöst (getriggert). Dieser führt im zweiten Schritt die Prozedur „NEW1_TRACE11_TRANSFER“ (2) aus und übergibt die Parameter an den Webservice (3) der seinerseits die Go-Methode „transferPatient“ (4) über die REST-Schnittstelle der Blockchain aufruft. Es spielen hier vier Komponenten zusammen.

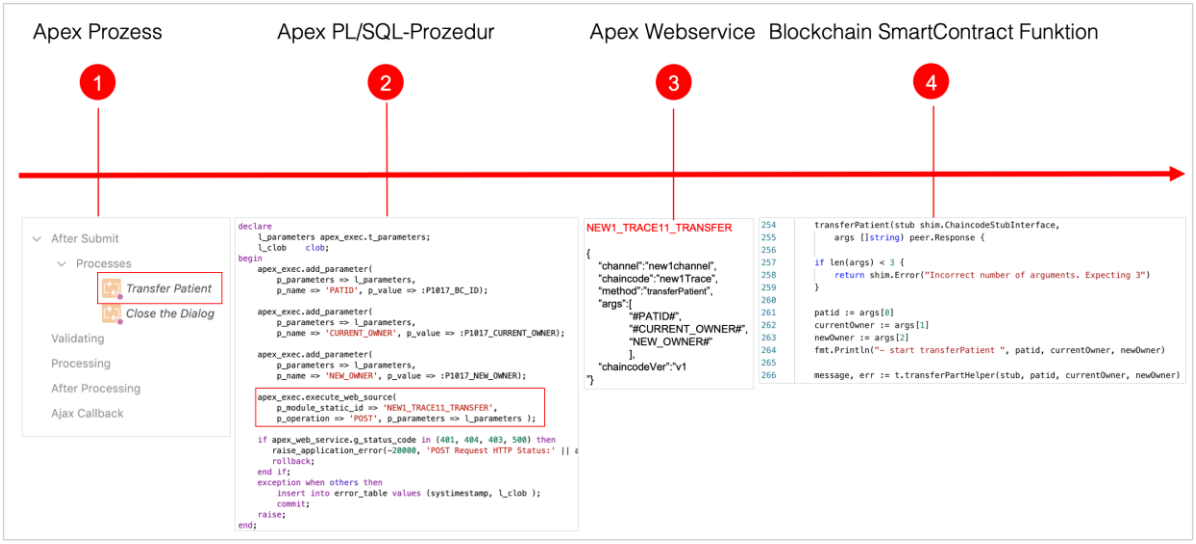


Abbildung 46: Prozessablauf beim Transfer der Patientenakte bzw. Überweisung an den Facharzt

Die Abbildung 47 zeigt die Möglichkeit einer Überweisung und des Widerrufs einer Diagnose bzw. Therapie. Die Transaktion wird automatisch in der Blockchain gespeichert und steht als Historie zur Verfügung.

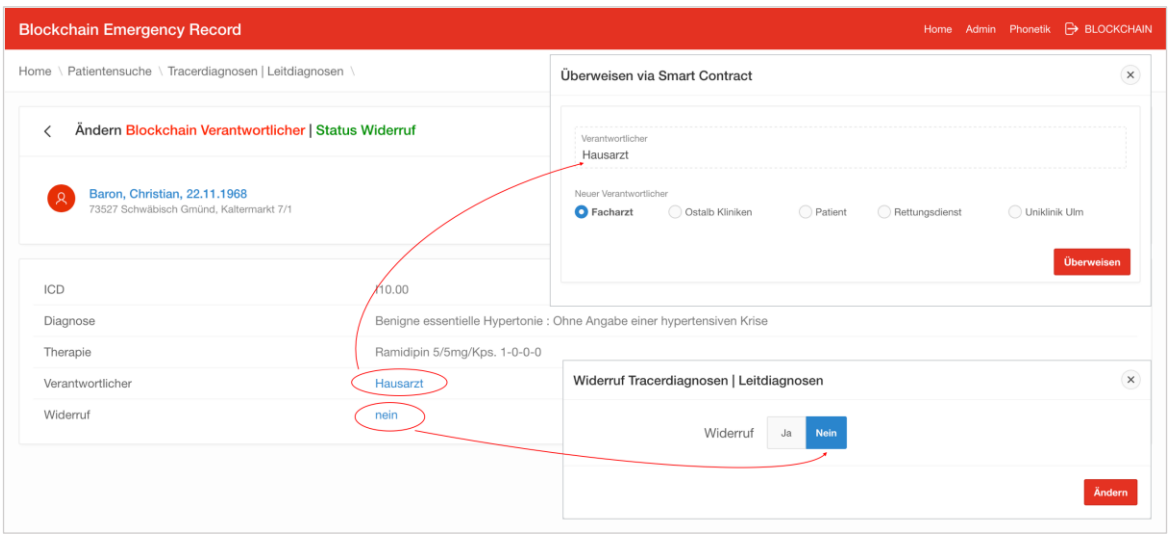


Abbildung 47: Überweisungsmöglichkeit mittels „Überweisen via Smart Contract“

Der letzte Schritt ist die Erstellung des Berichts in der Anwendung auf Basis des definierten Webservice Moduls. Der Auszug aus dem Listing (Abb. 48) zeigt den Quellcode des entwickelten „bc-wrapper“-Moduls, welches die Diagnosen, Therapien und die Historie des Patienten abfragt, umwandelt und als Webservice-Modul für einen Bericht auf den Applikationsseiten der „Blockchain Emergency App“ dienen kann.

```
begin
   apex_web_service.g_request_headers.delete;
   apex_web_service.g_request_headers( 1 ).name  := 'Content-Type';
   apex_web_service.g_request_headers( 1 ).value := 'application/json';

   for i in 1 .. l_argsarray.count loop

       l_args := l_args || case when l_args is not null then ',' end ||
                           '"' || l_argsarray( i ) || '"';
   end loop;

   l_clob := apex_web_service.make_rest_request(
       p_url => 'http://192.168.56.101:3100/bcsgw/rest/v1/transaction/query',
       p_http_method => 'POST',
       p_body => '
         {
               "channel":"'||l_channel||'",
               "chaincode":"'||l_chaincode||'",
               "method":"'|| :method || '",
               "args":['||l_args||'],"chaincodeVer":"'||l_chaincodeVer||'"
         }'

   );

   if apex_web_service.g_status_code = 200 then -- 200 = SUCCESS

       select result into l_result
         from xmltable(
                   '/json/result'
                   passing apex_json.to_xmltype( l_clob )
                   columns
                        returnCode      varchar2(250)  path 'returnCode/text()',
                        result          clob           path 'payload/text()',
                        info            varchar2(250)  path 'info/text()');
```

Abbildung 48: Auszug Quellcode der APEX-PL/SQL-Prozedur „bc-wrapper“

APEX-PL/SQL = Application Express Procedural Language / Structured Query Language

Darüber hinaus besteht die Möglichkeit einer Nachbearbeitung (Postprocessing) der Daten im Bericht. Dies ist dann erforderlich, wenn beispielsweise Datumswerte unterschiedlich behandelt werden oder ggf. Datentypkonvertierungen durchgeführt werden müssen. In der programmierten Anwendung ist ein Bericht der Tracer-Diagnosen abrufbar. Die Grundlage dafür ist ein „classic Report“, der als Quelle das erstellte Web Source Modul nutzt.

Bestandteile der Applikation

Die Applikation und die Definitionen der Webservices können als SQL-Dateien exportiert bzw. importiert werden. Sie sind in der VirtualBox VM im Verzeichnis „/home/bcsdemo/new1Trace-Apex“ unter folgenden Bezeichnungen zu finden:

- f101-Emergency-RadiologieApp.sql
- f101-Emergency-RadiologieApp-ORDS_REST_BLOCKCHAIN_ALL_2019_05_16.sql

2.4.6 Performance-Messungen

Für die Messung des Antwort-/Zeitverhaltens bei Transaktionen wurden Betriebssystemskripte entwickelt und Werkzeuge eingesetzt. Diese bilden unterschiedliche Szenarien und Gesamtarchitekturen ab, die im Ergebnisteil dargelegt werden. Um die Messreihen vergleichen zu können, wurden die Datenstrukturen aus der Blockchain in Form einer Datenbanktabelle abgebildet. In der „Blockchain Emergency App“ wurde hierfür ein Formular und zugehörige Berichte entwickelt, die auch im Falle einer Migration eingesetzt werden können. Die Generierung der Betriebssystem-Befehle, um über die verschiedenen Schnittstellen zugreifen zu können, wurden mit Hilfe von SQL entwickelt und liegen auf dem Betriebssystem der VM als Teil der Dissertation vor. Diese und die Messdatenprotokolle sowie deren Ergebnisse sind in Excel dokumentiert und in der VM im Verzeichnis unter „/home/bcsdemo/new1Trace-Zeitmessung“ zu finden.
Skripte für die Performance-Messungen:

- 01_cr_tab_bc_data.sql
- 02_cr_curl_from_bc_data.sql
- 03_cr_insert_bc_data.sql
- 04_select_from_bc_data4.sql
- 05_delete_from_bc_data4.sql
- Messdatenprotokoll_03-06-2019.xlsx

Testumgebung: VM 8 GB Hauptspeicher, 4 virtuelle CPU’s
Folgendes Vorgehen wurde für die Erstellung der Messdaten gewählt:

1. Tabelle BC_DATA gemäß der Blockchainstruktur im Go-Code erstellen.
2. Kopieren der Diagnosen und Therapien mittels Apex Pages.
3. Generierung der Testdaten mit URL für die Messreihen mit SQL Developer.
4. Generierung des ausführbaren Skripts zur Zeitmessung als Shell-Skript.
5. Ausführung der Befehle über das Postman-Programm (Abb. 49).

Die Kommandozeile wird immer dann genutzt, wenn Tests bzw. automatisierte Ausführungsanweisungen nacheinander abgearbeitet werden müssen.

Um die Messungen später vergleichen zu können, wurde als Bezugspunkt die Datenbank mit dem ORDS als Applikations-Server gewählt. Dabei werden die Daten, wie bei der Blockchain über die REST-Schnittstelle in die Datenbank eingepflegt (z.B. insert). Damit die Daten aus der Migrationstabelle BC_DATA nicht gelöscht bzw. neu eingefügt werden, wird die Tabelle BC_DATA2 und BC_DATA4 für die Messung genutzt.

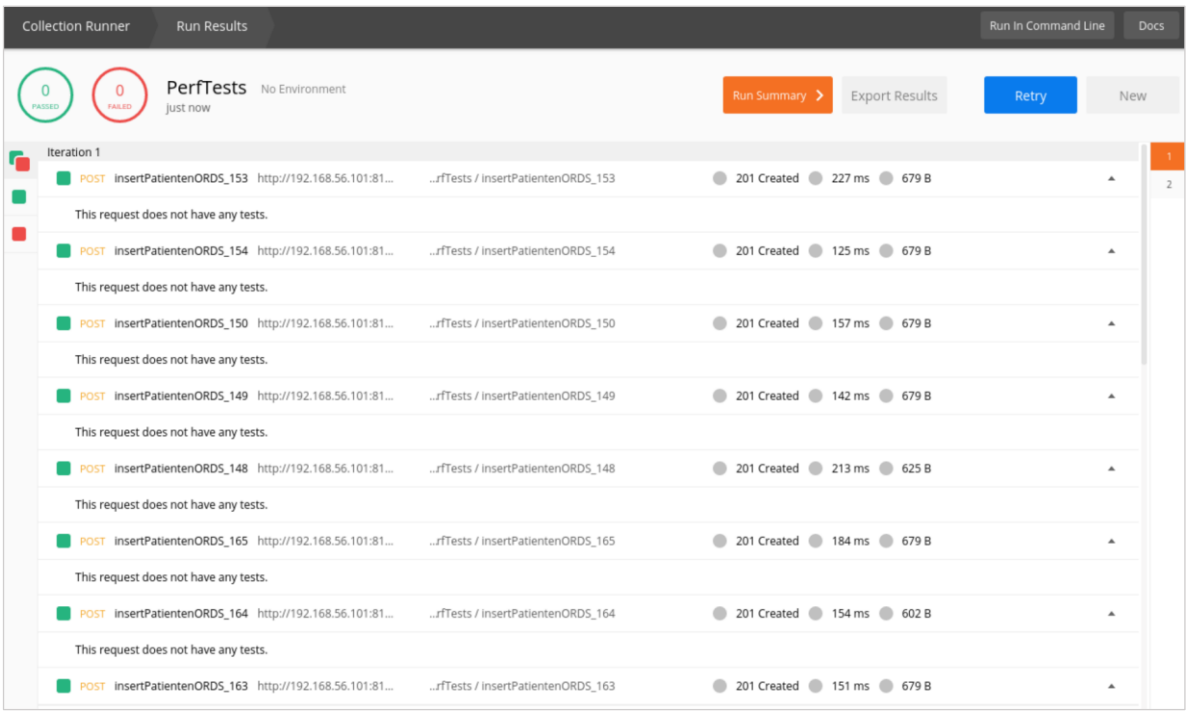


Abbildung 49: Ausführung einer Performancetestreihe für 20 Datensätze

2.5 Zusammenfassung Material und Methoden

Im vorangegangenen Teil wurde ausführlich beschrieben, welche Materialien und Methoden verwendet wurden. Die Blockchain-Struktur wurde entwickelt, konfiguriert und der passende Chaincode in der Programmiersprache „Go“ entwickelt und installiert. Der Aufbau des Blockchain-Netzwerks bedeutete erheblichen konzeptionellen und zeitlichen Aufwand, zumal die fachlichen Anforderungen gemäß den Zielen der Dissertation definiert werden mussten.

Für die Applikation wurde ein Datenbankdesign auf Basis einer Oracle Datenbank entworfen, um die vorhandenen Patientenstammdaten mit den Daten in der Blockchain zu integrieren und damit Interoperabilität und Koexistenz zu

gewährleisten. Die Ergebnisse aus den einzelnen Programmier- und Prozessschritten wurden als „Screenshots“ dokumentiert und verbergen die dahinterliegende Komplexität. Die Web-Applikation, bestehend aus Formularen und Berichten, wurde mit Application Express erstellt. Über die Oberfläche der App werden die Funktionen des Chaincodes aufgerufen. Die Messreihen zum Antwort-/ Zeitverhalten beziehen sich auf den Zugriff über das REST-Gateway der Blockchain. Als Referenz wurde die Oracle Datenbank genutzt. Dafür wurden Shell-Skripte entwickelt, die Testdaten generieren und die unterschiedlichen Operationen des Chaincodes aufrufen.

Im nächsten Kapitel werden die Ergebnisse der Arbeit behandelt. Ein Fokus liegt hierbei auf der Programmierung des Chaincodes „new1Trace“ und vor allem auf der inhaltlichen Darstellung und Entwicklung der APEX-Applikation „Blockchain Emergency App“ aus der Sicht der Endanwender und des Entwicklers.

3. Ergebnisse

Eine der zentralen Fragestellungen bei der Nutzung von Blockchain-Technologie ist der Anwendungsfall. Im Teil Material und Methoden wurde dargelegt, welchen Aufwand die Entwicklung bedeutet und wie viele Komponenten zusammenspielen müssen, um eine lauffähige Umgebung zur Verfügung zu stellen.

Das Ziel der Aufgabenstellung war es, die Eignung von Blockchain im Gesundheitswesen zu untersuchen und zukünftige Potentiale abzuleiten. Der Beweis war anhand eines praktischen Beispiels umzusetzen. Der Nachweis auf Eignung der Blockchain-Technologie wurde anhand eines Anwendungsfalls aus dem Rettungsdienst nachgewiesen und später auf die Verwaltung und Bereitstellung von radiologischem Bildmaterial erweitert. Die Anwendung selbst ist der Kern und das Ergebnis der Dissertation mit einem experimentellen Ansatz, basierend auf den Grundlagen der Blockchain und der Kombination mit relationaler Datenbanktechnologie. Aus diesem Grund ist es notwendig, die Applikation aus Sicht des Endanwenders und des Entwicklers näher zu betrachten.

Folgende Komponenten sind die wichtigsten drei Elemente der Dissertation, die bei der Programmierung der fachlichen Anforderungen definiert und umgesetzt wurden:

- Datenbank-Modell
- Chaincode: new1Trace
- Web-Applikation: Emergency App

3.1 Datenbank-Modell

Im Rahmen der Entwicklung wurde das logische Datenmodell (Abb. 39) in ein physisches „Entity-/Relationship-Modell“ abgeleitet. Die Struktur des Chaincodes existiert dabei unabhängig vom Datenbankmodell und dessen Beziehungen untereinander. Daher muss die Kenntnis über eine vorhandene Diagnose und Therapie in der Blockchain über die „PAT2BC“-Tabelle hergestellt werden und über die APEX-Applikation verknüpft werden.

Beide Modelle bilden ein sogenanntes Unternehmensmodell (Abb. 50), um unterschiedliche Anforderungen abzubilden. Die Integration in heutige KIS-Systeme könnte mit Hilfe dieses Ansatzes realisiert werden.

