Blockchain in der Vernetzung von Gesundheitsdaten in Patientenaktensystemen – Konstruktion einer Referenzarchitektur und eines Entscheidungsmodells zur Unterstützung von Forschung und Entwicklung

Von der Mercator School of Management, Fakultät für Betriebswirtschaftslehre, der

Universität Duisburg-Essen

zur Erlangung des akademischen Grades

eines Doktors der Wirtschaftswissenschaft (Dr. rer. oec.)

genehmigte Dissertation

von

Daniel Erkal

aus

Hildesheim

Referentin/Referent:	Prof. Dr. Peter Chamoni
Korreferentin/Korreferent:	Prof. Dr. Jochen Gönsch
Tag der mündlichen Prüfung:	14.12.2022

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABAC	Attribute-based Access Control, Attribute-based Access Control
ACL	Access Control Lists
ALMA	Architecture-Level Modifiability Analysis
AM	Access Management
AMS	Access Management System
APIs	Application Programming Interfaces
ARID	Active Reviews for Intermediate Designs
ARIS	Architektur integrierter Informationssysteme
ATAM	Architectural Trade-off Analysis Method
AVS	Apothekenverwaltungssystem
BA	Byzantine-Agreement-Algorithmus
BGB	Bürgerliches Gesetzbuch
BMBF	Bundesministeriums für Bildung und Forschung
BMRA	Blockchain Member Onboarding Reference Architecture
BNRA	Blockchain Network Reference Architecture
Bridge-CA	Bridge-Certificate-Authority
BSRA	Blockchain Solution Reference Architecture
CBAC	Capability-based Access Control
CBAM	Cost Benefits Analysis Method
CMS	Card Management System
DAC	Discretionary Access Control
DApp	Dezentrale Applikation
DIC	Datenintegrationszentrum
DIFUTURE	Data Integration for Future Medicine
DSRM	Design Science Research Methodology
e.V.	Eingetragener Verein

EA	Enterprise Architecture
eEPA	Einrichtungsübergreifende Elektronische Patientenakte
eFA	Einrichtungsübergreifende medizinische Fallakte
eGK	Elektronische Gesundheitskarte
EHCR	Electronic Health Care Records
EHR	Electronic Health Record, Electronic Health Record
EMR	Electronic Medical Record
engl.	Englisch
ePA	Elektronische Patientenakte
EPR	Electronic Patient Record
EVM	Ethereum Virtual Machine
FAAM	Family Architecture Assessment Method
FBA	Federated Byzantine Agreement
GB	Gigabyte
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
GI FB WI	Fachbereich Wirtschaftsinformatik der Gesellschaft für Informatik e.V.
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.
GMG	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
HiGHmed	Heidelberg-Göttingen-Hannover Medizininformatik
HMO	Health Maintenance Organization
IBAC	Identity-based Access Control, Identity-based Access Control
ICEHR	Electronic health record for integrated care
iEPA	Institutionelle Elektronische Patientenakte
IHE	Integrating the Health Enterprise
IRA	Individual Retirement Account
IS	Informationssysteme

IS-Architektur	Informationssystem-Architektur
ISO	International Organisation for Standardization
ISR	Information Systems Research
KBV	Kassenärztlichen Bundesvereinigung
KIS	Krankenhausinformationssystem
KSI	Keyless Signature Infrastructure
KV	Krankenversicherung
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MB	Megabyte
MBDS	Minimum Basic Data Set
MBO	(Muster-)Berufsordnung
MI	Medizininformatik
Mio	Millionen
MIRACUM	Medical Informatics in Research and Care in University Medicine
MPI	Master Patient Index
o. J.	Ohne Jahr
o. O.	Ohne Ort
o. S.	Ohne Seite
OECD	Organisation for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
ONC	Office of the National Coordinator for Health Information Technology
P2P	Peer-to-Peer-Netzwerk
PB	Petabyte
PBAC	Pseudonym-based Access Control
PCHR	Personally Controlled Health Record
pEPA	Persönliche Elektronische Patientenakte

PHI	Protected Health Information
PHR	Personal Electronic Health Record
PIX	Patient Identifier Cross-referencing Profile
PKI	Public-Key-Infrastructure
PoB	Proof-of-Burn
PoS	Proof-of-Stake
PoW	Proof-of-Work
PSR	Patient Summary Record
PVS	Praxisverwaltungssystem
RA	Referenzarchitektur
RA-Forschung	Referenzarchitekturforschung
RBAC	Role-based Access Control
ReBAC	Relationship-Based Access Control
RM	Referenzmodell
SA	Software-Architekturen
SAAM	Software Architecture Analysis Method
SDK	Software Development Kit
SMITH	Smart Medical Information Technology for Health Care
SSO	Single-Sign-On
StGB	Strafgesetzbuch
TI	Telematikinfrastruktur
TPC	Transactions per CPU
TPDIO	Transactions per disk I/O
TPMS	Transactions per memory second
TPND	Transactions per network data
TPS	Transactions per second
TSL	Trust-service-Status List

TSP	Trusted Service Provider
TSVG	Terminservice- und Versorgungsgesetz
TTP	Trusted Third Party
UFS	Update Flag Service
VHB	Verbands der Hochschullehrer für Betriebswirtschaft e.V.
VODD	Verordnungsdatendienst
VODM	Verordnungsdatenmanagement
VPN	Virtual Private Network
VSDD	Versichertenstammdatendienst
VSDM	Versicherungsstammdatenmanagement
WI	Wirtschaftsinformatik, Wirtschaftsinformatik
WKWI	Wissenschaftliche Kommission Wirtschaftsinformatik

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Motivation

Die Gesamtausgaben im deutschen Gesundheitswesen stiegen, von 1992 bis 2016 um 123% von 159.381 Mio. € auf 356.537 Mio. Euro.[1] Gleichzeitig wuchsen die Pro-Kopf-Ausgaben von 1996 bis 2016 um 81% von 2.390 Euro auf 4.330 Euro. Der Verlauf wird in *Abbildung 1-1* dargestellt.

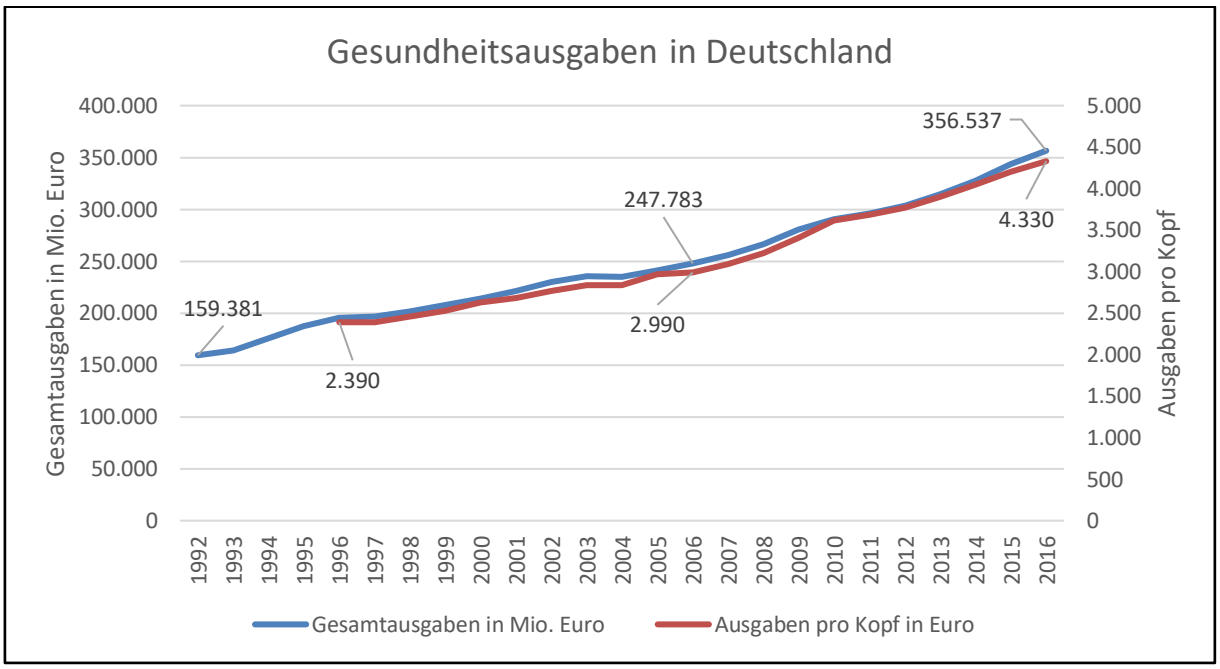


Abbildung 1-1: Gesundheitsausgaben in Deutschland von 1992 bis 2016[2]
(Quelle: Eigene Darstellung in Anlehnung an Statistisches Bundesamt (2018a) und Statistisches Bundesamt (2018c))

Deutschland liegt nach Bericht der ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)[3] über dem OECD-Durchschnitt und auf Platz 5 der 44 untersuchten Staaten. Lediglich Norwegen, Luxemburg, die Schweiz und die USA weisen höhere Ausgaben aus (siehe *Abbildung 1-2*).[4]

---

1 Detaillierte Zahlen finden sich im Anhang A und beim Statistischen Bundesamt (Suchcode: 23611-0001). Die Zahlen umfassen die folgenden Ausgabenträger: *Öffentliche Haushalte, Gesetzliche Krankenversicherung, Soziale Pflegeversicherung, Gesetzliche Rentenversicherung, Gesetzliche Unfallversicherung, Private Krankenversicherung, Arbeitgeber* und *Private Haushalte / Private Organisationen ohne Erwerbszweck*.

2 Detaillierte Zahlen finden sich in *Tabelle A-1* und *Tabelle A-2* unter *Anhang A*.

3 Deutsch: *Organisation für wirtschaftliche Zusammenarbeit und Entwicklung.*

4 Vgl. OECD (2017): 133. *Anmerkung*: Die hier dargestellten Zahlen sind in US-Dollar. Insofern kann es in Abhängigkeit zum Wechselkurs zu Abweichungen im Vergleich zu den Angaben des Statistischen Bundesamts (in Euro) geben.

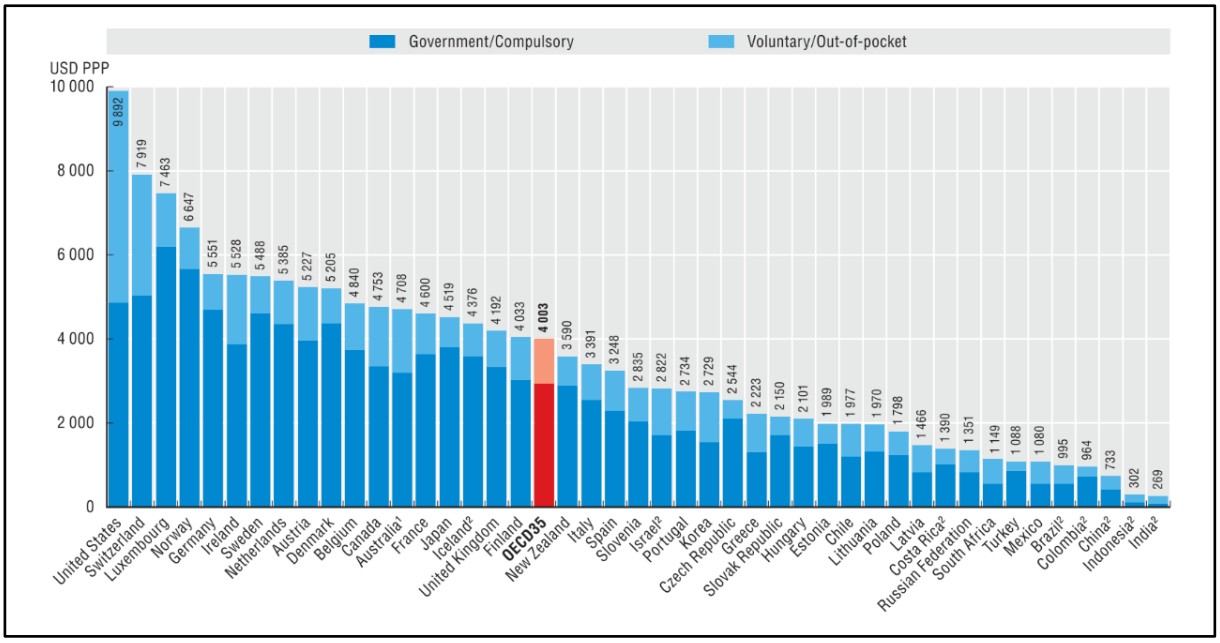


Abbildung 1-2: OECD-Studie von 2016 zu Gesundheitsausgaben pro Kopf im Ländervergleich (in US-Dollar) (Quelle: OECD (2017): 133)

In der Diskussion über Faktoren, die Gesundheitsausgaben verringern, steht der Zusammenhang zwischen der Anwendung adäquater Informationssysteme und der Optimierung von Gesundheitsdienstleistungen, folglich der durch Optimierung von Prozessen reduzierten Kosten, im Fokus.[5] Diskurse betrachten dabei vornehmlich die Optimierung klinikinterner Prozesse, wohingegen PORTER/TEISBERG allgemeiner an das Problem herangehen und neben strategischen und organisatorischen Ineffizienzen ebenfalls fehlerhafte Anreizsysteme im Gesundheitssystem und die nicht funktionierende Zusammenarbeit unterschiedlicher Akteure entlang des gesamten Behandlungspfades[6] über das einzelne Klinikum hinaus als Problem identifizieren.[7] Fehlende oder mangelhafte Zusammenarbeit führt zu Informationsasymmetrien, die bspw.

---

5 Vgl. Simoneit (1998): VII, 1. SIMONEIT begründet den Bedarf von Informationsmanagement mit der Notwendigkeit, den gesamten Behandlungsablauf innerhalb eines Klinikums mit entsprechenden Informationen zu versorgen und somit zu optimieren (vgl. Simoneit (1998): 2).

6 *Behandlungspfade* beschreiben sämtliche Stationen entlang eines spezifischen oder allgemein gültigen Behandlungsverlaufs eines Individuums bzw. einer Gruppe von Patienten gleicher Indikation (vgl. Richter/Schlieter (2019): 994f.).

7 Vgl. Porter/Teisberg (2006): 103. Beide vertreten die Meinung, dass das Problem steigender Kosten und nicht gleichzeitig steigender Qualität nicht durch einzelne Reformen bzw. Innovationen erfolgreich gelöst wird, sondern dass es einer vollumfänglichen Reform des gesamten Gesundheitswesens bedarf (vgl. Porter/Teisberg (2006): 2). Informationstechnologien bleiben ein wichtiger ‚Enabler' und haben unterstützende Funktion, denn eine reine Automatisierung bestehender Prozesse genügt aus Sicht der Autoren nicht. Prozesse müssen umfassend erfasst und analysiert werden sowie Prozesse zur kontinuierlichen Wissensentwicklung vorhanden sein (vgl. Porter/Teisberg (2006): 150).

doppelte Untersuchungen[8] und Medikations- bzw. Behandlungsfehler[9] zur Folge haben können. Eine vernetzte Informationslandschaft dagegen, also die einrichtungsübergreifende Bereitstellung von Gesundheitsdaten, trägt zu einer Verbesserung der Behandlungen bei, verringert Kosten und unterstützt zudem die medizinische Forschung.[10]

Die deutsche Politik verabschiedete 2003 das *Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GMG)*[11], das vorschreibt, *Effizienz* und *Effektivität* des Gesundheitswesens mittels digitaler Lösungen bzw. digitaler Kommunikation zu verbessern.[12] In der Folge wurde 2005 die GESELLSCHAFT FÜR TELEMATIKANWENDUNGEN DER GESUNDHEITSKARTE MBH (GEMATIK) gegründet, deren Gesellschafter leitende Verbände der Gesundheitswirtschaft und -politik sind.[13] Aufgabe dieser Einrichtung ist die Entwicklung und Einrichtung einer elektronischen Gesundheitskarte (eGK) sowie einer Infrastruktur, die den sicheren Austausch von Daten und Informationen sektorübergreifend ermöglicht.[14] Ergänzend soll eine elektronische Patientenakte betrieben werden, deren Funktionsumfang in § 291a SGB V definiert wird.

Parallel zu den Entwicklungen der GEMATIK kümmert sich das 2015 initiierte Förderprogramm *Medizininformatik* des BUNDESMINISTERIUMS FÜR BILDUNG UND FORSCHUNG (BMBF) um Konzepte, die einen einrichtungsübergreifenden Datenaustausch zur Unterstützung von Biomedizin- und Versorgungsforschung entwickeln.[15] Darüber hinaus arbeiten privatwirtschaftliche

---

8 Vgl. Schneider (2016): 38. Der Autor weist dennoch darauf hin, dass das Vertrauen in derartige Aktenlösungen nicht uneingeschränkt sein sollte, da sich die Gesundheit des Patienten verändert, und der in der Akte dokumentierte Zustand eines Patienten überholt sein kann (vgl. Schneider (2016): 53). Folglich soll ein Leistungserbringer übermittelte Daten überprüfen (vgl. van der Linden et al. (2009): 150).

9 Vgl. Schneider (2016): 31 mit Verweis auf Mutschler et al. (2013): Abschnitt A5 und Abschnitt A6.

10 Vgl. Liao et al. (2010): 1126; Rasmussen (2014): 612; Sutherland et al. (2016): 262f. Nutzenpotentiale sind teilweise empirisch belegt (vgl. Schneider (2016): 28, mit Verweis auf Bernnat (2006): 251 und Bönisch (2017): 130f.). Dennoch scheint der durch Vernetzung entstehende (positive) Nutzen der in diesem Rahmen entstehenden Netzwerke regional begrenzt bzw. von diversen Wirkfaktoren abhängig (vgl. Bönisch (2017): 132).

11 GMG (2003) Da bis Ende 2015 weder Fortschritte in der Entwicklung, noch, aufgrund politischer Neuausrichtungen, verlässliche zeitliche Vorgaben existieren, legt das Ende 2015 verabschiedete *E-Health-Gesetz* neue, verbindliche Fristen zur Einführung digitaler Dienste fest (siehe E-Health-Gesetz (2015)). Dieses wird wiederum im Frühjahr 2019 um das *Terminservice- und Versorgungsgesetz (TSVG)* ergänzt (siehe TSVG (2019)). Gemäß TSVG soll der Zugriff auf die geplante ePA auch via Smartphone und Tablet möglich werden, Krankenkassen eine mit der GEMATIK kompatible ePA anbieten müssen und die Einwilligung zur Datennutzung erleichtert werden (vgl. Bundesministerium für Gesundheit (2018)).

12 Vgl. Deutsche Krankenhausgesellschaft (2006): 2.

13 Vgl. gematik (o. J.b). Seit 2019 ist das Bundesministerium für Gesundheit (BMG) nach Inkrafttreten des TVSG Hauptgesellschafter der GEMATIK (vgl. gematik (o. J.a); ÄrzteZeitung.de (2019)).

14 Vgl. gematik (o. J.b).

15 Vgl. Bundesministerium für Bildung und Forschung (2015): 9.

Unternehmen und Krankenkassen (z.B. *CompuGroup Medical* oder die *Techniker Krankenkasse*) an eigenen Lösungen, die entsprechend § 68 SGB V ausgestaltet werden.[16]

Jede dieser Lösungen steht besonders in Sachen Datenschutz[17] und Informationssicherheit in der Diskussion. Gründe für Bedenken an der Lösung der GEMATIK finden sich beispielsweise in einem Arbeitspapier von HUBER/SUNYAEV/KRCMAR[18], das mehrere mögliche Bedrohungsszenarien für den von der GEMATIK konstruierten Konnektor präsentiert, der die Verbindung in die gesicherte Telematik-Infrastruktur herstellt.[19] Auch die KASSENÄRZTLICHE BUNDESVEREINIGUNG (KBV) äußert, bezugnehmend auf die geplante elektronische Patientenakte, Bedenken und rät ihren Mitgliedern, dass diese *„nur eine Ergänzung zu bereits bestehenden Dokumentations- und Kommunikationswegen"*[20] darstellt und folglich ausschließlich als sekundäre Informationsquelle genutzt werden soll. Von Patienten zur Einsicht freigegebene Daten sollen zudem aus forensischen Gründen in den Systemen der einzelnen Leistungserbringer gespeichert werden.[21] Diese Vorsicht ist begründet in der im Bürgerlichen Gesetzbuch (BGB) geregelten Dokumentationspflicht[22] und der daraus resultierenden Strafbarkeit bei mangelhafter Dokumentation und Missachtung vorhandener Informationen während einer Behandlung.

Unter der Annahme, dass für die Behandlung einer bestimmten Indikation mehrere unterschiedliche Leistungserbringer aufgesucht werden und jeder dieser Leistungserbringer seiner Pflicht nachkommt, sämtliche internen und externen Daten zu Dokumentationszwecken in seinem eigenen System zu speichern ergibt sich das in *Formel (1)* dargestellte Wachstum von Datenmengen.

---

16 Vgl. Deutscher Bundestag (2018): 1.

17 Die Datenschutzpflicht ergibt sich aus § 9 (Muster-)Berufsordnung (MBO) im Zusammenhang mit § 203 Strafgesetzbuch (StGB), die Leistungserbringer zur Wahrung des Arzt- und Patientengeheimnisses verpflichtet.

18 Vgl. Huber/Sunyaev/Krcmar (2008): 64-85. Ergänzend findet sich weitere Literatur, die sich kritisch mit der technischen Umsetzung in Deutschland bzw. der GEMATIK auseinandersetzt, wie z.B. SUNYAEV ET AL. (2009), SUNYAEV/LEIMEISTER/KRCMAR (2010) und SUNYAEV ET AL. (2010). Dieses Thema wird in *Kapitel 2.3.1* detailliert behandelt.

19 Mehr Informationen über den Aufbau der von der GEMATIK konstruierten Gesundheitstelematik sowie der von der GEMATIK geplanten elektronischen Patientenakte finden sich in *Kapitel 2.3.1*.

20 Kassenärztliche Bundesvereinigung (2017): 2. Die von der KBV genannte elektronische Patientenakte beschreibt eine Akte, die nicht im alleinigen Verantwortungsbereich eines Leistungserbringers liegt und beschreibt die vom Gesetzgeber initiierte (zentrale bzw. einheitliche) elektronische Patientenakte. Ob hier von der Lösung der GEMATIK oder einer dritten Partei, wie z.B. einer Krankenversicherung, die Rede ist, wird nicht klar.

21 Vgl. Kassenärztliche Bundesvereinigung (2017): 2.

22 Die Dokumentationspflicht wird in § 630f BGB geregelt. Absatz 1 definiert hierbei die Pflicht zur Dokumentation sowie die Kennzeichnungspflicht von (nachträglichen) Änderungen der Inhalte. Absatz 2 definiert den Umfang der elektronischen Patientenakte. Absatz 3 schreibt einen i.H.v. mindestens 10 Jahren vor.

$$D_{i,n+1} = D_{i,n} + L_{i,n+1} \qquad \textbf{Formel (1)}$$

Die Menge an Daten $D_{i,n+1}$ eines Patienten i in der Sphäre des aktuell mit der Behandlung beschäftigen Leistungserbringers $n+1$ ergibt sich aus der Summe der bereits vorhandenen Daten $D_{i,n}$ der bisherigen Leistungserbringer n mit den neuen Daten des aktuellen Leistungserbringers L_{n+1}.

Zur Vermeidung eines solchen Effekts verfolgt das deutsche Gesundheitswesen mit der vorgesehene elektronische Patientenakte, definiert in §291a SGB V, einen zentralisierten Ansatz.[23] Die Alternative eines virtualisierten Zugriffs ist nicht geplant, weil nicht davon ausgegangen wird, dass einzelne Systeme der Leistungserbringer für einen individuellen, direkten und spontanen Abruf einzelner Daten im Bedarfsfall dauerhaft zur Verfügung stehen.[24] Aus der Antwort des DEUTSCHEN BUNDESTAGES auf eine *Kleine Anfrage* verschiedener Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN (genauer Fragen 6, 7 und 8)[25] sowie aus der Regelung, dass bestehende (und neue) Drittanbieterlösungen auf Basis des §68 SGB V mit der Lösung der GEMATIK kompatibel sein und einen anbieterunabhängigen, interoperablen Datenaustausch ohne Datenverlust ermöglichen müssen,[26] lässt sich die Tendenz zu einer homogenen und von der GEMATIK kontrollierten Landschaft für eine elektronische Patientenakte ableiten.

Die GEMATIK tritt als Intermediär auf und stellt eine abgesicherte Infrastruktur bereit. Doch die zentrale Bereitstellung von Gesundheitsdaten bietet nicht nur die Chance eines Single-Point-of-Truth, sondern birgt ebenfalls das Risiko eines Single-Point-of-Failure.[27] Dieses Problem begründet das zunehmende Interesse, Intermediäre zu vermeiden, und alternativ auf Blockchain-Technologie zurückzugreifen.[28]

Die vorliegende Dissertation untersucht, inwiefern Blockchain-Technologien bereits in der Gesundheitsdatenvernetzung verwendet werden. Bestehende wissenschaftliche Literatur wird analysiert, aktuelle Erkenntnisse und Konzepte systematisiert und eine Referenzarchitektur abgeleitet, die sämtliche Variationen von Blockchain-Architekturen abbildet. Darüber hinaus wird

---

23 Vgl. Deutscher Bundestag (2018): 2.

24 Vgl. Schneider (2016): 49; Deutscher Bundestag (2018): 9.

25 Vgl. Deutscher Bundestag (2019a): 3f. Die Antwort ist zurückzuführen auf die *Kleine Anfrage* vom 25.04.2019 (vgl. Deutscher Bundestag (2019b): 2).

26 Vgl. Deutscher Bundestag (2018): 3. Andernfalls hätte die Finanzierung dieser Lösung keine Gesetzesgrundlage.

27 Vgl. Yue et al. (2016): 218.2; Xiao et al. (2018): 998.

28 NAKAMOTO gilt als Begründer der Blockchain-Technologie und beschreibt eine alternative Zahlungsmethode, die Banken als vertrauensvolle Intermediäre obsolet macht. Ein Zahlungstransfer findet direkt zwischen Sender und Empfänger statt. Das eigentlich für eine Transaktion notwendige Vertrauen werde aufgrund der Fälschungssicherheit in der Architektur gewährleistet (vgl. Nakamoto (2008)).

ein Entscheidungsmodell geliefert, das in der Entwicklung von Lösungen die Auswahl der relevanten Variation unterstützt.

Mit Blick auf die ökonomischen Interessen aller Stakeholder im Gesundheitswesen[29] wird als Kerndisziplin die Wirtschaftsinformatik (WI) gewählt, nicht die Medizininformatik (MI)[30]. Unter Zuhilfenahme der MI-Definitionsversuche der DEUTSCHEN GESELLSCHAFT FÜR MEDIZINISCHE INFORMATIK, BIOMETRIE UND EPIDEMIOLOGIE (GMDS) E.V.,[31] GREENES/SHORTLIFFE,[32] GRAHAM[33] und WYATT/LIU[34] lässt sich zwar als Gegenstandsbereich der MI die bessere Informationsversorgung in der Medizin und somit die Steigerung der Versorgungsqualität identifizieren, jedoch werden dabei keine ökonomischen Aspekte berücksichtigt, die entstehen, sobald eine Referenzarchitektur existiert.[35]

---

29 Auch SHABO identifiziert im Rahmen seiner Publikationen zu *longitudinal electronic health records* und der möglichen Einrichtung von Independent Health Record Banks (IHRB) die sozioökonomischen Besonderheiten der diversen Aufbewahrungsmodelle von Patientenakten und dass diese neben steigendem Nutzen für Patienten auch ökonomische Folgen für Leistungserbringer (z.B. sinkende Archivierungskosten) haben (vgl. Shabo (2006a): 244). Doch auch das bisher genutzte *Provider-centric-Modell* bzgl. der Aufbewahrung von Patientenakten ist schon aufgrund der Wettbewerbssituation der Leistungserbringer untereinander von wirtschaftlicher Relevanz (vgl. Shabo (2006b): 499).

30 In englischsprachiger Literatur existieren die Begriffe *Health (Care) Informatics* und *Medical Informatics*, die teilweise synonym verwendet werden (vgl. Wyatt/Liu (2002): 810).

31 *„[…] Wissenschaft der systematischen Erschließung, Verwaltung, Aufbewahrung, Verarbeitung und Bereitstellung von Daten, Informationen und Wissen in der Medizin und im Gesundheitswesen. Sie ist von dem Streben geleitet, damit zur Gestaltung der bestmöglichen Gesundheitsversorgung beizutragen"* (GMDS (o. J.)). Ähnlich formuliert REICHERTZ bereits 1975 die Aufgaben der MI als Informationsmanagement der Medizin, das sich neben der Dokumentation und Analyse auch um die Synthese von Informationen kümmert (vgl. Reichertz (1975): 710).

32 *"[…] field that concerns itself with the cognitive, information processing and communication tasks of medical practice, education, and research, including the information science and the technology to support these tasks."* (Greenes/Shortliffe (1990): 1114).

33 *„[…] evolving scientific discipline that deals with the collection, storage, retrieval, communication and optimal use of health related data, information and knowledge. The discipline utilises the methods and technologies of the information sciences for the purposes of problem solving, decision making and assuring highest quality health care in all basic and applied areas of the biomedical sciences"* (Graham (1994), zitiert nach Hovenga et al. (2010): 9).

34 *"[..] study and application of methods to improve the management of patient data, medical knowledge, population data and other information relevant to patient care and community health."* (Wyatt/Liu (2002): 810).

35 Auch ein von SCHUEMIE ET AL. durchgeführtes Mapping der MI-Literatur führt zu keinen Hinweisen auf die Betrachtung wirtschaftlicher Gesichtspunkte in der Entwicklung von MI-Lösungen. Stattdessen wird die von ihnen untersuchte Literatur in drei Cluster unterteilt: *"1) the organization, application, and evaluation of health information systems, 2) medical knowledge representation, and 3) signal and data analysis."* (Schuemie et al. (2009): 82).
Nichtsdestotrotz müssen Methoden der WI gegebenenfalls auf den Gesundheitssektor angepasst werden, solange Ergebnisse konkrete Berührungspunkte mit der Medizin aufweisen. GRAY/SOCKOLOW beschreiben in diesem Zusammenhang die Evaluation von Forschungsergebnissen, die ohne Berücksichtigung der Anwendungsdomäne (hier: Gesundheitswesen) durchgeführt wird und bei deren Berücksichtigung zu genaueren Resultaten geführt hätte (vgl. Gray/Sockolow (2016): e7.2).

1.2 Wissenschaftliche Positionierung der Wirtschaftsinformatik

Wirtschaftsinformatik (WI) entwickelte sich aus der

> *„[…] betrieblichen Notwendigkeit der Unternehmen, die Potenziale des Einsatzes von Informations- und Kommunikationstechnik zu heben"*[36].

Dabei orientiert sich die WI, wie jede andere Wissenschaft, an ihrem Gegenstandsbereich[37], den die WISSENSCHAFTLICHE KOMMISSION WIRTSCHAFTSINFORMATIK (WKWI) und der FACHBEREICH WIRTSCHAFTSINFORMATIK DER GESELLSCHAFT FÜR INFORMATIK E.V. (GI FB WI) definieren als *„Informationssysteme (IS) in Wirtschaft, Verwaltung und privatem Bereich"*[38].

Unter IS werden

> *„[…] soziotechnische Systeme [verstanden], die menschliche und maschinelle Komponenten (Teilsysteme) umfassen. Sie unterstützen die Sammlung, Strukturierung, Verarbeitung, Bereitstellung, Kommunikation und Nutzung von Daten, Informationen und Wissen sowie deren Transformation. IS tragen zur Entscheidungsfindung, Koordination, Steuerung und Kontrolle von Wertschöpfungsprozessen sowie deren Automatisierung, Integration und Virtualisierung unter insbesondere ökonomischen Kriterien bei. IS können Produkt-, Prozess- und Geschäftsmodellinnovationen bewirken."*[39]

Genauer beschreiben HEINRICH/HEINZL/RIEDL Informationssysteme als Sammlungen von Arbeitstechniken, die ineinandergreifen, nicht singulär betrachtet werden können und in den Kategorien *Mensch, Aufgabe* sowie *Informations- und Kommunikationstechnik* zusammengefasst werden (siehe *Abbildung 1-3*).[40]

---

[36] Leimeister (2015): 9.

[37] Unter einem Gegenstandsbereich werden im Rahmen der Epistemologie unter Berücksichtigung des Erkenntnisprozesses die zu untersuchenden Gegenstände verstanden (vgl. Becker et al. (2004): 337).

[38] WKWI/GI FB WI (2011): 1.

[39] WKWI/GI FB WI (2011): 1. Ergänzende Erläuterungen zu *soziotechnischen Systemen* finden sich bei Hansen/Mendling/Neumann (2015): 11-13.

[40] Vgl. Heinrich/Heinzl/Riedl (2011): 18.

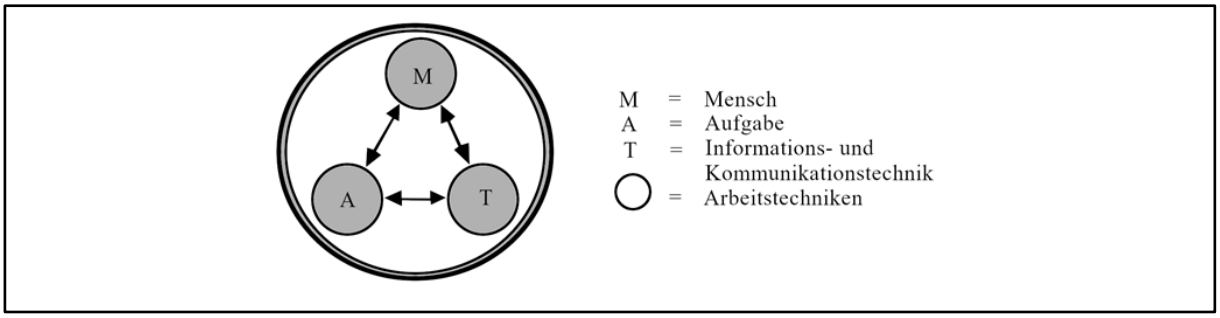


Abbildung 1-3: Struktur von soziotechnischen Systemen (Informationssystemen) (Quelle: Heinrich/Heinzl/Riedl (2011): 18)[41]

Die WI-Forschung, deren englische Bezeichnung *Information Systems Research (ISR)*[42] lautet, orientiert sich dabei aufgrund ihrer Interdisziplinarität an Forschungsmethoden der Informatik und der Wirtschaftswissenschaften,[43] folglich an gestaltungsorientierten und verhaltensorientierten Forschungsansätzen.[44]

Die Bewertung von Forschungsergebnissen basiert dabei auf den in der Forschung üblichen Formulierungen der Erkenntnisse, Ziele und Methoden. BECKER ET AL. entwickeln hierzu ein Bewertungsschema, dargestellt in *Abbildung 1-4*.

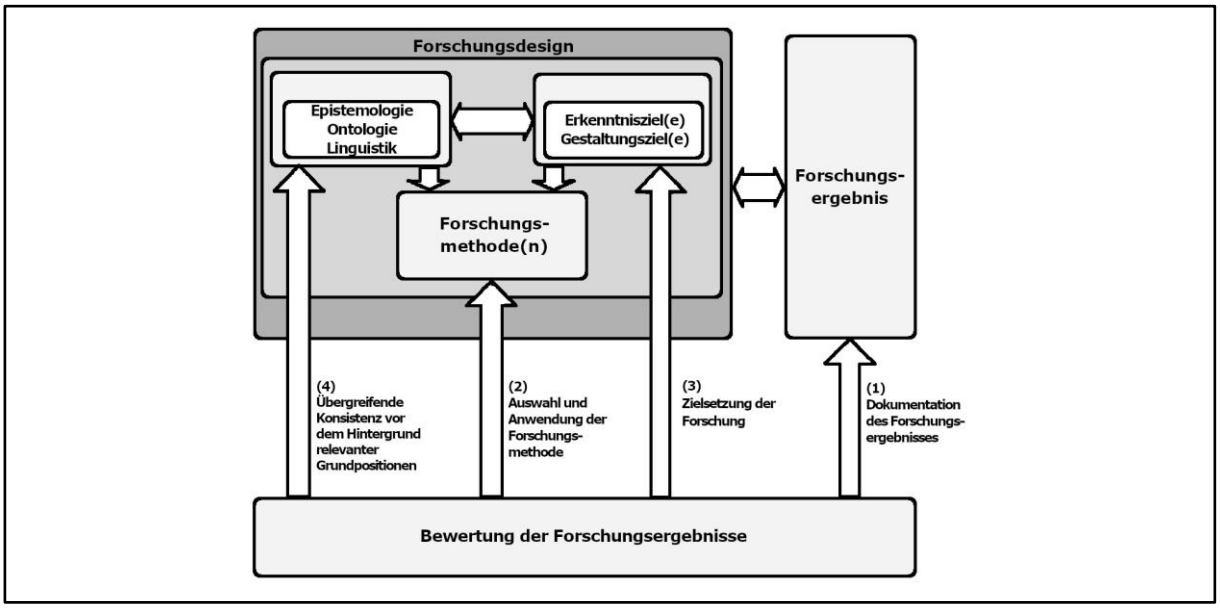


Abbildung 1-4: Begründungsinstanzen der Bewertung von Forschungsergebnissen[45] *(Quelle: Becker et al. (2004): 343)*

---

41 Eine systematische Darstellung von Erkenntniszielen gestaltungsorientierter Wirtschaftsinformatik-Forschung, aufgeteilt in *Komponententyp-orientierte Forschungsfelder*, *Beziehungstyp-orientierte Forschungsfelder* und *Ganzheitliche Forschungsfelder*, findet sich in Sinz (2010): 30f..

42 Vgl. Wilde/Hess (2006): 1.

43 Vgl. Becker et al. (2004): 335; Schwarzer/Krcmar (2014): 3.

44 Vgl. Hevner/March/Park (2004): 79; Leimeister (2015): 10.

45 *Anmerkung*: Die Original-Abbildung wurde farblich überarbeitet, sodass eine bessere Lesbarkeit erreicht wird. Eine inhaltliche Veränderung hat nicht stattgefunden.

1.2.1 Abgrenzung der gestaltungsorientierten zur verhaltensorientierten Wirtschaftsinformatik

Zunehmende Internationalisierung der Forschung in der Wirtschaftsinformatik[46] facht die Diskussion über die in der WI-Forschung genutzten Forschungsmethoden an. In der internationalen Forschungsliteratur werden insbesondere quantitative, verhaltenswissenschaftliche Ansätze verfolgt,[47] die in der Regel Hypothesen aufstellen und empirisch belegen bzw. verwerfen.[48] Im Vergleich hierzu ist die deutsche WI-Forschung betont konstruktivistisch ausgerichtet und praxisorientiert (*Relevance*).[49] Die Forschung schafft Abstrakte, die anhand beobachteter Probleme erstellt werden und deren Realisierung im Nachhinein kritisch untersucht und bewertet wird.[50] In der wissenschaftlichen Diskussion wird kritisiert, dass es diesem praxisorientierten Ansatz zumeist an fundierter Methodik (*Rigor*) fehle.[51]

Während in der Diskussion beide Forschungsansätze konkurrieren (*Rigor-vs-Relevance-Diskussion*), beschäftigen sich HEVNER/MARCH/PARK mit einer möglichen Synergie (siehe *Abbildung 1-5*) und kommen zu dem Ergebnis, dass sich beide Ansätze gegenseitig bedingen und erst gemeinsam eine Basis für die WI-Forschung, respektive die ISR, schaffen.[52]

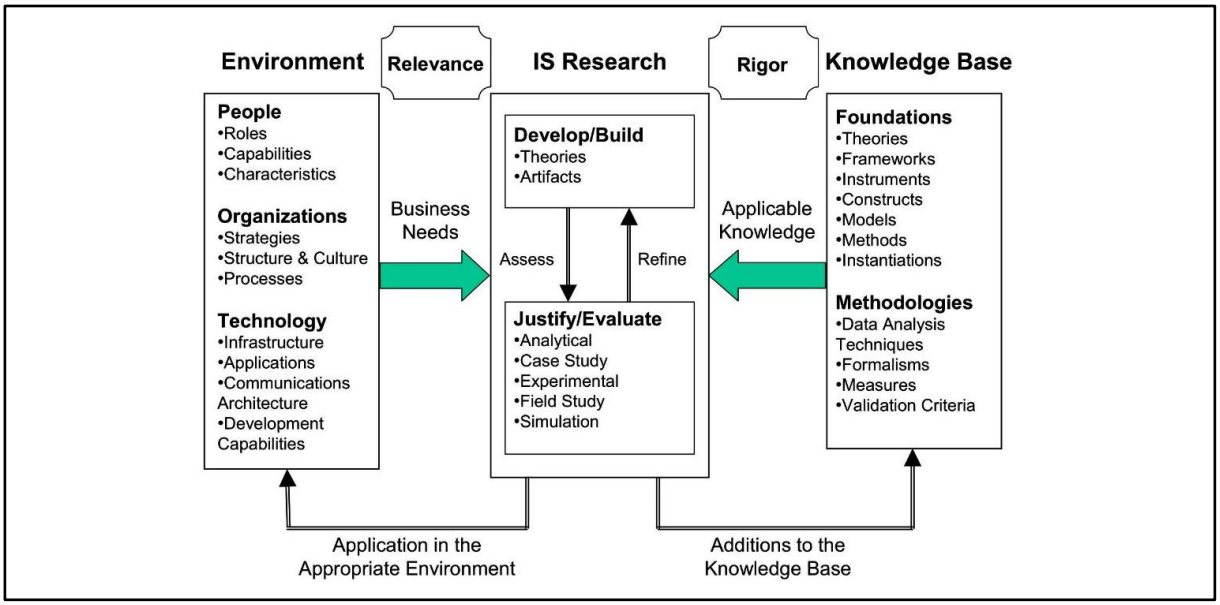


Abbildung 1-5: Framework Rigor & Relevance (Quelle: Hevner/March/Park (2004): 80)

46 Vgl. Becker et al. (2009): 4f.

47 Vgl. Becker et al. (2009): 5f.

48 Vgl. Hevner/March/Park (2004): 79; Leimeister (2015): 10f.

49 Vgl. Becker et al. (2009): 6.

50 Vgl. Hevner/March/Park (2004): 79f; Portmann/Risch (2017): 6.

51 Vgl. Heinrich (2005): 113.

52 Vgl. Hevner/March/Park (2004): 80.

Obwohl HEVNER/MARCH/PARK gestaltungsorientierte Forschung als *„[…] a problem solving process.“*[53] deklarieren, fehlt in ihren Ausführungen die Darstellung eines Prozesses.[54] Unter Verweis auf LIVARI werden drei sog. *Research Cycles* entwickelt, die sich an den von LIVARI aufgestellten zwölf Thesen orientieren (siehe *Abbildung 1-6*).[55]

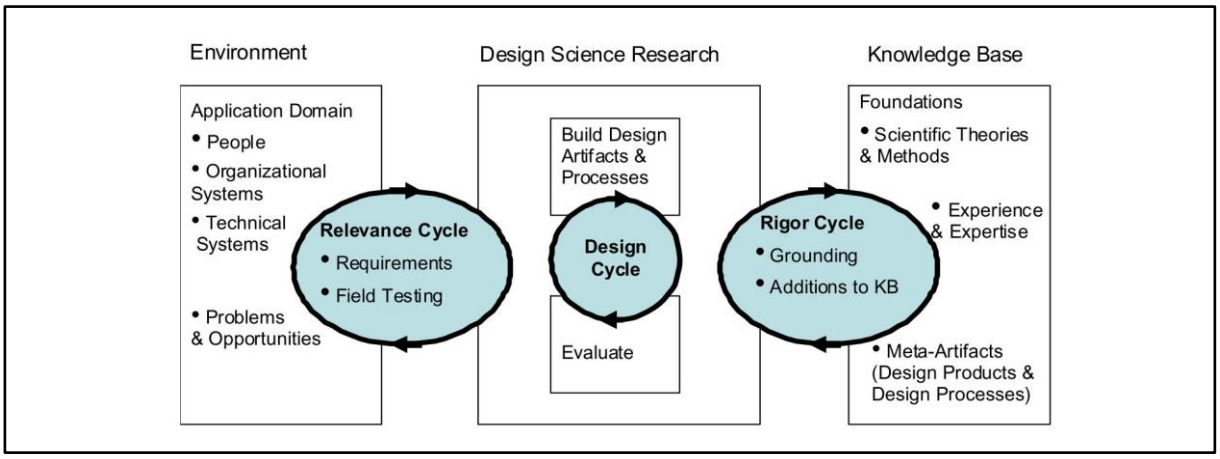


Abbildung 1-6: Design Science Research Cycles
(Quelle: Hevner (2007): 88)

Der *Relevance Cycle* legt eine Ausgangssituation sowie das geplante Ziel bzw. die Evaluierungskriterien der Problemlösung fest.[56] Der *Rigor Cycle* stellt das bereits vorhandene Wissen über Methoden und Theorien dar, die bei der Entwicklung eines Artefakts unterstützen.[57] Beide sind die Grundlage des *Design Cycle*, der unter Berücksichtigung von Ausgangslage und Ziel (*Relevance*) sowie gewählter Methode (*Rigor*) letztlich das eigentliche Artefakt konstruiert.[58]

1.2.2 Methodenprofil der Wirtschaftsinformatik

Vor dem Hintergrund methodischer Divergenzen in der Wirtschaftsinformatik führen WILDE/HESS eine empirische Untersuchung zur Identifikation der in der WI-Literatur genutzten Forschungsmethoden durch. Sie unterscheiden dabei zwischen der Makro- und der Mikroebene. In der Makro-Ebene wird die allgemeine Diskussion über *Rigor* und *Relevance* geführt,[59]

---

53 Hevner/March/Park (2004): 82. Die Autoren nutzen den Begriff *Design Science*.

54 Stattdessen definieren Hevner/March/Park sieben Richtlinien (Guidelines), die in der Forschung eingehalten werden sollen (vgl. Hevner/March/Park (2004): 82-90). Auch PEFFERS ET AL. verweisen auf einen fehlenden konkreten Prozess bzgl. des Vorgehens im DSR (vgl. Peffers et al. (2007): 51).

55 Vgl. Hevner (2007): 88; Livari (2007): 55f.

56 Vgl. Hevner (2007): 89; Riege/Saat/Bucher (2009): 70.

57 Vgl. Hevner (2007): 90.

58 Vgl. Hevner (2007): 90.

59 Vgl. Wilde/Hess (2007): 280.

während auf Mikroebene konkret in der wissenschaftlichen Literatur besprochene Methoden aufgezeigt und untersucht werden.[60] Per Definition sind Forschungsmethoden

> *„[…] mitteilbare Systeme von Regeln, die von Akteuren als Handlungspläne zielgerichtet verwendet werden können, intersubjektive Festlegungen zum Verständnis der Regeln und der darin verwendeten Begriffe enthalten und deren Befolgung oder Nichtbefolgung aufgrund des normativen und präskriptiven Charakters der Regeln feststellbar ist.“*[61]

In der durchgeführten empirischen Analyse zeigt sich, dass 91% der betrachteten WI-Literatur argumentativ-deduktiv, quantitativ empirisch, konzeptionell- bzw. formal-deduktiv orientiert sind, alternativ eine Fallstudie durchführen oder einen Prototyp erstellen. Referenzmodellierungen werden eher seltener vorgenommen und gehören mit Methoden der Simulation oder Laborexperimenten zu den verbleibenden 9% (siehe *Abbildung 1-7*).

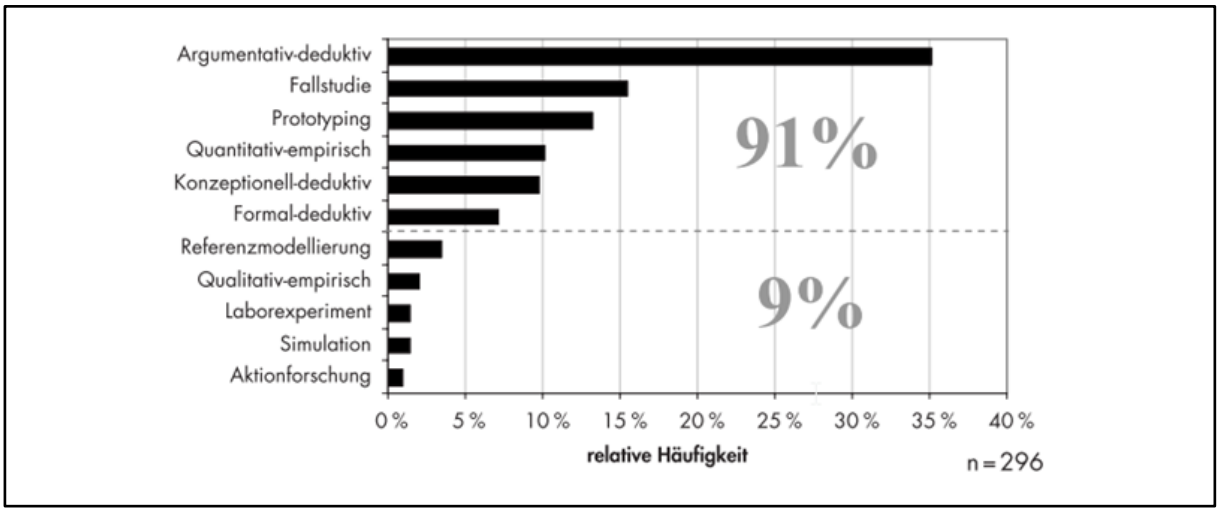


Abbildung 1-7: Einsatzhäufigkeiten der Methoden in der Stichprobe (Quelle: Wilde/Hess (2007): 284)

Demgegenüber zeigt *Abbildung 1-8* die Zuteilung der Methoden in Abhängigkeit von Formalisierungsgrad (*quantitativ* bzw. *qualitativ*) sowie Forschungsparadigma (*konstruktiv* bzw. *verhaltenswissenschaftlich*).

60 Vgl. Wilde/Hess (2007): 280f.

61 Wilde/Hess (2007): 281.

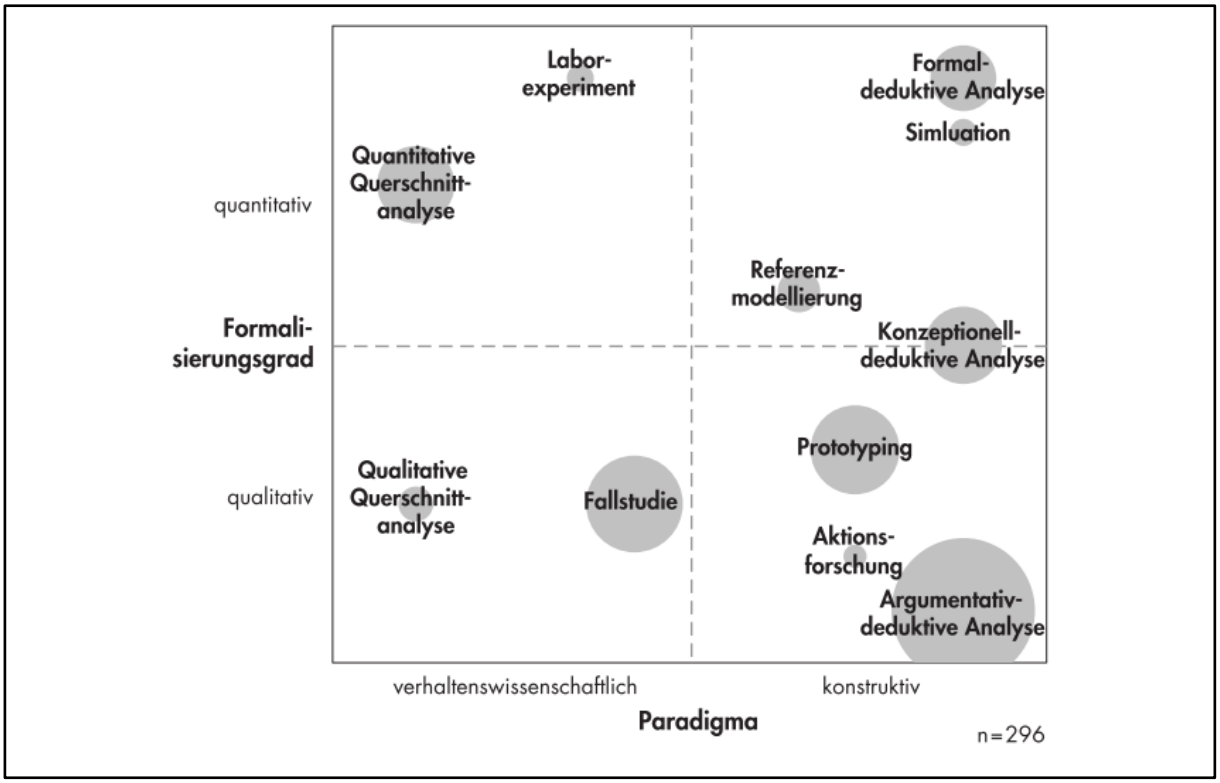


Abbildung 1-8: Methodenspektrum der WI (Quelle: Wilde/Hess (2007): 284)

Für die gestaltungsorientierte WI sind folglich sämtliche Methoden der rechten Hälfte des in *Abbildung 1-8* dargestellten Methodenspektrums relevant. Sie werden in *Tabelle 1-1* erläutert. Für diese Dissertation wird die Methode der Referenzmodellierung gewählt.

Tabelle 1-1: Auszug von Forschungsmethoden (Gekürzte Liste) (Quelle: Wilde/Hess (2007): 282)

Methode	Beschreibung
Formal-/konzeptionell- und argumentativ-deduktive Analyse	Logisch-deduktives Schließen kann als Forschungsmethode auf verschiedenen Formalisierungsstufen stattfinden: entweder im Rahmen mathematisch-formaler Modelle, in semi-formalen Modellen (konzeptionell, z. B. Petri-Netze oder rein sprachlich (argumentativ, z. B. die nicht-formale Prinzipal-Agenten-Theorie).
Simulation	Die Simulation bildet das Verhalten des zu untersuchenden Systems formal in einem Modell ab und stellt Umweltzustände durch bestimmte Belegungen der Modellparameter nach. Sowohl durch die Modellkonstruktion als auch durch die Beobachtung der endogenen Modellgrößen lassen sich Erkenntnisse gewinnen.
Referenzmodellierung	Die Referenzmodellierung erstellt induktiv (ausgehend von Beobachtungen) oder deduktiv (bspw. aus Theorien oder Modellen) meist vereinfachte und optimierte Abbildungen (Idealkonzepte) von Systemen, um so bestehende Erkenntnisse zu vertiefen und daraus Gestaltungsvorlagen zu generieren.
Aktionsforschung	Es wird ein Praxisproblem durch einen gemischten Kreis aus Wissenschaft und Praxis gelöst. Hierbei werden mehrere Zyklen aus Analyse-, Aktions-, und Evaluationsschritten durchlaufen, die jeweils gering strukturierte Instrumente wie Gruppendiskussionen oder Planspiele vorsehen.
Prototyping	Es wird eine Vorabversion eines Anwendungssystems entwickelt und evaluiert. Beide Schritte können neue Erkenntnisse generieren.

1.3 Aufbau der Dissertation

Bereits in der Abgrenzung der konstruktivistischer Forschungsparadigmen und deren Methoden wird festgestellt, dass es der DSR an einem einheitlichen Prozess mangelt,[62] an dem sich diese Dissertation orientieren könnte. Während BECKER den Prozess in vier Stufen unterteilt (Analyse, Entwurf, Evaluation und Diffusion),[63] leitet PEFFERS ET AL. die *Design Science Research Methodology* (DSRM) her, die sechs Schritte enthält (siehe *Abbildung 1-9*).

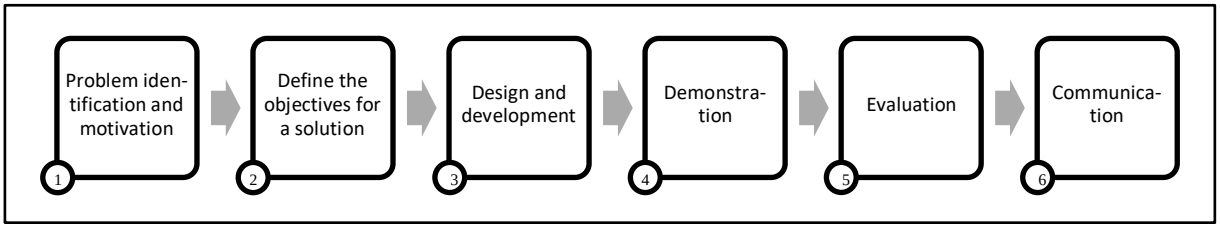


Abbildung 1-9: DSRM-Prozess
(Quelle: Eigene Darstellung in Anlehnung an Peffers et al. (2007): 52-56)

Darauf aufbauend entwickeln GREGOR/HEVNER ein Schema, das anhand einer strukturellen Analyse von DSR-Publikationen sieben Sektionen identifiziert und folglich einen idealtypischen Aufbau repräsentiert (siehe *Tabelle 1-2*).[64] Die Autoren berufen sich dabei auf eine Literatur-Analyse, die neben den bereits angeführten Publikationen von HEVNER/MARCH/PARK und PEFFERS ET AL.[65] auch Publikationen von HEVNER/CHATTERJEE (2010), SEIN ET AL. (2011), SØRENSEN (2002), VAISHNAVI/KUECHLER (2008) und ZOBEL (2005) mit einbeziehen.

Tabelle 1-2: DSR Publikationsschema
(Quelle: Gregor/Hevner (2013): 350)

Section	Content
1. Introduction	*Problem definition, problem significance/motivation, introduction to key concepts, research questions/objectives, scope of study, overview of methods and findings, theoretical and practical significance, structure of remainder of paper.* For DSR, the contents are similar, but the problem definition and research objectives should specify the **goals** that are required of the artifact to be developed.
2. Literature Review	*Prior work that is relevant to the study, including theories, empirical research studies and findings/reports from practice.* For DSR work, the prior literature surveyed should include any prior design theory/knowledge relating to the class of problems to be addressed, including artifacts that have already been developed to solve similar problems.

62 Vgl. Peffers et al. (2007): 51.

63 Vgl. Becker (2010): 13.

64 Vgl. Gregor/Hevner (2013): 342.

65 In Gregor/Hevner (2013) wird die Quelle mit dem Erscheinungsjahr 2008 angegeben. Diese Diskrepanz ergibt sich aus dem Umstand, dass Veröffentlichungen des Jahrgang 24 der Zeitschrift in 2007 und 2008 stattfanden. 2008 wäre allerdings erst für Ausgabe 4 zutreffend. Insofern ist von einem Fehler in Gregor/Hevner auszugehen.

3. Method	*The research approach that was employed.* For DSR work, the specific DSR approach adopted should be explained with reference to existing authorities.
4. Artifact Description	*A concise description of the artifact at the appropriate level of abstraction to make a new contribution to the knowledge base.* This section (or sections) should occupy the major part of the paper. The format is likely to be variable but should include at least the description of the designed artifact and, perhaps, the design search process.
5. Evaluation	*Evidence that the artifact is useful.* The artifact is evaluated to demonstrate its worth with evidence addressing criteria such as validity, utility, quality, and efficacy.
6. Discussion	*Interpretation of the results: what the results mean and how they relate back to the objectives stated in the Introduction section. Can include: summary of what was learned, comparison with prior work, limitations, theoretical significance, practical significance, and areas requiring further work.* Research contributions are highlighted and the broad implications of the paper's results to research and practice are discussed.
7. Conclusions	*Concluding paragraphs that restate the important findings of the work.* Restates the main ideas in the contribution and why they are important.

Die vorliegende Dissertation orientiert sich am in *Tabelle 1-2* dargestellten Aufbau und richtet sich entsprechend ihrer Fragestellungen an den von WILDE/HESS (2007) beschriebenen Methoden konstruktivistischer bzw. gestaltungsorientierter Forschung (siehe *Abbildung 1-8* und *Tabelle 1-1*) aus.

Tabelle 1-3: Aufbau der Arbeit
(Quelle: Eigene Darstellung)

Section	Chapter (Kapitel)
1. Introduction	Kapitel 1, 2 und 3
2. Literature Review	Kapitel 4
3. Method	Kapitel 5
4. Artifact Description	Kapitel 6 und 7
5. Evaluation	Kapitel 8
6. Discussion	Kapitel 8
7. Conclusions	Kapitel 8 und 9

2 Grundlagen der Gesundheitsdatenvernetzung

2.1 Patientenakten und Varianten der Speicherung von Gesundheitsdaten

Aufgrund terminologischer Uneinheitlichkeit bezüglich des Begriffs der (elektronischen) Patientenakte in der Literatur[66] wird zur Herstellung von Einheitlichkeit zunächst eine Abgrenzung der Begriffe vorgenommen.

Norm ISO/TR 20514:2005 der INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) beschäftigt sich mit der Bereitstellung von Patientendaten in elektronischer Form und definiert einen *Electronic Health Record (EHR)* als

> *„Repository of information regarding the health status of a subject of care, in computer processable form.“*[67]

Diese allgemeine Definition wird durch die Definition des *Electronic health record for integrated care* (ICEHR) weiter konkretisiert, der gemäß ISO ein

> *„repository of information regarding the health status of a subject of care, in computer processable form, stored and transmitted securely and accessible by multiple authorized users, having a standardized or commonly agreed logical information model that is independent of EHR systems and whose primary purpose is the support of continuing, efficient and quality integrated health care”*[68]

darstellt. Die zunächst allgemein gehaltene Definition ist den bereits von der ISO festgestellten unterschiedlichen Ausprägungen der EHR geschuldet, die in *Abbildung 2-1* dargestellt werden.[69]

---

66 Vgl. Haas (2017): 47.

67 International Organization of Standardization (2005): 2.

68 International Organization of Standardization (2005): 2.

69 Vgl. International Organization of Standardization (2005): 2.

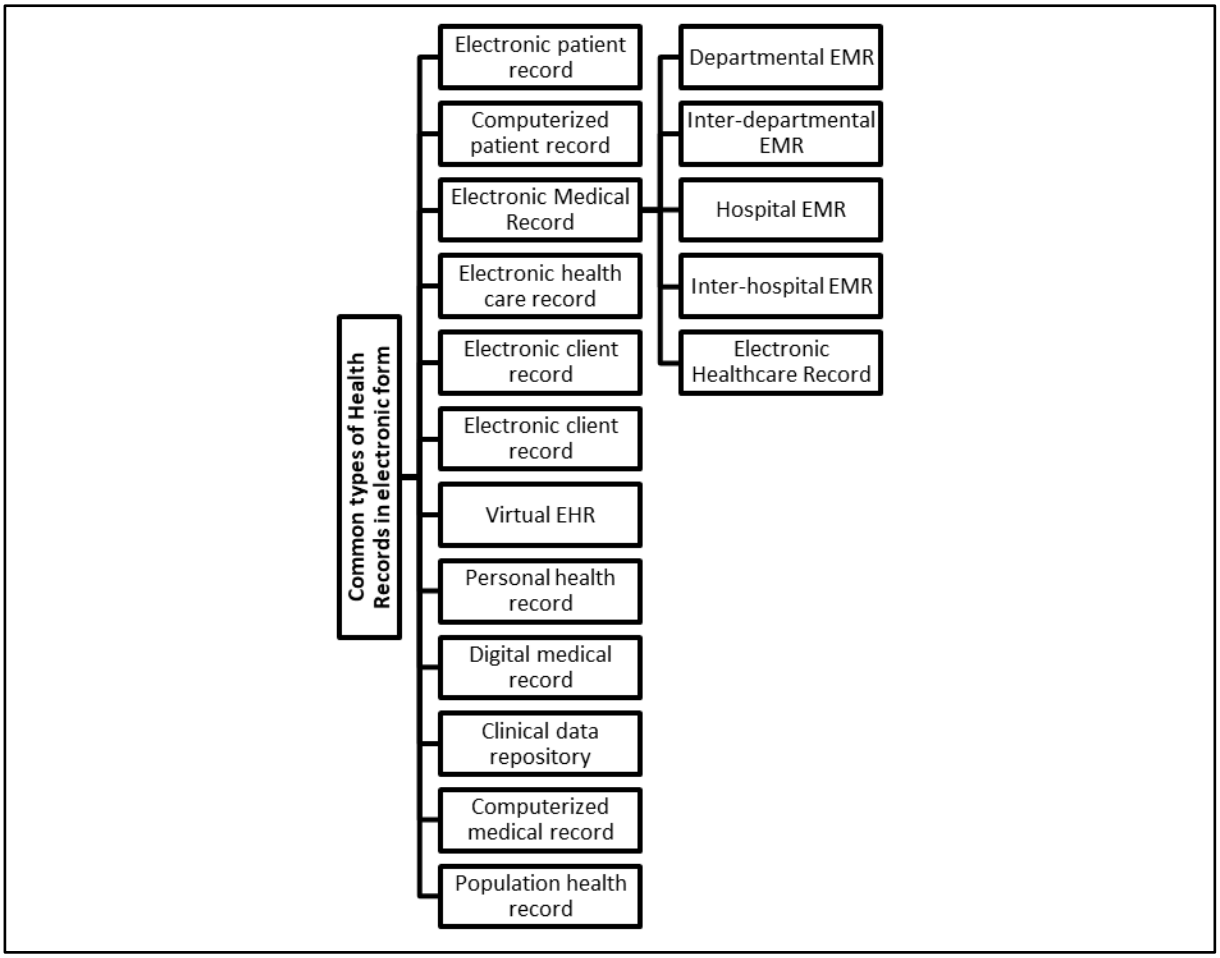


Abbildung 2-1: Begriffsvielfalt Electronic Health Records[70]
(Quelle: In Anlehnung an International Organization of Standardization (2005): 12-14)

Zur Systematisierung der verschiedenen Terminologien entwickelt ein bundesweit aktiver Arbeitskreis 2011 eine Übersicht und reduziert die in *Abbildung 2-1* genannten Begriffe auf sieben Aktentypen (siehe *Tabelle 2-1)*, deren Definitionen HAAS zu einem späteren Zeitpunkt weiter ergänzt.

[70] Die ISO nennt zwar die Begriffe *Electronic Health Records* (EHR) und *Electronic Health Care Records (EHCR)* separat, weist jedoch darauf hin, dass EHCR synonym mit EHR und insbesondere in Europa genutzt wird (vgl. International Organization of Standardization (2005): 13).

Tabelle 2-1: Aktentypen
(Quelle: Haas (2017): 55)

Aktentypen	Beschreibung
Institutionelle Elektronische Fallakte *International:* *Keine Entsprechung*	Alle Daten und Dokumente eines medizinischen Behandlungsfalles eines Patienten in einer Gesundheitsversorgungseinrichtung. Die Einträge sind ärztlich geführt und moderiert. Unter einem medizinischen Behandlungsfall werden dabei alle Maßnahmen zur Behandlung einer bestimmten Erkrankung verstanden. Während bei Papierakten, z. B. in Krankenhäusern, pro Aufenthalt eine solche Fallakte angelegt wurde, tritt die fallorientierte Sicht zumindest für Akten in der elektronischen Welt zunehmend in den Hintergrund, sodass es einfacher möglich ist, Informationen verschiedener Fälle zu einer gesamtheitlichen institutionellen Patientenakte zusammenzuführen.
Institutionelle Elektronische Patientenakte (iEPA) *International:* *Electronic Medical Record (EMR)* *Electronic Patient Record (*EPR*)*	Alle Daten und Dokumente aller Behandlungen eines Patienten in einer Gesundheitsversorgungseinrichtung. Die Einträge sind ärztlich geführt und moderiert. Dabei werden alle Informationen zu verschiedenen Fällen zu einer Akte zusammengeführt. Dies bedeutet nicht, dass die Fallsicht aufgelöst wird, aber es können immer fachübergreifende Aspekte verwaltet und zugegriffen werden. Aufgrund des deutschen Abrechnungsrechtes für den stationären Bereich ist es immer noch sehr wichtig, einzelne stationäre Fälle abgeschlossen und gegeneinander abgegrenzt zu dokumentierten. Insofern werden oftmals Vorinformationen aus älteren Fällen in den neuen Fall kopiert.
Einrichtungsübergreifende medizinische Fallakte (eFA) *International:* *Keine Entsprechung*	Hierbei werden die zur Entscheidungsfindung bei einer gemeinsamen Behandlung eines bestimmten medizinischen Problems von den Behandelnden als relevant eingestuften Daten und Dokumente über alle Gesundheitsversorgungseinrichtungen hinweg in einer einrichtungsübergreifenden Falldokumentation zusammengeführt, die Akte ist ärztlich geführt und moderiert. Es handelt sich also um eine dedizierte einrichtungsübergreifende Fallakte.
Einrichtungsübergreifende Elektronische Patientenakte (eEPA) *International:* *Electronic Health Record (EHR)* *Electronic Patient Record (EPR)*	Die wichtigsten Daten und Dokumente aller Behandlungen eines Patienten über alle medizinischen Fälle und Gesundheitsversorgungseinrichtungen hinweg. Die Einträge sind ärztlich geführt und moderiert, ggf. ergänzt mit behandlungsrelevanten eigenen Eintragungen des Patienten auf Anweisung des Arztes.
Persönliche Elektronische Patientenakte (pEPA) *International:* *Personal Electronic Health Record (PHR)* *Personally Controlled Health Record (PCHR)*	Fallübergreifende Akte unter der Datenhoheit des Patienten. Die Entscheidung über die konkrete Nutzung (Zweckbestimmung) erfolgt im Einzelfall durch den Patienten, indem dieser die Informationen bei Bedarf einem behandelnden Arzt zur Verfügung stellt. Der Patient kann Rechte auch an einen Arzt seines Vertrauens delegieren. Sinn der pEPA ist, als Quelle für die Speisung der zweckbestimmten Patientenakten in der Verantwortung der Ärzte zu dienen. Diese Art von *persönlichen* Akten wurde in Deutschland lange als Gesundheitsakte bezeichnet.
Elektronische Basisdokumentationsakte *International:* *Minimum Basic Data Set (MBDS)* *Patient Summary Record (PSR)*	Nur wenige ausgewählte lebenslang wichtige medizinische Daten, wie Diagnosen, Maßnahmen, Risikofaktoren etc., jedoch keine Dokumente. Die Einträge sind ärztlich geführt und moderiert. Eine solche minimale Akte mit jedoch vollständigen Informationen aller wichtigen Aspekte soll vor allen Dingen die Übersichtlichkeit verbessern und im Notfall oder bei Arztwechsel die Weiterbehandlung erleichtern. In abgewandelter Form stellt der Notfalldatensatz gemäß § 291a SGB V eine solche Basisdokumentation dar. Mancherorts wird diese auch als ‚Miniakte' bezeichnet.
Registerakte	Ganz wenige vollständig strukturierte und formalisierte Inhalte zu einer definierten Krankheitsklasse, wobei die Informationen zumeist pseudonymisiert abgelegt werden und der Verwendungszweck tertiär ist, also diese Akten für den wissenschaftlichen Erkenntnisgewinn oder die Gesundheitsberichterstattung geführt werden. Prominenteste Beispiele sind die epidemiologischen und klinischen Krebsregister.

Anmerkung: Ergänzte Fassung, beruhend auf ZTG (2011): 16.

Im direkten Vergleich ergeben sich Überschneidungen in den Aktentypen. So können mehrere EMR Basis von EHR sein und wiederum mehrere EHR Ausgangspunkt für PHR, während ein Patient auch wählen kann, welche EHR in einem PHR abgebildet werden dürfen.[71]

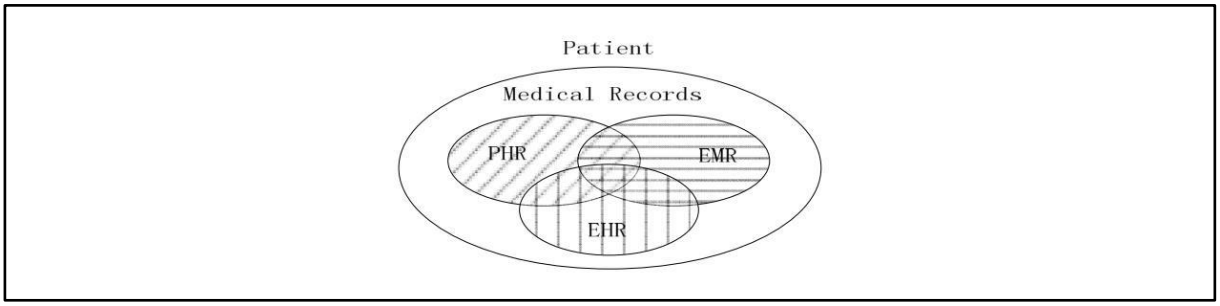


Abbildung 2-2: Schnittmengen der Aktentypen (Quelle: Zhang/Liu (2010): 269)

Zusammenfassend lassen sich Aktentypen in institutionell- und patientenkontrollierte Akten unterscheiden. Während bei institutionell-kontrollierten Aktentypen ausschließlich Leistungserbringer über die Preisgabe von Gesundheitsdaten entscheiden, liegt bei patientenkontrollierten Akten die Entscheidungsgewalt, über die Verwendung der eigenen Gesundheitsdaten beim Patienten selbst.[72] Auch erweitert sich der Umfang patientenkontrollierter Akten, indem neben den von Leistungserbringern erstellten Daten auch durch eigene (medizinische) Geräte erzeugte Daten enthalten sein können.[73]

2.2 Intermediäre im Gesundheitswesen

Intermediäre[74] werden im ökonomischen Kontext üblicherweise auf imperfekten Märkten[75] zur Befriedigung von Angebot und Nachfrage und gleichzeitiger Reduktion von Transaktions-Kosten eingesetzt.[76] Eine detaillierte Auseinandersetzung mit dem Wettbewerb im Gesundheitswesen wird in der vorliegenden Forschungsarbeit nicht vorgenommen und stattdessen unterstellt, dass die Wettbewerbsstruktur grundsätzlich kompliziert ist und ein imperfekter Markt

---

71 Vgl. Zhang/Liu (2010): 269.

72 Vgl. Haas (2017): 55.

73 Vgl. Mense/Athanasiadis (2018): 7.

74 *Intermediation* ist etymologisch betrachtet eine Kombination der beiden lateinischen Worte *inter* (übersetzt: inmitten, zwischen, unter) und *medius* (übersetzt: der mittlere, in der Mitte stehend, in der Mitte gelegen) (vgl. Duden.de (o. J.)).

75 Unter einem *Markt* wird dabei die Vermittlung von Leistung und Gegenleistung zwischen Anbieter und Nachfrager verstanden (vgl. Thiemer (2005): 285). *Imperfekte Märkte* zeichnen sich dadurch aus, dass Preise für das gleiche Gut aufgrund von Informationsasymmetrien (fehlende Markttransparenz), Transaktionskosten und bestehenden Handelsbarrieren (z.B. räumlich, zeitlich) verschieden sind (vgl. Thiemer (2005): 287). Ursache sind: fehlender Wettbewerb, externe Effekte, Informationsasymmetrien und Anpassungsmängel (vgl. Thiemer (2005): 290-292). Ergänzende Ausführungen zu *Marktversagen* finden sich bei FRITSCH/WEIN/EWERS (1999).

76 Vgl. Walter (2007): 30f; Goddard (2015): 567.

bzw. Marktversagen vorliegt.[77] Marktversagen wird durch Informationsasymmetrien verursacht,[78] wie sie bspw. bereits entlang der Behandlungspfade identifiziert wurden.[79] Informationsasymmetrien entstehen nicht nur zwischen Leistungserbringern entlang eines Behandlungspfades, sondern auch zwischen Leistungserbringer und Patient. Der Arzt hat im Vergleich zum Patienten einen Wissensvorsprung. Ein kritischer Vergleich im Wettbewerbsumfeld des Leistungserbringers ist für einen Patienten schwierig bis unmöglich.[80] Ein Intermediär verbessert die Position des Patienten, indem die relevanten Informationen unabhängig vom Stakeholder, in diesem Fall einem Leistungserbringer, bereitgestellt werden, und befähigt ihn dazu, an seiner eigenen Behandlung teilzuhaben.[81] Ein Intermediär nimmt in diesen Fällen die Rolle eines *Informationsintermediärs*[82] ein, dessen Aufgabe die Gewinnung und Aggregation von Informationen aus unterschiedlichen Quellen sowie die Steuerung der jeweiligen Bereitstellung zum Ausgleich von Informationsasymmetrien ist.[83] ROSE ergänzt diese Definition um eine ökonomische Komponente und definiert einen Informationsintermediär als ein

> *„(…) independent, profit maximizing economic information processing system performing its activities (information acquisition, processing and dissemination) on behalf of other economic agents´ information needs.“*[84]

---

77 Ob es im Gesundheitswesen tatsächlich zu einem Marktversagen kommt, ist abhängig vom betrachteten Teilbereich sowie der regionalspezifischen Ausgestaltung (vgl. Goddard (2015): 567).

78 Vgl. Thiemer (2005): 290-292.

79 Nur eine *Informationsasymmetrie* begründet noch kein Marktversagen (vgl. Thiemer (2005): 291). Jedoch existiert im Gesundheitswesen *kein wirklicher Wettbewerb* zwischen Leistungserbringern, denn dieser würde in der Regel anhand der Leistung von Leistungserbringern über ein Bestehen oder Nicht-Bestehen am Markt entscheiden. Zudem fehlt es aufgrund von Markteintrittsbarrieren an (neuen) Mitbewerbern (vgl. Porter/Teisberg (2006): 3f; Mwachofi/Al-Assaf (2011): 331). Ergänzend existieren externe Effekte, also nicht quantifizierbare Auswirkungen auf Preisgestaltung oder Volkswirtschaft (vgl. Thiemer (2005): 291). Der bestehende Fokus auf die sog. *Zero-Sum-Competition* zwischen den Versorgungseinrichtungen zielt auf individuelle wirtschaftliche Interessen und stellt dabei nicht die Qualität der Versorgung und Auswirkungen auf die Allgemeinheit in den Vordergrund (vgl. Porter/Teisberg (2006): 4). Folge ist eine mögliche Über- oder Unterversorgung, basierend auf wirtschaftlichen Interessen (vgl. Porter/Teisberg (2006): 68), die in der Folge nicht quantifizierbare Kosten für die Allgemeinheit begründen.

80 Vgl. Mwachofi/Al-Assaf (2011): 331f.

81 Vgl. Walter (2007): 67. WALTER klassifiziert die in seiner Arbeit betrachteten Content-Märkte (bezogen auf Medieninhalte, Zeitungsartikel, Filme, Musik) grundsätzlich als unvollkommen und verweist dabei auf die Institutionenökonomik, beschrieben von ERLEI (1998) und WILLIAMSON (2010). Aufgrund dessen, dass bei Gesundheitsdaten ebenfalls von Content, genauer *Healthcare Content* und dem damit verbundenen *Healthcare Content Management*, gesprochen werden kann, ist eine Übertragung der Schlussfolgerung möglich.

82 Alternativ können Informationsintermediäre auch als *Datentreuhänder* (engl. *Information Fiduciary*) bezeichnet werden, denn diese sind *„a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship.“* (Balkin (2016): 1209).

83 Vgl. Stanzel (2007): 14f. STANZEL beschreibt den Begriff im Zusammenhang mit Intermediation im Finanzsystem.

84 Rose (1999): 79.

Demzufolge wird einem Intermediär, zumindest den Netzwerkteilnehmern gegenüber, ein ökonomisches Interesse an der eigenen Tätigkeit unterstellt.

2.3 Ausgewählte Ansätze von Informationsintermediation in Deutschland

Dieses Kapitel gibt eine Überblick über die bereits gestarteten Initiativen in Deutschland, beginnend mit der Übernahme des gesetzlichen Auftrags[85] durch die GEMATIK, eine Infrastruktur zu schaffen, die einen (sicheren) Datenaustausch ermöglicht,[86] über das vom BMBF 2015 initiierte *Förderkonzept Medizininformatik*, das sich mit dem einrichtungsübergreifenden Austausch von Forschungsdaten unter Einbezug von Behandlungsdaten beschäftigt und sich hiervon Erkenntnisse für neue Behandlungsmethoden verspricht.[87]

2.3.1 Gesundheitstelematik und elektronische Patientenakte der GEMATIK

Die GEMATIK arbeitet seit 2005 an der Umsetzung einer zentralen Kommunikationsplattform zur Vernetzung der einzelnen Akteure im Gesundheitswesen. Sie agiert dabei als Dienstleister ihrer Gesellschafter, den Spitzenorganisationen im deutschen Gesundheitswesen.[88] Unter Kommunikationsplattform wird dabei der Betrieb einer Telematik-Infrastruktur (TI) verstanden, die bei der Übermittlung und Bereitstellung von Daten unterstützt und den Betrieb von Fachanwendungen ermöglicht.[89] *Abbildung 2-3* beschreibt den Konzeptentwurf der GEMATIK von 2008.