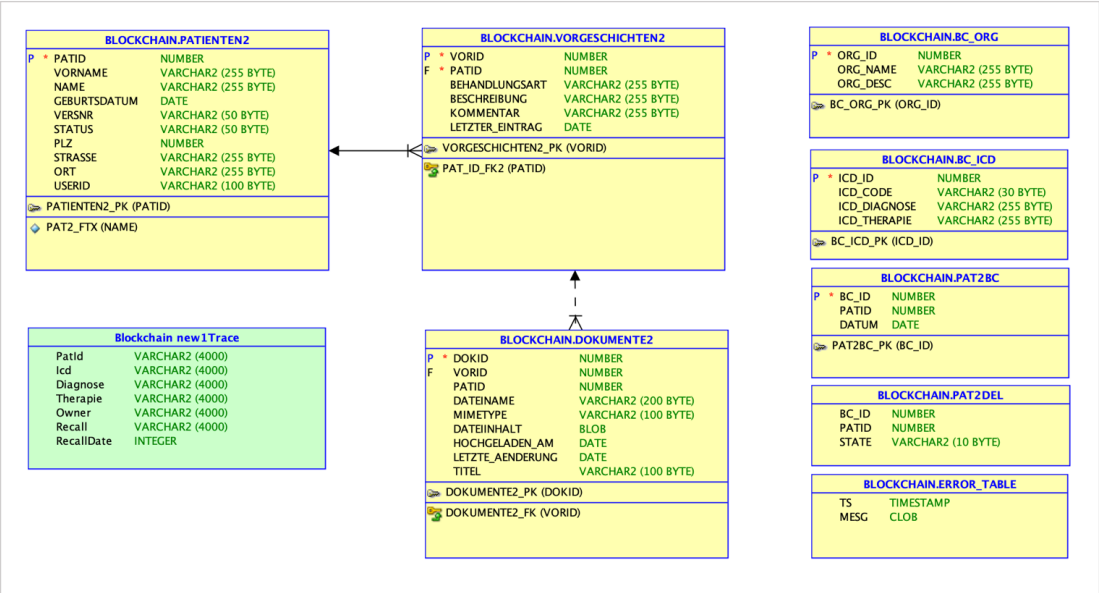


Abbildung 50: Entity-/Relationship-Modell

3.2 Chaincode / Smart Contract – new1Trace

Das Zusammenspiel aus der Programmierung und die Integration der Module in das Gesamtsystem müssen konzeptionell beachtet werden, damit das Verhältnis von Aufwand und Nutzen in Relation steht. Um auf die Blockchain-Struktur mit dem Chaincode zugreifen zu können, müssen Funktionen entwickelt werden, die später über die Oberfläche von APEX mit einem „Mausklick“ bedient und ausgeführt werden können. Dies ist beispielsweise dann der Fall, wenn die zum Patienten passenden Diagnosen und Therapien als Bericht aus der Blockchain gelesen und dargestellt werden. Folgende Chaincode-Funktionen stehen zur Verfügung:

Chaincode Funktionen

- readPatienten
- getHistoryForRecord
- initPatient
- transferPatient
- setPatientRecallState
- deletePatient

An der go-Funktion „**readPatienten**“ (Abb. 51) kann das Zusammenspiel der Blockchain und APEX dargestellt werden. Dabei wird eine Liste von Therapien und Diagnosen von der Blockchain zurückgegeben, die dann einem passenden Patienten zugeordnet werden müssen. Dies bildet sozusagen eine „1:n“-Zuordnung von Blockchain zur Datenbank ab. Die Stammdaten des Patienten sind dabei die übergeordnete Instanz (Master) und die von der Blockchain gelieferten Daten bilden die Detailinformation ab. Im beschriebenen Fall werden diese zwei unabhängigen Systeme in der Oberfläche der Applikation über das Element „BCLIST“ zusammengeführt. Basis hierfür ist die Tabelle „PAT2BC“ (Abb. 50) in der Datenbank, aus der die vorhandenen Daten ermittelt werden.

```
// ============================================================================
// readPatienten gets patient data based on a list of Trace IDs - BCLIST in Apex
// ============================================================================

func (t *AutoTraceChaincode)
      readPatienten(stub shim.ChaincodeStubInterface, args []string) peer.Response {

    var patid, jsonResp string
    var buffer bytes.Buffer
    // var err error

    buffer.WriteString("[")

    bArrayMemberAlreadyWritten := false
    for i := 0; i < len(args); i += 1 {
        patid = args[i]
        valAsbytes, err := stub.GetState(patid) //get the Patient Trace from chaincode state
        if err != nil {
            jsonResp = "{\"Error\":\"Failed to get state for Trace" + patid + "\"}"
            fmt.Println(jsonResp)
            return shim.Error(jsonResp)
        } else if valAsbytes == nil {
            jsonResp = "{\"Error\":\"Patient's Trace does not exist: " + patid + "\"}"
            fmt.Println(jsonResp)
            return shim.Error(jsonResp)
        }
        if bArrayMemberAlreadyWritten == true {
            buffer.WriteString(",")
        }
        buffer.WriteString("{\"Key\":")
        buffer.WriteString("\"")
        buffer.WriteString(patid)
        buffer.WriteString("\"")

        buffer.WriteString(", \"Record\":")
        // Record is a JSON object, so we write as-is
        buffer.WriteString(string(valAsbytes))
        buffer.WriteString("}")
        bArrayMemberAlreadyWritten = true
    }
    buffer.WriteString("]")

    fmt.Printf("- readPatienten queryResult:\n%s\n", buffer.String())

    return shim.Success(buffer.Bytes())
}
```

Abbildung 51: Codebeispiel der „readPatienten-Funktion“ zur Ermittlung der Diagnosen und Therapien des Patienten

Dabei wird geprüft, ob für den Patienten mit der Patienten ID eine Diagnose bzw. Therapie existiert.

Funktionen wie beispielweise „getHistoryForRecord“ liefern als Ergebnis die komplette Behandlungshistorie des Patienten. Der gesamte „Go“-Code besteht ohne Kommentare und Leerzeilen aus ca. 360 Zeilen und wird in der VM zur Verfügung gestellt.

3.3 Entwicklung der „Blockchain Emergency App“ mit APEX

Am Ende des Entwicklungsprozesses steht die Applikation, die als Webapplikation beim Nutzer auf unterschiedlichen Geräten ablaufen kann. In der Anwendung werden die im Chaincode programmierten Funktionen aufgerufen. Der Prozess für die Überweisung bzw. dem Übertragen der Berechtigung für die Behandlung wurde verwirklicht. Weitere Prozesse sind die Erfassung und Änderung von Diagnosen und Therapien, die Pflege der Patientenhistorie, Widerruf einer Therapie bzw. Diagnose, Volltextrecherche, Administrations- und Migrationsmöglichkeiten, Verwaltung der Teilnehmer und Up-/ und Download-Möglichkeit von radiologischem Bildmaterial, Befunden und Notfallprotokollen. Die Applikation besteht aus einer Vielzahl an Komponenten und Möglichkeiten, die im Folgenden beispielhaft dargestellt werden.

3.3.1 Homepage

Den Einstieg in die Applikation bietet die Homepage. Für die Nutzung der Anwendung wird nur ein Web-Browser benötigt. Die Applikation passt sich dem jeweiligen Endbenutzergerät bezüglich der Benutzeroberfläche an, wie in Abbildung 54 zu erkennen ist. Für den Aufruf der Anwendung kann in der Browser-URL die IP-Adresse oder der Hostname verwendet werden. Die Applikation kann über eine spezifische Nummer oder einen Namen aufgerufen werden. Um dies zu erreichen bietet APEX eine spezielle URL-Syntax an, die im Web-Browser eingegeben werden muss.

APEX-URL: http://server:port/ords/f?p=&APP_ID.:&PAGE_ID.:&APP_SESSION.

Für die spätere Verteilung der Anwendung muss nur der Link weitergegeben werden. Dies kann beispielsweise mittels E-Mail oder Chat-Programm geschehen.

Grundsätzlich wird zwischen Entwickler- und Endanwender-URL unterschieden. Der Login für den Entwickler (Abb. 52) benötigt zusätzlich den Namen des Workspaces (Arbeitsbereichs). Der Login für den Endanwender ist in Abbildung 53 dargestellt.

Entwickler-Login-URL:

- http://192.168.56.101:8181/ords

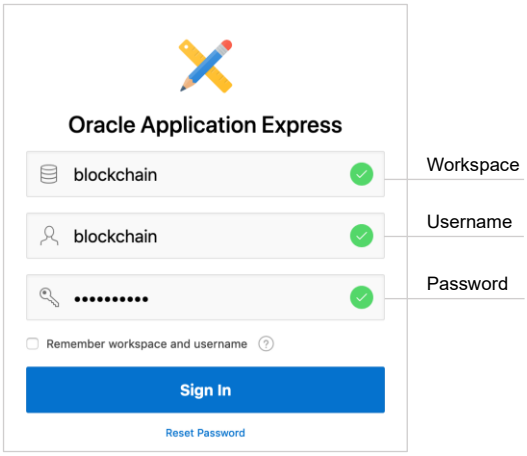


Abbildung 52: Anmeldung als Entwickler - „Copyright Oracle and its affiliates. Used with permission."

Endanwender-URL

- http://192.168.56.101:8181/ords/f?p=101
- http://192.168.56.101:8181/ords/f?p=blockchain

Endanwender-Login mit Benutzername und Passwort

- Benutzername: blockchain
- Passwort: blockchain

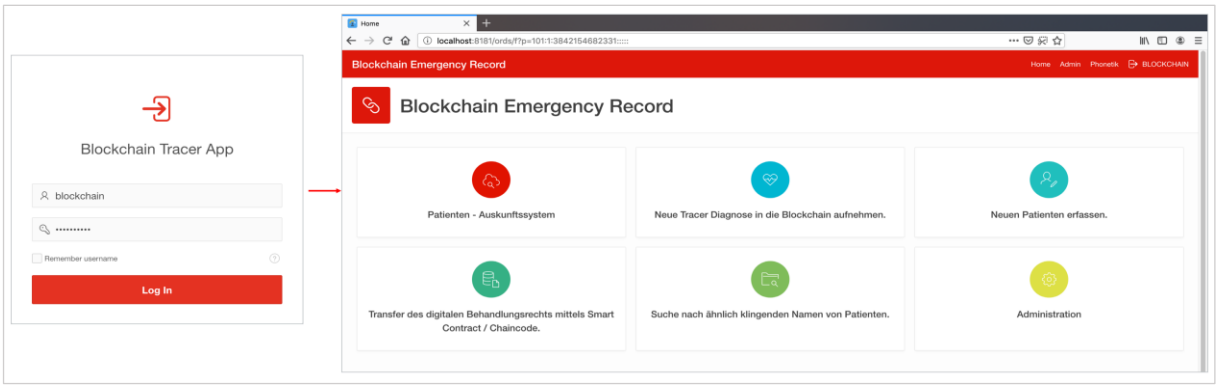


Abbildung 53: Anmeldebildschirm mit Homepage

Die Basis für die Navigation auf der Homepage ist ein Navigationsmenu, dessen Einträge in Form von sogenannten „Cards“ (Abb. 54) dargestellt werden. Dies ermöglicht eine Nutzung der Anwendung über direkte Navigationsmöglichkeiten zu den einzelnen Komponenten.

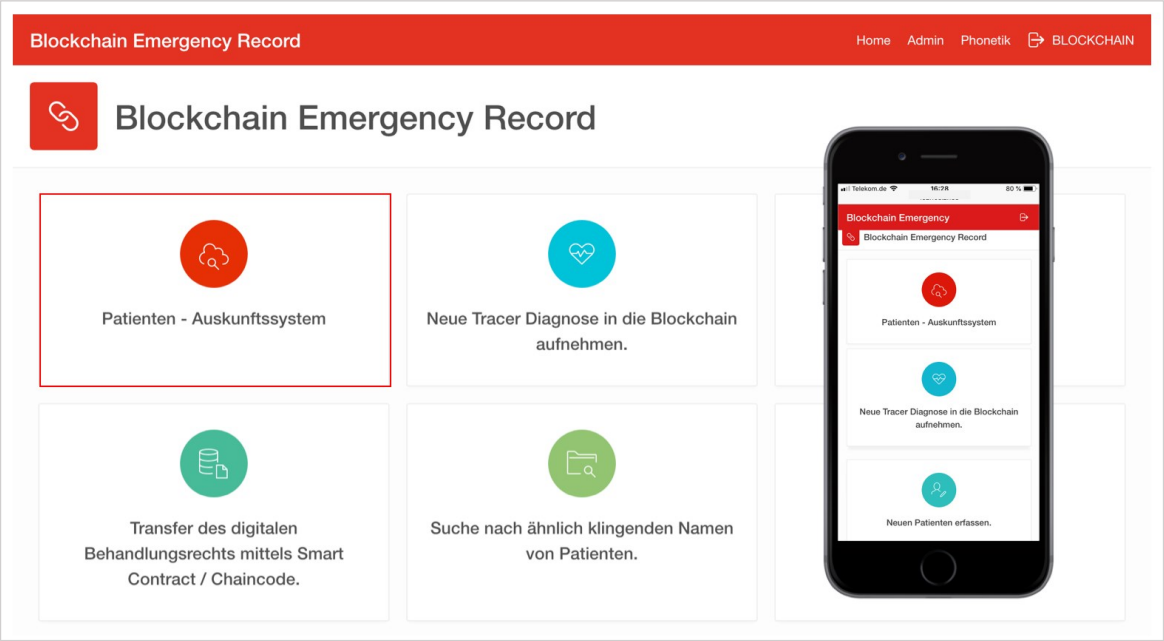


Abbildung 54: Homepage als Webanwendung oder auf dem Smartphone bzw. Tablet

3.3.2 Übersicht der Patientenfälle

Der Endanwender erhält nach der Auswahl des „Patienten – Auskunftssystem“ einen Bericht über vorhandene Patientenfälle (Abb. 55). Dieser basiert auf den Stammdatentabellen und den vorhandenen Fällen in der Blockchain.

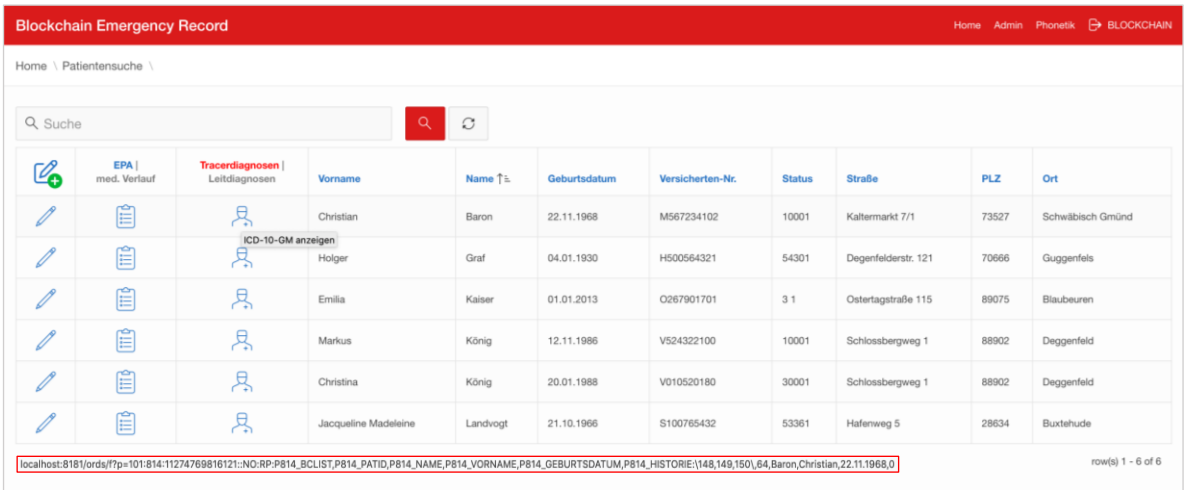


Abbildung 55: Patientenauskunft in Form eines Berichts mit Zusatzfunktionen
EPA = elektronische Patientenakte

Die ersten drei Spalten sind mit Zusatzfunktionen versehen. Durch Auswahl des „Stiftsymbols“ können die Stammdaten der Patienten bearbeitet werden, d.h. Aufnahme, Änderung und Löschen mittels Formular. Alle anderen Spalten sind sortierbar und mit dem Suchfeld können die Patientendaten recherchiert werden.

Entwickleransicht zu Abbildung 55 (Patientenfälle)

Als Entwickler ist für diese Auskunft ein Bericht mit Navigationsmöglichkeiten und Parameterübergabe zu entwickeln, der die PATIENTEN2-Tabelle und die PAT2BC-Tabelle über das gemeinsame Merkmal „PatID“ verknüpft (join). Gleichzeitig wird eine Liste mit den zugehörigen Einträgen der Diagnosen und Therapien, die in der Blockchain abgespeichert sind, vorbereitet. Um diese Liste zu generieren, müssen mit der „within group (order by …)“ Datenbankfunktion die tabellarischen Ergebnisse in Listenform abgefragt werden. Dem APEX-Entwickler stellt sich die zur Abbildung 56 gehörende Oberfläche mit den Regionen und Elementen dar.

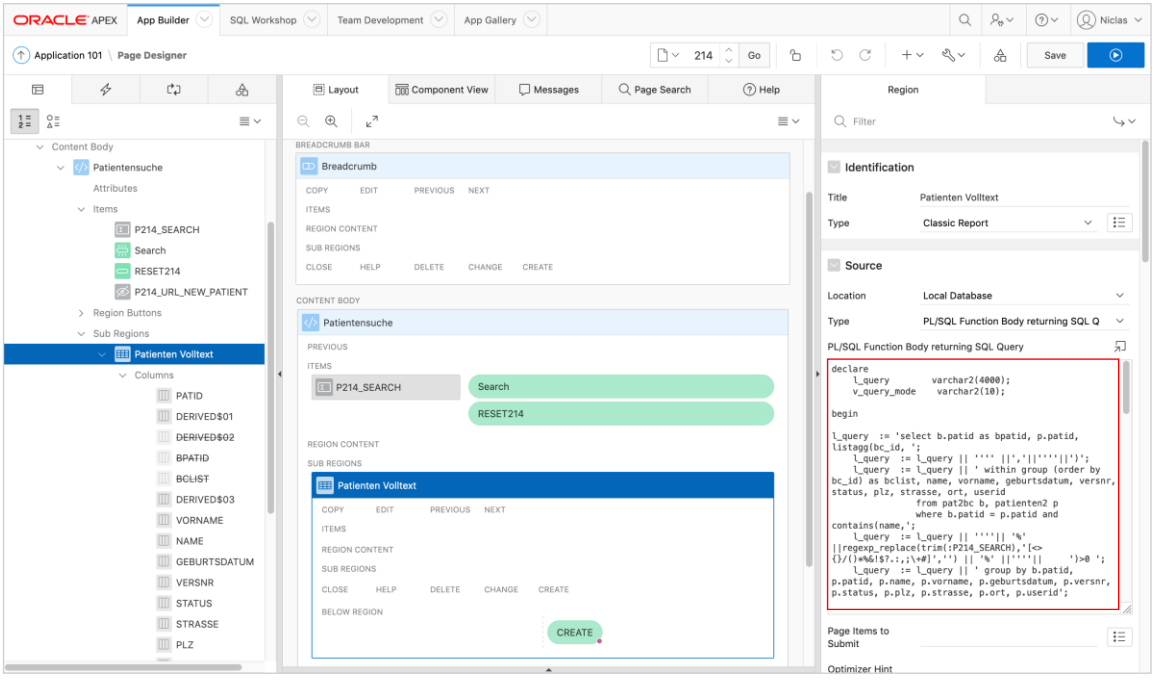


Abbildung 56: Entwicklungsoberfläche der Patientenauskunft - „Copyright Oracle and its affiliates. Used with permission.“

Es lässt sich erkennen, dass die Seite in Regionen aufgeteilt ist. Das Suchfeld (P214_SEARCH) und die zugehörigen Buttons „Search“ und „RESET214“ bilden die Suchregion. Die Darstellung der Ergebnisse findet in der Region „Patienten Volltext“ statt, die ihrerseits auf einer PL/SQL-Funktion basiert, die unter dem Bereich „Source“ rot markiert ist.

3.3.3 Medizinischer Verlauf

In der zweiten Spalte „EPA | med. Verlauf“ kann über die Auswahl des Akten-Symbols auf die medizinische Vorgeschichte (EPA, elektronische Patientenakte) zugegriffen und diese gepflegt werden. Für diesen Prozess mussten mehrere Formulare entwickelt werden. Über definierte Aktionen können Daten erfasst, geändert, gelöscht und Befunde hochgeladen werden. Die „Balloon“-Hilfe (grau) zeigt die entsprechende Möglichkeit bei der Symbolauswahl an, wie in Abbildung 57 zu erkennen ist.

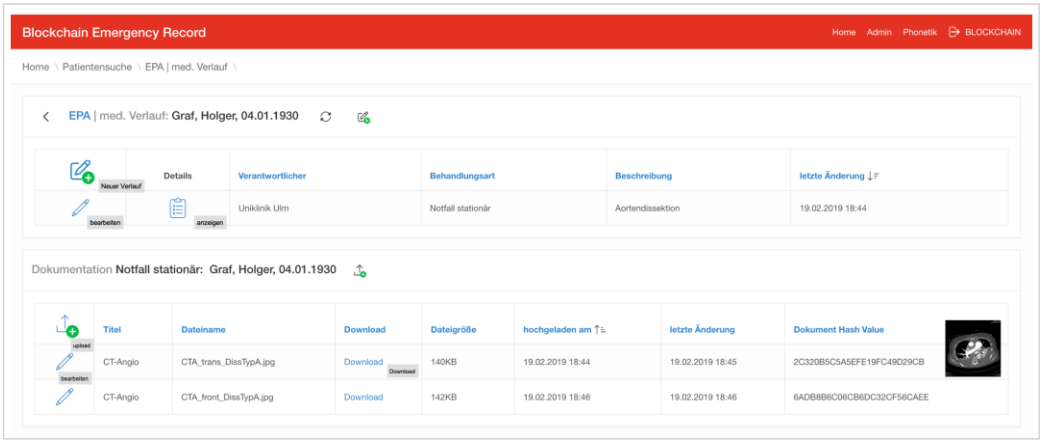


Abbildung 57: Pflege der medizinischen Vorgeschichte mit Zusatzfunktionen / EPA = elektronische Patientenakte

3.3.4 Speicherung und Sharing von Bildmaterial

Der Link für das Sharing (Download) von Inhalten kann sowohl intern als auch extern genutzt werden. Beim Speichern der Inhalte besteht die Möglichkeit, dies in der Datenbank zu speichern oder in einem Cloud-Speicher für die Ablage zu nutzen. In der Blockchain würde nur der Verweis auf das Dokument und die Berechtigung abgespeichert werden. Die Abbildung 58 zeigt ein Beispiel für eine Prozedur für eine mögliche Abfrage von Cloud-Speicher-Inhalten.

```
$sqlplus blockchain/blockchain@192.168.56.101:1526/xepdb1
BLOCKCHAIN@xepdb1>

  declare
    l_clob clob;
    l_result clob;
  begin
    apex_web_service.g_request_headers.delete;
    apex_web_service.g_request_headers( 1 ).name  := 'Content-Type';
    apex_web_service.g_request_headers( 1 ).value := 'application/json';

    l_clob := apex_web_service.make_rest_request(
        p_url => 'https://swiftobjectstorage.clouddatacenter.cloud.com/v1/tenant/upload-directory/',
        p_http_method => 'GET',
        p_username => 'v_username',
        p_password => 'v_password',
        p_wallet_path => 'file:///home/oracle/https_wallet/',
    );
    dbms_output.put_line(l_clob );
  end;
```

Abbildung 58: PL/SQL-Prozedur für eine Abfrage von Dokumenten eines Cloud-Speichers
PL/SQL = Procedural Language / Structured Query Language

Wesentlich einfacher ist dies für den Endanwender über die Applikation möglich. Über das Formular (Abb. 59) können Inhalte unterschiedlicher Formate hochgeladen werden. Im hier besprochenen Beispiel werden Notfallprotokolle, Befunde und Patientendokumentation in der Datenbank gespeichert.

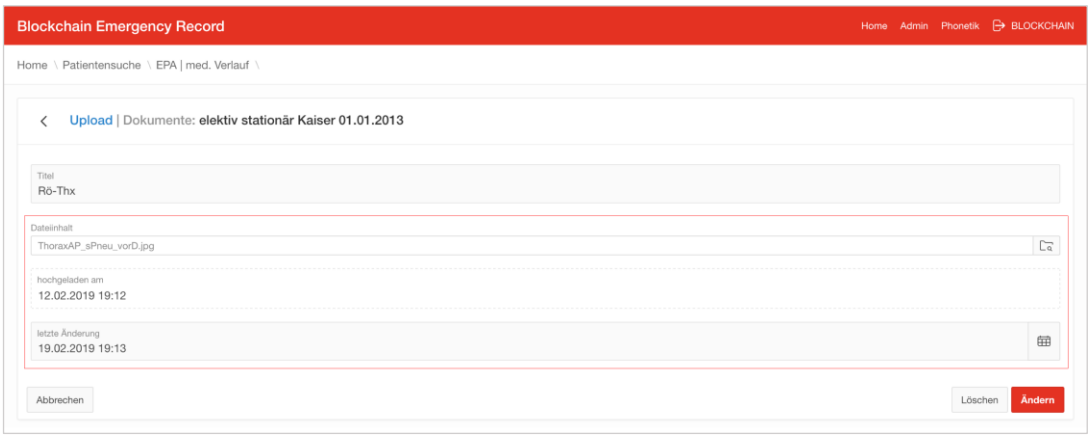


Abbildung 59: Upload und Download von Bildmaterial und medizinischen Dokumenten mit Zeitstempel
EPA = elektronische Patientenakte

Im Falle einer erneuten Untersuchung bzw. Weiterbehandlung können die Inhalte sicher, jederzeit, weltweit und ohne Medienbruch zur Verfügung gestellt werden.

3.3.5 Übersicht der Blockchain Diagnosen und Therapien

Die Liste der Einträge werden in der dritten Spalte „Tracerdiagnosen | Leitdiagnosen“ (Abb. 55) durch Auswahl des Symbols am unteren Bildrand angezeigt. Durch die Auswahl werden auf einer separaten Seite die zum Fall passenden Detailinformationen angezeigt (Abb. 60).

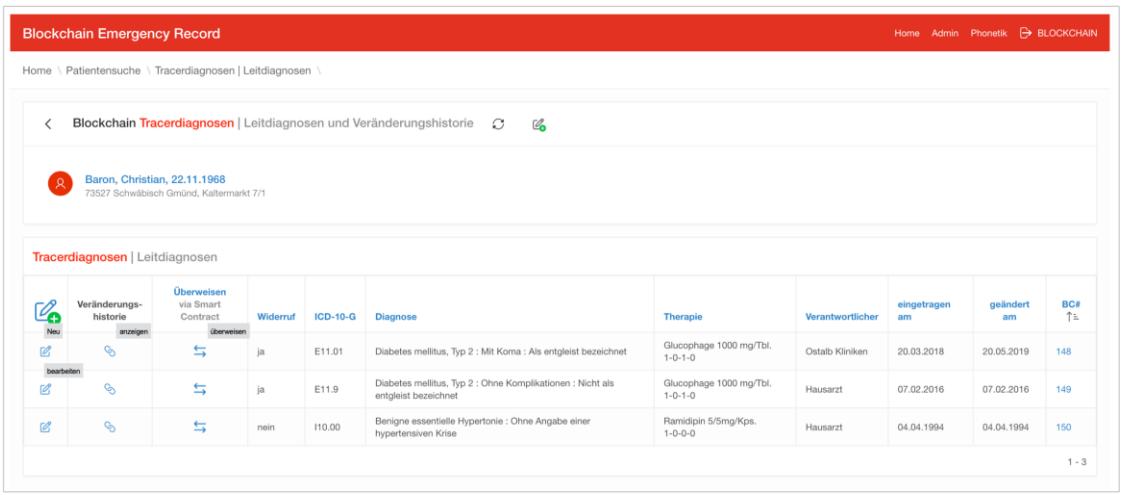


Abbildung 60: Bericht über bestehende Tracer-Diagnosen in der Blockchain

Sind die passenden Datensätze ermittelt, zeigt der Bericht die vorhandenen Einträge an. Als weitere Auskunftsmöglichkeit wird die Historienfunktion der Blockchain genutzt (getHistoryForRecord). Diese Funktion ist eine der wichtigsten Eigenschaften der Blockchain, um Nachvollziehbarkeit, Transparenz und Unveränderlichkeit zu garantieren. Über das „Kettensymbol“ der zweiten Spalte (Abb. 60) im Bericht kann die Veränderungshistorie der Tracer-Diagnosen passend zu vorhandenen abgerufen werden. Die letzte Spalte BC# des Berichts wurde zunächst für die Migration der Blockchain-Einträge in die Datenbankstruktur entworfen, um als Referenz für die späteren Performance-Messungen herangezogen werden zu können. Die Funktion stellt zusätzlich eine Interoperabilitäts-Möglichkeit zwischen unterschiedlichen Blockchain-Herstellern zur Verfügung. Die im Formular dargestellten Inhalte würden in diesem Fall über die REST-Schnittstelle in jede beliebige Blockchain-Plattform übertragen werden können.

Entwickleransicht zur Abbildung 60

Der „Quellcode“ der zum Bericht (Abb. 60) passenden Seite, die im Entwicklungsprozess entstanden ist, stellt sich in Abbildung 61 dar. Das SQL-Statement im Vordergrund bearbeitet die von der Blockchain kommenden Ergebnisse nach.

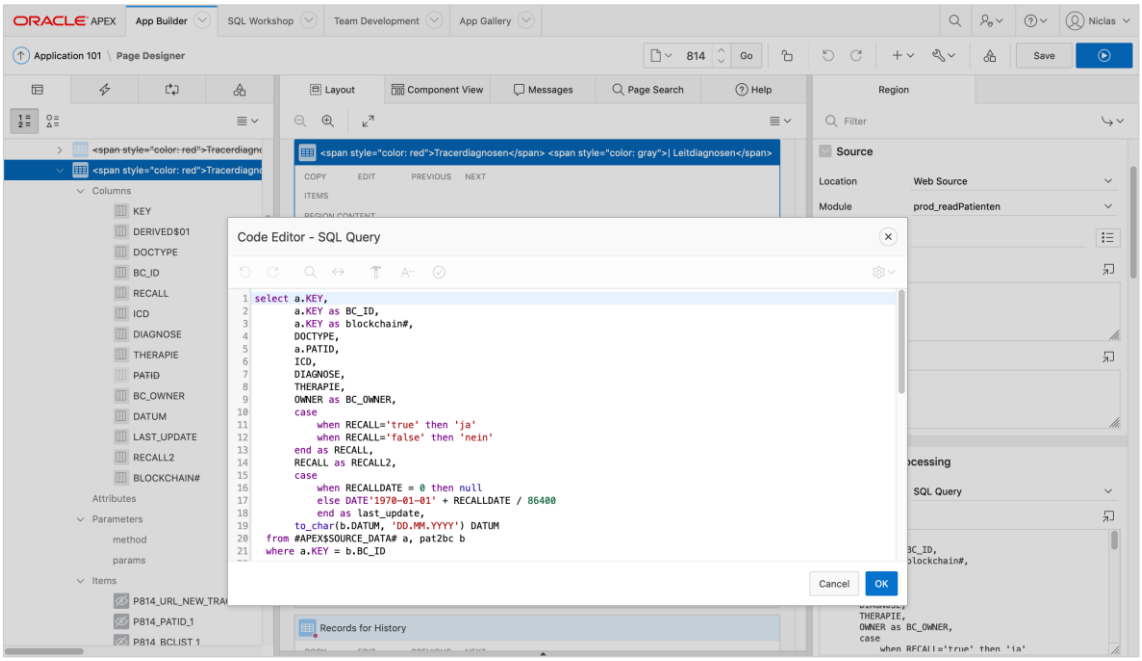


Abbildung 61: APEX-Page Designer zur Entwicklung der Berichte und Formulare / APEX = Application Express

„Copyright Oracle and its affiliates. Used with permission.“

3.3.6 Überweisung Facharzt – Weitergabe des digitalen Behandlungsrechts

Der Prozess für die Überweisung (Abb. 62) an den Facharzt wird über den „Link“ in der Spalte „Überweisen via Smart Contract“ durch Auswahl des Pfeilsymbols ⇆ in der ersten Spalte des Berichts initiiert. Entweder durch den Patienten oder Arzt.

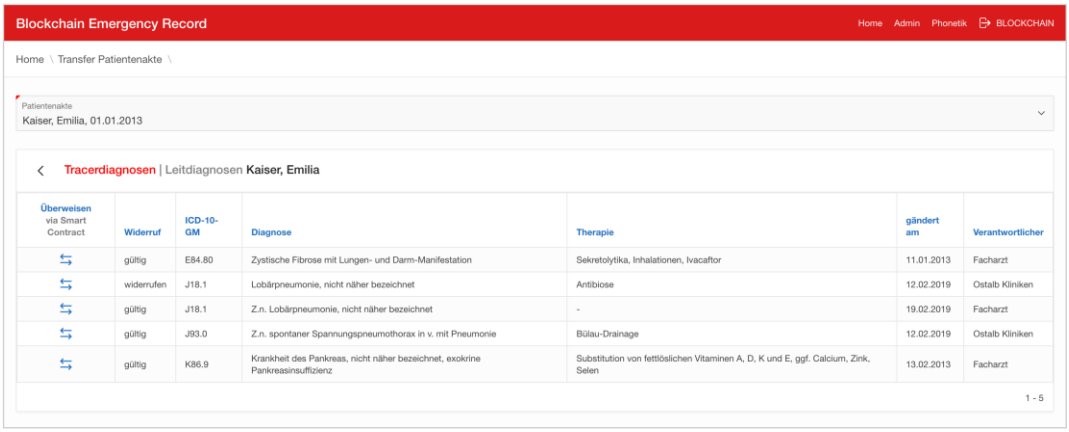


Abbildung 62: Übertragung des Behandlungsrechts oder Tranfer der Patientenakte

3.3.7 Neuaufnahme von Diagnosen und Therapien in der Blockchain

Für die Eingabe und das Ändern von Diagnosen bei bestehenden Patienten steht ein Formular zur Verfügung (Abb. 63), welches über einen APEX-Prozess die Daten in die Blockchain speichert. Als weitere Funktion kann die Diagnose bzw. die Therapie mit einem Widerruf versehen werden, Diagnosen und Therapien angepasst bzw. bei existierenden Einträgen kann der Befund als gelöscht markiert werden.

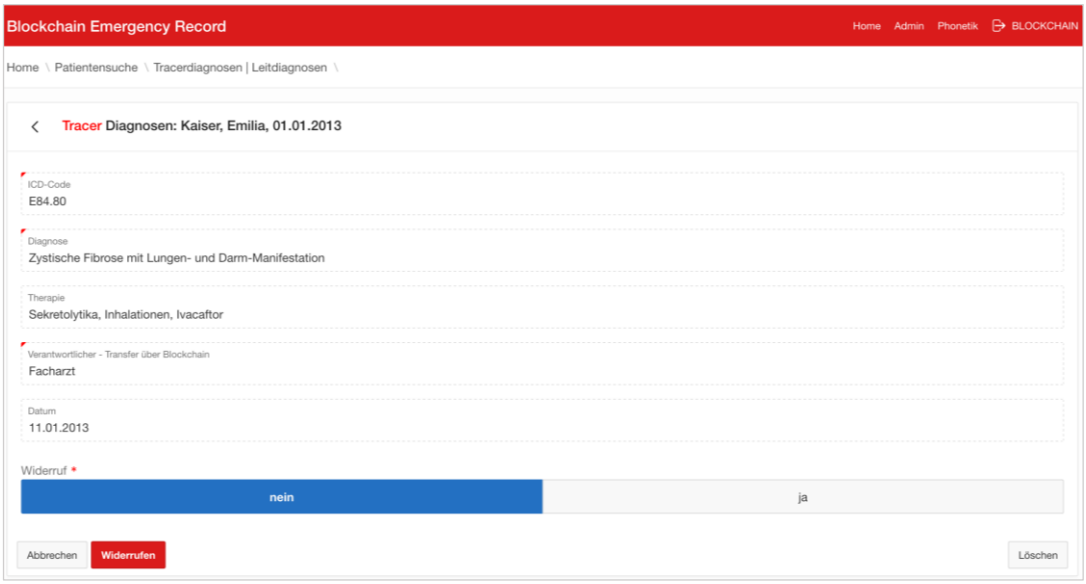


Abbildung 63: Formular für Änderung und Neuaufnahme von Diagnosen und Therapien mit Statusinformation

Der Widerruf einer Einzeldiagnose wird in der Blockchain automatisch mitprotokolliert und unveränderbar abgespeichert. Das Formular wird sowohl für die Neuaufnahme als auch für das Löschen von Diagnosen und Therapien verwendet.

3.3.8 Löschen von Diagnosen und Therapien in der Blockchain

Grundsätzlich gilt bei Blockchain-Anwendungen, dass keine Transaktion und die zugehörigen Daten gelöscht werden können. In der umgesetzten Anwendung werden „gelöschte“ Transaktionen bzw. Inhalte mit einem Attribut „isDelete“ versehen, d.h. diese existieren in der Blockchain weiter. Ausgelöst wird dies über den „Löschen“ Button in der Oberfläche der Applikation. Daraufhin wird der Datensatz in der Historiendatenbank der Blockchain gespeichert und kann nicht mehr verändert werden. Der zuständige Prozess dafür ist “UD_Blockchain (Update/Delete)” (Abb. 64). Für Testzwecke wurde die Historie zusätzlich in der Tabelle „PAT2DEL“ (Abb. 50) in der Datenbank gespeichert. Dies hat den Vorteil, dass eine einfache Möglichkeit besteht, die Historie in Form eines Berichts abzufragen.

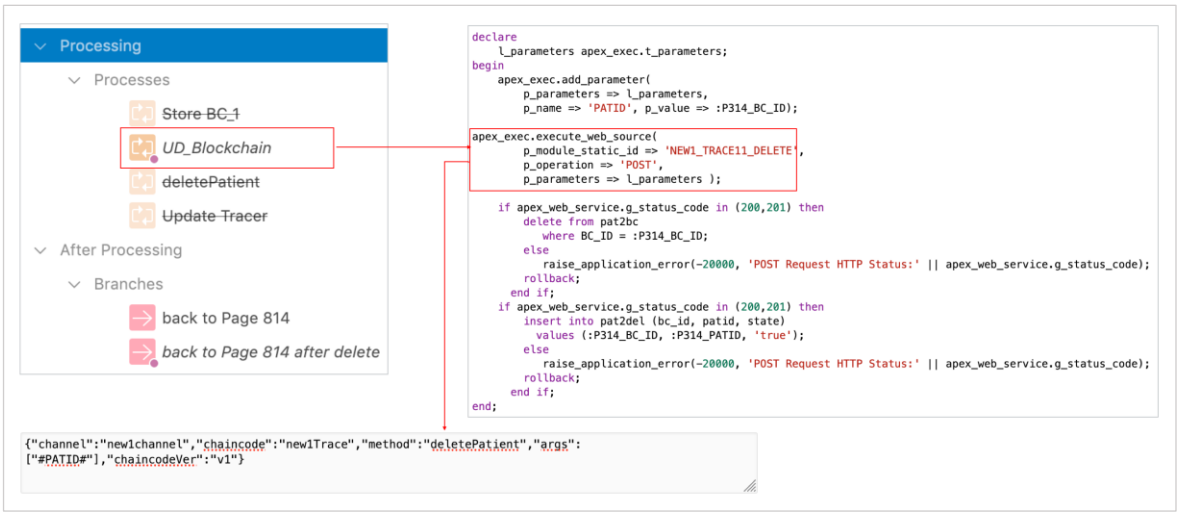


Abbildung 64: Prozess zur Markierung einer Transaktion mit dem isDelete-Merkmal

3.3.9 Administration und Migration der Blockchain-Einträge

Die Administrationsmöglichkeiten (Abb. 65) beziehen sich auf die Pflege der Blockchain-Personen, der Kontrolle der Blockchain-Einträge in der Mapping-Tabelle, der Eingabe von Stammdaten der ICD-10 Codes und der Migrationsmöglichkeit. Diese Funktionen stehen nur für autorisierte Benutzer zur Verfügung. Ein Autorisierungsschema verhindert den Zugriff ohne entsprechendes Privileg.

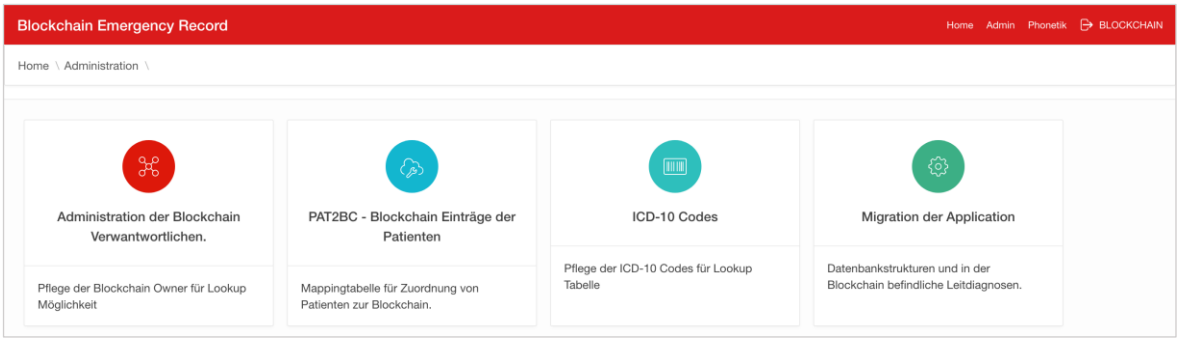
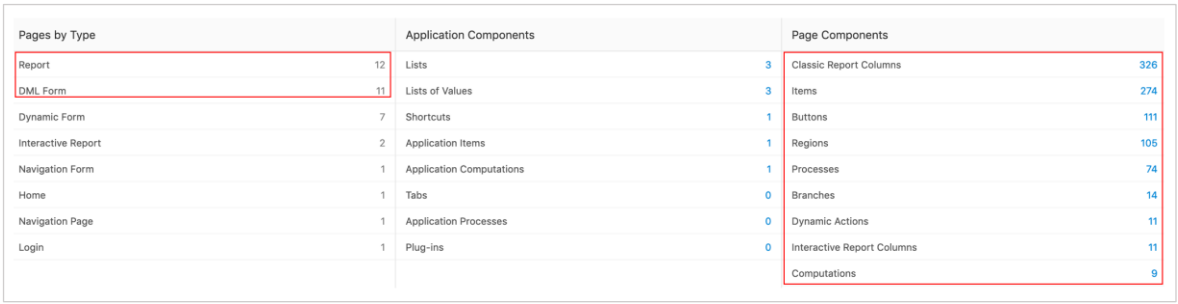


Abbildung 65: Administrationsmöglichkeiten

Bei der Softwareentwicklung entsteht die Dokumentation der Ergebnisse im Idealfall parallel zur Entwicklung. In der Realität werden Bedienungsanleitungen am Ende der Softwareentwicklung erstellt. Bei der Entwicklung einer APEX-Applikation dokumentiert diese sich rudimentär selbst (Abb. 66) und gibt Aufschluss über die entwickelten Objekte, z.B. 12 Berichte, 11 Formulare und 326 Felder.