---

85 Zurückzuführen auf das *Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung*, das bereits in *Kapitel 1.1* angesprochen wird.

86 Vgl. gematik (2014): 37.

87 Vgl. Bundesministerium für Bildung und Forschung (2015): 9.

88 Vgl. gematik (o. J.b).

89 Vgl. gematik (2014): 37. Es wird dabei zwischen *Fachanwendung* und *Fachdienst* unterschieden. Fachanwendungen nutzen die TI zur Bereitstellung ihrer Funktionen und berücksichtigen dabei die Vorschriften zur Anbindung an die TI (vgl. gematik (2014): 17). Ein Fachdienst hingegen ist innerhalb der TI aktiv und unterstützt die Fachanwendung in der Bereitstellung ihrer Funktionen (vgl. gematik (2014): 17).

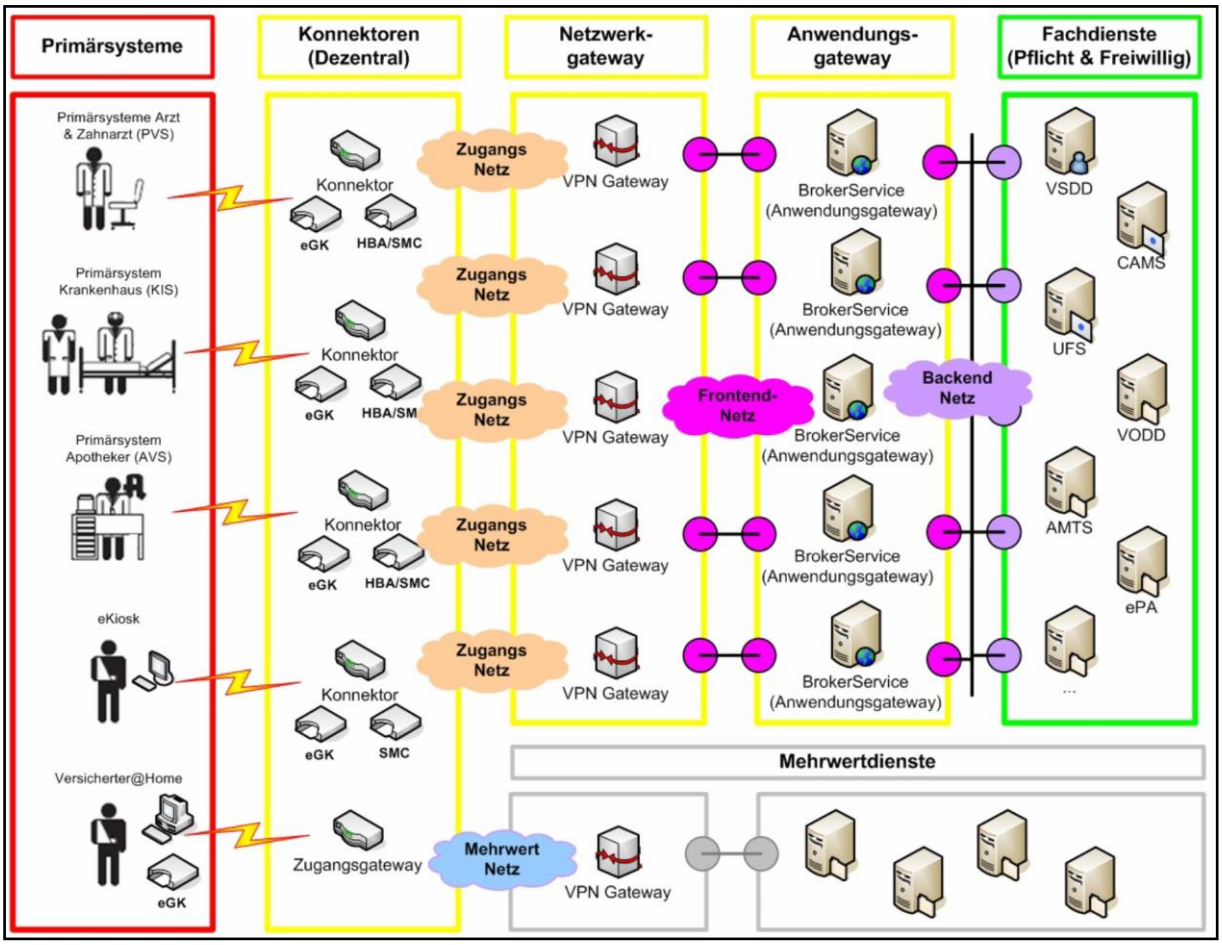


Abbildung 2-3: Gesamtarchitektur des gematik-Konzepts (Quelle: gematik (2008): 27)

Unter Primärsystemen werden alle Praxisverwaltungssysteme (PVS), Krankenhausinformationssysteme (KIS) und Apothekenverwaltungssysteme (AVS) verstanden.[90] Hinzu kommen das geplante *eKiosk* und *Versicherter@Home*, die beide Patienten den Zugriff auf die TO ermöglichen sollen,[91] in der Konzeptbeschreibung von 2008 jedoch noch keine tiefergehende Berücksichtigung finden. Über Konnektoren in Verbindung mit Kartenlesegeräten und den ausgege-

90 Vgl. gematik (2008): 28.

91 Vgl. gematik (2008): 28. *eKiosk* und *Versicherter@Home* sind Ideen und Bezeichnungen von 2008 und finden 2018 Berücksichtigung im *Systemspezifisches Konzept ePA* (siehe gematik (2018e)).

benen Smartcards werden mittels VPN-Gateways geschützte Verbindungen in die TI hergestellt.[92] Broker ermöglichen anschließend Zugriffe auf diverse Fachdienste, wie bspw. Versichertenstammdatendienst (VSDD)[93], Verordnungsdatendienst (VODD)[94] oder elektronische Patientenakte (ePA) bzw. Gesundheitsakte.

Der in *Abbildung 2-3* gelb dargestellte Bereich beschreibt die konkrete TI, deren Architektur in *Abbildung 2-4* präzisiert wird.

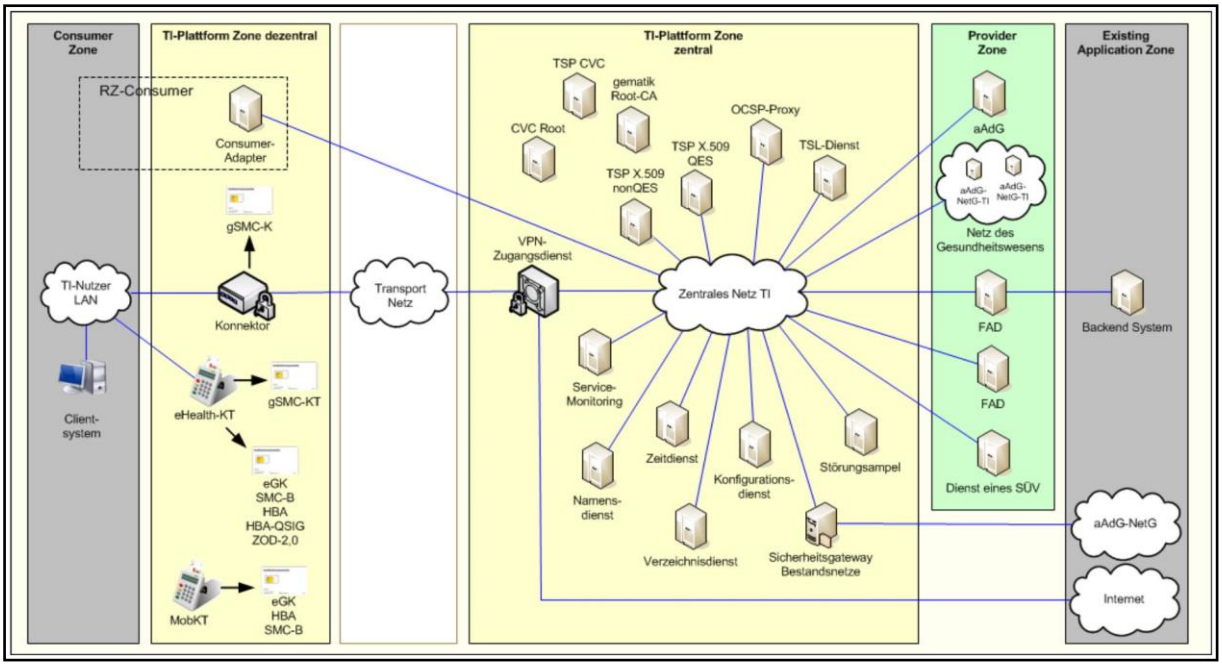


Abbildung 2-4: Konzept-Architektur der TI-Plattform (Quelle: gematik (2018c): 48)

Um Zugriff auf die TI über den Konnektor zu erhalten, benötigen Leistungserbringer ein Kartenterminal, das zur Identifikation sowie zur Ver- und Entschlüsselung der übertragenen Daten genutzt wird. Aus diesem Grund erhalten alle Netzwerkteilnehmer Smartcards, Patienten eine

---

92 Vgl. gematik (2008): 29. Statt einer direkten Verbindung zwischen zwei Partnern, z.B. durch eine direkte, eigene Leitung, die teuer und nicht flexibel ist, nutzt ein Virtual Private Network (VPN) eine bereits bestehende öffentliche Leitung, z.B. Internet, stellt einen Tunnel zwischen zwei Partnern (Hosts) her, verschlüsselt die zu übertragenden Daten im Vorfeld und überträgt diese sicher (vgl. Rao/Nayak (2014): 246).

93 Das *VSDD* ist ein Teildienst des Versicherungsstammdatenmanagements (VSDM). Das VSDM soll Leistungserbringern erlauben, den Versicherungsstatus eines Patienten zu überprüfen und ggf. anzupassen (vgl. gematik (2008): 30). Neben dem VSDD existieren weitere externe Schnittstellen, die in *Abbildung 2-3* nicht explizit genannt werden: den Update Flag Service (UFS) und das Card Management System (CMS). Diese drei Dienste werden in der technischen Dokumentation des VSDM näher erläutert (vgl. gematik (2017): 78-80).

94 Der *VODD* ist ein Teildienst des Verordnungsdatenmanagements (VODM) und soll die digitale Übermittlung von ärztlichen Verordnungen, z.B. an Apotheken oder andere Leistungserbringer, ermöglichen (vgl. gematik (2008): 30f.).

elektronische Gesundheitskarte (eGK), Leistungserbringer den *Heilberufsausweis* (HBA)[95] und die *Secure Module Card* (SMC-B)[96]. Diese enthalten das notwendige Schlüsselmaterial, um die für eine sichere Verbindung notwendigen kryptographischen Verfahren der TI durchzuführen.[97] Die tatsächliche Übermittlung oder Bereitstellung von Gesundheitsdaten wird auf drei Wegen angeboten:

i. Speicherung von vertraulichen Informationen direkt auf der eGK
ii. Kommunikationsdienst *KOM-LE*
iii. Fachanwendung *ePA*

Die Speicherung von Gesundheitsdaten auf der eGK (i) beschränkt sich auf allgemeine, persönliche und geschützte Versichertendaten.[98] Während allgemeine und persönliche Daten über ein Kartenterminal ohne Freigabe durch den Patienten abgerufen werden können,[99] werden geschützte Versichertendaten über das sog. Zwei-Karten-Prinzip abgerufen.[100] Neben der eGK ist ein HBA oder eine SMC-B sowie eine beidseitige PIN-Eingabe erforderlich.[101]

KOM-LE (ii) bzw. die Fachanwendung *Sichere Kommunikation zwischen Leistungserbringern* dient einer sicheren E-Mail-Kommunikation zwischen Leistungserbringern und erzeugt eine Ende-zu-Ende-Verschlüsselung inklusive digitaler Signatur zur Wahrung der Vertraulichkeit und Integrität übermittelter Daten oder Dokumente während des Transports.[102]

Das Ende 2018 vorgestellte Systemkonzept zur *Fachanwendung ePA*[103] (iii) beschreibt ergänzend zu *KOM-LE* und den Speichermöglichkeiten auf der eGK die von der GEMATIK zur Verfügung zu stellende Gesundheitsakte und wurde in den ursprünglichen Konzepten von 2008 noch als *eKiosk* und *Versicherter@Home* bezeichnet. Statt sich auf den E-Mail-Versand zu

---

95 Der HBA berechtigt Ärzte, Patientendaten, die entweder auf der eGK gespeichert sind oder in der ePA (allgemeiner: innerhalb der TI) liegen und mit der eGK freigegeben werden, einzusehen und ggf. zu bearbeiten (vgl. gematik (2016): 15).

96 Eine SMC-B ist eine Systemkarte und wird an alle Einrichtungen des Gesundheitswesens herausgegeben, sodass alle Mitarbeiter von Einrichtungen Funktionen der Telematik nutzen können, ohne einen HBA zu benötigen (vgl. Caumanns/Rode/Kraufmann (2017): 136).

97 Vgl. Caumanns/Rode/Kraufmann (2017): 135f. Für weiterführende Informationen zu den auf den Karten enthaltenen Zertifikaten wird auf die entsprechenden Spezifikationen der eGK (gematik (2019b)), respektive des HBA (gematik (2018d)) verwiesen.

98 Der genaue Aufbau dieser Informationsmodelle findet sich in: gematik (2019a): 21-34.

99 Vgl. gematik (2013): 6, 8.

100 Vgl. gematik (2013): 8.

101 Vgl. gematik (2016): 15. Die Notwendigkeit dieser Lösung ergibt sich aus §291a Abs. 5 SGB V.

102 Vgl. gematik (2018b).

103 Vgl. gematik (2018a). Die hier genutzte Abkürzung weicht von der bereits von HAAS genutzten eEPA ab, da es sich hier zwar auch um eine einrichtungsübergreifende Patientenakte handelt, sich die GEMATIK jedoch nicht an die bereits getätigten Definitionsbestrebungen hält.

beschränken, wird die ePA als Dokumentenmanagementsystem[104] eingesetzt und erlaubt dem Patienten den Zugriff auf die TI.[105] Der Patient selbst kann entscheiden, ob Dokumente vom Arzt in die ePA hochgeladen werden und welche bei einer Weiterbehandlung übermittelt werden dürfen. Außerdem soll der Patient eigene Dokumente einstellen dürfen.[106] Folglich handelt es sich bei der ePA um die in *Tabelle 2-1* beschriebene pEPA bzw. PHR.

Aufgrund der während der TI-Entwicklung parallel entstandenen Projekte der Privatwirtschaft und Krankenkassen hat sich die GEMATIK entschieden, als *Bridge-Certificate-Authority* (Bridge-CA) zu agieren, die verschiedenen, bestehenden sicheren Infrastrukturen (vornehmlich Public-Key-Infrastructure (PKI)) der unterschiedlichen Patientenaktentypen miteinander zu verbinden und auf diesem Weg deren Sicherheit übergreifend zu bestätigen.[107] Zu diesem Zweck wird eine *Trust-service-Status List* (TSL) geführt, die sämtliche vertrauenswürdigen CAs auflistet und diese als *Trusted Service Provider (TSP)* definiert.[108] Diese TSL wird bspw. auf die Hardware der TI (Konnektor und Kartenterminal) heruntergeladen und signalisiert der Hardware, ob ein ausgestelltes Zertifikat gültig ist oder mittlerweile als gesperrt markiert wurde (z.B. wegen Diebstahl/Verlust).

2.3.2 Förderkonzept Medizininformatik

Das *Förderkonzept Medizininformatik* ist ein von 2016 bis 2025 ausgelegtes Projekt des BMBF zur Entwicklung von Lösungen für einrichtungsübergreifenden Datenaustausch im Rahmen von biomedizinischer Forschung und Optimierung der Versorgung von Patienten.[109] Der Schwerpunkt des Projekts liegt auf der Unterstützung individualisierter Behandlungen durch die Verknüpfung von Behandlungsdaten mit Forschungsdaten.[110]

---

104 Vgl. gematik (2018e): 11.

105 Vgl. gematik (2018e): 13.

106 Vgl. gematik (2018e): 20f.

107 Vgl. Schwab (2014): 264. Alternativen zur Bridge-CA wären *Super-Root* und *Web-of-Trust*. Beide wurden aufgrund ihres erhöhten Abstimmungsaufwandes (*Super-Root*) oder Cross-Zertifizierungen (*Web-of-Trust*) verworfen (vgl. Schwab (2014): 263).

108 Vgl. Schwab (2014): 262.

109 Vgl. Bundesministerium für Bildung und Forschung (2015): 9; Gehring/Eulenfeld (2018): e46.

110 Vgl. Bundesministerium für Bildung und Forschung (2015): 10. Für den Nachweis, dass intersektorale Kommunikation mittels IT einen Mehrwert erzeugt, soll jedes an der Förderung teilnehmende Konsortium einen oder mehrere Fallstudien vorstellen, durchführen und anschließend evaluieren, ob die konzipierte intersektorale Datenvernetzung zu einem messbaren Mehrwert in der Versorgung geführt hat. (vgl. Knaup et al. (2018): 303). DIFUTURE nutzt Erkenntnisse bspw. zur Anwendung integrativer Datenanalyse bei der Behandlung von Multipler Sklerose sowie Parkinson und soll neue Ansätze für individualisierte Behandlungen liefern. Gleichzeitig können sich auf diesem Weg neue, allgemeingültige Behandlungsmöglichkeiten ergeben (vgl. Medizininformatik-Initiative (o. J.); Prasser et al. (2018): e63).

Im Förderzeitraum haben sich vier Konsortien durchgesetzt:

1. Data Integration for Future Medicine (DIFUTURE)
2. Heidelberg-Göttingen-Hannover Medizininformatik (HiGHmed)
3. Smart Medical Information Technology for Health Care (SMITH)
4. Medical Informatics in Research and Care in University Medicine (MIRACUM)

Im Rahmen des Förderkonzepts Medizininformatik werden an den in einem Konsortium beteiligten Institutionen Datenintegrationszentren (engl. *Data Integration Center*, DIC) aufgebaut, die die jeweilige Datenschnittstelle bilden und den Austausch von Versorgungs- und Forschungsdaten steuern.[111] Entgegen der vom BMBF kommunizierten Richtlinie, dass Daten nicht in den DIC gespeichert werden, sondern erst bei Bedarf abgerufen werden sollen,[112] werden in der aktuellen Planung der Konsortien DIC als harmonisierter Datenspeicher konzipiert und Patienten- und Forschungsdaten, teils nur bezogen auf die zu behandelnden Fallstudien, regelmäßig von den einzelnen in einer Institution vorgehaltenen Systemen in institutionseigene DICs überführt.[113]

Die Bereitstellung der harmonisierten, forschungskompatiblen Daten wird in den Konsortien unterschiedlich behandelt. *DIFUTURE* setzt bspw. auf eine Portallösung,[114] die Forschende bei Datenanfragen unterstützt und anschließend über eine Plattform abgesicherte, virtualisierte Zugriffe auf Analyseprogramme zur Verfügung stellt.[115] Auch sollen in diesem Rahmen Konzepte des *Distributed Computing* zur Unterstützung der Analysen genutzt werden.[116] Ähnlich geht *SMITH* vor, das den sog. *SMITH Market Place* (SMP) bereitstellt, der alle internen und externen Anfragen entgegennimmt und erst nach erfolgreicher Prüfung Daten bereitstellt.[117] Der SMP wird dabei über den im Fraunhofer-Institut entwickelten *Industrial Data Storage* (IDS) betrieben, der mittels Konnektoren auf alle Inhalte der DICs zugreift und diese anschließend dem

---

111 Vgl. Bundesministerium für Bildung und Forschung (2015): 11. Anders als beim Ansatz der GEMATIK müssen die Konsortien neben der reinen Konzeption einer Architektur auch deren (positiven) Nutzen auf Basis von Fallstudien o.ä. wissenschaftlich belegen. Grund zur Einrichtung von Datenintegrationszentren ist das Problem der fehlenden Interoperabilität zwischen den Einrichtungen (vgl. Bundesministerium für Bildung und Forschung (2015): 6).

112 Vgl. Bundesministerium für Bildung und Forschung (2015): 11. Die vom BMBF genutzte Wortwahl ist allerdings ungenau und ermöglicht somit einen gewissen Handlungsspielraum.

113 Vgl. Prasser et al. (2018): e61; Prokosch et al. (2018): e86; Winter et al. (2018): e97; Phan-Vogtmann et al. (2019): 88.

114 Vgl. Prasser et al. (2018): e62.

115 Vgl. Prasser et al. (2018): e63.

116 Vgl. Prasser et al. (2018): e63.

117 Vgl. Winter et al. (2018): e100-e101. Eine Kerneigenschaft des IDS ist die Dezentralität und föderale Architektur des Systems. Demnach bleiben die zu verarbeitenden Daten in den lokalen Quellsystemen (vgl. Otto et al. (2016): 13).

Forschenden bereitstellt.[118] Auch *MIRACUM* setzt auf föderierte Daten und schafft eine zentrale Anlaufstelle für Forschende mit einem *Central Search Broker*. Dieser kümmert sich um die Beschaffung von Daten und Dokumenten in den angeschlossenen, föderiert organisierten DICs und stellt die Ergebnisse anschließend in aggregierter Form zur Verfügung.[119] *HiGHmed* stellt in diesem Zusammenhang ein zweistufiges System bereit. Zu Beginn formulieren Forschende ihre Forschungsfrage und erhalten darauf basierend eine Rückmeldung über die Anzahl passender Patienten. Die Liste dieser passenden Patienten ist anschließend Grundlage der konkreten Anfrage an den Data Mart Manager, der die notwendigen Daten und Dokumente in einer separaten Instanz bereitstellt.[120]

Die Möglichkeiten des Patienten im Rahmen dieses Projekts, Zugriff auf eigene Daten zu erhalten bzw. Änderungen vorzunehmen oder vornehmen zu lassen, ist beschränkt auf die Erlaubniserteilung zur Datennutzung durch Dritte (*patient consent*) bzw. die Betrachtung der eigenen, bereitgestellten Daten.[121] Daraus ergibt sich, dass die in den DIC vorgehaltenen Informationen denen einer Institutionellen Elektronischen Patientenakte (iEPA) bzw. Registerakte gemäß *Tabelle 2-1* entsprechen.

2.4 Alternativkonzept: Independent Health Record Banks

Die GEMATIK plant mit der Überführung von Daten in die ePA nicht nur eine fallbezogene Informationsversorgung ohne Informationsbruch, sondern auch die lebenslange Vorhaltung dieser Daten, abhängig von der Zustimmung des Patienten.[122] Das MIRACUM-Konsortium äußert sich ähnlich und stellt aufgrund der Einrichtung der DICs eine zumindest virtualisierte Möglichkeit in Aussicht, Gesundheitsdaten lebenslang zu speichern, unabhängig von dem in der jeweiligen Einrichtung zugrundeliegenden System.[123] Ein solcher *Lifetime Health Record* ist per Definition eine Akte,

---

118 Vgl. Winter et al. (2018): e96.

119 Vgl. Prokosch et al. (2018): e87.

120 Vgl. Haarbrandt et al. (2018): e75.

121 Vgl. Haarbrandt et al. (2018): e69-e70; Haarbrandt et al. (2018): e71; Prasser et al. (2018): e64; Prasser et al. (2018): e62; Winter et al. (2018): e100. Während DIFUTURE wenigstens darauf hinweist, dass zumindest ein Patienten-Portal geplant ist, geht MIRACUM in keiner Publikation auf dieses Werkzeug ein und bezieht sich ausschließlich auf die Erlaubniserteilung als Basis für eine Datenzusammenführung.

122 Vgl. Deutscher Bundestag (2018): 9; gematik (2018a).

123 Vgl. Knaup et al. (2018): 303.

> *„[which] aggregates recordings created by all health care enterprises from which the subject of the lifetime record has received medical care throughout his/her life.“*[124]

HAAS schränkt diese Interpretation ein und unterscheidet definitorisch zwischen einer einrichtungsübergreifenden Elektronischen Patientenakte (eEPA), die die *„(..) wichtigsten Daten und Dokumente (…)“*[125] vorhält, und einer Elektronischen Basisdokumentationsakte, die *„nur wenige ausgewählte lebenslang wichtige medizinische Daten, wie Diagnosen, Maßnahmen, Risikofaktoren etc.“*[126] enthält. Grund für die Beschränkung der Daten ist das Prinzip der Datensparsamkeit im Datenschutzrecht, die fordert, dass der (temporäre) Nutzen von Daten und Informationen berücksichtigt werden muss.[127]

In den Überlegungen über den Betrieb von *Lifetime Health Records* diskutiert SHABO die in *Tabelle 2-2* dargestellten potentiellen Betriebsmodelle einer solchen Gesundheitsakte. So können bspw. die in *Kapitel 2.2* dargestellten Initiativen dem *Provider-centric Model* (DICs der BMBF-Konsortien) oder einer Mischform aus *National/Regional-centric Model* (ePA der GEMATIK gem. §291a SGB V) und *Consumer-centric Model* (ePAs des Privatsektors gem. § 68 SGB V) entsprechen.

Tabelle 2-2: Alternativen des Aktenbetriebs (Quelle: Haas (2017): 132 mit Verweis auf Shabo (2006b): 498-501)

Modell	Erläuterung
Provider-centric Model	Informationen bleiben in den dezentralen Systemen, Abruf bei Bedarf, „record on the fly“. Die Informationshoheit und der Zugriff liegen ausschließlich bei den einzelnen Institutionen. Speichernde bzw. verantwortliche Stelle im Sinne des Datenschutzrechtes ist die einzelne Institution.
Consumer-centric Model	Patienten selbst führen ihre Akte bei einem kommerziellen Provider ihrer Wahl und gewähren ihren behandelnden Ärzten, Pflegenden, Therapeuten etc. wahlweise Zugriff. Die Akte liegt bei einem kommerziellen Anbieter, der als Dienstleister für die Datenhaltung von pEPAn am Markt agiert und quasi eine Auftragsdatenverarbeitung für den Patienten durchführt. Genau genommen ist hier speichernde bzw. verantwortliche Stelle der Patient selbst.
National / Regional-centric Model	Aufbau und Betrieb von eEPA-Systemen unterliegen der Kontrolle und Betriebsverantwortung einer regionalen oder nationalen Behörde. Sie ist damit speichernde bzw. verantwortliche Stelle.
Non-centric IHRB Model	Es gibt spezielle neue rechtliche Entitäten, die ausschließlich für den Betrieb von eEPAen verantwortlich sind, die nun als Independent Health Record Banks (IHRB) bezeichnet werden. Sie können als Dienstleister qua Vertrag oder Gesetz für bestimmte bzw. alle Stakeholder gewisse Dienstleistungen erbringen.

[124] Shabo (2006a): 240f.

[125] Haas (2017): 55.

[126] Haas (2017): 55.

[127] Vgl. Haas (2017): 183.

In den in *Tabelle 2-2* genannten Modellen *Provider-centric, Consumer-centric* und *National/Regional-centric* sieht SHABO allerdings Partikularinteressen der jeweiligen Stakeholder, die wiederum zu einem Vertrauensverlust führen und einer freiwilligen Bereitstellung von Gesundheitsdaten durch Patienten bzw. der Nutzung bereitgestellter Daten durch einen Leistungserbringer entsprechend entgegenwirken können.[128] Auf Basis dieser Argumentation werden sogenannte *Independent Health Record Banks* (IHRB) eingeführt (siehe *Tabelle 2-2* zum Thema *Non-centric IHRB Model*), die Daten von Leistungserbringern entkoppeln, in deren Auftrag Daten vorhalten und bei Bedarf bereitstellen sowie Analysen durchführen und Ergebnisse übermitteln.[129]

2.5 Schwächen der Informationsintermediäre in den aktuellen Ansätzen der Gesundheitsdatenvernetzung und Blockchain als alternative Technologie

Mit der durch die GEMATIK kontrollierten ePA[130] und der von den BMBF-Konsortien konzipierten DIC[131] sowie der von SHABO dargestellten IHRB[132] werden die in *Kapitel 2.2* dargestellten Informationsintermediäre beschrieben, die als zwischengeschaltete Dritte Vertrauen in die Aussagekraft bereitgestellter Gesundheitsdaten schaffen sowie eine durch Leistungserbringer oder Patienten kontrollierte Freigabe von Daten ermöglichen.

Doch damit sämtliche Netzwerkteilnehmer Vertrauen in einen Intermediär haben, muss dieser die notwendige Informationssicherheit gewährleisten.[133] In der Literatur finden sich mehrere Arbeiten, die sich konkret mit den Schwachstellen der TI und deren Verbindungskomponenten

---

128 Vgl. Shabo (2006a): 244; Haas (2017): 132.

129 Vgl. Shabo (2006a): 240; Gold/Ball (2007): 45; Shabo (2014): 65. Die Idee der *Health Record Bank* ist auf RAMSAROOP/BALL zurückzuführen, die bereits 2000 eine *Bank of Health* statierten. Diese sollte aber, ähnlich wie HAAS es beschreibt, nur die essenziellen Inhalte enthalten, die den Patienten in die Lage versetzen, an seiner Behandlung teilzuhaben (vgl. Ramsaroop/Ball (2000): 47).

130 Die GEMATIK sammelt durch Nutzung der ePA Daten und Informationen von Patienten zur Bereitstellung und Informationsversorgung der an einer Behandlung beteiligten Ärzte (siehe *Kapitel 2.3.1*). Die BMBF-Konsortien setzen auf unterschiedliche Konzepte, von der Bereitstellung von Rohdaten bis zur Bereitstellung von Ergebnissen von in Auftrag gegebenen Analysen (siehe *Kapitel 2.3.2*).

131 Ein DIC ist ein Intermediär in unterschiedlicher Ausprägung. Einerseits bleiben Daten in einem Klinikum dezentral in den Abteilungen gespeichert und werden erst durch ein DIC zusammengeführt und bereitgestellt. Andererseits werden offene Marktplätze für Forschungsdaten angeboten, sodass Externe auf das jeweilige Klinikum und dessen Daten zugreifen können.

132 Vgl. Shabo (2010): 197. Ergänzend zur reinen Datenhaltung sieht SHABO Datenaggregation, -analyse und schlussendlich deren Bereitstellung ebenfalls als Aufgabe der IHRB (vgl. Shabo (2014): 65).

133 Vgl. Prasser et al. (2018): e58.

auseinandersetzen[134] und bspw. eine einwandfreie Installation der Schnittstelle zwischen lokalem System und dem Verantwortungsbereich des Intermediär voraussetzen.[135] Dass diese Installation eine Schwachstelle darstellt, ist bereits festgestellt.[136] Neben den technischen Schwachstellen bergen Intermediäre grundsätzlich das Risiko des sog. *Misplaced Trust*[137] sowie des Machtmissbrauchs gegenüber anderen Netzwerkteilnehmern.[138]

Diese Umstände untergraben das Vertrauen, das Informationsintermediäre den an einem Markt teilnehmenden Parteien versprechen. In der Forschung hat sich zur Lösung der Intermediationsproblematik bereits ein Fokus in Richtung *Blockchain-Technologie* herausgearbeitet.[139] Dies begründet sich in den Grundvoraussetzungen für den Einsatz dieser Technologie:[140]

i. Notwendigkeit einer gemeinsam genutzten Datenbank
ii. Gewährleistung von Datenintegrität
iii. Ziel ist eine Disintermediation trotz des geforderten Vertrauens zwischen Transaktionsteilnehmern

Zur genaueren Evaluation, ob Blockchain im Gesundheitswesen, genauer in der vernetzten Bereitstellung von Gesundheitsakten, tatsächlich eine passende Technologie ist, können wahlweise das Bewertungsframework von LO ET AL. oder WÜST/GERVAIS herangezogen werden, die beide in Form eines Entscheidungsbaums aufgebaut sind.

LO ET AL. (siehe *Abbildung 2-5)* beziehen sich bereits konkret auf das Gesundheitswesen und setzen für die erfolgreiche Anwendung der Blockchain-Technologie die Bereitschaft des Patienten voraus, seine Patientendaten transparent auf der Blockchain (on-chain) zu speichern. Wenn dem nicht so ist, müssen Daten zumindest im Netzwerk verteilt werden dürfen und die

---

134 Siehe bspw. Huber/Sunyaev/Krcmar (2008), Sunyaev et al. (2010), Sunyaev et al. (2009) und Sunyaev/Leimeister/Krcmar (2010).

135 Vgl. gematik (2018c): 12, 21.

136 Das Primärsystem eines Leistungserbringers (die Datenquelle für Patientendaten) und das Kartenterminal, das mittels der ausgegebenen Karten die Verschlüsselung und Signierung sicherstellt, werden zwar unabhängig voneinander an den Konnektor angeschlossen (siehe *Abbildung 2-4*). Aber bei entsprechender Konfiguration erlaubt der Konnektor, dass alle Kartenterminals im Netzwerk eines Leistungserbringers automatisch akzeptiert werden, sodass auch potenziell manipulierte Geräte zugelassen und Prozesse kompromittiert werden (vgl. Sunyaev et al. (2010): 231).

137 Vgl. Brennan-Marquez (2015): 623-629. Beschrieben wird, dass mehrere Gerichte (in den USA) davon ausgehen, dass nicht von einem uneingeschränkten Vertrauen auf Privatheit (abgeleitet aus dem vierten Zusatzartikel der Verfassung der Vereinigten Staaten) gegenüber Intermediären ausgegangen werden kann, wenn bspw. Strafverfolgungsorgane oder Regierungen ein Interesse an den vertraulich zu behandelnden Informationen haben könnten (ebenfalls beschrieben in SARGSYAN (2016): 2). Dennoch wird hier darauf hingewiesen, dass durch den Verzicht auf Intermediäre nur eine Instanz weggelassen wird. *Misplaced Trust* kann weiterhin direkt bei den Leistungserbringern entstehen.

138 Vgl. Balkin (2016): 1216f.

139 Vgl. Esmaeilzadeh/Mirzaei (2019): 5.

140 Vgl. Ploom (2016): 131; Rodrigues/Bocek/Stiller (2018): 169f.

Blockchain die Verwaltung dieser Daten übernehmen. In diesem Zusammenhang wird *MedRec*[141] erwähnt, das keine Rohdaten sondern Verweise auf lokal gespeicherte Patientendaten auf der Blockchain verwaltet.[142] Die Autoren kommen zu dem Schluss, dass die Blockchain-Technologie keine direkten Vorteile gegenüber dem Einsatz einer regulären Datenbank bietet, sehen aber Potentiale im Zusammenhang mit Identitätsmanagement.[143]

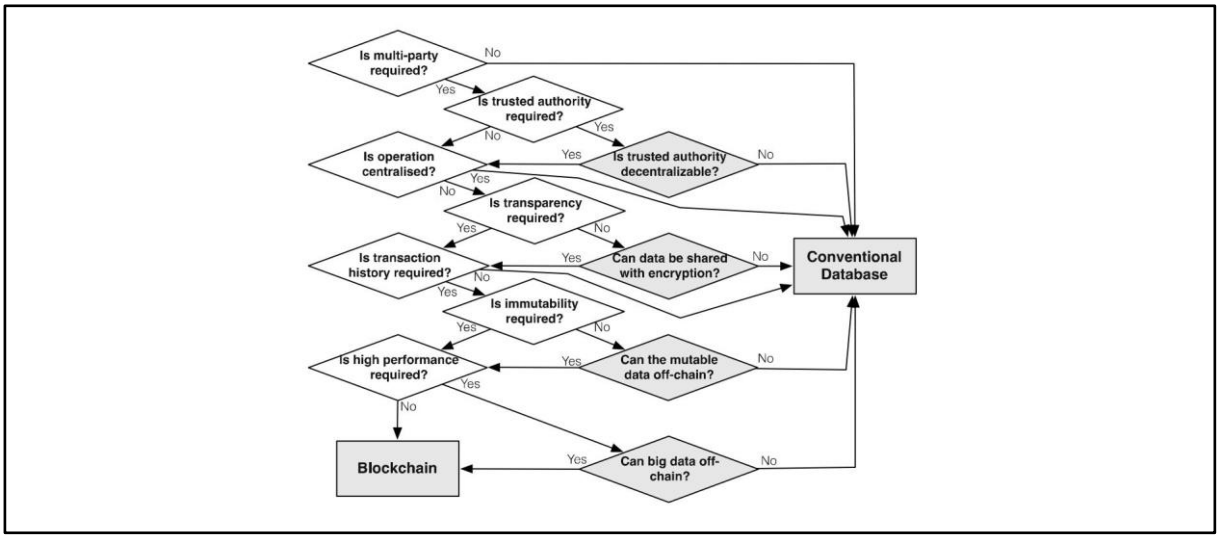


Abbildung 2-5: Bewertungsframework I (Quelle: Lo et al. (2017): 159)

Das von WÜST/GERVAIS entwickelte Bewertungsframework (siehe *Abbildung 2-6*) berücksichtigt nicht explizit die Anwendung der Blockchain im Gesundheitswesen. Unter der Annahme, dass die ersten beiden Fragen mit *yes* beantwortet werden können und eine *Trusted Third Party (TTP)*[144] weder in der Konzeption der GEMATIK noch der BMBF-Konsortien als *dauerhaft verfügbar* definiert wird,[145] wird der Schluss gezogen, dass Blockchain eine potentielle Alternativ-Technologie darstellt.

141 Details sind nachzulesen bei Azaria et al. (2016).

142 Vgl. Lo et al. (2017): 160.

143 Vgl. Lo et al. (2017): 161.

144 Eine *Trusted Third Party* ist eine Drittpartei, deren Aufgabe es ist, die Informationssicherheit in einem Netzwerk zu gewährleisten (vgl. Polemi (1998): 52).

145 Die Annahme wird mit den bereits genannten Sicherheitsrisiken der Konzeptionen begründet. Unter Berücksichtigung des Umstands, dass die gematik als Bridge-CA agiert, kann im Grunde von einer always online TTP ausgegangen werden, doch relativiert sich diese Einschätzung unter Einbezug der dargestellten Probleme (z.B. Offline-Modus in den Endgeräten ohne Aktualisierung der lokalen *Trusted Service Lists*).

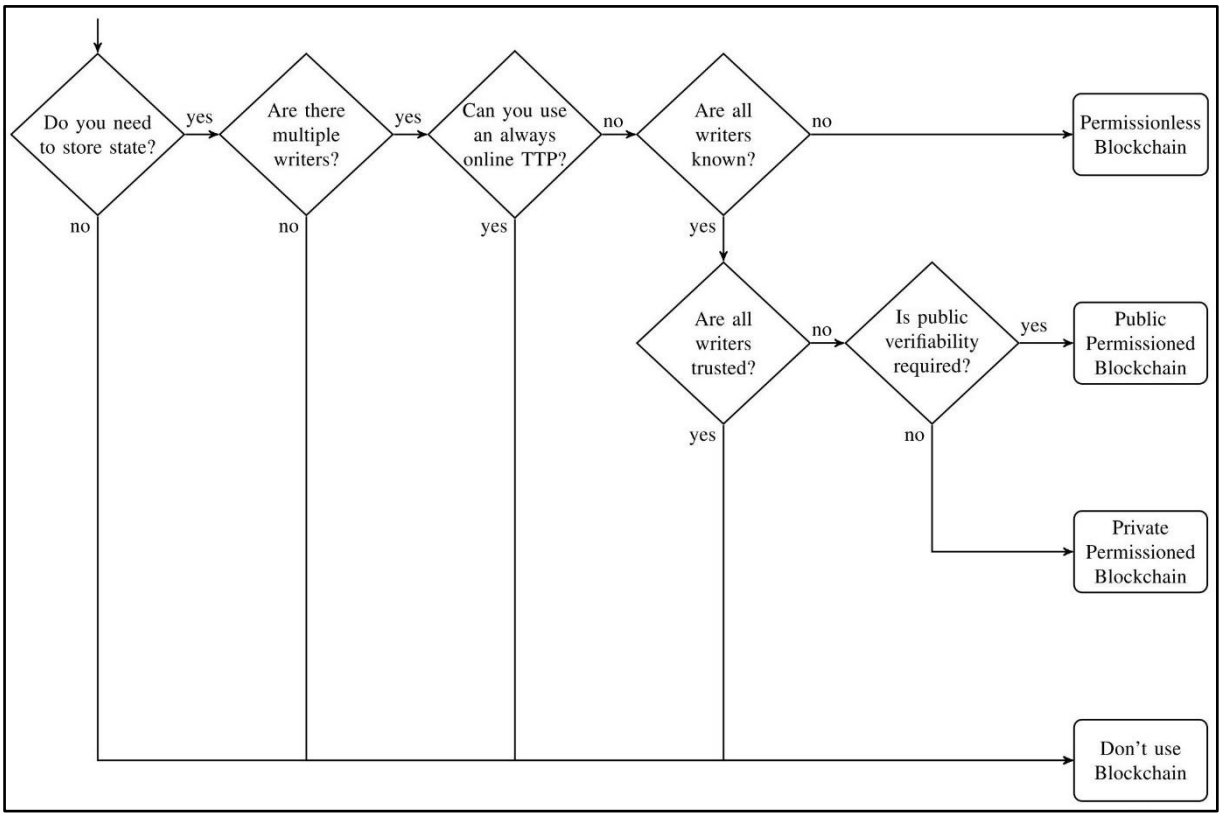


Abbildung 2-6: Bewertungsframework II (Quelle: Wüst/Gervais (2018): 47)

Auch die wissenschaftliche Literatur identifiziert eine zunehmende Relevanz von Blockchain im Gesundheitswesen. HÖLBL ET AL. kommen im Rahmen eines durchgeführten *Literature Reviews* zu dem Schluss, dass sich die Anwendung der Blockchain im Gesundheitswesen insbesondere auf die Themen Datenvernetzung, Gesundheitsakten und Zugriffsmanagement verteilt.[146]

[146] Vgl. Hölbl et al. (2018): 474.

3 Blockchain

3.1 Historische und allgemeine Grundlage der Blockchain-Technologie

Historisch betrachtet ist die Idee der Blockchain auf die Anforderung zurückzuführen, Dokumente chronologisch zu verifizieren. Dabei wird von HABER/STORNETTA unterstellt, dass die Nutzung eines Hashs[147] oder einer digitalen Signatur allein nicht ausreicht, einen zuverlässigen Zeitstempel zu gewährleisten.[148] In ihrer Arbeit wird ein kombinierter, hash-basierter Ansatz entwickelt, der verhindert, dass Änderungen an Dokumenten vorgenommen und Dokumente wiederholt gestempelt werden können.[149]

Das Risiko bei der ausschließlichen Nutzung digitaler Signaturen ist bereits in der Unterscheidung zwischen *symmetrischen* und *asymmetrischen* Verschlüsselungsverfahren erkennbar. *Symmetrische* Verschlüsselungsverfahren haben den Nachteil, dass sowohl Sender als auch Empfänger aufgrund der Nutzung eines einzelnen Schlüssels[150] Änderungen an digital signierten Daten vornehmen können, ohne dass nachvollziehbar ist, welche der beiden Seiten die Änderung vorgenommen hat.[151] Sie dient folglich einzig dem vertraulichen Transport einer Nachricht, jedoch nicht der Wahrung von Integrität. *Asymmetrische* Verschlüsselungsverfahren erzeugen hingegen ein Schlüsselpaar aus privatem und öffentlichem Schlüsseln.[152] Im regulären asymmetrischen Verschlüsselungsverfahren verschlüsselt *Alice* ihre Nachricht (*m)* mit dem Öffentlichen Schlüssel (*$ÖFF_{Bob}$)* von *Bob*. Dieser kann die Nachricht mit seinem Privaten Schlüssel *$PRIV_{Bob}$* wieder entschlüsseln. Digitale Signaturen drehen das reguläre Verschlüsselungs-Verfahren um: *Alice* nutzt das Entschlüsselungsverfahren *E* um *m* zu Beginn mit *$PRIV_{Alice}$* zu entschlüsseln und somit ein unlesbares Chiffrat *$E_{Alice}(m)$* zu erzeugen. Dieses Chiffrat wird mit *$ÖFF_{Bob}$* verschlüsselt (*V*) und an *B* gesendet (*$V_{Bob}(E_{Alice}(m))$*). Dieser entschlüsselt die Sendung mit seinem *$PRIV_{Bob}$* und erhält $E_{Alice}(m)$. Um nun auf *m* schließen zu können, wird der *$ÖFF_{Alice}$* dazu genutzt, Nachricht *m* mittels Verschlüsselungsverfahren wieder lesbar zu machen und

147 Ein Hash, genauer ein Hash-Wert, ist eine mittels Hash-Funktion ermittelte individuelle Zeichenfolge fester Länge eines bestimmten Ausgangswerts. Für den Fall, dass die Länge des Hashs zu kurz gewählt wurde, kann es zu Kollisionen kommen. (Vgl. Mahlmann/Schindelhauer (2007): 64f.).

148 Vgl. Haber/Stornetta (1991): 103.

149 Vgl. Haber/Stornetta (1991): 99f.

150 Vgl. Wobst (1998): 150.

151 Vgl. Wobst (1998): 260f.

152 Vgl. Spitz/Pramateftakis/Swoboda (2011): 109.

gleichzeitig die *Signatur von Alice* zu bestätigen.[153] Dieses Verfahren ist jedoch nur so lange sicher, wie der private Schlüssel einem Angreifer nicht bekannt ist.

Als Antwort auf die beschriebene Problematik kombinieren HABER/STORNETTA zwei Verfahren miteinander: *Linking* und *Distributed Trust*.[154] Unter *Linking* wird die Verkettung von bestehenden Zeitstempeln mit neuen Zeitstempeln verstanden,[155] sodass eine Manipulation erschwert wird.[156] *Distributed Trust* verlagert die Verantwortung für den Nachweis der Korrektheit von Zeitstempeln von einer zentralen Instanz auf alle Teilnehmer in einem Netzwerk und impliziert damit, dass sich im Falle abweichender Zeitstempel-Werte ein komplettes Netzwerk irren müsste.[157]

Dieses Konzept greift NAKAMOTO[158] auf und veröffentlicht, unter dem Eindruck der globalen Finanz- und Staatenkrise 2008/2009, eine Konzeptbeschreibung über eine neue elektronische Währung, den Bitcoin, der das Vertrauen, das Banken im allgemeinen Finanztransaktionsverkehr entgegengebracht wird, auf alle Teilnehmer eines Peer-to-Peer-Netzwerks (P2P-Netzwerks)[159] verteilt.[160] Statt Transaktionsdaten in der Hoheit einer zentralen Datenbank zu belas-

---

153 Vgl. Salomaa (1996): 73; Wobst (1998): 261; Spitz/Pramateftakis/Swoboda (2011): 28. WOBST greift ergänzend das Problem der uneinheitlichen Nutzung der Terminologie des *Ver-* und *Entschlüsselns* auf (vgl. Wobst (1998): 261). Während SALOMAA darauf hinweist, dass Ver- und Entschlüsselung invers genutzt werden, unterlassen es SPITZ/PRAMATEFTAKIS/SWOBODA. Aufgrund dessen, dass Private Schlüssel grundsätzlich zur Entschlüsselung und Öffentliche Schlüssel zur Verschlüsselung genutzt werden, muss auf die entsprechende Begriffsnutzung geachtet werden, denn beide nutzen in der Regel unterschiedliche mathematische Operationen. Gemäß WOBST wäre einzig bei einer RSA-Verschlüsselung die oben kritisierte Verwendung der Begriffe angemessen (vgl. Wobst (1998): 261).

154 Vgl. Haber/Stornetta (1991): 103.

155 Vgl. Haber/Stornetta (1991): 103-105.

156 Vgl. Haber/Stornetta (1991): 103.

157 Vgl. Haber/Stornetta (1991): 105f; Massias/Serret Avila/Quisquater (1999): 79.

158 Es ist unklar, ob sich hinter dem Pseudonym SATOSHI NAKAMOTO eine einzelne Person oder eine Gruppierung verbirgt. In der weiteren Betrachtung wird der Lesbarkeit halber davon ausgegangen, dass es sich um eine Person handelt, und das generische (maskuline) Personalpronomen genutzt.

159 Ein P2P-Netzwerk ist eine *„[.] distributed network architecture […], if the participants share a part of their own hardware resources (processing power, storage capacity, network link capacity, printers, ...). These shared resources are necessary to provide the Service and content offered by the network (e.g. file sharing or shared workspaces for collaboration): They are accessible by other peers directly, without passing intermediary entities. The participants of such a network are thus resource (Service and content) providers as well as resource (Service and content) requestors (Servent-concept).”* (Schollmeier (2001): 101). Gleichzeitig ist dabei relevant, dass kein *“[…] single, arbitrary chosen Terminal Entity can be removed from the network without having the network suffering any loss of network service.”* (Schollmeier (2001): 102).

160 Vgl. Nakamoto (2008): 1. Statt einer tatsächlichen Fiskalwährung werden sog. Bitcoins als Geldeinheit genutzt und stellen Registereinträge dar, die den Besitz der jeweiligen Einheit repräsentieren (vgl. Berentsen/Schär (2017): 49).

sen, werden Kopien verteilt gespeichert. Damit weicht er vom klassischen Client/Server-Konzept[161] ab und hält Ressourcen in jedem einzelnen Knoten vor, statt diese aufzuteilen.[162] *Abbildung 3-1* stellt, beschrieben als *Distributed networks (c)*, die Struktur von P2P-Netzwerken grafisch dar.

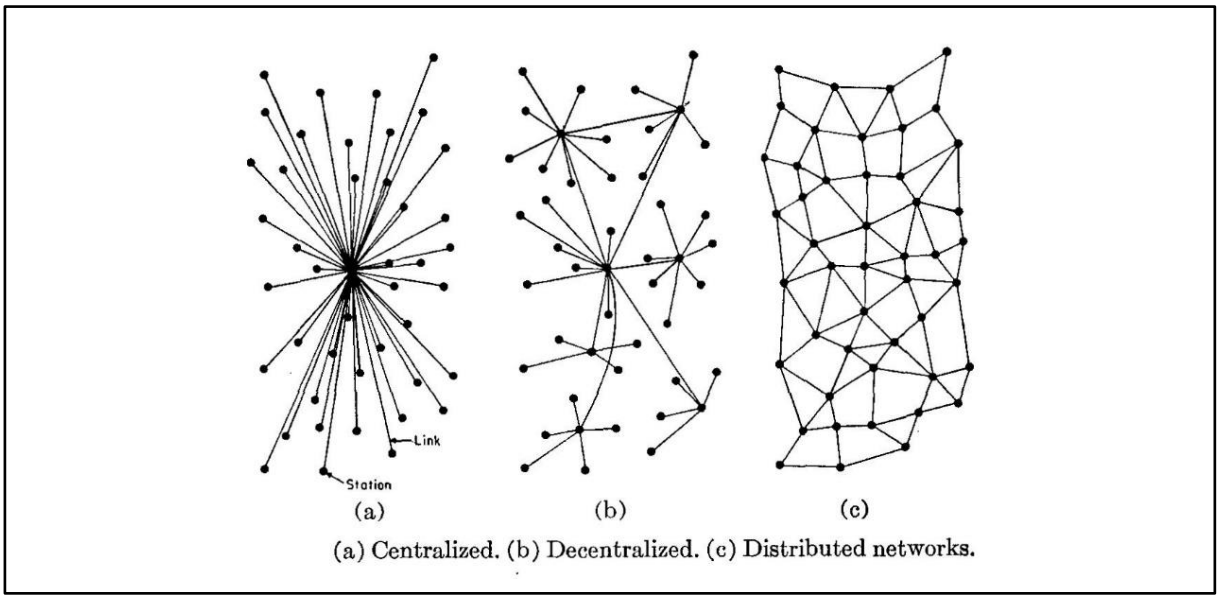


Abbildung 3-1: Netzwerktypen[163]
(Quelle: Baran (1964): 1)

[161] *„A Client/Server network is a distributed network which consists of one higher performance system, the Server, and several mostly lower performance systems, the Clients. The Server is the central registering unit as well as the only provider of content and service. A Client only requests content or the execution of services, without sharing any of its own resources.“* (Schollmeier (2001): 102).

[162] Vgl. Baran (1964): 1; Schollmeier (2001): 102.

[163] *Centralized* und *Distributed Networks* sind verbreitete Topologien. *Decentralized* stellt einen hierarchisch orientierten Mix beider Topologien dar, der zumeist in Kommunikationsnetzwerken genutzt wird (vgl. Baran (1964): 1). Es wird darauf hingewiesen, dass im Zusammenhang mit Blockchain in der Literatur gerne von einem dezentralen Netzwerk gesprochen wird, obwohl es sich in der Urform um verteilte Netzwerke (*Distributed Networks*) handelt.

3.2 Grundstruktur und Funktionsweise der Blockchain

3.2.1 Blockchain-System und Nodes

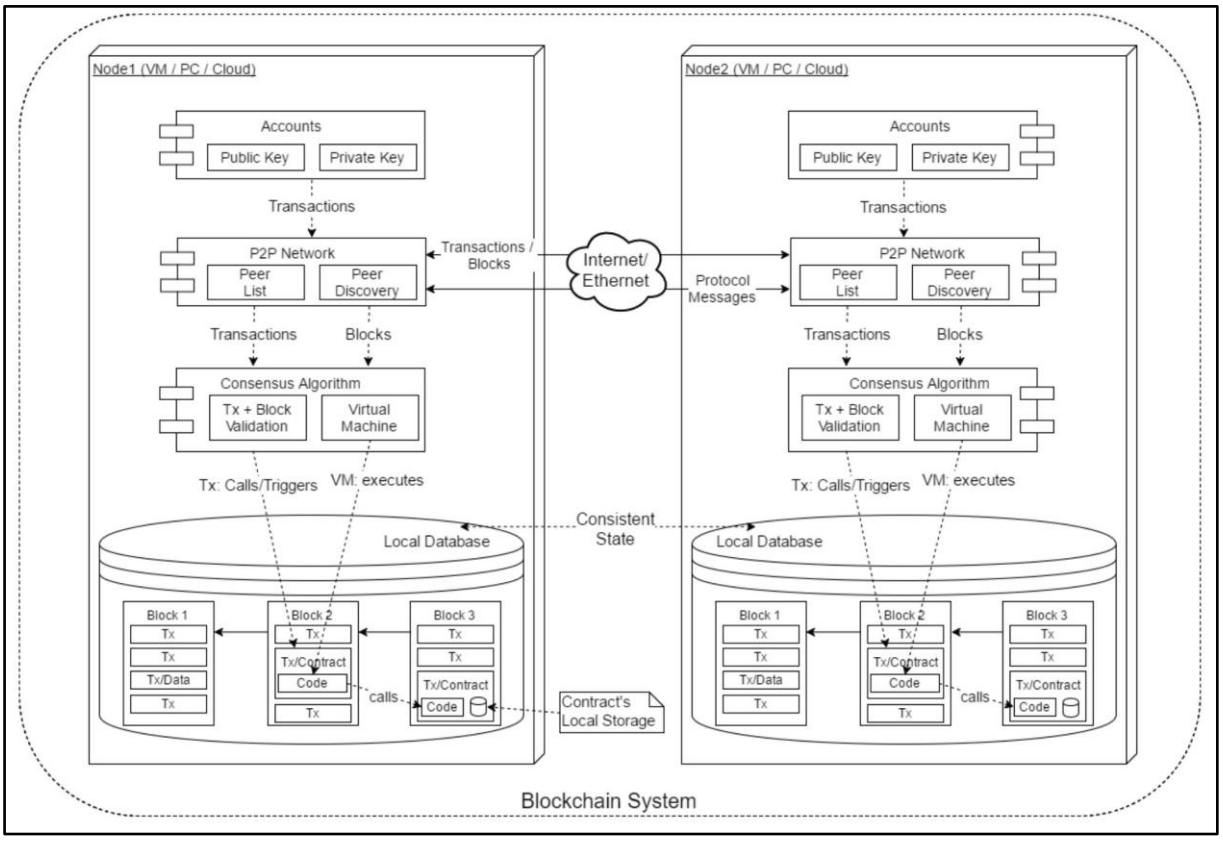


Abbildung 3-2: Konzept eines Blockchain-Systems (Quelle: Glaser (2017): 1546)

Jeder Teilnehmer an einer Blockchain ist im Netzwerk ein aktiver Knoten (engl. *Node*). *Abbildung 3-2* beschreibt den Aufbau eines Blockchain-Systems unter Darstellung zweier Nodes und ihrer jeweiligen Ausprägungen. *Nodes* unterscheiden sich bezüglich der wahrzunehmenden Aufgaben und werden in *Full-* und *Light-Nodes* unterschieden. *Full-Nodes* übernehmen die Prüfung der Validität von Transaktionen, die ihnen ihre direkten Nachbarn im Netzwerk zusenden, und leiten diese anschließend so lange zur erneuten Validierung weiter, bis eine Transaktion dem gesamten Netzwerk bekannt ist.[164] *Light-Nodes* hingegen übernehmen keine Validierungsaufgaben, sondern beschränken sich allein auf die Verwendung der Infrastruktur zum eigenen Nutzen, z.B. Bitcoin-Transfer und -Empfang.[165] Die tatsächliche Übernahme von Transaktionen in Blöcke wird von *Minern* übernommen.[166]

[164] Vgl. Sixt (2017): 39; Vora et al. (2018): 978; Bussac (2019): 65.

[165] Vgl. Bussac (2019): 65. Obwohl es diese Unterscheidung gibt, ist es technisch grundsätzlich möglich, dass jeder *Node* jede der genannten Aufgaben übernimmt. (vgl. Bussac (2019): 66).

[166] Vgl. Bussac (2019): 66.

3.2.2 Transaktionen und Blöcke

Transaktionen aktualisieren den Inhalt einer Blockchain und bestehen aus *Input* und *Output*. In der Bitcoin-Blockchain enthält der Output einer Transaktion die Empfängeradresse[167] und die Menge an zu übertragenden Einheiten, während der Input sämtliche Informationen zu vorherigen Transaktionen bereitstellt und bspw. ein vorhandenes Guthaben ausweist.[168] Wenn *Alice* und *Bob* Bitcoin übertragen möchten, wird diese Transaktions-Nachricht (In- und Output) mit dem öffentlichen Schüssel ($ÖFF_{Bob}$)verschlüsselt und zusammen mit dem Hash der vorherigen Transaktion mittels $PRIV_{Alice}$ digital signiert (siehe *Abbildung 3-3*). Dieses Verfahren weist nach, dass *Alice* im Besitz des notwendigen Inputs war, und übergibt *Bob* die Verfügungsgewalt über die übertragenen Einheiten, da nur *Bob* die Transaktion mit $PRIV_{Bob}$ entschlüsseln kann.[169]

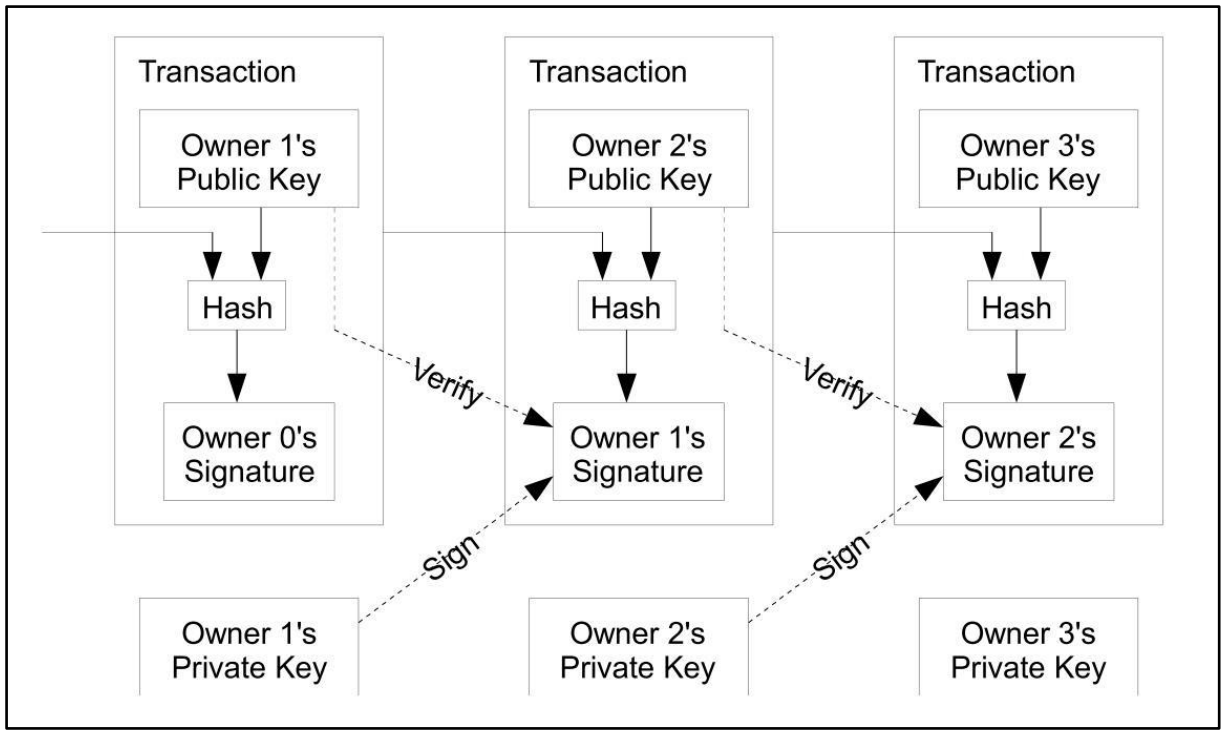


Abbildung 3-3: Bitcoin Transaktionen eines Bitcoins von Besitzer n zu Besitzer n+1[170]
(Quelle: Nakamoto (2008): 2)

[167] Die Empfangsadresse wird unter Anwendung kryptographischer Verfahren aus dem öffentlichen Schlüssel ($ÖFF_{Bob}$) des Empfängers generiert und als Hash dargestellt (vgl. Franco (2014): 75).

[168] Vgl. Franco (2014): 78; Berentsen/Schär (2017): 169f.

[169] Vgl. Brühl (2017): 136; Sixt (2017): 37. Aufgrund dieser Verkettung digitaler Signaturen spricht NAKAMOTO auch von der *„chain of digital signatures"* (Nakamoto (2008): 2).

[170] In dieser Grafik ist bspw. Alice *Owner 1* und Bob *Owner 2*.

Transaktionen werden in Blöcken zusammengefasst. Ein Block besteht aus allen neuen, durch das Netzwerk als valide eingestuften Transaktionen, der *Coinbase*[171], einer *Nonce*[172] sowie dem *Hash* des vorherigen Blocks.[173] Durch die Verknüpfung des neuen Blocks mit dem Hash des vorangegangenen Blocks entsteht die eigentliche Blockchain.[174] Die Berechnung des Blocks bzw. dessen Hash-Werts wird *Mining* genannt, das sich wiederum an Konsensprotokollen orientiert und schlussendlich den Block in die Blockchain überführt.

3.2.3 Konsensprotokolle

Ein *Konsens* ist zur Wahrung der Stabilität und zur Vermeidung von Falschinformationen in verteilten Systemen notwendig, denn je mehr Nodes existieren, desto eher können falsche Informationen bzw. Blöcke mit fehlerhaften Transkationen verteilt werden.[175] Nach der Berechnung eines neuen Blocks wird dieser über das Netzwerk verteilt und dessen Korrektheit geprüft.[176] Abhängig von der Größe des Netzwerks kommt es vor, dass mehrere Miner gleichzeitig einen neuen Block berechnen und verteilen. In diesem Fall entstehen mindestens zwei Stränge einer Blockchain, eine sogenannte *Fork* bzw. *Secondary Chain*.[177] Diese nutzen wiederum andere Miner, um ihre eigenen Blöcke der ihnen bekannten (Fork-)Blockchain anzuhängen. Für diesen Fall wird einzig die Blockchain weitergeführt, die in der Zwischenzeit die meisten neuen Blöcke angehängt hat. Sämtliche Blöcke auf Basis der *Secondary Chain* werden vom Netzwerk nicht mehr akzeptiert und die enthaltenen Transaktionen wieder zur erneuten Validierung freigegeben.[178] Zur Reduzierung von *Secondary Chains* sowie zur Vermeidung fehlerhafter Blöcke existieren Konsensprotokolle, deren Aufgabe es ist, die Sicherheit im Netzwerk aufrecht zu halten. Einen Auszug möglicher Protokolle zeigt die folgende Liste:[179]

---

171 Die *Coinbase* ist eine Transaktion, deren Input keinem Output einer vorangegangenen Transaktion zugewiesen werden kann. Dieser Teil eines Blocks spiegelt die Mining-Entlohnung wieder und enthält ebenfalls die vom Sender einer Transaktion bereitgestellten Gebühren (vgl. Franco (2014): 106f; Antonopoulos (2015): 176; Bussac (2019): 66).

172 Eine *Nonce* ist eine Zufallszahl, die im Mining gefunden werden muss, um die durch das Konsensprotokoll definierte Anforderung zu erfüllen (vgl. Xia et al. (2017b): 47; Agbo/Mahmoud (2019): 4). Für den Bitcoin muss bspw. abhängig vom Schwierigkeitsgrad eine gewisse Anzahl Nullen dem Hash vorangestellt sein.

173 Vgl. Franco (2014): 105. In den Anfängen der Bitcoin-Blockchain wurden zur zusätzlichen Absicherung des Netzwerks auch Blöcke erzeugt, die keine Transaktionen enthielten (vgl. Franco (2014): 107).

174 Vgl. Franco (2014): 105. Der erste Block einer Blockchain wird *genesis block* genannt und der jeweils vorangegangene Block wird als *parent block* bezeichnet (vgl. Franco (2014): 108).

175 Vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 44.

176 Vgl. Antonopoulos (2015): 200.

177 Vgl. Antonopoulos (2015): 203.

178 Vgl. Antonopoulos (2015): 203-206.

179 Vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 45. Diese Liste ist nicht abschließend, da abhängig von der gewählten Blockchain-Technologie und aufgrund des OpenSource-Charakters der Technologie unterschiedliche Variationen der hier genannten Konsensprotokolle sowie völlig neue Protokolle möglich sind.

i. Byzantine-Agreement-Algorithmus *(BA)*[180],
ii. Federated Byzantine Agreement *(FBA)*,
iii. Proof-of-Work *(PoW)*,
iv. Proof-of-Stake *(PoS)*,
v. Proof-of-Burn *(PoB)*.

Byzantine-Agreement-Algorithmus (i) wird bereits von LAMPORT/SHOSTAK/PEASE (1982) vorgestellt und beschreibt auf abstrakte Art, Vertrauen in Computersysteme zu garantieren. Grundsätzlich wird von fehlerhaftem Verhalten einzelner Knoten ausgegangen.[181] Bis zu einem Drittel der Knoten in einem Netzwerk dürfen fehlerhaft sein. Jeder Knoten prüft alle Transaktionen, deren Validität anschließend im Mehrheitsverfahren bestätigt wird.[182]

Federated Byzantine Agreement (ii) erweitert die Möglichkeiten des BA und unterstützt die Konsensfindung zwischen unbekannten Knoten durch die Aufteilung des gesamten Netzwerks in Gruppen, denen sich Knoten frei zuordnen können. Diese Menge an Knoten wird *Quorum* genannt, die erneut in *Quorum Slices* unterteilt werden und eine Menge an Knoten darstellen, die einen einzelnen Knoten von der Validität des Konsenses überzeugen.[183]

Das **Proof-of-Work** (iii) fordert die Lösung einer mathematischen Aufgabe[184] unter Anwendung der *partial hash inversion*, die auf BACK[185] zurückzuführen ist. Der in der Bitcoin-Blockchain genutzte PoW-Konsens sieht vor, dass dem zu errechnenden Hash eines Blocks eine bestimmte Anzahl an Nullen vorangestellt werden. Der Schwierigkeitsgrad dieser Aufgabe wird durch die Vorgabe, zusätzliche Nullen voranzustellen, erhöht. Die in jedem Block enthaltene *Nonce* dient zur Ermittlung des Hashs unter Berücksichtigung des Schwierigkeitsgrades, denn erst die Variation der Nonce bei gleichbleibendem Inhalt der Transaktionen verändert auch den Hash.[186]

Proof-of-Stake (iv) berücksichtigt im Gegensatz zum PoW nicht die Leistung eines Rechners, die ein Miner zum Lösen seiner Aufgabe vorhält, sondern ausschließlich den Besitz einer gewissen Menge der im Netzwerk relevanten digitalen Werteinheit. Je höher dieser Besitz ist,

---

180 Der hier verwendete Begriff wurde der Quelle entnommen. Es existiert kein Unterschied zwischen dem hier gewählten Begriff *Byzantine-Agreement-Algorithmus* und dem in *Kapitel 6.5.2* genutzten Begriff *Byzantine Fault Tolerant*.

181 Vgl. Lamport/Shostak/Pease (1982): 382.

182 Vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 45.

183 Vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 45f.

184 Vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 46.

185 Obwohl NAKAMOTO und FRANCO auf Back (2002) verweisen, wurde das Konzept bereits von Back (1997) beschrieben.

186 Vgl. Franco (2014): 103f.

desto stärker ist dessen Macht, neue Blöcke im Netzwerk freizugeben. Zur Vermeidung von Fehlanreizen fallen im PoS Transaktionsgebühren an, doch werden diese nicht dem Miner gutgeschrieben, sondern durch Übertragen an eine spezielle Adresse ohne Zugriffsmöglichkeit vernichtet.[187]

Ein ähnliches Vorgehen findet sich bei **Proof-of-Burn** (v), denn zum Mining von Blöcken müssen *Coins*[188] entrichtet werden, statt diese durch Mining zu verdienen. Auch in diesem Fall wird eine Zieladresse ohne Zugriffsrecht genutzt, sodass die übertragenen Coins verbrannt bzw. vernichtet werden. Ein fehlerhaftes Verhalten eines Netzwerkteilnehmers führt grundsätzlich zu einem Verlust.[189]

3.2.4 Blockchain-Taxonomy

Abgesehen von der Unterschiedlichkeit der Konsensprotokolle, unterscheiden sich Blockchains auch in der Form, wie dem Netzwerk beigetreten werden kann und wie eingesetzte Miner (Rechenknoten) organisiert werden. Der Zugang zum Netzwerk unterscheidet sich wiederum zwischen *Öffentlicher Blockchain (engl. Public Blockchain)* und *Privater Blockchain (engl. Private Blockchain)*.[190] Die Wahl der Rechenknoten für Mining und Validierung differenziert hingegen zwischen *Permissioned* und *Unpermissioned bzw. Permissionless*.[191] In der Regel werden in der Literatur einzig die Bezeichnungen *Public* und *Private* genutzt. Die Literatur unterstellt dabei in der Regel die Anwendung der Standard-Kombinationen *Public-Permissionless* sowie *Private-Permissioned*. *Abbildung 3-4* beschreibt sämtliche Kombinationsmöglichkeiten in Form einer Taxonomie-Matrix.

---

187 Vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 46. Im PoS-Konsensprotokoll wird die Erzeugung von Blöcken *Minting* genannt (vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 46).

188 *Coins* werden in der Literatur teils synonym mit dem Begriff *Token* genutzt (erkennbar bei Swan (2015): 73; Sixt (2017): 9), obwohl beide Begriffe unterschiedliche Konzepte beschreiben. *Coins* sind tatsächliche Währungseinheiten bzw. in Fiskalwährung tauschbare Werte. Token hingegen werden nicht als Währung, sondern als Einsatz zur Inanspruchnahme von Dienstleistungen eingesetzt. Dennoch existieren *Coins*, die gleichzeitig als Token fungieren. So kann bspw. Ether von Ethereum als Geldeinheit zur Bezahlung (*Coin*) sowie als Einsatz für Mining (*Token*) genutzt werden. (Vgl. Bussac (2019): 212f.).

189 Vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 47. PoB und PoS reduzieren den Energiebedarf beim *Mining*, ermöglichen durch ihre Konstruktion jedoch auch *Forking*, sodass Coins mehrfach ausgegeben werden können (vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 46f.).

190 Vgl. Burgwinkel (2016): 34f. Der Autor nennt überdies die Variante der *Konsortial-Blockchain (engl. Consortium Blockchain)*.

191 Vgl. Burgwinkel (2016): 35. *Unpermissioned* wird in der Literatur teilweise auch als *Permissionless* bezeichnet. In der folgenden Ausarbeitung wird der Begriff *Permissionless* genutzt.

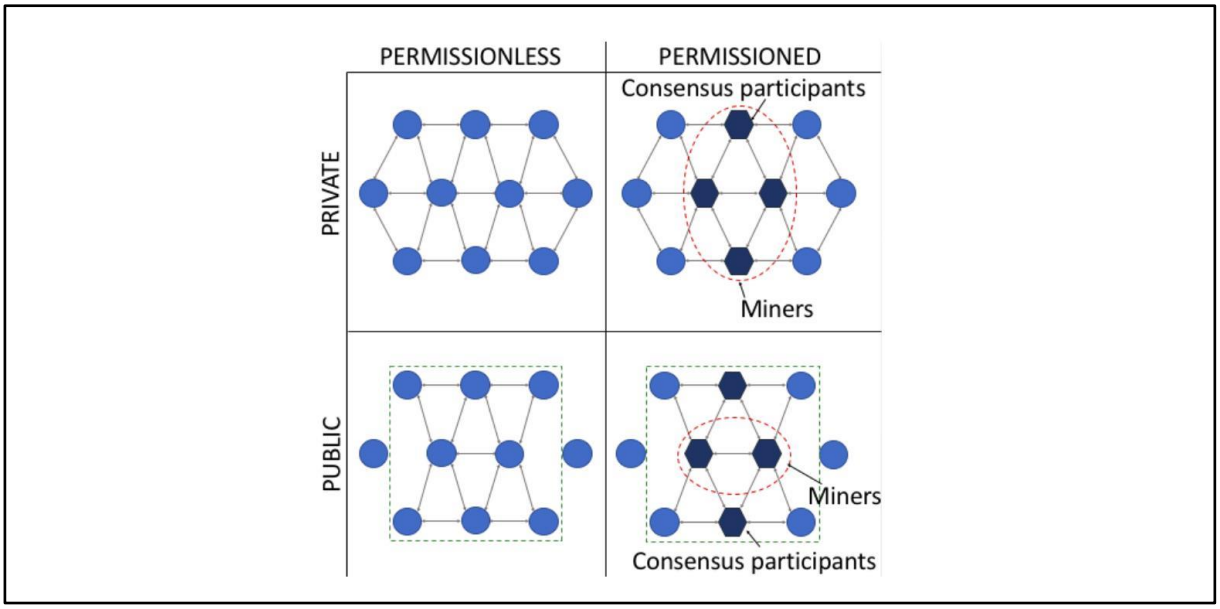


Abbildung 3-4: Blockchain-Taxonomy-Matrix (Quelle: Oliveira et al. (2019): 182)

Public-Permissionless-Blockchains können sich beliebige Nutzer ohne vorherige Kontrolle anschließen, Transaktionen validieren, auf diese zugreifen sowie neue Blöcke erstellen.[192]

Public-Permissioned-Blockchains können von jedem beliebigen Teilnehmer betrachtet werden, doch nur bestimmte Teilnehmer können die Validierung übernehmen, wovon ein noch kleinerer Kreis Mining betreibt.[193]

Private-Permissioned-Blockchains werden innerhalb einer fixierten Umgebung betrieben, Teilnehmer sind bekannt und zur Validierung von Transaktionen sowie Mining neuer Blöcke werden von der Organisation definierte Knoten genutzt.[194]

Private-Permissionless-Blockchains beschreibt eine spezielle Form der privaten Blockchain. Der Zugang ist nicht grundsätzlich gesperrt, sondern durch eine Registrierung kontrolliert. Validierung und Mining wird im Vergleich zu herkömmlichen privaten Blockchains nicht von vordefinierten Knoten durchführt, sondern allen Netzwerkteilnehmern erlaubt.[195]

---

[192] Vgl. Burgwinkel (2016): 48; Merz (2016): 57; Baumann et al. (2017): 11; Pohlmann (2018): 561; Swan (2018): 123f; Wüst/Gervais (2018): 45f; Hussien et al. (2019): 320.4; Klebsch/Hallensleben/Kosslers (2019): 6; Oliveira et al. (2019): 182.

[193] Vgl. Baumann et al. (2017): 18; Pohlmann (2018): 562; Klebsch/Hallensleben/Kosslers (2019): 6; Oliveira et al. (2019): 182.

[194] Vgl. Burgwinkel (2016): 48; Merz (2016): 57; Baumann et al. (2017): 15; Pohlmann (2018): 561f; Swan (2018): 124; Hussien et al. (2019): 320.4–5; Klebsch/Hallensleben/Kosslers (2019): 7; Oliveira et al. (2019): 182.

[195] Vgl. Baumann et al. (2017): 14f; Pohlmann (2018): 561; Klebsch/Hallensleben/Kosslers (2019): 7; Oliveira et al. (2019): 182.

Ergänzend zu dieser Taxonomy hat sich mit der sog. *Konsortial Blockchain* (*engl. Consortium Blockchain*) eine hybride Blockchain-Variante entwickelt.[196] Ein Netzwerk bleibt zwar privat, ist jedoch nicht mehr auf eine einzige geschlossene Gruppe beschränkt. Stattdessen schließen sich mehrere Gruppen zu einem Konsortium zusammen und verteilen die Validierung von Transaktionen und die Berechnung der Blöcke auf eine Auswahl der am Konsortium beteiligten Knoten.[197] *Abbildung 3-5* verdeutlicht die Unterschiede zwischen *Public*, *Private* und *Konsortial*.

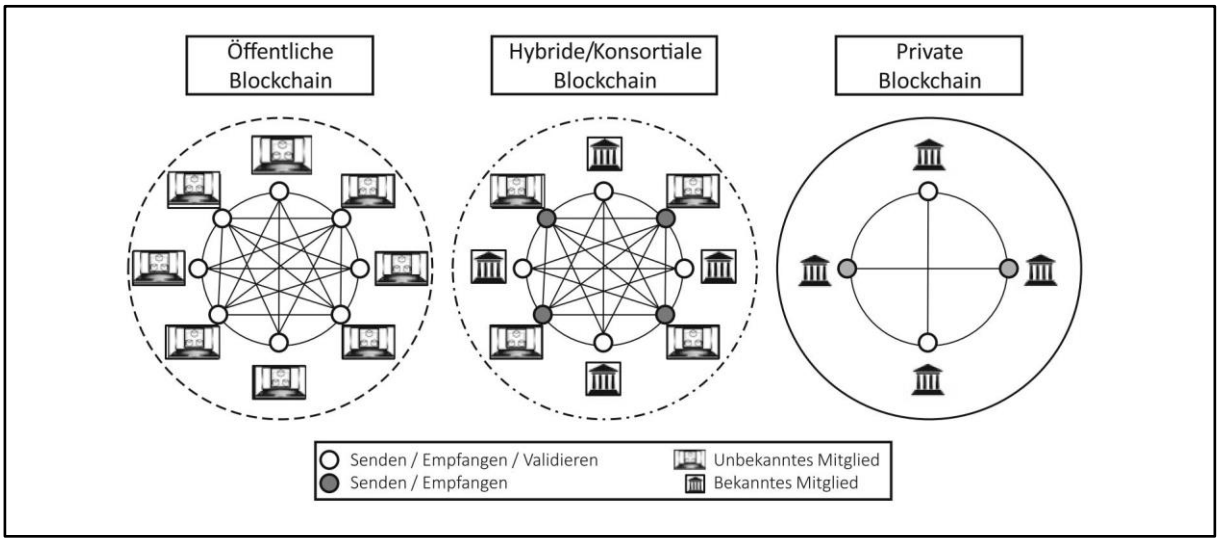


Abbildung 3-5: Blockchain-Typen
(Quelle: Reuse/Frère/Schaab (2019): 46)

Neben der Unterteilung in die oben dargestellte Blockchain-Taxonomie unterscheidet PLOOM ergänzend zwischen *Lokalität*, *Scripting-Fähigkeit* sowie *Applikationsspezifizität*.[198] *Lokalität* präzisiert, ob eine Blockchain verteilt oder lokal betrieben wird. Ein lokaler Betrieb wird, anders als die bereits beschriebene Form des verteilten Registers für den Bitcoin, in einer abgeschlossenen Umgebung durchgeführt. Ein hybrider Ansatz kann weiterhin gewählt werden. PLOOM weist hierbei auf die *Guardtime-Blockchain* hin, die zwar lokal die Integrität von Patientendaten mittels Blockchain garantiert, die Hash-Werte allerdings in einem verteilten Register abspeichert.[199] *Applikationsspezifizität* stellt den Einsatzzweck einer Blockchain in den Vordergrund. Der Einsatz ist entweder generisch für mehrere Problemlösungen oder speziell für

[196] Im Zusammenhang mit *Konsortial-Blockchains* ergänzen Hussien et al. die von Burgwinkel dargestellte Unterscheidung in *permissioned* und *unpermissioned* (vgl. Burgwinkel (2016): 35) um den Begriff *federated* (vgl. Hussien et al. (2019): 320.5). Dieser Begriff hat sich in der untersuchten Literatur jedoch nicht durchgesetzt. Aus diesem Grund wird der Begriff *federated* auch nicht weiter genutzt.