Pages by Type		Application Components		Page Components	
Report	12	Lists	3	Classic Report Columns	326
DML Form	11	Lists of Values	3	Items	274
Dynamic Form	7	Shortcuts	1	Buttons	111
Interactive Report	2	Application Items	1	Regions	105
Navigation Form	1	Application Computations	1	Processes	74
Home	1	Tabs	0	Branches	14
Navigation Page	1	Application Processes	0	Dynamic Actions	11
Login	1	Plug-ins	0	Interactive Report Columns	11
				Computations	9

Abbildung 66: Auswertung von genutzten und entwickelten APEX-Komponenten / APEX = Application Express

„Copyright Oracle and its affiliates. Used with permission."

Somit ist das Ziel der Dissertation, welches sich mit der Entwicklung und Dokumentation der „Blockchain Emergency App" beschäftigt hat, erfolgreich abgeschlossen. In den folgenden Abschnitten werden weitere Teilergebnisse wie Produktreife und Betriebsaspekte betrachtet.

3.4 Messergebnisse und Statistik

Gemessen wurde immer die durchschnittliche Antwortzeit in Millisekunden mit anschließender Umrechnung in Sekunden. Latenzzeiten (Verzögerungen) durch Netzwerkverbindungen können in der Umgebung vernachlässigt werden, da alle Komponenten in der virtuellen Maschine ablaufen und die Datenmengen zu gering sind.

3.4.1 Messergebnisse Blockchain mit REST-Gateway

Für die Zeitmessungen wurden die im Chaincode entwickelten Funktionen direkt über eine URL-Syntax vom Betriebssystem (Abb. 67) aufgerufen.

```
curl -H "Content-type:application/json" -X POST http://oabcs-vm:3100/bcsgw/rest/v1/transaction/query \
     -d'{"channel":"new1channel","chaincode":"new1Trace","method":"readPatienten","args":["153"],"chaincodeVer":"v1"}'
```

Abbildung 67: Beispiel für die Abfrage der Blockchain mittels „query“-Methode auf Kommandozeile mit curl
cURL = Client for URL

Um die Kommandos für den cURL-Zugriff (Abb. 67) zu generieren wurden die Daten mittels APEX aus der Blockchain in die Datenbank übertragen. Am Ende wurden die Daten mit Hilfe von SQL-Befehlen (Abb. 68) als Datei gespeichert und konnten wie ein Betriebssystem-Skript automatisiert ausgeführt werden.

```
##!bin/bash
##
## Script für die Erstellung der Testdaten: Daten werden über die REST API in die Datenbank via curl geschrieben
## Die curl-Aufrufe werden dynamisch via SQL erzeugt.
##
## wichtig: Tabellenspalte muss eine Spalte vom Type timestamp sein, sonst gibt es beim insert und update Probleme mit dem TZ Format -- YYYY-MM-DD"T"HH24:MI:SSTZR

## Zuerst muss das im Schema befindliche Object freigeschaltet werden. Entweder mittels SQL-Befehl oder mit Hilfe des SQL Developers
## Verbidnung wählen -> Tables -> BC_DATA -> rechte Maustaste und Menüpunkt "Enable REST Service" auswählen
## -> Checkbox für Enable object setzen
## -> Textfeld Object alias: vorausgefüllt
## -> Checkbox Authorization required nicht setzen
## -> Finish Button
#
#begin
#    ords.enable_schema;
#    ords.enable_object( p_object => 'BC_DATA' );
#end;
#/
#
## Tests
#   curl -X GET http://192.168.56.101:8181/ords/blockchain/bc_data
#    Browser: http://192.168.56.101:8181/ords/blockchain/bc_data
#
# select 'curl -H ' || '"' || 'Content-Type:application/json' || '"' from dual;
select 'curl -H ' || '"' || 'Content-Type:application/json' || '"' || '-d {' || '"' || 'BCID'||':' ||'"'||BCID as dbcurl from bc_data

select 'curl -H '    || '"' || 'Content-Type:application/json' || '"' || ' -X POST -d ' || ''''||'{' || '"' ||'BCID'||'"'||':'||BCID||',' ||
'"' || 'PATID'       || '"' || ':' || '"' || PATID || '"' || ',' ||
'"' || 'ICD'         || '"' || ':' || '"' || ICD || '"' || ',' ||
'"' || 'DIAGNOSE'    || '"' || ':' || '"' || DIAGNOSE || '"' || ',' ||
'"' || 'THERAPIE'    || '"' || ':' || '"' || THERAPIE || '"' || ',' ||
'"' || 'OWNER'       || '"' || ':' || '"' || OWNER    || '"' || ',' ||
'"' || 'RECALL'      || '"' || ':' || '"' || RECALL   || '"' || ',' ||
'"' || 'RECALLDATE' || '"' || ':' || '"' || to_char(RECALLDATE,'YYYY-MM-DD"T"HH24:MI:SS"Z"') || '"' || '}' ||
''''|| ' http://localhost:8181/ords/blockchain/bc_data2/' as dbcurl from bc_data
/
-- Ergebnis: curl Kommandos und passende Daten für den Aufruf über den ORDS

curl -H "Content-Type:application/json" -X POST -d '{"BCID":153,"PATID":"42","ICD":"I10.91","DIAGNOSE":"Essentielle Hypertonie, nicht näher bezeichnet : Mit Angabe einer hypertensi
ven Krise","THERAPIE":"Atacand Plus (Candesartan + Hydrochlorothiazid) 32/25 mg/Tbl. 1-0-0-0","OWNER":"Hausarzt","RECALL":"nein","RECALLDATE":"1976-02-06T00:00:00Z"}' http://localh
ost:8181/ords/blockchain/bc_data2/
curl -H "Content-Type:application/json" -X POST -d '{"BCID":154,"PATID":"42","ICD":"I71.01","DIAGNOSE":"Dissektion der Aorta thoracica, ohne Angabe einer Ruptur","THERAPIE":"-","OW
NER":"Uniklinik Ulm","RECALL":"nein","RECALLDATE":"2019-02-12T00:00:00Z"}' http://localhost:8181/ords/blockchain/bc_data2/
curl -H "Content-Type:application/json" -X POST -d '{"BCID":150,"PATID":"64","ICD":"I10.00","DIAGNOSE":"Benigne essentielle Hypertonie : Ohne Angabe einer hypertensiven Krise","THE
RAPIE":"Ramidipin 5/5mg/Kps. 1-0-0-0","OWNER":"Hausarzt","RECALL":"nein","RECALLDATE":"1994-04-04T00:00:00Z"}' http://localhost:8181/ords/blockchain/bc_data2/
curl -H "Content-Type:application/json" -X POST -d '{"BCID":149,"PATID":"64","ICD":"E11.9","DIAGNOSE":"Diabetes mellitus, Typ 2 : Ohne Komplikationen : Nicht als entgleist bezeichn
et","THERAPIE":"Glucophage 1000 mg/Tbl. 1-0-1-0","OWNER":"Hausarzt","RECALL":"ja","RECALLDATE":"2016-02-07T00:00:00Z"}' http://localhost:8181/ords/blockchain/bc_data2/
curl -H "Content-Type:application/json" -X POST -d '{"BCID":148,"PATID":"64","ICD":"E11.01","DIAGNOSE":"Diabetes mellitus, Typ 2 : Mit Koma : Als entgleist bezeichnet","THERAPIE":"
Glucophage 1000 mg/Tbl. 1-0-1-0","OWNER":"Ostalb Kliniken","RECALL":"nein","RECALLDATE":"2018-03-20T00:00:00Z"}' http://localhost:8181/ords/blockchain/bc_data2/
```

Abbildung 68: Auszug aus dem entwickelten SQL-Skript zur Generierung der Testaufrufe und Daten über den ORDS
SQL = Structured Query Language / ORDS = Oracle REST Data Services
REST = Representational State Transfer

Das Antwort-/Zeitverhalten des Systems bei Abfragen der Patientendaten ist schnell und nahezu stabil in der Geschwindigkeit, wie in Tabelle 2 zu erkennen ist. Dabei wird die „readPatienten“-Funktion über die URL als „query“-Methode in der URL ausgeführt.

Tabelle 2: Ergebnisse Performancemessung mittels Postman mit der readPatienten-Funktion
Tx = Transaktion / avg. = durchschnittlich / sec. = Sekunden / ms = Millisekunden

readPatienten / query					
Tx	avg. response time	Messung 1	Messung 2	Messung 3	Messung 4
	sec.	ms	ms	ms	ms
1	0,06	56	72	57	67
10	0,08	84	67	113	74
20	0,13	86	70	88	276

Die Tabelle 3 zeigt eine durch die „invocation“ Methode in der URL ausgeführte Transaktion und deren durchschnittliche Dauer. Die Funktion des Chaincodes „setPatientRecallState“ ändert den Status einer Diagnose bzw. einer Therapie (Widerruf) des Patienten.

Tabelle 3: Ergebnisse Performancemessung mittels Postman mit der setPatientRecallState-Funktion
Tx = Transaktion / avg. = durchschnittlich / sec. = Sekunden / ms = Millisekunden

setPatientRecallState / query					
Tx	avg. response time	Messung 1	Messung 2	Messung 3	Messung 4
	sec.	ms	ms	ms	ms
1	0,063	66	79	62	46
10	0,085	98	106	81	53
20	0,080	92	62	90	75

Im Gegensatz zur „query“-Methode wird durch den Aufruf „invocation“ die Transaktion tatsächlich ausgeführt. Die an der Blockchain beteiligten Rechner bzw. Organisation durchlaufen den gesamten „Konsens“-Mechanismus, bevor Daten geändert und in die Blockchain aufgenommen werden. Dies hat einen gravierenden Anstieg der Antwortzeit zur Folge, wie in Tabelle 4 in der Spalte „avg response time“ (durchschnittliche Antwortzeit) zu erkennen ist.

Tabelle 4: Ergebnisse Performancemessung mittels Postman mit der setPatientRecallState-Funktion
Tx = Transaktion / avg. = durchschnittlich / sec. = Sekunden / ms = Millisekunden

setPatientRecallState / invocation					
Tx	avg response time	Messung 1	Messung 2	Messung 3	Messung 4
	sec.	ms	ms	ms	ms
1	2,16	2181	2143	2164	2144
10	2,16	2169	2224	2131	2106
20	2,24	2495	2145	2190	2141

Die ersten beiden Spalten „Tx“ (Anzahl Transaktionen) und „avg response time“ der Tabelle 4 stellen das Antwortzeitverhalten bei der Erfassung einer Diagnose und Therapie dar. Bei Tabelle 5 zeigen die letzten beiden Spalten „Tx“ und „response time“ die Antwortzeit beim Löschen eines Datensatzes.

Tabelle 5: Performancevergleich initPatient vs. deletePatient-Funktion
Tx = Transaktion / sec. = Sekunden

initPatient / invocation		deletePatient / invocation	
Tx	response time	Tx	response time
	sec.		sec.
1	2,14	1	2,14
10	2,19	10	2,20
20	2,16	20	2,10

Fazit: Performance Blockchain und REST-Gateway

Die Testreihen zeigen, dass die Antwortzeiten beim Erfassen und Löschen von Daten in der Blockchain nahezu identisch sind. Gleiches gilt, wenn der Status der Diagnose bzw. Therapie verändert wird. Das bedeutet, dass die Antwortzeit in Bezug auf die gewählte Konfiguration stabil bleibt. Dies ist unabhängig von der Transaktionsart und bei zunehmendem Transaktionsvolumen. Die Antwortzeit in Bezug auf lesende Operationen ist beim Funktionsaufruf über das REST-Gateway der Blockchain sehr gut und vergleichbar mit etablierten Datenbanksystemen.

3.4.2 Messergebnisse Oracle Datenbank und ORDS

Für die Referenzwertbestimmung eignet sich die bestehende Datenbank, da diese die Grundlage der Applikationsentwicklung und eine Standardinfrastruktur darstellt. Für die Messungen wurden die Transaktionen über den ORDS in eine der Chaincode-Struktur gleichwertigen Tabellenstruktur übersetzt. Beim Aufruf der Datenbankoperation über das http-Protokoll (Hypertext Transfer Protokoll) muss die sogenannte „rowid“ als Parameter am Ende der URL (Abb. 69) mit übergeben

werden. Um dies zu automatisieren, wurden mit Hilfe eines SQL-Befehls die gespeicherten Datensätze als Bericht abgefragt und somit die notwendigen curl-Kommandos für die Tests generiert.

```
# Dateiname
#       04_select_from_bc_data4.sql
#
# Pfad
#       /home/bcsdemo/new1Trace-Zeitmessung
#
# Zweck
#       Generierung der Kommandos für die automatisierte Zeitmessung
#
# Kommentar
#       Die Datensätze müssen vorab in die Datenbank geladen werden, danach können die Anweisungen erzeugt werden
#
# SQL Statement
#       select 'curl -X GET ' || '"' ||'http://192.168.56.101:8181/ords/blockchain/bc_data4/' || ROWID ||'"'
#       from bc_data4
#       where rownum <11
#       order by bcid
#/
# Output

curl -X GET "http://192.168.56.101:8181/ords/blockchain/bc_data4/AAATGFAAMAAAA4TAAA"
curl -X GET "http://192.168.56.101:8181/ords/blockchain/bc_data4/AAATGFAAMAAAA4TAAB"
curl -X GET "http://192.168.56.101:8181/ords/blockchain/bc_data4/AAATGFAAMAAAA4TAAC"
curl -X GET "http://192.168.56.101:8181/ords/blockchain/bc_data4/AAATGFAAMAAAA4TAAD"
curl -X GET "http://192.168.56.101:8181/ords/blockchain/bc_data4/AAATGFAAMAAAA4TAAE"
curl -X GET "http://192.168.56.101:8181/ords/blockchain/bc_data4/AAATGFAAMAAAA4TAAF"
curl -X GET "http://192.168.56.101:8181/ords/blockchain/bc_data4/AAATGFAAMAAAA4TAAG"
curl -X GET "http://192.168.56.101:8181/ords/blockchain/bc_data4/AAATGFAAMAAAA4TAAH"
curl -X GET "http://192.168.56.101:8181/ords/blockchain/bc_data4/AAATGFAAMAAAA4TAAI"
curl -X GET "http://192.168.56.101:8181/ords/blockchain/bc_data4/AAATGFAAMAAAA4TAAJ"
```

Abbildung 69: Auszug aus dem entwickelten SQL-Skript 04_select_from_bc_data4.sql“

SQL = Structured Query Language

Mit Hilfe des Postman-Programms wurden die Anforderungen (Requests) in der Datei „new1Trace-Postman-Collection.json“ zusammengefasst. Für die automatisierte Ausführung kam der Collection Runner als Komponente zum Einsatz. Diese erlaubt es mehrere Durchläufe pro Messung auszuführen. Die Datenmenge und die Varianz der Daten sind gering, d.h. auf zufällig generierte Daten kann verzichtet werden. Etwaige Caching-Effekte wurden vernachlässigt, da die Datenmengen zu klein sind. Die Tabellen 6,7,8 zeigen die gemessenen Zeiten.

Tabelle 6: Antwortzeit beim Abfragen von Diagnosen und Therapien über ORDS in die Datenbank

Tx = Transaktion / avg. = durchschnittlich / sec. = Sekunden / ms = Millisekunden

ORDS = Oracle REST Data Services / REST = Representational State Transfer

select Patienten / ORDS + Datenbank						
Tx	avg. response time	Messung 1	Messung 2	Messung 3	Messung 4	Messung 5
	sec.	ms	ms	ms	ms	ms
1	0,109	132	135	98	70	-
10	0,106	102	94	106	127	100
20	0,108	96	118	131	89	125
		116	101	97	103	106

Tabelle 7: Antwortzeit beim Erfassen von Diagnosen und Therapien über ORDS in die Datenbank

Tx = Transaktion / avg. = durchschnittlich / sec. = Sekunden / ms = Millisekunden

ORDS = Oracle REST Data Services / REST = Representational State Transfer

	insert Patienten / ORDS + Datenbank					
Tx	avg. response time	Messung 1	Messung 2	Messung 3	Messung 4	Messung 5
	sec.	ms	ms	ms	ms	ms
1	0,15	146	-	-	-	-
10	0,17	170	131	164	196	182
20	0,16	227	125	157	142	159
		159	179	152	124	164

Tabelle 8: Antwortzeit beim Löschen von Diagnosen und Therapien über ORDS in die Datenbank

Tx = Transaktion / avg. = durchschnittlich / sec. = Sekunden / ms = Millisekunden

ORDS = Oracle REST Data Services / REST = Representational State Transfer

			delete Patienten / ORDS + Datenbank			
Tx	avg response time	Messung 1	Messung 2	Messung 3	Messung 4	Messung 5
	sec.	ms	ms	ms	ms	ms
1	0,13	106	186	84	139	-
10	0,12	123	137	132	106	115
20	0,10	111	89	97	115	110
		89	107	120	91	86

Fazit: Performancebetrachtung Oracle Datenbank und ORDS

Die Antwortzeiten der Datenbank sind bei allen Operationen unter einer Sekunde. Das ist verständlich, denn die Daten liegen nach dem ersten Aufruf im Datenbankcache. Die meiste Zeit wird über den REST-Zugriff vom ORDS verbraucht. Lineare Skalierung ist auch ohne Messung aufgrund der Verbreitung des Oracle Datenbanksystems zu erwarten und stellt keinen Engpass dar.

3.4.3 Performancevergleich Blockchain und Datenbank

Beim Lesen der Diagnosen und Therapien kann es aufgrund von Caching-Effekten Ausreiser geben, die jedoch die Gesamtbetrachtung nicht beeinflussen (Abb. 70).

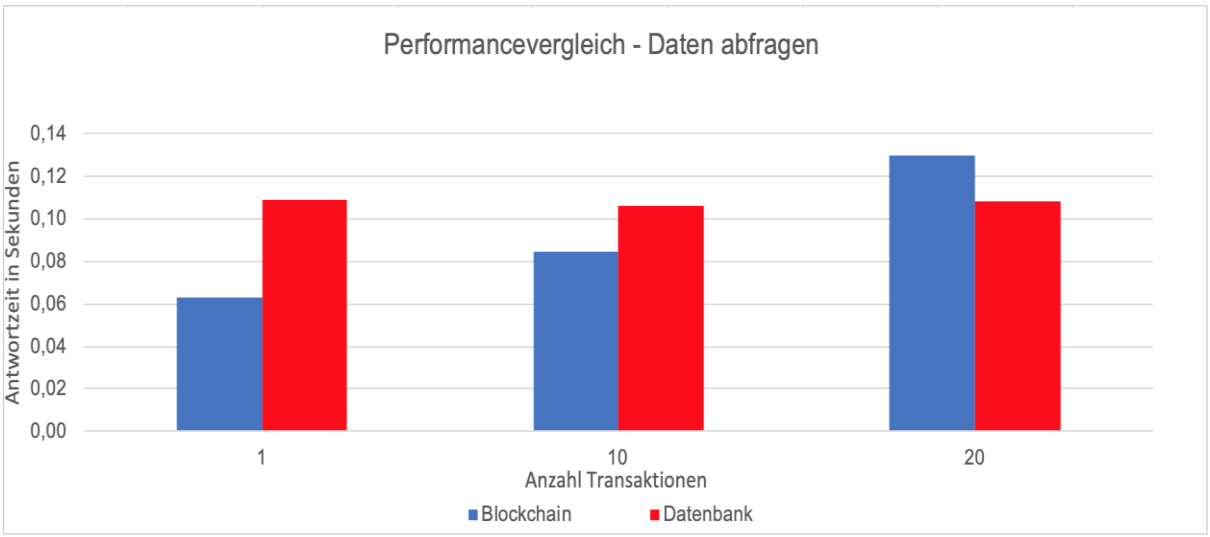


Abbildung 70: Vergleich Antwortzeiten beim Abfragen von Diagnosen und Therapien

Werden die Werte aus Tabelle 7 (InsertPatienten) und Tabelle 8 (DeletePatienten) zu den Messwerten aus Tabelle 5 (Performancevergleich: initPatient/deletePatient) ins Verhältnis gesetzt, ergibt sich ein 14-facher Performancefaktor zu Gunsten der Datenbank bei der Erfassung von Diagnosen bzw. Therapien.

Das gleiche Verhältnis (Abb. 71) ist für die Transaktionen festzustellen, die die Patientendiagnosen in der APEX-Anwendung ändern und löschen.

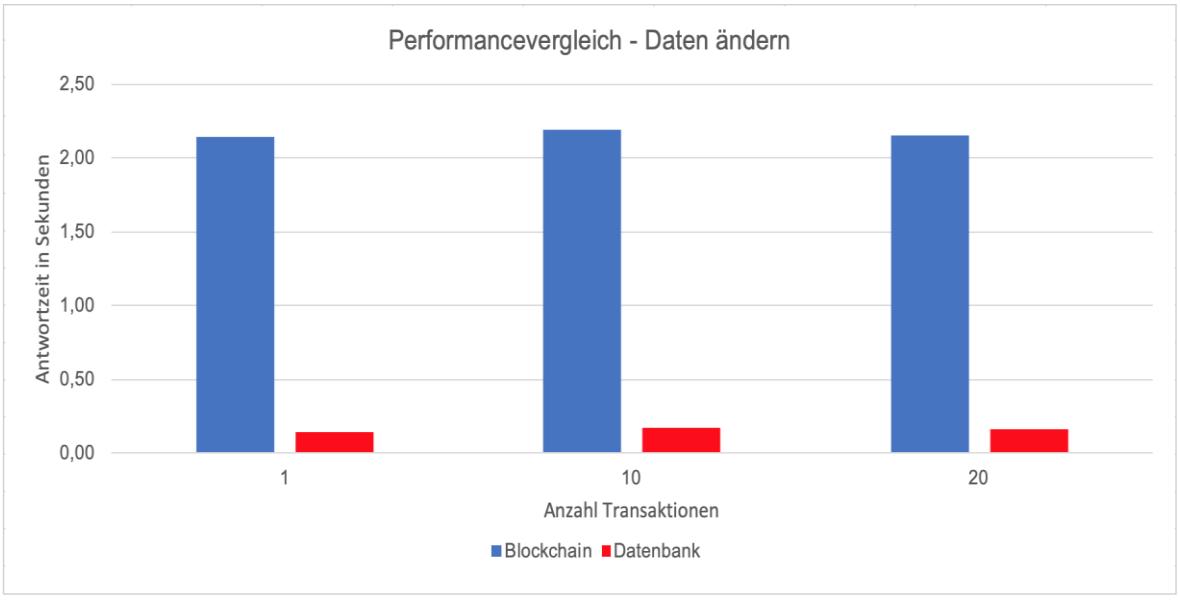


Abbildung 71: Vergleich Antwortzeiten beim Erfassen von Diagnosen und Therapien

Fazit: Performancevergleich Blockchain und Datenbank

Werden die Messwerte bei vergleichbaren Operationen gegenübergestellt, ist die Datenbank die schnellere Variante. Die für die Dissertation entwickelte Blockchain ist verhältnismäßig einfach strukturiert und zeigt bei lesenden Operationen gleichwertige Ergebnisse in Bezug auf die relationale Datenbank. Die Performance des Gesamtsystems und die damit verbundene Skalierung ist eine Schwachstelle der Blockchain-Technologie und bleibt eines der wichtigsten von der Industrie zu lösenden Aufgaben. Diese ist durch die verteilte Datenhaltung und die Konsens-Mechanismen vorgegeben und lässt sich nur durch entsprechende Betriebsformen verbessern. Aus dem Antwort-/Zeitverhalten lässt sich ableiten, dass eine Speicherung von unstrukturierten Informationen in der Blockchain zu aufwendig und teuer ist. Die Blockchain ist für Anwendungen, die auf hohe Performance Wert legen ungeeignet [14]. Im Bereich der Healthcare-Applikationen gibt es darüber hinaus noch wenig Erfahrungswerte, da die Partner ihre Anwendungen zunächst auf sinnvollen Einsatz prüfen und zertifizieren müssen. Diese Fragestellung wird auch von Leeming et al. [29] diskutiert und als Herausforderung betrachtet. Die Performance ist bei Endanwendern, neben dem Fachlichen, das wichtigste Kriterium für die Akzeptanz von Anwendungen.

3.5 Blockchain-Produktreife

Obwohl die Blockchain-Technologie seit zehn Jahren bekannt ist, findet die Weiterentwicklung in extrem kurzen Release-Zyklen statt. Dies macht deutlich, dass viele Funktionen für einen produktiven Einsatz verbessert oder neu entwickelt werden müssen. Während der Dissertation wurden von der Oracle Corporation mehrere Updates zur Datenbank, Application Express, SQL Developer, ORDS, Oracle Linux Betriebssystem, VirtualBox und dem Blockchain SDK geliefert. Dies hatte eine permanente Einarbeitung in die neuen Produktversionen, Schnittstellen sowie mehrere Updates und Migrationen zur Folge. Eine hohe Fehlertoleranz war notwendig, um die technischen Unverträglichkeiten der unterschiedlichen Softwarekomponenten auszugleichen und dennoch das Gesamtsystem stabil am Laufen zu halten. Teilweise war das Verhalten der Softwarekomponenten nach dem Update unterschiedlich, so dass Schnittstellen wieder angepasst werden mussten. Funktionen, die bei relationalen Datenbanken mit einer SQL-Anweisung ausgeführt werden, müssen bei der Blockchain als fachliche Logik programmiert werden.

Automatisierte Startverfahren für die Datenbank und den ORDS wurden entwickelt und eingerichtet.

3.6 Betriebsmodelle von Blockchain-Lösungen

Die für die Dissertation genutzte Umgebung besteht aus einer virtuellen Maschine, die alle für die in der Entwicklung benötigten Komponenten beinhaltet. Die genutzte Umgebung ist für eine Test-/Entwicklungs-Umgebung ideal, da keine Kosten entstehen und Standardkomponenten verwendet werden. Im Produktionsumfeld muss ein professioneller Betrieb dieser Infrastruktur gewährleistet werden. Neben den klassischen Aufgaben im IT-Betrieb kommen bei der Blockchain neue Aufgaben bezüglich der Dezentralität und die Komplexität hinzu. Unter diesem Aspekt ist die zukünftige Betriebsvariante ein ernstzunehmender Erfolgsfaktor für Projekte. Ein Datenbankadministrator, Netzwerk-, Speicher-, Betriebssystem- und Serververantwortliche müssten alle gemeinsam für einen unterbrechungsfreien Betrieb in der lokalen Infrastruktur zusammenarbeiten.

Eine mögliche Betriebsvariante wurde für die Entwicklung bereits erfolgreich getestet. Dabei handelt es sich um die Nutzung von „Infrastructure as a Service“ (IaaS) bei einem Cloudanbieter wie z.B. Oracle. Die Oracle VM VirtualBox wird in diesem Fall direkt in eine sogenannte „Compute Instanz“ exportiert (Abb. 8) und dort betrieben. Dies setzt die Erstellung einer Public-/Private-Key Wertepaares voraus, um die Sicherheitsanforderungen bei einer Cloudlösung abzusichern. Das ist heute gängige Praxis und kann eine Einsparung bei Lizenz- und Betriebskosten erzielen.

Bei den Betriebsmodellen können folgende Varianten unterschieden werden:

- **Platform as a Service (PaaS)**
  - Datenbank, ORDS und Blockchain stehen in der Cloud als Ablaufkomponenten zur Verfügung.

- **Infrastruktur as a Service und Plattform as a Service** (IaaS, PaaS)
  - Datenbank und ORDS als Compute Service in der Cloud
  - Blockchain als Plattform Service

- **Blockchain as a Service** (BaaS)
    - Dabei wird ausschließlich die Blockchain-Infrastruktur in der Cloud genutzt. Die bekannten Schnittstellen und Programmiermöglichkeiten können übernommen werden. Für einen funktionalen Test ist dies erfolgreich umgesetzt worden.
- **Hybrid**
    - Kombination aus lokaler Infrastruktur und Cloud
    - Datenbank, ORDS und die Apex Anwendung im Rechenzentrum des Krankenhauses oder deren Betreiber.

Fazit: Betriebsmodelle einer Blockchain-Infrastruktur

Alle Betriebsmodelle haben Ihre Vor- und Nachteile. Die Vorteile einer Cloud-Lösung liegen eindeutig im Betrieb, d.h. der Performance, der Skalierbarkeit, der Sicherheit, der weltweiten Verfügbarkeit, der Agilität und einem geringeren Administrationsaufwand.

3.7 Herausforderungen und Probleme

In den vorausgegangenen Kapiteln wurden die technischen Grundlagen, die Realisierung und Erkenntnisse dargelegt. Die aus der Aufgabenstellung erwachsenen notwendigen Maßnahmen führten nicht geradlinig zur Lösung des Problems. Vor allem der Bezug zur Medizin war lange Zeit unklar und ergab kein komplettes Bild.

Die ersten konzeptionellen Überlegungen sind in Abbildung 72 dargestellt. Damals ausgehend von der Annahme, dass nur der Patient mit den unterschiedlichen Organisationen bidirektional kommuniziert. Im Zuge der Weiterentwicklung der Arbeit, hat sich dies zu einem echten Blockchain-Netzwerk (Abb. 19) entwickelt, in dem alle Teilnehmer gleichberechtigt mit- und untereinander interagieren können.

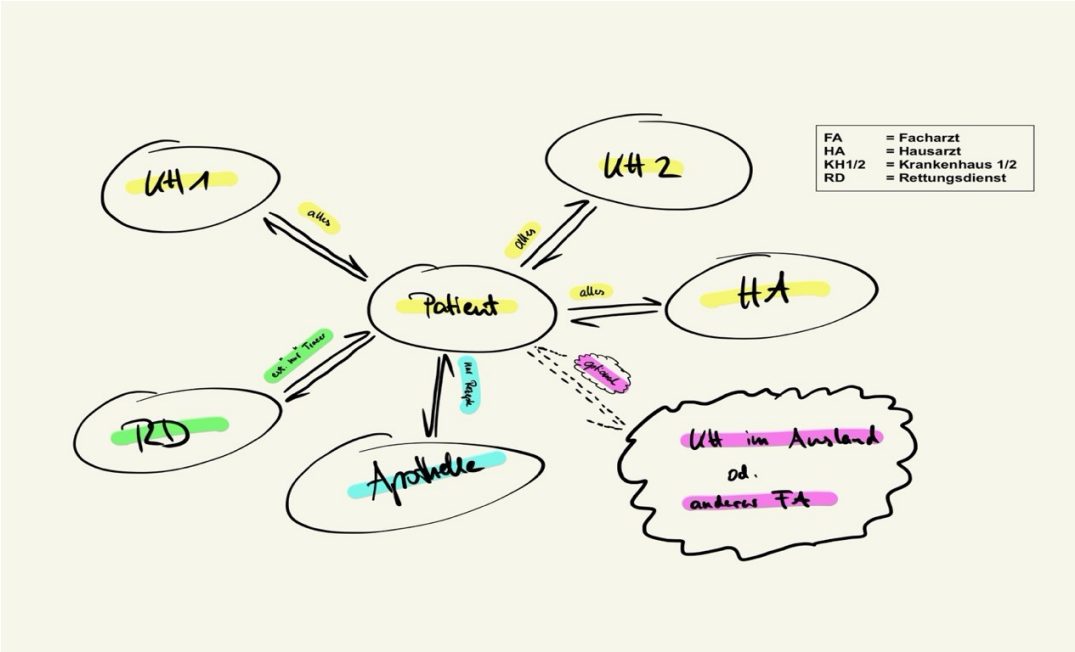


Abbildung 72: Entwurf des Blockchain-Netzwerks für die Dissertation

Im Internet stehen Fragmente von Lösungsansätzen zur Verfügung, aber kein durchgängig zu Ende gedachtes Beispiel mit einem realen Anwendungsfeld. Die Blockchain selbst ist für den Endanwender nicht sichtbar, stellt jedoch den wichtigsten, aufwendigsten und schwierigsten Teil dar. Den Nutzen einer sicheren Infrastruktur und einer möglichen Interoperabilität von Systemen im medizinischen Umfeld konnte ich aus den Erfahrungen im Rettungsdienst ableiten. Daher hat sich der Anwendungsfall zunächst auf die Notfallmedizin fokussiert. Die Ideen für eine Erweiterung der Anwendung in Richtung radiologischen Anwendungsmöglichkeiten entstanden durch die Diskussionen mit meinem späteren Doktorvater. Aus diesem Grund wurden Funktionen wie die Verwaltung von radiologischem Bildmaterial und die Pflege der Patientenhistorie (medizinischer Verlauf) entwickelt. In diesem Zusammenhang sind wertvolle Ideen entstanden, die auch der permanenten Veränderung und Entwicklung des Themas gerecht geworden sind.

Problem: Wahl des Blockchain-Designs

Es war offen, welche Komponenten benötigt werden, um ein reales Beispiel umzusetzen. Hinzu kam, dass ich zwar technisch versiert, aber kein Entwickler oder IT-Architekt bin. Grundsätzlich wurde eine Blockchain-Infrastruktur benötigt. Von vornherein war klar, dass es ein Cloud-Service sein sollte, damit Verfügbarkeit und ein weltweiter Zugriff jederzeit ermöglicht wird. Danach stellte sich die Frage, was die Kriterien sind, um einen passenden Anbieter auszuwählen. Bei meinen

Famulaturen und der Arbeit im Rettungsdienst hatte ich unterschiedliche KIS-Systeme kennengelernt, die oftmals auf dem relationalen Datenbanksystem der Firma Oracle Corporation basierten. Während der Auswahlphase wurde ein Blockchain-Cloud-Service von Oracle angekündigt. Nach der Ankündigung war ich mir sicher, dass es einfacher ist, die Komponenten eines Herstellers für meine Arbeit zu nutzen, d.h. Blockchain, Datenbank, Linux und APEX. Informationen, wie diese Infrastruktur verwendet werden kann, waren sehr oberflächlich in einem Whitepaper beschrieben. Vor allem die Schnittstellen waren allgemein dokumentiert. Die Firma Oracle hatte zunächst den Ansatz verfolgt, eine konfigurierbare Lösung anzubieten. Das hätte bedeutet, die Entwicklung der Chaincode-Funktionen wäre deklarativ mittels Vorlagen (engl. Templates) möglich gewesen. Das wurde von Oracle verworfen und eine Implementierung auf Standards wurde verwirklicht, was einleuchtete. Ein Cloud-Service wurde in einem Test-Account bereitgestellt. Die Schnittstellen waren zwar vorhanden, aber die Lösung war nur eingeschränkt nutzbar. Die Softwarestände des Cloud-Service unterschieden sich später von denen in der Virtuellen Maschine. Die Produktstrategie wurde ebenso schnell verändert, wie sich die Standards der Technologie weiterentwickelten. Das Innovationstempo war unglaublich hoch und kaum mitzuhalten. War Blockchain nur als eine Technologieplattform für Entwickler geplant, entschied das Unternehmen, sie nun als Basis von Branchenlösungen (z.B. Lieferketten) anzubieten, was eine Schnittstellenänderung und neue Versionen zur Folge hatte. Die Hoffnung auf einen leicht konfigurierbaren Cloud-Service ohne viel Programmierung war so nicht umsetzbar. Meine Erwartungen waren zu optimistisch. Die Zeitplanung verschob sich immer weiter nach hinten. Zu diesem Zeitpunkt waren bereits sechs Monate vergangen, in denen die Arbeit keinen Fortschritt machte und ausschließlich Recherche betrieben werden konnte. Im Prinzip war die Dissertation nicht wie geplant umsetzbar und schien zu Ende, noch bevor sie begonnen hatte. Vor allem der praktische Teil, der das Kernstück der Arbeit bildet.

Die Situation entschärfte sich erst, als Oracle Mitte 2018 eine virtuelle Maschine mit einer Blockchain-Infrastruktur und Beispielen bereitstellte. Das war der Zeitpunkt, an dem ich beginnen konnte, mir über die praktische Realisierung konkrete Gedanken zu machen. Nachdem die virtuelle Maschine stabil lief, musste

entschieden werden, wie das Blockchain-Netzwerk aufgebaut werden muss. Das beinhaltete, welche Personen bzw. Fachbereiche am Blockchain-Netzwerk teilnehmen sollen. Trotz fehlender Erfahrung und bestehendem Zeitdruck musste eine Architekturentscheidung getroffen werden. Auf welcher Basis sollte die Entscheidung getroffen werden, ohne die Auswirkungen dieser Festlegung auf die spätere Komplexität, die Entwicklung, den Betrieb und die Performance zu kennen? Hier half nur mutiges Vorangehen mit der Bereitschaft, eventuell auch zu scheitern. Im Nachhinein ist nicht mehr nachvollziehbar, wie häufig die Bezeichnungen, Teilnehmer und Organisationen verändert wurden und wieviele Fehlversuche stattfanden. Schätzungsweise waren mehr als zwanzig Iterationen notwendig, um eine passende Variante für die Strukturen zu finden, die als Ablaufumgebung für die spätere fachliche Logik und mein Beispiel passte. Manchmal war bei einer Problemlösung einfach Glück im Spiel, wenn ein passendes Beispiel in einem BLOG bei der APEX-Programmierung gefunden wurde. Für das Verständnis ist es wichtig, dass das Blockchain-Netzwerk, der „Chaincode“ und die Applikation zusammenpassen müssen. Nachdem das Blockchain-Netzwerk (Kapitel 2) aufgebaut war, mussten deren Schnittstellen verstanden und getestet werden.
Um auf die Blockchain von außen zugreifen zu können, gibt es nur die REST-Schnittstelle (Abbildung 34), d.h. alle Programme müssen die Möglichkeit besitzen, darüber zu kommunizieren. Dies hat auch entscheidenden Einfluss auf die für die Entwicklung der Oberfläche möglichen Entwicklungswerkzeuge.