[197] Vgl. Burgwinkel (2016): 48; Alhadhrami et al. (2017): 376; Thwin/Vasupongayya (2018): 197.

[198] Vgl. Ploom (2016): 123.

[199] Vgl. Ploom (2016): 123.

einen einzigen Anwendungsfall möglich.[200] *Scripting-Fähigkeit* unterscheidet Blockchains in der Möglichkeit, eigene Programme bzw. Skripte, sogenannte *Smart Contracts*, auszuführen.[201] Während Transaktionen bereits Willenserklärungen zweier Parteien abbilden,[202] erweitern Smart Contracts diese um Protokolle, die weitere Bestandteile möglicher Verträge zwischen mindestens zwei Parteien beinhalten. Dabei können bspw. ergänzende Transaktionen automatisiert durchgeführt oder externe Applikationen ausgeführt werden.[203] Smart Contracts werden in der für die Blockchain relevanten Programmiersprache verfasst,[204] auf der Blockchain gespeichert und zusammen mit den Transaktionen im Netzwerk verteilt.[205]

3.2.5 Ausgewählte Blockchain-Technologien

In diesem Kapitel werden die bekanntesten Blockchain-Technologien beschrieben, und zwar unter Anwendung der in *Kapitel 3.2.4* dargestellten Unterscheidungsmöglichkeiten:[206]

i. Bitcoin
ii. Ethereum
iii. Guardtime
iv. Hyperledger

Bitcoin (i) ist, wie bereits dargestellt, eine öffentliche Blockchain zur verteilten Verwaltung von Zahlungsinformationen in einem P2P-Netzwerk, in dem Nutzer Transaktionen pseudonymisiert durchführen und Kryptowährung (hier: Bitcoin)[207] übertragen bzw. durch Mining verdienen.[208] Eine Bitcoin-Blockchain wird verteilt betrieben[209] und beschränkt sich im Scripting

---

200 Vgl. Ploom (2016): 124.

201 Vgl. Ploom (2016): 123f.

202 Vgl. Drescher (2017): 249.

203 Vgl. Swan (2015): 16; Burgwinkel (2016): 48; Merz (2016): 58. Die Idee hinter Smart Contracts ist zurückzuführen auf SZABO (vgl. Sixt (2017): 166), der die Notwendigkeit von Intermediären mittels Automatisierung von Transkationen minimiert (vgl. Szabo (1994)).

204 Während Ethereum als erste Blockchain Smart Contracts einsetzt und diese in der Programmiersprache *Solidity* verfasst (vgl. Ploom (2016): 129, mit Verweis auf die Online-Dokumentation von READ THE DOCS (2019)), werden *Smart Contracts* in der Hyperledger-Blockchain *Chaincode* genannt (vgl. Kienzler (2016): 118). Zur Wahrung der Lesbarkeit wird im Verlauf der Dissertation aufgrund der inhaltlichen Überschneidung weiterhin der Begriff *Smart Contract* genutzt.

205 Vgl. Ploom (2016): 128; Drescher (2017): 249.

206 Vgl. Burgwinkel (2016): 11. BURGWINKEL bezieht sich auf das Jahr 2016. Beginn der Dissertation ist 2017.

207 Unter Verwendung der Bitcoin-Blockchain-Technologie haben sich sogenannte Altcoins (Abkürzung für den englische Begriff *alternative coins*) entwickelt, die sich zwar an der Bitcoin-Blockchain orientieren, jedoch eine andere Kryptowährung (z.B. LiteCoin) nutzen (vgl. Bussac (2019): 195).

208 Vgl. Burgwinkel (2016): 23; Burgwinkel (2016): 25.

209 Vgl. Ploom (2016): 123.

auf die Durchführung von Transaktionen, deren Aufbau standardisiert ist.[210] Auch ist die Bitcoin-Technologie generischer Natur, da sie nicht nur für Zahlungs-Transaktionen, sondern auch für andere Szenarien eingesetzt werden kann.[211]

Ethereum (ii) ist eine Weiterentwicklung der Bitcoin-Blockchain, ebenfalls öffentlich und verteilt organisiert. Sie ermöglicht als erste Blockchain Smart Contracts und somit eine erweiterte Form des Scripting.[212] Ethereum ist weniger eine eigene Blockchain als eine Plattform, die ihre Ressourcen in Form einer virtuellen Maschine (Ethereum Virtual Machine (EVM)) für den Betrieb diverser Blockchains bereitstellt.[213] Auch ist die genutzte Kryptowährung *Ether* in diesem Zusammenhang nicht nur Kryptowährung, sondern auch eine Einheit, die den Betrieb der Plattform und die Ausführung von Smart Contracts ermöglicht.[214] Wie bei der Bitcoin-Technologie wird auch für die Ethereum-Blockchain derzeit der PoW-Konsens genutzt, der in Zukunft aber durch den PoS-Konsens abgelöst wird.[215] Neben der reinen Durch- bzw. Ausführung von Transaktionen und Smart Contracts können auf der Ethereum-Blockchain sog. dezentrale Applikationen (engl. *decentral applications (DApp)*)[216] sowie dezentrale autonome Organisationen (engl. *Decentralized/Distributed Autonomous Organizations* oder *Decentralized/Distributed Autonomous Corporations)* betrieben werden. Die Begriffe *DApp* und *dezentrale Organisation* werden teilweise synonym genutzt,[217] beschreiben aber im engeren Sinne das Gleiche, nämlich die Erweiterung von Smart Contracts von der Ausführung von Verträgen hin zur Durchführung aufeinander aufbauender Aktionen, die dem Handeln einer Organisation gleichkommen.[218] Wie die Bitcoin-Blockchain ist auch die Ethereum Blockchain generisch und kann in unterschiedlichen Szenarien eingesetzt werden.[219]

---

210 Vgl. Ploom (2016): 124.

211 Vgl. Ploom (2016): 124.

212 Vgl. Brühl (2017): 138.

213 Vgl. Swan (2015): 21; Bussac (2019): 26.

214 Vgl. Burgwinkel (2016): 26; Bussac (2019): 26.

215 Vgl. Bussac (2019): 26.

216 *DApps* sind eigene Programme, die auf der EVM ausgeführt werden. Eine *DApp* muss dabei vier Kriterien entsprechen: Open-Source-Applikation, Betrieb auf einer (eigenen) Blockchain, Existenz eines Tokens/Coins, Vorhandensein eines Konsens-Protokolls (vgl. Johnston et al. (2014): o. S.).

217 Vgl. Franco (2014): 184.

218 Vgl. Swan (2015): 24f; Burgwinkel (2016): 47; Meinel/Gayvoronskaya/Schnjakin (2018): 74; Wüst/Gervais (2018): 52.

219 Vgl. Ploom (2016): 124.

Guardtime (iii) ist eine vom gleichnamigen Unternehmen entwickelte Lösung für ein auditfähiges, transparentes und sicheres Blockchain-System, dessen Ziel die Integritätssicherung sämtlicher Daten des estnischen Gesundheitswesens unter Anwendung einer Keyless Signature Infrastructure (KSI) ist.[220]

Hyperledger (iv), 2017 von der Linux Foundation vorgestellt, ist, ähnlich Ethereum, eine Plattformlösung. Statt eines öffentlichen Konzepts verfolgt Hyperledger einen konsortialen Ansatz. Der Nutzerkreis kann privat sowie öffentlich definiert werden und beschränkt die Kernfunktionalitäten, wie Mining und Validierung, gleichzeitig auf ausgewählte Nodes im Netzwerk. Hyperledger ist eine Open-Source-Lösung, die ebenfalls die Ausführung von Smart Contracts, hier Chaincode genannt,[221] ermöglicht.[222] Hyperledger Fabric ist die erste auf Hyperledger basierende Technologie[223] und zählt zu den Permissioned-Blockchains, besitzt einen Member Service zur Verwaltung der Teilnehmer und nutzt als Sicherheits-Infrastruktur eine PKI. Im Gegensatz zu anderen Blockchain-Technologien können innerhalb der Hyperledger Fabric einzelne Kanäle erstellt werden, sodass einem bestimmten Nutzerkreis nur die für ihn relevanten Inhalte zur Verfügung gestellt werden.[224] Diese Technologie ist ebenso wie Bitcoin und Ethereum generisch und verspricht auch aufgrund ihres konsortialen Ansatzes ein breites Spektrum an Einsatzszenarien in transaktionsbasierten Industrien.[225]

3.3 Potentiale und Limitationen der Blockchain-Technologie im Kontext von Gesundheitsdaten

Der Einsatz von Blockchain-Technologie verspricht im Vergleich zur Verwendung herkömmlicher Daten-Infrastruktur diverse Verbesserungen organisatorischer und technischer Natur wie auch Limitationen, die insbesondere die der Technologie zugrundeliegenden Prinzipien geschuldet sind. Die folgende Auseinandersetzung mit diesem Thema wird bereits auf den Einsatz der Blockchain-Technologie im Gesundheitswesen ausgerichtet.

Eine Blockchain verspricht Teilnehmern Transparenz über alle im Netzwerk durchgeführten Transaktionen und ermöglicht nicht nur den zeitnahen Zugriff auf relevante Informationen, sondern befähigt einen Patienten, die Kontrolle über seine bei diversen Leistungserbringern

---

220 Vgl. Burgwinkel (2016): 26-27, 48; Guardtime (2016); Angraal/Krumholz/Schulz (2017): 2; Rodrigues/Bocek/Stiller (2018): 177f.

221 Vgl. Kienzler (2016): 118.

222 Vgl. Ploom (2016): 124; Meinel/Gayvoronskaya/Schnjakin (2018): 74.

223 Vgl. Burgwinkel (2016): 48.

224 Vgl. Rouhani et al. (2018): 1534.

225 Vgl. Burgwinkel (2016): 27f; Kienzler (2016): 111; Ploom (2016): 124.

verteilten Daten zu übernehmen.[226] Auch ist die Verwendung von Daten entlang des gesamten Behandlungspfades möglich, ohne dass ihre Integrität leidet oder Interoperabilitäts-Barrieren[227] entstehen, sodass sämtliche möglicherweise relevanten Informationen zur optimalen Behandlung zur Verfügung stehen.[228] Zudem wird der medizinischen Forschung auf diesem Weg ein vereinfachter Zugriffsmechanismus auf akkurate Daten ermöglicht.[229] Doch gerade diese Transparenz von Informationen kann in bestimmten Ausprägungen deren Vertraulichkeit gefährden, da Algorithmen und Mustererkennungsverfahren eine Identifikation von Personen ermöglichen, obwohl sämtliche Daten verschlüsselt abgelegt sind.[230] Gerade die Speicherung von Daten in den Infrastrukturen der Leistungserbringer, doch genauso die Speicherung dieser Daten auf der Blockchain und damit die Replizierung im gesamten Netzwerk gewährleisten nicht deren Vertraulichkeit gegenüber unberechtigten Dritten.[231] Der in der Europäischen Union geltende strenge Datenschutz verlangt neben einer Verschlüsselung, die eben diese De-Anonymisierung unterbindet,[232] eine sichere Zugriffssteuerung.[233] Auch sind Funktionen notwendig, die bspw. die Löschung von Inhalten auf der Blockchain ermöglichen.[234] Doch existieren diese bislang nicht. Grundsätzlich fehlt es auf politischer Ebene an einer gemeinsamen Leitlinie zur Definition von Mindeststandards zur Sicherung der Vertraulichkeit trotz geforderter Transparenz sämtlicher Daten und Informationen.[235]

Die hier beschriebene Transparenz-Offensive durch die Blockchain führt zu einem vereinfachten Zugang für Kostenträgern zu Patienteninformationen. Dies ermöglicht die Überprüfung abgerechneter Leistungen und eine Identifikation möglicher Betrugsfälle, deren Schaden meist die Allgemeinheit trägt.[236] Ebenso können durch eine Überwachung von Ereignissen, wie bspw.

---

226 Vgl. Gökalp et al. (2018): 179.

227 Gegenüber bestehenden Systemen im Gesundheitswesen und ihrer heterogenen Konstruktionen erlaubt eine Blockchain durch erzwungene Anwendung von Interoperabilitätsstandards eine einrichtungs- oder anwendungsübergreifende Kommunikation und beschleunigt Datenfreigaben und deren Analyse (vgl. Gökalp et al. (2018): 180). Die Notwendigkeit, Interoperabilitätsstandards zu nutzen, bedarf jedoch der Abstimmung der Stakeholder auf eine gemeinsame Governance (vgl. Gökalp et al. (2018): 181; Kamel Boulos/Wilson/Clauson (2018): 25.8; Kumar et al. (2018): 157).

228 Vgl. Liu et al. (2017): 41; Gökalp et al. (2018): 180.

229 Vgl. Gökalp et al. (2018): 181.

230 Vgl. Angraal/Krumholz/Schulz (2017): 3; Kuo/Kim/Ohno-Machado (2017): 1217; Gordon/Catalini (2018): 228.

231 Vgl. Alhadhrami et al. (2017): 376; Thwin/Vasupongayya (2018): 197.

232 Vgl. Angraal/Krumholz/Schulz (2017): 3; Kuo/Kim/Ohno-Machado (2017): 1217; Gordon/Catalini (2018): 228; Meinel/Gayvoronskaya/Schnjakin (2018): 51.

233 Vgl. Alhadhrami et al. (2017): 376; Gökalp et al. (2018): 182; Kumar et al. (2018): 158.

234 Vgl. Kamel Boulos/Wilson/Clauson (2018): 25.8.

235 Vgl. Gökalp et al. (2018): 182; Kumar et al. (2018): 158.

236 Vgl. Liu et al. (2017): 41; Gökalp et al. (2018): 179f.

häufiges Aufsuchen bestimmter Leistungserbringer, neue Erkenntnisse für eine künftige Vertragsgestaltung mit Leistungserbringern gewonnen werden, sodass Kostenträger Kostensenkungspotentiale identifizieren können.[237] Doch ausgerechnet diese Kostenvorteile können von den Kosten überholt werden, die die Entwicklung und der spätere Betrieb eines Blockchain-Netzwerkes mit sich bringen.[238] Insbesondere der mit Blockchain-Systemen einhergehende Energieverbrauch für die Erstellung von Blöcken ist hier zu erwähnen.[239]

Trotz der Potentiale, die der Einsatz der Blockchain-Technologie mit sich bringt, müssen Stakeholder motiviert werden, an einem Blockchain-Netzwerk aktiv teilzunehmen, mit bisherigen Prozessen zu brechen und ihre Endgeräte mit diesem Netzwerk zu verbinden.[240] Dabei ist vorstellbar, dass nicht jeder Stakeholder ein Interesse daran hat, die von der Blockchain proklamierte Transparenz herzustellen. Oder es blockieren kommerzielle Interessen den Zugang zu Patientendaten.[241] Auch können Vorbehalte gegenüber der Automatisierung von Prozessen durch Smart Contracts existieren oder die Sicherheit der Verschlüsselung in Frage gestellt werden.[242]

Insbesondere wenn Stakeholder Speicherkapazitäten für die gesamte Blockchain vorhalten müssen, stellt sich die Frage, ob bestehende Systeme und Netzwerke den täglich wachsenden Umfang der Daten verarbeiten können. Neben der Größe ist die Verarbeitungsgeschwindigkeit der Transaktionen relevant, die abhängig ist von der gewählten Blockchain-Technologie und vom Konsensprotokoll.[243] Auch die Anbindung neuer Teilnehmer ans Netzwerk erfordert den Abruf der kompletten bereits bestehenden Blockchain, sodass neue Teilnehmer entsprechende Speicher- und Netzwerkkapazitäten vorhalten müssen.[244]

---

237 Vgl. Gökalp et al. (2018): 180f.

238 Vgl. Liu et al. (2017): 41; Gökalp et al. (2018): 183; Kumar et al. (2018): 157.

239 Vgl. Thwin/Vasupongayya (2018): 197. Eine nähere Evaluation des tatsächlichen Kosten-Nutzen-Verhältnisses steht noch aus (vgl. Angraal/Krumholz/Schulz (2017): 3).

240 Vgl. Gökalp et al. (2018): 182; Kumar et al. (2018): 158.

241 Vgl. Kumar et al. (2018): 158.

242 Vgl. Qiu et al. (2018): 684. Insbesondere der Diebstahl von Schlüsselmaterial führt zu einer Preisgabe von persönlichen Informationen (vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 52). Auch der Verlust von Schlüsselmaterial verhindert den Zugriff auf sämtliche im Netzwerk vorhandenen Daten (vgl. Gökalp et al. (2018): 182).

243 Vgl. Swan (2015): 84; Angraal/Krumholz/Schulz (2017): 3; Kuo/Kim/Ohno-Machado (2017): 1217; Gökalp et al. (2018): 182; Meinel/Gayvoronskaya/Schnjakin (2018): 53-56; Thwin/Vasupongayya (2018): 197.

244 Vgl. Meinel/Gayvoronskaya/Schnjakin (2018): 52f. Es muss in diesem Zusammenhang zwischen den Nutzern unterschieden werden, da nicht jeder eine vollständige Kopie der Blockchain benötigt. Siehe hierzu die Differenzierung zwischen Light- und Full-Nodes in *Kapitel 3.2.1*.

Folglich ergibt sich zu einem nicht näher definierten Zeitpunkt zwischen dem Nutzen der Blockchain und den verarbeiteten Gesundheitsdaten ein Trade-off, der einer Blockchain ein ökonomisches Limit setzt.[245]

[245] Vgl. Kumar et al. (2018): 157.

4 Identifikation der für die Forschungsarbeit relevanten wissenschaftlichen Literatur

4.1 Auswahlprozess und Festlegung der relevanten Literaturquellen

Die Identifikation aktueller, wissenschaftlich relevanter Literatur unter Anwendung des von WEBSTER/WATSON und LEVY/J. ELLIS beschriebenen Verfahrens der Literaturanalyse ist Ziel dieses Kapitels. Eine Literaturanalyse (engl. *Literature Review*) beschreibt einen strukturierten Ansatz, wissenschaftliche Literatur zu identifizieren, zu systematisieren und zu analysieren.[246]

Der Fokus bei der Literaturauswahl liegt auf der konkreten Anwendung von Blockchain im Gesundheitswesen, mit inhaltlicher Ausrichtung zu institutionsinternen, einrichtungsübergreifenden sowie persönlichen Patientenakten. Publikationen, die darüber hinaus den Einsatz von Blockchain in der Telemedizin[247] behandeln, werden unter Berücksichtigung der Definition von Telemedizin nicht in die Analysen der Forschungsarbeit eingebunden, da sich diese Themen nicht mit der Dokumentation von Behandlungen, sondern der konkreten Unterstützung der Gesundheitsversorgung beschäftigen.

Im ersten Schritt des Auswahlprozesses wird in den Ranking-Listen des VERBANDS DER HOCHSCHULLEHRER FÜR BETRIEBSWIRTSCHAFT E.V. (VHB), genauer dem Fachbereich Betriebswirtschaftslehre (Teilbereich *Management im Gesundheitswesen*), nach möglicherweise relevanten Journalen[248] gesucht. Zur Identifikation wird zunächst auf das Suchwort *Blockchain* reduziert, doch führt die Suche in den Zeitschriften, gleichgültig ob im A-, B- oder C-Ranking, zu keinen Ergebnissen. Lediglich im *British Journal of Healthcare Management* finden sich zwei allgemein gehaltene Artikel zum Thema Blockchain, auf die wegen fehlender Lizenzen nicht zugegriffen werden kann.[249] Im zweiten Schritt wird der *Fachbereich Wirtschaftsinformatik* betrachtet. Die Suchergebnisse verteilen sich, wie *Tabelle 4-1* zeigt, auf die diversen Journal-Rankings, weisen jedoch in keinem einzigen Fall einen Bezug zu Gesundheitsdaten auf.[250]

---

246 Vgl. Levy/J. Ellis (2006): 182.

247 Telemedizin wird definiert als *„[…] Leistungserbringung im medizinischen Umfeld unter Verwendung von Telekommunikationssystemen, wobei die Überwindung räumlicher und/oder zeitlicher Distanz zwischen den Akteuren wesentliches Ziel ist.“* (Lux (2017): 9).

248 Gemäß WEBSTER/WATSON ist die Suche in angesehenen Journalen ein guter Ausgangspunkt für die Identifikation relevanter Publikationen (vgl. Webster/Watson (2002): 16).

249 Eine Liste der untersuchten Journale/Zeitschriften findet sich in *Anhang B, Tabelle B-1*.

250 Eine Liste der untersuchten Journale/Zeitschriften findet sich in *Anhang B, Tabelle B-2*.

Tabelle 4-1: Literatursuche in VHB-Journalen des Fachbereichs Wirtschaftsinformatik (Quelle: Eigene Darstellung)

Ranking	Anzahl der Suchergebnisse	Relevanz
A+	6	0
A	13	0
B	20	0

Da die Ranking-Listen des VHB somit keine für diese Forschungsarbeit geeigneten Ergebnisse liefern, wird die Suche auf wissenschaftliche Internet-Suchmaschinen ausgeweitet. Unter Berücksichtigung der Diversität zwischen den teilweise verlagsabhängigen Suchmaschinen werden für die Literaturanalyse folgende Suchmaschinen ausgewählt: *AIS eLibrary, IEEE Xplore, ProQuest, PubMed, Sciencedirect, Scopus und SpringerLink.*[251] Mithilfe logischer Operatoren[252] wird das bisher genutzte Suchwort *Blockchain* weiter spezifiziert und eine feingranulare Suchwort-Kombination genutzt:[253]

"blockchain" AND ("health" OR "health care" OR "healthcare" OR "medical")[254]

[251] Ähnliche Suchmaschinen, wie *GoogleScholar* oder *HealthIT.gov*, wurden nicht berücksichtigt. Grund hierfür ist die Überschneidung der Ergebnisse mit den im Text genannten Suchmaschinen und die fehlende Differenzierung zwischen wissenschaftlicher Publikation und (privat-)wirtschaftlich orientierten Whitepapern.

[252] AND (Konjunktion) sowie OR (Disjunktion) entspringen der Aussagenlogik (vgl. Büning/Lettmann (1994): 2). AND stellt hier eine verpflichtende Verknüpfung zwischen Blockchain und dem Gesundheitswesen her. OR hingegen ermöglicht die differenzierte Nutzung verschiedener Begriffe.

[253] Entgegen der üblichen Nutzung von Anführungszeichen in der wissenschaftlichen Arbeit als Kennzeichnung wörtlicher Zitate sind die in dieser Aufzählung genutzten Zeichen logische Operatoren, die die Suchbegriffe spezifizieren und entsprechende Funktionen in den Suchmaschinen abbilden.

[254] Die Verwendung von Anführungsstrichen entspricht in diesem Fall nicht der wissenschaftlichen Notation für direkte Zitate, sondern der in Suchmaschinen üblichen Fixierung von Suchbegriffen bzw. Suchausdrücken.
In der Keyword-Auswahl hätte auf [*OR "health care"*] verzichtet werden können, wenn es nicht in der AIS eLibrary zu weniger, möglicherweise relevanten Suchergebnissen gekommen wäre. In allen anderen Suchmaschinen bleibt die Menge an Suchergebnissen unverändert. Zur Vermeidung der Missachtung von potentiell relevanter Literatur wird dieses Suchwort weiterhin genutzt.
Die doppelte Nutzung des Suchbegriffs *Healthcare* und *Health Care* ist aufgrund ihrer synonymen Nutzung in der Literatur notwendig. *Healthcare* ist per Definition *„a set of services provided by a country or an organization for the treatment of the physically and the mentally ill."* (Procter (2002): 655). Die getrennte Schreibweise *Health Care* geht in eine ähnliche Richtung, fokussiert sich jedoch auf die eigentliche Behandlung (*Health* (Gesundheit) und *Care* (Behandlung)). Das Problem der synonymen Nutzung greift ISSEL in einem Editorial auf, diskutiert kurz die Verwendung beider Begriffe in der Literatur und kommt zu dem Ergebnis, dass eigentlich nur die getrennt geschriebene Variante genutzt werden sollte (vgl. Issel (2014): 269). Dennoch lässt dich bei Durchsicht der Literatur nicht bestätigen, dass sich diese Ansicht durchgesetzt hat.

Aufgrund der englischsprachigen Ausrichtung der Suchmaschinen wird die Suche nicht mit deutschen Begriffen durchgeführt.[255] Eine alternative Suchwort-Kombination, die bereits Patientenakten mit einschließt, wurde nicht genutzt,[256] weil diese das Risiko birgt, relevante Literatur in einem zu frühen Stadium der Suche auszuschließen.[257]

Die Suche in den Internet-Datenbanken wird auf den Zeitraum von 2008 bis 2018[258] beschränkt.[259] Entsprechend den vorliegenden Filterkriterien innerhalb der genutzten Suchmaschinen, ergibt sich die in *Tabelle 4-2* dargestellte positive Filterauswahl der konkreten Publikations-Typen.

Tabelle 4-2: Filterung in den Suchmaschinen (Quelle: Eigene Darstellung)

Suchmaschine	Publikations-Typ-Filter
AIS eLibrary	Conference Journal
IEEE Xplore	Conferences Journals
ProQuest	Wissenschaftliche Zeitschriften
PubMed	*Keine Filterung*
Sciencedirect.com	Review Article Research Article
Scopus	Article Conference Paper
SpringerLink	Article Conference Paper

Die erste Suche anhand der genannten Suchwort-Kombination führt in den Internet-Datenbanken zu insgesamt 912 Treffern (siehe *Tabelle 4-3*). Ergänzt werden diese Ergebnisse um das erst 2018 aufgelegte Peer-Review-Journal *Blockchain in Healthcare Today*, das sich explizit mit dem Einsatz von Blockchain im Gesundheitssektor auseinandersetzt, und eigene Recherchen (siehe *Tabelle 4-4*).

---

255 Eine stichprobenartige Überprüfung durch Ergänzung der Kombination von ("blockchain" AND ("health" OR "health care" OR "healthcare" OR "medical")) auf ("blockchain" AND ("health" OR "health care" OR "healthcare" OR "medical" OR "gesundheitswesen" OR "versorgung")) führte zu keiner Veränderung der Suchergebnisse.

256 Eine solche Keyword-Kombination könnte lauten: "blockchain" AND ("patient record" OR "health record" OR "medical record")

257 In diesem Zusammenhang wird ebenfalls auf die uneinheitliche Verwendung des Begriffs Patientenakte bzw. deren englische Pendants hingewiesen, die bereits in *Kapitel 2.1* thematisiert wird.

258 Der konkrete Stichtag ist der 31.12.2018.

259 Blockchain wurde erst mit der Veröffentlichung von NAKAMOTO im Jahr 2008 bekannt.

Tabelle 4-3: Suchergebnisse nach der ersten Schlagwort-Suche (Quelle: Eigene Darstellung)

Suchmaschine	Anzahl Suchergebnisse
AIS eLibrary	93
IEEE Xplore	156
ProQuest	63
PubMed	64
Sciencedirect.com	16
SpringerLink	266
Scopus	254
Summe	912

Tabelle 4-4: Zusätzliche Ergebnisse anderer Quellen (Quelle: Eigene Darstellung)

Andere Quelle/Anderes Journal	Anzahl Publikationen
Blockchain in Healthcare Today	10
Eigene Ergänzung	1

Diese 923 Suchergebnisse können aufgrund von Duplikaten auf 713 reduziert werden. Die dann folgende Vorsortierung schließt weitere 565 Ergebnisse aus. Hierzu gehört Literatur, deren Sprache weder Deutsch noch Englisch ist (n = 14), auf deren Volltext nicht zugegriffen werden kann (n = 29) sowie Literatur, die im Rahmen der Auswertung von *Titel* und *Abstract* inhaltlich nicht relevant ist (n = 522). Im letzten Schritt werden Volltexte auf Relevanz hin untersucht, was zu einem Endergebnis von 109 relevanten Literaturergebnissen führt. Inhaltliche Relevanz beschränkt sich nicht auf Publikationen, die eine konkrete Lösung beschreiben, sondern schließt ebenfalls die Bearbeitung von Teilbereichen, wie bspw. sichere Übertragung von Gesundheitsdaten oder (abgesicherte) Datenhaltung großer Datenmengen, mit ein. Des Weiteren können zwei bereits durch YLI-HUUMO ET AL.[260] und HÖLBL ET AL.[261] durchgeführte Literaturanalysen identifiziert werden, deren Ergebnisse ebenfalls in den Literaturauswahlprozess einbezogen werden.[262] Der gesamte Auswahl-Prozess ist in *Abbildung 4-1* dargestellt.

[260] *„RQ1: What research topics have been addressed in current research on Blockchain? RQ2: What applications have been developed with and for Blockchain technology? RQ3: What are the current research gaps in Blockchain research? RQ4: What are the future research directions for Blockchain?"* (Yli-Huumo et al. (2016): e0163477.4–5).

[261] *„RQ1: To what extent is blockchain established in healthcare and how did this change over time? RQ2: What are the current research trends for blockchain use in healthcare? RQ3: What are the elements of blockchain technology used in the healthcare publications?"* (Hölbl et al. (2018): 470.6).

[262] Die von YLI-HUUMO ET AL. durchgeführte Analyse beschäftigt sich allgemein mit der Forschung zu Blockchain-Technologien und stellt keinen direkten Zusammenhang mit dem Gesundheitswesen her.

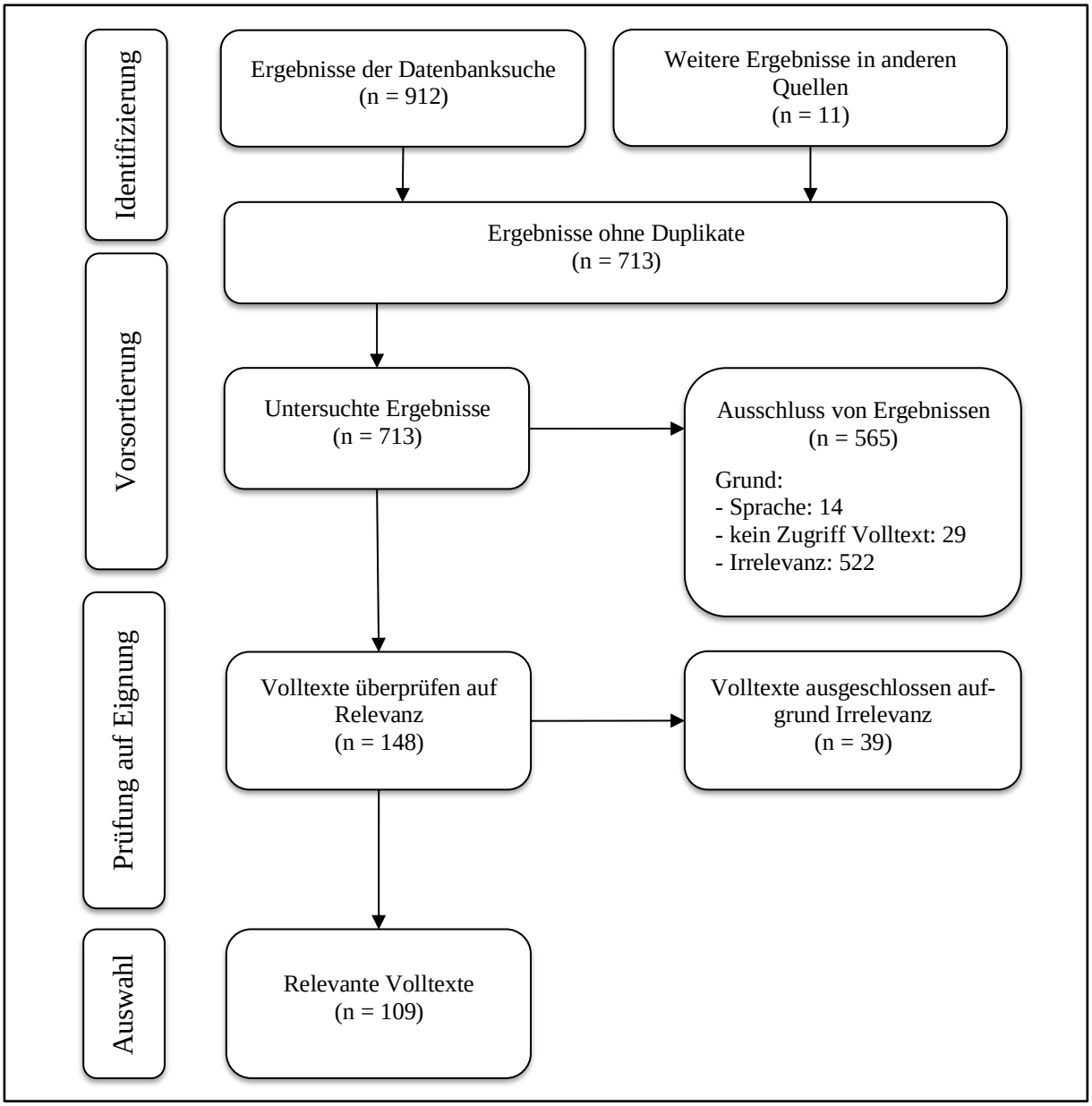


Abbildung 4-1: Ablauf und Ergebnisse der initialen Literatur-Suche (Quelle: Eigene Darstellung in Anlehnung an Moher et al. (2009): e1000097.3)

Die bis zu diesem Schritt durchgeführte Stichwortsuche ist zur umfänglichen Identifikation von Forschungsliteratur nicht ausreichend, denn die Wahl der Stichworte ist vom Suchenden abhängig und schränkt folglich die Ergebnisse ein.[263] Um eine solche Einschränkung möglichst auszuschließen, wird auf Basis der 109 identifizierten Literaturquellen eine *Backward-Suche* mit anschließender *Forward-Suche* durchgeführt. Während der **Backward-Suche** wird die in den bereits identifizierten Quellen zitierte Literatur auf Relevanz hin analysiert. Dieser Vorgang

[263] Vgl. Levy/J. Ellis (2006): 190.

wird iterativ auf Basis der neu identifizierten Literatur fortgesetzt, bis sich keine neuen Quellen finden.[264]

Die *Backward-Suche* bedarf in dieser Forschungsarbeit einer einzigen Iteration und ergänzt die bereits identifizierten Quellen um 21. Darauf aufbauend wird eine Suche nach weiterer Literatur in den Publikationslisten der am häufigsten zu findenden Autoren[265] vorgenommen, die allerdings zu keiner weiteren Ergänzung der Ergebnisse führt.[266]

Aus dieser erweiterten Literaturbasis (n = 130) werden die besonders relevanten Quellen herausgefiltert (hier: TOP10 der am häufigsten zitierten Publikationen) und mittels einer **Forward-Suche** Literatur identifiziert, die diese bereits als besonders relevant gekennzeichneten Publikationen zitieren.[267] Die Ermittlung der TOP10-Publikationen wird mithilfe einer Matrix-Analyse[268] durchgeführt. Diese visualisiert mittels Darstellung von Kreuzverweisen dominierende Literatur auf Basis ihrer Zitationshäufigkeit. Das Ergebnis wird in *Tabelle 4-5* dargestellt.

Tabelle 4-5: TOP10 der im Literaturüberblick zitierten Literatur nach Backward-Suche (Quelle: Eigene Darstellung)

Autor(en)	Titel	Zitationen
Azaria et al. (2016)	MedRec: Using Blockchain for Medical Data Access and Permission Management	40
Yue et al. (2016)	Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control	35
Ekblaw et al. (2016)	A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data	26
Zyskind/Nathan/Pentland (2015)	Decentralizing Privacy: Using Blockchain to Protect Personal Data	26
Peterson et al. (2016)	A Blockchain-Based Approach to Health Information Exchange Networks	22
Kuo/Kim/Ohno-Machado (2017)	Blockchain distributed ledger technologies for biomedical and health care applications	16
Xia et al. (2017a)	MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain	14
Xia et al. (2017b)	BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments	11

[264] Vgl. Webster/Watson (2002): 16. Darüber hinaus kann auch nach den zitierten Autoren sowie mittels der von diesen genutzten Keywords nach weiterer Literatur gesucht werden (vgl. Levy/J. Ellis (2006): 191).

[265] Bowden, Daniel (n = 3); Sifah, Emmanuel Boateng (n = 3); Xia, Qi (n = 3); Liang, Xueping (n = 5); Shetty, Sachin (n = 5).

[266] Gesucht wird in den Autoren-Profilen, in den Suchmaschinen sowie, wenn abrufbar, in den Publikationslisten an Universitäten oder in an Forschungsprojekten beteiligten Unternehmen.

[267] Vgl. Webster/Watson (2002): 16. Wie bei der Backward-Suche kann auch hier nach neuer Literatur gesucht werden, die die referenzierten Autoren verfasst haben, ohne dass diese auf die explizit identifizierte Literatur verweisen (vgl. Levy/J. Ellis (2006): 191).

[268] Diese Matrix führt in Spalte und Zeile die gleichen Publikationen auf und prüft, ob der Spaltenwert in den Verweisen des Zeilenwerts erscheint. Abschließend werden sämtliche positiven Verweise summiert und ergeben die in *Tabelle 4-5* dargestellten Summen in der Spalte *Zitationen*.

Dubovitskaya et al. (2017)	Secure and Trustable Electronic Medical Records Sharing using Blockchain	9
Kish/Topol (2015)	Unpatients - Why patients should own their medical data	9

Die eigentliche *Forward-Suche* wird in *GoogleScholar* durchgeführt und auf die ersten zehn Ergebnisseiten beschränkt.[269] In diesem Suchschritt werden in zwei Iterationen zwei neue Literaturquellen gefunden, sodass sich die Gesamtzahl relevanter Literatur auf 132 erhöht. Eine erneute *Backward*-Suche, beschränkt auf die zwei neu identifizierten Ergebnisse, führt zu keinen neuen Erkenntnissen, weshalb der Prozess der Literaturermittlung mit 132 relevanten Literaturquellen beendet ist.

4.2 Grobanalyse der vorliegenden Literatur

Sämtliche Publikationen verteilen sich, dargestellt in *Abbildung 4-2*, auf die Jahre 2015 bis 2018, nehmen in diesem Zeitraum exponentiell zu und repräsentieren damit eine wissenschaftliche Relevanz der Thematik. Publikationen in Tagungs- oder Sammelbänden sind annähernd häufig wie Publikationen in Fachzeitschriften (siehe *Abbildung 4-3*).

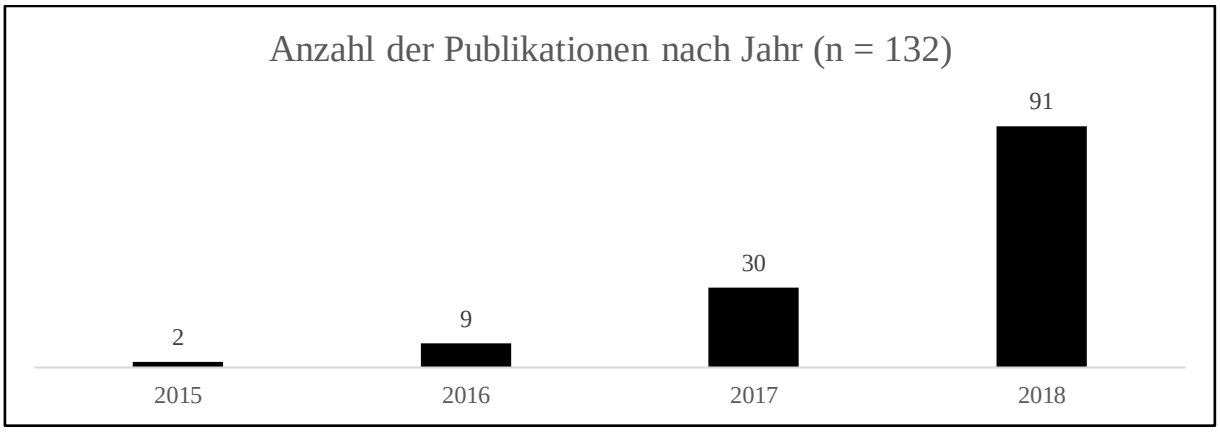


Abbildung 4-2: Verteilung der Literatur nach Veröffentlichungsjahr (Quelle: Eigene Darstellung)

[269] Die Sortierung der Ergebnisse basiert auf dem Relevanz-Algorithmus von Google. In der Suche werden die gleichen Parameter wie bisher genutzt.

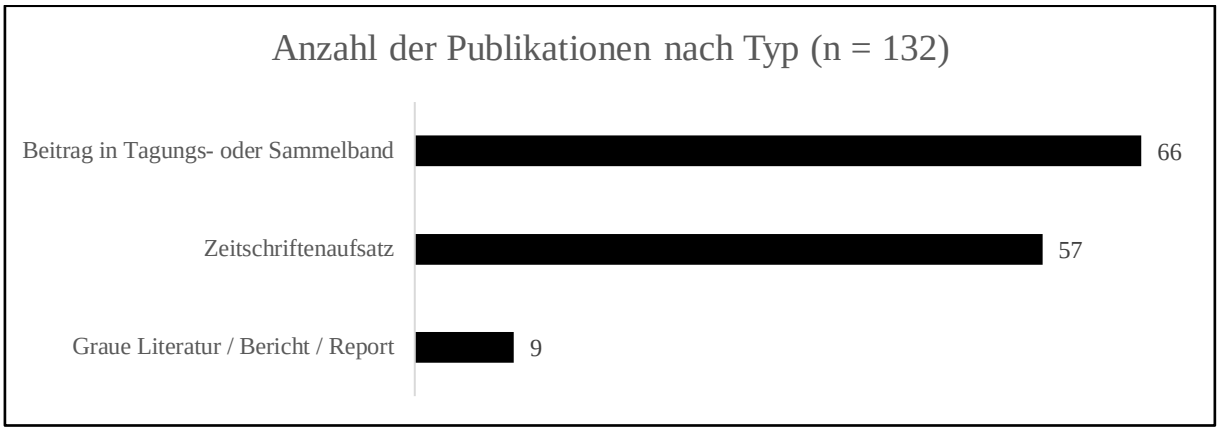


Abbildung 4-3: Verteilung der Literatur nach Typ (Quelle: Eigene Darstellung)

Insgesamt verteilt sich die endgültige für die Forschungsarbeit relevante Literaturauswahl auf 25 Publikationen (PUB-I)[270], die konkret Blockchain-Infrastrukturen zur Vernetzung von Gesundheitsdaten beschreiben, sowie 107 Publikationen (PUB-II)[271], die den Einsatz von Blockchain in der Vernetzung von Gesundheitsdaten allgemein oder in ausgewählten Anwendungsszenarien untersuchen.

Zur Identifikation thematischer Trends in der Literatur wird die Häufigkeit der von den Autoren oder der publizierenden Zeitschrift bzw. des Tagungsbands vergebenen Schlagworte untersucht und in *Abbildung 4-4* zusammengefasst.[272] Um Verzerrungen aufgrund unterschiedlicher Schreibweisen oder Bezeichnungen gleicher bzw. ähnlicher Begriffe zu vermeiden, werden Angleichungen der Schlagworte vorgenommen.[273]

---

[270] Zur Differenzierung der beiden Publikations-Gruppen wird diese Gruppe im Folgenden als PUB-I bezeichnet.

[271] Zur Differenzierung der beiden Publikations-Gruppen wird diese Gruppe im Folgenden als PUB-II bezeichnet.

[272] Die in der Abbildung dargestellte Zahl steht für die Menge an Publikationen, die dieses Schlagwort nutzen. Eine vollständige Liste aller Schlagworte findet sich in *Tabelle C-1* in *Anhang C*.
An dieser Stelle wird darauf hingewiesen, dass nicht jede Publikation eine Stichwortliste zur Verfügung stellt und die in den Abbildungen dargestellten Mengen keinen Anspruch auf Vollständigkeit erheben.

[273] Bsp.: Aus *smart contract* wird *Smart Contracts*. Aus *Cybersecurity* und *Cyber Security* wird *Security*. Darüber hinaus werden die in der Suchphrase verwendeten Begriffe *Blockchain, Health, Healthcare/Health Care* und *Medical* in der Stichwort-Analyse nicht betrachtet.

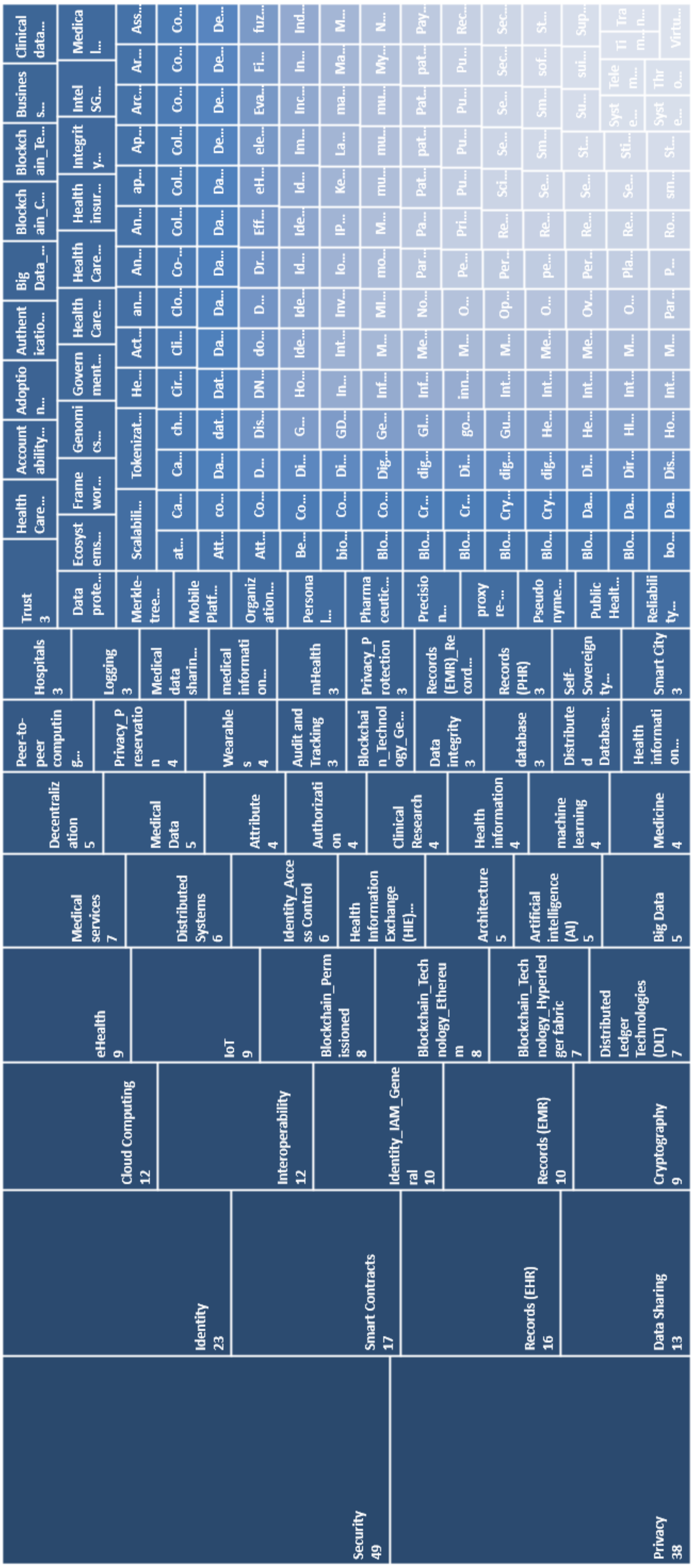


Abbildung 4-4: Analyse der genutzten Schlagworte (Quelle: Eigene Darstellung)

Diese Analyse zeigt, dass ein Fokus der Publikationen auf *Security*, *Privacy* und *Identity* liegt. Darüber hinaus können nicht nur *Electronic Health Records (EHR)*, die nach HAAS den einrichtungsübergreifenden Patientenakten gleichkommen, sondern auch *Electronic Medical Records (EMR)*, die mit institutionsinternen Patientenakten vergleichbar sind, als dominierendes Anwendungsfeld identifiziert werden.[274] Weniger Berücksichtigung scheinen *Personal Health Records (PHR)* zu finden. Bevorzugte Forschungsgebiete sind auf technologischer Seite *Cloud-Computing* und *Internet of Things (IoT)*[275] sowie die gemeinsame Nutzung von Daten (*Data Sharing*) und die Herstellung von *Interoperabilität* durch Blockchain. Auch zeigt sich, dass ein Fokus auf *Permissioned Blockchains* liegt.

Durch Analyse der in *Abbildung 4-4* dargestellten Schlagworte werden thematische Schwerpunkte identifiziert, die Grundlage der zu konzipierenden Referenzarchitektur sind und als Bezeichner der Architektur-Sichten dienen:

i. Aktentyp (engl. *Record Type*)
ii. Datenhaltung und -bereitstellung (engl. *Data Storage & Provisioning*)
iii. Sicherheit (engl. *Security*)
iv. Technologie (engl. *Technology*)

4.3 Zwischenfazit zur groben Literaturanalyse und Schärfung des Forschungsziels

Diese erste Grobanalyse der Literatur zeigt ein vielschichtiges Bild der bisherigen Forschungsbemühungen in der Verwendung der Blockchain-Technologie im Zusammenhang mit Gesundheitsdaten. Die Unterscheidung zwischen PUB-I und PUB-II repräsentiert die unterschiedlichen thematischen Durchdringungsgrade der Publikationen, doch allein schon der Blick in die als PUB-I klassifizierte Literatur zeigt, dass sich derzeit noch kein einheitliches Vorgehen in der Beschreibung von Blockchain-Konzeptionen durchgesetzt hat. So fokussieren sich bspw. AL OMAR ET AL. (2017) auf die Beschreibung von Protokollen und Prozessschritten, beschreiben den technischen Aufbau nachrangig und beschränken sich hier auf allgemeine Ausführungen. Ähnlich widmen sich JIANG ET AL. (2018) vornehmlich den Prozess der Datenspeicherung auf einer Blockchain und eher oberflächlich die konzipierte Architektur. Anders CHANG ET AL.

[274] Vgl. Haas (2017): 55. Erneut wird auf die uneinheitliche Verwendung der Begriffe hingewiesen, die zu einer Verzerrung der hier getätigten Aussage führen kann.

[275] IoT ist *„[...] a set of technologies to enable a wide range of appliances, devices, and objects (or simply "things") to interact and communicate among themselves using networking technologies."* (Tarouco et al. (2012): 6121).

(2018) und AZARIA ET AL. (2016), die ihre Konzeption bereits detaillierter beschreiben und dabei nicht nur die in der Blockchain eingesetzten Smart Contracts beschreiben, sondern auch, welcher Blockchain-Typ und welches Konsensprotokoll verwendet werden sowie, wie eine Verbindung in die Quellsysteme der Leistungsbringer hergestellt wird.

Unter Anwendung der in *Kapitel 4.2* identifizierten thematischen Kategorien ergibt sich die in *Tabelle 4-6* dargestellte Abdeckung.

Tabelle 4-6: Verteilung der PUB-I-Literatur auf Themenkategorien der Literatur-Grobanalyse (Quelle: Eigene Darstellung)

Publikation	Datenhaltung und -bereitstellung	Sicherheit	Technologie
Ahram et al. (2017)	X		X
Al Omar et al. (2017)	X	X	X
Azaria et al. (2016)	X	X	X
Chang et al. (2018)	X	X	X
Du et al. (2018)	X		X
Ekblaw et al. (2016)	X	X	X
Fan et al. (2018)	X	X	
Gropper (2016)	X	X	
Hanley/Tewari (2018)	X	X	X
Ito/Tago/Jin (2018)	X		X
Jiang et al. (2018)	X	X	X
Kuo/Ohno-Machado (2018)	X	X	X
McFarlane et al. (2017)	X	X	X
Medicalchain (2018)	X	X	X
Quaini et al. (2018)	X	X	X
Rouhani et al. (2018)	X	X	X
Staffa et al. (2018)		X	X
Vora et al. (2018)	X	X	X
Xia et al. (2017a)	X	X	X
Xiao et al. (2018)	X	X	X
Yang/Li (2018)	X	X	X
Yue et al. (2016)	X		
Zhang/Lin (2018)	X	X	X
Zhang et al. (2018b)	X	X	X
Zhou/Wang/Sun (2018)	X	X	X
Summe	***24***	***21***	***22***

Die in *Tabelle 4-6* abgebildete Übersicht der Kategorien berücksichtigt noch nicht den Detailgrad der Beschreibung, zeigt aber bereits, dass nicht jede Publikation einen vollständigen Überblick über eine potentielle Blockchain-Architektur liefert. Selbst innerhalb der Kategorien ergeben sich Unterschiede. So werden bspw. in *Datenhaltung und -bereitstellung* von HANLEY/TEWARI (2018) Themen wie Möglichkeiten der Datenspeicherung auf der Blockchain,

Datenbereitstellung durch Gatekeeper sowie die eigentliche Datenhaltung in den Leistungserbringereinrichtungen diskutiert, während JIANG ET AL. (2018) sich auf die Möglichkeiten der Datenspeicherung auf der Blockchain beschränkt. Gleiches gilt in der *Sicherheit*. VORA ET AL. (2018) formulieren ihre Beschreibungen sehr allgemein und beschränken sich auf Identity-Management und die Verwendung von multiplen Identitäten sowie auf die Verwendung der Blockchain als Logging- bzw. Audit-Instrument. Dem gegenüber stehen ZHANG ET AL. (2018B), die sich mit Themen wie der Verwendung von potentiellen Zugriffsmethoden (bspw. Role-Based-Access-Control) sowie Infrastrukturthemen (PKI) und dazugehörigen Authentifizierungsmechanismen (z.B. asymmetrische Schlüsselpaare) auseinandersetzen. Der Blick auf die *Technologie* zeigt Ähnliches. ZHOU/WANG/SUN (2018) benennen konkret die anzuwendende Blockchain-Technologie (Ethereum), während sich STAFFA ET AL. (2018) auf die Blockchain-Taxonomy (*Private-Permissioned*) beschränken und DU ET AL. (2018) überhaupt keine Angaben zur Technologie machen.

Diese Diskrepanz der in der Literatur zu findenden Informationen aufzulösen und einen umfänglichen Blick auf mögliche Architekturen zu geben, ist Ziel dieser Forschungsarbeit. Dabei sollen die bereits existierenden Erkenntnisse aggregiert und Schwerpunkte identifiziert werden. Ergebnis wird eine Referenzarchitektur sein, die mit der zusätzlichen Darstellung von Variationspunkten Architekten und Entwicklern Unterstützung in der Konzeption neuer Lösungen bietet. Darüber hinaus wird ein Entscheidungsmodell entwickelt, das die Entscheidungen der diversen Autoren aggregiert und eine Einschränkung der tatsächlich für einen Anwendungsfall relevanten Variationspunkte erlaubt.

Eine detaillierte Analyse der Kategorien findet im Verlauf der Referenzarchitektur-Konstruktion ab *Kapitel 6* statt. Mangels einheitlicher Definition und Nutzung der Begriffe *Referenzarchitektur (RA)*[276] und *Referenzmodell (RM)* werden im folgenden Kapitel definitorische Abgrenzungen vorgenommen und diesbezüglich etablierte Forschungsmethoden beschrieben, die in der weiteren wissenschaftlichen Analyse angewendet wird.

[276] Vgl. Fettke/Loos (2004): 332; Reidt/Pfaff/Krcmar (2018): 895.

5 Forschungsmethodik zur Konstruktion von Referenzarchitekturen

5.1 Terminus Referenzmodell

Bereits die sprachliche Trennung des Begriffs *Referenzmodell* in *Referenz* und *Modell* zeigt dessen Ziel, nämlich die glaubwürdige und allgemeingültige Repräsentation einer *„Klasse von Anwendungsfällen"*[277].[278]

Die in *Tabelle 5-1* genannten Definitionen eines Referenzmodells behandeln den Terminus in unterschiedlicher Granularität. Die von BROCKE formulierte Definition ist dabei die differenziertere und enthält gemeinsame Elemente der Definitionen von SCHÜTTE und ALPAR ET AL.

Tabelle 5-1: Drei Definitionen eines Referenzmodells (Quelle: Eigene Darstellung)

Autor(en)	Definition
Schütte (1998): 70	„Referenzmodelle sind Typisierungen möglicher (denkbarer) Originale."
Brocke (2015): 64	„Ein Referenzmodell (ausführlich: Referenz-Informationsmodell) ist ein Informationsmodell, das Menschen zur Unterstützung der Konstruktion von Anwendungsmodellen entwickeln oder nutzen, wobei die Beziehung zwischen Referenz- und Anwendungsmodell dadurch gekennzeichnet ist, dass Gegenstand oder Inhalt des Referenzmodells bei der Konstruktion des Gegenstands oder Inhalts des Anwendungsmodells [wiederverwendet] werden."
Alpar et al. (2019): 197	„Ein Referenzmodell ist ein Informationsmodell, dessen Inhalt bei der Entwicklung von Anwendungsmodellen wiederverwendet werden kann."

Referenzmodelle beschreiben im Gegenstandsbereich bereits bekannte Fakten und beruhen auf wissenschaftlich beobachtbaren Erkenntnissen, die als theoretische Konstrukte formuliert werden und entsprechend der in *Tabelle 5-2* dargestellten Kategorien unterschieden werden.[279]

Tabelle 5-2: Referenzmodell Varianten (Quelle: Eigene Darstellung in Anlehnung an Fettke/Loos (2004): 332f.)

Referenzmodell als …	Beschreibung
Terminologischer Apparat	Herleitung einer terminologischen Konzeption, vergleichbar mit der Bildung von Ontologien.
Menge singulärer Aussagen	Beschreibung von konkreten, bestehenden Modellen und Aggregation singulärer Aussagen in ein übergeordnetes Modell. Modellierung entweder auf sprachlicher Ebene oder durch Bereitstellung von Prozessen.

[277] Schütte (1998): 70.

[278] Vgl. Schütte (1998): 70f.

[279] Vgl. Fettke/Loos (2004): 332. Statt des Begriffes *Inhaltsbereich*, verwenden FETTKE/LOOS die Bezeichnung *Aussagenbereich*.

Menge genereller Aussagen	Beschreibung von konkreten, bestehenden Modellen und Aggregation singulärer Aussagen in ein übergeordnetes Modell ohne Beschränkung auf ein konkretes Unternehmen.
Technik	Werkzeugkasten zur Konstruktion von Informationssystemen, dessen Effizienz von der WI untersucht wird.
Menge normativer Aussagen	Darstellung von Regeln und Maßstäben, die in der Konstruktion eingehalten werden sollten.

Referenzmodelle bieten folglich Modellierern Unterstützung in der Konzeption neuer Modelle und schaffen bei Anwendung wirtschaftliche und wissenschaftliche Vorteile. Konstruktionsprozesse können mithilfe vorhandenen Expertenwissens systematisiert, durch Wiederverwendung effizient durchgeführt und in der Wissenschaft als Basis zur Ableitung neuer Erkenntnisse oder Theorien genutzt werden.[280]

5.2 Terminus Referenzarchitektur

REIDT/PFAFF/KRCMAR definieren auf Grundlage einer Literaturanalyse *Referenzarchitekturen* als

> *„[…] eine abstrakte Architektur, die den Menschen die Entwicklung von Systemen, Lösungen und Applikationen erleichtern soll, indem sie Wissen bereitstellt und einen Rahmen zur Entwicklung vorgibt. Die Beziehung zwischen Referenzarchitektur und konkreter Architektur ist dadurch gekennzeichnet, dass Gegenstand oder Inhalt der Referenzarchitektur bei der Konstruktion der konkreten Architektur des jeweiligen zu entwickelnden Systems (wieder-)verwendet werden. Die Referenzarchitektur besitzt einen technischen Fokus, verbindet diesen jedoch mit dem dazugehörigen Fachwissen der jeweiligen Domäne. Sie bildet durch ihre Ausprägung und ihren Inhalt ein gemeinsames Rahmenwerk, um das detaillierten Diskussionen aller bei der Entwicklung beteiligten Stakeholder geführt werden können.“*[281]

Diese Definition ähnelt der zitierten Definition des *Referenzmodells* von BROCKE aus *Kapitel 5.1*, ergänzt diese allerdings um technische Aspekte. *Abbildung 5-1* zeigt die hierarchische Positionierung von RA im Rahmen von Implementierungs-Konstruktionen und die möglichen Inhalte einer Referenzarchitektur, zu denen auch Referenzmodelle gehören.[282]

---

[280] Vgl. Brocke/Buddendick (2004): 341; Brocke (2015): 67.

[281] Reidt/Pfaff/Krcmar (2018): 903.

[282] Vgl. Reidt/Pfaff/Krcmar (2018): 903f. Gleichzeitig weisen die Autoren darauf hin, dass ein Referenzmodell nicht in jedem Fall einer Referenzarchitektur untergeordnet wird, sondern, dass Referenzmodelle auch Teil einer Architektur sein können.

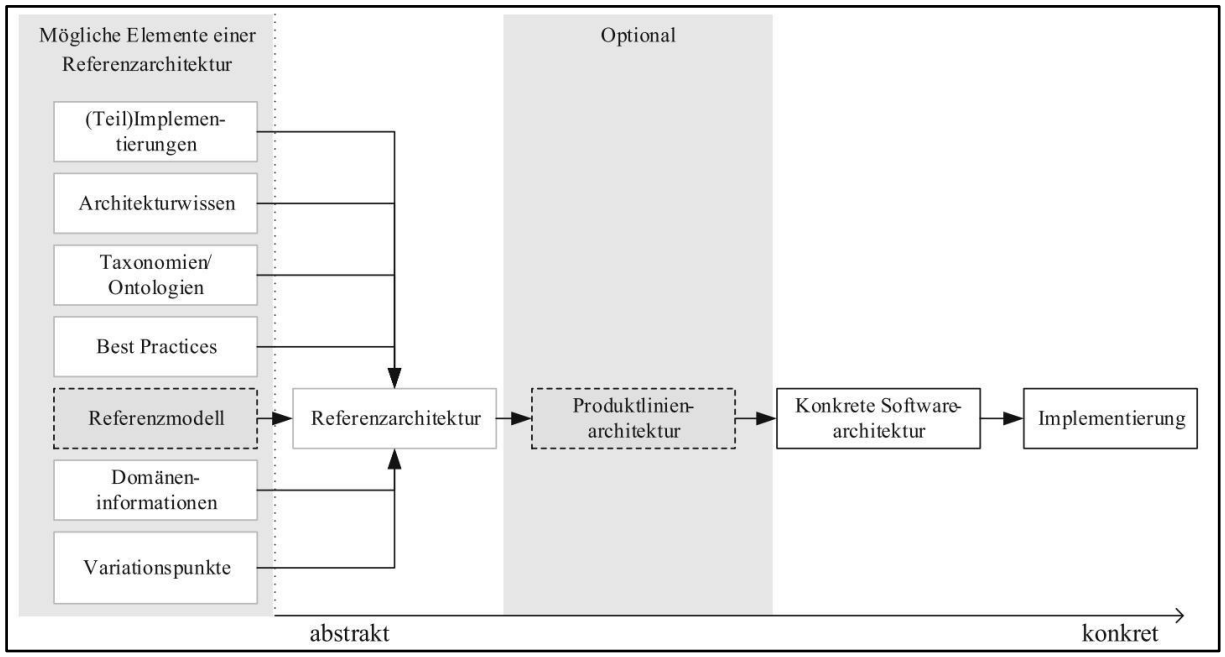


Abbildung 5-1: Abstraktionsniveau und Architekturhierarchie von Referenzarchitekturen[283] (Quelle: Reidt/Pfaff/Krcmar (2018): 904)

REIDT/PFAFF/KRCMAR identifizieren in ihrer Analyse diverse Charakteristiken, deren unterschiedliche Ausprägungen die Vielfältigkeit von RA unterstreichen. Dabei wird unterschieden zwischen:[284]

i. *Abstraktionsgrad*

   Der Abstraktionsgrad ist abhängig von der geplanten Nutzung. So existieren Arbeiten, die eine Architektur als Informationsmittel zur allgemeinen Darstellung von Zusammenhängen und als Basis zur individualisierten Umsetzung sehen, genauso wie es Arbeiten gibt, die einen Standard definieren und folglich durch einen niedrigen Abstraktionsgrad eine individualisierte Umsetzung nahezu unterbinden.[285]

ii. *Technologieneutralität*

   In der Regel wird in einer RA keine Technologie bevorzugt behandelt, jedoch kommt es hier ebenfalls auf den Einsatz bzw. den Abstraktionsgrad an. Entsprechend können Architekturen auch auf Basis einer bestimmten Technologie konstruiert werden oder Empfehlungen zum Einsatz bestimmter Technologien geben. Dabei muss dies nicht die gesamte RA betreffen, sondern gegebenenfalls auch nur einzelne Teilbereiche.[286]

---

[283] Die in der Grafik genannte Produktlinienarchitektur ist der branchenbezogenen und inhaltlichen Ausrichtung der Literaturquelle geschuldet und hier nicht relevant.

[284] Vgl. Reidt/Pfaff/Krcmar (2018): 899-903.

[285] Vgl. Reidt/Pfaff/Krcmar (2018): 900.

[286] Vgl. Reidt/Pfaff/Krcmar (2018): 900f.

iii. *Industriefokus*

Diese Eigenschaft beschreibt, ob eine RA branchenübergreifend oder branchenbezogen konzipiert wird.[287]

iv. *Produktfokus*

Für diese Eigenschaft wird unterstellt, dass RA die Produktion eines fertigen oder eines teilweise fertigen Produkts ermöglichen. Darüber hinaus existieren RA, die für mehrere unterschiedliche Produkte eingesetzt werden können.[288]

v. *Unternehmensfokus*

Ähnlich (iii) und (iv) beschreibt diese Eigenschaft, ob eine RA ausschließlich für ein Unternehmen konzipiert ist oder je nach Abstraktionsgrad auch Anwendung in anderen Unternehmen finden kann.[289]

vi. *Referenzcharakter*

Der Referenzcharakter beschreibt die Allgemeingültigkeit, die gegeben ist, wenn eine Architektur als Standard betrachtet werden kann. Gültigkeit kann entweder durch allgemeine Anerkennung der jeweiligen Stakeholder definiert werden oder durch eine abstrahierende Beschreibung bestehender Konzepte. Je detaillierter eine Referenzarchitektur ist und je mehr Best-Practice-Beschreibungen enthalten sind, desto eher hat eine Referenzarchitektur einen Empfehlungscharakter und konkrete Bezugspunkte für neue Entwicklungen.[290]

vii. *Variationspunkte*

Das Vorhandensein von Variationspunkten beschreibt mögliche Konfigurationen in der Anwendung der RA, die einem Architekten in der Konzeption der Ergebnisarchitektur Abweichungen vom Standard ermöglichen.[291]

viii. *Technischer Fokus*[292]

Der technische Fokus geht über die in (ii) dargestellte Technologieneutralität hinaus und definiert, ob eine RA rein technischer Natur ist oder zusätzliche fachkonzeptionelle Informationen enthalten sind.[293]

---

287 Vgl. Reidt/Pfaff/Krcmar (2018): 901.

288 Vgl. Reidt/Pfaff/Krcmar (2018): 901.

289 Vgl. Reidt/Pfaff/Krcmar (2018): 901.

290 Vgl. Reidt/Pfaff/Krcmar (2018): 901f.

291 Vgl. Reidt/Pfaff/Krcmar (2018): 902.

292 Die Autoren haben diese Charakteristik als *Technisch Fokus* bezeichnet. Das erste Wort weist offensichtlich einen Rechtschreibfehler auf und wird folglich in dieser Dissertation als *Technischer Fokus* bezeichnet.

293 Vgl. Reidt/Pfaff/Krcmar (2018): 902.

ix. *Vollständigkeit*

Das Merkmal der Vollständigkeit unterscheidet, ob eine RA einen Bereich vollständig oder unvollständig beschreibt. Unvollständige RA können invariante Komponenten enthalten, deren Variationspunkte entweder offengehalten oder eindeutig definiert werden.[294]

x. *Praxis- oder Forschungsgetrieben*

Diese Eigenschaft unterscheidet, ob eine RA aus vorhandenem Domänenwissen der Praxis stammt und somit praxisgetrieben oder für die weiterführende Forschung konzipiert ist.[295]

Auf Basis dieser Charakteristiken entwickelt REIDT das in *Tabelle 5-3* dargestellte Klassifikationsschema.

Tabelle 5-3: Klassifikationsschema Referenzarchitekturen[296] (Quelle: Reidt (2019): 31)

Charakteristik	**Ausprägung**		
Abstraktionsgrad	Detailliert (Codebasis)	Mischform	Abstrakt
Technologieneutralität	Ja	Teilweise	Nein
Industriefokus	Industriespezifisch	Industrieübergreifend	
Produktfokus	Fokus auf ein Produkt	Produktfamilie	Produktübergreifend
Unternehmensfokus	Unternehmensspezifisch	Unternehmensübergreifend	
Referenzcharakter	Bezugspunkt	Allgemeingültigkeit	Empfehlungscharakter
Variationspunkte	Enthalten	Nicht enthalten	
Technischer Fokus	Rein technisch	Technisch mit Domäneninformationen	
Vollständigkeit	Vollständig	Unvollständig	
Praxis- oder Forschungsgetrieben	Praxis	Forschung	
Ziel	Standardisierung	Erleichterung	
Vorgehensweise	Induktiv	Kombination	Deduktiv
Enthaltenes Wissen	Architekturwissen	Softwareelemente	Richtlinien
	Weiteres Wissen:		

294 Vgl. Reidt/Pfaff/Krcmar (2018): 902f.

295 Vgl. Reidt/Pfaff/Krcmar (2018): 899f.

296 *Anmerkung:* Die Original-Abbildung wird hier als Tabelle nachgestellt und ist folglich nicht im gleichen Format und der gleichen farblichen Gestaltung im Vergleich zur Original-Abbildung. Eine inhaltliche Veränderung, außer einer redaktionellen Änderung, wurde nicht vorgenommen. In der ursprünglichen Darstellung wird der Begriff *Technisch Fokus* genutzt. Da dieser Begriff im Text grammatikalisch korrekt genutzt wird (*„Technischer Fokus"* (Reidt/Pfaff/Krcmar (2018): 902)), wird in dieser Darstellung, wie auch im Fließtext, eine entsprechende redaktionelle Änderung vorgenommen.

Den Punkten (i) bis (x) werden die drei Aspekte *Ziel, Vorgehensweise* und *Enthaltenes Wissen* hinzugefügt. Während das *Ziel* unterscheidet, ob eine RA Standardisierung oder künftige (Konstruktions-)Erleichterung verfolgt,[297] beschreibt die *Vorgehensweise*, wie die Konstruktion einer RA erfolgt ist.[298] Die Charakteristik *Enthaltenes Wissen* ist auf die RA-Definitionsfindung zurückzuführen, in deren Ausarbeitung REIDT/PFAFF/KRCMAR bereits auf BASS/CLEMENTS/KAZMAN[299] und VOGEL ET AL.[300] verweisen, deren entsprechende Äußerungen bspw. zu Architekturwissen und Softwareelementen bereits in *Abbildung 5-1* als Elemente einer RA genannt werden.

5.3 Exkurs: Informationssystem-Architektur versus Softwarearchitektur

Die Inhalte des vorangegangenen *Kapitels 5.2* fokussieren auf die Konzeption von Referenzarchitekturen bezogen auf Softwarearchitekturen. Aus diesem Grund wird in diesem Exkurs eine Differenzierung der Begriffe *Softwarearchitektur* und *Informationssystemarchitektur* vorgenommen, da letztgenanntes im Fokus der Wirtschaftsinformatik steht und die sozioökonomische Betrachtung von Informationssystemen über die reine Software hinausgeht. Trotz dieser Differenzierung werden beide Begriffe in der Literatur teils synonym genutzt, wie bspw. an den Ausführungen zu *Informationssystemarchitekturen* durch DÜNNEBEIL ET AL. zu erkennen ist, deren Einführung das Thema *Informationssystemarchitekturen* anreißt, dann jedoch ohne eine thematische Überleitung in *Softwarearchitekturen* übergeht.[301]

Eine *Informationssystemarchitektur* (IS-Architektur), alternativ auch *Enterprise Architecture* (EA) genannt, schließt neben der technischen Umsetzung fachliche Aspekte einer Architektur mit ein und erlaubt die Unterteilung in mehrere Einzelarchitekturen. KRCMAR stellt dies in Form eines Kreisel-Modells dar (siehe *Abbildung 5-2*), dessen Kern eine Informationssystem-Strategie ist, an der sich alle anderen Architekturkomponenten orientieren.[302]

---

297 Vgl. Reidt/Pfaff/Krcmar (2018): 898.

298 Vgl. Reidt (2019): 31.

299 *„A reference architecture is a reference model mapped onto software elements (that cooperatively implement the functionality defined in the reference model) and the data flows between them. Whereas a reference model divides the functionality, a reference architecture is the mapping of that functionality onto a system decomposition."* (Bass/Clements/Kazman (2010): 25).

300 *„Referenzarchitekturen kombinieren allgemeines Architektur-Wissen und allgemeine -Erfahrung mit spezifischen Anforderungen zu einer architektonischen Gesamtlösung für einen bestimmten Problembereich. Sie dokumentieren die Strukturen des Systems, die wesentlichen Systembausteine, deren Verantwortlichkeiten und deren Zusammenspiel."* (Vogel et al. (2009): 254).

301 Vgl. Dünnebeil et al. (2013): 6f.

302 Krcmar bezieht dabei den Umstand mit ein, dass sich Strategie und IS bedingen. Einerseits unterstützen IS die Erfüllung der Unternehmensstrategie (*align*), können andererseits aber auch Grundlage für die Ausgestaltung einer Unternehmensstrategie (*enable*) sein (vgl. Krcmar (2015): 396).

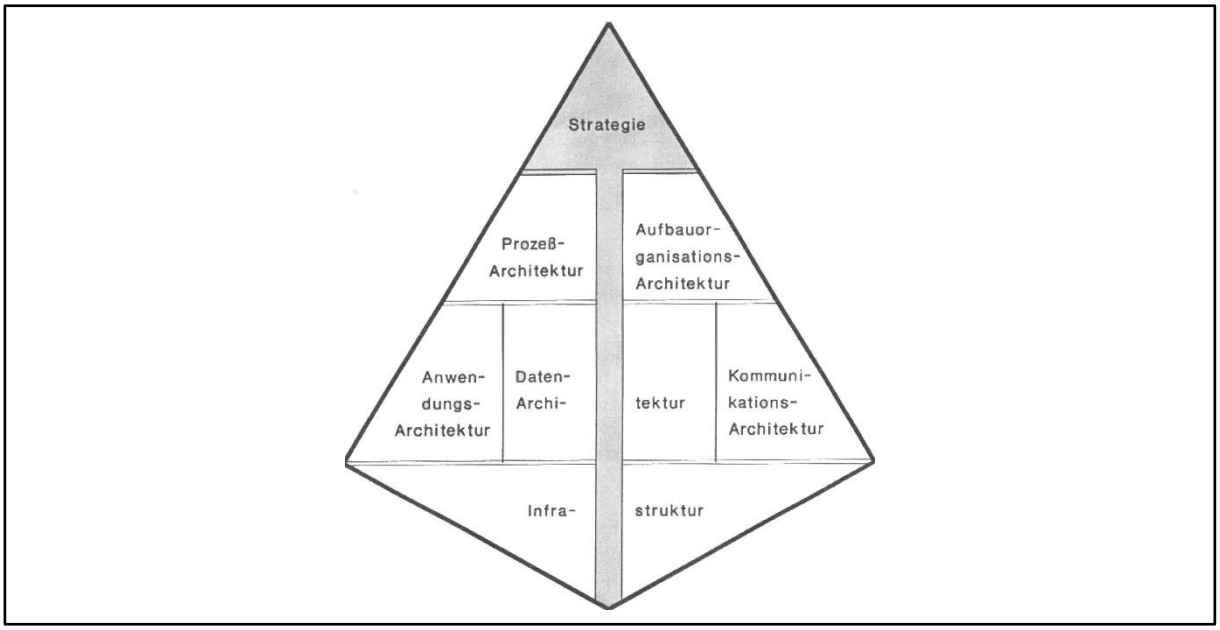


Abbildung 5-2: Ganzheitliches Modell der Informationssystem-Architektur (Quelle: Krcmar (1990): 399)

In der obersten Ebene, der Spitze des Kreiselmodells, ist die verfolgte Strategie verortet, die Grundlage für eine IS-Architektur ist und den Rahmen vorgibt.[303] Die Ebene darunter beschäftigt sich mit den organisatorischen Anforderungen,[304] während Ebene 3 technischer Natur ist. Hier werden neben den notwendigen Daten auch Anwendungsarchitekturen betrachtet und die Kommunikation zwischen den einzelnen Komponenten eines Systems.[305] Ebene 4 beschreibt die tatsächlich genutzten Technologien.[306] Diesen Ebenen ergänzen AIER/WINTER eine als *Alignment* bezeichnete Ebene. Aufgabe dieser ist die virtuelle Bereitstellung von Diensten zur flexiblen, entkoppelten Übersetzung fachlicher bzw. strategischer Anforderungen an eine zumeist starr orientierte IT-Infrastruktur.[307]

Auch WINTER/FISCHER unterteilen Informationssystem-Architekturen in fünf Bereiche:[308]

i. *Business Architecture*
   Ähnlich der Ebenen 1 und 2 in *Abbildung 5-2* beschreibt *Business Architecture* die verfolgte Unternehmensstrategie und den Aufbau der Geschäftstätigkeiten.
ii. *Process Architecture*
   Konkreter als Business Architecture beschreibt dieser Bereich sämtliche Prozesse und

303 Vgl. Krcmar (1990): 399.
304 Vgl. Krcmar (1990): 399.
305 Vgl. Krcmar (1990): 400.
306 Vgl. Krcmar (1990): 400.
307 Vgl. Aier/Winter (2009): 178, 180.
308 Vgl. Winter/Fischer (2006): 30.2.

die Aufbau- und Ablauforganisation von Unternehmungen und ist mit Ebene 2 in *Abbildung 5-2* vergleichbar.

iii. *Integration Architecture*
An dieser Stelle werden sämtliche Komponenten der Informationssysteme organisiert (Ebene 3 aus *Abbildung 5-2*).

iv. *Software Architecture*
Auch dieser Bereich kann Ebene 3 aus *Abbildung 5-2* zugewiesen werden, beschränkt sich jedoch auf die reine Organisation von Software und deren Erstellung.

v. *Infrastructure Architecture*
Dieser Bereich organisiert die einem Informationssystem zugrundeliegende (technische) Infrastruktur (ähnlich Ebene 4 aus *Abbildung 5-2*).

Software-Architekturen (SA) sind entsprechend den Ausführungen von PERRY/WOLF

> *"[…] architectural elements of data, processing, and connection, highlights their relationships and properties, and captures constraints on their realization or satisfaction."*[309]

und decken im Vergleich zu den in *Abbildung 5-2* dargestellten Ebenen einer IS-Architektur allein Ebene 3 ab. Ähnlich definieren BRUNS/DUNKEL SA als

> *„[…] übergeordnete Struktur[en] eines Softwaresystems und deren globale Kontrollstrukturen. Sie [beschreiben] die wesentlichen Softwarebausteine in Form von Komponenten und [legen] fest, wie diese interagieren und kooperieren."* [310]

Im direkten Vergleich der beiden SA-Definitionen mit den Ausführungen von KRCMAR und WINTER/FISCHER zu ISA wird ersichtlich, dass die Unterschiede zwischen ISA und SA gering sind und der Unterschied im abgebildeten Umfang der Architektur zu finden ist. So haben Softwarearchitekturen keinen strategischen Einfluss auf die Ausgestaltung der sie limitierenden Rahmenbedingungen,[311] wohingegen IS-Architekturen auch Infrastrukturentscheidungen darstellen können. Aus diesem Grund bilden Software-Architekturen eine Teilmenge von IS-Architekturen.[312] Mit Blick auf die in dieser Forschungsarbeit geplante Referenzarchitektur ist damit der Fokus auf ISA zu richten, da die Architektur aufgrund der zu definierenden Strategie,

---

309 Perry/Wolf (1992): 51.

310 Bruns/Dunkel (2010): 202.

311 Vgl. Bass/Clements/Kazman (2010): 34. In diesem Zusammenhang wird, bezugnehmend auf SA, auf das *4+1 View Model* von KRUCHTEN verwiesen, das die Grundstruktur von SA beschreibt und dessen detaillierte Beschreibung der Originalquelle zu entnehmen ist (vgl. Kruchten (1995): 43-47).

312 Vgl. Winter/Fischer (2006): 30.2; Dern (2009): 21f.

abhängig von der Wahl des zu konzipierenden Aktentyps, einen übergreifenden Ansatz verfolgt und sich nicht ausschließliche auf Ebene 3 der ISA beschränkt. Darüber hinaus werden Technologien diskutiert und Prozesse (siehe Smart Contracts) in die Betrachtung mit einbezogen.

5.4 Methoden zur Entwicklung von Referenzarchitekturen

Basis von RA ist die Repräsentation bereits vorhandenen Wissens in abstrakter Form.[313] Dabei werden in bestehenden Architekturen Mustern (engl. *pattern*) identifiziert, die sich in der Praxis bewährt haben.[314] Doch spätestens, wenn Architekturen auf neuen Technologien basieren, gestaltet sich die Identifikation von Muster schwierig bis unmöglich.[315] Aus diesem Grund wird in der Forschung zwischen *practice-driven* und *research-driven* unterschieden. *Practice-driven* beschreibt dabei die Nutzung unterschiedlicher, bestehender und bereits als effektiv eingestufter Architekturen zur Konstruktion von RA, während *research-driven* den Fokus auf Forschungsbemühungen eines abgestimmten Anwendungsbereichs richtet und auf Basis beschriebener Konzepte eine RA ermittelt.[316]

Das von CLOUTIER ET AL. dargestellte Vorgehen zur Konzipierung einer RA beschreibt einen sehr allgemein formulierten, insbesondere *practice-driven*-orientierten Ansatz (siehe *Abbildung 5-3*). Dabei werden unter Anwendung eines iterativen Prozesses bestehende Architekturen und Dokumentationen impliziten und expliziten Wissens genutzt.[317]

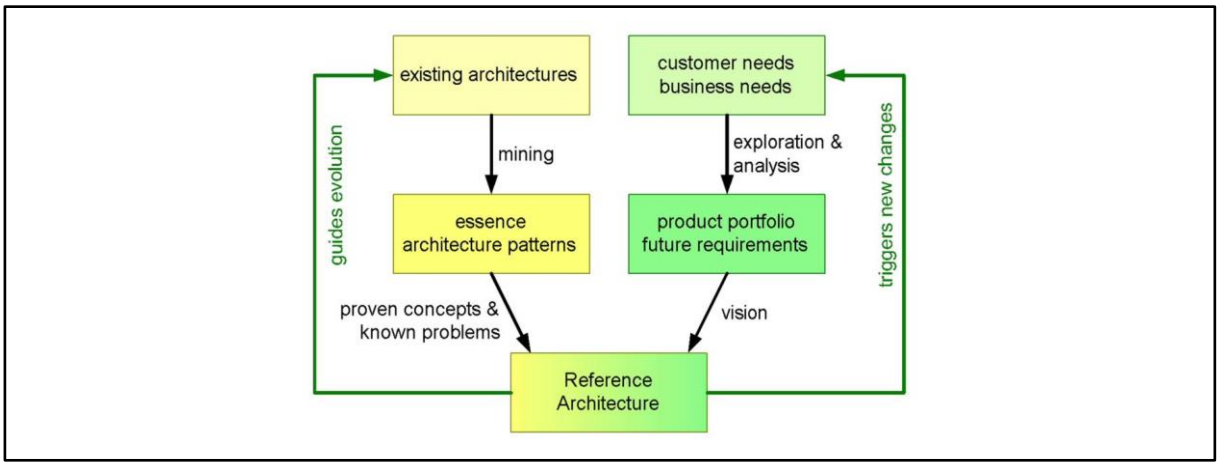


Abbildung 5-3: Inputs of a Reference Architecture (Quelle: Cloutier et al. (2009): 21)

313 Vgl. Muller/van de Laar (2011): 109.

314 Vgl. Cloutier et al. (2009): 21. In der Regel wird von einem Muster ausgegangen, wenn eine Beschreibung mindestens dreimal aufzufinden ist.

315 Vgl. Cloutier et al. (2009): 20.

316 Vgl. Galster/Avgeriou (2011): 154f.

317 Vgl. Cloutier et al. (2009): 22.

GALSTER/AVGERIOU weisen auf die fehlende Empirie in der Referenzarchitekturforschung (RA-Forschung) hin und konzipieren alternativ zu CLOUTIER ET AL. ein Vorgehensmodell in sechs Schritten (siehe *Tabelle 5-4*).

Tabelle 5-4: Konstruktionsmodell Referenzarchitekturen (Quelle: Eigene Darstellung in Anlehnung an Galster/Avgeriou (2011): 154-156)

Schritt	Beschreibung
Schritt 1	**Decision on Type of RA** Die Zielsetzung der RA wird definiert und unterschieden in einer Kombination aus den Dimensionen *usage context* und *characterization*.
Schritt 2	**Selection of Design Strategy** Es wird zwischen der Entwicklung von RA auf Basis mehrerer bestehender Architekturen oder der Konzeption einer absolut neuen Architektur unterschieden. Dabei wird zwischen *practice-* und *research-driven* unterschieden.
Schritt 3	**Empirical Acquisition of Data** Zur Gestaltung einer RA werden entsprechend den in Schritt 1 gewählten Dimensionskategorien relevante Daten und Informationen zusammengestellt. Dabei können bspw. bestehende Prozessdokumentationen oder bereits beschriebene Architekturen identifiziert werden. Im Falle von komplett neu entwickelten Architekturen können auch Interviews eine Ausgangslage für die Konstruktion darstellen.
Schritt 4	**Construction of RA** Die Konstruktion von RA wird auf Basis der in Schritt 3 identifizierten Daten erstellt. Dabei können Themenblöcke identifiziert, an denen sich die Architektur orientiert. Die Strukturierung einer RA kann in Sichten entsprechend ISO/IEC 42010 durchgeführt werden. Auch sollten dabei nicht nur technische Informationen dargestellt werden, sondern auch Informationen zum Geschäft und zu den Kunden enthalten. Ergänzend werden auch Qualitätskriterien in die Konstruktion miteinbezogen.
Schritt 5	**Enabling RA with Variability** Variationen sind für die Konstruktion relevant und können entweder durch Darstellung von Anpassungsmöglichkeiten in Sichten oder Modellen konstruiert oder durch Anmerkungen sichtbar werden.
Schritt 6	**Evaluation of the RA** Die konstruierte RA wird in der Praxis getestet. Dabei wird nicht nur die Passgenauigkeit geprüft, sondern auch, ob die RA einen tatsächlichen Nutzen mit sich bringt. Je stärker eine RA eine Neuschöpfung ist, desto relevanter ist eine Evaluation. Dies birgt jedoch auch das Problem, dass besonders die Betrachtung (disruptiver) Technologien die Evaluation erschwert.

Anmerkung: Tiefergehende Informationen und ergänzende Nachweise finden sich in der Originalquelle.

Ähnlich beschreiben NAKAGAWA ET AL. eine auf vier Schritte reduzierte Konstruktionsprozedur, genannt *ProSA-RA* (siehe *Abbildung 5-4*),[318] die die ersten beiden Schritte von GALSTER/AVGERIOU auslässt. Im *ersten* Schritt werden sämtliche Informationen zusammengetragen, sodass neben Software- und Domänen-Wissen auch Inhalte aus wissenschaftlichen, themenbezogenen Publikationen und bestehenden Architekturen einbezogen werden. Der *zweite* Schritt definiert auf Basis der Erkenntnisse des ersten Schritts nicht nur Bedarfe von Systemen

[318] Vgl. Nakagawa et al. (2014): 144-148.

und RA, sondern auch domänenspezifische Rahmenbedingungen. In Schritt *drei* werden sämtliche Erkenntnisse in die Konstruktion übernommen[319] und anschließend im *vierten* Schritt evaluiert.

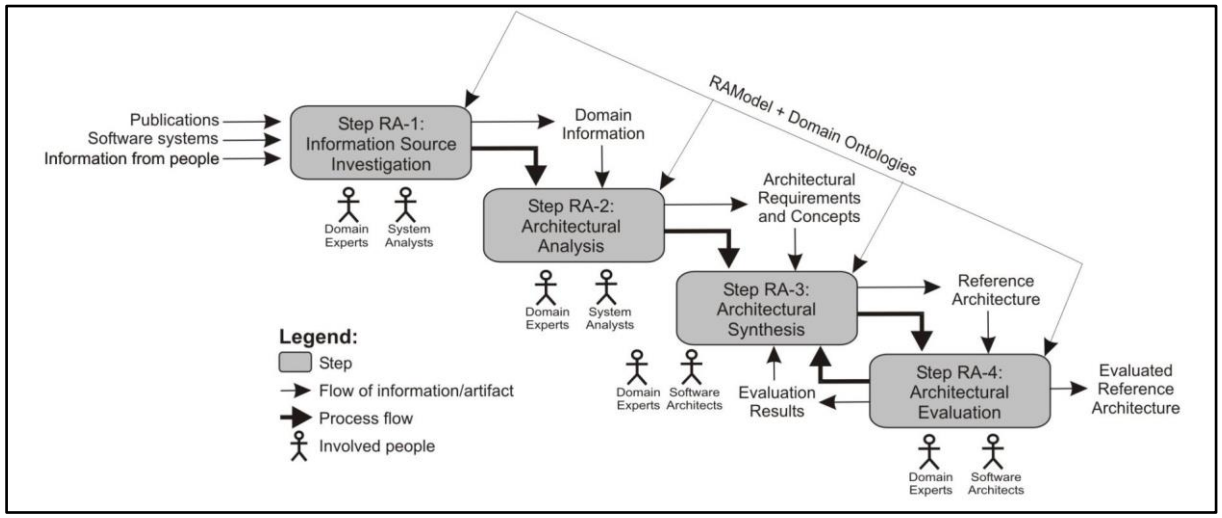


Abbildung 5-4: Referenzarchitektur-Modell ProSA-RA (Quelle: Nakagawa et al. (2014): 145)

5.5 Verwendete Methodik und Design-Entscheidungen zur Referenzarchitektur-Modellierung

Basis der Methodenauswahl ist das in *Kapitel 5.2* vorgestellte Klassifikationsschema, dessen Felder in *Tabelle 5-5* entsprechend der Zielsetzung in dieser Forschungsarbeit dunkelgrau hervorgehoben werden und das die Ziele bzw. Absichten der RA definiert.

Tabelle 5-5: Eigenschaften der Referenzarchitektur in der Forschungsarbeit (Quelle: Eigene Darstellung in Anlehnung an Reidt (2019): 31)

Charakteristik	**Ausprägung**		
Abstraktionsgrad	Detailliert (Codebasis)	Mischform	Abstrakt
Technologieneutralität	Ja	Teilweise	Nein
Industriefokus	Industriespezifisch	Industrieübergreifend	
Produktfokus	Fokus auf ein Produkt	Produktfamilie	Produktübergreifend
Unternehmensfokus	Unternehmensspezifisch	Unternehmensübergreifend	
Referenzcharakter	Bezugspunkt	Allgemeingültigkeit	Empfehlungscharakter
Variationspunkte	Enthalten	Nicht enthalten	
Technisch Fokus	Rein technisch	Technisch mit Domäneninformationen	
Vollständigkeit	Vollständig	Unvollständig	

[319] Die Autoren verweisen im Rahmen der Konstruktion auf das von NAKAGAWA/OQUENDO/BECKER (2012) entwickelte Referenzmodell zur Konstruktion von Referenzarchitekturen (*RAModel*). Dieses Modell wird an dieser Stelle nicht weiter erörtert, der Vollständigkeit halber aber genannt.

Praxis- oder Forschungsgetrieben	Praxis	Forschung	
Ziel	Standardisierung	Erleichterung	
Vorgehensweise	Induktiv	Kombination	Deduktiv
Enthaltenes Wissen	Architekturwissen	Softwareelemente	Richtlinien
	Weiteres Wissen:		

Die zu konzipierende RA ist **abstrakt** gehalten und stellt die Erkenntnisse der in der Literaturanalyse (*Kapitel 4*) identifizierten Publikationen zusammen.[320] Eine Darstellung auf Code-Ebene wird nicht gewählt.

Die **Technologieneutralität** wird bereits durch den Fokus auf die Blockchain-Technologie negiert, doch erlaubt eine Unterscheidung in die unterschiedlichen Blockchain-Technologien, wie Ethereum oder Hyperledger. Der technische Fokus wird um Domänenwissen ergänzt und zielt auf die konkrete Anwendung im Gesundheitswesen.

Die Referenzarchitektur wird **Variationspunkte** enthalten, da nicht jede Blockchain-Technologie die gleichen Anforderungen aufweist. Allerdings wird die Liste der Variationspunkte nicht abschließend sein, sodass die konzipierte RA als **unvollständig** bezeichnet wird.

Der **Industriefokus** ist aufgrund des besonderen Schutzbedarfs von Gesundheitsdaten industriespezifisch auf das Gesundheitswesen und explizit auf die **Produktfamilie** Patientenakten (EHR, PHR, u.a.) beschränkt. Die Betrachtung unternehmens- bzw. einrichtungsübergreifender Akten führt überdies zur Definition eines **unternehmensübergreifenden Unternehmensfokus**.

Ziel der Referenzarchitektur ist im Sinne des Klassifikationsschemas eine Empfehlung auszusprechen und einen Bezugspunkt darzustellen (Referenzcharakter), statt eine Standardisierung vorzunehmen.

Bisher hat die Blockchain-Technologie nicht den Weg in die Praxis gefunden, höchstens in Form von Fallstudien[321] oder als kommerzielles Produkt bzw. als Unterstützungstechnologie

[320] Die detaillierte Analyse der Literatur wird in *Kapitel 6* vorgenommen.

[321] *MedRec* ist die einzige in der Literaturanalyse identifizierte Fallstudie zur Evaluation der Blockchain-Konzeption (siehe Ekblaw et al. (2016)).

eines Geschäftsmodells[322]. Dieser fehlende Einsatz in der Praxis definiert die RA als **forschungsgetrieben**.[323]

Die RA wird mittels **induktiver Methoden** konstruiert. Bestehende Architektur-Beschreibungen sowie Beschreibungen von Teilbereichen werden in die Analyse mit einbezogen (induktiv).[324]

Bei der Konstruktion der in dieser Forschungsarbeit zu erstellenden RA dient methodisch das Modell von GALSTER/AVGERIOU und NAKAGAWA ET AL. als Orientierung, denn es ist prozessorientierter gestaltet als jenes von CLOUTIER ET AL.. REIDT kritisiert zwar beide Methoden aufgrund ihrer starren Ausrichtung auf bestehende Architekturen und der fehlenden praxisnahen Anforderungsanalyse. Jedoch kann REIDT nicht auf bereits beschriebene Architekturen zurückgreifen, die in der Bearbeitung hätten berücksichtigt werden können (siehe die in dieser Literatur als PUB-I bezeichnete Literatur).[325]

Im direkten Vergleich beider Methoden finden sich inhaltliche Überschneidungen, doch GALSTER/AVGERIOU beginnen nicht direkt mit der empirischen Analyse, sondern mit der Klassifizierung der geplanten RA sowie der Definition der Design-Strategie (siehe *Tabelle 5-6*). Aus diesem Grund dient im Folgenden dieses Konstruktionsmodell als Orientierung. Daraus ergibt sich die in *Tabelle 5-6* dargestellte Abfolge von Konstruktionsschritten und der damit verbundenen Kapitel in dieser Forschungsarbeit.

Tabelle 5-6: Konstruktionsmodell Referenzarchitekturen (gekürzt)
(Quelle: Eigene Darstellung in Anlehnung an Galster/Avgeriou (2011): 154-156)

Schritt	Beschreibung	Kapitel
Schritt 1	Decision on Type of RA	Kapitel 5.5
Schritt 2	Selection of Design Strategy	Kapitel 5.5
Schritt 3	Empirical Acquisition of Data	Kapitel 4 Kapitel 6
Schritt 4	Construction of RA	Kapitel 6 Kapitel 7
Schritt 5	Enabling RA with Variability	Kapitel 6 Kapitel 7
Schritt 6	Evaluation of the RA	Kapitel 8

[322] *Medicalchain* ist ein kommerzielles Projekt, dessen Prozesse durch die Blockchain unterstützt werden (siehe Medicalchain (2018)).

[323] Vgl. Angelov/Trienekens/Grefen (2014): 2. Der in der Literaturanalyse identifizierten Literatur fehlt es zu einem großen Teil an der notwendigen Evaluation der konzipierten Architekturen. Ausnahmen bilden hier bspw. EKBLAW ET AL. (2016) und ROEHRS/DA COSTA/DA ROSA RIGHI (2017).

[324] Vgl. Reidt (2019): 31.

[325] Vgl. Reidt (2019): 37.

Bisher hat sich keine klare Notation und Darstellungsform für Referenzarchitekturen etabliert. Bereits in der durchgeführten Literaturanalyse wird offensichtlich, dass alle behandelten Konzepte nicht nur sehr abstrakt beschrieben, sondern auch selten grafisch dargestellt werden, und wenn doch, wird keine einheitliche Form gewählt. Mit Bezug auf Software-Architekturen etabliert sich insbesondere das *4+1 View Model*.[326] Für IS-Architekturen existieren die von WINTER/FISCHER aufgeführten fünf Bereiche.[327] Für diese Forschungsarbeit sind beide Varianten nur begrenzt hilfreich, da weder eine Software noch ein vollständiges IS konstruiert wird. Stattdessen ergibt sich mit Blick auf Referenzarchitekturen, die sich konkret mit der Blockchain auseinandersetzen,[328] die Erkenntnis, dass die Darstellung von Ebenen bzw. Sichten hilfreich ist. So trennen bspw. BALANI/HATHI ihre Architektur in fünf Ebenen, von denen vier aufeinander aufbauen und eine Ebene (Security) sämtliche 4 Ebenen umfasst (siehe *Abbildung 5-5*).[329]

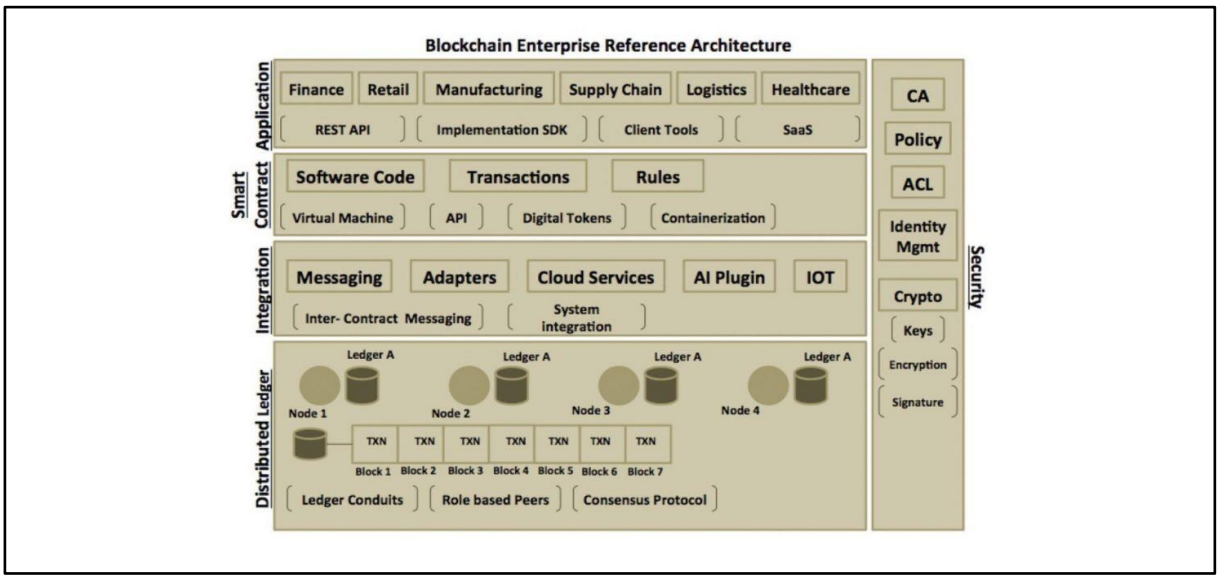


Abbildung 5-5: Blockchain Enterprise Reference Architecture (Quelle: Balani/Hathi (2017): 8)

Auch VISWANATHAN/DASGUPTA/GOVINDASWAMY unterteilen ihre als *Blockchain Solution Reference Architecture* (BSRA) bezeichnete Lösung in mehrere Ebenen, trennen die Gesamtar-

326 Vgl. Kruchten (1995): 43-47.

327 Vgl. Winter/Fischer (2006): 30.2. Business architecture, Process architecture, Integration architecture, Software architecture, Technology (or infrastructure) architecture.

328 Beide Referenzarchitekturen sind allgemein auf Blockchain-Technologie anzuwenden und lassen sich nur bedingt auf die in dieser Dissertation verfolgte Fragestellung übertragen, denn sie berücksichtigen die im Gesundheitswesen relevanten Domänen-Anforderungen nicht. In der weiteren Bearbeitung werden Parallelen dennoch erkennbar.

329 Vgl. Balani/Hathi (2017): 9-15. Die Autoren bezeichnen eine Ebene als *Distributed Ledger*, unterscheiden an dieser Stelle jedoch zu wenig zwischen Blockchain und Distributed Ledger. So ist Blockchain zwar ein Distributed Ledger, aber nicht jeder Distributed Ledger ist eine Blockchain (vgl. Brühl (2017): 140).

chitektur aber noch auf Makro-Ebene in zwei Konstruktionsbereiche (*Blockchain Network Reference Architecture (BNRA)* und *Blockchain Member Onboarding Reference Architecture (BMRA)).*[330]

Für diese Forschungsarbeit wird folglich festgelegt, dass sich die Darstellung der hier konzipierten Referenzarchitektur und des Entscheidungsmodells an der von BALANI/HATHI gewählten Schichten-Architektur orientiert und mögliche Variationen innerhalb dieser Schichten darstellt. Inwiefern Zusammenhänge zwischen den Schichten bestehen, wird im folgenden *Kapitel 6* eruiert und eine angepasste Darstellungsform in *Kapitel 7* definiert.

[330] Vgl. Viswanathan/Dasgupta/Govindaswamy (2019): 1.2.

6 Analyse der relevanten Literatur zur Artefakt-Konstruktion

6.1 Einführung

Die in *Kapitel 4* durchgeführte Literaturanalyse identifiziert bereits vier thematische Cluster in der Literatur:

i. Aktentyp (engl. *Record Type*)
ii. Datenhaltung und -bereitstellung (engl. *Data Storage & Provisioning*)
iii. Sicherheit (engl. *Security*)
iv. Technologie (engl. *Technology*)

Auf dieser Erkenntnis wird nachfolgend aufgebaut und pro Cluster *Variationspunkte* in der als relevant eingestuften Literatur identifiziert. Variationspunkte stellen verschiedene Ausprägungen[331] eines Clusters dar und erlauben einem Architekten die Auswahl der für den konkreten Anwendungsfall passenden Variation.

Die Bezeichnung der Cluster und Variationspunkte wird in englischer Sprache verfasst, sodass eine internationale Verwendung der Ergebnisse möglich ist. Darüber hinaus wird statt des Begriffs *Cluster* fortan der Begriff *Sicht* genutzt. Der Begriff *Sicht* wird in der Modellierungssprache genutzt, um eine Gesamtarchitektur in mehrere Teilmodelle bzw. Teilarchitekturen zu gliedern, die anschließend wieder zu einem Gesamtbild zusammengefasst werden können.[332]

6.2 Sicht: Record Type

Ausgangspunkt dieser Sicht ist die von HAAS in *Kapitel 2.1* beschriebene Übersicht von *Aktentypen* (engl. *Record Types*) im Gesundheitswesen (genauer *Tabelle 2-1*). Daraus ergeben sich als potentielle Kategorien *EHR*, *Patient Summary* und *PHR*. *Forschungsdatenbanken/ -netzwerke (Clinical Trial/Clinical Research)* und *Kostenträger (Insurance and other payers).* Die beiden letzteren werden von HAAS zwar nicht als eigener Aktentyp definiert, doch aufgrund der von BERNNAT beschriebenen interorganisationalen Positionierung von Forschung wird diese als eigenständiger Aktentyp identifiziert.[333] Zudem existieren auf Kostenträgerseite neben der Optimierung von Zahlungsprozessen ein Kollaborationsinteresse,[334] bspw. zur Identifikation

---

331 Hierzu gehören Gemeinsamkeiten sowie Unterschiede.

332 *Sicht* ist auf die Architektur integrierter Informationssysteme (ARIS) zurückzuführen. SCHEER unterteilt dabei seine Architektur in unterschiedliche Sichten, um eine Gesamtarchitektur in mehrere Bereiche aufzuteilen und diese gesondert zu bearbeiten (vgl. Scheer (1997): 11-13).

333 Vgl. Bernnat (2016): 33.

334 Diese Erkenntnis ist aus der von der GEMATIK dargestellten Architektur der Telematik-Infrastruktur abzuleiten, die eine Übertragung von Informationen an Kostenträger vorsieht (vgl. gematik (2018c): 28).

von Präventionsmaßnahmen in der Gesundheitsversorgung. Dass diese in Deutschland bedeutsam sind, ist an der von der GEMATIK und BMBF verfolgten Strategie zur Anbindung von Kostenträgern und Forschungsnetzwerken erkennbar.

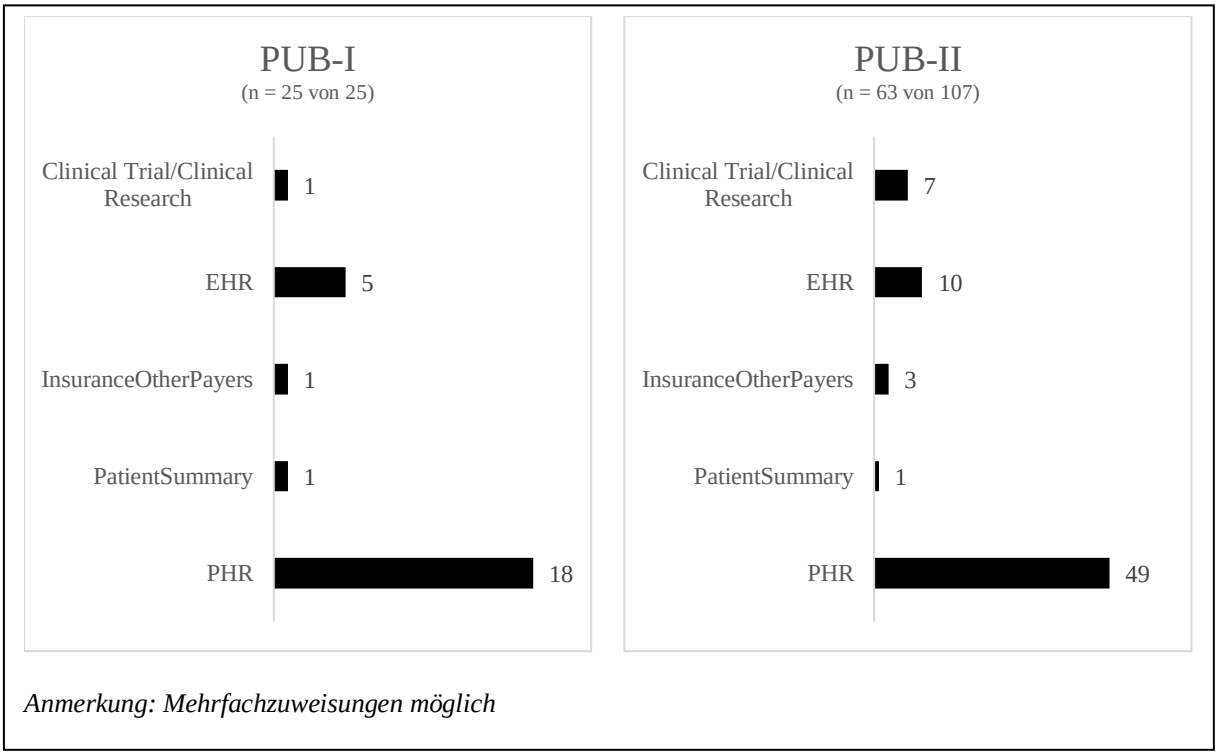


Abbildung 6-1: Mengen in Literatur-Kategorie 'Record Type' PUB-I und PUB-II (Quelle: Eigene Darstellung)

Die in der Literatur identifizierte Verteilung (*Tabelle D-1* (siehe *Anhang D*) und *Abbildung 6-1*) lässt erkennen, dass Blockchain nicht nur in der Vernetzung von Gesundheitsdaten zwischen Leistungserbringern (EHR), sondern bereits intensiv als Instrument zur liberalisierten Verwaltung von Gesundheitsdaten unter der Hoheit des Patienten diskutiert wird (PHR).

Doch in der Analyse der PHR hat sich eine uneinheitliche Verwendung des Terminus durch die Autoren ergeben. Eine konkrete Differenzierung der vom Patienten oder vom Leistungserbringer erhobenen Daten wird in den analysierten Publikationen nur in geringem Maße vorgenommen. So nutzen bspw. AHRAM ET AL. und GROPPER den Terminus *Protected Health Information* (PHI). Während AHRAM ET AL. noch auf die Definition der HIPAA[335] verweisen, unterlässt GROPPER diesen Hinweis gänzlich.[336] Gemäß HIPAA-Definition sind *PHI* alle

[335] Vgl. Ahram et al. (2017): 139.

[336] Die uneinheitliche Nutzung des Begriffs PHI sprechen auch RAHMADIKA/RHEE an und beschränken die Variation von PHI auf den entsprechenden Nutzerkreis und die im jeweiligen Netzwerk vorhandenen Daten (vgl. Rahmadika/Rhee (2018): 11).

> *„(..) individually identifiable health information (…), that is: (…) (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium."*[337]

Auch die Differenzierung der Verfügungsgewalten (Moderation durch Leistungserbringer oder Patient) wird nicht konsequent dargestellt. Grundsätzlich ist für die Identifikation des entsprechenden Aktentyps in der Literatur relevant, welche Anspruchsgruppen an der Erstellung und Moderation des Aktensystems beteiligt sind. Dabei ist anzumerken, dass in den identifizierten Publikationen ausgerechnet zur Definition dieser Stakeholder teils generische Begriffe wie *user* oder *(data-)owner* verwendet werden. *Tabelle 6-1* beschreibt, welche Gruppen unter dem Begriff *user* zusammengefasst werden und dass dieser teils nur durch die Beschreibung der Kompetenzen (rechte Hälfte) definiert wird.

Tabelle 6-1: Varianten der USER-Definition
(Quelle: Eigene Darstellung auf Basis von Zyskind/Nathan/Pentland (2015): 181; Linn/Koo (2016): 5; Genestier et al. (2017): 1; Liang et al. (2017b): 1168; Magyar (2017): 138; McFarlane et al. (2017): 6–7, 11; Xia et al. (2017b): 44.6; Yang/Yang (2017): 102, 104; Conceição et al. (2018): 9; Dias et al. (2018): 1; Pussewalage/Oleshchuk (2018): 1206; Sun et al. (2018): 281; Thwin/Vasupongayya (2018): 198; Zhang/Lin (2018): 140.5; Zhang/Poslad/Ma (2018): 3725; Zheng et al. (2018): 161, 163)

Literaturquelle	LE	KT	P	R		Berechtigungen verwalten	Zugriff ermöglichen	Erstellung/ Upload
Zyskind/Nathan/Pentland (2015)						X		
Linn/Koo (2016)			X			X		
Genestier et al. (2017)			X			X		
Liang et al. (2017b)			X			X		
Magyar (2017)	X	X	X	X				
McFarlane et al. (2017)			X			X		
Xia et al. (2017b)	X			X		X	X	
Yang/Yang (2017)	X		X				X	
Conceição et al. (2018)			X			X		
Dias et al. (2018)							X	
Pussewalage/Oleshchuk (2018)	X	X					X	
Sun et al. (2018)	X		X	X				
Thwin/Vasupongayya (2018)							X	
Zhang/Lin (2018)			X				X	
Zhang/Poslad/Ma (2018)	X		X	X				
Zheng et al. (2018)			X			X		X

Anmerkung: LE=Leistungserbringer; KT=Kostenträger; P=Patient; R=Research/Forschung

[337] U.S. Department of Health and Human Services Office for Civil Rights (2013).

Ähnliches findet sich bei der Nutzung des *(data) owner*. Dieser hat zwar grundsätzlich volle Verfügungsgewalt über die Berechtigungsverwaltung, ist jedoch in unterschiedlichen Rollen im Netzwerk aktiv:

i. nur Patient[338]
ii. nur Leistungserbringer[339]
iii. als Patient oder Leistungserbringer[340]
iv. als User[341]
v. allgemeine Entität im Besitz von Daten[342]

Eine eindeutige Definition für den Eigentümer von Gesundheitsdaten ist Gegenstand laufender Diskussionen in Wissenschaft und Politik.[343]

In der folgenden Unterteilung der Variationen wird aufgrund dieser Diskussionen einzig die Verfügungshoheit des beschriebenen *user* bzw. (*data-)owner* als Unterscheidungskriterium zugrunde gelegt und die Literatur entsprechend dem jeweiligen Aktentyp zugeordnet.

6.2.1 Electronic Health Records

Entsprechend der von HAAS geführten Definition von Electronic Health Records (EHR) bzw. einrichtungsübergreifenden Elektronischen Patientenakten, umfassen diese

> *„[d]ie wichtigsten Daten und Dokumente aller Behandlungen eines Patienten über alle medizinischen Fälle und Gesundheitsversorgungseinrichtungen hinweg. Die Einträge sind ärztlich geführt und moderiert, ggf. ergänzt mit behandlungsrelevanten eigenen Eintragungen des Patienten auf Anweisung des Arztes.“*[344]

Diese bei den Leistungserbringern geführten Patientenakten können ebenfalls mittels einer Blockchain geführt oder unterstützt werden.[345] Die Technologie übernimmt vornehmlich die

---

338 Vgl. Conceição et al. (2018): 10; Zhang/Lin (2018): 140.6.

339 Vgl. Liu (2016): 255.

340 Vgl. Chang et al. (2018): 175; Grishin et al. (2018): 11.

341 Vgl. Zyskind/Nathan/Pentland (2015): 181; Liang et al. (2017b): 1168.

342 Vgl. Thwin/Vasupongayya (2018): 198; Wu et al. (2018): 350.

343 Siehe in JENTZSCH (2018). Aus diesem Grund kann nicht abschließend geklärt werden, ob Patientendaten Eigentum des Leistungserbringers sind (Datenbankschutzrecht) und der Patient im Rahmen seiner Datenschutzrechte nur die Verwendung steuern kann oder ob der Patient wegen der Erhebung personenbezogener Informationen das Eigentumsrecht besitzt.

344 Haas (2017): 55.

345 Vgl. Gropper (2016): 2; Zhang et al. (2018b): 271. Für zwei Publikationen ergibt sich die Zuordnung in EHR durch die als Dateneigentümer (vgl. Liu (2016): 255f.) oder als User (vgl. Xia et al. (2017a): 14760) beschriebenen Nutzergruppen.

Moderation der Inhalte,[346] die wiederum durch den Leistungserbringer kontrolliert werden.[347] In der vorliegenden Literatur fehlt in einigen Publikationen eine eindeutige Definition des Moderationsberechtigten,[348] sodass aufgrund der Beschreibungen von einem EHR auszugehen ist.

6.2.2 Clinical Trial / Clinical Research

Dieser Aktentyp orientiert sich an den in *Kapitel 2.3.2* dargestellten Aktensystemen der BMBF-Konsortien, die Patientendaten für die medizinische Forschung zur Verfügung stellen. Blockchain-Technologien unterstützen ebenfalls diese Form von Aktensystemen,[349] bspw. die Verwaltung von Einwilligungserklärungen[350] eines Patienten, von der allgemeinen Einwilligung bis zum Umfang der zur Verfügung gestellten Daten.[351] Darüber hinaus stellen sie die Integrität der für Studien benötigten Daten sicher und erlauben Rückschlüsse, ob eine Quelle sicher oder unsicher ist und eine Studie somit belastbar bleibt.[352]

6.2.3 Insurance and other payers

HAAS erwähnt diesen Aktentyp nicht. Auch fällt dieser nicht in die in §68 SGB V beschriebenen Akten-Konzeptionen der Krankenversicherungen. Aufgabenschwerpunkt des in der Literatur aufgeführten Typs ist die Bereitstellung von Abrechnungsdaten an bzw. von Krankenversicherungen. Ein Beispiel ist das von ZHOU/WANG/SUN dargestellte Konzept *MIStore*, dessen Fokus auf der Abwicklung von Abrechnungsprozessen liegt und das die Speicherung sämtlicher abrechnungsbezogener Informationen auf der Blockchain ermöglicht.[353]

In der Gruppe der PUB-II Publikationen berücksichtigen ebenfalls einzelne Publikationen die Rolle der Kostenträger und identifizieren Potentiale in der automatisierten Abwicklung von

---

346 Vgl. Pirtle/Ehrenfeld (2018): 172.1-2.

347 Vgl. Hanley/Tewari (2018): 250; Jiang/Peng/Dian (2018): 012006.3; Nagasubramanian et al. (2018): 644; Pussewalage/Oleshchuk (2018): 1205; Sun et al. (2018): 281; Yang/Li (2018): 262.

348 Vgl. Angraal/Krumholz/Schulz (2017): 1; Magyar (2017): 138; Hussein et al. (2018): 1; Zhang/Poslad/Ma (2018): 3725.

349 Vgl. Kuo/Ohno-Machado (2018): 1. In der medizinischen Forschung, insbesondere der Epidemiologie, müssen Daten schnell und interoperabel zur Verfügung stehen, und es muss neben einer gemeinsamen Datenbasis ein Rechtesystem integriert werden. Jeder dieser Punkte ist mit einer Blockchain umsetzbar (vgl. Cisneros/Aarestrup/Lund (2018): 3).

350 Im Englischen als *Consent Management* bezeichnet.

351 Vgl. Benchoufi/Ravaud (2017): 335.2-3; Dubovitskaya et al. (2017): 653; Bell et al. (2018): 3.

352 Vgl. Angeletti/Chatzigiannakis/Vitaletti (2017): 10; Benchoufi/Ravaud (2017): 335.2-3; Shae/Tsai (2017): 1975, 1977; Radanović/Likić (2018): 587.

353 Vgl. Zhou/Wang/Sun (2018): 149.1.

Zahlungsprozessen[354] mittels *Smart Contracts* sowie die Einführung von individuellen Versicherungstarifen auf Basis fälschungssicherer Gesundheitshistorien.[355]

6.2.4 Patient Summary

Entsprechend der von HAAS geführten Definition von Patient Summary Records, bzw. Elektronischer Basisdokumentationsakten, sind diese

> *„[n]ur wenige ausgewählte lebenslang wichtige medizinische Daten, wie Diagnosen, Maßnahmen, Risikofaktoren etc., jedoch keine Dokumente. Die Einträge sind ärztlich geführt und moderiert. Eine solche minimale Akte mit jedoch vollständigen Informationen aller wichtigen Aspekte soll vor allen Dingen die Übersichtlichkeit verbessern und im Notfall oder bei Arztwechsel die Weiterbehandlung erleichtern. In abgewandelter Form stellt der Notfalldatensatz gemäß § 291a SGB V eine solche Basisdokumentation dar. Mancherorts wird diese auch als „Miniakte" bezeichnet."*[356]

Die wenigen identifizierten Publikationen beziehen sich auf das von der EU durchgeführte epSOS3-Projekt, das einen Patientendaten-Austausch, beschränkt auf ein Patient Summary, innerhalb der Europäischen Union ermöglicht.[357] Kernaufgabe der Blockchain ist dabei nicht die Übermittlung von Daten, sondern die Bereitstellung eines auditfähigen Logs über die transferierten Daten.[358]

6.2.5 Patient Health Records

HAAS definiert Personal Electronic Health Record (PHR), bzw. Persönliche Elektronische Patientenakten (pEPA), als

> *„[f]allübergreifende Akte[n] unter der Datenhoheit des Patienten. Die Entscheidung über die konkrete Nutzung (Zweckbestimmung) erfolgt im Einzelfall durch den Patienten, indem dieser die Informationen bei Bedarf einem behandelnden Arzt zur Verfügung stellt. Der Patient kann Rechte auch an einen Arzt seines Vertrauens*

---

354 Vgl. Radanović/Likić (2018): 586f.

355 Vgl. Liang et al. (2017b): 1168; Liang et al. (2018a): e3.8. Die Autoren verweisen bereits darauf, dass Patienten den Zugriff auf ihre eigenen Daten freigeben müssen. Sie würden dies auch tun, um einen besseren Versicherungstarif zu erhalten. Dieses Vorgehen beschreibt die Erosion von Privatsphäre, die im Rahmen der Datenökonomie als problematisch eingestuft wird (vgl. Jentzsch (2018): 10).

356 Haas (2017): 55.

357 Vgl. Staffa et al. (2018): 13.

358 Vgl. Castaldo/Cinque (2018): 47f, 55. Mehr Informationen im Rahmen von *Logging und Audit* in *Kapitel 6.4.4*.

> *delegieren. Sinn der pEPA ist, als Quelle für die Speisung der zweckbestimmten Patientenakten in der Verantwortung der Ärzte zu dienen. Diese Art von persönlichen Akten wurde in Deutschland lange als Gesundheitsakte bezeichnet.“*[359]

PHR beschreiben insbesondere wegen der Moderation durch den Patienten einen konkreten Anwendungsfall für die Blockchain-Technologie.[360] Der Patient erhält mithilfe der Blockchain-Technologie ein Werkzeug zur Moderation von Zugriffsberechtigungen, ohne dabei seine Identität öffentlich preiszugeben.[361] Darüber hinaus können Blockchains so konstruiert werden, dass neben dem Betrieb einer Blockchain eine dritte Instanz Identitäten und Zugriffe verwaltet.[362] Abgesehen vom Betrieb einer einzigen Blockchain für das gesamte Gesundheitswesen existiert auch die Möglichkeit, dass jeder Patient eine eigene Blockchain führt und während seiner Behandlung die Erlaubnis erteilt, Inhalte von seiner Blockchain in die eines Leistungserbringers zu übertragen.[363]

6.3 Sicht: Data Storage & Provisioning

Diese Sicht beschäftigt sich mit den in den Publikationen behandelten Varianten der Datenspeicherung und -bereitstellung. Neben der allgemeinen Diskussion, ob Daten auf einer Blockchain

---

[359] Haas (2017): 55. Eine Steigerung des PHR ist ein Personal Data Storage (PDS), das sämtliche privaten Informationen an einer zentralen Stelle verwaltet und in dieser Analyse im Zusammenhang mit PHR betrachtet werden kann (vgl. Chowdhury et al. (2018): 1331).

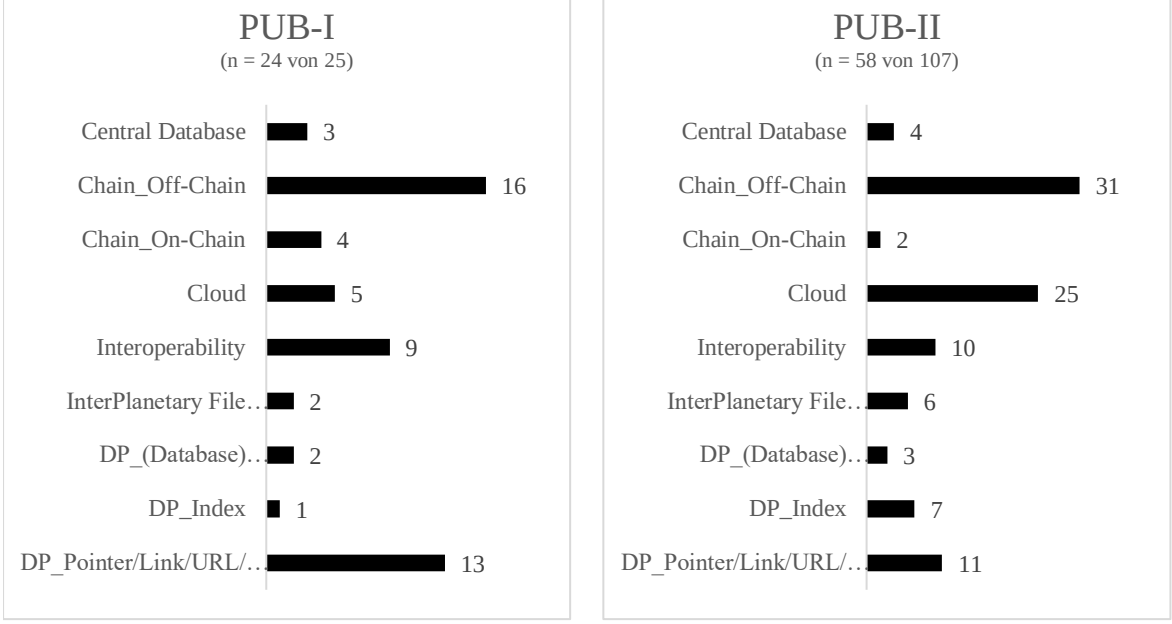
[360] Vgl. Gropper (2016): 2; Kamau et al. (2018): 4f; Mense/Athanasiadis (2018): 10. Problematisch wird in diesem Zusammenhang die Anzahl von Duplikaten, die im Netzwerk verteilt gespeichert werden (vgl. Bell et al. (2018): 4).

[361] Vgl. Azaria et al. (2016): 26; Ekblaw et al. (2016): 3; Linn/Koo (2016): 5; Nichol/Brandt (2016): 7; Yue et al. (2016): 218.1; Al Omar et al. (2017): 535, 537; Cunningham/Ainsworth (2017): 45; Dubovitskaya et al. (2017): 653, 657; Genestier et al. (2017): 2; Kim/Hong (2017): 80; Liang et al. (2017b): 1168f; McFarlane et al. (2017): 11; Noh et al. (2017): 134; Rifi et al. (2017): 200; Roehrs/da Costa/da Rosa Righi (2017): 76; Yang/Yang (2017): 102, 104; Zhang et al. (2017): 124; Alexaki et al. (2018): 256; Amofa et al. (2018): 167; Bhuiyan et al. (2018): 62; Chang et al. (2018): 176; Chen et al. (2018a): 207; Chen et al. (2018b): 5.5; Conceição et al. (2018): 9; Cyran (2018): 2; Dagher et al. (2018): 284f; Du et al. (2018): 36; Esposito et al. (2018): 35; Fan et al. (2018): 136.3; Gökalp et al. (2018): 178; Gordon/Catalini (2018): 227; Grishin et al. (2018): 11; Guo et al. (2018): 11677; Han et al. (2018): 586; Ito/Tago/Jin (2018): 831; Jiang et al. (2018): 52; Jiang/Peng/Dian (2018): 012006.4; Kotsiuba et al. (2018): 115f; Liang et al. (2018a): e3.6; Liang et al. (2018b): 388; Liu et al. (2018): 6187; Medicalchain (2018): 20; Mendes et al. (2018): 382; Novikov et al. (2018): 700f; Patel (2018): 6; Quaini et al. (2018): 169f; Radanović/Likić (2018): 585; Ramani et al. (2018): 3718; Rouhani et al. (2018): 1535; Theodouli et al. (2018): 1375; Thwin/Vasupongayya (2018): 198; Vora et al. (2018): 981; Wang et al. (2018a): 14; Wang et al. (2018b): 948; Wang/Song (2018): 154f; Xiao et al. (2018): 1002; Zhang/Lin (2018): 140.6, 140.13; Zheng et al. (2018): 161; Zhuang et al. (2018): 1168. Darüber hinaus existiert eine Beschreibung, in der ein Patient die erste Version eines PHR erstellt und Zugriffe anschließend über Rechtezuweisung gesteuert werden. Jedoch wird nicht beschrieben, wer (Patient, Leistungserbringer, Dritte) diese Rechte verwaltet (vgl. Ahram et al. (2017): 140).

[362] Vgl. Gagnon/Stephen (2018): 3f.

[363] Vgl. Badr/Gomaa/Abd-Elrahman (2018): 160.

verwaltet werden oder nicht (*on-* versus *off-chain-Speicherung*), werden diverse Technologieansätze zur Datenspeicherung identifiziert. Die Verteilung in der Literatur wird in *Tabelle D-2* (siehe *Anhang D*) und *Abbildung 6-2* dargestellt.



Anmerkung: Mehrfachzuweisungen möglich. DP steht ausschließlich in dieser Abbildung für für 'Data Provisioning'

Abbildung 6-2: Mengen in Literatur-Kategorie 'Data Storage & Provisioning' PUB-I und PUB-II (Quelle: Eigene Darstellung)

6.3.1 Datenspeicherung auf (on-chain) oder abseits (off-chain) der Blockchain

Eine grundlegende Diskussion in der Konzeption blockchain-basierter Aktensysteme ist die Speicherung von Daten entweder auf der Blockchain (*on-chain*) oder abseits der Blockchain (*off-chain*).

Für eine **on-chain**-Speicherung von Gesundheitsdaten existieren in den analysierten Publikationen wenige Szenarien. So werden bspw. ausschließlich Abrechnungsdaten auf einer Blockchain gespeichert[364] oder innerhalb von Leistungserbringer-Einrichtungen *Private Blockchains* betrieben, die erst mit Bereitstellung von Metadaten auf einer öffentlichen bzw. konsortial-organisierten Blockchain diese institutionsinternen Daten externen Datenkonsumenten zur Verfügung stellen.[365] Darüber hinaus existieren Konzeptionsbeschreibungen, die die Durchführung

[364] Vgl. Zhou/Wang/Sun (2018): 149.1.

[365] Vgl. Han et al. (2018): 582; Zhang/Lin (2018): 140.2.

von Blockchain-Prozessen bzw. -Protokollen für das Szenario einer on-chain-Speicherung beschreiben, dabei aber nicht tiefer ins Detail gehen.[366]

Die Alternative zu einer on-chain-Speicherung von Gesundheitsdaten, die off-chain-Speicherung, wird von einem Großteil der Publikationen thematisiert. Bei dieser Variante werden Gesundheitsdaten in herkömmlichen Speichersystemen belassen und deren Metadaten wiederum auf einer Blockchain gespeichert.[367] Diese Metadaten beinhalten entweder Referenzen in physischen Speichermedien, Kombinationen aus Referenzen und Hashwerten der eigentlichen Daten[368] oder Informationen über Zugriffsberechtigungen.[369]

Grund für den Fokus auf off-chain sind Limitationen der Blockchain. Während in der Bitcoin-Blockchain einfache Transaktionen durchgeführt werden, deren Transaktionsgröße wenige Kilobyte umfasst, können einzelne Gesundheitsdaten wesentlich umfangreicher sein, insbesondere im Fall von Bilddateien.[370] Hinzu kommen datenschutzrechtliche Bedenken (EU-DSGVO oder HIPPA), denn weder dürfen Gesundheitsdaten öffentlich bereitgestellt werden noch lassen sich diese aufgrund der fehlenden Löschfunktion nachträglich löschen.[371]

6.3.2 Einrichtung einer zentralen Datenbank

Trotz des verteilten Konzepts der Blockchain-Technologie existieren Publikationen, die die Einrichtung einer zentralen Datenbank als gemeinsame Datenbasis beschreiben, allerdings wird nicht deutlich, ob diese institutionsintern oder -extern geführt wird.[372] Die damit verbundene Datenhaltung wird mit dem sogenannten Data-Lake-Konzept umgesetzt.[373]

---

366 Vgl. Ahram et al. (2017): 140f; Al Omar et al. (2017): 535, 537; Benhamouda/Halevi/Halevi (2018): 359.

367 Vgl. Azaria et al. (2016): 28; Ekblaw et al. (2016): 6; Gropper (2016): 3; Linn/Koo (2016): 4; Lo et al. (2017): 160; Magyar (2017): 138; McFarlane et al. (2017): 11; Simić/Sladić/Milosavljević (2017): 3; Bayle et al. (2018): 790; Chen et al. (2018a): 208; Chowdhury et al. (2018): 1332; Cisneros/Aarestrup/Lund (2018): 5; Desai et al. (2018): 1554; Gökalp et al. (2018): 177; Hanley/Tewari (2018): 246; Kaur et al. (2018): 156.8; Patel (2018): 6; Pirtle/Ehrenfeld (2018): 172.2; Quaini et al. (2018): 169; Rouhani et al. (2018): 1537; Vora et al. (2018): 981; Yang/Li (2018): 262; Zheng et al. (2018): 164.

368 Zur Absicherung der Datenintegrität.

369 Vgl. Dubovitskaya et al. (2017): 656; Rifi et al. (2017): 200; Banerjee/Lee/Choo (2018): 156; Bhuiyan et al. (2018): 66; Chang et al. (2018): 175; Chen et al. (2018b): 5.3; Conceição et al. (2018): 9; Esposito et al. (2018): 36; Fan et al. (2018): 136.3; Gagnon/Stephen (2018): 3; Ito/Tago/Jin (2018): 831; Jiang et al. (2018): 53; Jiang/Peng/Dian (2018): 012006.2; Liu et al. (2018): 6188; Medicalchain (2018): 20; Mense/Athanasiadis (2018): 8; Nagasubramanian et al. (2018): 643, 645; Pukas/Smal/Zabchuk (2018): 173; Ribitzky et al. (2018): 8; Sun et al. (2018): 279, 281; Theodouli et al. (2018): 1375; Wang et al. (2018b): 947; Xiao et al. (2018): 1001; Zhang et al. (2018b): 272.

370 Vgl. Ali et al. (2016): 54; Chen et al. (2018b): 5.3; Esposito et al. (2018): 36; Gordon/Catalini (2018): 228; Zheng et al. (2018): 164f.

371 Vgl. Esposito et al. (2018): 35f; Rodrigues/Bocek/Stiller (2018): 177.

372 Vgl. Bhuiyan et al. (2018): 66; Hanley/Tewari (2018): 249.

373 Vgl. Linn/Koo (2016): 4; Gökalp et al. (2018): 177; Medicalchain (2018): 34.

Ein *Data Lake* empfängt ohne einen im Data Warehousing üblichen ETL-Prozess[374] heterogene Daten und speichert diese unabhängig von Größe oder Typ als Rohdaten ab.[375] Vorteil dieser Methode ist die Analyse sämtlicher Daten ohne künstliche Grenzen.[376] Zur Identifikation und Nachverfolgung relevanter Daten werden Metadaten ergänzt, die wiederum in einem Datenkatalog zusammengeführt werden.[377] Data Lakes werfen allerdings das Problem auf, dass es unterschiedliche Konzepte und keine einheitlichen Architekturen oder ein gemeinsam abgestimmtes Metadaten-Management gibt.[378] Auch stellt sich die Frage, ob ein Data Lake Daten on-premise, in der Cloud oder auf andere Weise abspeichert.[379]

In diesem Zusammenhang wird in der Blockchain-Diskussion die Einrichtung eines Personal Data Storage (PDS), also eines gemeinsamen Speichers für sämtliche personenbezogenen Daten mit zusätzlicher Berechtigungssteuerung,[380] debattiert. PHR sind dabei eine Teilmenge des PDS und übernehmen Aufgaben in der Berechtigungsverwaltung.[381] Diesbezüglich wird bereits auf die alternative Speichermethode mittels *InterPlanetary File System (IPFS)* hingewiesen.[382]

6.3.3 Cloud

Insbesondere hinsichtlich off-chain-Speicherung lässt sich in der Literatur eine Tendenz in Richtung Cloud-Infrastruktur identifizieren. Sie erlaubt eine flexible Anpassung des Ressourcenbedarfs und ermöglicht die Verarbeitung einer großen Menge von Daten.[383] Aufgrund dieser Ressourcenelastizität ergeben sich für Nutzer Kosteneinsparungen, da nur der tatsächliche Bedarf abgerechnet wird.[384] Cloud-Infrastrukturen können zudem unterschiedliche Anforderungen beteiligter Stakeholder adressieren und dennoch eine Kooperation über Institutionsgrenzen hinweg ermöglichen.[385]

---

374 ETL: E - Extract, T - Transform, L - Load.

375 Vgl. Mathis (2017): 289; Maini/Venkateswarlu/Gupta (2020): 596.

376 Vgl. Mathis (2017): 290.

377 Vgl. Giebler et al. (2019): 184; Maini/Venkateswarlu/Gupta (2020): 596.

378 Vgl. Giebler et al. (2019): 184f.

379 Vgl. Mathis (2017): 290f.

380 Vgl. Kirkham et al. (2013): 13.

381 Vgl. Chowdhury et al. (2018): 1331. Abweichend können Blockchains hier ergänzend eine Integritätsabsicherung vornehmen. Wenn bspw. ein Krankenhaus einen EMR erstellt, kann der Patient von diesem eine Kopie erhalten, und gleichzeitig können ein aus diesem EMR erstellter Hash-Wert sowie weitere Informationen in einer Transaktion auf Blockchain gespeichert werden (vgl. Jiang et al. (2018): 52f.).

382 Vgl. Alessi et al. (2018): 176, 178. Mehr Informationen zu Cloud und IPFS in *Kapitel 6.3.3*.

383 Kuo (2011): e67.5; Casola et al. (2016): 12; Esposito et al. (2018): 33.

384 Li et al. (2010): 90; Kaur et al. (2018): 156.1–2; Wang/Song (2018): 152.1.

385 Talia (2013): 98f; Kaur et al. (2018): 156.1, 156.4; Wang/Song (2018): 152.2.

Aufgrund dieser Eigenschaften werden *Cloud-Dienste* zur Speicherung der heterogenen und umfangreichen Gesundheitsdaten genutzt.[386] Eine Blockchain übernimmt in diesen Modellen die Aufgabe, Metadaten und Verweise hochgeladener Daten sowie die damit verbundenen Sicherheitsinformationen unveränderlich zu speichern.[387] Auch kann die Verbindung mehrerer bestehender Cloud-Infrastrukturen durch eine Blockchain unterstützt werden.[388]

Sämtliche Blockchain-Konzepte, die identifiziert werden, bauen auf bestehenden Infrastrukturen auf und haben einen unterstützenden Charakter. Tatsächlich werden Blockchain-Infrastrukturen nur in wenigen Publikationen in einer Cloud aufgebaut, sodass die bereits genannten Vorteile einer Cloud für die rechenintensiven Prozesse einer Blockchain derzeit nicht genutzt werden.[389]

6.3.4 InterPlanetary File System

Als Alternative zur Cloud-Infrastruktur wird der Einsatz eines *InterPlanetary File System (IPFS)* beschrieben.[390] Ein IPFS ist ein verteiltes Speichersystem, organisiert dessen Daten allerdings nicht mit Speicherpfaden, sondern auf Basis des entsprechenden Inhalts.[391] Speichersysteme bleiben lokal organisiert, und Daten werden auf mehreren dieser lokalen Speicher repliziert, wodurch ein verteiltes System entsteht.[392] Eine Blockchain wird parallel zu einem IPFS betrieben und beinhaltet Metadateien zu den im IPFS gespeicherten Daten, bspw. deren Dateireferenz und Identifier.[393] IPFS gilt insbesondere mit Blick auf die EU-DSGVO als eine valide Alternative zur Nutzung einer Cloud.[394]

---

386 Vgl. Dubovitskaya et al. (2017): 656; Liang et al. (2017a): 471; Liang et al. (2017b): 1169; Xia et al. (2017b): 44.1; Yang/Yang (2017): 104; Chen et al. (2018b): 5.3; Conceição et al. (2018): 9; Desai et al. (2018): 1555; Guo et al. (2018): 11681; Liang et al. (2018a): e3.6, e3.8; Liu et al. (2018): 6188; Nagasubramanian et al. (2018): 640; Thwin/Vasupongayya (2018): 198; Wang/Song (2018): 152.4–5; Zhang et al. (2018a): 3; Zheng et al. (2018): 164. Darüber hinaus können Gesundheitsdaten lokal und ergänzend in Cloud-Diensten gespeichert werden (vgl. Badr/Gomaa/Abd-Elrahman (2018): 162). Ebenfalls können bestehende Cloud-Dienste mit den Systemen der Leistungserbringer verbunden werden, um Gesundheitsdaten und behandlungsfremde Daten in einem einzigen System zusammenzuführen (vgl. Chowdhury et al. (2018): 1331).

387 Vgl. Dubovitskaya et al. (2017): 656; Noh et al. (2017): 134; Badr/Gomaa/Abd-Elrahman (2018): 162; Chen et al. (2018b): 5.3-5.4; Liu et al. (2018): 6187; Nagasubramanian et al. (2018): 640; Wang/Song (2018): 152.4–5; Zheng et al. (2018): 164f.

388 Vgl. Casola et al. (2016): 12; Xia et al. (2017a): 14758; Guo et al. (2018): 11680.

389 Vgl. Yue et al. (2016): 218.2; Ahram et al. (2017): 140f; Kaur et al. (2018): 156.5.

390 Vgl. Grishin et al. (2018): 14.

391 Vgl. Benet (2014): 1; Cisneros/Aarestrup/Lund (2018): 5; Wu et al. (2018): 351.

392 Benet (2014): 7; Rifi et al. (2017): 200; Quaini et al. (2018): 168.

393 Vgl. Cisneros/Aarestrup/Lund (2018): 6; Cyran (2018): 3; Quaini et al. (2018): 169.

394 Vgl. Ribitzky et al. (2018): 9.

6.3.5 Interoperabilität

Grundsätzlich sind aktuelle Konstruktionen geprägt von heterogenen Daten und dem fehlenden Willen von Leistungserbringern und Softwareherstellern, Interoperabilität herzustellen.[395] Eine Möglichkeit, Leistungserbringer zu Interoperabilität zu verpflichten, ist die Trennung von Zugriffskontrolle und Datenhaltung, die zurzeit beide von der datenerhebenden Institution übernommen werden.[396]

Die Anwendung der Blockchain-Technologie verspricht Interoperabilität,[397] doch kann nicht grundsätzlich von einer daraus resultierenden Interoperabilität innerhalb des jeweiligen Netzwerks ausgegangen werden, denn insbesondere die Art und Weise, wie Daten auf den Systemen der Institutionen abgelegt werden, bestimmt den tatsächlichen Grad an Interoperabilität.[398] Speziell wenn Begriffe auf einer Blockchain gespeichert werden, die für eine Suche genutzt werden können, bedarf es klar definierter Standards[399] und einheitlicher Semantik.[400] In einem Teil der PUB-I-Publikationen werden aus diesem Grund *Schnittstellen* (Application Programming Interfaces (APIs)) oder ein *Translator* in eine Architektur übernommen, die lokale Daten in ein für die Blockchain passendes Format transformieren.[401]

Im Design einer Blockchain-Lösung ist die Nutzung bestehender Standards essenziell, denn eine Blockchain kann insbesondere im Falle einer off-chain-Speicherung nicht kontrollierend eingreifen.[402] Bisher haben sich Standards wie *openEHR* und *FHIR* durchgesetzt.[403] Der Vorteil an der Nutzung von openEHR ist dessen Kompatibilität zu weiteren Standards wie HL7, LOINC, SNOMED-CT und DICOM.[404]

Interoperabilität muss Teil der Implementierungsstrategie sein und darf gleichzeitig nicht die existierenden Infrastrukturen einschränken. Insofern können zur Akzeptanzsteigerung zwei Anforderungen an ein Blockchain-Netzwerk gestellt werden: *Nutzung bestehender Infrastrukturen*

---

395 Vgl. Azaria et al. (2016): 25; Kaur et al. (2018): 156.7–8.

396 Vgl. Gropper (2016): 2. Durch den Einbezug des Patienten, der den Zugriff zukünftig steuern soll, sind Einrichtungen in Zukunft stärker dazu gezwungen, Interoperabilität zu adressieren (vgl. Gropper (2016): 4).

397 Vgl. McFarlane et al. (2017): 11; Ito/Tago/Jin (2018): 830.

398 Vgl. Yang/Yang (2017): 109; Mense/Athanasiadis (2018): 10; Ribitzky et al. (2018): 9.

399 Vgl. Zhang/Lin (2018): 140.7.

400 Vgl. Nichol/Brandt (2016): 7.

401 Vgl. Azaria et al. (2016): 26; Ekblaw et al. (2016): 9; Linn/Koo (2016): 7; Randall/Goel/Abujamra (2017): 1000276.3; Roehrs/da Costa/da Rosa Righi (2017): 75f; Gordon/Catalini (2018): 227; Kamau et al. (2018): 4; Ribitzky et al. (2018): 9f.

402 Vgl. Zhang et al. (2018b): 270f; Zhang et al. (2018b): 275f.

403 Vgl. Azaria et al. (2016): 29; Quaini et al. (2018): 173.

404 Vgl. Roehrs/da Costa/da Rosa Righi (2017): 73.

und *Modularität*.[405] Letzteres ist insbesondere als Reaktion auf stetige Weiterentwicklungen in den bestehenden IT-Systemen der Leistungserbringer relevant.[406]

6.3.6 Data Provisioning (Datenbereitstellung)

Die unter diesem Aspekt untersuchte Literatur steht in engem Zusammenhang zur Datenhaltungskomponente, insbesondere der off-chain-Speichervariante. Wie bereits geschildert, wird die Blockchain statt zur Speicherung von Gesundheitsdaten zur Bereitstellung der mit diesen Daten verbundenen Metadaten, also bspw. den Pfad (Pointer, Links , URL oder URI), verwendet und speichert Informationen revisionssicher.[407] Alternativ zur Nutzung von direkten Verweisen kann bei Anwendung der IPFS-Speicher-Konzeption die als effizienter bewertete Methode des *Content-Adressing* genutzt werden.[408] *Content-Adressing* erstellt dabei einen einmaligen Pfad, der auf Basis des gehashten Inhalts (Content-Hash) erzeugt wird.[409]

Diese Bereitstellungs-Informationen werden in ausgewählten Konzepten nicht im Klartext in den Block einer Blockchain geschrieben, sondern vorher verschlüsselt, gehasht oder beides.[410] In diesen Fällen wird ein zusätzliches Register geführt, das den Zusammenhang des auf der Blockchain gespeicherten Hashs mit dem Originalpfad wiederherstellt.[411]

Der eigentliche Zugriff auf Daten in den off-chain-Speichern erfolgt über entsprechende *Database Gatekeeper*.[412]

Im Rahmen der Datenbereitstellung wird die Blockchain vornehmlich als Index genutzt und speichert sämtliche Verweise.[413] Statt umfangreich Informationen zu Daten und ihren Speicherorten zu indizieren, können sich diese Register auch auf eine Liste sämtlicher Leistungserbringer beschränken, in deren Systemen Daten eines Patienten liegen.[414]

---

405 Vgl. Kuo/Ohno-Machado (2018): 3.

406 Vgl. Zhang et al. (2018b): 271.

407 Vgl. Azaria et al. (2016): 26; Ekblaw et al. (2016): 3; Peterson et al. (2016): 3; McFarlane et al. (2017): 9; Bhuiyan et al. (2018): 66; Chang et al. (2018): 175; Conceição et al. (2018): 8-10; Fan et al. (2018): 136.7; Hanley/Tewari (2018): 248f; Kaur et al. (2018): 156.8; Medicalchain (2018): 20; Patel (2018): 4; Quaini et al. (2018): 169; Ribitzky et al. (2018): 6; Sun et al. (2018): 279; Theodouli et al. (2018): 1375; Xiao et al. (2018): 1001; Zhang et al. (2018b): 272.

408 Vgl. Du et al. (2018): 35.

409 Vgl. Benet (2014): 7.

410 Vgl. Linn/Koo (2016): 4; Rouhani et al. (2018): 1537; Vora et al. (2018): 978.

411 Vgl. Bayle et al. (2018): 790f.

412 Vgl. Azaria et al. (2016): 28f; Ekblaw et al. (2016): 7f; Dagher et al. (2018): 287; Pukas/Smal/Zabchuk (2018): 173; Zhang et al. (2018a): 4.

413 Vgl. Simić/Sladić/Milosavljević (2017): 3; Banerjee/Lee/Choo (2018): 156; Chen et al. (2018a): 208; Chen et al. (2018b): 5.3, 5.5; Dagher et al. (2018): 284; Li et al. (2018): 141.10; Liu et al. (2018): 6188.

414 Vgl. Yang/Li (2018): 262.

6.4 Sicht: Security

Diese Sicht stellt die in den Publikationen behandelten Themen rund um Security und Informationssicherheit heraus und umfasst dabei sämtliche für eine sichere Identifikation und Berechtigungsverwaltung relevanten Kernthemen wie *Identity and Access Management*, *Infrastrukturen* sowie *Logging bzw. Audit* wie sie auch in *Abbildung 6-3* für herkömmliche Systeme beschrieben wird.

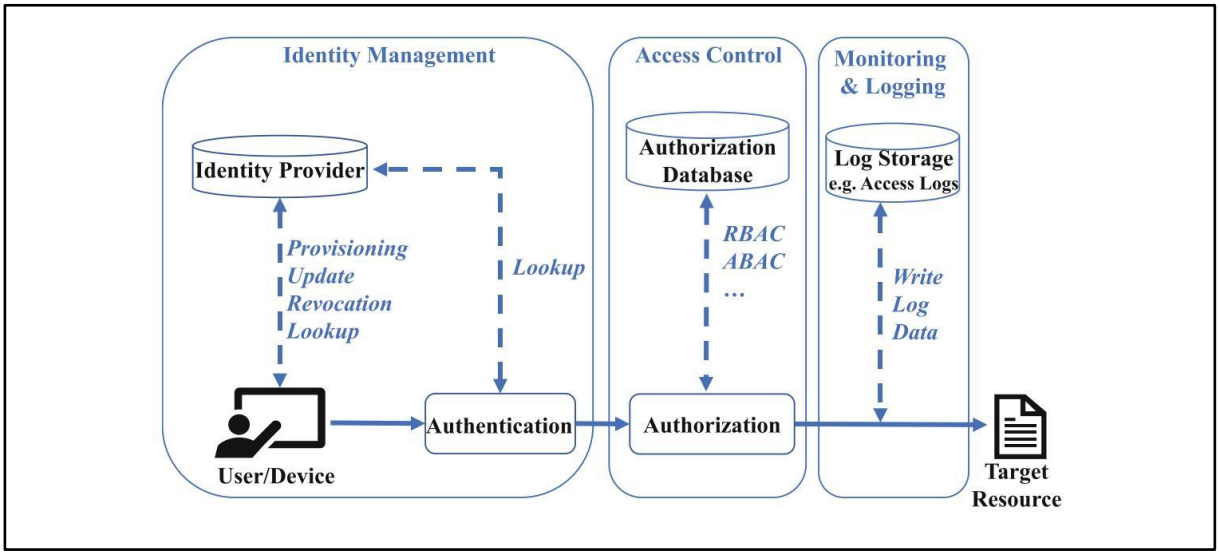


Abbildung 6-3: IAM-Kernfunktionalitäten (Quelle: Nuss/Puchta/Kunz (2018): 168)

Aufgrund dessen, dass hier die Analyse tiefer geht als in den vorangegangenen Kapiteln wird die eine detaillierte quantitative Verteilung der Inhalte auf die Publikationen in den jeweiligen Unterkapiteln dargestellt. *Tabelle D-3* (siehe *Anhang D*) und *Abbildung 6-4* aggregieren diese Informationen.

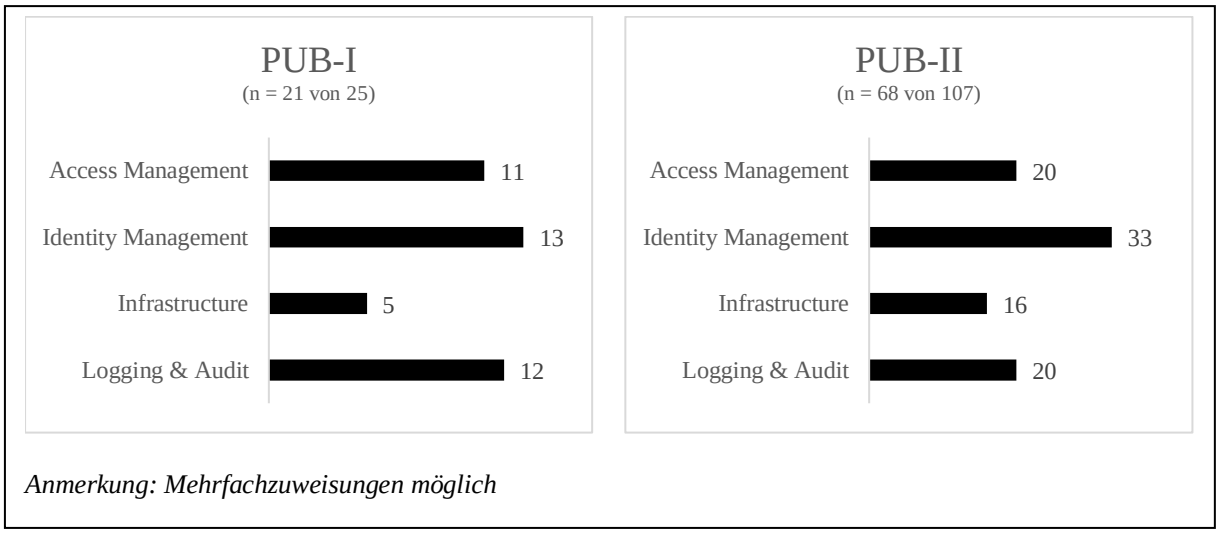


Abbildung 6-4: Verteilung ‚Security' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

6.4.1 Exkurs: Grundlagen des ‚Identity and Access Managements' und dessen Relevanz im Gesundheitswesen

6.4.1.1 Identitäten und ihre Ausprägungen

Eine *Identität* ist die Summe aller Attribute, die eine Entität[415] innerhalb eines Anwendungsgebietes beschreiben.[416] Während das *Anwendungsgebiet* als der Bereich betrachtet wird, in dem eine Entität sich mittels ihrer Eigenschaften identifiziert, fehlt es der *Entität* selbst an einer einheitlichen Definition. Zumeist wird dieser Begriff auf Personen oder Organisationen beschränkt,[417] kann jedoch auch auf sämtliche Objekte, also auch Geräte, z.B. im Rahmen von IoT, erweitert werden.[418]

Grundsätzliche unterscheiden sich Identitäten in drei Kategorien:[419]

i. *Physische Identität*
Eine physische Identität ist bereits durch die bloße Existenz einer Entität gegeben und als Sammelstelle aller Berechtigungen und Rollen zu verstehen.

ii. *Teilidentität*
Teilidentitäten können unterschieden werden in *gelebte* und *kontextuelle* Identität. *Gelebte* Identitäten betrachten bspw. eine Person und die in einer speziellen Umgebung wahrgenommene Aufgabe. Eine Teilidentität kann sich beim Wechsel von Aufgaben ändern. *Kontextuelle* Identitäten sind konkret auf einzelne Rollen zu beziehen und können eine Teilmenge gelebter Identitäten darstellen. Beide zeigen nur einen Ausschnitt der vollständigen Identität.[420]

iii. *Logische Identität*
Logische Identitäten sind technische Abbildungen und Teil von (Informations-)Systemen. Sie werden bspw. als Konto (engl. *account*) organisiert. Hierzu gehören auch *Di-*

---

415 Vgl. ISO/IEC (2019): 1. Des Weiteren existieren *Identifier*, die ein einzigartiges Attribut sind (oder aus einer Kombination mehrerer Attribute bestehen) und nur einer Identität zugewiesen sein können (vgl. Camp (2004): 35; ISO/IEC (2019): 2) sowie *Credentials*, die eine Identität authentifizieren (vgl. ISO/IEC (2019): 4).

416 Vgl. Camp (2004): 35f; Tsolkas/Schmidt (2017): 24; ISO/IEC (2019): 1f.

417 Vgl. Glasser/Vajihollahi (2008): 139; Chadwick (2009): 96.

418 Vgl. Fragoso Rodriguez/Laurent Maknavicius/Incera Dieguez (2006): 1. Die Autoren erweitern die Definition einer Entität auf jedes Objekt, das Transaktionen durchführen kann. Ähnlich gehen TSOLKAS/SCHMIDT vor, die neben natürlichen Personen auch Organisationen, IT-Systeme und IT-Applikationen als Identitätsträger definieren (vgl. Tsolkas/Schmidt (2017): 27-30).

419 Vgl. Tsolkas/Schmidt (2017): 25-27.

420 Vgl. Gomes de Andrade/Monteleone/Martin (2013): 75.

gitale Identitäten, die den von der ISO definierten Begriff der Identität um maschinenlesbare Informationen zur Identifizierung einer Entität ergänzen.[421] Sie bilden dabei Teilidentitäten eines Individuums und können anhand einer Kennung identifiziert werden.[422]

6.4.1.2 Identity-Management

Zur Verwaltung von Identitäten wird ein Identitätsmanagement (IdM) eingesetzt. Es umfasst entsprechend der Definition der ISO alle

> *"processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes (.) in identities (.) known in a particular domain (.)".*[423]

Technisch wird IdM mittels eines Identity Management Systems (IMS) umgesetzt,[424] dessen Aufgabe die *Identifizierung* und *Authentifizierung*[425] von Entitäten ist.[426]

Grundsätzlich werden drei Verwaltungsansätze unterschieden:

i. Isoliertes IdM

Isoliertes IdM beschreibt die Notwendigkeit, dass eine Entität für jeden Anwendungsbereich eine eigene Identität vorzuweisen hat, deren Authentizität von den jeweiligen Service Providern einzeln geprüft wird. Aus Sicht der Service Provider ist diese Variante eine einfache Lösung, jedoch nicht aus Sicht des Anwenders, da dieser mehrere, voneinander unabhängige Identitäten verwalten muss.[427]

---

421 Vgl. Pfitzmann/Hansen (2008): 30f. Digitale Identitäten sind abzugrenzen von elektronischen und virtuellen Identitäten. *Elektronische Identitäten* repräsentieren Identitäten, deren Legitimation auf Basis physischer Nachweise geprüft werden kann (vgl. Grönlund (2010): 195f; Gomes de Andrade/Monteleone/Martin (2013): 78). *Virtuelle Identitäten* stellen weniger die Identität einer Entität als vielmehr die virtuelle Repräsentation dieser dar, bspw. in Form von Avataren in Online-Rollenspielen (vgl. Pfitzmann/Hansen (2008): 31).

422 Vgl. Hansen/Meints (2006): 543.

423 ISO/IEC (2019): 5. Ein IdM ist per Definition ein *privacy-enhancing identity management*, wenn es die Vertraulichkeit wahrt und durch Kenntnis von Teilidentitäten keine Rückschlüsse auf die tatsächliche (Real-)Identität erlaubt (vgl. Pfitzmann/Hansen (2010): 33).

424 Vgl. Ferdous/Poet (2013): 736.

425 Eine Authentifizierung kann dabei mittels wissensbasierter, eigentumsbasierter oder biometrischer Identitätsnachweise durchgeführt werden (vgl. Fragoso Rodriguez/Laurent Maknavicius/Incera Dieguez (2006): 2) und wird an dieser Stelle nicht ausführlicher betrachtet.

426 Vgl. ISO/IEC (2019): 6.

427 Vgl. Jøsang et al. (2005): 100.

ii. Föderiertes IdM

Föderierte Strategien verbinden mehrere, bisweilen isoliert geführte IdM und schaffen einen gemeinsamen Vertrauensraum. Nutzer authentifizieren sich in mehreren Systemen mit den gleichen Identitätsnachweisen. Ein bekannter Ansatz ist bspw. Single-Sign-On (SSO).[428] Aufgrund des gemeinsamen Vertrauensraums und der Möglichkeit, dass mehrere Institutionen auch einen gemeinsamen Identity Provider nutzen können, wird in diesem Zusammenhang auch von *zentralisiertem IdM* gesprochen.[429]

iii. Nutzerzentriertes IdM

Nutzerzentriertes IdM fokussiert auf die Verwaltung von Identitäten durch den Nutzer selbst. Dabei kann dieser selbstständig festlegen, welche Attribute erfasst werden dürfen und welche von anderen abgerufen werden dürfen.[430]

6.4.1.3 Access-Management

Ergänzt wird ein IdM durch die Verwaltung von Zugriffen unter Anwendung ausgewählter Methoden zur Steuerung und Kontrolle von Zugriffen und Zugriffsrechten, dem sogenannten *Access Management (AM)*.[431] Der Zusammenhang zwischen einem IMS und einem *Access Management System (AMS)* wird in *Abbildung 6-5* dargestellt.