Problem: Chaincode-Entwicklung

Nachdem klar war, wie die Blockchain funktioniert, musste entschieden werden, welche Daten in der Blockchain abgespeichert werden sollen und welche in der Datenbank, falls ein hybrider Ansatz gewählt wird. Die Konsequenzen der Entscheidung waren noch nicht absehbar. Üblicherweise werden Patienten-Stammdaten in Tabellen einer relationalen Datenbank verwaltet. Würden alle Patienten-Informationen in die Blockchain verlagert, müsste eine zusätzliche Patientenverwaltung entwickelt werden. Zunächst wurde der Ansatz verfolgt, die Beziehungen der Patienten zu Diagnosen und Therapien in der Blockchain am Patientendatensatz als Wertebereich (Range) mitzuführen. Nach einem Test wurde dieser Ansatz verworfen. Das war zu umständlich, komplex und mit meinem Wissensstand nicht umsetzbar. Dafür müsste der „Go-Code“, die Datenbank und

die Applikation jeweils separat verändert und angepasst werden. Hier waren die Grenzen meiner technischen Möglichkeiten erreicht. Der Aufwand wäre auch zu hoch gewesen und hätte keinen wirklichen Nutzen zur Folge gehabt, was sich später auch bewahrheitete.

Nach mehreren Versuchen und Abwägen der Konsequenzen der unterschiedlichen Varianten fiel die Entscheidung auf die Abspeicherung der PatientenID, ICD-Schlüssel, Diagnosen und Therapie von Patienten in der Blockchain. Dafür war die Entwicklung eines entsprechenden Softwarecodes notwendig, der die Daten abspeichert und später für ein Berichtswesen der Anwendung zur Verfügung stellt. Als Vorlage wählte ich ein Beispiel für eine Lieferkette von Fahrzeugteilen aus. Das Beispiel war zwar unpassend, diente jedoch als Vorlage und zum Wissensaufbau. Der Programmcode musste erweitert und verändert werden. Grund war die Entwicklung des für die Logik in der Blockchain notwendigen „Smart Contracts“ bzw. „Chaincodes“. Als Programmiersprache wurde nur die OpenSource Programmiersprache „golang“ der Firma Google unterstützt. Mehrere Wochen Aufwand hat es benötigt, um am Ende festzustellen, dass der Chaincode zuverlässig läuft, aber nur einzelne Datensätze zurückgeliefert werden, d.h. für einen Patienten existiert nur eine einzige Diagnose bzw. Therapie, was in der Praxis eher unwahrscheinlich ist. Der Ansatz, den Wertebereich der Diagnosen und Therapien am Patienten zu speichern war bereits verworfen worden, d.h. nun musste ein anderer Weg gefunden werden. Ein neuer Programmteil musste entwickelt werden, um eine Liste von Diagnosen und Therapien passend zu einem Patienten an das aufrufende Programm zurückzugeben. Das war zumindest ein gangbarer Weg, denn dadurch wurden gleich mehrere Problemstellungen, sowohl in der Datenbank als auch bei der Anwendungsentwicklung gelöst. Zu diesem Zeitpunkt war die Applikationsentwicklung für die Oberfläche bereits weit fortgeschritten, d.h. der neue Programmteil harmonierte nicht mit den Schnittstellen der Anwendung und es musste erneut nachgebessert werden. Bei einem Test des Gesamtsystems fiel auf, dass Groß- und Kleinschreibung nicht berücksichtigt worden war. Die Diagnosen und Therapien wurden fälschlicherweise nur in Kleinbuchstaben abgespeichert. Damals war die komplette Umgebung bereits in der Oracle Cloud als Testumgebung verfügbar. Der Chaincode musste erneut angepasst und installiert werden. War ein Problem gelöst, tat sich an anderer Stelle

ein weiteres auf, das der Nachbesserung bzw. Lösung bedurfte. Eine fehlende Versionsverwaltung führte dazu, dass bereinigte Fehler erneut auftraten und Wechselwirkungen zeigten, was zu Zeitverzögerungen führte. Nach etwa vierzig unterschiedlichen Versionen mit verschiedenen Strukturen und Installationen war der Chaincode fertig und passte sowohl zur Blockchain als auch zur Anwendung. Am Ende wurde auch ein automatisiertes Vorgehen für die Entwicklung und Verteilung des Programmcodes erreicht. Eine komplett automatisierte Softwareentwicklung und Verteilung (Kapitel 1.8 Agile Softwareentwicklung und Methoden) konnte aufgrund der Vielzahl an Komponenten nicht erreicht werden. Dies wäre für ein Projekt dieser Größenordnung auch zu umfangreich gewesen.

Im Prinzip war der praktische Teil fertiggestellt, jedoch war die Verarbeitung der Datensätze der Blockchain umständlich in APEX realisiert. Das war der Rückgabe der Daten als verschachteltes JSON-Format geschuldet (Abb. 42). Selbst nach mehreren Änderungen im Chaincode und datenbankseitiger Programmierung ließ sich dieser Punkt nicht verändern. Das war funktional nicht nachteilig und hätte später Programmieraufwände reduziert. Dennoch musste an dieser Stelle abgebrochen werden, um den bereits mehrfach verschobenen Zeitplan nicht noch mehr zu gefährden. Seit der APEX-Version 19.2 werden REST-Schnittstellen besser unterstützt. Diese Version wurde für meine Umsetzung jedoch zeitlich zu spät freigegeben, so dass nahezu alle Funktionen manuell programmiert werden mussten.

Fazit: Herausforderungen und Probleme

Die Entwicklung und Synchronisation aller Komponenten untereinander war herausfordernd. Dabei waren vor allem die Überlegungen bzgl. der Architektur und Design von großer Bedeutung, deren spätere Auswirkungen zu Beginn nicht sicher beurteilt werden konnten. Die Programmierung der medizinisch-fachlichen Funktionen wie Patientenüberweisung, Eingabe der Patientendaten, Änderung der Diagnosen und Therapien, Patientenhistorie, etc., war mit hohem Aufwand verbunden. Die im Hintergrund ablaufende Komplexität wird durch die Oberfläche gesteuert. Deren Entwicklung und Anpassung wäre ohne BLOG’s und Beispiele nicht möglich gewesen, zudem hier immer eine Transferleistung und Anpassung notwendig war.

3.8 Zusammenfassung

Die Blockchain-Technologie schafft Vertrauen zwischen den am Behandlungsprozess beteiligten Personen und Organisationen. Grundlage hierfür sind kryptografische Verfahren. Für die Realisierung von fachlichen Anforderungen werden die sogenannten „Smart Contracts“ genutzt. Die wichtigsten Eigenschaften der Blockchain sind Transparenz, Unveränderbarkeit, Nachvollziehbarkeit, Dezentralität und Sicherheit. Eine Blockchain benötigt immer neben den zu entwickelnden Funktionen eine Anwendung, die einen nicht unerheblichen Aufwand bei der Entwicklung darstellt. Neben dem Entwicklungsaufwand und der Identifizierung von sinnvollen Anwendungsfällen gibt es auch technische Limitierungen. Hinzu kommen Innovationsstau, Ressourcenengpässe, prozesstechnische Gründe und Sicherheitsbedenken, die die Adoption der Technologie im Gesundheitswesen erschweren. Der Aufwand an internem und externem Personal, das für die Umsetzung einer fachlichen Lösung notwendig ist, darf nicht unterschätzt werden. Während der Entwicklungsphase wurde erst nach und nach klar, welch großen Umfang die Arbeit annehmen würde. Neben dem Wissen, wie eine Blockchain funktioniert mussten weitere Technologien und Methoden betrachtet werden. Mit viel Aufwand musste das notwendige „Know how“ erarbeitet werden.

Folgende Punkte sind kritische Erfolgsfaktoren für den Einsatz und bilden die Grundlage für den anschließenden Diskussionsteil:

- Anwendungsfall
- Nutzen
- Komplexität
- Kosten
- Datenschutz
- Performance
- Personal

Aus der heutigen Sicht betrachtet spielt die Technologie und deren Verständnis eine wichtige Rolle, um eine Machbarkeit im Vorfeld einschätzen zu können.

4. Diskussion

Der für die Dissertation als Hybrid-Ansatz verfolgte Lösungsweg war erfolgreich und hat einen realitätsnahen Anwendungsfall abgebildet. Dieser Grundgedanke hat gezeigt, wie strukturierte Daten, die in Datenbanken verwaltet werden, mit den Eigenschaften einer Blockchain und deren völlig anderen Datenhaltungs-mechanismus kombiniert werden können. Dies schafft Mehrwerte für Ärzte, Patienten, Krankenhäuser, Versicherer und alle am Gesundheitsprozess beteiligten Personen. Die „Blockchain Emergency App“ basiert auf der These, dass vorhandene Systeme mit einer Blockchain interoperabel und integrierbar sind. Dies bedarf eines „hybriden“ Ansatzes, der eine Transformationsphase und Koexistenz sicherstellt. Um dies zu erreichen, ist es nicht sinnvoll, vorhandene Systeme und deren Anforderungen als Vorgabe für ein Blockchain-Projekt zu definieren. Hier müssen neue Ideen, neue Projekte und Anwendungsfälle einfließen.

4.1 Beurteilung der Blockchain-Entwicklung

Die Entwicklung von Anwendungen auf Basis der Blockchain-Technologie ist komplex, wie anhand der „Blockchain Emergency App“ gezeigt wurde. Speziell die Entwicklung der fachlichen Anforderungen (Smart Contract/Chaincode) hat extrem viel Zeit in Anspruch genommen. Neben der fachlichen Kenntnis in der Programmierung der Struktur und Prozesse müssen eine Vielzahl an weiteren Technologien beherrscht werden. Die konzeptionellen Überlegungen haben einen entscheidenden Einfluss auf Performance, Skalierbarkeit, Betrieb, Integration und Interoperabilität. Hier ist Expertenwissen ein kritischer Erfolgsfaktor und die Wahl des Anwendungsfalls von zentraler Bedeutung. Aktuell sind diese Kenntnisse vor allem bei Start-up Unternehmen anzutreffen. Ein großes Problem für Firmen stellt momentan sicherlich die Situation auf dem Arbeitsmarkt dar. Das für Projekte notwendige Personal ist aktuell nicht verfügbar. Dies kann zu einer Abhängigkeit von Kunden bezogen auf eine Lösung führen. Die großen Softwarehäuser verhalten sich abwartend und versuchen die Technologie nach und nach in ihre Systeme zu integrieren. Die meisten in der Industrie gestarteten Projekte befinden sich im Status „In progress“, wie im Kapitel 1 (Tabelle 1) dargestellt. Es fehlen konkrete Projektumsetzungen, die einen erkennbaren Nutzen generieren [41], um die Aufwände und Kosten zu rechtfertigen.

Der Grund liegt in den Eigenschaften der Blockchain-Technologie selbst. Grundsätzlich lässt sich die Eignung dieser Technologie für Applikationen im Gesundheitswesen positiv bewerten. Die Blockchain wird neue Applikationen ermöglichen, die Daten sicherer verwalten, Prozesse automatisierter ausführen und ohne eine Vermittlerfunktion auskommen. Die Nutzung von Smartphones für mobile Anwendungen kann ein Treiber für die schnellere Adoption der Technologie bedeuten. Neben den positiven Aspekten und dem „Technologie-Hype“ (Abb. 3) gibt es aber auch Hindernisse wie die Komplexität, die einen Einsatz erschweren bzw. als nicht sinnvoll erscheinen lassen. Bei einer Migration der Blockchain müssen die Transaktionen und die Historieninformationen überführt werden. Andernfalls wären gerade die Kerneigenschaften der Blockchain ausgehebelt.

Die Frage, ob eine interne IT-Abteilung mit dem Betrieb und den zugehörigen Tools zurechtkäme oder überfordert wäre, lässt sich nicht eindeutig beantworten. Die fachlichen Anforderungen der Blockchain sind sehr speziell. Dennoch kommt der IT eine tragende Rolle zu, denn sie kennt die vorhandenen Systeme und deren Schnittstellen. Bei dem in der Dissertation untersuchten hybriden Ansatz ist deutlich mehr Wissen notwendig, da sowohl der relationale Ansatz als auch die Integration der Blockchain realisiert wurde. Die Komplexität steigt mit jeder für die Implementierung notwendigen Schnittstelle und jedem Werkzeug. Aus diesem Grund ist für die Applikationsentwicklung und einen späteren Betrieb eine Cloudlösung in Betracht zu ziehen.

4.2 Nutzen der Blockchain-Technologie für die Radiologie

Mit Hilfe der Blockchain können in der Radiologie unterschiedliche Anwendungsfälle umgesetzt werden. Beispiele hierfür sind:

- Sicherer Austausch und das Teilen von Bildmaterial und Befunden zwischen Organisationen und Personen.
- Autorisierter Zugriff auf Patientendaten aller am Behandlungsprozess beteiligten Akteuren.
- Datenmanipulation und Missbrauch erkennen und verhindern.
- Predictive Maintenance von radiologischen Geräten (Internet of Things).
- Anreizsysteme für Patienten, Ärzte, Forscher bei Studien (allgemeingültig).

Durch die entwickelte Applikation konnte nachgewiesen werden, dass eine Blockchain das Problem der Interoperabilität und sicheren Bereitstellung von sensiblen Gesundheitsdaten lösen kann. Beim Einsatz der Technologie muss auf einen geeigneten Anwendungsfall geachtet werden, der die Eigenschaften der Blockchain nutzt. Weitere Effekte und Vorteile für die Radiologie sind in Zusammenhang mit Kostensenkung, Verbesserung der Diagnostik und Therapie durch maschinelles Lernen und Bereitstellung von medizinischen Patientendaten zu erkennen. Darüber hinaus ist die Nutzung von teleradiologischen Anwendungen, die eine digitale Identität mit den entsprechenden Berechtigungen auf die Patientenakte erfordern, ein weiterer Anwendungsfall. Die radiologischen Befunde könnten dadurch weltweit zugreifbar sein und bieten in Verbindung mit einem Big Data Ansatz einen ganzheitlichen Blick auf den Patienten. Dadurch ist ein hohes Potential vorhanden, um die Diagnostik und Therapie zu verbessern, Mehrfacherhebungen zu vermeiden und Kosten einzusparen. Für die Mediziner müssen diesbezüglich regulativ und ethisch konforme Anreizsysteme geschaffen werden, um das Teilen (engl. Sharing) der Patienteninformationen zu unterstützen.

Im Bereich der radiologischen Ausbildung könnten Lerninhalte einfach und ohne Sicherheitsbedenken zugänglich gemacht werden. Dies wird von Verde et al. [56] als ein Ziel für den Einsatz von Blockchain-Anwendungen gesehen. Diese Chancen, in Verbindung mit der Wahrung der Persönlichkeitsrechte des Patienten, dem Schutz der Gesundheitsdaten und einer weltweiten Verfügbarkeit, machen die Blockchain für die Radiologie, das Gesundheitswesen und nahezu alle Branchen interessant. Sie kann Prozesse verschlanken, vereinfachen und automatisieren ohne den Sicherheitsaspekt zu vernachlässigen.

4.3 Nutzen der Blockchain-Technologie für den Patienten

Im entwickelten Beispiel wurde das digitale Behandlungsrecht (Überweisung) an die teilnehmenden Personen und Organisationen übertragen. Der Patient muss in diesem Fall selbstverständlich mündig und interessiert sein, die eigenen Patienteninformationen zu verwalten und ggf. die Einzeldiagnosen und Therapien an die Fachärzte zu übertragen. Prozesse und Abläufe in Arztpraxen und Kliniken könnten vereinfacht und verkürzt werden. Die Arztbriefe könnten nach der Erstellung durch das Krankenhaus für den Hausarzt freigeschaltet werden.

Dieser erhält über den Blockchain-Mechanismus die Nachricht, dass ein medizinisches Dokument vorliegt. Das digitale Bildmaterial wird für den Transport von einer Behandlungsinstanz zur nächsten oftmals dem Patienten als CD/DVD ausgehändigt. Von Verde et al. [56] wird dieser Prozess als möglicher Mehrwert für den Patienten im Abschnitt „Could It Empower Patients“ diskutiert.

Weitere Vorteile für den Patienten ergeben sich beispielsweise aus der Teilnahme an Studien für die heute keine Entschädigung bzw. Rückvergütung ohne einen Mittelsmann vorgesehen ist. Der Patient hätte dabei die Wahl, ob er seine Daten an Forschungsinstitute, Pharmakonzerne oder Versicherer anonym und sicher weitergeben möchte. Im Fall von Versicherungen könnte die Reduzierung des Beitrages ein Anreiz sein.

4.4 Medizinische Anwendungsfälle und Ausblick

Im Zentrum der Überlegungen bei Blockchain-Technologie ist immer der jeweilige Anwendungsfall entscheidend. Aus diesem Grund stellt der folgende Ausblick lediglich einen Ausschnitt über mögliche Einsatzszenarien dar.

Teleradiologie

Die Radiologie profitiert vor allem durch die mögliche Unterstützung von Artificial Intelligence (AI) und Machine Learning (ML) Algorithmen, die der Qualitätssicherung dienen und den Mediziner unterstützen. Oftmals werden diese Algorithmen von den Softwarefirmen nicht offengelegt, so dass ein Risiko beim Einsatz hinsichtlich Eignung und den Resultaten besteht. Im Artikel von Marenco (President, Sweden/Nordic Chapter Government Blockchain Association) [34], wird Blockchain als „Enabler“-Technologie für die Teleradiologie gesehen. Gründe sind die großen Datenmengen, die aufgrund des radiologischen Bildmaterials entstehen. Sie repräsentieren etwa 90% der gesamten Gesundheitsdaten bei Patientenfällen. Vor diesem Hintergrund ist es extrem wichtig, eine Infrastruktur zu schaffen, die per Definition einen extrem hohen Sicherheitsstandard bietet. Stand heute sind fragmentierte Systeme mit Individuallösungen der Fachbereiche die Realität, die viele Ressourcen binden und einen erheblichen Kostenfaktor darstellen. Dies korrespondiert mit der These, dass eine Cloudlösung eine mögliche

Betriebsvariante sein kann, um den maximalen Nutzen für Ärzte und Patienten im Verhältnis zu den Kosten zu gewährleisten.

Nutzung von radiologischem Bildmaterial mittels KI

In der Regel stehen die Patientendaten nicht allen Fachgebieten in der Medizin zur Verfügung. Das Thema BigData und Machine Learning kann nur dann erfolgreich sein, wenn große Datenmengen zur Mustererkennung zur Verfügung stehen, wie es in der Radiologie der Fall ist. Die größte Herausforderung in diesem Umfeld sind die Daten aus den unterschiedlichen KIS-Systemen nutzbar bereitzustellen. Am Uniklinikum Regensburg steht das Thema BigData [1] auf dem Weiterbildungsplan von Ärzten. Um die für das maschinelle Lernen notwendigen Daten zu sammeln, müssen der Datenschutz, die Nutzung und Weitergabe geklärt sein.

Tatsache ist auch, dass die Algorithmen und die Datenauswahl entscheidend für ein gutes Diagnoseergebnis sind. In diesem Zusammenhang hat der Fachbereich „Google Health ©“ in Verbindung mit Forschern aus Amerika und England eine Studie zur Brustkrebserkennung in der Fachzeitschrift „Nature“ veröffentlicht [37]. Ein Abstrakt hierzu wurde von Heise am 02.01.2020 online gestellt [59]. Darin wird beschrieben, wie ein KI-Modell mit 91.000 Aufnahmen angelernt wurde, um Tumorgewebe zu erkennen. In die Studie flossen zusätzlich 28.000 Röntgenaufnahmen von Frauen ein, die dann sowohl von der KI als auch von Experten begutachtet wurden. Die daraus resultierenden Ergebnisse zeigen, dass eine KI im Vergleich zu Experten unter gewissen Umständen weniger falsch Negative erkennen kann. Dabei soll die Technik die Experten nicht ersetzen, sondern diese unterstützen, um damit ein noch exakteres Diagnose- und Therapieergebnis zum Wohle des Patienten erzielen zu können. Alle Daten der Studienteilnehmer wurden anonymisiert verwendet. Das Thema „künstliche Intelligenz“ wird im medizinischen Umfeld immer mehr an Bedeutung für die Analyse und Beurteilung von Patientenfällen gewinnen. In Deutschland können hier noch mehr Potentiale gehoben werden, wie ein Artikel mit der Überschrift „Wird Künstliche Intelligenz von der Regierung vernachlässigt?“ in der Stuttgarter Zeitung vom 28.12.2019 [27] beschreibt. Im Umkehrschluss ist eine Öffnung in Bezug auf anonyme Wiederverwendung des Materials für die Forschung in Deutschland sinnvoll und sollte diskutiert werden. Blockchain kann hier einen Beitrag leisten,

diese Anonymität zu gewährleisten und Datenmissbrauch zu verhindern. Dennoch bleibt ein Restrisiko, dass die großen Internetgiganten mit ihren Algorithmen die gesammelten, persönlichen Daten und die Gesundheitsdaten mit dem täglichen Leben kombinieren und so den gläsernen Patienten entstehen lassen.