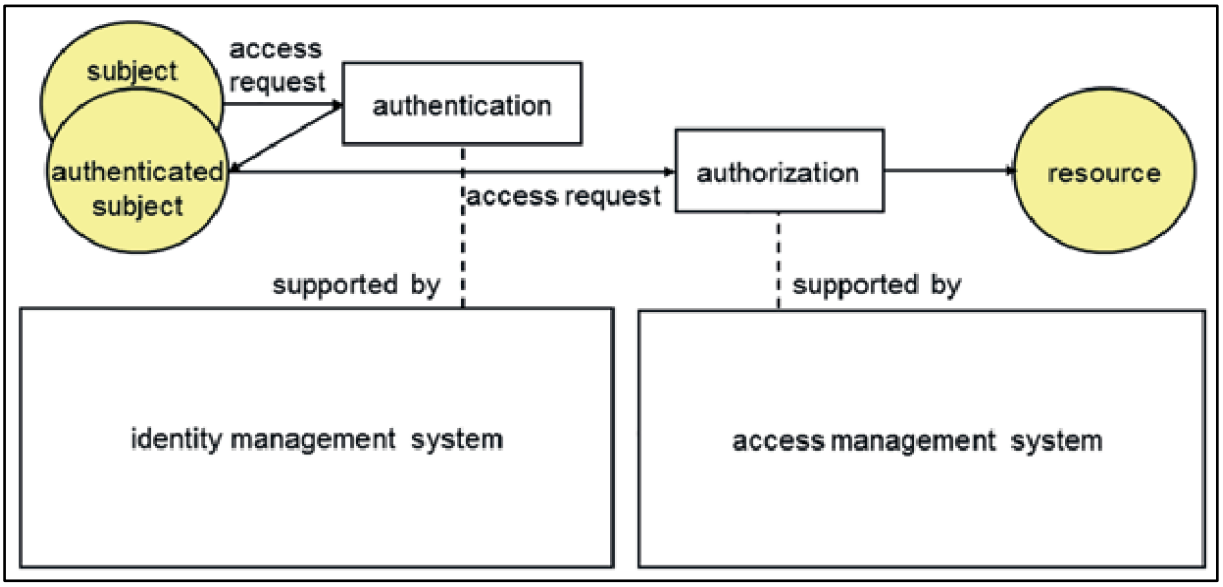


Abbildung 6-5: Zusammenhang zwischen IMS und AMS[432] (Quelle: ISO/IEC (Hrsg.) (2016): 7)

[428] Vgl. Jøsang et al. (2005): 101; Fragoso Rodriguez/Laurent Maknavicius/Incera Dieguez (2006): 2f.

[429] Vgl. Jøsang et al. (2005): 103.

[430] Vgl. Kim et al. (2008): 1308f; Pfitzmann/Hansen (2010): 34.

[431] Vgl. ISO/IEC (2016): 8f; Pohlmann (2019): 214.

[432] Sobald ein Subjekt authentifiziert ist, wird der Zugriff über das AMS gewährt oder verweigert (vgl. ISO/IEC (2016): 6).

Hinter Access Management stehen diverse Modelle, die allgemein in die drei Kategorien *Mandatory Access Control (MAC)*, *Discretionary Access Control (DAC)* und *Role-based Access Control (RBAC)* unterschieden werden.[433] Die entsprechende ISO-Norm 29146 differenziert genauer:[434]

i. Identity-based Access Control (IBAC)
ii. Role-based Access Control (RBAC)
iii. Attribute-based Access Control (ABAC)
iv. Capability-based Access Control (CBAC)
v. Pseudonym-based Access Control (PBAC)

Insbesondere (i), (ii) und (iii) werden in zentral oder verteilt organisierten Architekturen genutzt und über sogenannte Access Control Lists (ACL)[435] überwacht.[436] Die in den drei Kategorien genutzten Identifier der zugreifenden Entität unterscheiden sich insofern als diese bei (i) systemübergreifend genutzt werden können, (ii) diese kategorisiert und entsprechenden Rollen zuweist und (iii) sich einzig auf vorhandene Attribute bezieht, ohne dabei Rolle oder Identität zu berücksichtigen.[437]

6.4.1.4 Identity and Access Management im vernetzten Gesundheitswesen

Zur Vermeidung von medizinischen Behandlungsfehlern durch Fehlidentifikation und zur Vermittlung der bestmöglichen Behandlung ist eine sichere Patientenidentifikation notwendig.[438] Neben der organisatorischen Einrichtung entsprechender Prozesse übernehmen IdM-Systeme die Verwaltung sämtlicher (Teil-)Identitäten. Besonders im Gesundheitswesen ist im Falle von kollaborativem Verhalten die Notwendigkeit eines einrichtungsübergreifenden IAM relevant.

---

433 Vgl. Ni et al. (2010): 24.2. *DAC* sind identitätsbezogene Zugriffsmodelle, bei denen die Identität des Nutzers entscheidet, ob Zugriff gewährt wird oder nicht (vgl. Zhang/Jin (2004): 2691). *MAC* beschreibt Methoden, die sich nicht nur auf die Identität beschränken, sondern auch systemspezifische Attribute zur Kontrolle nutzen (vgl. Eckert (2014): 692). *MAC* und *DAC* bereiten anschließend den Weg zur Gestaltung von *RBAC* (vgl. Zhang/Jin (2004): 2691) und verbinden Identitäten mit Aufgabenbeschreibungen, die über Rollenkonzeptionen Zugriffsmodalitäten organisieren (vgl. Eckert (2014): 268f.).

434 Vgl. ISO/IEC (2016): 19. Die Beschreibung aller in der Auflistung genannten Methoden findet sich in Annex A der zitierten ISO-Norm (siehe ISO/IEC (2016): 31-34).

435 Vgl. ISO/IEC (2016): 9. PBAC wird ebenfalls im Zusammenhang mit ACL genannt, jedoch nicht zusammen mit zentral oder verteilt organisierten Architekturen. Insgesamt sind ACL ähnlich den bereits dargestellten TSL in der Konzeption der GEMATIK.

436 Vgl. ISO/IEC (2016): 9.

437 Vgl. ISO/IEC (2016): 32f; ISO/IEC (2016): 32f.

438 Vgl. Looser (2010): 1; Schneider (2016): 43.

Derzeit existiert kein gemeinsam geführtes Identitätsmanagement im Gesundheitswesen und ebenso wenig gemeinsame Strukturen oder Standardisierungen.[439]

In der Praxis dominieren, bezogen auf *Patientenidentifikation*, zwei Ansätze, die sowohl einrichtungsintern wie auch -übergreifend Anwendung finden:[440]

i. Einsatz eines globalen Identifikators
ii. Zentrale Verwaltung von Identitäten durch eine TTP

Ein *globaler Identifikator (i)*, auch *Master Patient Index* (MPI) genannt, fasst sämtliche Einzelidentitäten eines Patienten zusammen und ermöglicht auf diese Weise eine system- oder sogar einrichtungsübergreifende Identifikation.[441] Im Rahmen der *Integrating-the-Health-Enterprise*-(IHE)-Initiative in den USA wird dieser MPI als *Patient Identifier Cross-referencing Profile (PIX)* bezeichnet.[442] Dabei wird zwischen zwei Sphären, der *Patient Identifier Domain* und der *Patient Identifier Cross-Reference Domain*, unterschieden. Erstere identifiziert einen Patienten innerhalb einer spezifizierten Umgebung. Letztere erlaubt eine Identifikation über Einrichtungs-/Systemgrenzen hinaus (siehe *Abbildung 6-6*).[443]

[439] Vgl. DeSalvo (2016): 12; Gropper (2016): 2f; Roehrs/da Costa/da Rosa Righi (2017): 79; Zhang et al. (2018b): 270. *Anmerkung*: Mit der von der GEMATIK konzipierten elektronischen Gesundheitskarte geht das deutsche Gesundheitswesen schon einen Schritt in diese Richtung.

[440] Vgl. Peterson et al. (2016): 7.

[441] Vgl. Deng et al. (2008): 3; Baksi (2009): 162; Looser (2010): 8f.

[442] Vgl. ACC/HIMSS/RSNA (2005): 33.

[443] Vgl. ACC/HIMSS/RSNA (2005): 34.

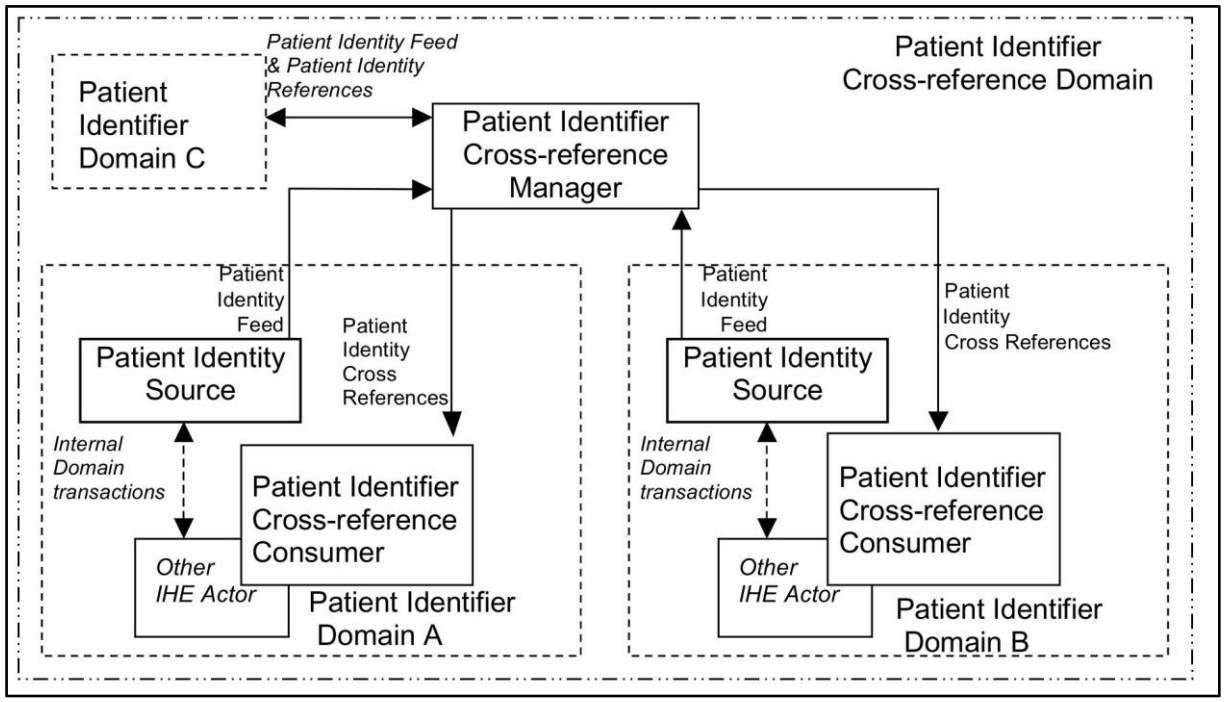


Abbildung 6-6: Prozess für übergreifende Referenzierung von Patienten Identifikatoren (Quelle: ACC/HIMSS/RSNA (2005): 33)

Ein MPI unterstützt die Standardisierung von Prozessen und Zugriffsmethoden und stärkt die Vertraulichkeit von Informationen, erlaubt aber ebenso Rückschlüsse auf Personen und die Erstellung umfangreicher Profile.[444] Aus diesem Grund existieren bereits Methoden, die entweder auf einen MPI verzichten[445] oder einen MPI verwenden, dessen Konstruktion aber einen Rückschluss auf die Realidentität nicht zulässt.[446]

Die zentrale *Verwaltung von Identitäten mittels einer TTP (ii)* unterstützt Netzwerkteilnehmer, die mit der einrichtungsübergreifenden Identifikation überfordert sind. Diese TTP führt als Intermediär eine Liste sämtlicher Identitäten und ermöglicht eine gemeinsame Kommunikation unter Anwendung individueller Semantik.[447] Der Einsatz einer TTP, im Weiteren als *Mediator* bezeichnet, wird in *Abbildung 6-7* beschrieben. Ein Risiko ist dabei jedoch die Abhängigkeit des Netzwerks von der Zuverlässigkeit der TTP (*Misplaced Trust*).[448]

444 Vgl. Appavu (1997): 28f.

445 Vgl. Soenens (2009): 61f. In diesem Zusammenhang wird auf ein Forschungsprojekt namens ARTEMIS verwiesen, dessen Publikationen jedoch nicht mehr abrufbar sind. Dort wird von einem *Patient Identification Process* gesprochen, der Patienten ohne einen eindeutigen Identifier dennoch in Systemen identifiziert und Gesundheitsinformationen lokalisiert (vgl. Phys.org (2006)).

446 Vgl. Schaar (2005): 165f.

447 Vgl. Hu/Peyton (2009): 105; National HIE Governance Forum (2013): 3. Der hier genannte *Master Index* ist ein Register und kein MPI, wie er in (i) beschrieben wurde.

448 Vgl. Dólera Tormo et al. (2013): 34.

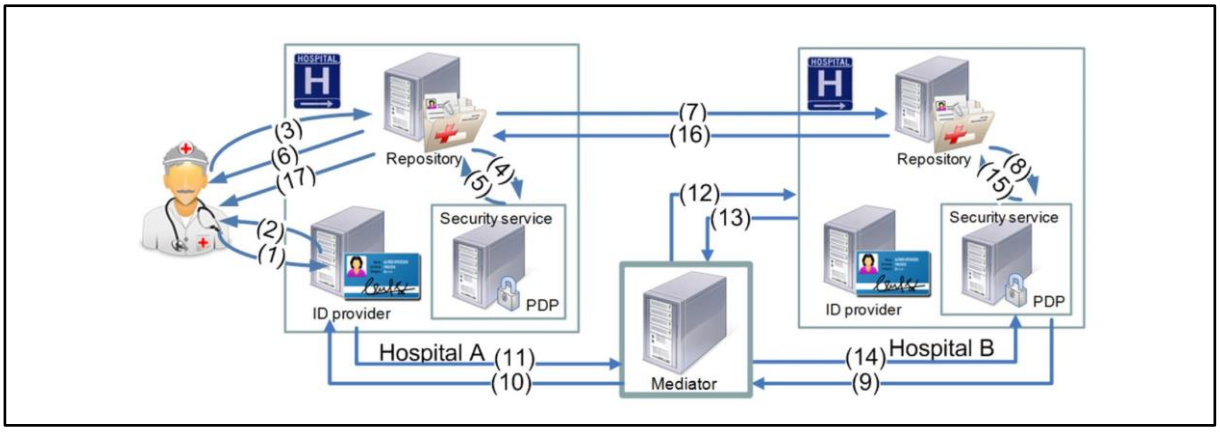


Abbildung 6-7: Ablauf einer interinstitutionellen Datenanfrage[449]
(Quelle: Deng et al. (2008): 5)

Auch die einrichtungsübergreifende und interoperable Verwaltung von Zugriffsberechtigungen eines AM ist herausfordernd.[450] Auf der einen Seite stehen die Leistungserbringer und Netzwerkbetreiber, die den Ansprüchen der Informationssicherheit gerecht werden müssen, auf der anderen Seite die Patienten, die von ihrem Recht auf informationelle Selbstbestimmung Gebrauch machen möchten.[451] Daher ist Ziel eines AM nicht nur die Absicherung der direkten Zugriffe auf Daten, sondern ebenfalls die Kontrolle sekundärer Zugriffe.[452] Anforderungen an ein solches AM sind:[453]

i. Openness
ii. Individual control
iii. Collection limitation
iv. Purpose specification
v. Consent
vi. Data quality
vii. Data security

Für die Ausgestaltung des IAM und zur Wahrung von Datensicherheit und -schutz werden IdM und AM getrennt voneinander konzipiert.[454] Diesem Ansatz folgen die nächsten Kapitel, die konkret auf die Konstruktion der Referenzarchitektur eingehen.

---

449 Eine Beschreibung der in der Abbildung gezeigten Schritte findet sich in Deng et al. (2008): 4.

450 Vgl. Schneider (2016): 50.

451 Vgl. Haas (2017): 9.

452 Vgl. Ardagna et al. (2008): 370.

453 Vgl. Ardagna et al. (2008): 370f. Die Anforderungen sind abgeleitet aus einem Bericht der OECD, der nur in einer aktualisierten Fassung von 2013 vorliegt (siehe OECD (2013)). In diesem fehlt es an konkreter Nennung dieser sieben Anforderungen. Letztere sind, jedoch verklausuliert, noch in der Online-Quelle zu finden.

454 Vgl. Soenens (2009): 62.

6.4.2 Identity and Access Management

Dieses Kapitel unterteilt das Thema Security in *Access Management* und *Identity Management* und betrachtet dabei die unterschiedlichen Zugriffmethoden, die in Blockchain-Netzwerken Anwendung finden, bspw. *Role-based* oder *Attribut-based Access*. Darüber hinaus werden die unterschiedlichen Formen von Identitäten betrachtet sowie deren Authentifikation.

6.4.2.1 Access Management

Blockchain übernimmt im Access-Management (AM) eine verwaltende Funktion und erlaubt eine sichere Speicherung von erteilten Berechtigungen in Form von Transaktionen,[455] die wiederum über Smart Contracts[456] automatisiert abgerufen oder verwaltet werden.[457] Ein Beispielprozess, wie ein AM unter Einsatz einer Blockchain durchgeführt werden kann, findet sich bei ZHANG/POSLAD/MA, wird an dieser Stelle aber aufgrund der Komplexität nicht ausführlicher beschrieben.[458]

Grundsätzlich verspricht Blockchain eine feingranulare Steuerung von Berechtigungen.[459] Unter Einbezug der in *Kapitel 6.4.1.3* beschriebenen Zugriffs-Modelle können in den hier zugrunde gelegten Publikationen folgende Zugriffskontrollmechanismen identifiziert werden:[460]

i. Attribute-based Access Control (ABAC)
ii. Discretionary Access Control (DAC)
iii. Entity-based Access Control (EBAC)
iv. Identity-based Access Control (IBAC)
v. Role-based Access Control (RBAC)

Diese verteilen sich entsprechend *Tabelle 6-2* und *Abbildung 6-8* auf die Literatur.

---

455 Vgl. Zyskind/Nathan/Pentland (2015): 181; Azaria et al. (2016): 26; Ekblaw et al. (2016): 3f; Linn/Koo (2016): 3; Genestier et al. (2017): 2f; Rifi et al. (2017): 200; Xia et al. (2017b): 48; Hussein et al. (2018): 2f; Medicalchain (2018): 12, 14, 20; Mikula/Jacobsen (2018): 701f; Quaini et al. (2018): 169; Ramani et al. (2018): 3718; Ribitzky et al. (2018): 4; Theodouli et al. (2018): 1376; Xiao et al. (2018): 1002; Zhang et al. (2018a): 3.

456 Siehe *Kapitel 6.5.3*.

457 Vgl. Alhadhrami et al. (2017): 376; McFarlane et al. (2017): 9; Yang/Li (2018): 265. Dies ist insbesondere bei *Konsortialen Blockchains* der Fall (vgl. Theodouli et al. (2018): 1376).

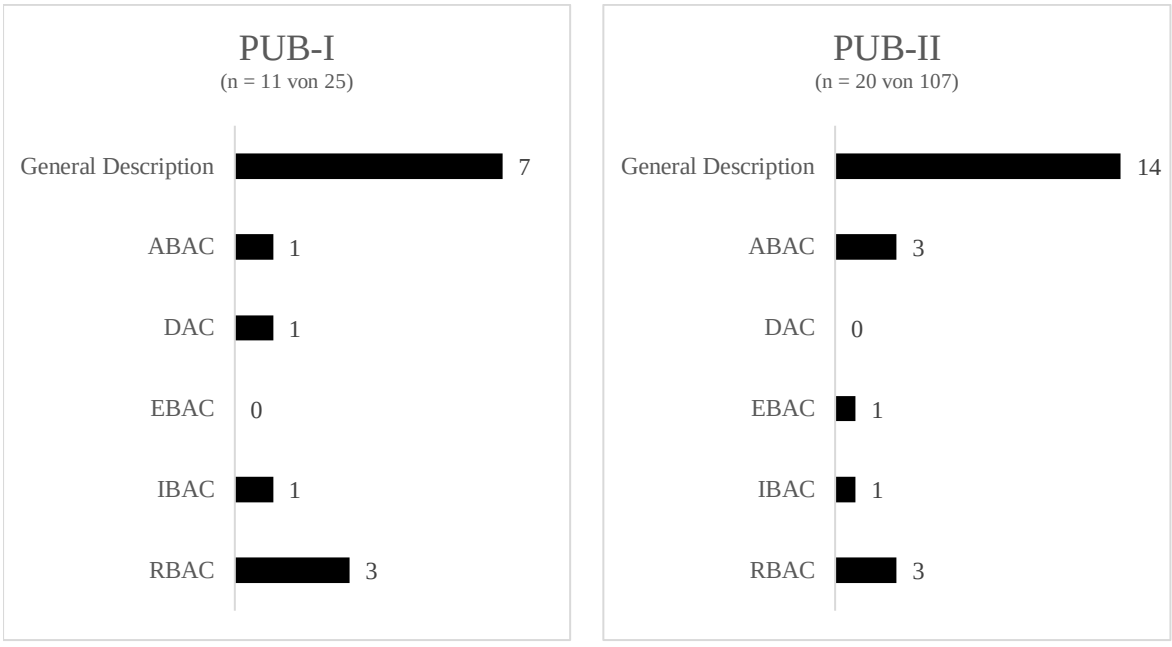
458 Vgl. Zhang/Poslad/Ma (2018): 3726f.

459 Vgl. Liu et al. (2017): 39.

460 Es existieren Publikationen, die einzig den Einsatz von ACL benennen und nicht differenzierter auf die AM-Methoden eingehen (vgl. Alhadhrami et al. (2017): 376f; Patel (2018): 7). Aufgrund dessen, dass ACL die Grundlage für ABAC, IBAC und RBAC sind (vgl. ISO/IEC (2016): 9), werden diese nicht separat betrachtet und in Zusammenhang mit den hier bezeichneten AM-Methoden berücksichtigt.

Tabelle 6-2: Literatur-Kategorien ‚Security – Identity and Access Management – Access Management' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
General Description	Azaria et al. (2016); Ekblaw et al. (2016); McFarlane et al. (2017); Medicalchain (2018); Quaini et al. (2018); Xiao et al. (2018); Yang/Li (2018)	Linn/Koo (2016); Alhadhrami et al. (2017); Genestier et al. (2017); Liu et al. (2017); Rifi et al. (2017); Xia et al. (2017b); Hussein et al. (2018); Mikula/Jacobsen (2018); Patel (2018); Ramani et al. (2018); Ribitzky et al. (2018); Theodouli et al. (2018); Zhang et al. (2018a); Zhang/Poslad/Ma (2018)
ABAC	Zhang et al. (2018b)	Cyran (2018); Dias et al. (2018); Pussewalage/Oleshchuk (2018)
DAC	Rouhani et al. (2018)	
EBAC		Dias et al. (2018)
IBAC	Al Omar et al. (2017)	Zhang et al. (2018a)
RBAC	Chang et al. (2018); Rouhani et al. (2018); Zhang et al. (2018b)	Dubovitskaya et al. (2017); Kim/Hong (2017); Dias et al. (2018)



Anmerkung: Mehrfachzuweisungen möglich

Abbildung 6-8: Verteilung ‚Security – Identity and Access Management – Access Management' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

6.4.2.1.1 Attribute-based Access Control (ABAC)

ABAC sowie RBAC[461] sind etablierte Kontrollmechanismen im Gesundheitswesen.[462] ABAC orientiert sich an den Attributen, die einer Entität zugewiesen sind, und gestattet auf dieser

[461] Siehe *Kapitel 6.4.2.1.5.*

[462] Vgl. Li et al. (2010): 92; Dias et al. (2018): 2; Zhang et al. (2018b): 272.

Basis den Zugriff. Dabei werden neben der einzelnen Entität Attribute der relevanten Umwelt und der abgelegten Daten in die Bewertung mit einbezogen.[463] Der Umstand, dass identitätsunabhängige Attribute zur Gewährung von Zugriffen genutzt werden, erlaubt es dieser Form des AM, insbesondere in der interorganisationalen Verwaltung von Zugriffen, Anwendung zu finden. Problematisch ist jedoch die fehlende Standardisierung in der Auswahl der relevanten Attribute.[464]

6.4.2.1.2 Discretionary Access Control (DAC)

DAC verknüpft Objekte direkt mit dem Eigentümer und erlaubt auch nur diesem die Kontrolle über sämtliche Zugriffe. Aufgrund dieser 1:1-Beziehung muss in Systemen zu jedem Objekt auch eine Information über dessen Eigentümer abgelegt sein.[465]

6.4.2.1.3 Entity-based Access Control (EBAC)

EBAC kombiniert in der Zugriffssteuerung die Konzepte der ABAC und des Relationship-Based Access Control (ReBAC),[466] sodass nicht nur die Attribute von Entitäten, sondern auch definierte Beziehungen der Entitäten untereinander in die Erteilung von Berechtigungen einbezogen werden.[467] Aufgrund dessen, dass die Erstellung von Entitäten sowie ihre Beziehungen untereinander in Transaktionen dargestellt werden, kann die Blockchain diese Informationen aufnehmen und verwalten.[468]

6.4.2.1.4 Identity-based Access Control (IBAC)

Bei Verwendung der Blockchain werden abhängig von der Validierung einer Identität und der auf der Blockchain verfügbaren Informationen Zugriffsberechtigungen erteilt.[469] Die Überprüfung der Identität kann beispielsweise durch ein Gateway erfolgen, das die Identität über die Abfrage von Benutzername und Passwort prüft und entsprechend die Freigaben erteilt.[470]

---

463 Vgl. Hu et al. (2014): 7; Cyran (2018): 3; Zhang et al. (2018b): 272.

464 Vgl. Pussewalage/Oleshchuk (2018): 1204.

465 Vgl. Rouhani et al. (2018): 1536.

466 ‚ReBAC' wird in diesem Zusammenhang nicht näher thematisiert. Es wird diesbezüglich auf Hu/Ahn/Jorgensen (2013) verwiesen.

467 Vgl. Bogaerts et al. (2015): 293.

468 Vgl. Dias et al. (2018): 4f.

469 Vgl. Zhang et al. (2018a): 5.

470 Vgl. Al Omar et al. (2017): 537-539. Die beschriebene *Privacy Accessible Unit* ist keine Lösung unter Anwendung der Blockchain, sondern ein vorgeschaltetes Gateway, das prüft, ob Daten an den Anfragenden herausgegeben werden können. Bei positiver Entscheidung wird die Position der Daten auf der Blockchain übermittelt.

6.4.2.1.5 Role-based Access Control (RBAC)

RBAC sowie ABAC[471] sind etablierte Kontrollmechanismen im Gesundheitswesen.[472] Den Netzwerkteilnehmern werden Rollen zugewiesen, an denen sich die Zugriffsberechtigungen orientieren.[473] Diese Rollen variieren je nachdem, welche Entitäten im Netzwerk teilnehmen.[474] Dennoch führt die ausschließliche Nutzung von RBAC ohne Kombination mit ABAC oder I-BAC nicht zu einer absolut sicheren Zugriffskontrolle.[475]

6.4.2.2 Identity Management

Blockchain übernimmt im Identitätsmanagement vornehmlich die Authentifikation von Identitäten und verwendet hierfür bekannte Instrumente, wie bspw. Biometrie oder Benutzername-Passwort-Kombinationen. Darüber hinaus wird in diesem Zusammenhang auch die Verwaltung mehrerer Identitäten sowie deren Zusammenführung in einem Master-Patient-Index diskutiert. *Tabelle 6-3* und *Abbildung 6-9* beschreiben die Verteilung auf die Literatur, während die folgenden Kapitel detailliert auf die einzelnen Ausprägungen eingehen.

Tabelle 6-3: Literatur-Kategorien ‚Security – Identity and Access Management – Identity Management' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
General Description	Gropper (2016); Vora et al. (2018); Zhang et al. (2018b)	Cunningham/Ainsworth (2017); Bhuiyan et al. (2018); Chen et al. (2018a); Chowdhury et al. (2018)
Authentication _General Description		Yang/Yang (2017); Qiu et al. (2018)
Authentication_Attriute-based_Asymmetric	Zhang et al. (2018b)	Conceição et al. (2018); Mikula/Jacobsen (2018)
Authentication_Attriute-based_Biometric	Medicalchain (2018)	Linn/Koo (2016)
Authentication_Identity-based_Two-Factor		Yli-Huumo et al. (2016)
Authentication_Identity-based_UserName-Password	Al Omar et al. (2017); Hanley/Tewari (2018)	Dubovitskaya et al. (2017); Conceição et al. (2018); Pukas/Smal/Zabchuk (2018); Wu/Tsai (2018)

[471] Siehe *Kapitel 6.4.2.1.1*.

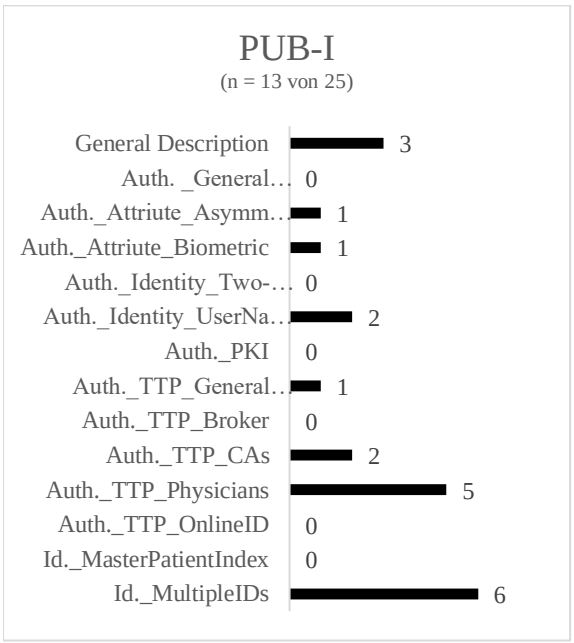
[472] Vgl. Li et al. (2010): 92; Dias et al. (2018): 2; Zhang et al. (2018b): 272.

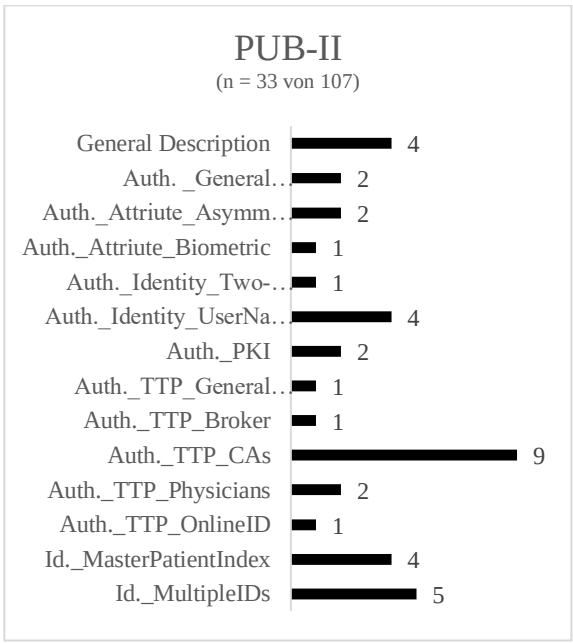
[473] Vgl. Dubovitskaya et al. (2017): 655; Kim/Hong (2017): 80f; Rouhani et al. (2018): 1536.

[474] Chang et al. beschränken sich auf zwei Rollen, Patient und Leistungserbringer (vgl. Chang et al. (2018): 176). Sie begründen ihre Beschränkung mit der Notwendigkeit, dass die Entscheidung über die Verteilung und Nutzung von Gesundheitsdaten Aufgabe des Patienten ist. Sie differenzieren ihre Stakeholder nicht explizit und beziehen Forschung und Kostenträger erst bei der Bezeichnung der *Data Guests* in ihre Betrachtung mit ein (vgl. Chang et al. (2018): 175).

[475] Vgl. Deng et al. (2008): 3. Ein potenzielles Szenario wird in der Quellenangabe genannt. Die Komplexität von ABAC ist in der Kombination mit RBAC nicht zu unterschätzen (vgl. Zhang/Liu (2010): 273).

Authentication_PKI		Chen et al. (2018b); Thwin/Vasupongayya (2018)
Authentication_TTP_General Description	Gropper (2016)	Dubovitskaya et al. (2017)
Authentication_TTP_Broker		Gagnon/Stephen (2018)
Authentication_TTP_CAs	Fan et al. (2018); Rouhani et al. (2018)	Dubovitskaya et al. (2017); Genestier et al. (2017); Liang et al. (2017b); Liu et al. (2017); Noh et al. (2017); Bhuiyan et al. (2018); Castaldo/Cinque (2018); Liang et al. (2018a); Zhang et al. (2018a)
Authentication_TTP_Physicians	Azaria et al. (2016); Ekblaw et al. (2016); Hanley/Tewari (2018); Quaini et al. (2018); Zhang/Lin (2018)	Mikula/Jacobsen (2018); Ramani et al. (2018)
Authentication_TTP_OnlineID		Liang et al. (2018b)
Identity_MasterPatientIndex		Peterson et al. (2016); Gordon/Catalini (2018); Mense/Athanasiadis (2018); Sharma/Sekharan/Zuo (2018)
Identity_MultipleIDs	Azaria et al. (2016); Ekblaw et al. (2016); Hanley/Tewari (2018); Jiang et al. (2018); Vora et al. (2018); Zhang/Lin (2018)	Zyskind/Nathan/Pentland (2015); Badr/Gomaa/Abd-Elrahman (2018); Gutierrez et al. (2018); Pukas/Smal/Zabchuk (2018); Pussewalage/Oleshchuk (2018)





Anmerkung: Mehrfachzuweisungen möglich

Abbildung 6-9: Verteilung ‚Security – Identity and Access Management – Identity Management' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

6.4.2.2.1 Authentication

Der Begriff der *Authentication* bzw. *Beglaubigung* definiert die endgültige Bestätigung, dass eine Entität entsprechend ihren Eigenschaften zu einer Aktion berechtigt ist.[476] Der deutsche Begriff von Authentication lautet *Authentifikation* und unterscheidet genauso wie *Autorisierung* im Access-Management zwischen identitätsbasierter und attributsbasierter Authentifizierung. Während Erstere nur die Beziehung zwischen einer Entität und eines Identifiers prüft und auf Informationen zurückgreift, die nur der zu Identifizierende kennt,[477] beschäftigt sich Letztere mit der Beziehung zwischen einer Entität und eines mit dieser Entität verknüpften Attributs.[478]

Im Rahmen der Literaturanalyse haben sich für die blockchain-basierte Gesundheitsdatenvernetzung folgende Ansätze der Authentifizierung ergeben:

i. Identitätsbasierte Authentifizierung (*Identity Authentication*)
    a. Benutzername und Passwort[479]
    b. Zwei-Faktor-Authentifizierung[480]
ii. Attributsbasierte Authentifizierung (*Attribute Authentication*)
    a. Biometrie[481]
    b. Asymmetrische Schlüsselpaare (Public/Private-Keys (ohne Public-Key-Infrastructure))[482]
iii. Public Key Infrastructure[483]
iv. Nutzung einer TTP[484]

Die Nutzung von *Benutzername und Passwort (i.a.)* ist die für einen Nutzer bekannteste Verifizierungsmethode und kann über die *Zwei-Faktor-Authentifizierung (i.b.)*, die einen weiteren Faktor, wie z.B. einen Hardware-Token, nutzt, erweitert werden. Eine weitere Steigerung dieser Authentifizierungsmethoden findet sich in der *Biometrie (ii.a.)*, die bspw. einen Fingerabdruck

476 Vgl. Camp (2004): 36.

477 Vgl. Camp (2004): 36.

478 Vgl. Camp (2004): 36.

479 Vgl. Al Omar et al. (2017): 539; Dubovitskaya et al. (2017): 652; Conceição et al. (2018): 9; Hanley/Tewari (2018): 250; Pukas/Smal/Zabchuk (2018): 174; Wu/Tsai (2018): 70.

480 Vgl. Yli-Huumo et al. (2016): e0163477.15–16.

481 Vgl. Linn/Koo (2016): 6; Medicalchain (2018): 12.

482 Vgl. Conceição et al. (2018): 9; Mikula/Jacobsen (2018): 699; Zhang et al. (2018b): 272.

483 Vgl. Chen et al. (2018b): 5.3; Thwin/Vasupongayya (2018): 199.

484 Vgl. Dubovitskaya et al. (2017): 657.

oder andere biometrische Marker einer Entität nutzt. Dennoch ist der tatsächliche Grad an Sicherheit bei der Nutzung dieser Methoden eingeschränkt.[485]

Eine mögliche Lösung wird in der Nutzung von *Public/Private-Keys (ii.b.)* gesehen, die zwar an eine *Public-Key-Infrastructure (iii)* erinnern, jedoch abweichend von einer PKI ohne eine zentrale *Certificate Authority* auskommen. Dies erlaubt es Entitäten, mehrere Public-Keys unter einem Private-Key zu führen und in einer eigenen Wallet zu verwalten. Sie haben damit im Vergleich zur Authentifizierung von Identitäten über eine PKI einen höheren Grad an Anonymität.[486] Eine nähere Beschreibung der Nutzung von Public-Key-Infrastrukturen (iii) ist in *Kapitel 6.4.3* zu finden.

Die *Nutzung einer TTP (iv)* beruht auf der Notwendigkeit, Teilnehmer im Netzwerk eindeutig zu identifizieren. Die in *Kapitel 6.4.2.2.1* dargestellten pseudonymen Identitäten ermöglichen keinen Rückschluss auf die Realidentität von Patienten, sodass insbesondere bei der Nutzung öffentlicher Blockchains Vertraulichkeit gewahrt bleibt,[487] läuft allerdings der Gewährleistung einer sicheren Patientenidentifikation zuwider.[488] Aus diesem Grund gibt es Überlegungen, diese Identitäten mit der Real-Identität eines Patienten zu verknüpfen.[489] Dabei wird die Annahme vertreten, dass die Aufgabe einer sicheren Identitätsverwaltung nicht von der Öffentlichkeit, respektive den Blockchain-Netzwerk-Teilnehmern, übernommen werden kann, sondern von denen, die Daten bereitstellen bzw. verwahren.[490] Die Einrichtung dieser TTP wird in den identifizierten Publikationen in unterschiedlicher Form konzipiert und entweder in Form von Broker-Netzwerken,[491] einer Registrierungspflicht von Patienten in Einrichtungen der Leistungserbringer[492], einer Online-ID[493] oder durch Nutzung von *Certificate Authorities* (CA)[494] realisiert. Grundsätzlich gilt bei der Auswahl einer TTP, dass derjenige die Verwaltung

485 Vgl. Qiu et al. (2018): 681. Mehr Informationen zu diesem Thema finden sich bei XIAO (2005).

486 Vgl. Yang/Yang (2017): 107f.

487 Vgl. Vora et al. (2018): 981.

488 Vgl. Zhang et al. (2018b): 271.

489 Vgl. Gropper (2016): 2; Chen et al. (2018a): 206; Chowdhury et al. (2018): 1332.

490 Vgl. Cunningham/Ainsworth (2017): 46.

491 Vgl. Gagnon/Stephen (2018): 3f. Zugriff erhalten Organisationen durch Anfrage bei den Brokern, die anschließend den Zugriff gewähren, indem der Private Schlüssel des Patienten übermittelt wird.

492 Vgl. Azaria et al. (2016): 27; Ekblaw et al. (2016): 5; Hanley/Tewari (2018): 250; Mikula/Jacobsen (2018): 703; Quaini et al. (2018): 170; Ramani et al. (2018): 3720f; Zhang/Lin (2018): 140.5; Zhang/Lin (2018): 140.9.

493 Vgl. Liang et al. (2018b): 391.

494 Vgl. Liu et al. (2017): 40; Noh et al. (2017): 135, 141f; Bhuiyan et al. (2018): 63; Castaldo/Cinque (2018): 52; Fan et al. (2018): 136.3. Darüber hinaus enthält der von Hyperledger Fabric eingerichtete Membership Service eine CA (vgl. Dubovitskaya et al. (2017): 655; Genestier et al. (2017): 2; Liang et al. (2017b): 1170; Liang et al. (2018a): e3.10; Rouhani et al. (2018): 1534; Zhang et al. (2018a): 3). Die Aufgaben der Certificate Authority im Rahmen der Public-Key-Infrastruktur wird in *Kapitel 6.4.3.1* behandelt.

von Identitäten übernehmen sollte, der kein Interesse an der Verwertung von Gesundheitsdaten hat.[495]

6.4.2.2.2 Master Patient Index - Verwendung mehrerer Identitäten und deren Zusammenfassung

IdM-Lösungen zur Vernetzung von Gesundheitsdaten stehen vor der Herausforderung, nicht nur eine sichere Patientenidentifikation gewährleisten zu müssen, sondern gleichzeitig die Vertraulichkeit von Gesundheitsdaten sicherzustellen.[496]

Blockchain-basierte Architekturen hängen die relevanten Identitätsinformationen den auf der Blockchain enthaltenen Transaktionsinformationen an, sodass jede Transaktion einer Identität zugeordnet wird.[497] Die Identitätsinformation kann eine zufällig gewählte Blockchain-Adresse sein,[498] die nicht in einer TTP registriert werden muss,[499] aber auch ein konkreter Hashwert auf Basis einer Kombination diverser demographischer Informationen, die in einer TTP im Vorfeld registriert wurden.[500]

Während Letzteres eine statische Lösung ähnlich der Versichertennummer in Deutschland darstellt, führt die Nutzung einer Blockchain-Adresse zur Erstellung eines *Master Patient Index* (MPI)[501]. Dieser fasst sämtliche Teilidentitäten eines Patienten in einer übergeordneten Identität in Form eines Register zusammen und hat sich in der wissenschaftlichen Literatur bereits im Zusammenhang mit *Patient Matching*, dessen Aufgabe die Zuordnung von verteilt abgelegten Informationen zu einem bestimmten Patienten ist, etabliert.[502] Eine Blockchain bildet dabei das

---

[495] Vgl. Gropper (2016): 2. Der Autor beschreibt in diesem Zusammenhang den Einsatz von *Dezentralen Identitäten* (Decentralized Identity (DID)) als Alternativen zu dem bisher genutzten Domain Name System (DNS), das bspw. im Internet die IP-Adresse einer lesbaren Webadresse zuweist (vgl. Gropper (2016): 6).

[496] Siehe *Kapitel 6.4.1.4*.

[497] Vgl. Bhuiyan et al. (2018): 66.

[498] Vgl. Zyskind/Nathan/Pentland (2015): 182; Gutierrez et al. (2018): 212; Jiang et al. (2018): 52; Pukas/Smal/Zabchuk (2018): 172; Vora et al. (2018): 980; Zhang/Lin (2018): 140.9. Grund für die Nutzung mehrerer Adressen ist die Möglichkeit der Identifizierung von Patienten. So können bspw. auf Basis der Meta-Daten einer Ethereum-Adresse Rückschlüsse auf den Echtnamen einer Entität gemacht werden, sollte diese häufiger verwendet werden (vgl. Pukas/Smal/Zabchuk (2018): 172).

[499] Vgl. Pussewalage/Oleshchuk (2018): 1210. Die Erstellung der Blockchain-Adresse führt zur Entstehung eines Public/Privat-Schlüsselpaars, das die virtuelle Identität (siehe *Logische* bzw. *Digitale Identität* in *Kapitel 6.4.1.1*) des Patienten widerspiegelt (vgl. Badr/Gomaa/Abd-Elrahman (2018): 160).

[500] Vgl. Azaria et al. (2016): 26; Ekblaw et al. (2016): 3f; Hanley/Tewari (2018): 247f. Die Nutzung der Sozialversicherungsnummer steht in der Kritik (vgl. Hanley/Tewari (2018): 250).

[501] Bei der Nutzung des Begriffs muss unterschieden werden zwischen einem identitätsbezogenen und einem inhaltsbezogenen Index. Der Fokus eines Großteils der MPI-Literatur liegt auf einem übergeordneten Index, der Identitäten bündelt, während einzelne Publikationen diesen Begriff auch nutzen, wenn eine Gesamtübersicht aller Daten eines Patienten hergestellt werden soll. In dieser Dissertation wird ein MPI mit identitätsbezogenen Indizes gleichgestellt.

[502] Vgl. Just et al. (2016): 1e.2; Gordon/Catalini (2018): 227.

Register dieser Identitäten und verwaltet jede Einzelidentität in der Wallet eines Patienten.[503] Die Verwaltung dieses MPI kann alternativ auch von Smart Contracts übernommen werden.[504] Zur Verwendung von Blockchain-Adressen als Einzelidentität wird diese entweder vom Leistungserbringer weiterverwendet oder mit dem lokalen Identifier des eigenen Systems verknüpft.[505]

6.4.3 Infrastrukturen

Die analysierten Publikationen unterscheiden zwischen zwei Infrastrukturen, nämlich der *Public-Key-Infrastructure* (PKI) und der *Keyless Signature Infrastructure* (KSI). Die Verteilung wird in *Tabelle 6-4* und *Abbildung 6-10* dargestellt und in den Folgekapiteln beschrieben.

Tabelle 6-4: Literatur-Kategorien ‚Security – Infrastructure' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
KSI		Benchoufi/Ravaud (2017); Liang et al. (2017a); Nagasubramanian et al. (2018)
PKI	Fan et al. (2018); Rouhani et al. (2018); Xiao et al. (2018); Zhang et al. (2018b); Zhou/Wang/Sun (2018)	Nichol/Brandt (2016); Dubovitskaya et al. (2017); Genestier et al. (2017); Liang et al. (2017b); Liu et al. (2017); Noh et al. (2017); Bhuiyan et al. (2018); Castaldo/Cinque (2018); Gordon/Catalini (2018); Liang et al. (2018a); Thwin/Vasupongayya (2018); Zhang et al. (2018a); Zheng et al. (2018)

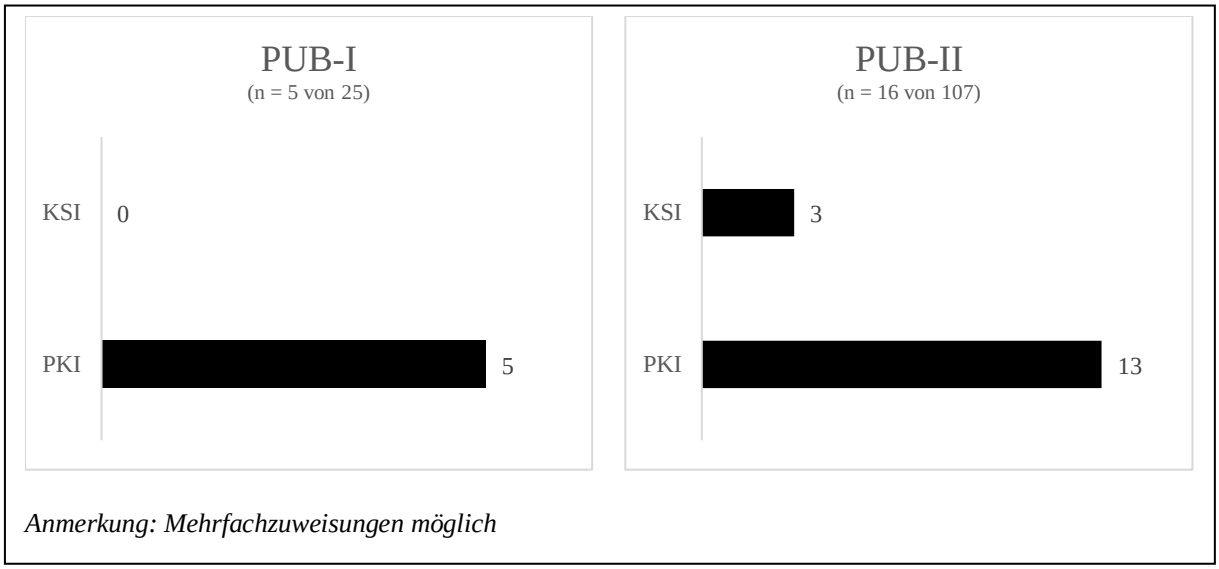


Abbildung 6-10: Verteilung ‚Security – Infrastructure' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

[503] Vgl. Peterson et al. (2016): 7; Sharma/Sekharan/Zuo (2018): 984.

[504] Vgl. Mense/Athanasiadis (2018): 9.

[505] Vgl. Gordon/Catalini (2018): 227.

6.4.3.1 Public-Key-Infrastructure

Eine PKI erstellt im Rahmen der asymmetrischen Verschlüsselung ein Schlüsselpaar aus Privatem und Öffentlichem Schlüssel. Eine ergänzend genutzte CA bestätigt als zentrale Instanz die Validität des Schlüsselpaars über die Ausstellung eines Zertifikats (siehe *Abbildung 6-11*).[506]

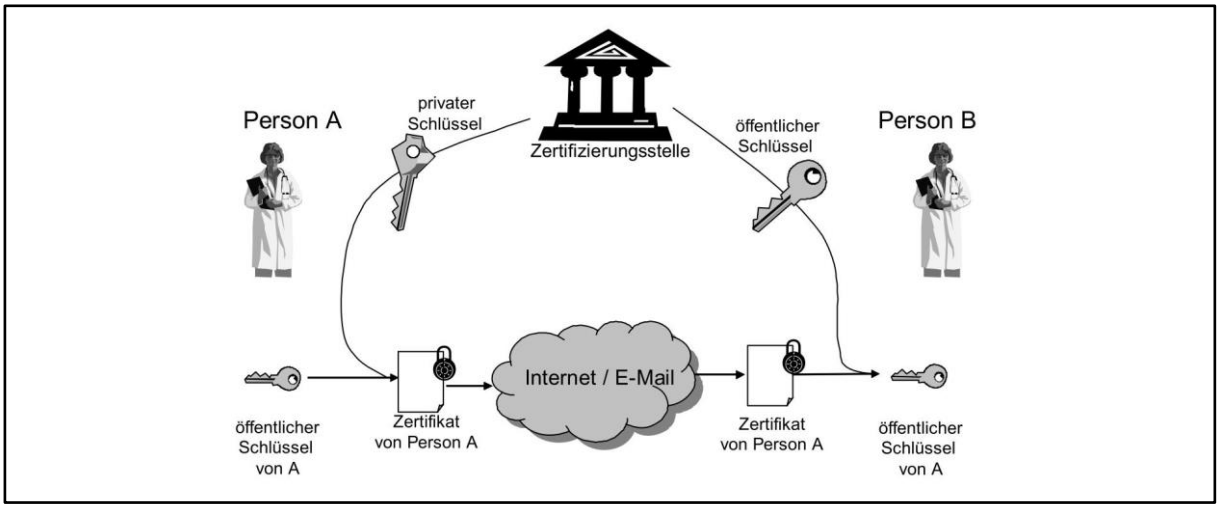


Abbildung 6-11: Struktur einer Public-Key-Infrastruktur (Quelle: Haas (2006): 176)

Obwohl einzelne Publikationen die Nutzung der Blockchain-Technologie mit der Nutzung einer Public-Key-Infrastruktur gleichsetzen und die daraus resultierende höhere Vertraulichkeit von Gesundheitsdaten betonen,[507] muss darauf hingewiesen werden, dass Blockchain per se keine herkömmliche PKI darstellt. Innerhalb der Blockchain existieren zwar die genannten asymmetrischen Schlüsselpaare,[508] doch beruht das Vertrauen in die Blockchain auf der Liste sämtlicher historischer Transaktionen und nicht auf der Nutzung einer CA als TTP.[509]

Dennoch beschreibt ein Teil der identifizierten Publikationen Tendenzen, sich weiterhin auf die Sicherheitsmechanismen der etablierten Public-Key-Infrastrukturen (PKI) zu verlassen, wie auch auf die Nutzung einer CA.[510] Ziel ist dabei, die Identität der am Blockchain-Netzwerk

---

506 Vgl. Franco (2014): 55.

507 Vgl. Liang et al. (2017b): 1167; Liang et al. (2018a): e3.2.

508 Vgl. Zhang et al. (2018b): 271f; Zhou/Wang/Sun (2018): 149.3.

509 Auch existieren Methoden, eine PKI ohne CA auf einer Blockchain darzustellen (vgl. Ali (2017): 39). Eine tiefergehende Betrachtung dieser Thematik wird an dieser Stelle nicht vorgenommen.

510 Vgl. Nichol/Brandt (2016): 2; Dubovitskaya et al. (2017): 655; Genestier et al. (2017): 2; Liu et al. (2017): 40; Noh et al. (2017): 135; Bhuiyan et al. (2018): 63; Castaldo/Cinque (2018): 52; Fan et al. (2018): 136.3; Thwin/Vasupongayya (2018): 199; Xiao et al. (2018): 1001; Zhang et al. (2018a): 3; Zheng et al. (2018): 165. PKI ist im Gesundheitswesen grundsätzlich vorgeschrieben. Grund ist die notwendige Verknüpfung von Schlüsseln mit der Real-Identität der an einer PKI beteiligten Person, die im Gesundheitswesen vorgeschrieben ist (vgl. Haas (2006): 175-177).

beteiligten Knoten zu bestätigen.[511] Bei der Hyperledger-Blockchain (Hyperledger Fabric) konstruiert der *Membership Service* eine PKI,[512] deren Zertifizierungsstelle (*Fabric CA*) eine einwandfreie Identifikation verspricht und gleichzeitig als Root-CA oder Bridge-CA eingesetzt wird.[513]

6.4.3.2 Keyless Signature Infrastructure

Die *Keyless-Signature-Infrastruktur* (engl. *Keyless Signature Infrastructure*, KSI) ist auf die Entwicklung des niederländischen Unternehmens Guardtime zurückzuführen.[514] Im Gegensatz zu einer PKI trennt eine KSI die Prozesse der Identifikation und der Integritätsabsicherung von Signaturen, sodass zwar weiterhin ein asymmetrisches Schlüsselpaar genutzt wird, Erstellung und Validierung von Signaturen jedoch nicht von einer CA übernommen, sondern über *one-way collision-free hash functions* und einem Netz aus Aggregations-Servern vorgenommen werden.[515]

Bei der Betrachtung des Verarbeitungs-Prozesses[516] von KSI wird deutlich, dass die Blockchain in dieser Infrastrukturform nicht die Verwaltung von Gesundheitsdaten und ihre Distribution übernimmt, sondern bisher ausschließlich die Gewährleistung der Datenintegrität, indem die berechneten Hash-Werte als Transaktion auf der Blockchain gespeichert werden.[517]

In der Literatur findet sich allerdings keine konkrete Lösungsbeschreibung für die Anwendung einer KSI-Blockchain, lediglich der Hinweis auf die Möglichkeit der KSI.[518]

6.4.4 Logging & Audit

Blockchain stellt IAM-Funktionalitäten bereit und wird darüber hinaus zur Führung von unveränderlichen Logs genutzt, die ein sicheres Audit ermöglichen. In den Publikationen hat sich

511 Vgl. Gordon/Catalini (2018): 227.
512 Vgl. Rouhani et al. (2018): 1534.
513 Vgl. Hyperledger (2021): 49.
514 Vgl. Liang et al. (2017a): 470; Andoni et al. (2019): 158.
515 Vgl. Buldas/Kroonmaa/Laanoja (2013): 313f.
516 Vgl. Buldas/Kroonmaa/Laanoja (2013): 313f; Buldas/Laanoja/Truu (2017): 120.
517 Vgl. Nagasubramanian et al. (2018): 644.
518 Vgl. Benchoufi/Ravaud (2017): 335.3; Liang et al. (2017a): 470; Nagasubramanian et al. (2018): 644.

insbesondere das *KONFIDO*-Projekt[519] hervorgetan, das die Bereitstellung eines auditfähigen Logs[520] zur intraeuropäischen Datentransaktion beschreibt. [521]

Blockchain bietet hier die Möglichkeit, ein Log zu führen, das sämtliche Daten-Transaktionen unter Vermeidung von Manipulation verfolgt.[522] Inhalt dieser Logs können dabei sämtliche Informationen über Transaktionen[523] sein oder auch nur ein Access-Log.[524] Auch können bereits erstellte Logs in verschlüsselter Form auf der Blockchain gespeichert werden.[525]

Darüber hinaus können auf der Blockchain gespeicherte Hash-Werte von medizinischen Daten, die zumeist off-chain vorgehalten werden, nicht nur die Integrität dieser Daten schützen, sondern ebenfalls erlauben, sämtliche Veränderungen an diesen nachzuverfolgen und Manipulationen nachzuweisen.[526] Ein solches Log kann alternativ in einer eigenen Blockchain-Infrastruktur parallel zu einer Gesundheitsdaten-Blockchain betrieben werden.[527]

Tabelle 6-5 und *Abbildung 6-12* verdeutlichen die Verteilung auf die entsprechenden Publikationen.

---

519 KONFIDO entsteht im Rahmen des epSOS3-Projekts (mehr unter: Staffa et al. (2018): 13-15) und stellt eine Sammlung von Tools zur Verfügung, die den Datenaustausch unterstützen sollen (vgl. Staffa et al. (2018): 16).

520 Vgl. Staffa et al. (2018): 19.

521 Vgl. Staffa et al. (2018): 12, 15.

522 Vgl. Xiao et al. (2018): 1001.

523 Vgl. Kiyomoto/Rahman/Basu (2017): 89; Xia et al. (2017a): 14761; Amofa et al. (2018): 169; Staffa et al. (2018): 19; Wu et al. (2018): 354; Xiao et al. (2018): 1001; Yang/Li (2018): 262.

524 Vgl. Liu (2016): 255f; Noh et al. (2017): 141; Yang/Yang (2017): 102; Liang et al. (2018b): 392; Mense/Athanasiadis (2018): 8; Pukas/Smal/Zabchuk (2018): 172; Xiao et al. (2018): 1002; Zhang et al. (2018b): 275.

525 Vgl. Castaldo/Cinque (2018): 52f.

526 Vgl. Azaria et al. (2016): 26; Ekblaw et al. (2016): 3; Angeletti/Chatzigiannakis/Vitaletti (2017): 10; Bayle et al. (2018): 790f; Chang et al. (2018): 176; Chen et al. (2018a): 208; Chen et al. (2018b): 5.6; Chowdhury et al. (2018): 1335; Dagher et al. (2018): 287; Fan et al. (2018): 136.6; Hanley/Tewari (2018): 249; Jiang et al. (2018): 52; Theodouli et al. (2018): 1376f; Vora et al. (2018): 981; Wang et al. (2018b): 947; Xiao et al. (2018): 1001.

527 Vgl. Banerjee/Lee/Choo (2018): 156.

Tabelle 6-5: Literatur-Kategorien ‚Security – Logging & Audit' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
Access Logs	Xiao et al. (2018); Zhang et al. (2018b)	Liu (2016); Noh et al. (2017); Yang/Yang (2017); Liang et al. (2018b); Mense/Athanasiadis (2018); Pukas/Smal/Zabchuk (2018); Thwin/Vasupongayya (2018)
Hash-Value of data	Azaria et al. (2016); Ekblaw et al. (2016); Chang et al. (2018); Fan et al. (2018); Hanley/Tewari (2018); Jiang et al. (2018); Vora et al. (2018); Xiao et al. (2018)	Angeletti/Chatzigiannakis/Vitaletti (2017); Banerjee/Lee/Choo (2018); Bayle et al. (2018); Chen et al. (2018a); Chen et al. (2018b); Chowdhury et al. (2018); Dagher et al. (2018); Theodouli et al. (2018); Wang et al. (2018b)
Transaction Logs	Xia et al. (2017a); Staffa et al. (2018); Xiao et al. (2018); Yang/Li (2018)	Kiyomoto/Rahman/Basu (2017); Amofa et al. (2018); Castaldo/Cinque (2018); Wu et al. (2018)

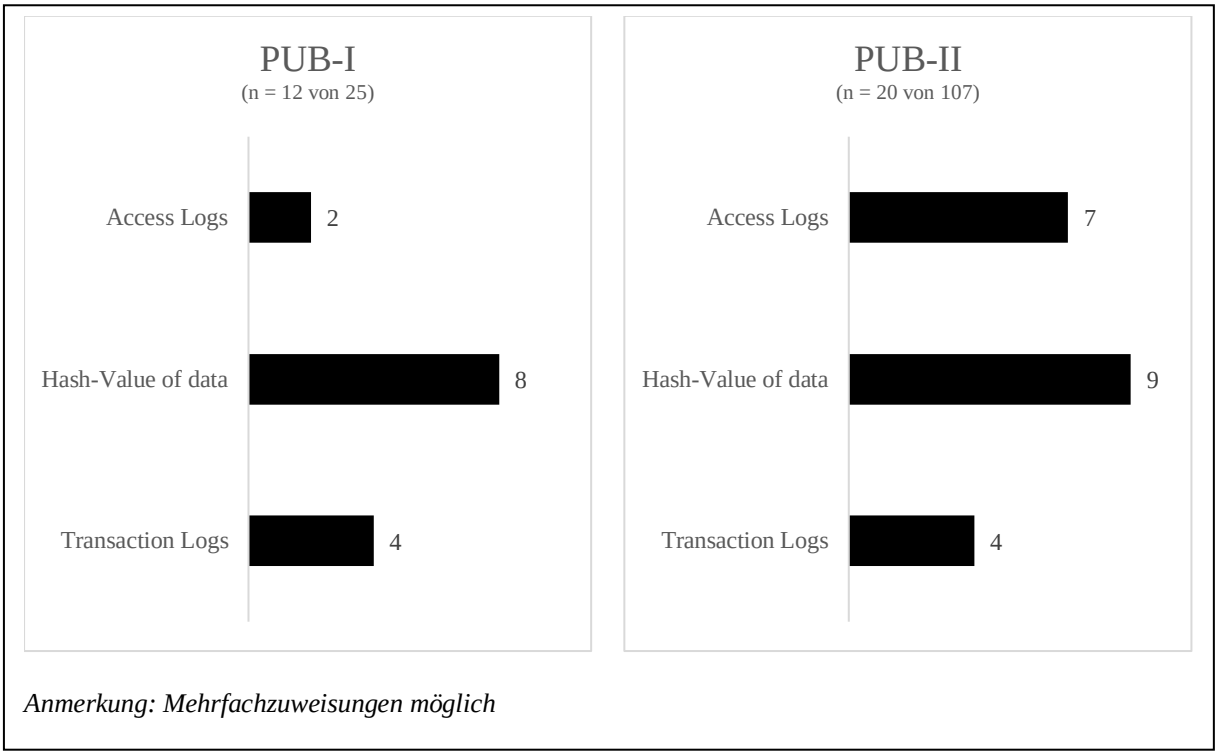


Abbildung 6-12: Verteilung ‚Security – Logging & Audit' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

6.5 Sicht: Technology

Diese Sicht betrachtet sämtliche technologischen Aspekte der in den Publikationen beschriebenen Konzepte. Dabei unterteilen sich die thematischen Schwerpunkte auf die Anzahl eingesetzten Blockchains (Quantity), die Eingruppierung in die Blockchain Taxonomy (Taxonomy) sowie die konkrete Technologie (Blockchain-Technology). Darauf aufbauend wird weiter unterschieden, welches Konsensprotokoll (Consensus Protocol) eingesetzt wird, welche Smart

Contracts (Smart Contracts/Chaincode) Anwendung finden und ob ein Coin (Coin/Token) zum Einsatz kommt.

Die Verteilung dieser Kategorien wird in *Tabelle D-4* (siehe *Anhang D*) und *Abbildung 6-13* dargestellt und in den folgenden Kapiteln detailliert betrachtet.

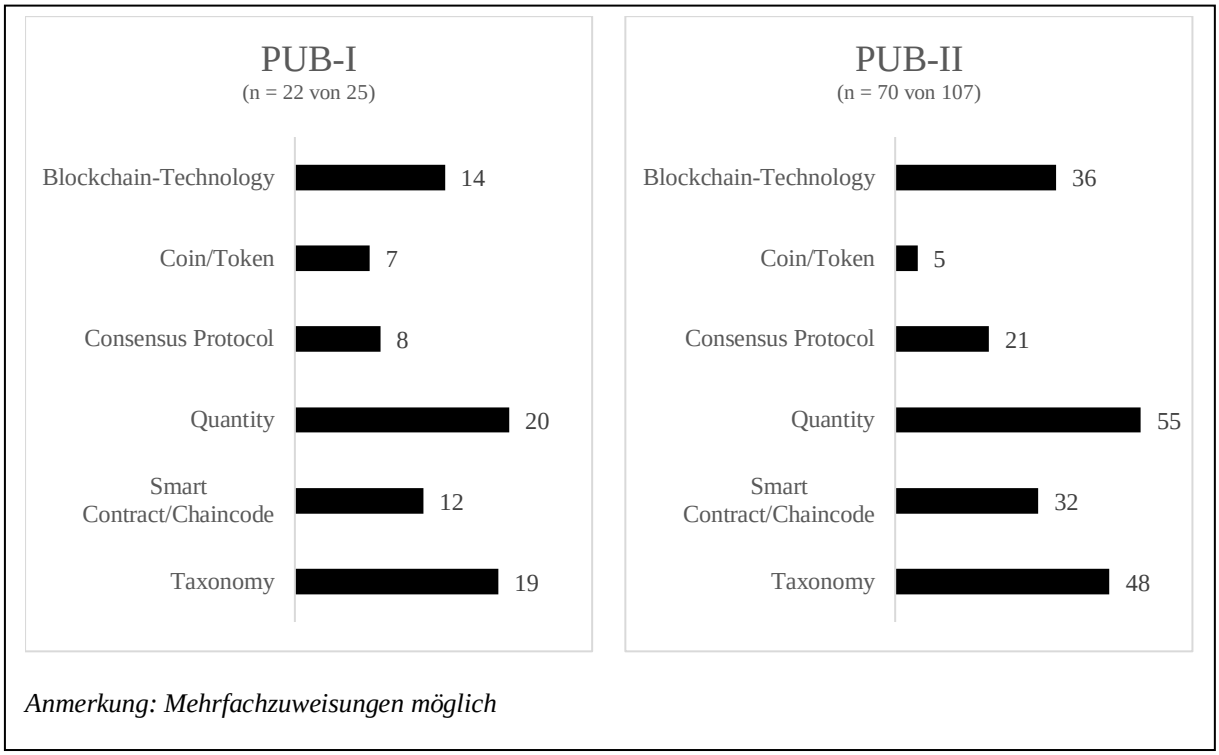


Abbildung 6-13: Verteilung ‚Technology' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

6.5.1 Blockchain-Taxonomie, Blockchain-Technologien und die Verwendung von Dual Blockchain, Multi-Layer oder SideChains

In einem ersten Schritt wird untersucht, inwieweit die Kategorisierung der in *Abbildung 3-4* (Seite 40) dargestellten Blockchain-Taxonomie-Matrix berücksichtigt wird. Dabei ist zu erkennen, dass der Fokus der Publikationen auf *Private-Permissioned-Blockchains* liegt, gefolgt von *Public-Permissioned* und *Public-Permissionless* (siehe *Tabelle 6-6* und *Abbildung 6-14*). *Private-Permissionless Blockchains* haben keine nennenswerte Relevanz in den Architekturen und Beschreibungen. *Permissioned Blockchains* sorgen für die notwendige Absicherung des Netzwerks gegen Beitritt und Veränderung durch Unbefugte und für eine schnellere Transaktionsabwicklung im Vergleich zu öffentlichen und unkontrollierten Netzwerken, denn gerade die Verteilung sensibler privater Daten bedarf einer eindeutigen Identifikation der Netzwerkteilnehmer.[528]

[528] Vgl. Linn/Koo (2016): 3; Dubovitskaya et al. (2017): 654; Chowdhury et al. (2018): 1333.

Tabelle 6-6: Literatur-Kategorien ‚Technology – Taxonomy' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
Private-Permissioned Blockchains	Azaria et al. (2016); Ekblaw et al. (2016); Ahram et al. (2017); Al Omar et al. (2017); McFarlane et al. (2017); Hanley/Tewari (2018); Ito/Tago/Jin (2018); Medicalchain (2018); Quaini et al. (2018); Rouhani et al. (2018); Staffa et al. (2018); Xiao et al. (2018); Zhang et al. (2018b); Zhang/Lin (2018)	Dubovitskaya et al. (2017); Genestier et al. (2017); Kim/Hong (2017); Kiyomoto/Rahman/Basu (2017); Liang et al. (2017b); Magyar (2017); Noh et al. (2017); Rifi et al. (2017); Wanitcharakkhakul/Rotchanakitumnuai (2017); Yang/Yang (2017); Alexaki et al. (2018); Amofa et al. (2018); Badr/Gomaa/Abd-Elrahman (2018); Bayle et al. (2018); Bell et al. (2018); Benhamouda/Halevi/Halevi (2018); Bhuiyan et al. (2018); Castaldo/Cinque (2018); Chen et al. (2018a); Chowdhury et al. (2018); Cisneros/Aarestrup/Lund (2018); Dagher et al. (2018); Dias et al. (2018); Gökalp et al. (2018); Han et al. (2018); Liang et al. (2018a); Liu et al. (2018); Mendes et al. (2018); Mikula/Jacobsen (2018); Thwin/Vasupongayya (2018); Zhang et al. (2018a); Zhuang et al. (2018)
Private-Permissioned Blockchains_Consortial	Zhang et al. (2018b); Zhang/Lin (2018)	Wanitcharakkhakul/Rotchanakitumnuai (2017); Bayle et al. (2018); Chowdhury et al. (2018); Dias et al. (2018); Han et al. (2018); Liu et al. (2018)
Private-Permissionless Blockchains	Kuo/Ohno-Machado (2018)	Han et al. (2018)
Public-Permissioned Blockchains	Chang et al. (2018); Yang/Li (2018); Zhou/Wang/Sun (2018)	Liang et al. (2017a); Pukas/Smal/Zabchuk (2018); Sun et al. (2018); Wang et al. (2018b)
Public-Permissionless Blockchains	Medicalchain (2018); Vora et al. (2018)	Zyskind/Nathan/Pentland (2015); Linn/Koo (2016); Angeletti/Chatzigiannakis/Vitaletti (2017); Cunningham/Ainsworth (2017); Magyar (2017); Badr/Gomaa/Abd-Elrahman (2018); Bell et al. (2018); Brogan/Baskaran/Ramachandran (2018); Colón (2018); Conceição et al. (2018); Cyran (2018); Desai et al. (2018); Li et al. (2018); Ramani et al. (2018); Zheng et al. (2018)

Anmerkung: Mehrfachzuweisungen möglich

Abbildung 6-14: Verteilung ‚Technology – Taxonomy' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

Private-Permissioned Blockchains werden in den Publikationen mit den in *Kapitel 3.2* aufgeführten Eigenschaften beschrieben. Danach wird ein Netzwerk entwickelt, dessen Zugang beschränkt ist und nur ein Teil der Netzwerkteilnehmer Veränderungen an der Blockchain vornehmen darf.[529] MultiChain ist hier als Beispieltechnologie zu nennen.[530] Der Zugang ins Netzwerk verlangt eine Registrierung[531], die entweder selbst oder durch Dritte vorgenommen wird.[532] Zur sicheren Identifikation sind zwar Pseudonyme erlaubt, doch müssen diese mit einer Real-Identität in Verbindung gebracht werden.[533] Das Private Netzwerk erlaubt zudem entweder eine institutionsinterne oder -übergreifende Gestaltung. Die institutionsübergreifende Variante wird dabei in der Regel durch die sog. **Konsortial-Blockchain** umgesetzt.[534] Ein Beispiel für diesen Ansatz ist die Hyperledger-Blockchain, doch existieren ebenfalls Ansätze einer privaten Ethereum-Blockchain, obwohl diese in der Regel zur Gruppe der *Public-Permissionless-Blockchains* gehört.[535] Die Flexibilität der Ethereum-Blockchain erlaubt jedoch die Konstruktion sowohl von öffentlichen wie auch von privaten Blockchain-Netzwerken.[536]

Private-Permissionless Blockchains finden sich nur in zwei Publikationen, deren Beschreibungen nicht detailliert sind. So beschreiben HAN ET AL. zwar eine *Fully-Private-Blockchain*, doch bezeichnen diese in der Folge als Konsortium-Blockchain, in der wiederum jeder Knoten Veränderungen an der Blockchain vornehmen kann.[537] Auch bei KUO/OHNO-MACHADO kann jeder am Netzwerk beteiligte Knoten Transaktionen verifizieren und Mining betreiben.[538] Da

---

529 Vgl. Ahram et al. (2017): 140; Kim/Hong (2017): 79f; Magyar (2017): 138; McFarlane et al. (2017): 9; Noh et al. (2017): 135; Yang/Yang (2017): 103, 108; Gökalp et al. (2018): 178; Ito/Tago/Jin (2018): 831; Staffa et al. (2018): 19; Thwin/Vasupongayya (2018): 198; Zhang et al. (2018b): 276; Zhuang et al. (2018): 1170. Weitere Nachweise konnten nur auf Basis einer Ableitung anhand der eingesetzten Technologie erfolgen. Die hier eingesetzten Technologien Hyperledger (siehe Dubovitskaya et al. (2017): 652; Genestier et al. (2017): 2; Kiyomoto/Rahman/Basu (2017): 90; Benhamouda/Halevi/Halevi (2018): 359; Chen et al. (2018a): 205; Liang et al. (2018a): e3.2; Medicalchain (2018): 12; Mendes et al. (2018): 383; Mikula/Jacobsen (2018): 701; Xiao et al. (2018): 1000, 1003; Zhang et al. (2018a): 3) und MultiChain (siehe Peterson et al. (2016): 6; Castaldo/Cinque (2018): 54; Hanley/Tewari (2018): 249) erlauben die Zuordnung zu *Private-Permissioned*.

530 Vgl. MultiChain.com (2015): 5.

531 Dies gilt für Leistungserbringer, Patienten und einzelne Geräte gleichermaßen.

532 Vgl. Al Omar et al. (2017): 538f; Liang et al. (2017b): 1167, 1168, 1170; Badr/Gomaa/Abd-Elrahman (2018): 162; Cisneros/Aarestrup/Lund (2018): 6; Rouhani et al. (2018): 1535.

533 Vgl. Alexaki et al. (2018): 255f; Chowdhury et al. (2018): 1332.

534 Vgl. Wanitcharakkhakul/Rotchanakitumnuai (2017): 55; Bayle et al. (2018): 790; Bhuiyan et al. (2018): 67; Dias et al. (2018): 6; Liu et al. (2018): 6186; Zhang et al. (2018b): 276; Zhang/Lin (2018): 140.4.

535 Vgl. Azaria et al. (2016): 26, 29; Ekblaw et al. (2016): 3, 8; Rifi et al. (2017): 200; Amofa et al. (2018): 169-171; Chowdhury et al. (2018): 1331; Dagher et al. (2018): 287; Quaini et al. (2018): 169.

536 Vgl. Dagher et al. (2018): 284. Obwohl die Autoren von einer Ethereum-Blockchain sprechen, nutzen die Autoren in ihrer Beschreibung das QuorumChain-Konsensprotokoll und verweisen in der Grundlagenarbeit auf Quorum (vgl. Dagher et al. (2018): 286). Dies lässt den Schluss zu, dass sie den privat ausgerichteten Ableger der Ethereum-Blockchain nutzen.

537 Vgl. Han et al. (2018): 583-585.

538 Vgl. Kuo/Ohno-Machado (2018): 6.

dies dem Konzept der reinen *Private-Permissioned Blockchain* widerspricht, werden diese Publikationen der Rubrik der *Private-Permissionless Blockchains* zugeordnet.

Public-Permissioned Blockchains kann jeder beitreten und Transaktionen erstellen, doch existieren in den Netzwerken vordefinierte Knoten, die Mining betreiben. Teilweise wird dies speziellen *Record Nodes* überlassen, aber auch einzelnen Einrichtungen oder dem Cloud-Anbieter, auf dessen Systemen die Blockchain ausgeführt wird.[539]

Public-Permissionless Blockchains und die Identifikation dieses Blockchain-Typs in der Literatur basiert größtenteils auf der Ableitung aus der in den Publikationen dargestellten Technologie, wie z.B. Bitcoin[540], Ethereum[541] und IOTA[542]. Diese Blockchains werden zur Verarbeitung unkritischer Informationen genutzt oder befinden sich unter vollständiger Kontrolle eines Patienten. Letzteres beschreibt die Führung einer öffentlichen Blockchain zur Nachverfolgung individueller Behandlungsverläufe, ohne diese Blockchain in einem Netzwerk freizugeben. Obwohl die Autoren hier den Begriff der *Public Blockchain* verwenden, stellt sich die Frage, warum es sich in diesem Fall nicht um eine *Private Blockchain* handelt.[543]

Auf Basis dieser Erkenntnisse wird im Folgenden eine Analyse der konkreten Blockchain-Technologien vorgenommen, deren Verteilung in *Tabelle 6-7* und *Abbildung 6-15* dargestellt wird.

---

539 Vgl. Liang et al. (2017a): 471, 476; Sun et al. (2018): 278, 280, 283; Wang et al. (2018b): 947; Yang/Li (2018): 262; Zhou/Wang/Sun (2018): 149.1, 149.5. Darüber hinaus existieren Publikationen, die zwar eine Ethereum-Blockchain nutzen (Public-Permissionless), Mining aber ausgewählten Knoten überlassen. Aus diesem Grund werden diese Publikationen der Gruppe *Public-Permissioned Blockchains* zugewiesen (siehe Chang et al. (2018): 175; Pukas/Smal/Zabchuk (2018): 171).

540 Vgl. Zyskind/Nathan/Pentland (2015): 182.

541 Vgl. Linn/Koo (2016): 3; Angeletti/Chatzigiannakis/Vitaletti (2017): 10; Cunningham/Ainsworth (2017): 45f; Colón (2018): 7; Conceição et al. (2018): 3; Cyran (2018): 3f; Desai et al. (2018): 1553f; Li et al. (2018): 141.2, 141.4-5; Medicalchain (2018): 12; Ramani et al. (2018): 3718; Vora et al. (2018): 979; Zheng et al. (2018): 164.