In China ist der Schutz der Privatsphäre rein theoretischer Natur. In seiner Arbeit „Künstliche Intelligenz als Staatsziel“ [17] geht „Axel Dorloff“ auf diesen Umstand ein. In seiner Veröffentlichung im Deutschlandradio [18] werden ganz konkrete Szenarien und Anwendungsfälle genannt, die dies belegen. Aus den dort dargelegten Argumenten ist ersichtlich, dass sich ein ideales Umfeld für Firmen in der KI-Branche bietet. Hier herrscht die größte Dichte von Firmen, die exakt auf diesem Gebiet tätig sind. Es ist ein politisch erklärtes Ziel, dass China in Sachen KI-Entwicklung und Forschung eine Vorreiterrolle [38] einnehmen möchte und wird.

Analyse medizinischer Abrechnungsdaten

In der Zukunft könnten Überlegungen bezüglich der späteren Relevanz der Daten von entscheidender Bedeutung sein. Dies hat Bundesgesundheitsminister Jens Spahn erkannt. Mit der fortschreitenden Digitalisierung im Gesundheitswesen soll nun auch die Sammlung und Weitergabe der Gesundheitsdaten von 73 Millionen Versicherten ermöglicht werden [61]. Über den Gesetzesentwurf wird der Bundestag entscheiden. Aus Sicht der Forschung sicher ein wichtiger Schritt, um die Gesundheitsversorgung zu verbessern und neue Erkenntnisse bei Krankheiten zu gewinnen. Im Fokus stehen dabei lt. Medienbericht der „Zeit-Online“-Redaktion die Abrechnungsdaten. Der Datenschutz und deren Umsetzung stehen dabei im Mittelpunk der Debatte. Dies wird von Daten- und Patientenschützern sehr kritisch gesehen, da es sich um äußerst sensible Daten handelt und das Recht auf selbstbestimmte Information berührt wird.

Notfallmedizin

Am Anfang der Überlegungen zur Dissertation über Blockchain erschien die Notfallmedizin ein geeigneter Einstieg und Anwendungsfall zu sein. Bei Rettungseinsätzen wäre es beispielsweise von Vorteil, Patienteninformationen wie Allergien, verordnete Medikamente und deren Dosierung, medizinische Vorgeschichten, eventuelle Herzinsuffizienz, Schlaganfallrisiko oder

endokrinologische Befunde abrufen zu können. Diese Informationen in Verbindung mit den Stammdaten des Patienten können zu einem besseren Einsatzergebnis führen, ggf. auch Leben retten.

Konkret können durch die Realisierung der Lösung die wichtigsten Diagnosen und laufenden Therapien gespeichert und weiteren in der Behandlungskette beteiligten Personen zur Verfügung gestellt werden. Dazu zählt auch die Möglichkeit, dass der Patient seine Behandlungshistorie selbst verwalten kann und diese komplett oder in Teilen online zur Verfügung stellen kann. Dabei kann der Patient direkt mit dem behandelnden Arzt die nächsten Behandlungsschritte besprechen, ohne dafür weitere Praxisbesuche vereinbaren zu müssen, was eine Aufwandsreduzierung und Kosteneinsparung zur Folge haben kann. Für den Arzt kann die Patientenführung und Patientenversorgung durch mehr Transparenz der Vorgeschichte erleichtert werden.

Medikamenteninteraktionen

Durch die Festschreibung und lückenlose Dokumentation der Therapien und den damit verbundenen Medikationen und Dosierungen sind diese gesamtheitlich ersichtlich. Dadurch können Kombinationen und Wechselwirkungen von Wirkstoffen wie beispielsweise Calciumkanalblocker mit Betablocker und Digoxin, die einen Herzstillstand provozieren könnten, frühzeitig erkannt und vermieden werden. Sind beispielsweise die Kenntnisse über allergische Reaktionen auf Medikamente, z.B. Penicilline bekannt, können zusätzliche Vorteile für den Patienten und die behandelnden Ärzte entstehen.

Medizinische Vorgeschichte

Durch die Kenntnisse der medizinischen Vorgeschichte des Patienten kann die empirische präklinische Therapie zurückgefahren und die gezielte Therapie (z.B. COPDler) gesteigert werden. Dieses Wissen kann auch zu einer besseren Klinikauswahl und im Endeffekt zu besseren Behandlungsergebnissen für den Patienten führen.

Schlaganfall Door-to-Needle-Time

Bei Verdacht auf einen akuten Schlaganfall ist die Minimierung der „Door-to-Needle“-Zeit entscheidend. Idealerweise liegt der Wert bis zum Therapiestart innerhalb von 60 Minuten [35]. Der zeitliche Ablauf der einzelnen Schritte kann dabei als Messwert erfasst und in der Blockchain unveränderbar protokolliert werden. Damit könnte Klarheit darüber geschaffen werden, welcher der Schritte ggf. zu einer Zeitverzögerung geführt hat. Grundsätzlich eignen sich alle Arten von Anwendungen, die einen Zeitstempel bzw. Datum benötigen. Beispielsweise könnte mit einer Applikation die Zeit zwischen den einzelnen Behandlungsschritten bei einem Notfall erfasst werden, um so die Schritte zu identifizieren, die den größten zeitlichen Anteil an der Behandlungskette hatten, um diese zu optimieren. Ein weiterer Ansatz könnte die Aufzeichnung des Herzschlags und die Abspeicherung in einer Blockchain-Applikation sein. Dies wird bereits heute in Smartphones und Wearables unterschiedlicher Hersteller auf dem lokalen Gerät umgesetzt. Dennoch muss sorgsam abgewogen werden, welcher Anwendungsfall sinnvoll ist und welche Technologie verwendet wird. Liegt der Schwerpunkt dabei eher auf Dokumentation und Nachweis oder auf Echtzeitverarbeitung der Messwerte und Bereitstellung von Auswertungen und Statistiken.

Speicherung von medizinischen Dokumenten und radiologischen Befunden

Die Blockchain wächst permanent, da alle Transaktionen unveränderbar gespeichert werden. In der Regel werden medizinische Dokumente oder Bildmaterial nicht in der Blockchain gespeichert. Neben Performanceproblemen würden die gesamten Inhalte und Transaktionen auf alle im Netzwerk verteilten Server kopiert werden. Das würde enorme Speicher- und Stromkosten zur Folge haben. Zusätzlich würden sehr hohe Netzwerkbandbreiten erforderlich sein, was wiederum zu hohen Kosten führt und das Kosten-/Nutzen-Verhältnis in Frage stellt. Für die Speicherung könnten kostengünstige Cloud-Lösungen genutzt werden. Dies hätte zusätzlich den Vorteil, dass für den Austausch von Bildmaterial eine einheitliche, verfügbare, sichere und skalierbare Plattform mit standardisierten Schnittstellen zur Verfügung steht. Das ist auch der Grund, warum die Blockchain für die Dokumentation der Zugriffe auf sensibles Bildmaterial genutzt werden kann. Im Protokoll steht unveränderlich wer, wann und auf welches Bildmaterial zugegriffen hat.

Die dezentrale Speicherung kann auch dann sinnvoll sein, wenn die vorhandene Infrastruktur in einem Land unzureichend ist oder aufgrund gesetzlicher Vorgaben innerhalb des Landes oder über Landesgrenzen hinweg erfolgen muss.

Digitales Identitäten- und Berechtigungs-Management für med. Bildmaterial

Aus den geschilderten Anforderungen lässt sich der Schluss ziehen, dass zusätzlich zu den Eigenschaften einer „permissioned“ Blockchain ein Identitätsmanagement notwendig ist, um eine zusätzliche Sicherheitsschicht zu ermöglichen. In der Blockchain können dann die entsprechenden Metainformationen wie Teilnehmer, Zeitstempel, Speicherort, Bildmaterial etc. mitgeführt werden. In diesem Fall erhält der Nutzer ein digitales Zertifikat, welches ihn eindeutig identifiziert. Ein Missbrauch oder Fälschung von persönlichen Daten oder deren Herkunft ist damit ausgeschlossen. Die Ausstellung dieser Zertifikate muss dann sinnvollerweise von einer zentralen und/oder staatlich anerkannten Stelle erfolgen. In seinem LinkedIn [14] Artikel geht Dahm auf sinnvolle Einsatzgebiete einer Blockchain ein und definiert dies allgemeingültig wie folgt: „Blockchain ist dort sinnvoll, wo fälschungssicher Anrechte oder Privilegien verwaltet werden sollen“. Dies bedeutet, dass medizinische Identitäten über die unterschiedlichen Systeme geprüft und weitergegeben werden müssen, um den Mehrwert für die Nutzung von Patientendaten zu gewährleisten. Die Herausforderung dabei ist die Anbindung von vorhandenen Systemen. Der Datenaustausch von sensiblen Patientendaten wird in der Regel innerhalb der Patientenmanagement-Systeme von der Aufnahme bis zur Abrechnung über Schnittstellen realisiert. Die vorhandenen Infrastrukturen sind heterogen, so dass Interoperabilität oftmals nicht gegeben ist und Schnittstellen aufwendig programmiert werden müssen. Die Zugriffsprivilegien sind in der Regel in der jeweiligen Anwendung gekapselt oder es werden Standardmechanismen der jeweiligen Datenbanken genutzt.

Medizinische Studien- und Forschungsergebnisse

Den Aspekt der gemeinsamen Nutzung von Bildmaterial zur Nutzung von maschinellem Lernen, welches den Mediziner bei der Diagnose und Therapieentscheidung unterstützt, wurde bereits angesprochen. Dies kann jedoch nur dann erfolgreich umgesetzt werden, wenn sehr viel Bildmaterial zur Verfügung gestellt wird. Anreizsysteme können an dieser Stelle helfen.

Gleichzeitig muss der Studiendurchführende sicher sein, keine Datenschutzverletzung zu begehen oder gegen Compliance-oder Ethik-Richtlinien zu verstoßen. Die Blockchain kann sicherstellen, dass die Dokumentation der Studien- und Forschungsergebnisse nachvollziehbar, transparent und unveränderbar gespeichert wird. Dieser Fragestellung widmet sich der Artikel von Bosato [5] im Detail. Bereits während der Forschung könnten die Projektfortschritte und Ergebnisse veröffentlicht, geteilt, qualitätsgesichert und dem Studiendurchführenden zweifelsfrei zugeordnet werden. Dadurch werden Urheberrechte bzw. Erfindungen geschützt.

Arzneimittelherstellung und Nachweispflicht

Im Zusammenhang mit dem Skandal um den Blutdrucksenker Valsartan wurden stärkere Kontrollen und Verantwortlichkeiten bei der Arzneimittelherstellung gefordert. Eine Mitarbeiterin des Bayerische Rundfunks, Frau Grimmer hat hierzu einen Artikel [21] veröffentlicht, der sich mit der grundsätzlichen Verunreinigung von Medikamenten beschäftigt. Der Nachweis der Inhaltsstoffe, Herstellungsland, Produktionsverfahren, Lagerung und Haltbarkeit können mit Hilfe einer Blockchain unveränderlich festgehalten werden. Leeming et al. [29] beschreibt dies wie folgt: „…the recording of the delivery of a drug package could be created for every step of its journey from the factory to the patient, including details of whether it has been stored at the correct temperature, the price at which it was sold…". Damit würde Klarheit geschaffen, ob es sich um ein echtes oder ein nachgemachtes Medikament handelt. Eine lückenlose und transparente Chargenrückverfolgung von der Herstellung bis zur Auslieferung würde so ermöglicht. Damit würde die Blockchain dem Patienten optimalen Schutz vor verunreinigten Medikamenten bieten.

Pharmaindustrie

Die Pharmabranche hat großes Interesse an der Blockchain-Technologie und kann konkrete Anwendungsfälle aufweisen. Im ePharmaINSIDER" wurde dazu ein Artikel [22] veröffentlicht, der auf Anwendungsfälle, wie „Zurückgegebene Pharmazeutika", „Verhinderung von Fälschungen", „Compliance-Checks", „Klinische Studien mit Consent-Vereinbarungen und die Verbesserung von Klinischen Studien hinweist. Dadurch könnten die Forschungsergebnisse, Logistik und Transport transparent und nachvollziehbar dokumentiert werden. Die Blockchain-Technologie könnte für

ein Rückvergütungssystem für Patienten geeignet sein, um passende Studienteilnehmer zu gewinnen und deren Daten für die Entwicklung bzw. Freigabe von Medikamenten anonymisiert zu nutzen. Dennoch ist selbst der Pharmabranche klar, dass der Anwendungsfall kritisch hinterfragt werden muss, um einen Mehrwert zu erhalten.

Betäubungsmittel Buch - BTM-Buch

Das BTM-Buch muss nach dem vier-Augenprinzip handschriftlich geführt werden. Die darin dokumentierten Kriterien wie Bestände, das Ausgabedatum, das Ablaufdatum und die Verantwortlichen eignen sich sehr gut für eine Onlineumsetzung mit einer Blockchain-Technologie. Die Unveränderlichkeit und Nachvollziehbarkeit könnten gleiche Sicherheitsstandards garantieren. Diesen Gedanken haben Hardt und Sigler erkannt. Mit ihrem Ansatz, das Betäubungsmittelbuch auf Basis Blockchain [13] umzustellen konnten sie den Ideenwettbewerb des Bundesgesundheitsministeriums (BMG) zum Thema Blockchain im Gesundheitswesen gewinnen. Dieser Anwendungsfall ist ein weiterer Beweis für den sinnvollen Einsatz von Blockchain-Technologie, die die Daten der Patienten vertraulich schützen und so die Privatsphäre garantieren kann.

Genetik und Stammbäume

Dieser Anwendungsfall könnte Patienten zu Gute kommen, bei denen über Generationen hinweg eine Fortschreibung der Krankenakte nicht möglich ist bzw. war oder diese nicht mehr existiert. Dennoch ist es für die Diagnose und spätere Therapieentscheidung ein wichtiges Kriterium, um erblich bedingte Krankheiten im ganzheitlichen Zusammenhang zu betrachten oder auszuschließen. Mit Blockchain wird dies auf nachvollziehbare Art und Weise ermöglicht.

Hausarztwechsel

Beim Hausarztwechsel entstehen häufig Lücken in der Patientenhistorie. Oftmals fehlt die komplette Vorgeschichte, die aber für den neuen Hausarzt für die Weiterbehandlung relevant wäre. Die Weitergabe der Patientenakte oder Teile davon wurden in der Dissertation mit der Blockchain-Applikation realisiert.

Der Nutzen für den Patienten, der online seine bisherige Krankengeschichte übertragen kann, ist sofort erkennbar. Der aufnehmende Arzt kann auf die vorhandene Behandlungshistorie aufsetzen und dadurch Zeit und Kosten einsparen.

Medizinische Geräte und Internet of Things (IoT)

Die meisten Daten entstehen auf Smartphones, Wareables, Watches oder sonstigen „Internet of Things"-Geräten. Diese sind standardmäßig mit Sensoren und intelligenten Schnittstellen ausgestattet und bieten die Möglichkeit, Gesundheitsdaten zu speichern. Mit dem Smartphone können persönliche Daten hinterlegt, der Puls gemessen, ein EKG erstellt, ein Notfalleinsatz beispielsweise durch den Sturz einer Person ausgelöst, der Blutdruck gemessen, der Body-Mass-Index (BMI) sowie Bewegungsdaten gemessen und gespeichert werden. Die aktuelle Datenschutzkampagne von Apple zeigt, dass hier Defizite bestehen. Die für Studien und Produktentwicklung benötigten Daten entstehen auch außerhalb der Labors an Studienteilnehmern und Patienten. Der Trend wird weiter zunehmen. Die entsprechende Infrastruktur ist noch zu komplex, zu teuer und bietet unzureichenden Schutz bei wenig oder keiner Transparenz, wie die Daten weiterverwendet werden. Im Hinblick auf den Einsatz von Blockchain-Technologie könnte ein medizinisches Gerät (CT, MRT etc.) wie eine Person mit einer digitalen Signatur auf Basis einer Public-Private Key Infrastruktur behandelt werden. Damit wäre Anonymität gewährleistet. Die Hersteller selbst nutzen diese Schnittstellen, um „Predictive Maintenance" durchzuführen, d.h. Fehlersituationen der Geräte frühzeitig zu erkennen und proaktiv zu beseitigen.

Apotheke Medikamenten-Dispenser - Blockchain mit IoT-Gerät

Im Falle der Anbindung einer Apotheke (Abb. 2) an die Blockchain würde diese über das Ereignis „Ausstellung eines Rezeptes" (z.B. E-Rezept) [58] nach erfolgter Behandlung informiert werden. Ein „Tablettenspender" (engl. Pill Dispenser) könnte im Anschluss die entsprechenden Medikamente zusammenstellen und unveränderlich dokumentieren. Weitere Beispiele für Funktionen finden sich auf der Homepage eines Herstellers [51]. Im Falle eines intelligenten Dispensers könnte dieser das Medikationsschemata überwachen, welches vom Arzt verordnet wurde. Die Nachverfolgung einer Charge, wer, wann, welches Medikament ausgegeben

hat, wäre einfach zu realisieren. Der Verlust eines Rezepts würde nicht zwangsläufig die Neuausstellung bedeuten. Ein Missbrauch wäre erschwert, wenn es zu einem Wechsel der behandelnden Ärzte kommen sollte.

4.5. Außermedizinische Anwendungsfälle

Zertifizierungen und Ausbildungsnachweise

Der National Health Service in England (NHS) [15] hat bei einem Blockchain-Projekt den Anwendungsfall einer zentralen Kompetenzplattform untersucht. Ziel war es, die erworbenen Abschlüsse, Zertifikate und Titel der im NHS tätigen Personen sicher und unveränderbar vorzuhalten. Besonders für Neueinstellungen in den jeweiligen Fachgebieten war diese Nachweismöglichkeit von Bedeutung, um einmal die benötigten Kompetenzen zu erkennen und ggf. Berufsangebote und Ausbildungen daran zu orientieren. Weitere Einsatzgebiete und Betrachtungen finden sich von Southey [50].

Öffentliche Verwaltung

Die Regierung von Estland gilt seit zehn Jahren als Vorreiter für die Einführung und Nutzung der Blockchain in der öffentlichen Verwaltung. Im Bericht „Blockchains rocken Estland“ wird beispielsweise die Fälschungssicherheit von Dokumenten als Nutzen hervorgehoben. Zitat: „… sie sorgt für Transparenz von öffentlichen Daten und stellt sicher, dass ein Dokument „echt“ ist“ [39]. Darunter fallen beispielsweise eine Geburtsurkunde, der Personalausweis bis hin zu Ausbildungszertifikaten und Anträgen. Die Automatisierung durch Programmierung der fachlichen Aufgaben und deren Ausführung aufgrund eines Ereignisses (z.B. Geburt), erlaubt es, Prozesse schnell, unbürokratisch und ohne einen Intermediär abzuarbeiten. Das kommt sowohl dem Staat in Form von Kostenersparnis sowie den Bürgern in Form von Bürokratieabbau und schneller Bearbeitung der Fälle zu Gute. Um die Blockchain-Technolgie in Deutschland voranzutreiben, hat die Bundesregierung ein 42-seitiges Dokument [16] erstellt, um die Rechtsgrundlage für den Einsatz im Finanzsektor und dem behördlichen Umfeld zu ermöglichen.