542 Vgl. Brogan/Baskaran/Ramachandran (2018): 258.

543 Vgl. Magyar (2017): 138; Badr/Gomaa/Abd-Elrahman (2018): 162f.

Tabelle 6-7: Literatur-Kategorien ‚Technology – Blockchain-Technology' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
Bitcoin		Zyskind/Nathan/Pentland (2015); Bell et al. (2018)
Ethereum	Azaria et al. (2016); Ekblaw et al. (2016); McFarlane et al. (2017); Chang et al. (2018); Medicalchain (2018); Quaini et al. (2018); Vora et al. (2018); Zhang et al. (2018b); Zhou/Wang/Sun (2018)	Angeletti/Chatzigiannakis/Vitaletti (2017); Cunningham/Ainsworth (2017); Kim/Hong (2017); Rifi et al. (2017); Yang/Yang (2017); Zhang et al. (2017); Alexaki et al. (2018); Amofa et al. (2018); Bell et al. (2018); Bhuiyan et al. (2018); Chowdhury et al. (2018); Colón (2018); Conceição et al. (2018); Cyran (2018); Dagher et al. (2018); Desai et al. (2018); Li et al. (2018); Novikov et al. (2018); Pukas/Smal/Zabchuk (2018); Ramani et al. (2018); Zheng et al. (2018)
Ethereum_Quorum		Alexaki et al. (2018); Bell et al. (2018); Dagher et al. (2018)
GuardTime		Angraal/Krumholz/Schulz (2017)
Hyperledger (Fabric)	Ahram et al. (2017); Ito/Tago/Jin (2018); Medicalchain (2018); Rouhani et al. (2018); Xiao et al. (2018)	Dubovitskaya et al. (2017); Genestier et al. (2017); Kiyomoto/Rahman/Basu (2017); Liang et al. (2017b); Benhamouda/Halevi/Halevi (2018); Bhuiyan et al. (2018); Chen et al. (2018a); Liang et al. (2018a); Mendes et al. (2018); Mikula/Jacobsen (2018); Thwin/Vasupongayya (2018); Zhang et al. (2018a)
IOTA		Brogan/Baskaran/Ramachandran (2018)
MultiChain	Hanley/Tewari (2018)	Castaldo/Cinque (2018)

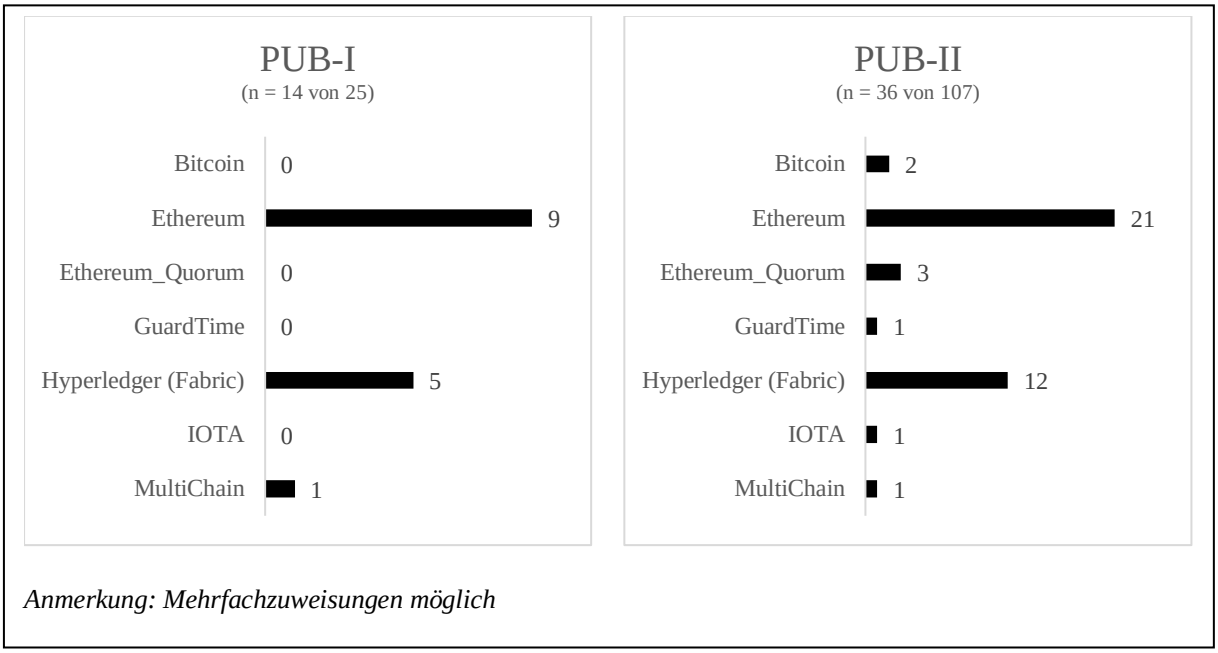


Abbildung 6-15: Verteilung ‚Technology – Blockchain-Technology' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

Der Schwerpunkt der Publikationen liegt auf der Nutzung der *Ethereum*-Blockchain-Technologie, gefolgt von *Hyperledger* und *MultiChain*. Einzig in den PUB-II werden noch Alternativen wie *Bitcoin*, *IOTA*, *Guardtime* und *Quorum* genannt. **Guardtime** wird, trotz Einsatzes im

Gesundheitswesen in Estland, in keiner anderen Publikation beschrieben und findet lediglich in Reviews, aber in keinen anderen Architekturbeschreibungen Erwähnung.

Die Nutzung von **Ethereum** bietet im Allgemeinen die Möglichkeit, Smart Contracts[544] auszuführen und einen Token bzw. Coin[545] einzusetzen.[546] Die Konstruktion einer privaten Variante der Blockchain-Technologie ist dabei bspw. durch die Nutzung des go-Ethereum Clients *Geth* möglich.[547] Auch findet sich in der **Quorum**-Blockchain eine als *Private-Permissioned Blockchain* konzipierte Weiterentwicklung der Ethereum-Blockchain.[548]

Hyperledger, genauer *Hyperledger Fabric*, erlaubt eine konsortiale Konstruktion einer Private Blockchain.[549] Deren modularer Aufbau[550] ermöglicht eine Mitgliederverwaltung[551] sowie Automatisierungen mittels Smart Contracts, die in dieser Technologie als Chaincode bezeichnet werden.[552]

Den Betrieb mehrerer parallellaufender Blockchains, die wiederum miteinander kommunizieren können, erlaubt **MultiChain**.[553] Trotz dieses variablen Ansatzes wird MultiChain kaum in den Publikationen thematisiert.[554] Das Gleiche gilt für **IOTA**[555] und **Bitcoin.**[556]

Trotz des geringen Interesses an MultiChain existieren Beschreibungen, die unter dem Begriff Dual Blockchain, Multi-Layer-Blockchain, Multi-Tier oder SideChains ein ähnliches Konzept

---

544 Vgl. Azaria et al. (2016): 26; Ekblaw et al. (2016): 3; Alexaki et al. (2018): 256; Amofa et al. (2018): 171; Conceição et al. (2018): 3; Desai et al. (2018): 1553; Pukas/Smal/Zabchuk (2018): 171.

545 Vgl. Colón (2018): 7; Medicalchain (2018): 12.

546 Vgl. Angeletti/Chatzigiannakis/Vitaletti (2017): 10; Cunningham/Ainsworth (2017): 45; McFarlane et al. (2017): 14; Yang/Yang (2017): 104; Zhang et al. (2017): 123; Bell et al. (2018): 2; Bhuiyan et al. (2018): 66; Chang et al. (2018): 175; Chowdhury et al. (2018): 1331; Cyran (2018): 3; Li et al. (2018): 141.2; Novikov et al. (2018): 700; Quaini et al. (2018): 169; Ramani et al. (2018): 3718; Vora et al. (2018): 977; Zhang et al. (2018b): 274; Zheng et al. (2018): 164; Zhou/Wang/Sun (2018): 149.9.

547 Vgl. Kim/Hong (2017): 82; Rifi et al. (2017): 200; Dagher et al. (2018): 287.

548 Vgl. Alexaki et al. (2018): 256; Bell et al. (2018): 2. Erneut wird auf die unklare Nutzung des Begriffs der privaten Ethereum-Blockchain von DAGHER ET AL. hingewiesen. Deren Beschreibung begründet die Zuteilung dieser Publikation zum Variationspunkt *Quorum* (vgl. Dagher et al. (2018): 286).

549 Vgl. Kiyomoto/Rahman/Basu (2017): 90; Liang et al. (2017b): 1167f; Benhamouda/Halevi/Halevi (2018): 357; Bhuiyan et al. (2018): 66; Ito/Tago/Jin (2018): 831; Liang et al. (2018a): e3.2; Mendes et al. (2018): 383; Mikula/Jacobsen (2018): 699; Rouhani et al. (2018): 1533; Thwin/Vasupongayya (2018): 197; Xiao et al. (2018): 1003.

550 Vgl. Ahram et al. (2017): 140.

551 Vgl. Dubovitskaya et al. (2017): 652; Chen et al. (2018a): 205; Medicalchain (2018): 12.

552 Vgl. Genestier et al. (2017): 2; Zhang et al. (2018a): 3.

553 Vgl. Greenspan (2015): 8.

554 Vgl. Castaldo/Cinque (2018): 54; Hanley/Tewari (2018): 249.

555 Vgl. Brogan/Baskaran/Ramachandran (2018): 258.

556 Vgl. Zyskind/Nathan/Pentland (2015): 182; Bell et al. (2018): 2.

verfolgen.[557] Dabei wird nicht nur die MultiChain-Technologie genutzt, sondern es werden auch andere Blockchain-Technologien miteinander kombiniert. Ziel ist dabei der Betrieb mehrerer Blockchains und eine Trennung organisatorischer Aufgaben. Beispielsweise können auf einer Blockchain sämtliche Accounts oder Zugriffsregelungen verwaltet werden, wohingegen eine zweite Blockchain diese Zugriffe protokolliert oder die im Netzwerk geplanten Automatisierungen durchführt.[558] Auch kann ein Metadatenregister geführt werden, das um Transaktionsdaten auf einer zweiten Blockchain ergänzt wird,[559] oder die Datenintegrität durch entsprechende Informationen gewährleistet.[560] Die konkrete Trennung entsprechend der Datenkategorie wird bei JIANG ET AL. beschrieben, denn hier werden EMR/EHR-Daten und von Patienten generierte Daten auf zwei getrennten, lose gekoppelten Blockchains (EMR-Chain, PHD-Chain) verwaltet.[561] Eine Variante der organisatorischen Separierung kann entweder auf Ebene der Leistungserbringer durchgeführt werden, wo jede Einrichtung eine eigene private Blockchain betreibt und eine zweite Blockchain erst die Verbindung sämtlicher Einrichtungen herstellt,[562] bspw. zur Ergänzung einer Währung zur Incentivierung.[563] Auch kann jeder Patient eine eigene Blockchain besitzen und relevante Inhalte in Blockchains der Leistungserbringer übertragen.[564] Des Weiteren erlauben parallel verlaufende Blockchains Methoden zur Proxy Re-Encryption,[565] die hier allerdings nicht detaillierter behandelt werden. Die Motivation zur Nutzung multipler Blockchains resultiert aus unterschiedlichen Sicherheitsbedürfnissen. Ein Leistungserbringer geht mit hochsensiblen Daten um, persönliche Gesundheitsdaten bspw. aus Fitnessgeräten sind dagegen eher auf Masse ausgelegt.[566] Während nicht jede Beschreibung darlegt, welche Technologien eingesetzt werden, können einzelne Angaben für die Ableitung möglicher Technologie-Kombinationen genutzt werden:

---

[557] Hintergrund ist das sog. CAP-Theorem, ursprünglich von Brewer vorgestellt (vgl. Chang et al. (2018): 174). Das CAP-Theorem beschreibt das Problem verteilter Systeme, Konsistenz (C – Consistency), Verfügbarkeit (A – Availability) und Partitionstoleranz (P – Tolerance to network Partitions) nicht gleichzeitig einhalten zu können. Stattdessen können nur zwei dieser Eigenschaften parallel gewährleistet werden (vgl. Brewer (2002): 4; Gilbert/Lynch (2002): 51). Weitere Informationen, insbesondere zur CAP-Terminologie, finden sich in GILBERT/LYNCH (2012): 30F..

[558] Vgl. Medicalchain (2018): 12; Wang et al. (2018a): 12; Zhang et al. (2018a): 4.

[559] Vgl. Jiang/Peng/Dian (2018): 012006.4; Wu et al. (2018): 351, 354.

[560] Vgl. Banerjee/Lee/Choo (2018): 156.

[561] Vgl. Jiang et al. (2018): 51.

[562] Vgl. Chang et al. (2018): 175; Zhang/Lin (2018): 140.4-5.

[563] Vgl. Medicalchain (2018): 12.

[564] Vgl. Badr/Gomaa/Abd-Elrahman (2018): 162f.

[565] Vgl. Jiang/Peng/Dian (2018): 12006.3-4.

[566] Vgl. Jiang et al. (2018): 51.

i. Hyperledger[567]

ii. Hyperledger + Ethereum[568]

iii. Ethereum + Public-Permissioned Blockchain[569]

iv. Private-Permissioned Blockchain[570]

v. Private-Permissioned Blockchain + Public-Permissionless Blockchain[571]

Die Verteilung der Literatur wird in *Tabelle 6-8* und *Abbildung 6-16* dargestellt.

Tabelle 6-8: Literatur-Kategorien ‚Technology – Quantity' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
DualBC/Multilayer/Sidechain	Chang et al. (2018); Jiang et al. (2018); Medicalchain (2018); Zhang/Lin (2018)	Badr/Gomaa/Abd-Elrahman (2018); Banerjee/Lee/Choo (2018); Jiang/Peng/Dian (2018); Wang et al. (2018a); Wu et al. (2018); Zhang et al. (2018a)
Single	Azaria et al. (2016); Ekblaw et al. (2016); Ahram et al. (2017); Al Omar et al. (2017); McFarlane et al. (2017); Hanley/Tewari (2018); Ito/Tago/Jin (2018); Kuo/Ohno-Machado (2018); Quaini et al. (2018); Rouhani et al. (2018); Staffa et al. (2018); Vora et al. (2018); Xiao et al. (2018); Yang/Li (2018); Zhang et al. (2018b); Zhou/Wang/Sun (2018)	Zyskind/Nathan/Pentland (2015); Linn/Koo (2016); Angeletti/Chatzigiannakis/Vitaletti (2017); Angraal/Krumholz/Schulz (2017); Cunningham/Ainsworth (2017); Dubovitskaya et al. (2017); Genestier et al. (2017); Kim/Hong (2017); Kiyomoto/Rahman/Basu (2017); Liang et al. (2017b); Liang et al. (2017a); Magyar (2017); Noh et al. (2017); Rifi et al. (2017); Wanitcharakkhakul/Rotchanakitumnuai (2017); Yang/Yang (2017); Zhang et al. (2017); Alexaki et al. (2018); Amofa et al. (2018); Bayle et al. (2018); Bell et al. (2018); Benhamouda/Halevi/Halevi (2018); Bhuiyan et al. (2018); Brogan/Baskaran/Ramachandran (2018); Castaldo/Cinque (2018); Chen et al. (2018a); Chowdhury et al. (2018); Cisneros/Aarestrup/Lund (2018); Colón (2018); Conceição et al. (2018); Cyran (2018); Dagher et al. (2018); Desai et al. (2018); Dias et al. (2018); Gökalp et al. (2018); Han et al. (2018); Li et al. (2018); Liang et al. (2018a); Liu et al. (2018); Mendes et al. (2018); Mikula/Jacobsen (2018); Novikov et al. (2018); Pukas/Smal/Zabchuk (2018); Ramani et al. (2018); Sun et al. (2018); Thwin/Vasupongayya (2018); Wang et al. (2018b); Zheng et al. (2018); Zhuang et al. (2018)

567 Vgl. Zhang et al. (2018a): 3.

568 Vgl. Medicalchain (2018): 12.

569 Vgl. Chang et al. (2018): 175.

570 Vgl. Zhang/Lin (2018): 140.4.

571 Vgl. Badr/Gomaa/Abd-Elrahman (2018): 162f.

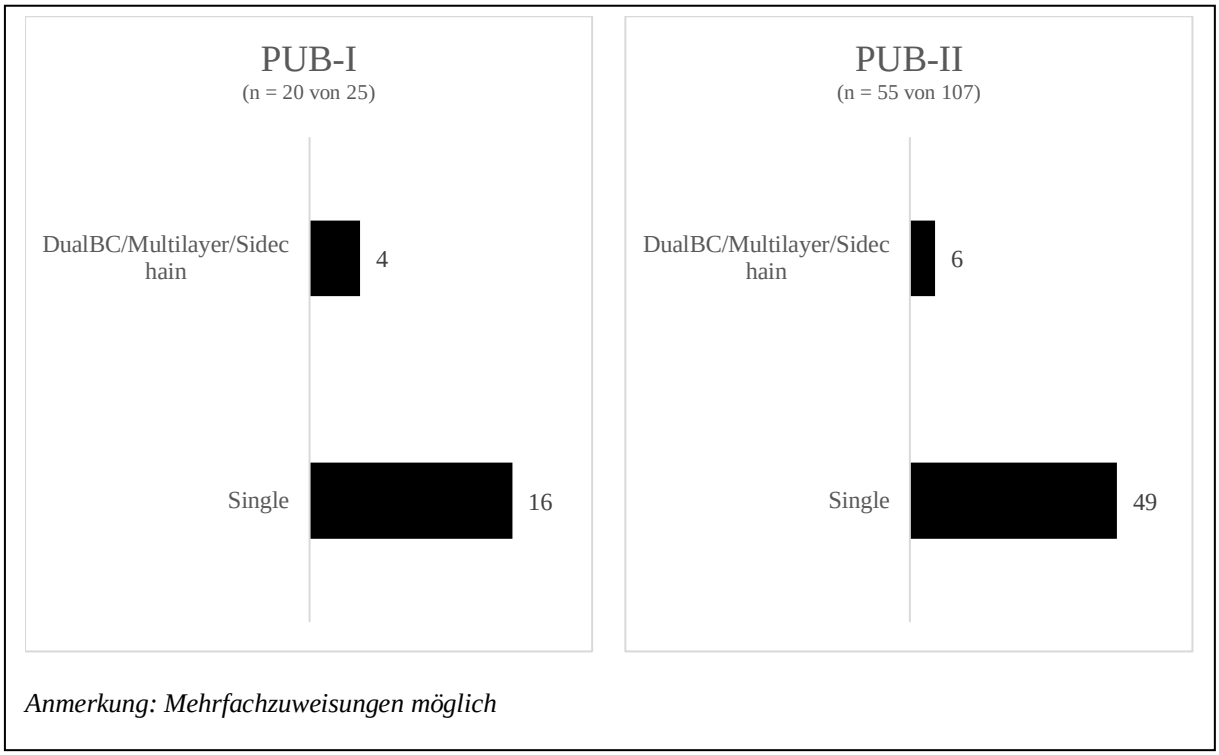


Abbildung 6-16: Verteilung ‚Technology – Blockchain-Technology' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

6.5.2 Consensus (Konsensmechanismen)

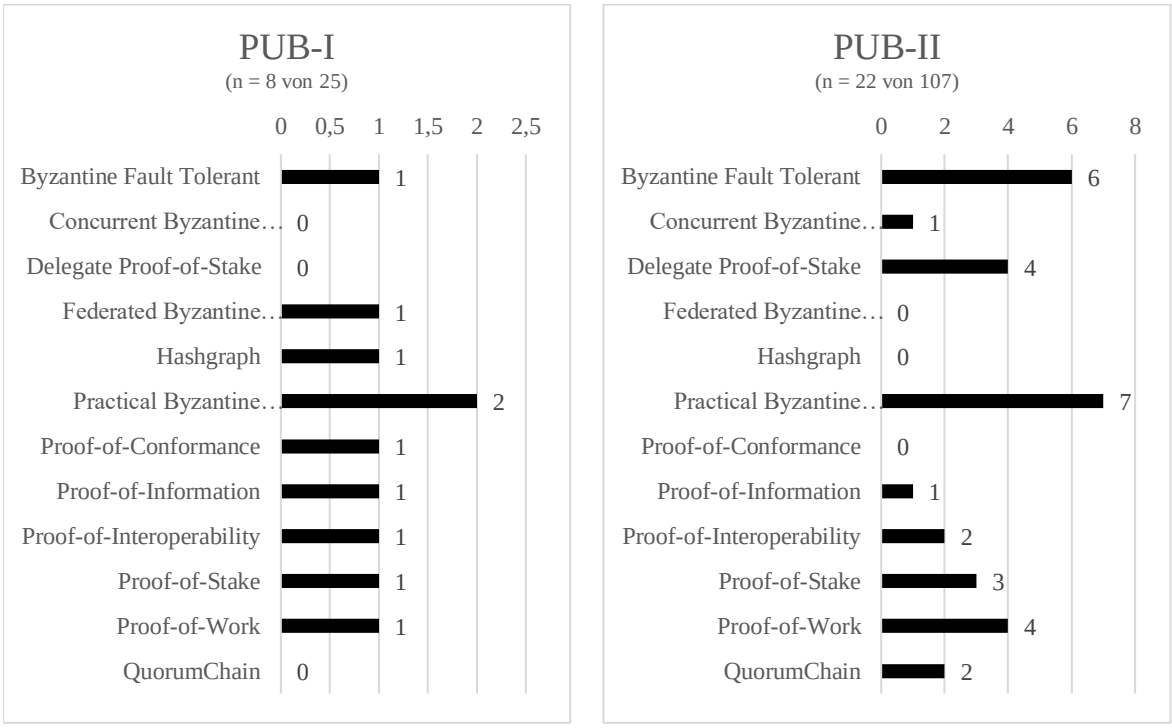
Konsensmechanismen werden nur in einem Bruchteil der Publikationen konkret benannt oder beschrieben. Dies ist möglicherweise dem Umstand geschuldet, dass bestimmte Konsensprotokolle bereits mit dem konkreten Einsatz einer bestimmten Blockchain-Technologie vordefiniert werden. So setzt bspw. Ethereum auf den Proof-of-Work-Konsens[572], sodass vonseiten der Autoren es keiner ergänzenden Nennung bedarf.

Insgesamt werden 12 verschiedene Konsensprotokolle identifiziert (siehe *Tabelle 6-9* und *Abbildung 6-17*), die in PUB-I und PUB-II genutzt oder beschrieben werden. Während in PUB-I und PUB-II ein Fokus auf *Practical Byzantine Fault Tolerant* liegt, wird das Spektrum von PUB-II um *Byzantine Fault Tolerant*, *Delegate Proof-of-Stake* und *Proof-of-Work* erweitert.

[572] In Zukunft soll jedoch ein Wechsel von PoW zu PoS stattfinden (vgl. Bussac (2019): 26).

Tabelle 6-9: Literatur-Kategorien ‚Technology – Consensus' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
Byzantine Fault Tolerant	Du et al. (2018)	Cunningham/Ainsworth (2017); Chowdhury et al. (2018); Kombe/Ally/Sam (2018); Kotsiuba et al. (2018); Liang et al. (2018a); Mendes et al. (2018)
Concurrent Byzantine Fault Tolerant		Wang et al. (2018a)
Delegate Proof-of-Stake		Chen et al. (2018b); Kombe/Ally/Sam (2018); Liu et al. (2018); Wang et al. (2018b)
Federated Byzantine Agreement	Chang et al. (2018)	
Hashgraph	Chang et al. (2018)	
Practical Byzantine Fault Tolerant	Ahram et al. (2017); Zhou/Wang/Sun (2018)	Dubovitskaya et al. (2017); Kiyomoto/Rahman/Basu (2017); Chen et al. (2018a); Hölbl et al. (2018); Sun et al. (2018); Thwin/Vasupongayya (2018); Zhang et al. (2018a)
Proof-of-Conformance	Zhang/Lin (2018)	
Proof-of-Information	Kuo/Ohno-Machado (2018)	Hölbl et al. (2018)
Proof-of-Interoperability	Zhang/Lin (2018)	Peterson et al. (2016); Hölbl et al. (2018)
Proof-of-Stake	Yang/Li (2018)	Hölbl et al. (2018); Kombe/Ally/Sam (2018); Patel (2018)
Proof-of-Work	Jiang et al. (2018)	Han et al. (2018); Hölbl et al. (2018); Jiang/Peng/Dian (2018); Kombe/Ally/Sam (2018)
QuorumChain		Dagher et al. (2018); Hölbl et al. (2018)



Anmerkung: Mehrfachzuweisungen möglich

Abbildung 6-17: Verteilung ‚Technology – Consensus' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

Byzantine Fault Tolerant (BFT) wird im Zusammenhang mit konsortial ausgerichteten Blockchains, wie z.B. Hyperledger, oder anderen Konstruktionen mit mehreren parallel laufenden Blockchains, den sogenannten Sidechains, genannt.[573] Hintergrund ist, dass durch die vordefinierten Validierenden, z.B. Netzwerk Administratoren oder Data Custodians, schnell und mit weniger Rechenleistung ein Ergebnis erzielt wird.[574] Ähnlich wie bei Bitcoin muss im BFT mindestens die Hälfte der relevanten Validierenden vertrauenswürdig sein.[575]

Concurrent Byzantine Fault Tolerant (CBFT), als Variante, wird lediglich in einer Publikation genannt.[576] Eine Begründung wird von den Autoren nicht angeführt.

Delegate Proof of Stake (DPoS) zählt im Vergleich zu Proof-of-Work oder Proof-of-Stake zu den schnelleren und effizienteren Konsensverfahren für *Permissionless*-Blockchains.[577] In diesem Verfahren werden Netzwerkteilnehmer ausgewählt, die Transaktionen sammeln, validieren und der Blockchain hinzufügen.[578] Ein Kritikpunkt ist die Möglichkeit, dass der gewählte Netzwerkteilnehmer doch nicht so vertrauenswürdig ist, wie im Vorfeld angenommen. Auf diese Annahme hin verweisen LIU ET AL. darauf, dass die Implementierung eines Bewertungssystems, das je nach Verhalten eines Netzwerkteilnehmers einen Score berechnet, der wiederum die zu übernehmende Aufgabe im Netzwerk anhand von Score-Grenzen definiert, unterstützt, dieses Problem zu lösen.[579]

Federated Byzantine Agreement (FBA) nutzt die in jedem Node vorhandenen Listen der von diesem als vertrauenswürdig bewerteten Nodes im System. Dieses Vorgehen unterstützt ein organisches Wachstum innerhalb eines Netzwerks und gewährt dabei jedem Knoten eine gewisse Flexibilität.[580]

Hashgraph-Konsensus-Protokolle werden insbesondere bei *Private* und *Permissioned Blockchains* angewandt und bestehen aus drei Schritten: *Syncing*, *Voting* und *Time-Stamping*. Das Protokoll benötigt bei deren Durchführung keine Netzwerkressourcen, jedoch ist die Netzwerk-

---

573 Vgl. Liang et al. (2018a): e3.5–6; Mendes et al. (2018): 383f. Doch in einem Fall wird es im Zusammenhang mit Ethereum erwähnt (vgl. Cunningham/Ainsworth (2017): 46).

574 Vgl. Chowdhury et al. (2018): 1333; Kombe/Ally/Sam (2018): 474; Kotsiuba et al. (2018): 116.

575 Vgl. Du et al. (2018): 38.

576 Vgl. Wang et al. (2018a): 13.

577 Vgl. Chen et al. (2018b): 5.7; Kombe/Ally/Sam (2018): 474. Dennoch existieren Publikationen, die dieser Aussage widersprechen und DPoS eine starke Ressourcenverschwendung unterstellen (vgl. Fan et al. (2018): 136.5). Für sich allein betrachtet, kann diese Behauptung begründet sein, doch in den Publikationen wird nicht klar, ob diese Aussage im Vergleich zu Proof-of-Work oder Proof-of-Stake getroffen wurde.

578 Vgl. Wang et al. (2018b): 947.

579 Vgl. Liu et al. (2018): 6187.

580 Vgl. Chang et al. (2018): 177. Mehr Informationen über das Verfahren finden sich in der Literatur.

Bandbreite der einzelnen Knoten relevant, denn diese führt die Synchronisierung von Transaktionslisten entweder langsamer oder schneller durch und hat folglich Einfluss auf die Priorisierung von Transaktionen.[581]

Practical Byzantine Fault Tolerant (PBFT) verspricht einen Effizienzvorteil gegenüber BFT, insbesondere in einem Anwendungsfeld, das einer schnellen Datenbereitstellung bedarf.[582] Seinen Einsatz findet das Protokoll in *Private* und *Permissioned* Blockchains, insbesondere bei *Hyperledger*.[583]

Proof of Conformance (PoC) wird in Zusammenhang mit privaten und konsortialen Blockchains beschrieben und sorgt für die im Netzwerk einzuhaltende Konformität. Das Protokoll auf einer *Private Blockchain* sorgt dafür, dass Daten weiterhin privat bleiben und auf konsortialen Blockchains ein einheitliches Vokabular genutzt wird.[584]

Proof of Information[585] berücksichtigt in seinem Protokoll die von einem Knoten definierte Notwendigkeit der Verarbeitung von Informationen und legt auf dieser Basis die Priorität in der Verarbeitung fest.[586]

Proof of Interoperability[587] ist ähnlich wie der PoC für konsortiale Blockchains konzipiert und sorgt dafür, dass Transaktionen semantisch und syntaktisch interoperabel sind. Diese Aufgabe wird zumeist von Menschen und nicht von einem Algorithmus übernommen.[588]

Proof of Stake (PoS) wird bei *Permissionless Blockchains* angewendet, ist schwierig zu skalieren und orientiert sich in der Entscheidung, ob ein Miner erfolgreich ist oder nicht, an der

---

581 Vgl. Chang et al. (2018): 177f.

582 Vgl. Ahram et al. (2017): 140f; Sun et al. (2018): 282f. Die Effizienz ergibt sich durch die Beschränkung von Aufgaben auf bestimmte vordefinierte Knoten, teils auch als *Record Nodes* bezeichnet (vgl. Zhou/Wang/Sun (2018): 149.2-3). Dennoch existieren Publikationen, die dieser Aussage widersprechen und PBFT eine starke Ressourcenverschwendung unterstellen (vgl. Fan et al. (2018): 136.5). Für sich alleine betrachtet, kann diese Behauptung begründet sein, doch in den Publikationen wird nicht klar, ob diese Aussage im Vergleich zu Proof-of-Work oder Proof-of-Stake getroffen wurde.

583 Vgl. Dubovitskaya et al. (2017): 652; Kiyomoto/Rahman/Basu (2017): 90; Chen et al. (2018a): 207; Thwin/Vasupongayya (2018): 199-200; Zhang et al. (2018a): 6. Ein weiterer Beleg für das Vorhandensein dieses Konsens-Protokolls findet sich bei HÖLBL ET AL. (2018): 470.13.

584 Vgl. Zhang/Lin (2018): 140.7-8.

585 Auf die Nennung einer Abkürzung für *Proof of Information* wird hier verzichtet, da sich diese in der Literatur gleichlautend mit der Abkürzung von *Proof of Interoperability* ist.

586 Vgl. Kuo/Ohno-Machado (2018): 3. Ein weiterer Beleg für das Vorhandensein dieses Konsens-Protokolls findet sich bei HÖLBL ET AL. (2018): 470.13.

587 Auf die Nennung einer Abkürzung für *Proof of Interoperability* wird hier verzichtet, da sich diese in der Literatur gleichlautend mit der Abkürzung von *Proof of Information* ist.

588 Vgl. Peterson et al. (2016): 5f. Weitere Belege für das Vorhandensein dieses Konsens-Protokolls finden sich bei HÖLBL ET AL. (2018): 470.13 und ZHANG/LIN (2018): 140.3.

Größe des Besitzes der auf der Blockchain gehandelten Einheit.[589] So ist bspw. der Besitz von Währungseinheiten genauso relevant wie die Menge an zu verarbeitenden Patienten- oder Forschungsdaten.

Proof of Work (PoW) ist das Konsensprotokoll, das bereits in der Bitcoin-Blockchain eingesetzt wird und bei Ethereum ebenfalls Anwendung findet. Es wird in *Public* und *Permissionless Blockchains* verwendet und gehört zu den nicht gut skalierbaren Konsensprotokollen.[590] Zur Reduzierung dieses Problems werden in der Regel mehrere Blockchains parallel betrieben und der Schwierigkeitsgrad der im PoW-Protokoll zu lösenden Aufgabe konstant gehalten.[591]

QuorumChain wird als Konsensprotokoll in *Private* oder *Permissioned Blockchains* genutzt und führt das Protokoll mithilfe von Smart Contracts aus.[592] Grundlage ist ein Voting-Konzept, das einer bestimmten Auswahl an Knoten das Recht einräumt, welche Information als nächstes der Blockchain angefügt wird. Dabei wird der aktuellste mit den meisten Stimmen ausgewählt.[593]

6.5.3 Smart Contract/ChainCode

Ein *Smart Contract* bzw. *Chaincode* automatisiert Prozesse, die in bzw. über die Blockchain durchgeführt werden. Dabei reichen die Aufgaben von der Berechtigungssteuerung über Identitäts- und Consent Management bis zur Verwaltung von Daten und Abwicklung von Zahlungen.[594]

Beim Einsatz von Smart Contracts oder Chaincode ist zu beachten, dass diese nicht nur die Vorteile einer Automatisierung mitbringen, sondern auch Risiken aufgrund ihrer Komplexität. So sind sowohl für die Konzeption als auch für ein Verständnis der Inhalte bzw. Prozessschritte Programmierkenntnisse notwendig. Sollte sich nun ein Fehler im Code befinden, würde dieser

589 Vgl. Kombe/Ally/Sam (2018): 474; Patel (2018): 7f; Yang/Li (2018): 263. Ein weiterer Beleg für das Vorhandensein dieses Konsens-Protokolls findet sich bei HÖLBL ET AL. (2018): 470.13.

590 Vgl. Jiang et al. (2018): 51; Kombe/Ally/Sam (2018): 474. Ein weiterer Beleg für das Vorhandensein dieses Konsens-Protokolls findet sich bei HÖLBL ET AL. (2018): 470.13.

591 Vgl. Han et al. (2018): 585; Jiang/Peng/Dian (2018): 012006.2.

592 Vgl. Dagher et al. (2018): 286. Ein weiterer Beleg für das Vorhandensein dieses Konsens-Protokolls findet sich hier: Hölbl et al. (2018): 470.13. Dieses Protokoll ist inhaltlich auf das Whitepaper Quorum (2018) zurückzuführen.

593 Vgl. Teeter (o. J.): 2.

594 Siehe folgende Unterkapitel.

automatisch ausgeführt ohne Möglichkeit der Korrektur.[595] Der dadurch entstehende Vertrauensverlust in die Automatisierungen ist nicht zu unterschätzen.[596]

In der Entwicklung von Smart Contracts im Gesundheitssektor orientieren sich Entwickler an den folgende Designentscheidungen[597] des *Office of the National Coordinator for Health Information Technology (ONC)*:[598]

1. Verifying Identity and Authenticating all Participants
2. Storing and Exchanging Data Securely
3. Consistent Permissioned Access to Data Sources
4. Applying Consistent Data Formats
5. Maintaining Modularity

Verwaltung sowie eigentlicher Betrieb werden auf jedem Knoten vorgenommen, doch finden sich in den Publikationen auch Konstruktionen, die ein zusätzliches Contract Layer oder spezielle, für den Betrieb von Smart Contracts installierte Nodes beschreiben.[599]

Die Verteilung der Varianten von Smart Contracts wird in *Tabelle 6-10* und *Abbildung 6-18* zusammengefasst.

Tabelle 6-10: Literatur-Kategorien ‚Technology – Smart Contract/ChainCode' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
General Description	Quaini et al. (2018); Zhang et al. (2018b)	Amofa et al. (2018); Kumar et al. (2018); Liang et al. (2018a); Qiu et al. (2018)
Access Contracts	Rouhani et al. (2018); Vora et al. (2018)	Dubovitskaya et al. (2017); Liang et al. (2017b); Simić/Sladić/Milosavljević (2017); Alexaki et al. (2018); Chen et al. (2018a); Conceição et al. (2018); Dagher et al. (2018); Liu et al. (2018); Novikov et al. (2018); Theodouli et al. (2018); Zhang et al. (2018a)
Consent Management Contracts	Vora et al. (2018)	Peterson et al. (2016); Benchoufi/Ravaud (2017); Dubovitskaya et al. (2017); Genestier et al. (2017); Kim/Hong (2017); Dagher et al. (2018); Desai et al. (2018)
Data Management Contracts	Ahram et al. (2017); Al Omar et al. (2017); Chang et al. (2018); Ito/Tago/Jin (2018)	Simić/Sladić/Milosavljević (2017); Alexaki et al. (2018); Benhamouda/Halevi/Halevi (2018); Conceição et al. (2018); Cyran (2018); Gökalp et al. (2018); Mense/Athanasiadis (2018); Theodouli

595 Vgl. Kumar et al. (2018): 158; Liang et al. (2018a): e3.4. Insbesondere die Modularität von Smart Contracts ist zur Vermeidung dieses Problems relevant (vgl. Zhang et al. (2018b): 271).

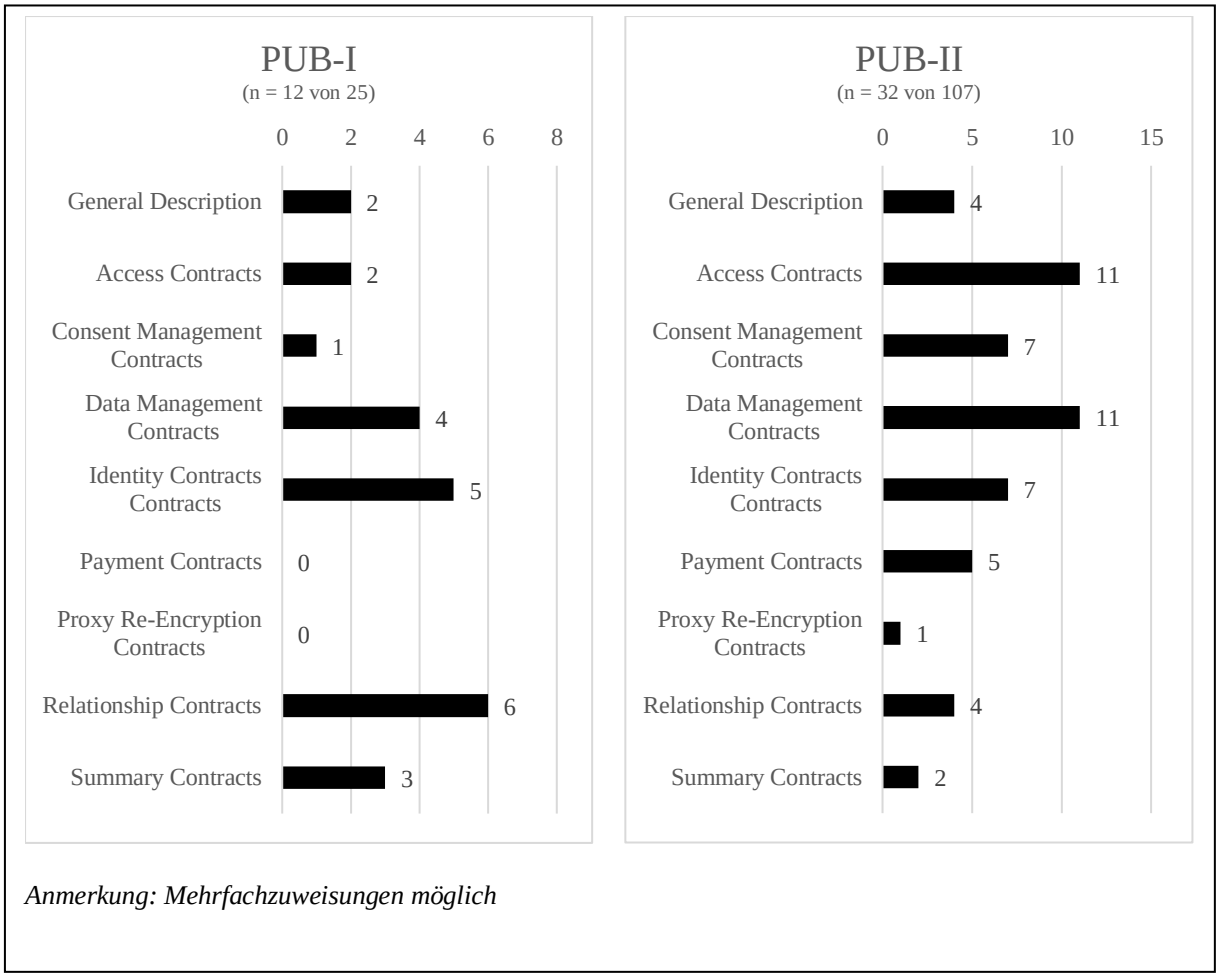
596 Vgl. Qiu et al. (2018): 684.

597 Vgl. Zhang et al. (2018b): 269-271. Nähere Informationen finden sich bei DESALVO (2016) (ZHANG ET AL. verweisen jedoch auf eine nicht mehr abrufbare Version von 2015).

598 Zhang et al. (2018b): 270f.

599 Vgl. Amofa et al. (2018): 170f; Quaini et al. (2018): 170.

		et al. (2018); Zhang et al. (2018a); Zhou et al. (2018); Zhuang et al. (2018)
Identity Contracts	Azaria et al. (2016); Ekblaw et al. (2016); Chang et al. (2018); Vora et al. (2018); Zhang et al. (2018b)	Yang/Yang (2017); Alexaki et al. (2018); Cyran (2018); Dagher et al. (2018); Mense/Athanasiadis (2018); Pukas/Smal/Zabchuk (2018); Theodouli et al. (2018)
Payment Contracts		Chen et al. (2018a); Colón (2018); Desai et al. (2018); Grishin et al. (2018); Radanović/Likić (2018)
Proxy Re-Encryption Contracts		Dagher et al. (2018)
Relationship Contracts	Azaria et al. (2016); Ekblaw et al. (2016); Xia et al. (2017a); Chang et al. (2018); Vora et al. (2018); Yang/Li (2018)	Yang/Yang (2017); Bhuiyan et al. (2018); Dagher et al. (2018); Pukas/Smal/Zabchuk (2018)
Summary Contracts	Azaria et al. (2016); Ekblaw et al. (2016); Yang/Li (2018)	Yang/Yang (2017); Zhuang et al. (2018)



Anmerkung: Mehrfachzuweisungen möglich

Abbildung 6-18: Verteilung ‚Technology – Smart Contract/ChainCode' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

Access Smart Contracts verwalten und steuern Zugriffe auf Gesundheitsdaten, die durch eine konkrete Anfrage[600] ausgelöst werden. Neben der Befolgung von Regeln, können solche Smart Contracts Listen über sämtliche in einem Netzwerk relevanten Zugriffsberechtigungen enthalten, auf deren Basis Zugriff gewährt bzw. verwehrt wird.[601] Auf diese Weise ist eine feingranulare Zugriffsteuerung, auch auf ausgewählte Inhalte einer Patientenakte, möglich.[602] Diese Abfragen haben eine direkte Abhängigkeit zu Identitäten der Netzwerkknoten, denn diese sind Bestandteil der mehrstufigen Überprüfung von Berechtigungen.[603]

Smart Contracts zur Verwaltung von **Consent Management** führen ein Log über sämtliche historischen Datenverarbeitungen und prüfen gleichzeitig den aktuellen Stand der von Patienten erteilten Zugriffsberechtigungen.[604] Es wird darauf geachtet, dass gelöschte oder für ein Netzwerk gefährliche Knoten nicht mehr an der Konsensfindung teilhaben können,[605] oder, entsprechend dem Konsens-Protokoll, nur eine (zufällige) Auswahl von vertrauenswürdigen Knoten einen Konsens durchführen.[606]

Data Management Smart Contracts haben zumeist verwaltende Funktion. So erstellen diese bspw. automatisiert neue Einträge im Wallet der relevanten Knoten oder definieren Restriktionen, sodass Patienten nur die Autorisierung haben, eine initiale Variante eines EHR anzulegen.[607] Alternativ werden Listen verwaltet, die entweder

i. sämtliche EHR-Eintragungen eines Patienten auf dessen Netzwerkknoten,[608]
ii. alle potentiell freizugebenen Eintragungen,[609]
iii. Metadaten der (in externen Speichern vorgehaltenen) Daten,[610]
iv. die am Blockchain-Netzwerk beteiligten Aktensysteme[611] oder

600 Vgl. Conceição et al. (2018): 10.

601 Vgl. Alexaki et al. (2018): 256; Dagher et al. (2018): 289; Vora et al. (2018): 979.

602 Vgl. Liang et al. (2017b): 1170; Simić/Sladić/Milosavljević (2017): 3; Alexaki et al. (2018): 256; Liu et al. (2018): 6187; Novikov et al. (2018): 700f; Rouhani et al. (2018): 1536.

603 Vgl. Dubovitskaya et al. (2017): 656f; Chen et al. (2018a): 206f; Theodouli et al. (2018): 1377; Zhang et al. (2018a): 5f; Zhang et al. (2018a): 5.

604 Vgl. Peterson et al. (2016): 7; Benchoufi/Ravaud (2017): 335.3–4; Dubovitskaya et al. (2017): 657; Genestier et al. (2017): 2; Kim/Hong (2017): 81f.

605 Vgl. Dagher et al. (2018): 287f; Vora et al. (2018): 978.

606 Vgl. Desai et al. (2018): 1557.

607 Vgl. Ahram et al. (2017): 140; Conceição et al. (2018): 9f; Gökalp et al. (2018): 180f.

608 Vgl. Al Omar et al. (2017): 540; Alexaki et al. (2018): 256; Mense/Athanasiadis (2018): 9f; Zhou et al. (2018): 1102.

609 Vgl. Mense/Athanasiadis (2018): 9f.

610 Vgl. Chang et al. (2018): 176; Cyran (2018): 3.

611 Vgl. Mense/Athanasiadis (2018): 9.

v. sämtliche berechtigten Teilnehmer (Sponsoren) in der klinischen Forschung[612]

enthalten. Darüber hinaus wahren Smart Contracts durch Abfolge eines Prozesses die Sicherheit von Datenübermittlungen.[613] Durch permanente Überwachung der Transaktionen werden Statistiken bereitgestellt oder an der Behandlung beteiligte Akteure beim Erreichen von Schwellwerten in den Daten benachrichtigt.[614]

Identity Smart Contracts übernehmen die Steuerung der im Blockchain-Netzwerk aktiven Identitäten. Das Aufgabenspektrum reicht dabei von einfachen Knoten-Klassifikation (z.B. Patient, Leistungserbringer)[615] über die Definition von Besitzverhältnissen[616] oder aller relevanten Identifikationsinformationen[617] bis zur Führung eines Registers, das reale Identifikationsmerkmale dem im Netzwerk verwendeten Pseudonym zuweist.[618]

Schwerpunkt von **Payment Smart Contracts** ist die automatisierte Abwicklung von Zahlungen. Diese entstehen bei der Zahlungsabwicklung mit Kostenträgern[619] wie auch bei der Durchführung finanziell orientierter Transaktionen von Gesundheitsdaten.[620]

Smart Contracts zur **Proxy Re-Encryption** beschreiben die Möglichkeit der Nutzung von Proxy-Re-Encryption-Methoden zur sicheren Ver- und Entschlüsselung von Daten, ohne sämtliche Informationen preiszugeben.[621]

---

612 Vgl. Zhuang et al. (2018): 1171f.

613 Vgl. Ito/Tago/Jin (2018): 831; Theodouli et al. (2018): 1376f; Zhang et al. (2018a): 5.

614 Vgl. Simić/Sladić/Milosavljević (2017): 3; Benhamouda/Halevi/Halevi (2018): 357, 359.

615 Vgl. Dagher et al. (2018): 288; Vora et al. (2018): 978. Alternativ kann auch bei Eintritt in ein Netzwerk ein Smart Contract auf dem neuen Knoten ausgeführt werden, der die tatsächliche Identität beschreibt (vgl. Mense/Athanasiadis (2018): 9f.).

616 Vgl. Cyran (2018): 3; Dagher et al. (2018): 288; Vora et al. (2018): 978f.

617 Vgl. Chang et al. (2018): 176.

618 Vgl. Azaria et al. (2016): 27; Ekblaw et al. (2016): 5; Yang/Yang (2017): 101; Alexaki et al. (2018): 256; Pukas/Smal/Zabchuk (2018): 171; Zhang et al. (2018b): 274. Auch ist es möglich, dass ein Smart Contract ein Register über alle bekannten Teilnehmer im Netzwerk enthält (vgl. Mense/Athanasiadis (2018): 9; Theodouli et al. (2018): 1376).

619 Vgl. Radanović/Likić (2018): 586f.

620 Vgl. Chen et al. (2018a): 206f; Colón (2018): 7; Desai et al. (2018): 1555; Grishin et al. (2018): 12.

621 Vgl. Dagher et al. (2018): 289.

Relationship Smart Contracts definieren die Verknüpfungen zwischen den im Netzwerk vorhandenen Nodes, und beschreiben damit die Verbindungen zwischen Patienten und Leistungserbringern oder zwischen den Leistungserbringern selbst.[622] Darüber hinaus werden Akteninformationen mit den relevanten Personen verknüpft.[623] Varianten dieser Smart Contracts führen ein Log über aktuelle und ehemalige Verknüpfungen.[624]

Summary Smart Contracts erstellen automatisiert eine Liste sämtlicher besuchter Einrichtungen und Referenzen zu Gesundheitsdaten, inklusive der damit verbundenen Zeitstempel und speichern diese Informationen auf der Blockchain. Ergänzend existieren Konzeptionen, die diese Smart Contracts mit einer Benachrichtigungsfunktion versehen und über neue Inhalte informieren.[625]

6.5.4 Coin/Token

Coins bzw. Token werden in einem Bruchteil der Publikationen behandelt (siehe *Tabelle 6-11* und *Abbildung 6-19*). Grundsätzlich besteht eine Nachfrage nach Kostenübernahme bzw. Incentivierung operativer Aufgaben im Netzwerk, wie bspw. Mining.[626] Leistungserbringer werden dabei entweder für die Bereitstellung von Daten und/oder Durchführung von Validierungs-/Mining-Aufgaben mit Geldleistungen oder Zugriffsberechtigungen auf anonymisierte Daten im Netzwerk belohnt.[627] Bei fehlerhaftem Verhalten und Schädigung des Netzwerks ermöglicht ein eingesetzter Coin zudem eine automatisierte Strafzahlung.[628]

Alternative Finanzierungsmodelle legen operative Kosten auf den Patienten um,[629] indem dieser je nach Auslastung seiner Speicher ergänzende Speicherkontingente erwirbt.[630] Gleichzeitig existieren Varianten, die den Patienten für eine Freigabe eigener Daten belohnen, deren Auszahlung wiederum für Dienstleistungen eingesetzt werden können.[631]

---

622 Vgl. Azaria et al. (2016): 27; Ekblaw et al. (2016): 5; Yang/Yang (2017): 101; Bhuiyan et al. (2018): 67; Pukas/Smal/Zabchuk (2018): 171; Vora et al. (2018): 978.

623 Vgl. Bhuiyan et al. (2018): 67; Chang et al. (2018): 176; Yang/Li (2018): 262.

624 Vgl. Xia et al. (2017a): 14762f; Dagher et al. (2018): 288; Pukas/Smal/Zabchuk (2018): 171.

625 Vgl. Azaria et al. (2016): 27f; Ekblaw et al. (2016): 5f; Yang/Yang (2017): 101; Yang/Li (2018): 262; Zhuang et al. (2018): 1172.

626 Vgl. Magyar (2017): 138.

627 Vgl. Azaria et al. (2016): 29; Ekblaw et al. (2016): 8; Kuo/Ohno-Machado (2018): 6.

628 Vgl. Grishin et al. (2018): 18f; Zhou/Wang/Sun (2018): 149.6.

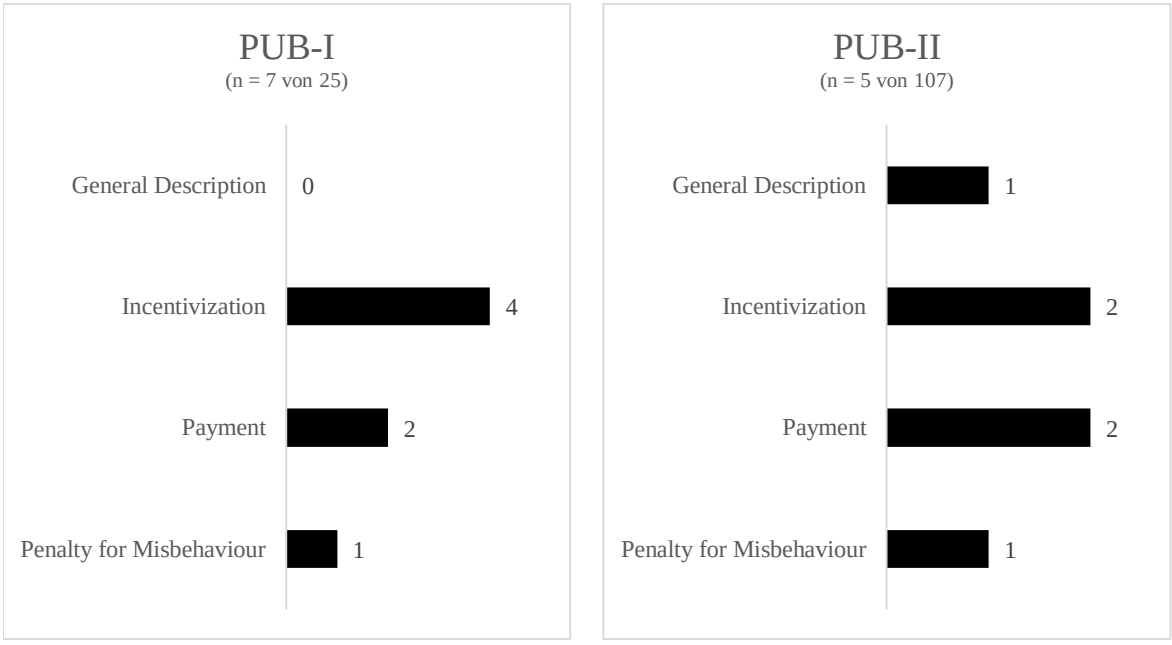
629 Vgl. Wanitcharakkhakul/Rotchanakitumnuai (2017): 55.

630 Vgl. McFarlane et al. (2017): 12f. Die Preisgestaltung kann individuell bspw. mit einem Ask/Bid-System umgesetzt werden (vgl. Du et al. (2018): 36, 38–39).

631 Vgl. Colón (2018): 7; Medicalchain (2018): 26f; Zheng et al. (2018): 165.

Tabelle 6-11: Literatur-Kategorien ‚Technology – Coin/Token' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
General Description		Magyar (2017)
Incentivization	Azaria et al. (2016); Ekblaw et al. (2016); Kuo/Ohno-Machado (2018); Medicalchain (2018)	Colón (2018); Zheng et al. (2018)
Payment	McFarlane et al. (2017); Du et al. (2018)	Wanitcharakkhakul/Rotchanakitumnuai (2017); Zheng et al. (2018)
Penalty for Misbehaviour	Zhou/Wang/Sun (2018)	Grishin et al. (2018)



Anmerkung: Mehrfachzuweisungen möglich

Abbildung 6-19: Verteilung ‚Technology – Coin/Token' auf PUB-I und PUB-II (Quelle: Eigene Darstellung)

7 Konstruktion des Artefakts und Ableitung eines Entscheidungsmodells

7.1 Referenzarchitektur

7.1.1 Definition der in der Architektur genutzten Notation

Die Architektur besteht aus Gruppen, Variationspunkten und Ausprägungen. Variationspunkte stehen entweder für sich selbst oder erlauben eine ergänzende Unterteilung in mehrere Ausprägungen und können in Gruppen zusammengefasst werden. Variationspunkte und Ausprägungen werden durch Kanten miteinander verbunden und beschreiben folglich Hierarchien von Variationspunkten (siehe *Abbildung 7-1*).

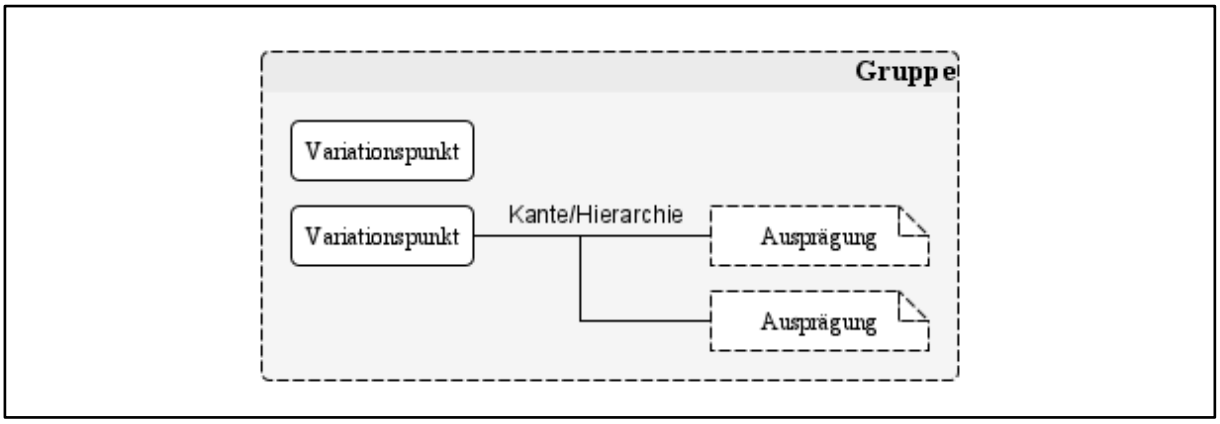


Abbildung 7-1: Notation in der Darstellung der Referenzarchitektur (Quelle: Eigene Darstellung)

7.1.2 Sicht: Record Type

Ausgehend von den Ausführungen des *Kapitels 6.2* können die in *Abbildung 7-2* beschriebenen Variationen der Sicht *Record Type* konstruiert werden. Die Unterteilung der EHR in die Ausprägungen *EMR* und *patientengenerierte Inhalte* ist aufgrund der unklaren Begriffsbezeichnung in der Literatur notwendig. In diesem besonderen Fall liegt der Unterscheid in der Verwaltung dieser Daten. Da weiterhin der Leistungserbringer und nicht der Patient die Verwaltung übernimmt, grenzt sich EHR weiterhin von *Patient Health Records* ab.

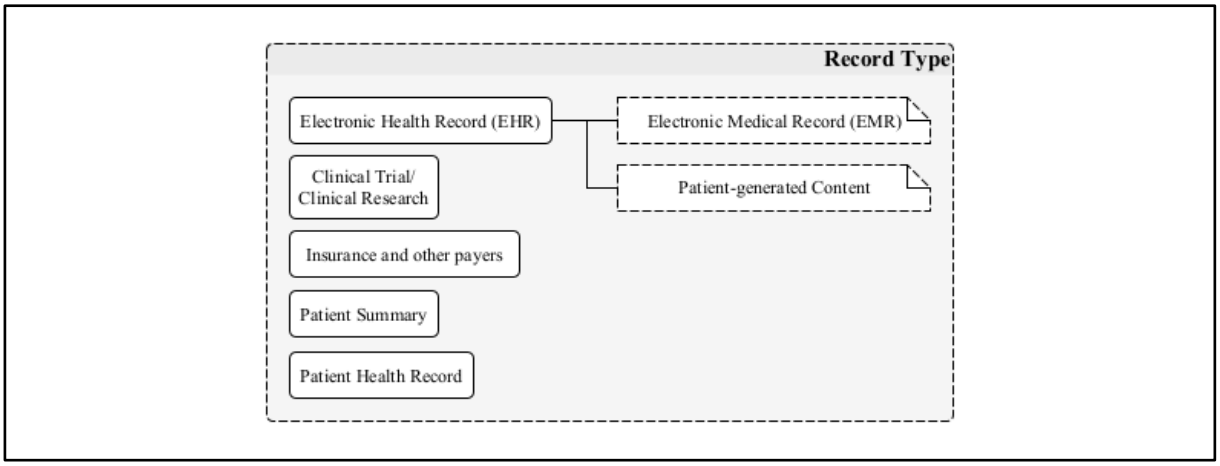


Abbildung 7-2: Sicht ‚Record Type'
(Quelle: Eigene Darstellung)

7.1.3 Sicht: Data Storage & Provisioning

Auf Basis der in *Kapitel 6.3* gewonnenen Erkenntnisse lässt sich die in *Abbildung 7-3* veranschaulichte Teil-Sicht der Referenzarchitektur inklusive der entsprechenden Variationspunkte konstruieren.

Kern dieser Sicht ist die allgemeine Unterscheidung zwischen *on*- und *off-Chain*-Datenhaltung sowie Datenbereitstellung. Ausgehend von der allgemeinen Diskussion zum Thema Datenhaltung können, in den Variationspunkten diverse Technologien identifiziert werden, die die Datenhaltung unterstützen, bspw. durch Hosting in einer Cloud oder Verwendung von IPFS. Gleichfalls werden bestehende und im Gesundheitswesen etablierte Standards genannt, die aufgrund der Forcierung von Interoperabilität eine Relevanz für die Datenhaltung und gemeinsame Verwaltung über die Blockchain entwickeln.

Die Verwaltung wiederum geschieht durch die Bereitstellung von Gatekeepern oder die Verwendung von Pointern, die auf der Blockchain zusammen mit den Gesundheitsdaten abgelegt oder in einem separaten Index geführt werden.

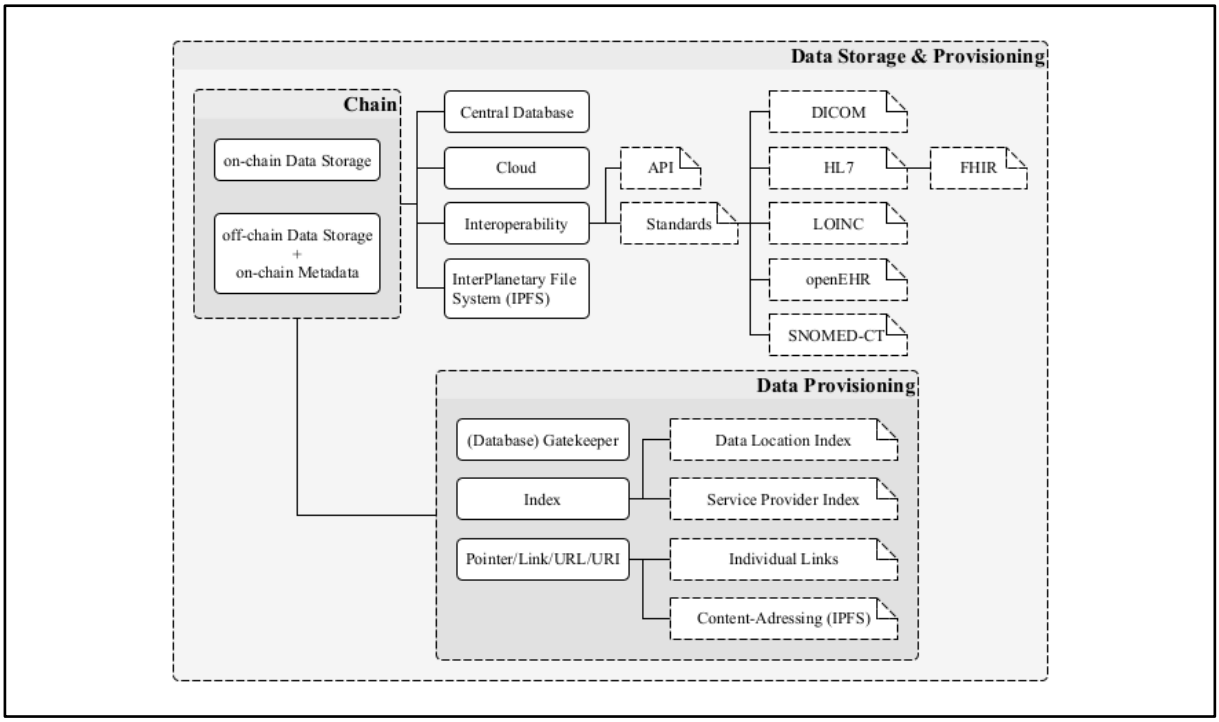


Abbildung 7-3: Sicht ‚Data Storage & Provisioning'
(Quelle: Eigene Darstellung)

7.1.4 Sicht: Security

Ergebnisse aus *Kapitel 6.4* führen zu der in *Abbildung 7-4* dargestellten Sichtenkonstruktion der Referenzarchitektur. Der Aufbau dieser Sicht orientiert sich am Aufbau von IAM-Systemen, die wie die Ausführungen in *Kapitel 6.4.1* zeigen Access Management bzw. Identity Management getrennt voneinander betrachten. Darüber hinaus existieren allgemeine Infrastrukturthemen, die den Einsatz einer PKI oder KSI diskutieren, sowie unterschiedliche Ansätze, ein Logging und Audit zu realisieren.

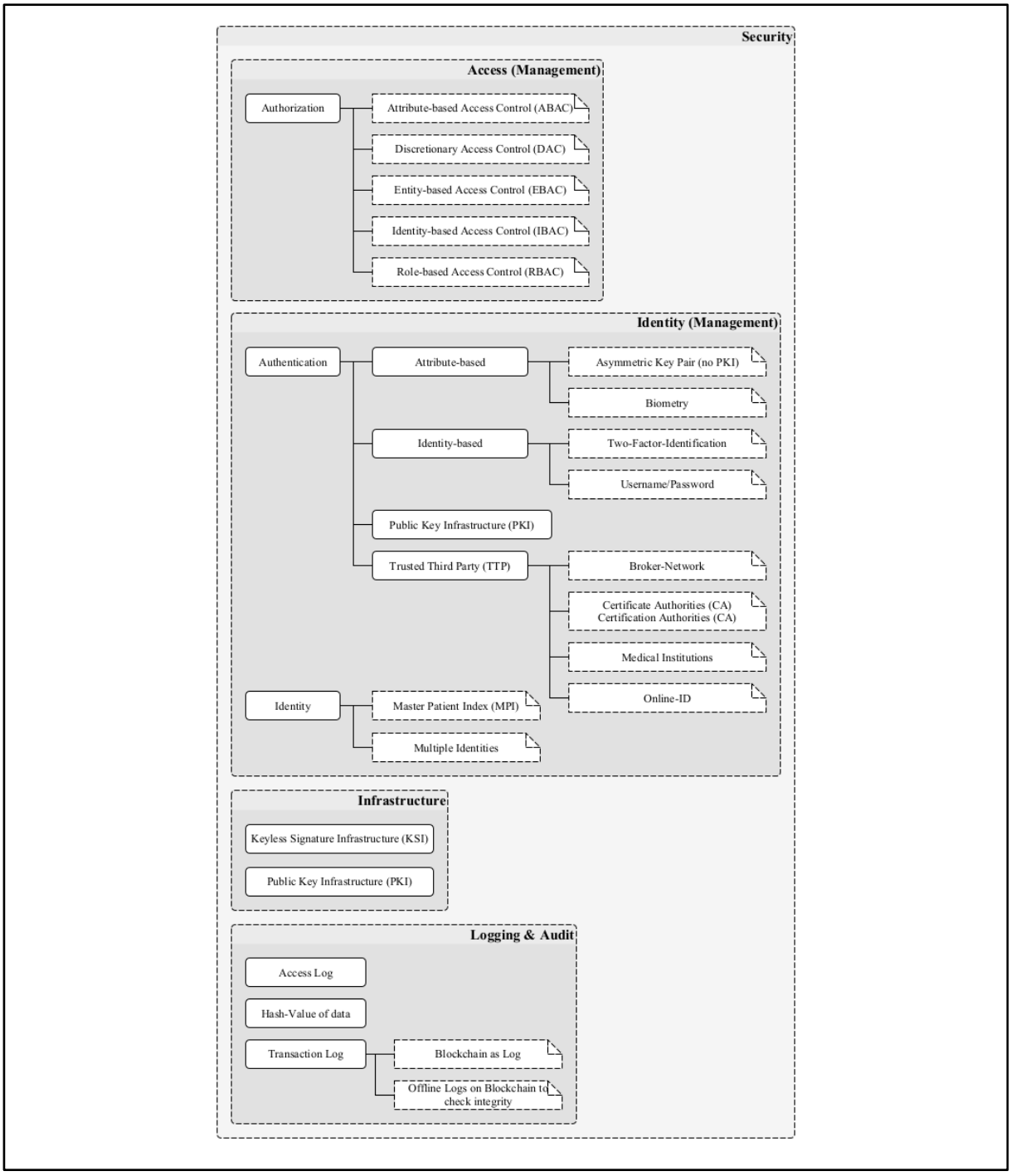


Abbildung 7-4: Sicht ‚Security'
(Quelle: Eigene Darstellung)

7.1.5 Sicht: Technology

Diese Sicht folgt in der Anordnung ihrer Variationspunkte einem hierarchischen Prinzip und beginnt mit der Überlegung, ob eine einzige Blockchain oder mehrere parallel verlaufende Blockchains betrieben werden. Darauf folgt die Betrachtung der Klassifikation der Blockchain-Taxonomie bis zur konkreten Technologieauswahl. Damit einher geht die Auswahl des notwendigen Konsensprotokolls, die potentielle Verwendung sowie Auswahl von Smart Contracts bzw. Chaincode sowie die Möglichkeit, Coins/Token, bspw. zur Incentivierung, einzusetzen.

Die entsprechende Struktur der Variationspunkte ist in *Abbildung 7-5* dargestellt.

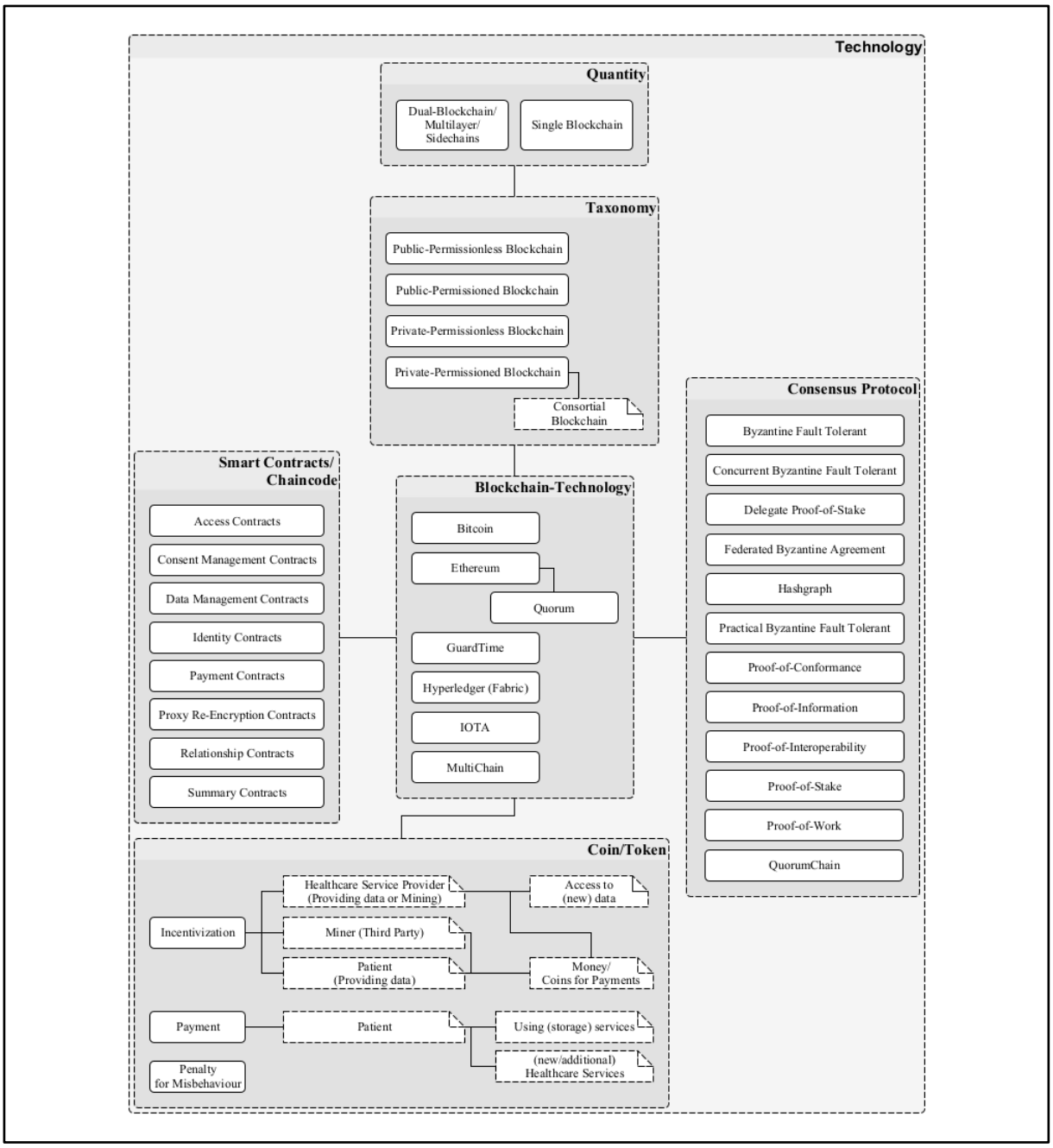


Abbildung 7-5: Sicht ‚Technologie'
(Quelle: Eigene Darstellung)

7.1.6 Gesamtansicht: Referenzarchitektur

Auf Basis der Analysen sowie der in den *Kapiteln 7.1.2* bis *7.1.5* schematisch dargestellten Sichten ist die Zusammenführung der Ergebnisse in die in *Abbildung 7-6* dargestellte Gesamtarchitektur möglich.

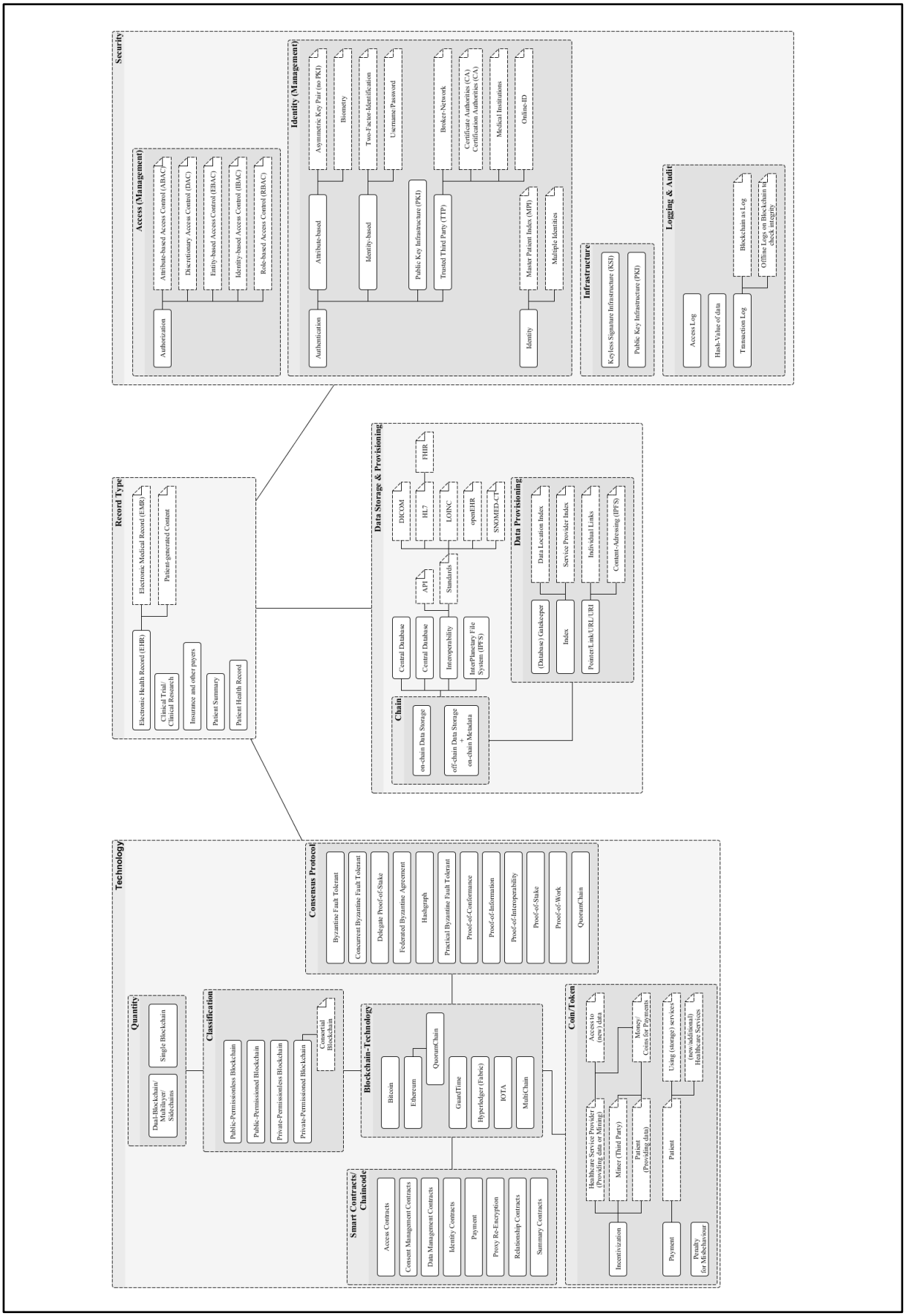


Abbildung 7-6: Referenzarchitektur (Gesamtübersicht) (Quelle: Eigene Darstellung)

Grundsätzlich wird davon ausgegangen, dass zwischen sämtlichen Schichten der Architektur ein Zusammenhang existiert, doch stellt sich in der vorangegangenen Analyse heraus, dass alle Architekturen auf Grundlage einer Anforderungsdefinition (bestehender oder zukünftiger Aktensysteme) entwickelt werden. Deshalb wird auch in der Darstellung der Referenzarchitektur die Sicht *Record Type* als zentraler Faktor dargestellt und folglich eine Abhängigkeit der weiteren Variationswahl definiert. Diese Erkenntnis ist insbesondere in der Modellkonstruktion im folgenden *Kapitel 7.2* von Bedeutung, da sich ausgehend von der Wahl eines Aktensystems die zur Verfügung stehenden Variationspunkte verändern.

7.2 Entscheidungsmodell zur Wahl von Variationspunkten

Die in *Kapitel 7.1.6* dargestellte Gesamtarchitektur erlaubt unter Anwendung der Analyseergebnisse aus *Kapitel 6* die Ableitung eines Modells, das sämtliche Entscheidungsvariationen aufführt und künftige Architekten in der Anwendung der Referenzarchitektur bzw. der Auswahl der für die Entwicklung einer Blockchain-Lösung relevanten Variationspunkte unterstützt. Zudem sind weitere offene Felder in der wissenschaftlichen Forschung identifizierbar.

Zur Entwicklung des Entscheidungsmodells wird eine Matrix-Analyse genutzt, die zeilenweise alle 132 als relevant eingestuften Publikationen aufführt und spaltenweise sämtliche Variationspunkte, die in *Kapitel 6* analysiert bzw. in den Unterkapiteln des *Kapitels 7.1* in den Abbildungen dargestellt werden. Ein boolescher Operator (0 = nicht relevant, 1 = relevant) markiert Zuweisungen der Literatur zu dem jeweiligen inhaltlich identifizierten Variationspunkt. Eine Teilansicht der beschriebenen Matrix wird in *Abbildung 7-7* dargestellt.[632] Diese Methode erlaubt neben der Identifikation von inhaltlichen Clustern die Ableitung von zusammenhängenden Designentscheidungen und folglich die Konstruktion des Entscheidungsmodells.

Kurztitel unten enthät Schlagwort von rechts	Kat	DataStorage_ Chain_ off-chain	DataStorage_ Chain_ on-chain	DataStorage_ Cloud	RecordType_ PHR	Technology_ SmartContracts/Chaincode_ DataMgmt	Technology_ SmartContracts/Chaincode_ Identity
Ahram, Sargolzaei et al. 2017 – Blockchain technology innovations	PUB-I		1	1	1	1	
Al Omar, Rahman et al. 2017 – MediBchain	PUB-I		1		1	1	
Alexaki, Alexandris et al. 2018 – Blockchain-based Electronic Patient Records	PUB-II				1	1	1
Alhadhrami, Alghfeli et al. 2017 – Introducing blockchains for healthcare	PUB-II						
Amofa, Sifah et al. 2018 – A Blockchain-based Architecture Framework	PUB-II				1		

Abbildung 7-7: Auszug aus Matrix zur Analyse der Entscheidungspfade durch Variationspunktidentifikation (Quelle: Eigene Darstellung)

[632] Die Darstellung der gesamten Matrix ist aufgrund der Größe nicht möglich. Stattdessen werden entsprechende Literaturverweise in den Übersichtstabellen der jeweiligen Kapitel zusammengefasst.

Die Abhängigkeit der Designentscheidungen vom gewählten *Record Type* wird bereits in *Kapitel 7.1.6* thematisiert. Daher werden die Folgekapitel nicht mehr in Sichten aufgeteilt, sondern entsprechend dem gewählten *Record Type* strukturiert.

Die Notation in den Grafiken orientiert sich dabei an *Abbildung 7-1* aus *Kapitel 7.1.1*. Einziger Unterschied ist, dass sich die dargestellte *Kante* in eine *gerichtete Kante (Pfeil)* verändert und so eine prozessuale Abfolge von Entscheidungen simuliert wird. Darüber hinaus wird in einem Kreis die Anzahl der relevanten Publikationen genannt, sodass eine Gewichtung der jeweiligen Variation erkennbar ist.

7.2.1 Clinical Trial / Clinical Research

In der Sicht **Data Storage & Provisioning** (siehe *Abbildung 7-8*)existieren für diesen Record Type ausschließliche Publikationen, die off-chain-Konzepte verfolgen und zur Speicherung von Daten auf Cloud und IPFS zurückgreifen. Darüber hinaus ist das Thema Interoperabilität relevant. Unter der Annahme hierarchischer Abhängigkeiten ergibt sich bei Filterung auf den off-chain-Variationspunkt, dass Datenhaltung entweder in der Cloud oder unter Anwendung von IPFS durchgeführt wird (siehe *Abbildung 7-9*).