Finanzsektor - Digitale Währung

Am häufigsten wird beim Einsatz von Blockchain der Finanzsektor angeführt. Das ist auch nachvollziehbar, denn bei der Erfindung von Blockchain waren im Wesentlichen die Banken im Fokus. Der Finanzbereich könnte durch den Einsatz von kostenfreien Konten und damit verbundenen Finanztransaktionen tatsächlich in Bedrängnis geraten. Die Banken sind die Mittelsmänner, die mittels Blockchain nicht mehr benötigt werden. Das ist auch der Grund, warum die Finanzinstitute kein Interesse haben, dass Kryptowährungen wie „echtes“ Geld behandelt werden. Dennoch wird sich der digitale Zahlungsverkehr in den Entwicklungsländern zuerst, durchsetzen. Dort können sich aufgrund der finanziellen Situation nur wenige ein Konto leisten. Der Zugang zum Internet ist dabei ein Erfolgsfaktor. In Deutschland fehlen hier noch Vorgaben der BaFin bzw. der Bundesregierung. Doch es ist gerade ein Umdenken in der Politik zu erkennen. Holtermann will in seinem Artikel [23] diesem Umstand begegnen und einen Blockchain-Wertpapierhandel ermöglichen.

Nachverfolgung von Spendengelder

Die Verfolgung von Spendengelder in Länder mit korrupten Regierungen wäre ein sehr sinnvoll umzusetzender Anwendungsfall für die Blockchain. Damit wäre Transparenz gegeben und eine Nachvollziehbarkeit garantiert.

Logistik

Die Logistik wird als Paradedisziplin für den Einsatz einer Blockchain-Lösung gesehen. Die komplette Lieferkette von der Herstellung über Lagerung, Transport und Auslieferung eignet sich optimal als Prozess, um diesen mit einer Blockchain abzubilden. Jedes Produkt erhält einen eindeutigen „Code“, z.B. einen Barcode und mehrere Sensoren messen permanent die wichtigsten Parameter passend zum Produkt und vergleichen diese mit Sollwerten. Diese Daten könnten in einer Blockchain mittels Zeitstempel, Status, Ist- und Sollwert unveränderbar und nachvollziehbar für jeden Teilnehmer transparent abgespeichert und zur Verfügung gestellt werden. Damit wäre transparent, ob beispielsweise ein Medikament gemäß den Vorschriften hergestellt, gelagert und transportiert wurde.

Automobilsektor

Dem Autofahrer droht durch die Keylessnutzung der Fahrzeugschlüssel Ärger, wenn das Fahrzeug gestohlen wird. Es ist seit Jahren bekannt, dass die Funkverbindung zwischen Fahrzeug und Fahrzeugschlüssel nicht verschlüsselt ist. Mit Porsche® hat ein Hersteller nun die Idee der Blockchain aufgenommen und ins Fahrzeug integriert. Dabei werden die Möglichkeiten der Verriegelung und Entriegelung des Fahrzeugs als ein Anwendungsfall umgesetzt und einen „Proof of Concept“ (PoC) für das bargeldlose Bezahlen von Parktickets auf Basis einer Blockchain durchgeführt [26]. Weitere Produktideen werden folgen und durch Anwendungen aus dem autonomen Fahren ergänzt. Ein weiterer Anwendungsfall könnte die Reduzierung von Funktionen oder die Reduzierung der Motorleistung sein, falls die Blockchain feststellt, dass die letzte Leasingrate zu spät oder gar nicht bezahlt wurde.

Fazit

Die Frage, ob eine Blockchain für alle Arten von Anwendungen geeignet ist, kann mit einem klaren „Nein“ beantwortet werden. Anwendungen, die mit großen Workloads (Arbeitslasten) arbeiten, wie ERP-Systeme (Enterprise Resource Planning), Handelsplattformen, Kernbankensysteme und KIS-Umgebungen sind kein geeigneter Anwendungsfall. Speziell diese eignen sich jedoch für die Integration der Blockchain-Technologie in ihre Produkte, um Kosten für Sicherheitsmechanismen und Banktransaktionen zu reduzieren. Die Möglichkeit einer mehrfachen Nutzung von Patienteninformationen und Bildmaterial kann sicher ermöglicht werden, wenn die Rechtslage geklärt ist.

Der Ansatz, eine Blockchain mit einem relationalen Datenbanksystem zu verbinden war erfolgreich und herausfordernd zugleich. Hervorzuheben ist die Entwicklung der „Blockchain Emergency App“, die den praktischen Nachweis des in der Aufgabenstellung formulierten Zieles erbracht hat.

Wie wichtig das Thema Sicherheit im Gesundheitswesen ist, verdeutlicht der von Zierer et al. am 17.09.2019 veröffentlichte Artikel [62]. Bei Recherchen in Zusammenarbeit mit der US-Investigativplattform ProPublica wurde bekannt, dass hochsensible Gesundheitsdaten ungeschützt im Internet aufgetaucht sind.

Persönliches Fazit

Aufgrund der Aufgabenstellung, den Recherchen und der späteren praktischen Umsetzung konnte ich viele IT-Technologien mit Bezug auf das Gesundheitswesen kennenlernen und mir aneignen. Dieses sehe ich als absolut positiv an, denn die Medizin wird in Zukunft immer mehr und sicherere Softwarekomponenten zur besseren Patientenversorgung und Forschung benötigen. An den Herausforderungen, wie der Aneignung von fachbereichsübergreifenden Wissen in Kombination mit medizinischen Kenntnissen, konnte ich mich weiterentwickeln. Gleichwohl sind Motivation, Wille, Durchhaltevermögen und der Umgang mit Rückschlägen, Fehlern sowie die Bereitschaft die Lösung nicht im ersten Schritt zu finden, für die erfolgreiche Lösung dieser Aufgabe essentiell gewesen.

5. Zusammenfassung

Die Realisierung und der Nachweis für die Eignung von Blockchain-Technologie in der Radiologie, dem Rettungsdienst und für die an der Behandlung beteiligten Organisationen hat sich als zeitaufwendiger herausgestellt als dies zu Beginn abzusehen war. Das ist selbstverständlich auch der Tatsache geschuldet, dass ich Medizinstudent und kein Programmierer bin. Am Anfang war nicht zu erkennen, ob der Ansatz trägt und ob ein belastbares Ergebnis am Ende der Dissertation steht. Die entwickelte Applikation ist der Nachweis und die Forschungsarbeit zugleich. Der Schwierigkeitsgrad hat sich durch die Kombination der vielen unterschiedlichen Softwarekomponenten extrem erhöht und bedurfte den Aufbau von breiten als auch tiefen Kenntnissen.

Die Fragestellung, ob die Blockchain-Technologie Potential für den Einsatz im Gesundheitswesen besitzt, kann mit „Ja“ beantwortet werden. Der Durchbruch der Technologie im Gesundheitswesen hängt entscheidend von den Lösungen der Partner im Gesundheitswesen und den passenden Anwendungsfällen ab. Patienten, Ärzte und Gesundheitsorganisationen können davon profitieren, wenn die Möglichkeit zur Weitergabe von Gesundheitsinformationen anonym und sicher ermöglicht wird. Hier muss ein permanenter Dialog mit den Fachbereichen, der IT, den Entwicklern und allen am Prozess beteiligten Organisationseinheiten stattfinden. Überlegungen zu den Anforderungen und der daraus abzuleitenden Architektur der Blockchain, des Datenbankmodells, der Integration von Fremdsystemen und die notwendigen Soft- und Hardwarekomponenten sind essentiell. Die Methoden aus der Softwareentwicklung waren eine Hilfe, um einen strukturierten Ansatz für die Problemlösung zu verfolgen. Dabei wurden neue Ideen generiert und wieder verworfen. Aufgrund von Softwarebugs mussten „Workarounds“ gefunden werden, so dass auch ein erheblicher Teil von „Trial and Error“ auf teilweise völlig unbekanntem Terrain die Folge war. Der Ansatz, sowohl strukturierte Stammdaten als auch unstrukturierte medizinische Dokumente und Bildmaterial mit der Blockchain-Technologie zu verknüpfen, hat sich als sinnvoll erwiesen. Dass diese Technologie Zukunft hat, lässt sich auch daran erkennen, dass die Firma Oracle mit der neuen Datenbankversion sogenannte „Blockchain-Tables“ einführen wird.

Die Technologie ist in einem Stadium der permanenten Weiterentwicklung. Sie wird nach und nach in die Standardprodukte des Gesundheitswesens, der Verwaltung und Industrie integriert werden (müssen). Dadurch können Synergien entstehen, Kosten gesenkt, Prozesse vereinfacht und beschleunigt, Bürokratieabbau und Innovationsbereitschaft unter Berücksichtigung der Privatsphäre gefördert werden. Blockchain kann einen entscheidenden Beitrag zur Weiterentwicklung und Verbesserung der medizinischen Versorgung leisten und zu einer besseren Behandlungserfahrung für die Patienten führen.

6. Literaturverzeichnis

[1] Aust M, Piontek R: https://richard-magazin.de/eins_2020/in-die-zukunft/ (04.01.2020)

[2] BAMF, Projektgruppe-Wirtschaftsinformatik-FIT: Unterstützung der Kommunikation und Zusammenarbeit im Asylprozess mit Hilfe von Blockchain, Whitepaper der Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT (2018)

[3] Biselli A, Köver C: https://netzpolitik.org/2019/das-bamf-will-seine-probleme-mit-der-blockchain-auf-die-kette-kriegen/ (05.06.2019)

[4] Börner Y: https://praxistipps.focus.de/was-ist-fiatgeld-einfach-erklaert_101338 (10.11.2019)

[5] Bosato A: https://247med.de/uncategorized/die-blockchain-technologie-im-umfeld-der-medizindatenverarbeitung-und-speicherung/ (20.08.2018)

[6] Bundesregierung: Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode: 44 (2018)

[7] Bundesverband Informationswirtschaft TunMeV, Berg A: Bitkom Digital Health, Bitkom Pressekonferenz e-health (2019)

[8] Corporation O: https://docs.oracle.com/en/database/other-databases/blockchain-enterprise/19.3/rest-api/index.html (16.09.2019)

[9] Czarski C: https://blogs.oracle.com/author/carsten-czarski (12.06.2019)

[10] Czarski C: https://apex.oracle.com/pls/apex/germancommunities/apexcommunity/tipp/1502/index.html (12.06.2019)

[11] Czeschik C: https://www.serapion.de/wp-content/uploads/2017/05/Blockchain-Gesundheitswesen-040517.pdf (08.06.2017)

[12] Czeschik C, Stambolija R: Blockchain im Gesundheitswesen für Eilige, 1. Auflage, Intellicore Press, Essen (2017)

[13] Czeschik C: https://e-health-com.de/details-news/btm-goes-blockchain-zentrale-superbehoerde-ist-unwirtschaftlich/ (17.09.2019)

[14] Dahm I: https://www.linkedin.com/pulse/blockchain-wo-sinnvoll-nicht-dr-ingo-dahm (12.07.2019)

[15] Dang PL: https://heartbeat-med.com/de/blog/gesundheitssystem-england-nhs/ (13.02.2018)

[16] Dernbach C: https://www.welt.de/newsticker/dpa_nt/infoline_nt/netzwelt/article200468650/Bundesregierung-will-Blockchain-Technologie-voranbringen.html (18.09.2019)

[17] Dorloff A: https://www.deutschlandfunk.de/china-kuenstliche-intelligenz-als-staatsziel.724.de.html?dram:article_id=440743 (07.05.2019)

[18] Dorloff A: https://www.deutschlandfunkkultur.de/kuenstliche-intelligenz-in-china-die-supermacht-der.979.de.html?dram:article_id=439978 (04.02.2020)

[19] Europaparlament (2016, 2018). General Data Protection Regulation, EU-Datenschutz-Grundverordnung (EU DS-GVO). EU law Document 32016R0679, European Union.

[20] Finck M: https://www.sueddeutsche.de/digital/blockchain-dsgvo-michele-finck-technologie-1.4304641 (02.02.2019)

[21] Grimmer C: https://www.br.de/nachrichten/bayern/global-gepanscht-der-skandal-um-verunreinigte-medikamente,RIWlSmZ (12.04.2019)

[22] Höllerer F, GmbH eIeSdH: https://www.epharmainsider.com/5-praxisbeispiele-von-blockchain-nutzung-in-der-pharma-branche/ (04.02.2020)

[23] Holtermann F: https://www.handelsblatt.com/finanzen/geldpolitik/elektronische-anleihen-bundesregierung-will-noch-2019-blockchain-wertpapiere-einfuehren/25023216.html (18.09.2019)

[24] Horchert J, Klofta J: https://www.spiegel.de/netzwelt/netzpolitik/ccc-hacker-finden-sicherheitsluecken-in-der-telematikinfrastruktur-a-1302902.html (02.01.2020)

[25] Hudson PR, Augsten S: https://www.dev-insider.de/blockchain-eine-einfuehrung-in-die-konzepte-a-624577/ (23.09.2017)

[26] Johannes K: https://www.cio.de/a/porsche-ermoeglicht-parken-per-blockchain,3596240 (12.06.2019)

[27] Knuf T: https://www.stuttgarter-zeitung.de/inhalt.schlechtes-zeugnis-fuer-die-koalition-wird-kuenstliche-intelligenz-vernachlaessigt.847eba22-e909-428b-aa77-005edfd8ec19.html?reduced=true (03.01.2020)

[28] Krolop S, Benthin F, Koch- Büttner T, Siegel D: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/life-sciences-health-care/Blockchain_LSHC_komplett_Version_neu_safe.pdf (05.01.2018)

[29] Leeming G, Ainsworth J, Clifton DA: Blockchain in health care: hype, trust, and digital health, The Lancet 393: 2476-2477 (2019)

[30] Livshits A: https://www.btc-echo.de/bitwise-richtet-sich-erneut-an-die-sec/ (22.01.2020)

[31] Lohwasser R: https://www.lition.de/about-us (09.09.2019)

[32] Madiba HC: https://en.decentral.news/german-carmaker-volkswagen-to-use-ibm-blockchain-to-track-its-minerals/ (08.07.2019)

[33] Manset D, Bernal L, Koscina M, Kemper OP: Blockchain and GDPR compliance for the healthcare industry, HealthManagement.org 19: 42-44 (2019)

[34] Marenco M: Can Blockchain support advances in radiology?, HealthManagement.org 19: 31-32 (2019)

[35] Marler JR, Winters Jones P, Emr M, (NINDS) NIoNDaS: Proceedings of a National Symposium on Rapid Identification and Treatment of Acute Stroke (1996)

[36] Mau J, Naumann J: https://www.kma-online.de/themenwelten/dmea/artikel/detail/die-top-7-kis-anbieter-2017-a-34535 (19.12.2019)

[37] McKinney SM, Sieniek, M., Godbole, V. et al.: International evaluation of an AI system for breast cancer screening, Nature 577: 89-94 (2020)

[38] Meier C: https://www.welt.de/kultur/article191734655/Wie-China-mit-kuenstlicher-Intelligenz-zum-Ueberwachungsstaat-wird.html (07.05.2019)

[39] Müller D, Ostler U: https://www.datacenter-insider.de/blockchains-rocken-estland-a-789277/ (15.04.2019)

[40] Nakamoto S: https://bitcoin.org/bitcoin.pdf (10.06.2019)

[41] Peppel-Schulz J: https://www.gq-magazin.de/auto-technik/article/untersuchung-0-von-43-blockchain-projekten-liefern-ergebnisse (09.01.2019)

[42] Pittet S: https://www.atlassian.com/continuous-delivery/principles/continuous-integration-vs-delivery-vs-deployment (16.09.2019)

[43] Price K: https://docs.oracle.com/en/database/other-databases/blockchain-enterprise/19.3/administer/index.html (16.09.2019)

[44] Price K, development OBP, management p, teams qa: https://docs.oracle.com/en/database/other-databases/blockchain-enterprise/19.3/user/index.html (16.09.2019)

[45] Rasinski A: Blockchain-Technologie : Analyse ausgewählter Anwendungsfälle und Bewertung rechtlicher Aspekte, Abschlussarbeit (Master; Diplom) Universität Ulm (2017)

[46] Ricotta F, Laidlaw R: Healthcare 2019: the year of the Big Data Blockchain, HealthManagement.org 19: 45-46 (2019)

[47] Scheuer E: Blockchain solves healthcare data obstacles, HealthManagement.org 19: 24-26 (2019)

[48] Sebek M: https://www.focus.de/finanzen/boerse/kryptowaehrungen/ethereum-grundlage-fuer-smart-contracts-und-dapps_id_8071541.html (15.09.2019)

[49] Shannoun F, Blettner M, Schmidberger H, Zeeb H: Strahlenschutz in der diagnostischen Radiologie, Deutsches Ärzteblatt 105: 41-46 (2008)

[50] Southey S: https://www.healtheuropa.eu/blockchain-distributed-ledger/89316/ (08.09.2019)

[51] Stithi I: https://www.stithi.in/#services (14.09.2019)

[52] Tapscott D, Tapscott A: https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services (26.12.2017)

[53] TheLinuxFoundation: http://www.hyperledger.org/projects/fabric (10.06.2019)

[54] Urbanek Margarethe, Hauke G: https://www.aerztezeitung.de/Wirtschaft/Millionen-Patientendaten-auf-ungesicherten-Servern-401247.html (02.01.2020)

[55] V. DKe: https://www.dkgev.de/dkg/presse/details/bsi-gibt-gruenes-licht-fuer-dkg-sicherheitsstandard/ (02.01.2020)

[56] Verde F, Stanzione A, Romeo V, Cuocolo R, Maurea S, Brunetti A: Could Blockchain Technology Empower Patients, Improve Education, and Boost Research in Radiology Departments? An Open Question for Future Applications, Journal of Digital Imaging 32: 1112-1115 (2019)

[57] Walden J: https://www.ipoint-systems.com/blog/products-solutions/ (05.04.2019)

[58] Waschinski G: https://www.handelsblatt.com/politik/deutschland/gesundheitspolitik-wie-das-e-rezept-den-markt-fuer-apotheken-veraendert/24235770.html?ticket=ST-3190730-RAMKahEUN0wg5lyqfwBM-ap4 (15.09.2019)

[59] Weiß E-M: https://www.heise.de/newsticker/meldung/Studie-Googles-KI-bei-Brustkrebserkennung-besser-als-Aerzte-4626531.html (03.02.2020)

[60] Wulf N: https://www.private-banking-magazin.de/nach-urteil-gegen-verwaltungspraxis-der-bafin-bmf-stuft-handel-mit-krypto-assets-als/ (05.09.2019)

[61] ZEIT ONLINE GmbH, Esser R, Röpke C, Tarragona E: https://www.zeit.de/politik/deutschland/2019-11/digitale-versorgung-gesetz-elektronische-patientenakte-gesundheitsapps-datenschutz (27.12.2019)

[62] Zierer M, Tanriverdi H: https://www.br.de/nachrichten/deutschland-welt/millionenfach-patientendaten-ungeschuetzt-im-netz,RcF09BW (17.09.2019)

Danksagung

Ich danke meinem Doktorvater Herrn Prof. Dr. med. Stefan Schmidt und Herrn Prof. Dr.med. Meinrad Beer für Ihre Unterstützung, das mit vielen Denkanstößen verbundene Feedback und zuletzt die Chance und Ihre Bereitschaft diese fachübergreifende Arbeit an der Klinik für Diagnostische und Interventionelle Radiologie zu ermöglichen.

Niclas Vester

Lebenslauf aus Gründen des Datenschutzes entfernt.

Lebenslauf aus Gründen des Datenschutzes entfernt.