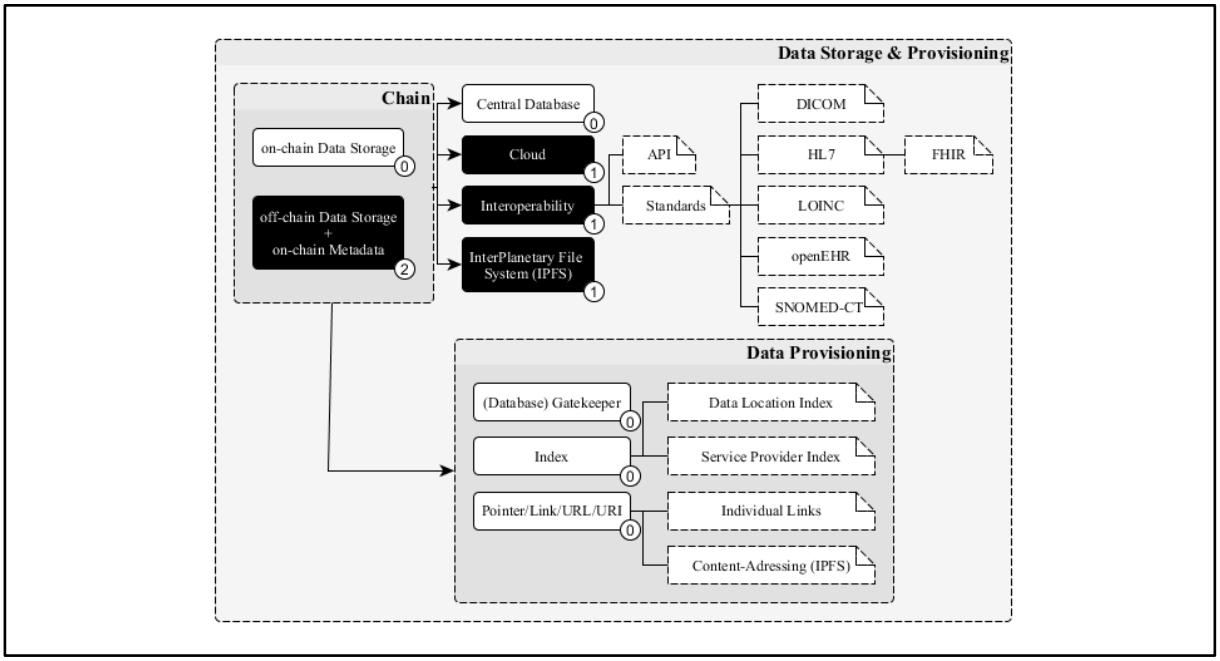


Abbildung 7-8: Clinical-Trial-Variationen in der Sicht ‚Data Storage & Provisioning' ohne Filterung (Quelle: Eigene Darstellung)

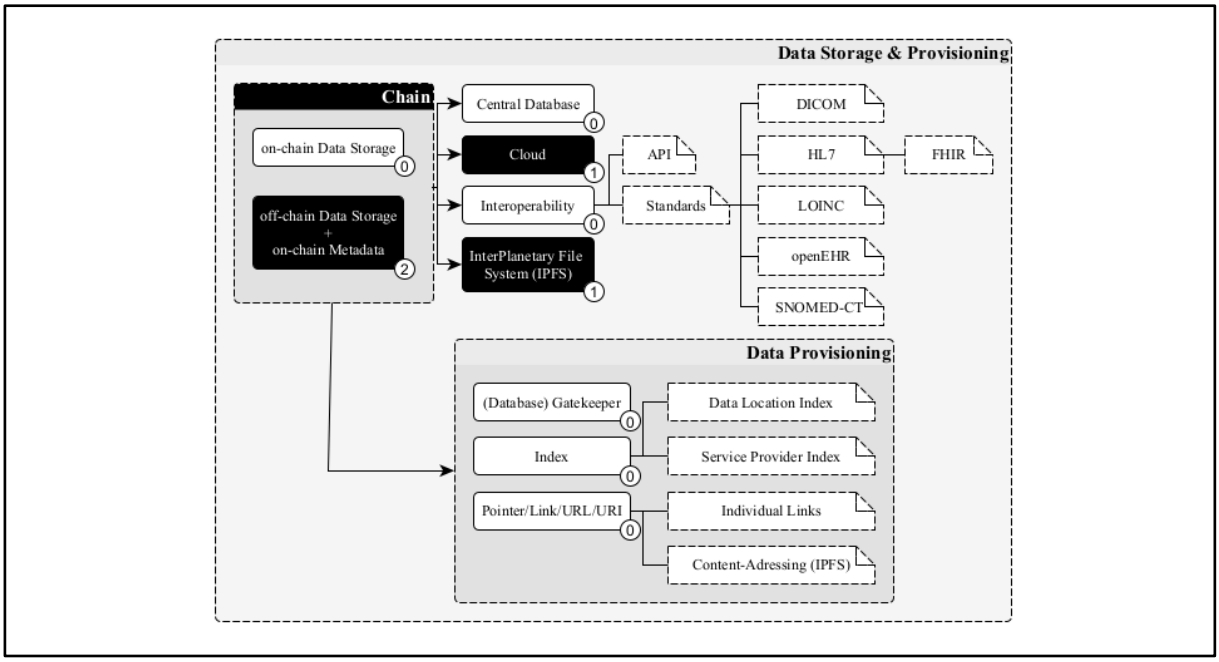


Abbildung 7-9: Clinical-Trial-Variationen in der Sicht ‚Data Storage & Provisioning' mit Filterung auf ‚off-chain Data Storage'
(Quelle: Eigene Darstellung)

Die Betrachtung der **Security** umfasst sämtliche identifizierten Bereiche (siehe *Abbildung 7-10*). In der Autorisierung beschränken sich die relevanten Publikationen auf der rollenbasierten Umsetzung (RBAC). Zur Authentifizierung werden identitätsbasierte Verfahren (Benutzername und Passwort) genutzt. Die Validierung von Identitäten wird durch TTP, insbesondere der Verwendung von CAs vorgenommen. Hintergrund dieser Wahl ist der Fokus der Literatur auf PKI-Infrastrukturen. KSI wird zwar ebenfalls erwähnt, dessen Potential in der Literatur jedoch nicht tiefergehend erläutert. Im Bereich *Logging & Audit* beschränken sich Lösungen auf die Speicherung des Hash-Werts von Daten auf der Blockchain, um deren Integrität zu gewährleisten. Dies erlaubt die Nachvollziehbarkeit von Ergebnissen der klinischen Forschung.

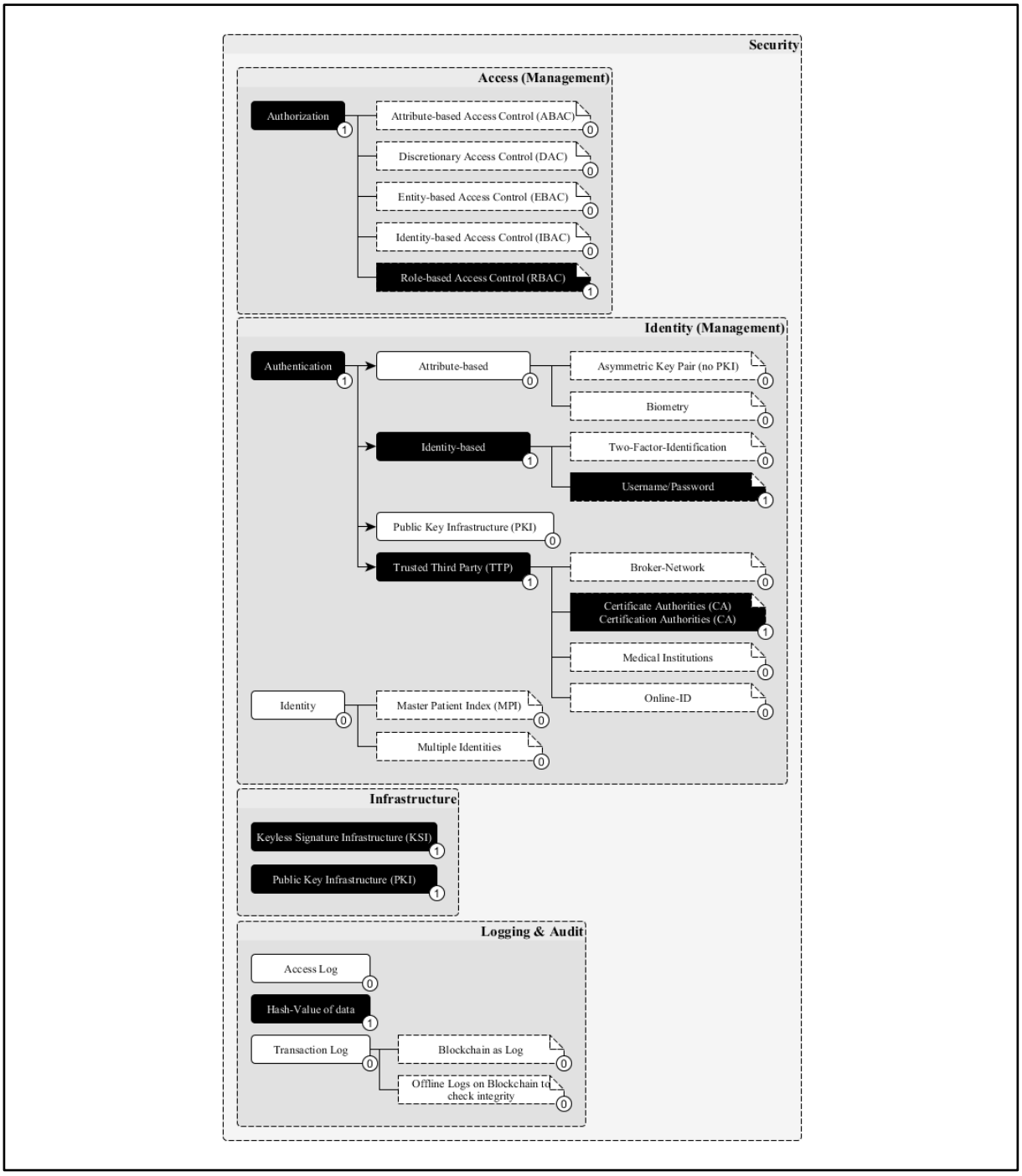


Abbildung 7-10: Clinical-Trial-Variationen in der Sicht ‚Security' ohne Filterung (Quelle: Eigene Darstellung)

Sämtliche Entscheidungen der Sicht **Technology** für diesen Record Type sind in *Abbildung 7-11* aufgezeigt. Bereits zu Beginn ist erkennbar, dass sich die Literatur auf den Betrieb einer einzigen Blockchain beschränkt. Auch werden trotz der Nennung von *Hyperledger* im Grunde keine konsortialen Blockchains behandelt. Der Einsatz von Smart Contracts beschränkt sich auf *Access*, *Consent Management* und *Payment*. Letzteres ist insbesondere wegen der thematisierten Incentivierungen relevant.

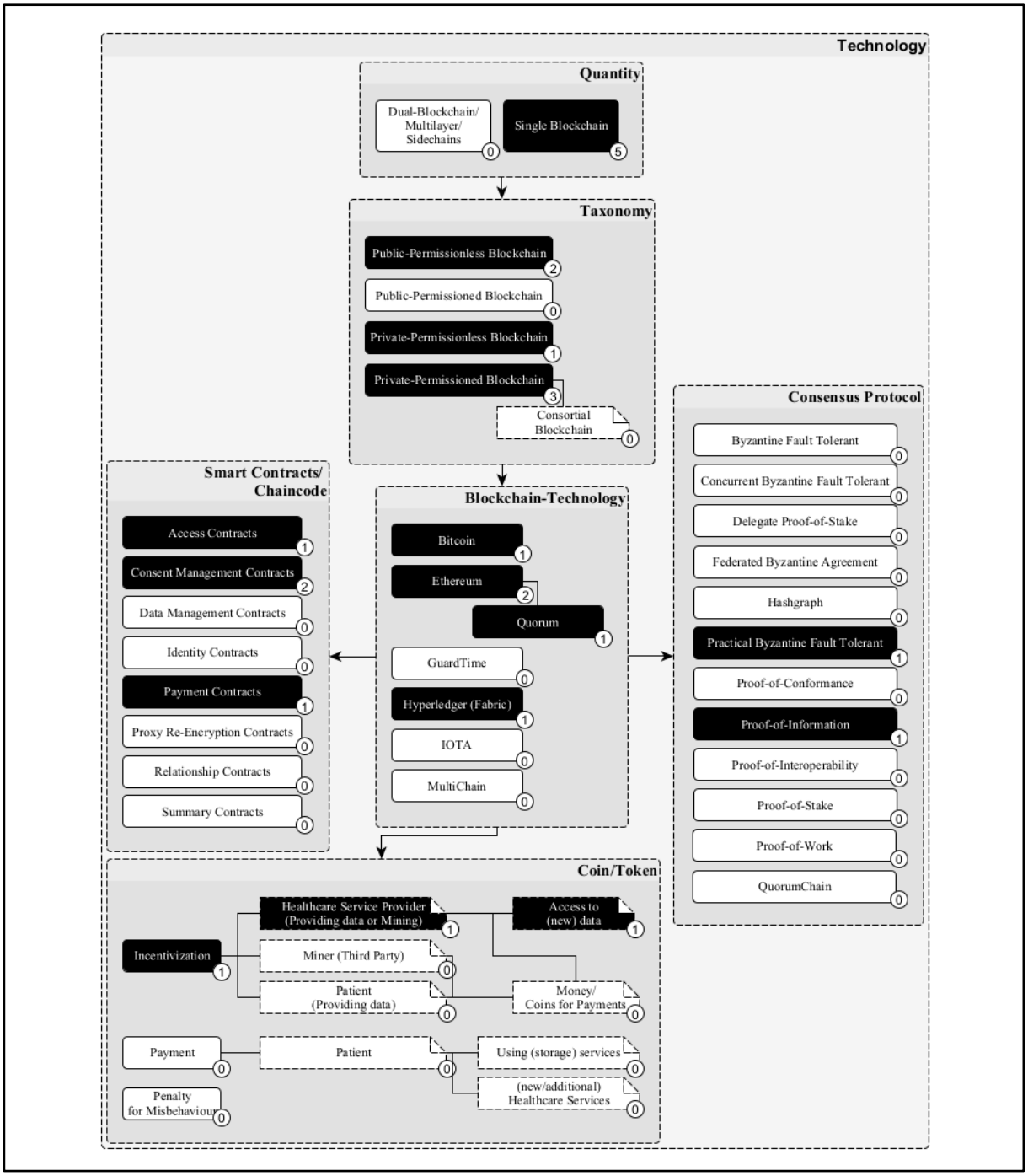


Abbildung 7-11: Clinical-Trial-Variationen in der Sicht ‚Technology' ohne Filterung (Quelle: Eigene Darstellung)

Für eine genaue Entscheidungsfindung werden erneut Filter verwendet, die sich auf die Blockchain-Taxonomie bzw. -Technologie beschränken. Die Ergebnisse dieser Filtereinsätze sind allerdings nur bedingt auf die Realität übertragbar, da einige Publikationen Themen nur anreißen.[633] Dies ist in den folgenden Filterungen ersichtlich. In einem ersten Schritt wird der Filter auf die *Taxonomy* gesetzt:

633 Aus diesem Grund ist die Gesamtsicht entsprechend *Abbildung 7-11* aussagekräftiger.

i. Public-Permissionless (siehe *Abbildung 7-12*)

ii. Private-Permissionless (siehe *Abbildung 7-13*)

iii. Private-Permissioned (siehe *Abbildung 7-14*)

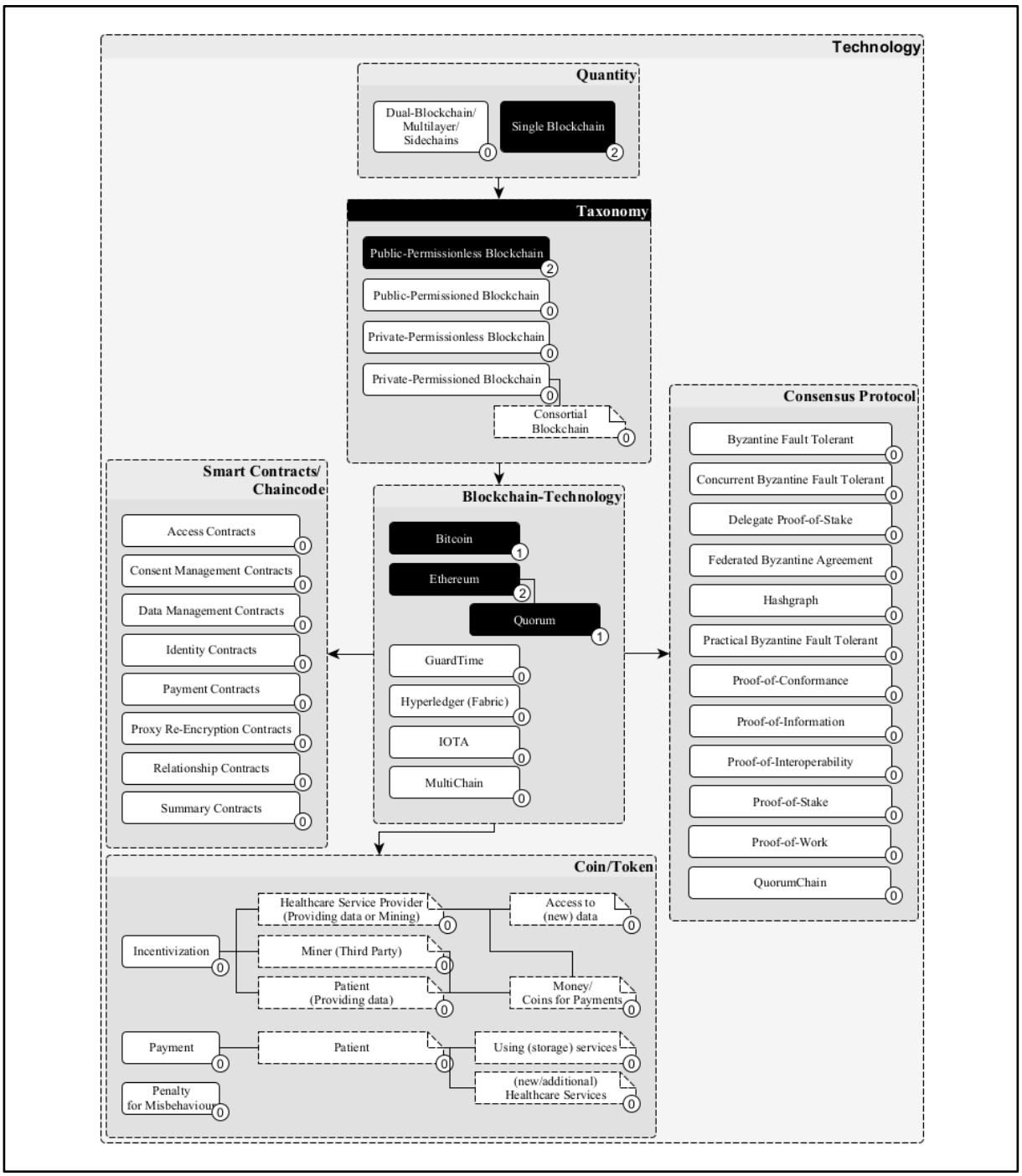


Abbildung 7-12: Clinical-Trial-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Public-Permissionless Blockchain'
(Quelle: Eigene Darstellung)

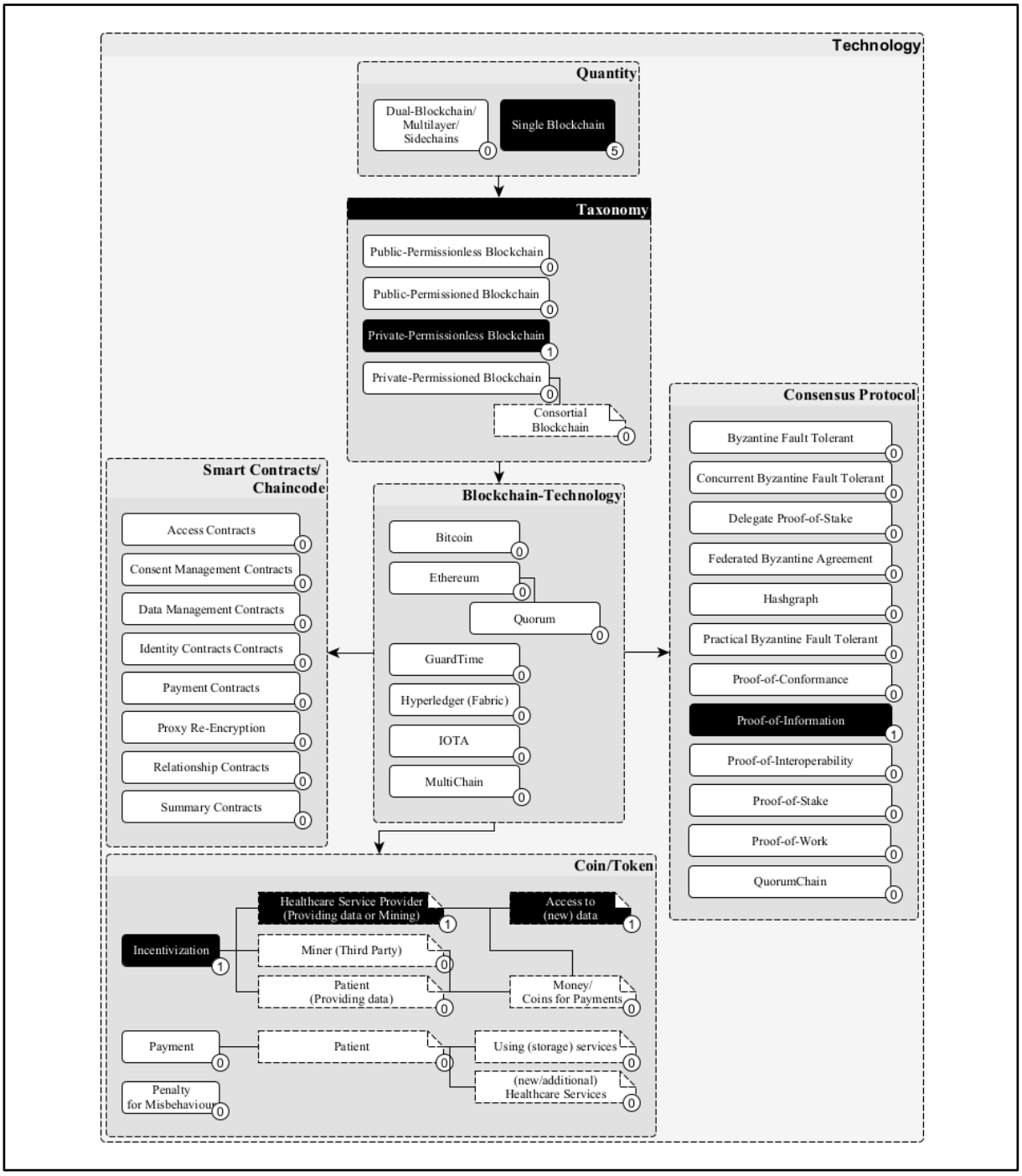


Abbildung 7-13: Clinical-Trial-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Private-Permissionless Blockchain'
(Quelle: Eigene Darstellung)

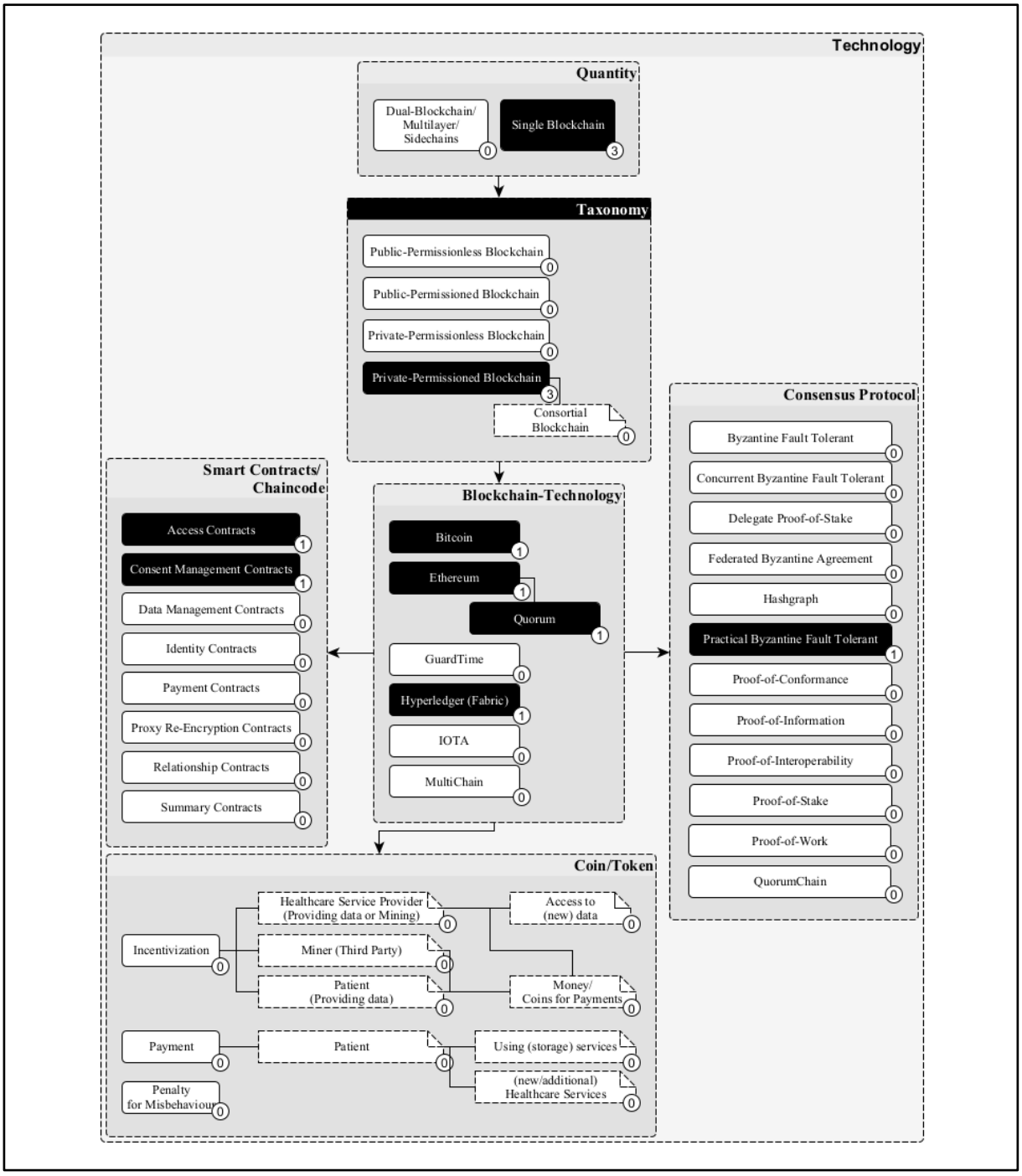


Abbildung 7-14: Clinical-Trial-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Private-Permissioned Blockchain'[634]
(Quelle: Eigene Darstellung)

634 Bitcoin wird in der Publikation von BELL ET AL. (2018) genannt, die einen Gesamtüberblick über potentielle Anwendungsmöglichkeiten von Blockchain im Gesundheitswesen gibt. Es existiert kein Zusammenhang zwischen Taxonomie und Technologie.

Ein weiterer Ansatz ist die Fokussierung auf die Blockchain-Technologie statt auf Taxonomie. Hier ergeben sich die folgenden möglichen Ausprägungen und Abbildungen:

i. Bitcoin (siehe *Abbildung 7-15*)
ii. Ethereum (siehe *Abbildung 7-16*)
iii. Quorum (siehe *Abbildung 7-17*)
iv. Hyperledger (Fabric) (siehe *Abbildung 7-18*)

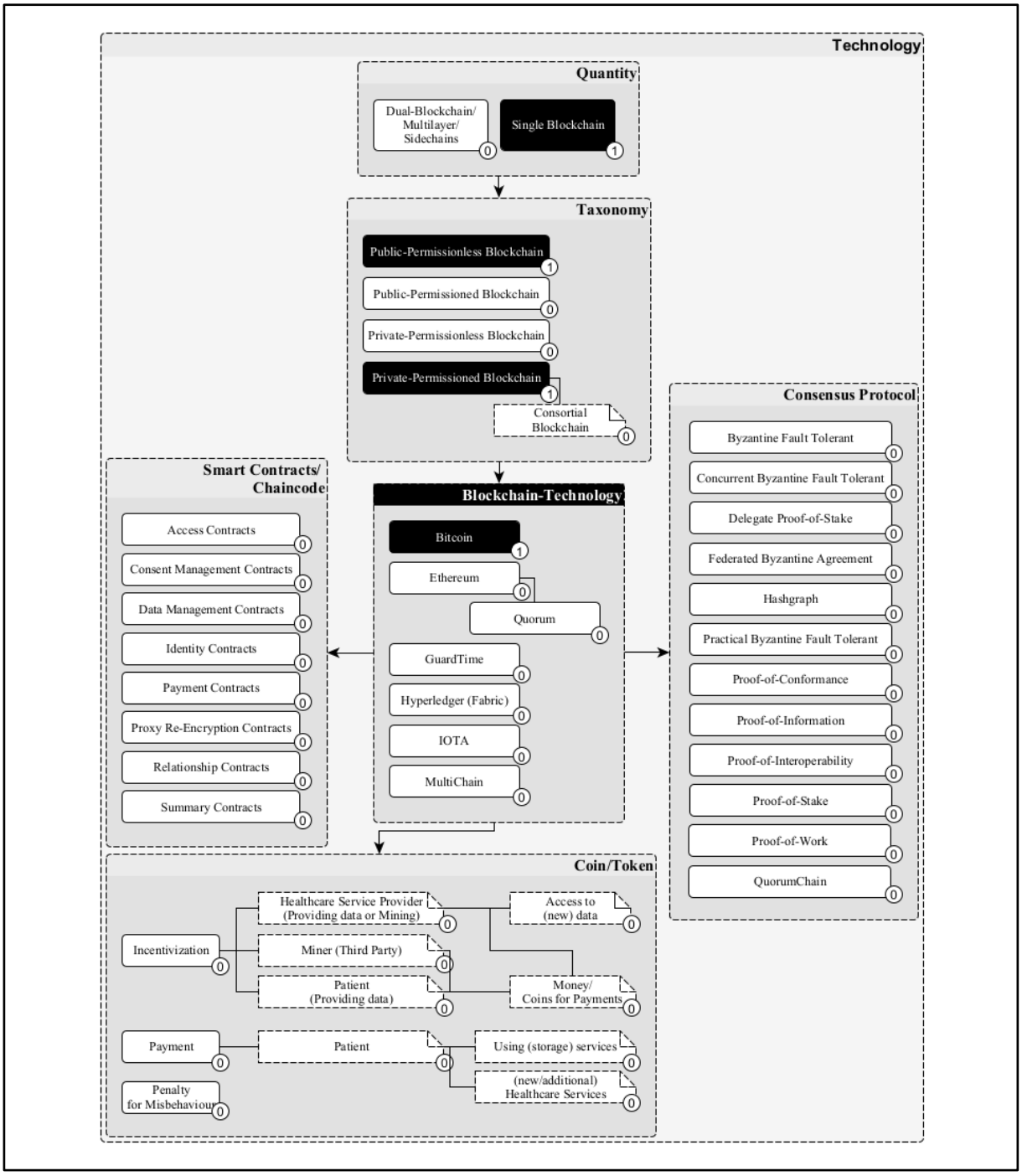


Abbildung 7-15: Clinical-Trial-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Bitcoin' (Quelle: Eigene Darstellung)[635]

635 Bitcoin wird in der Publikation von BELL ET AL. (2018) genannt, die einen Gesamtüberblick über potentielle Anwendungsmöglichkeiten von Blockchain im Gesundheitswesen gibt. Es existiert kein Zusammenhang zwischen Taxonomie und Technologie.

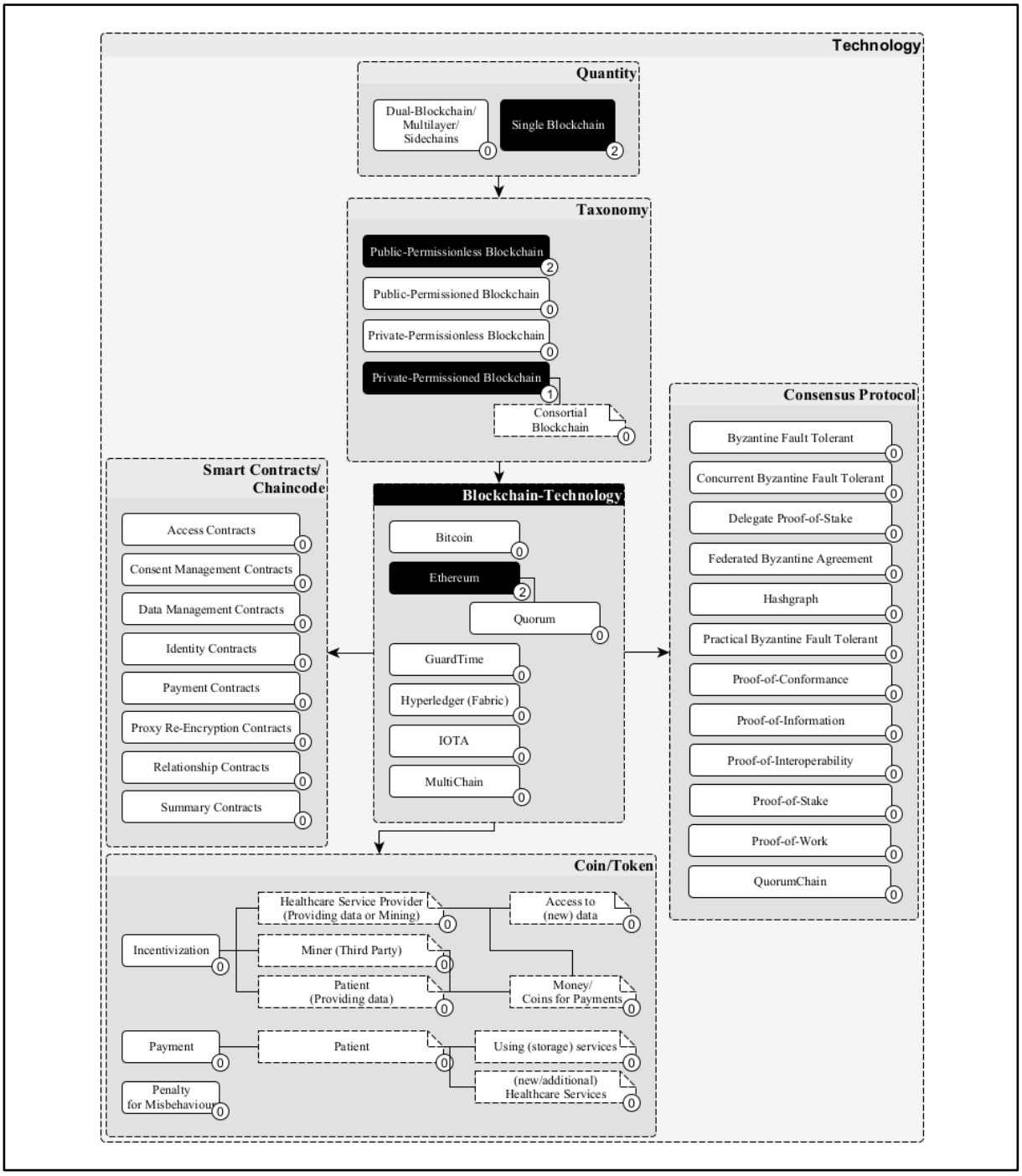


Abbildung 7-16: Clinical-Trial-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Ethereum' (Quelle: Eigene Darstellung)[636]

636 *Ethereum* wird in der Publikation von BELL ET AL. (2018) genannt, die einen Gesamtüberblick über potentielle Anwendungsmöglichkeiten von Blockchain im Gesundheitswesen gibt. Es existiert kein Zusammenhang zwischen Taxonomie und Technologie.

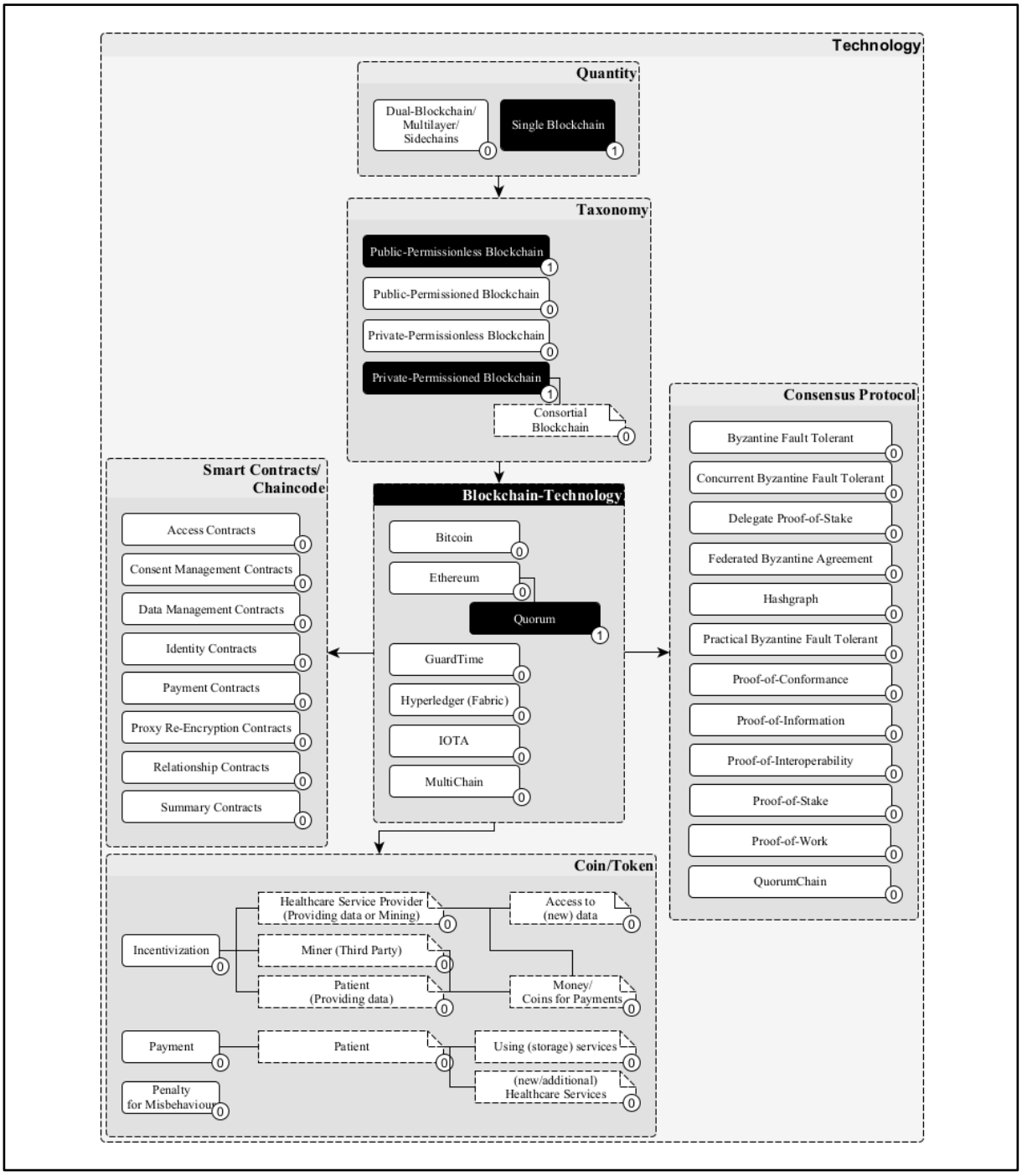


Abbildung 7-17: Clinical-Trial-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Quorum'[637] *(Quelle: Eigene Darstellung)*

637 *Quorum* wird in der Publikation von BELL ET AL. (2018) genannt, die einen Gesamtüberblick über potentielle Anwendungsmöglichkeiten von Blockchain im Gesundheitswesen gibt. Es existiert kein Zusammenhang zwischen Taxonomie und Technologie.

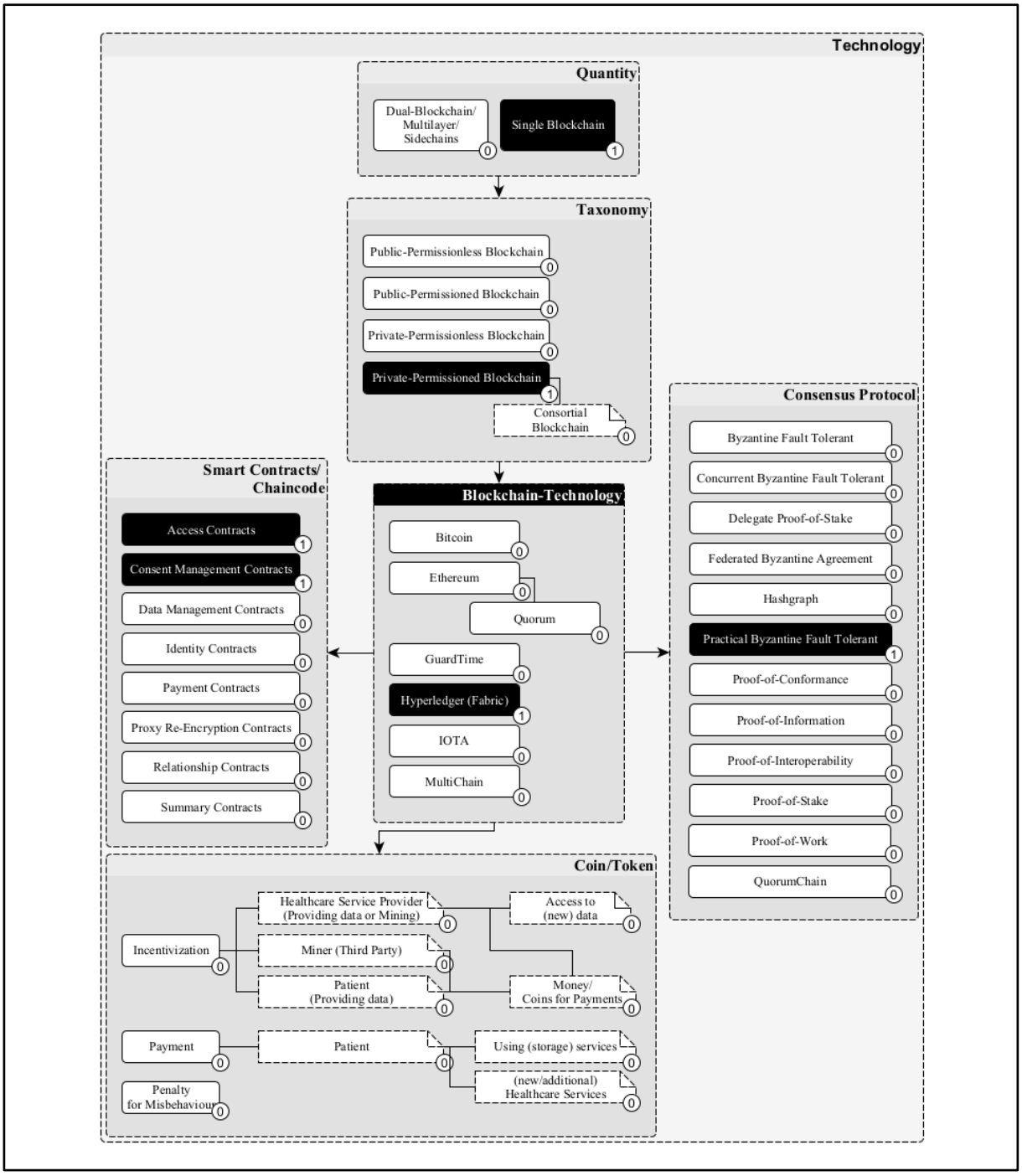


Abbildung 7-18: Clinical-Trial-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Hyperledger (Fabric)' (Quelle: Eigene Darstellung)

7.2.2 Electronic Health Records

Im Rahmen von **Data Storage & Provisioning** ergibt sich für diesen Record Type, dass ausschließlich eine off-chain-Datenspeicherung in Frage kommt und so die bereits in den Einrichtungen bestehenden Datenspeicher zum Einsatz kommen. Dabei spielen Cloud, IPFS und zentral organisierte Datenbanken eine Rolle. Auch wird diskutiert, ob Blockchain insgesamt die Interoperabilität von Gesundheitsdaten unterstützt. Die Blockchain übernimmt grundsätzlich die Verwaltung von Metadaten und stellt in diesem Zusammenhang auch die Pointer in externen Datenspeicher bereit. Sämtliche Entscheidungspunkte sind in *Abbildung 7-19* dargestellt. Eine Veränderung dieser Variationen ergibt sich nach einer Filterung auf ‚off-chain Data Storage' nicht (siehe *Abbildung 7-20*).

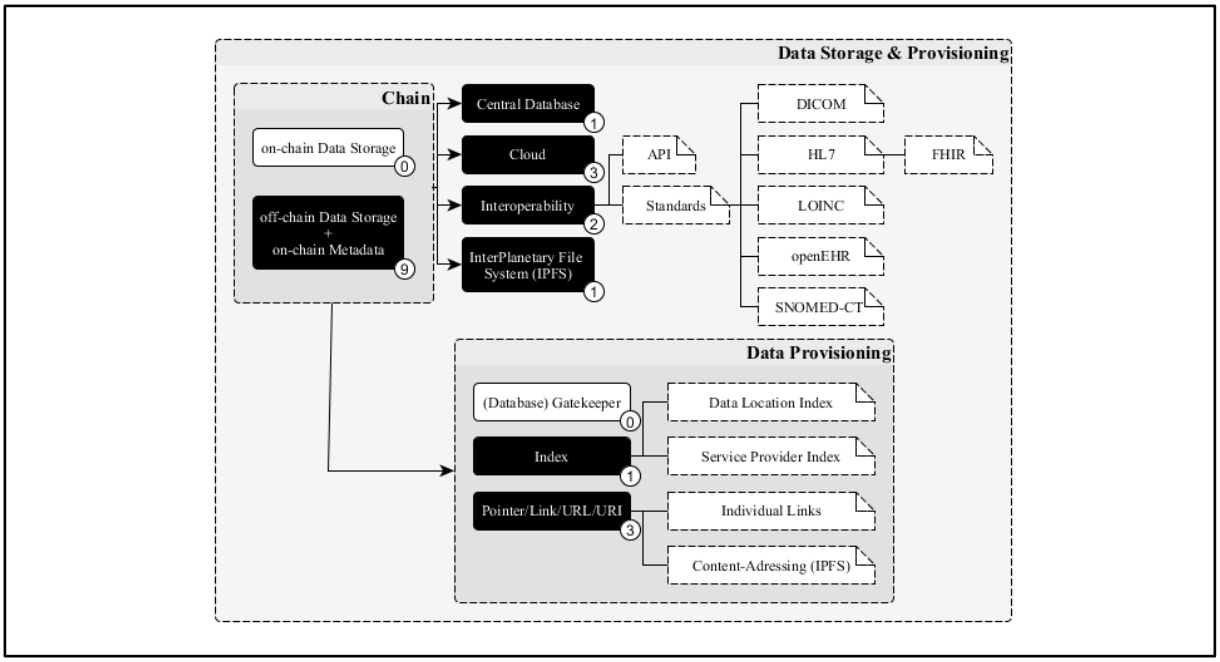


Abbildung 7-19: EHR-Variationen in der Sicht ‚Data Storage & Provisioning' ohne Filterung (Quelle: Eigene Darstellung)

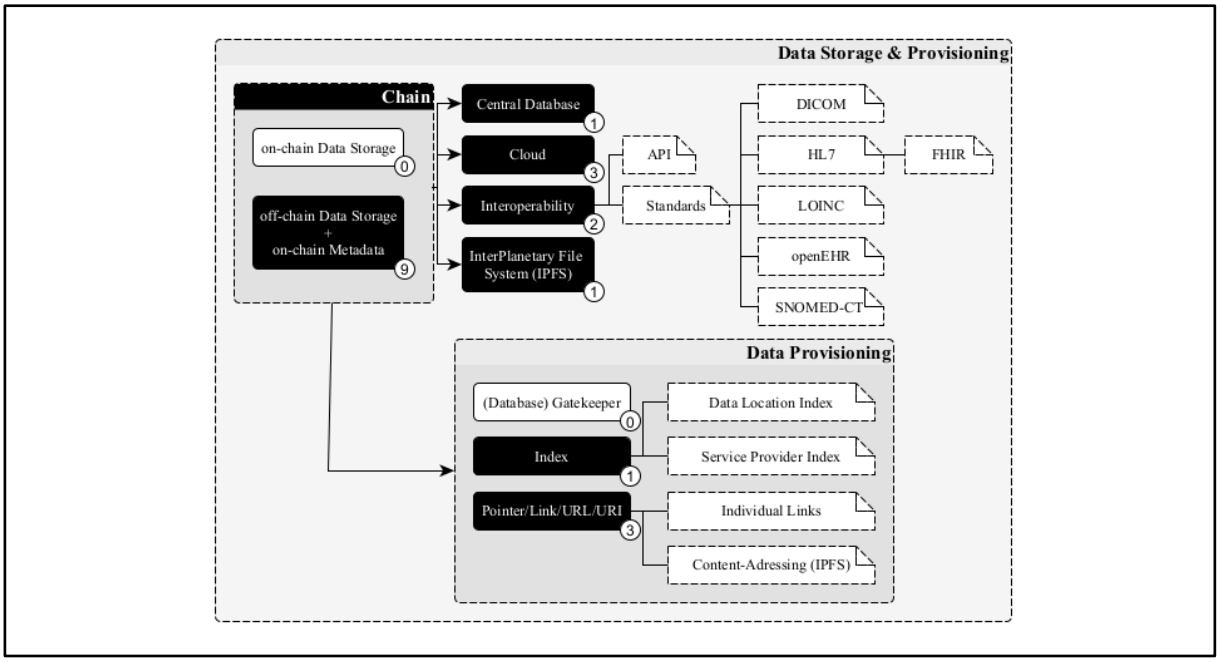


Abbildung 7-20: EHR-Variationen in der Sicht ‚Data Storage & Provisioning' mit Filterung auf ‚off-chain Data Storage'
(Quelle: Eigene Darstellung)

Beim Thema **Security** finden sich alle vier Security-Kategorien wieder (siehe *Abbildung 7-21*). Im Access-Management wird für die Autorisierung auf Konzepte des ABAC und RBAC gesetzt. Die Authentifizierung im Identity Management wird entweder durch bereits etablierte Kontrollmechanismen umgesetzt, wie die Eingabe von Benutzername und Passwort, oder über asymmetrische Schlüsselpaare, die keine PKI voraussetzen. Im Netzwerk können mehrere Identitäten genutzt werden, deren Validität durch TTPs, genauer medizinische Einrichtungen, sichergestellt wird. Im Rahmen des *Logging & Audit* speichert die Blockchain Access Logs, Hash-Werte zur Integritätssicherung sowie Logs aller durchgeführten Transaktionen. Sämtliche Aufgaben werden auf beiden Infrastrukturvarianten ausgeführt, der PKI und der KSI. Insbesondere Letztere ist auf den möglichen Einsatz der *Guardtime*-Blockchain-Technologie zurückzuführen (siehe *Abbildung 7-22*)

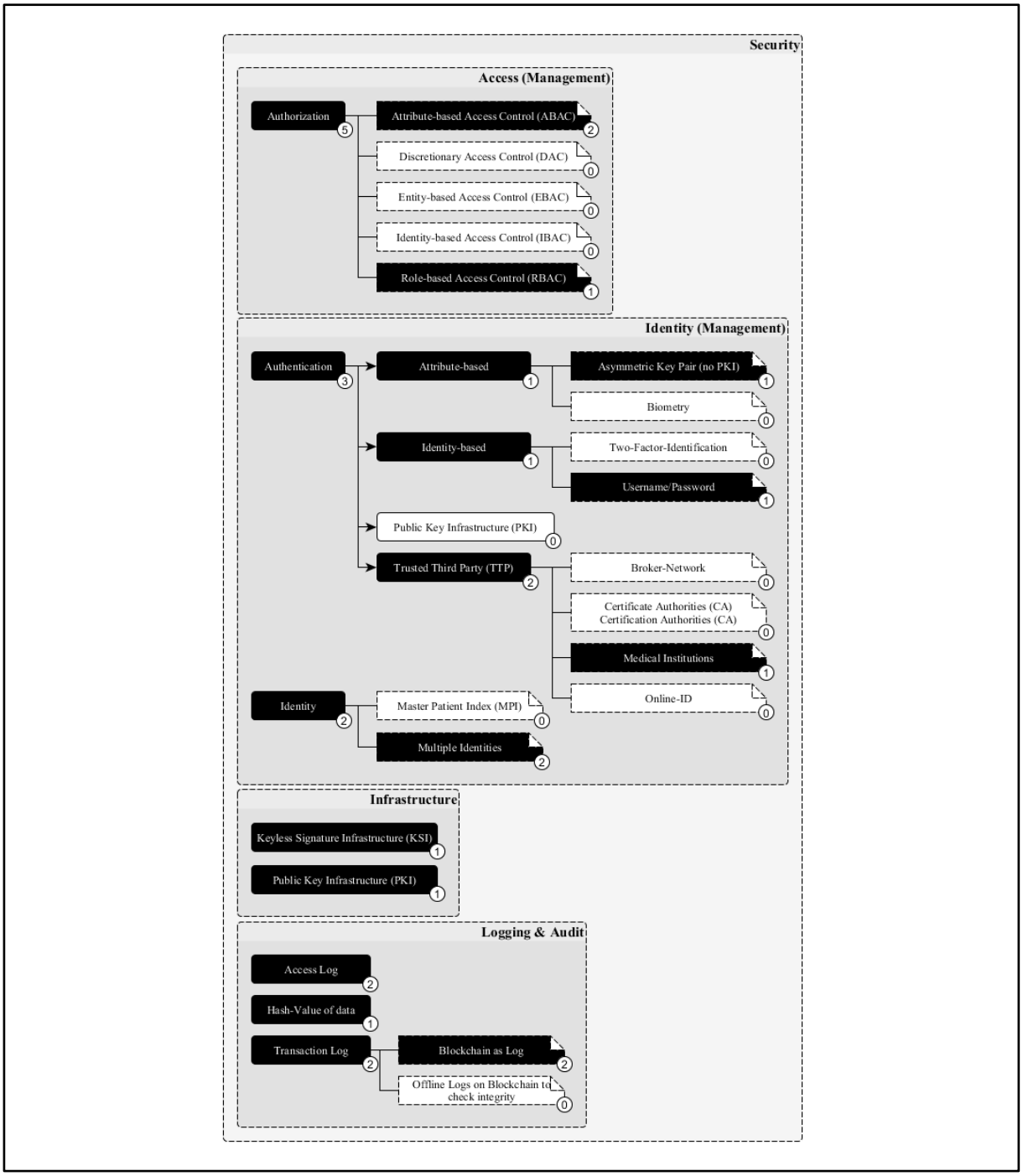


Abbildung 7-21: EHR-Variationen in der Sicht ‚Security' ohne Filterung (Quelle: Eigene Darstellung)

Bei der Wahl von Variationspunkten in der Sicht **Technology** liegt der Fokus erneut auf dem Betrieb einer einzelnen Blockchain (siehe *Abbildung 7-22*). Ausgehend von der dann folgenden Blockchain-Klassifikation ergeben sich als konkrete Technologien *Ethereum*, *GuardTime* und *MultiChain*. Sie können dabei Smart Contracts zur Verwaltung von *Identitäten* und *Beziehungen* sowie zur *Zusammenfassung* bestehender Daten ausführen. Die einzigen hier genannten Consens-Algorithmen sind *Practical Byzantine Fault Tolerant*, *Proof-of-Stake* und *Proof-of-Work*.

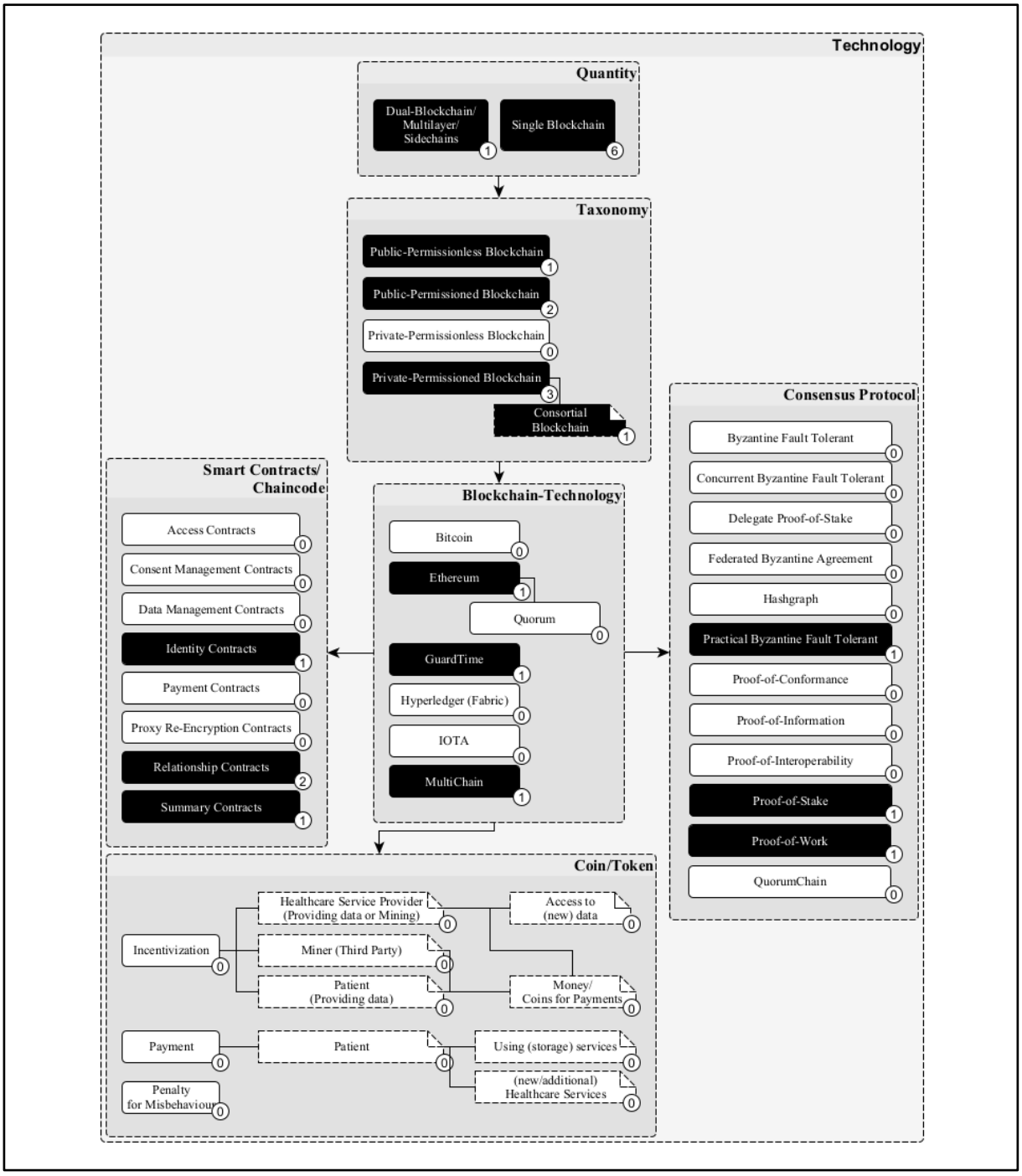


Abbildung 7-22: EHR-Variationen in der Sicht ‚Technology' ohne Filterung (Quelle: Eigene Darstellung)

Auch hier können weitere Filter für eine genaue Entscheidungsfindung verwendet werden, die sich auf die Blockchain-Taxonomie oder -Technologie beschränken.[638] In einem ersten Schritt wird der Filter auf die *Taxonomy* gesetzt:

638 Diese Erkenntnisse lassen sich aufgrund der geringen Datenbasis nur bedingt auf die Realität übertragen. Aus diesem Grund ist die Gesamtsicht entsprechend *Abbildung 7-22* grundsätzlich aussagekräftiger.

i. Public-Permissionless (siehe *Abbildung 7-23*)

ii. Public-Permissioned (siehe *Abbildung 7-24*)

iii. Private-Permissioned (siehe *Abbildung 7-25*)

iv. Consortial (siehe *Abbildung 7-26*)

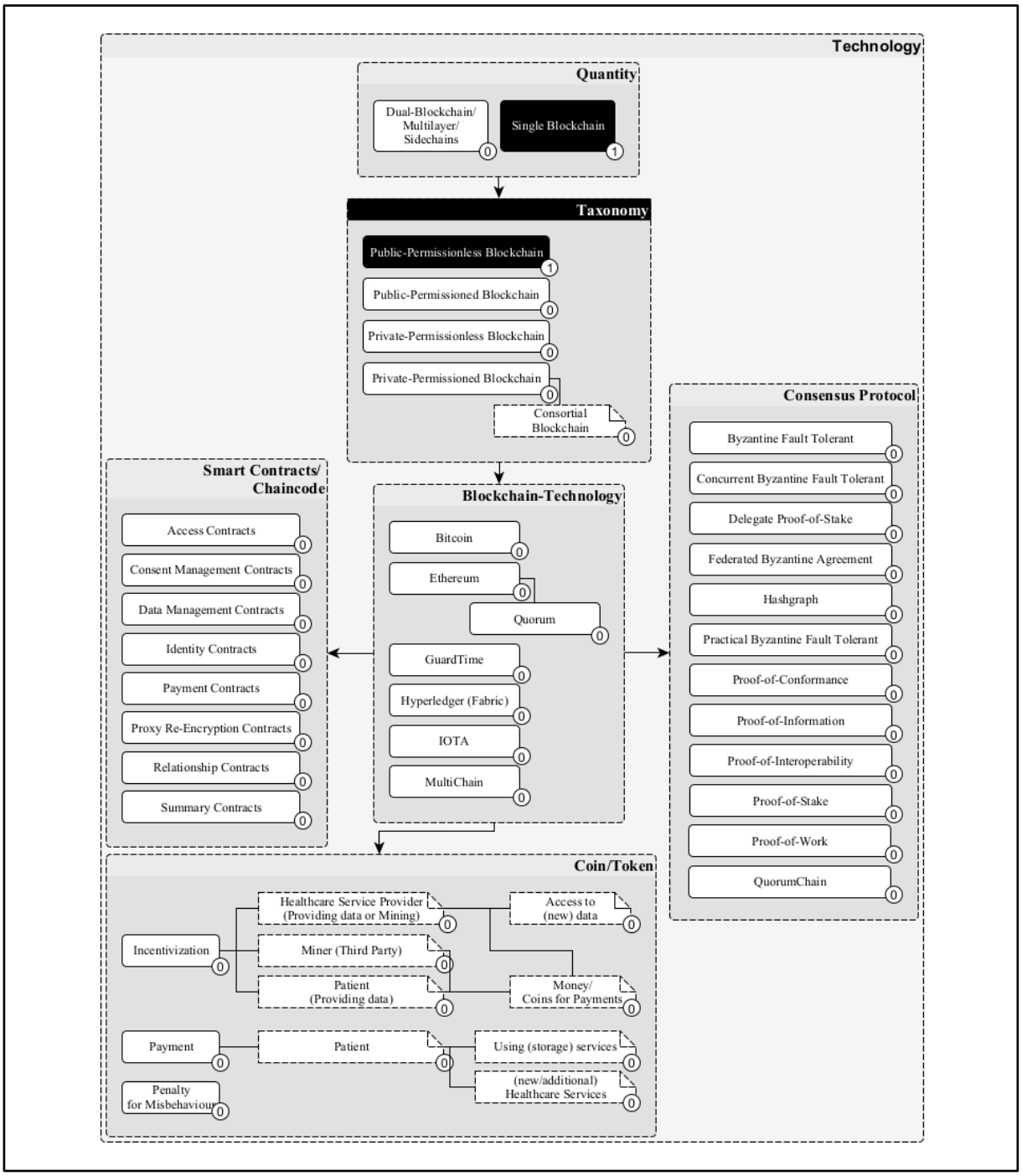


Abbildung 7-23: EHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Public-Permissionless Blockchain'
(Quelle: Eigene Darstellung)

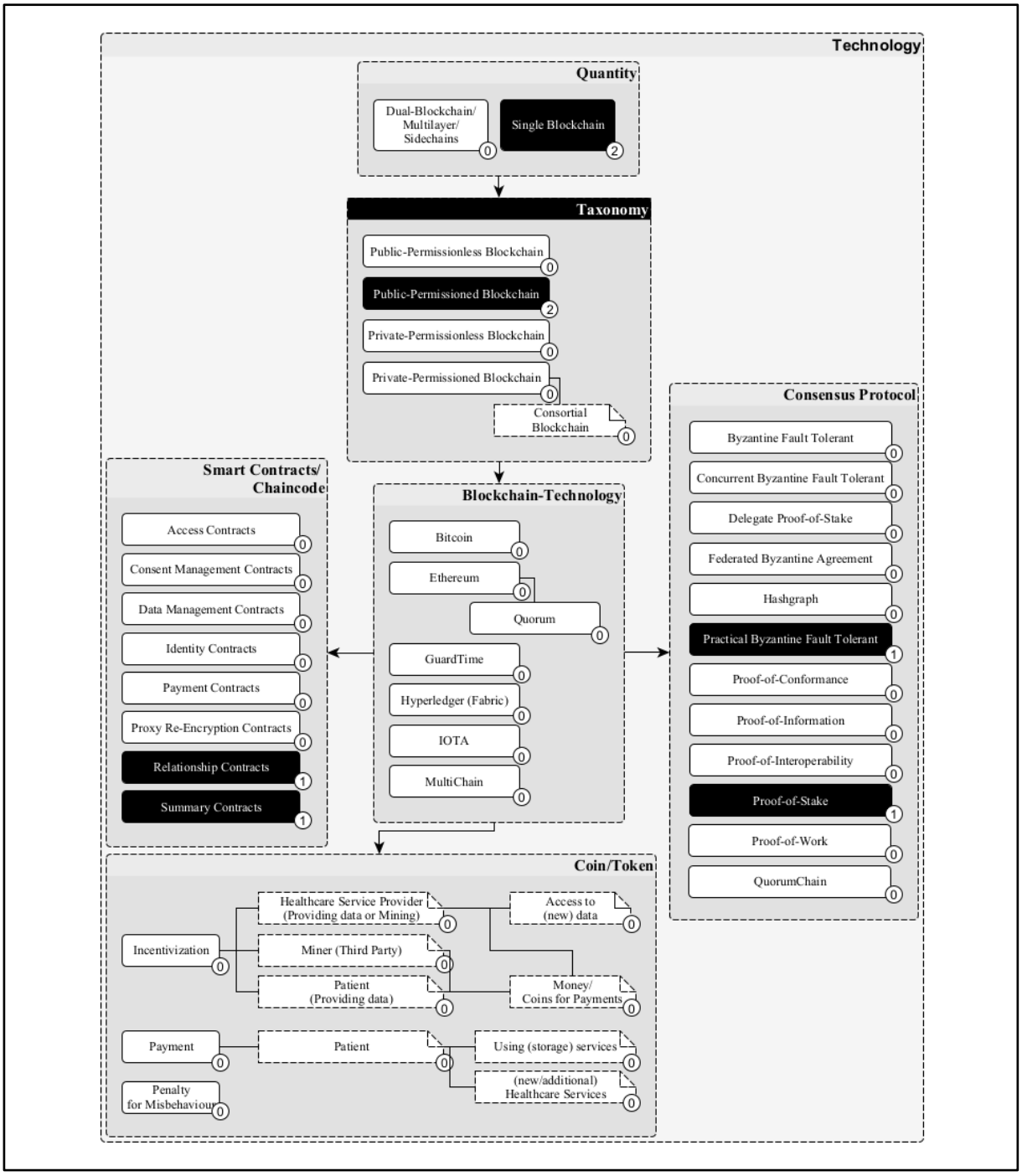


Abbildung 7-24: EHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Public-Permissioned Blockchain'
(Quelle: Eigene Darstellung)

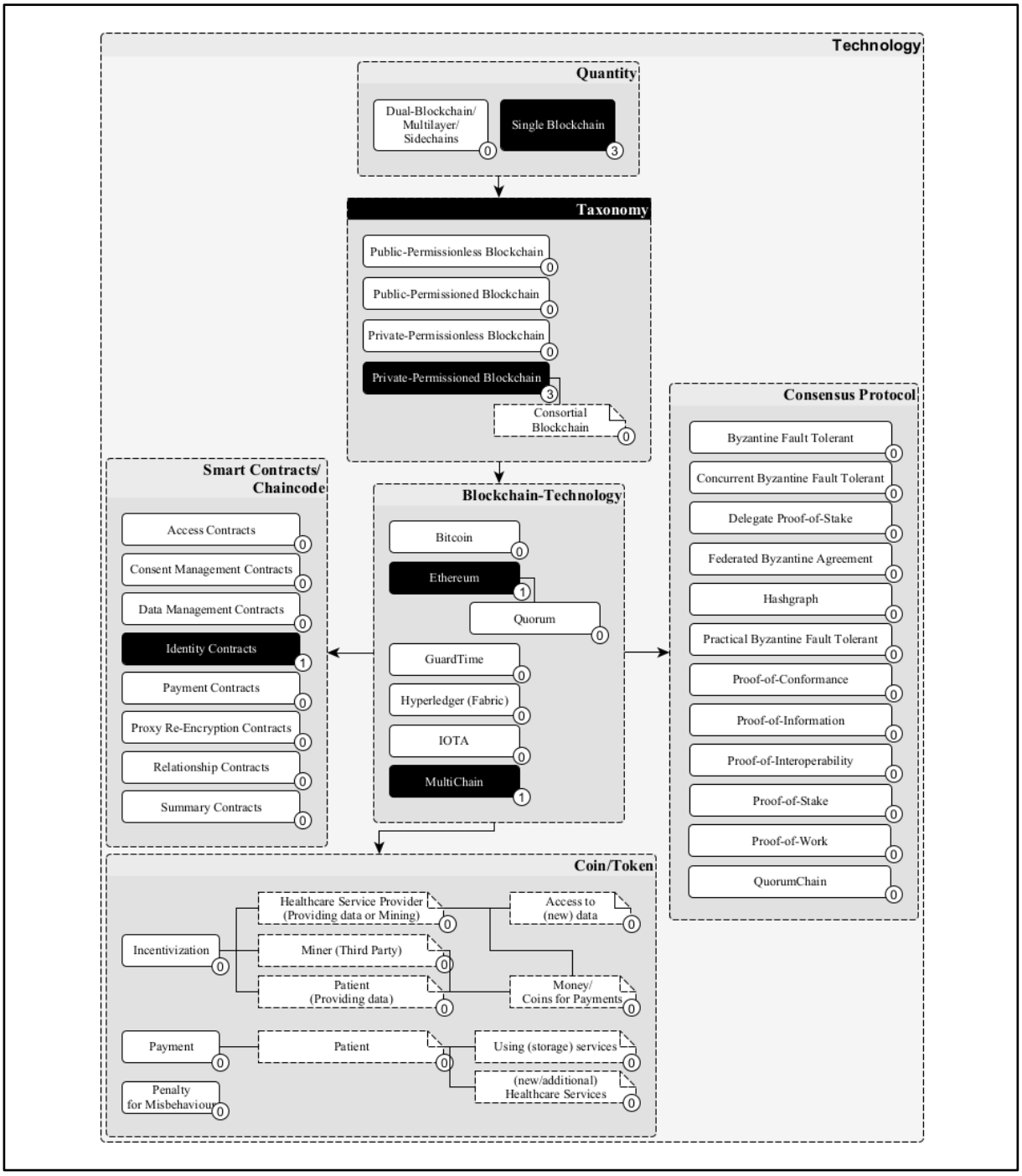


Abbildung 7-25: EHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Private-Permissioned Blockchain'
(Quelle: Eigene Darstellung)

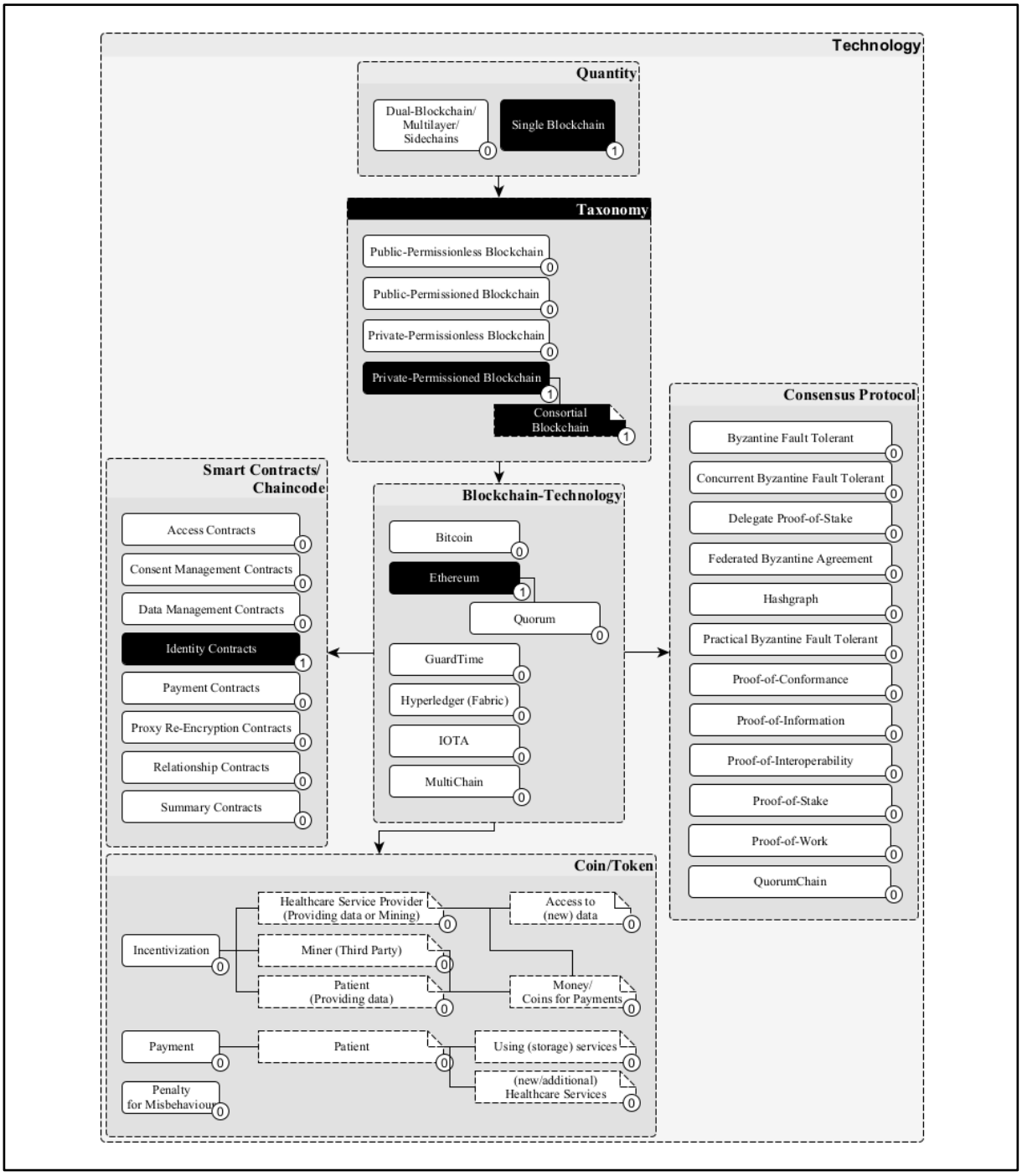


Abbildung 7-26: EHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Consortial Blockchain' (Quelle: Eigene Darstellung)

Ein weiterer Ansatz ist die Fokussierung auf die Blockchain-Technologie statt auf Taxonomie. Hier ergeben sich die folgenden möglichen Ausprägungen und *Abbildung*en:

i. Ethereum (siehe *Abbildung 7-27*)

ii. Guardtime (siehe *Abbildung 7-28*)

iii. MultiChain (siehe *Abbildung 7-29*)

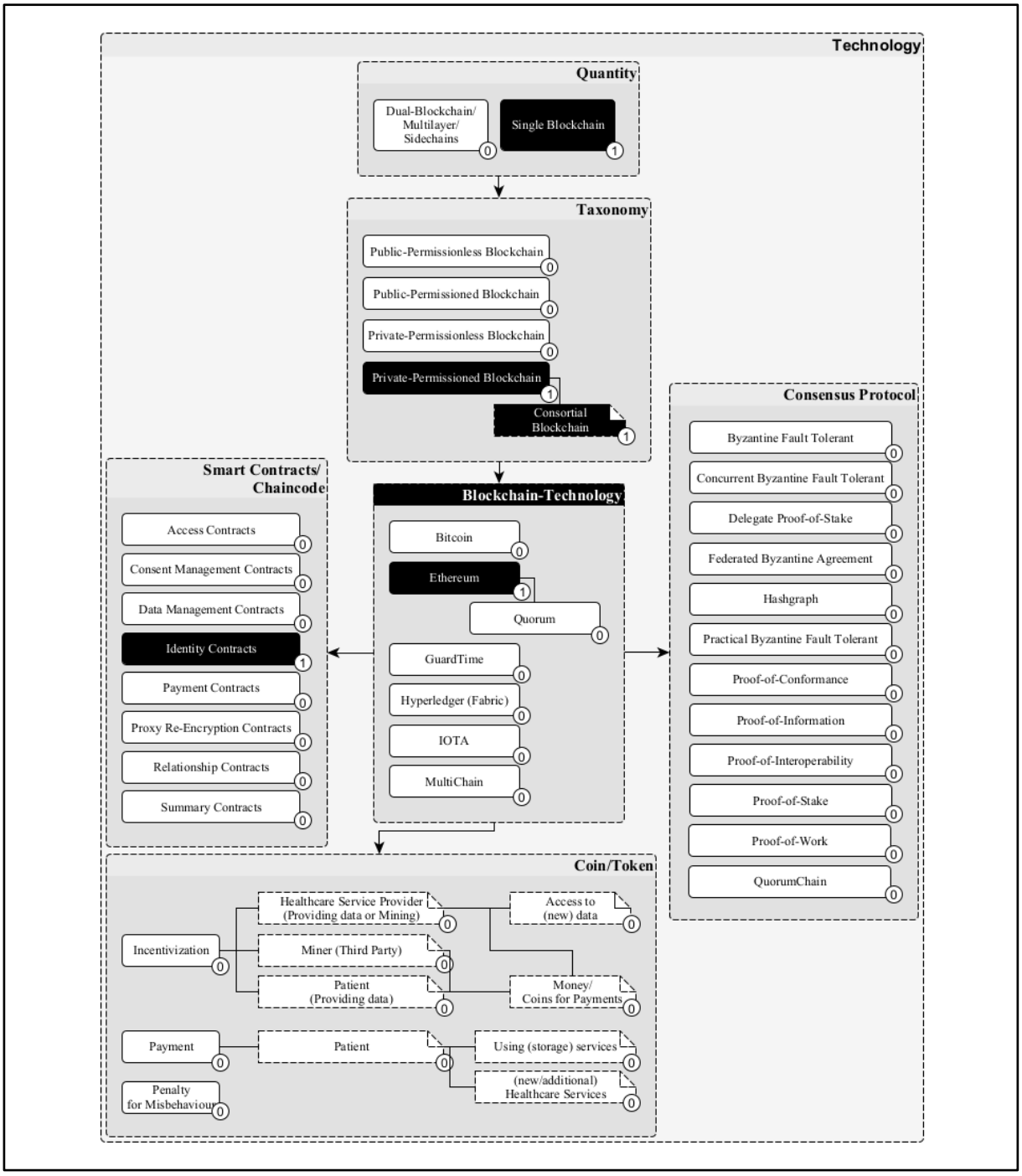


Abbildung 7-27: EHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Ethereum' (Quelle: Eigene Darstellung)

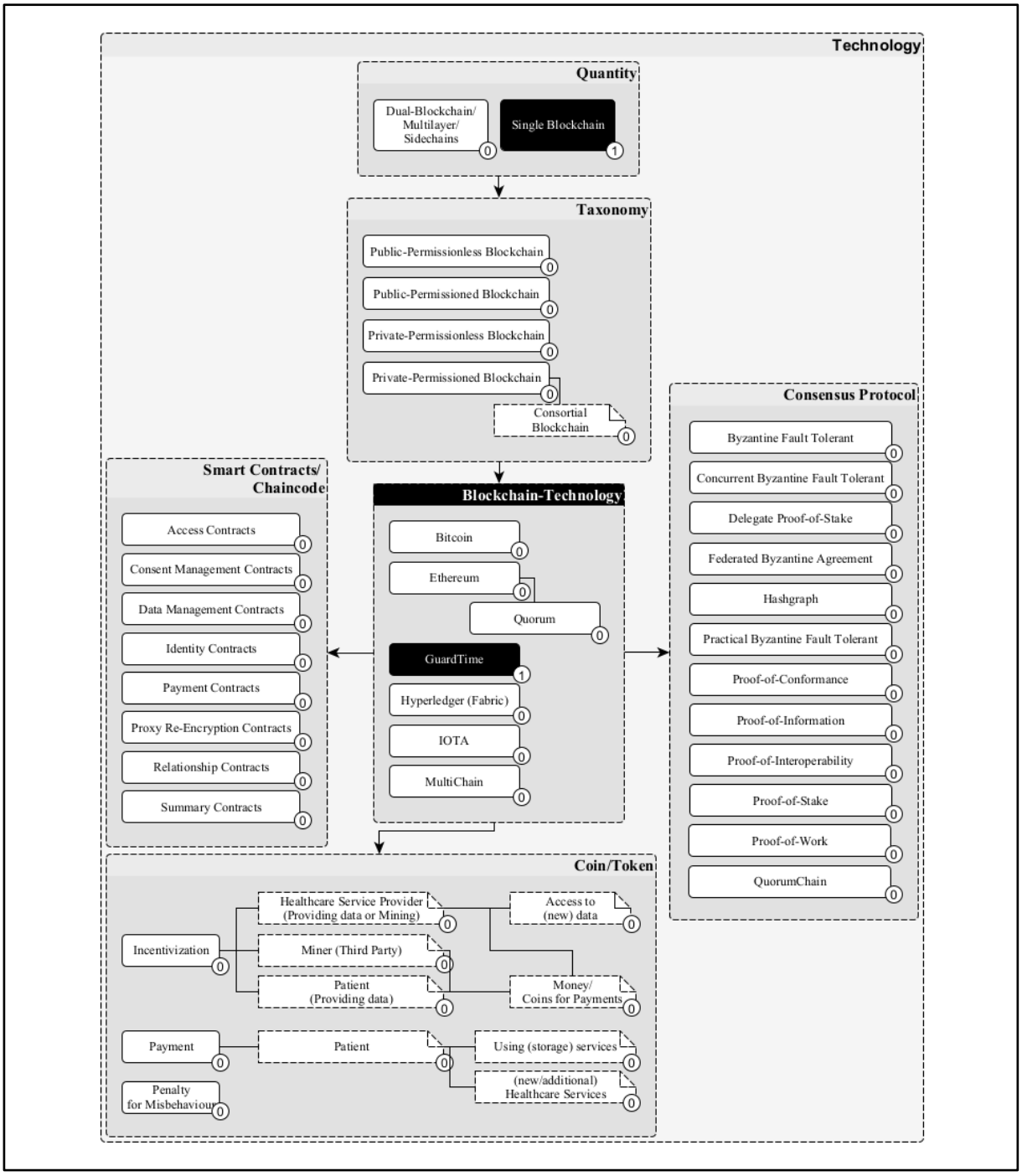


Abbildung 7-28: EHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚GuardTime' (Quelle: Eigene Darstellung)

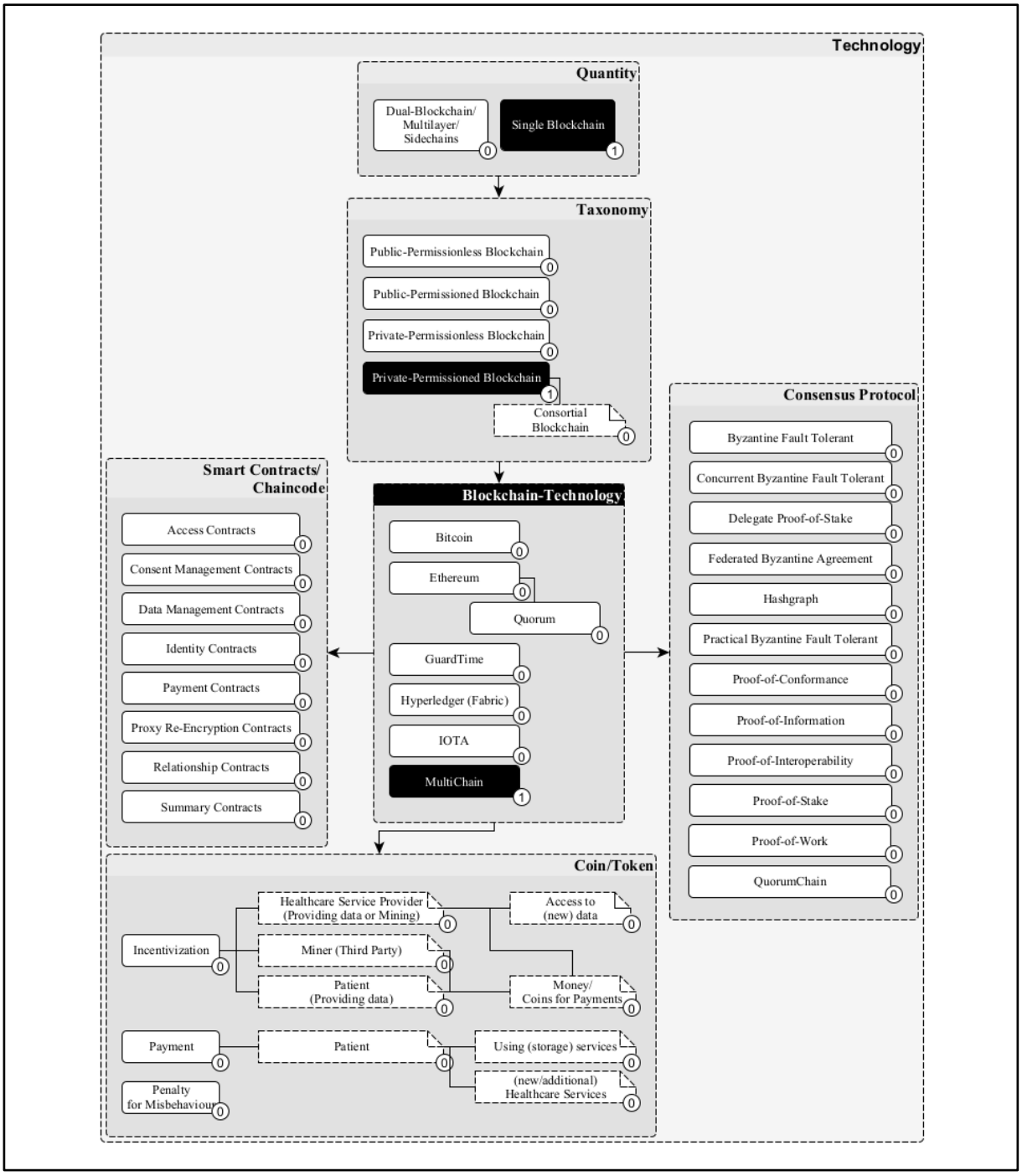


Abbildung 7-29: EHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚MultiChain' (Quelle: Eigene Darstellung)

7.2.3 Insurance and other payers

Der Betrachtung der Kostenträger sind keine umfangreichen Erkenntnisse oder eindeutigen Abhängigkeiten für eine Entscheidungsmodellierung zu entnehmen. In der Sicht der **Data Storage & Provisioning** wird nur die on-chain-Datenhaltung und die Verwendung von Cloud-Speichern betrachtet (siehe *Abbildung 7-30*). Zwischen beiden wird unter Einbezug der Literatur kein direkter Zusammenhang identifiziert (siehe *Abbildung 7-31*).

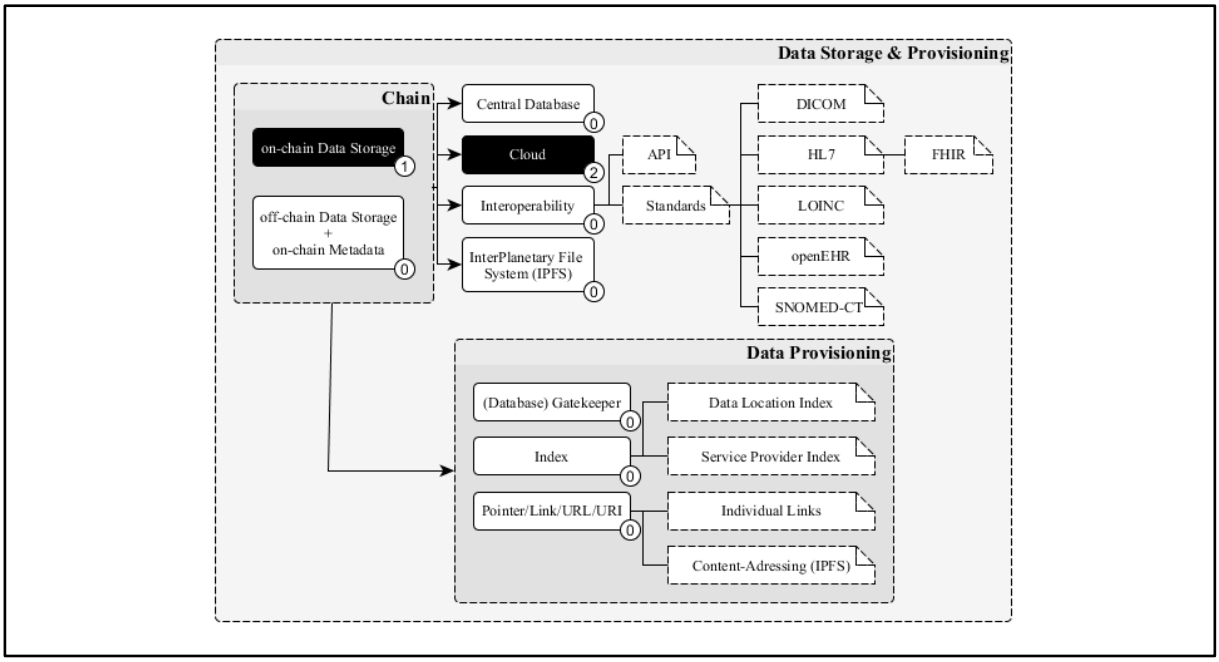


Abbildung 7-30: Insurance-Variationen in der Sicht ‚Data Storage & Provisioning' ohne Filterung (Quelle: Eigene Darstellung)

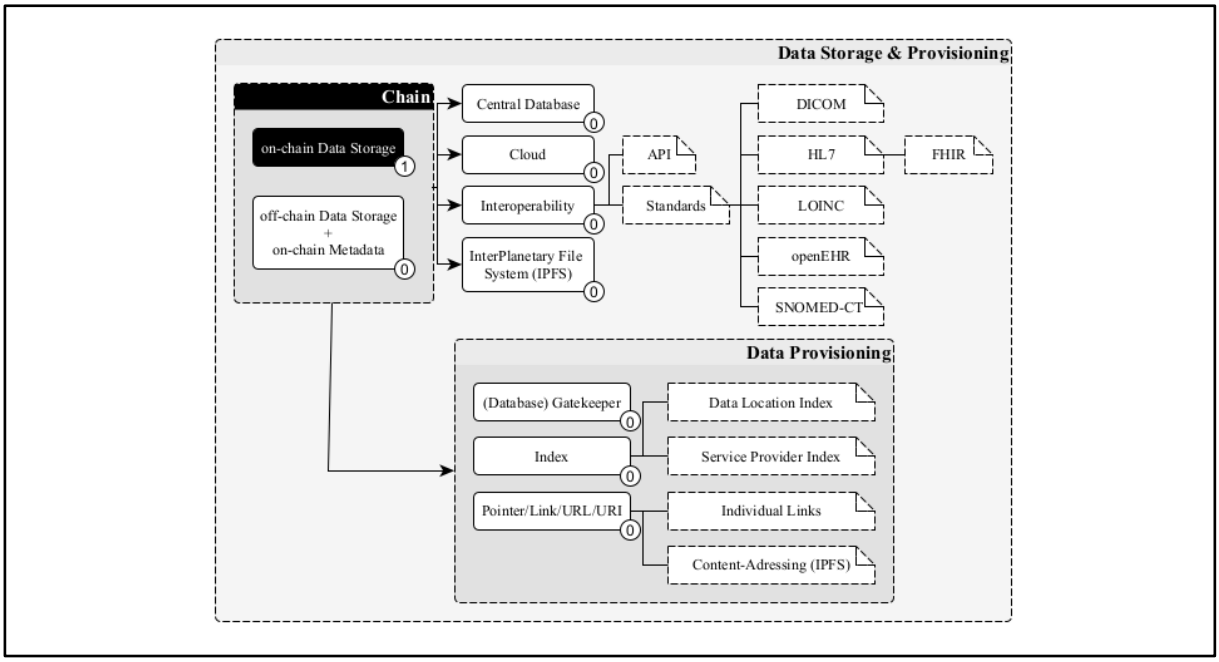


Abbildung 7-31: Insurance-Variationen in der Sicht ‚Data Storage & Provisioning' mit Filterung auf ‚on-chain Data Storage' (Quelle: Eigene Darstellung)

Die Sicht **Security** beschränkt sich auf den Einsatz einer PKI und der damit verbundenen Authentifizierung unter Zuhilfenahme einer TTP, genauer CAs (siehe *Abbildung 7-32*). Weitere Ableitungen sind aus der Literatur nicht zu ermitteln.

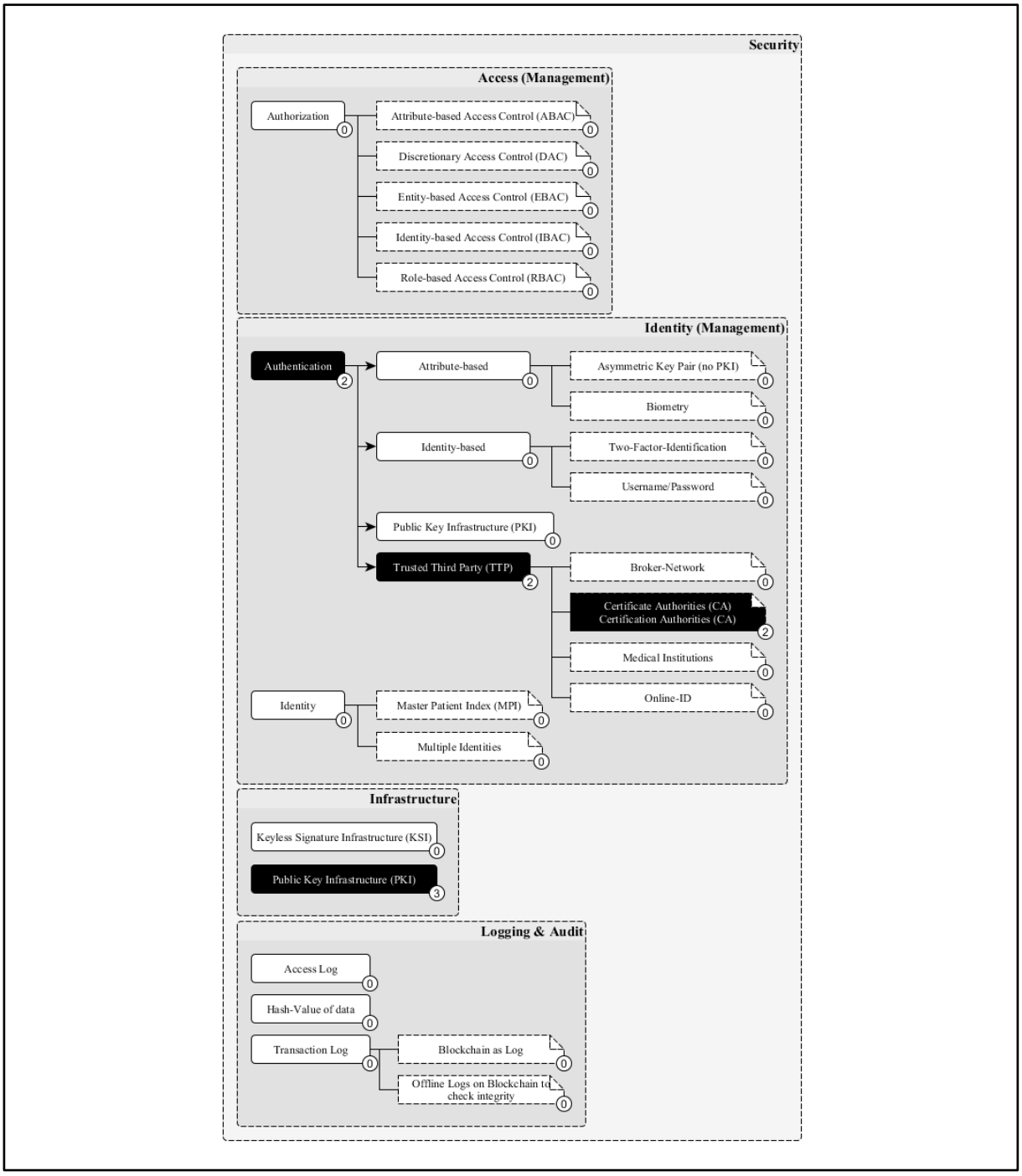


Abbildung 7-32: Insurance-Variationen in der Sicht ‚Security' ohne Filterung (Quelle: Eigene Darstellung)

In der Auswahl der **Technology** finden sich mehr Ausprägungen und Variationspunkte als in den genannten Sichten (siehe *Abbildung 7-33*). So ist festzuhalten, dass ausschließlich Single-Blockchains genutzt werden und sich die Technologieauswahl auf Ethereum und Hyperledger beschränkt. Automatisierungen durch Smart Contracts betreffen Zugriffskontrollen oder die Ausführung von Zahlungsvorgängen. Letztere beschränken sich auf die Validierung von Leis-

tungen und der daraus resultierenden Auslösung von Zahlungen über ein extern geführtes Buchhaltungssystem der Kostenträger. Ein Token bzw. Coin wird nicht zur Finanzierung der Blockchain, sondern zur Bestrafung von Fehlverhalten genutzt.

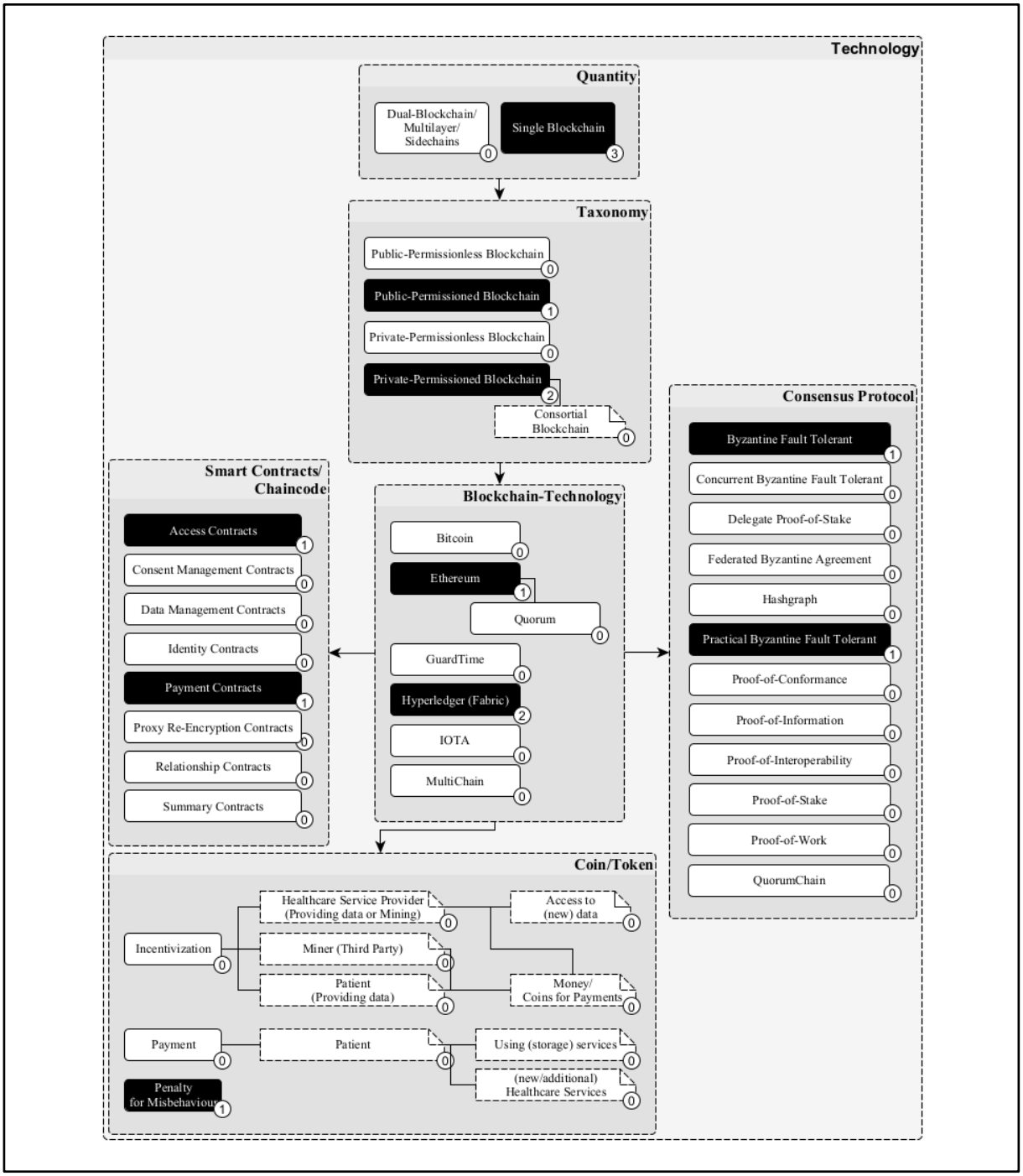


Abbildung 7-33: Insurance-Variationen in der Sicht ‚Technology' ohne Filterung (Quelle: Eigene Darstellung)

Diese Erkenntnisse können erneut durch die bereits genutzten Filterlogik weiter heruntergebrochen werden.[639] In einem ersten Schritt wird der Filter auf die *Taxonomy* gesetzt:

i. Public-Permissioned (siehe *Abbildung 7-34*)

ii. Private-Permissioned (siehe *Abbildung 7-35)*

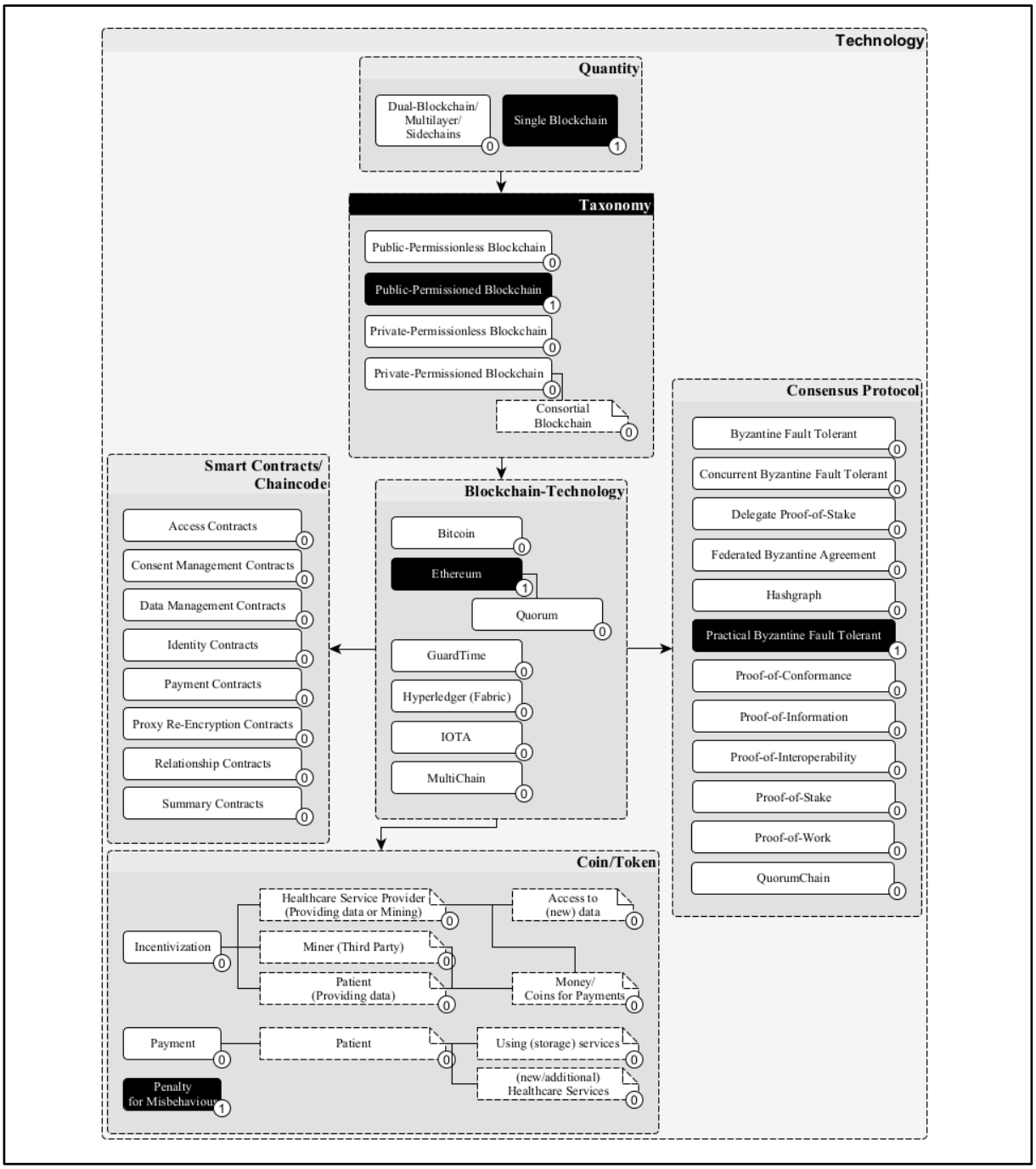


Abbildung 7-34: Insurance-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Public-Permissioned Blockchain'
(Quelle: Eigene Darstellung)

639 Durch die geringe Datenbasis sind die Erkenntnisse durch Anwendung der Filterlogik nur bedingt auf die Realität überführbar. Aus diesem Grund ist die Gesamtsicht entsprechend *Abbildung 7-22* aussagekräftiger.

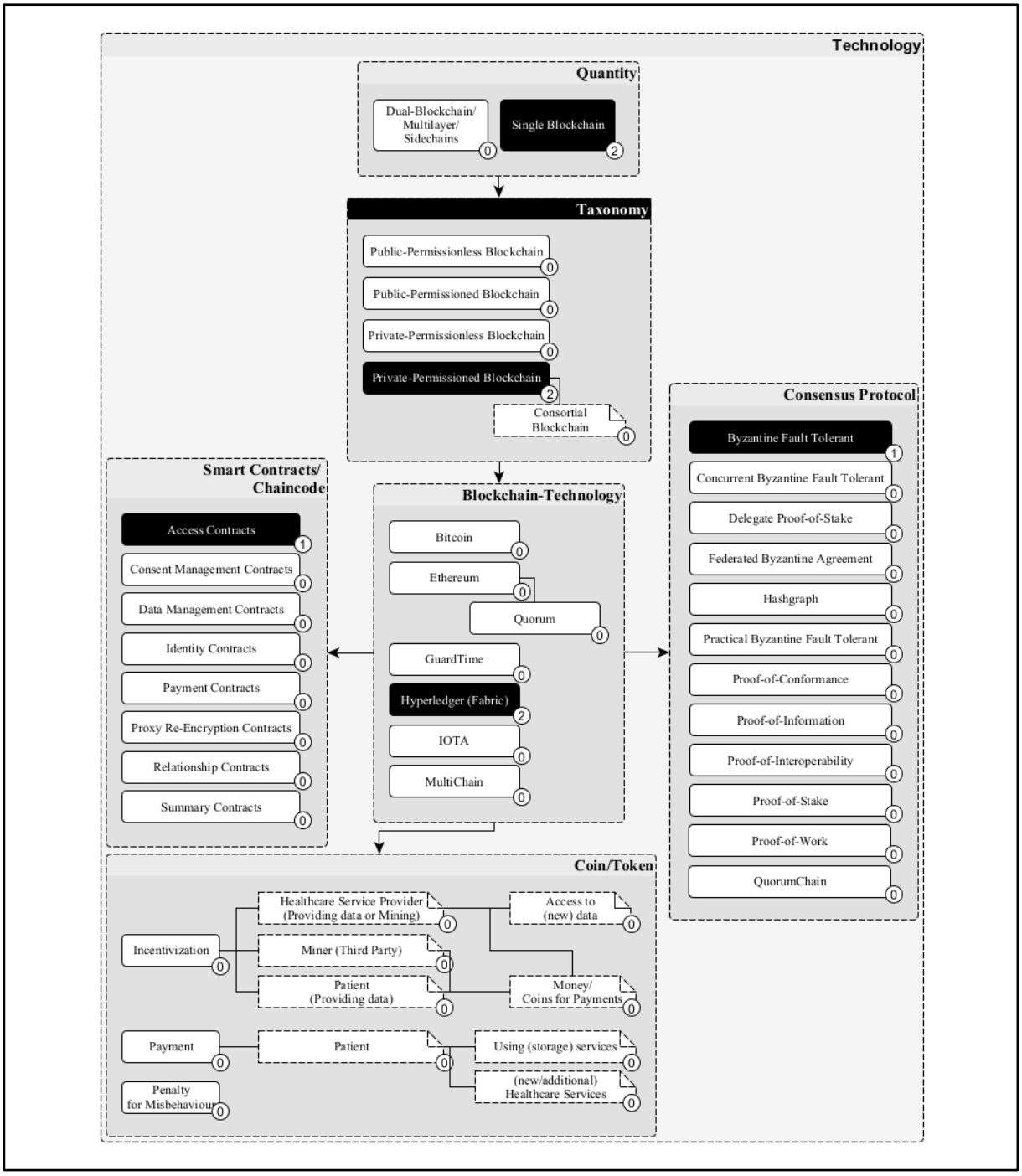


Abbildung 7-35: Insurance-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Private-Permissioned Blockchain'
(Quelle: Eigene Darstellung)

Ein weiterer Ansatz ist die Fokussierung auf die Blockchain-Technologie statt ihrer Taxonomie. Hier ergeben sich die folgenden möglichen Ausprägungen:

i. Ethereum (siehe *Abbildung 7-36*)

ii. Hyperledger (Fabric) (siehe *Abbildung 7-37*)

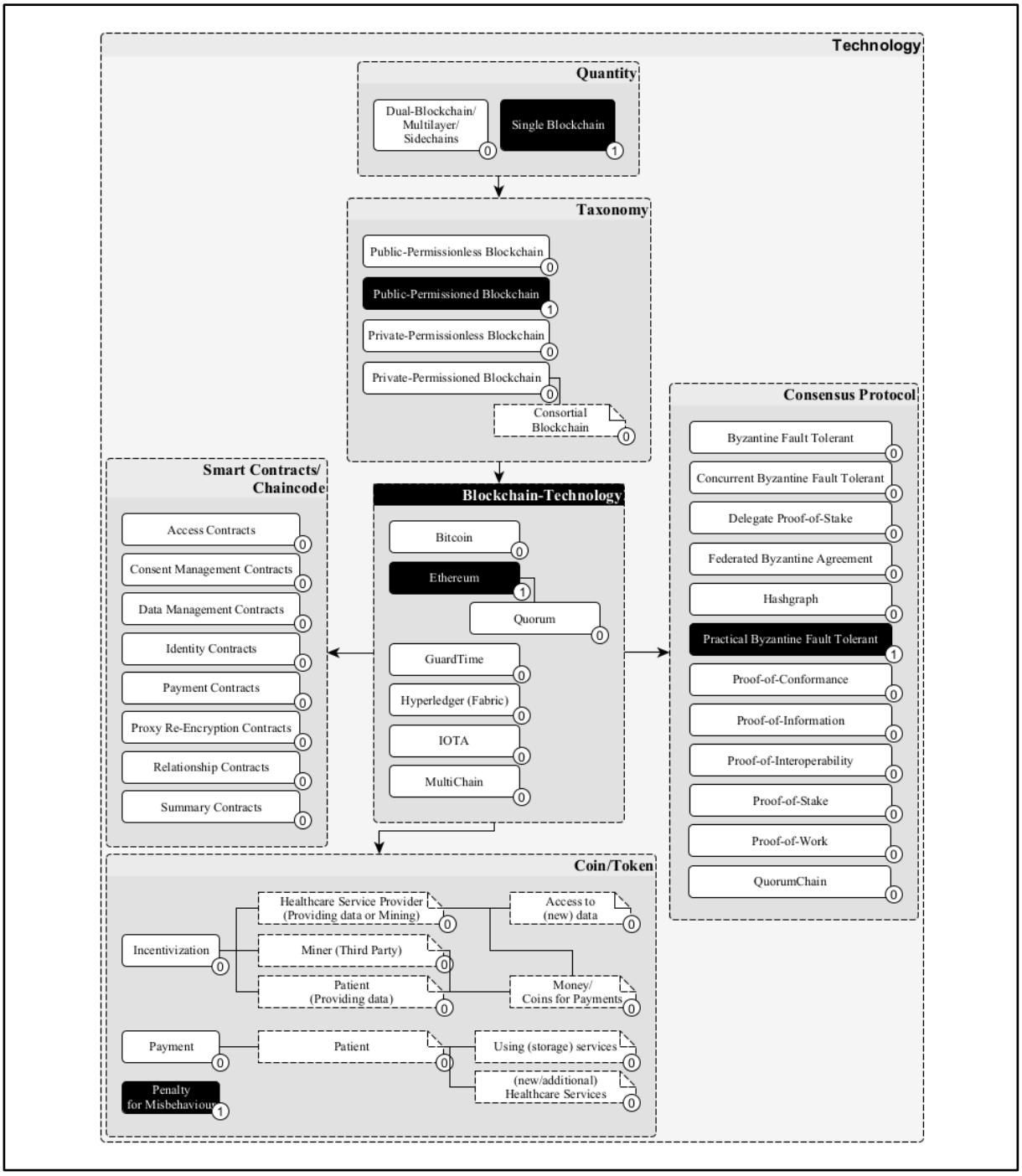


Abbildung 7-36: Insurance-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Ethereum' (Quelle: Eigene Darstellung)

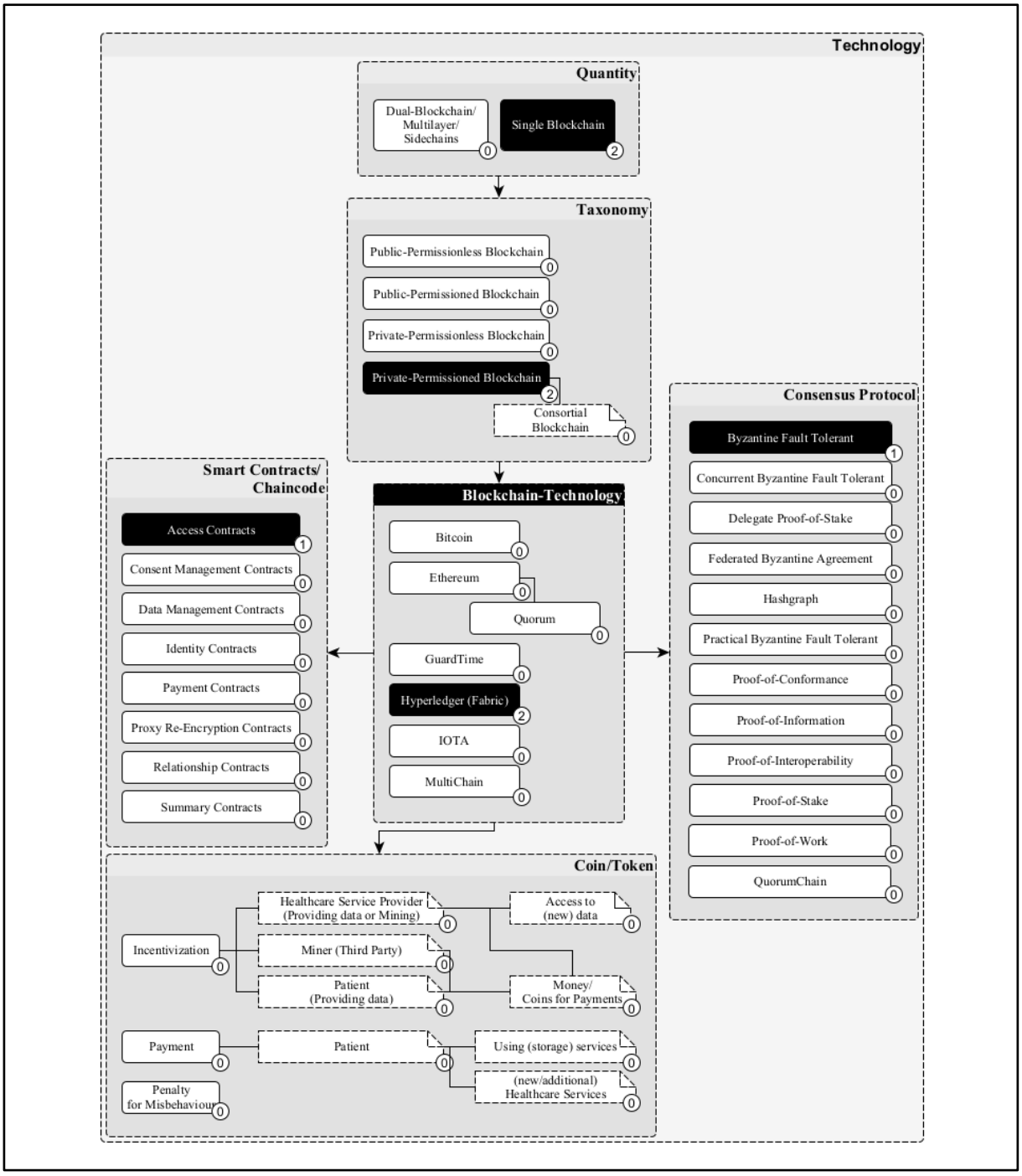


Abbildung 7-37: Insurance-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Hyperledger' (Quelle: Eigene Darstellung)

7.2.4 Patient Summary

Für diesen Record Type ergeben sich keine Erkenntnisse in der Sicht **Data Storage & Provisioning**, da diese in keiner Publikation dediziert behandelt wird (siehe *Abbildung 7-38*).

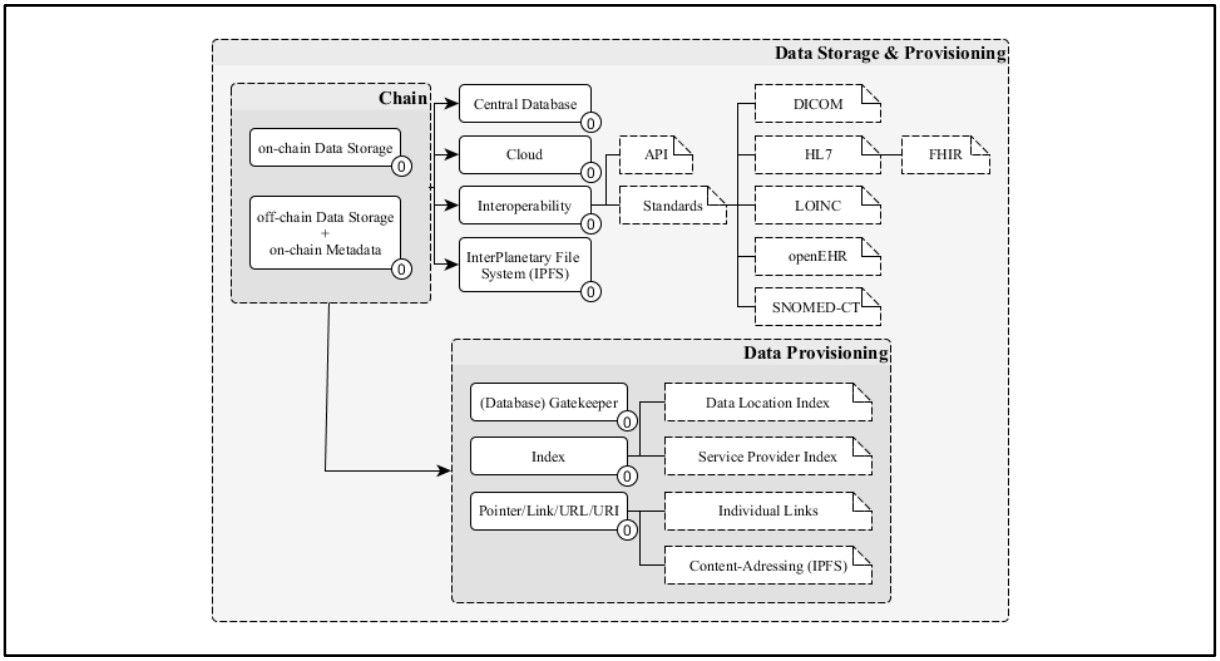


Abbildung 7-38: Patient-Summary-Variationen in der Sicht ‚Data Storage & Provisioning' ohne Filterung (Quelle: Eigene Darstellung)

Die Sicht **Security** ähnelt im Aufbau der Security-Sicht für Kostenträger[640] aufgebaut. Der Fokus liegt auf PKI und den damit verbundenen Einsatz von CAs. Die Blockchain hat einen unterstützenden Charakter und dient insbesondere als Log sämtlicher im Netzwerk durchgeführter Transaktionen (siehe *Abbildung 7-39*).

640 Siehe *Kapitel 7.2.3*.

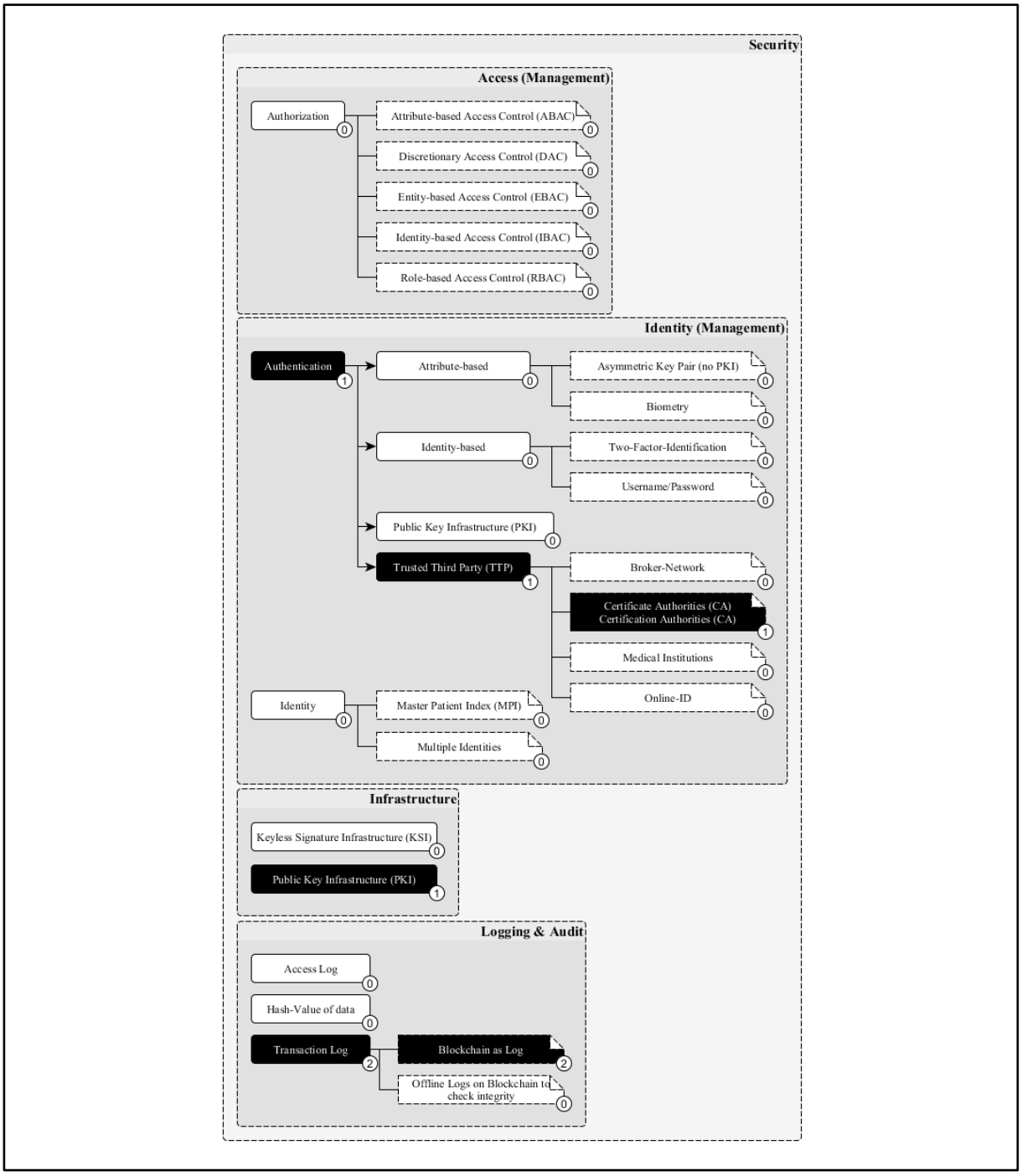


Abbildung 7-39: Patient-Summary-Variationen in der Sicht ‚Security' ohne Filterung (Quelle: Eigene Darstellung)

Auch die Sicht **Technology** beschränkt sich auf den Betrieb einer einzigen Blockchain, genauer einer Private-Permissioned Blockchain, die die MultiChain-Technologie verwendet (siehe *Abbildung 7-40*). Weitere Variationen finden sich nicht in der Literatur. Auch wird hier aufgrund der mangelnden Variationen auf eine separierte Betrachtung von *Taxonomy* bzw. *Technology*, wie in den vorangegangenen Kapiteln durchgeführt, verzichtet.

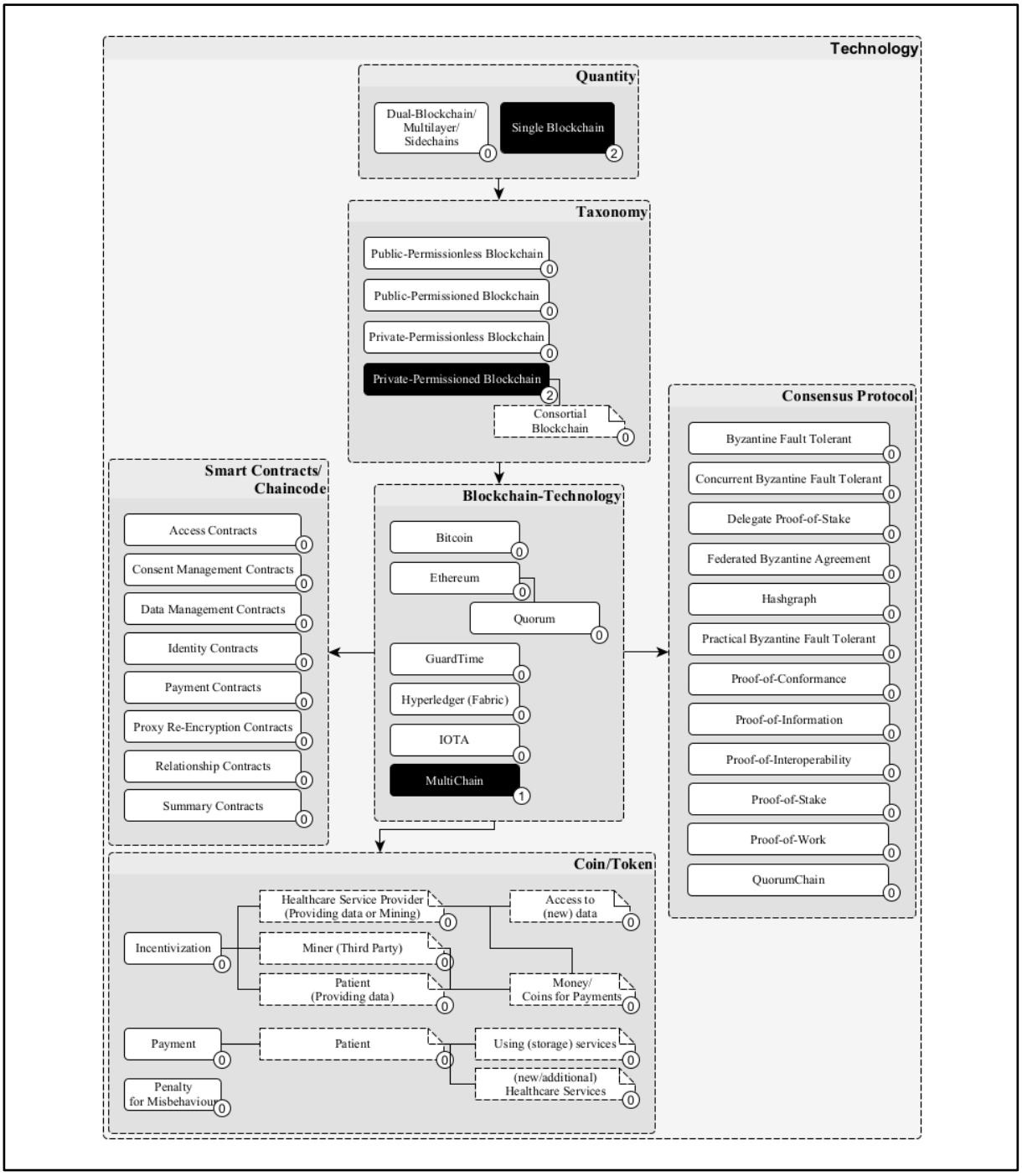


Abbildung 7-40: Patient-Summary-Variationen in der Sicht ‚Technology' ohne Filterung (Quelle: Eigene Darstellung)

7.2.5 Patient Health Records

Im Rahmen der PHR werden sämtliche Variationen der Sicht **Data Storage & Provisioning** in der Literatur besprochen. Der Schwerpunkt liegt hier auf der Speicherung von Gesundheitsdaten abseits der Blockchain (off-chain). Das Thema Cloud wird in diesem Zusammenhang intensiver diskutiert als IPFS (siehe *Abbildung 7-41*). Auch das Thema Interoperabilität wird umfangreich besprochen, da PHR ein hohes Maß an Kooperation verlangen und eine Blockchain diese forciert. Die Datenbereitstellung findet aufgrund der off-chain-Datenspeicherung mittels auf der Blockchain gespeicherter *Links* bzw. *Pointer* statt. Die Bereitstellung von Daten wird wiederum von *Gatekeepern* kontrolliert.

Ausgehend von der Speichervariation *Chain* und konkret bezogen auf *off-chain-Datenspeicherung* (siehe *Abbildung 7-42*) sind die gleichen Schwerpunkte zu identifizieren. Unter Beschränkung auf reine *on-chain-Datenspeicherung* (siehe *Abbildung 7-43*) reduzieren sich die Gewichtung der potenziellen Variationen auf *Cloud* und die Anwendung von Standards zur Herstellung von Interoperabilität.

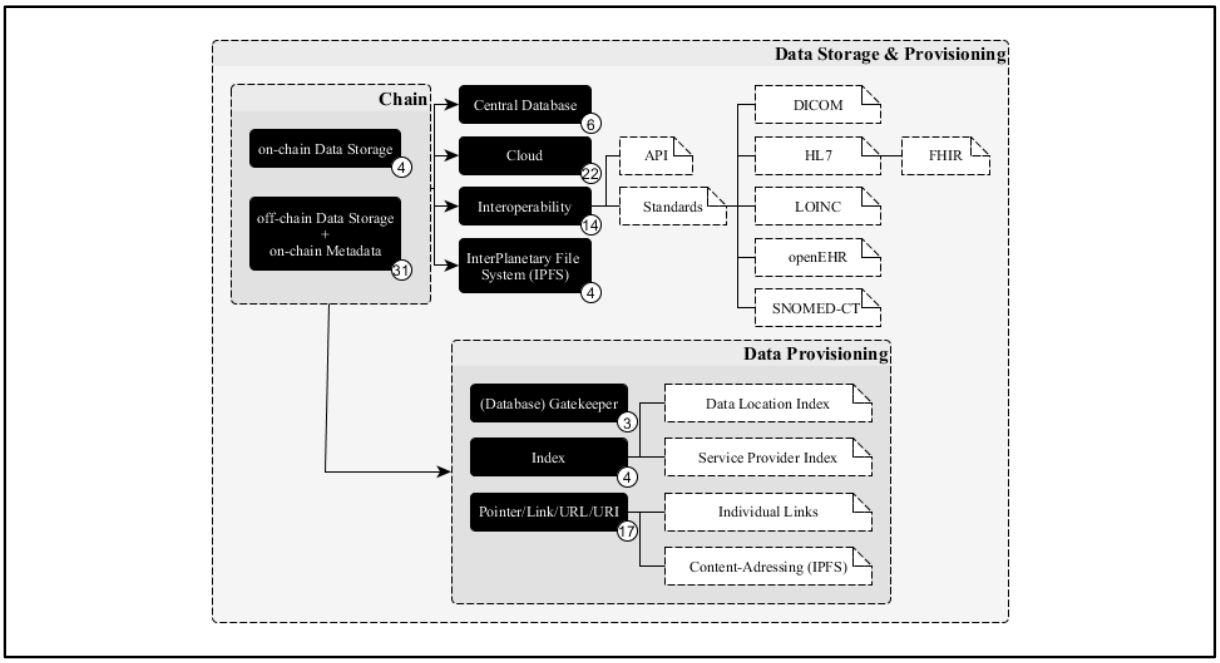


Abbildung 7-41: PHR-Variationen in der Sicht ‚Data Storage & Provisioning' ohne Filterung (Quelle: Eigene Darstellung)

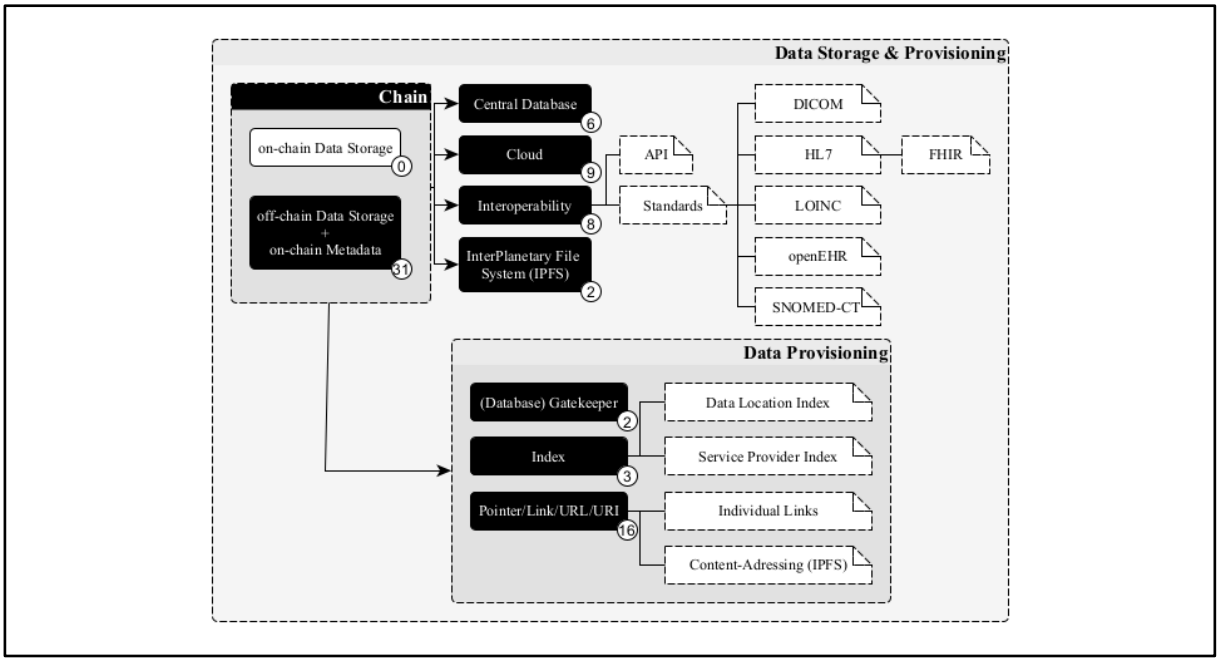


Abbildung 7-42: PHR-Variationen in der Sicht ‚Data Storage & Provisioning' mit Filterung auf ‚off-chain Data Storage'
(Quelle: Eigene Darstellung)

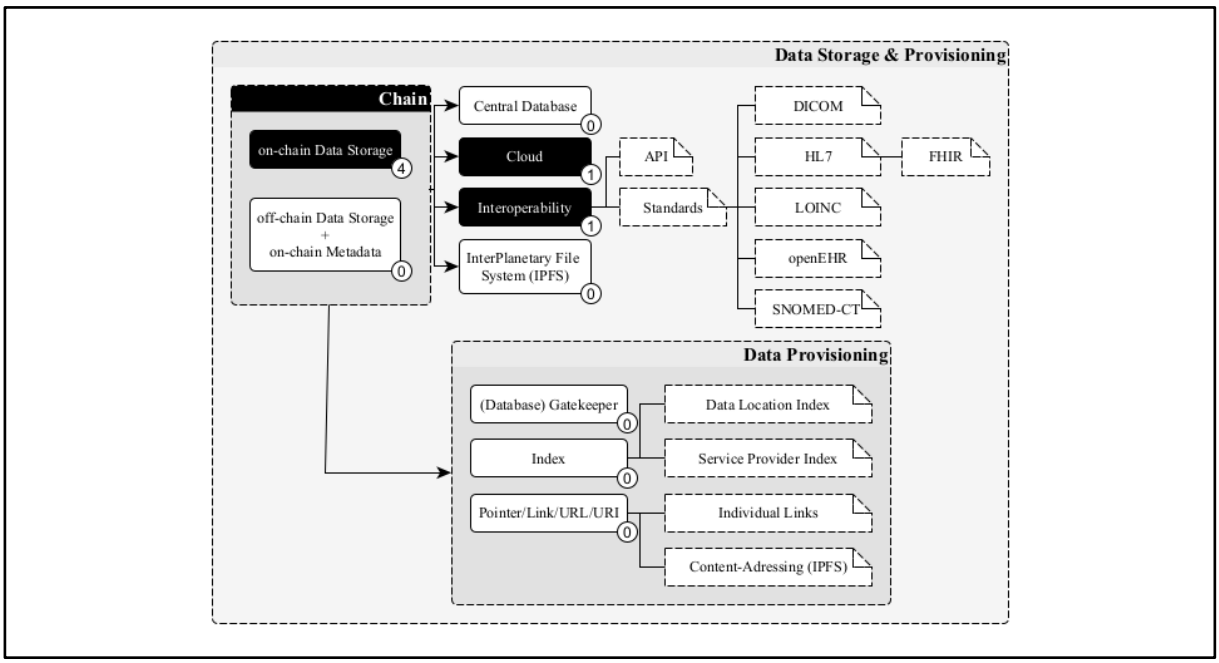


Abbildung 7-43: PHR-Variationen in der Sicht ‚Data Storage & Provisioning' mit Filterung auf ‚on-chain Data Storage'
(Quelle: Eigene Darstellung)

Variationen der Sicht **Security** werden für PHR annähernd vollständig bedient (siehe *Abbildung 7-44*). Zur Autorisierung der Nutzer wird der Fokus auf RBAC gelegt und EBAC nicht betrachtet. Im Rahmen der Authentifizierung werden attribut- und identitätsbasierte Authentifizierungsmechanismen genutzt, wobei die Zwei-Faktor-Identifikation ausgeschlossen bleibt.

TTPs werden in einem Großteil der Publikationen besprochen und zumeist CAs oder medizinische Einrichtungen zur Validierung der Identitäten genutzt. Infrastrukturell wird der Fokus auf PKI gesetzt und auf KSI verzichtet.

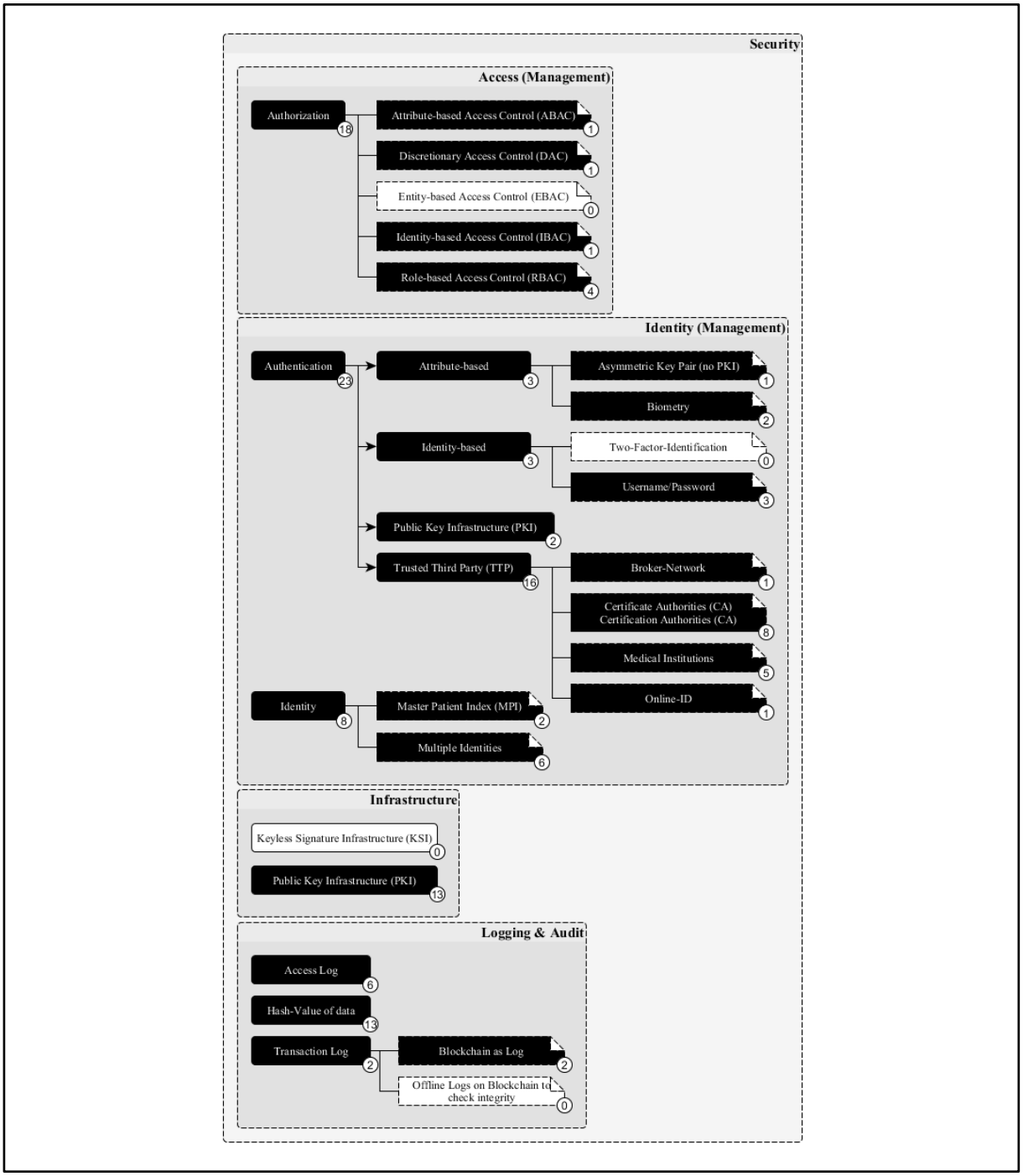


Abbildung 7-44: PHR-Variationen in der Sicht ‚Security' ohne Filterung (Quelle: Eigene Darstellung)

Die Sicht **Technology** umfasst ebenfalls einen Großteil der identifizierten Variationen. Ausgelassen werden in dieser Sicht einzig die Technologien *GuardTime*, *IOTA* und *MultiChain*. In den Konsensprotokollen wird auf *Proof-of-Information* verzichtet.

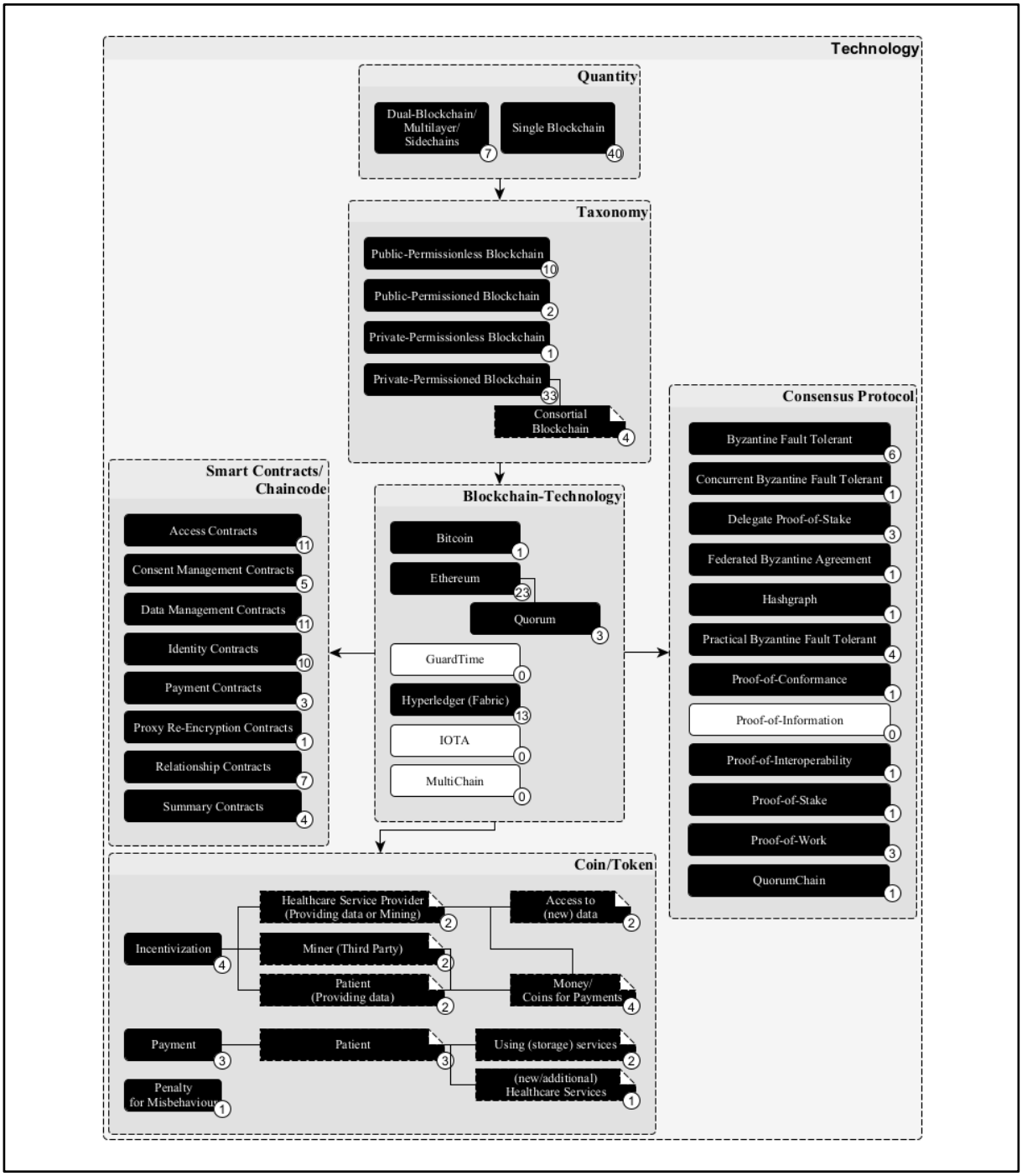


Abbildung 7-45: PHR-Variationen in der Sicht ‚Technology' ohne Filterung (Quelle: Eigene Darstellung)

Letztmalig werden für die weitere Differenzierung der Variationen Filter verwendet, die sich hier auf die Anzahl von Blockchains, die Blockchain-Taxonomie oder -Technologie beschränken. Die Ergebnisse dieser Filtereinsätze sind nur bedingt auf die Realität übertragbar, da einige

Publikationen Themen nur anreißen.[641] In einem ersten Schritt wird der Filter auf die Anzahl der Blockchains gesetzt:

i. Single Blockchain (siehe *Abbildung 7-46*)

ii. Dual-Blockchain/Multilayer/Sidechains (siehe *Abbildung 7-47*)

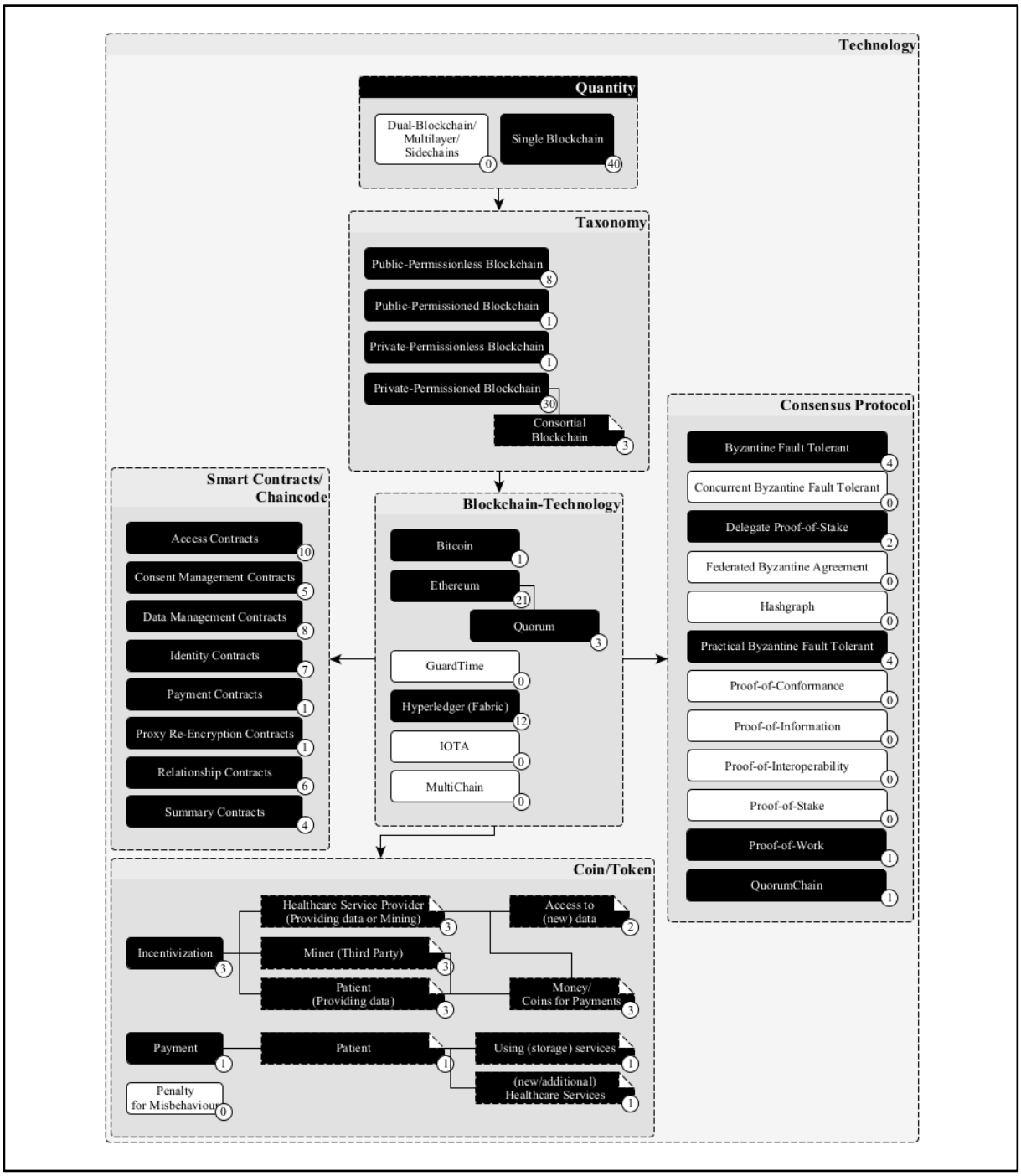


Abbildung 7-46: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Single Blockchain' (Quelle: Eigene Darstellung)

641 Aus diesem Grund ist die Gesamtsicht entsprechend *Abbildung 7-45* aussagekräftiger.

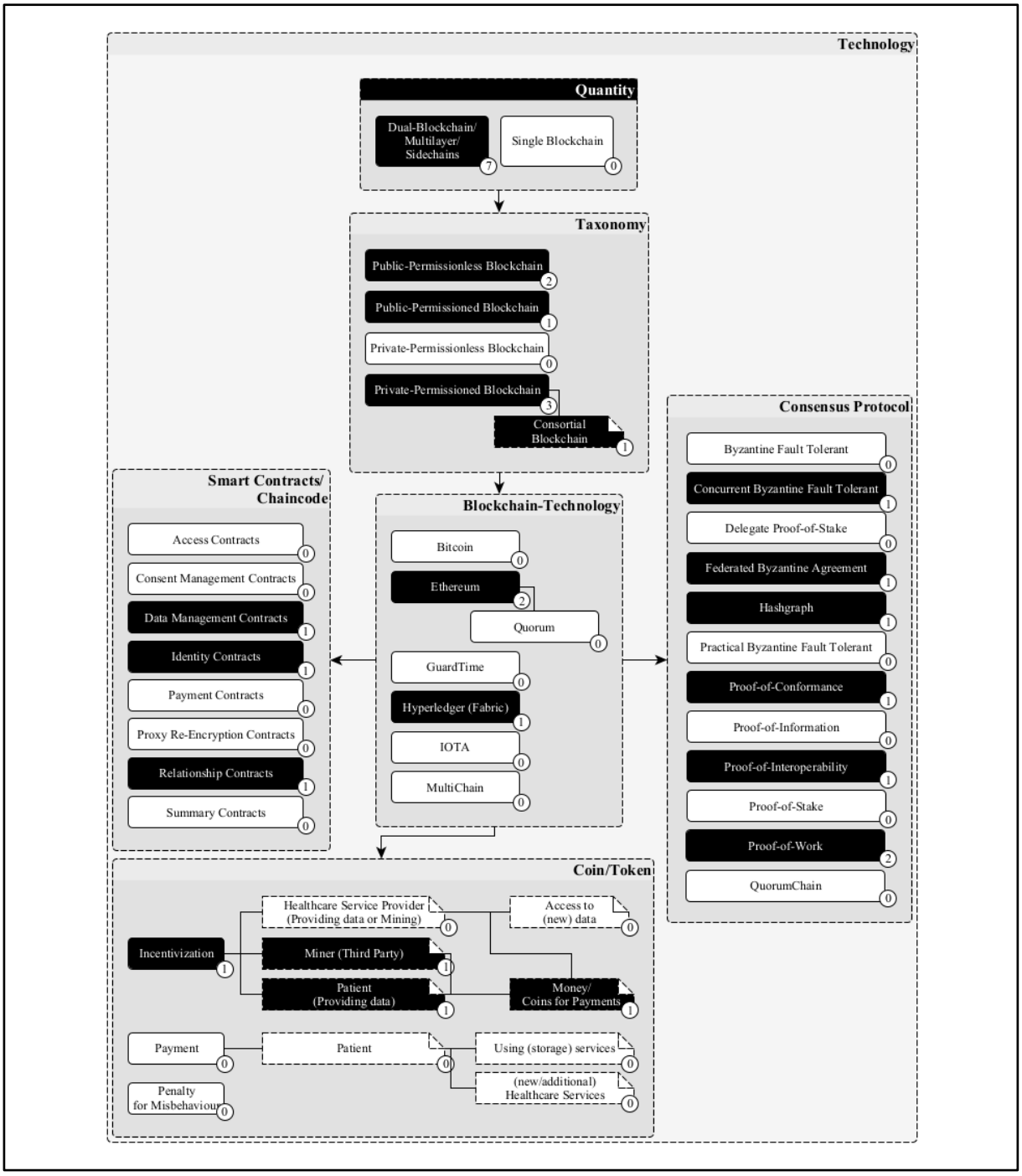


Abbildung 7-47: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Dual-Blockchain/Multilayer/Sidechains'
(Quelle: Eigene Darstellung)

Eine alternative Filterung auf *Taxonomy* unterscheidet wie folgt:

i. Public-Permissionless (siehe *Abbildung 7-48*)

ii. Public-Permissioned (siehe *Abbildung 7-49*)

iii. Private-Permissionless (siehe *Abbildung 7-50*)

iv. Private-Permissioned (siehe *Abbildung 7-51*)

v. Consortial (siehe *Abbildung 7-52*)

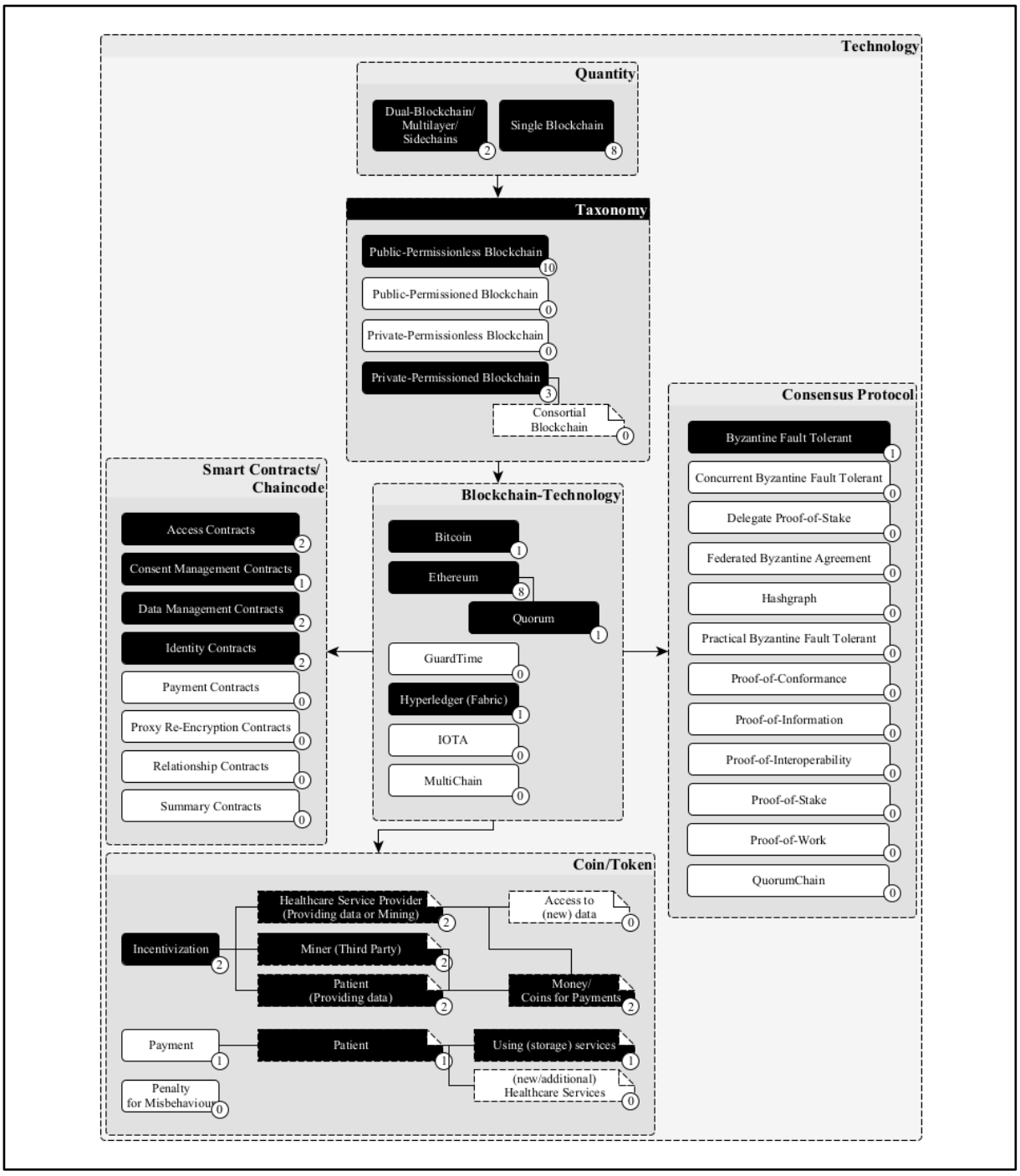


Abbildung 7-48: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Public-Permissionless Blockchain'
(Quelle: Eigene Darstellung)

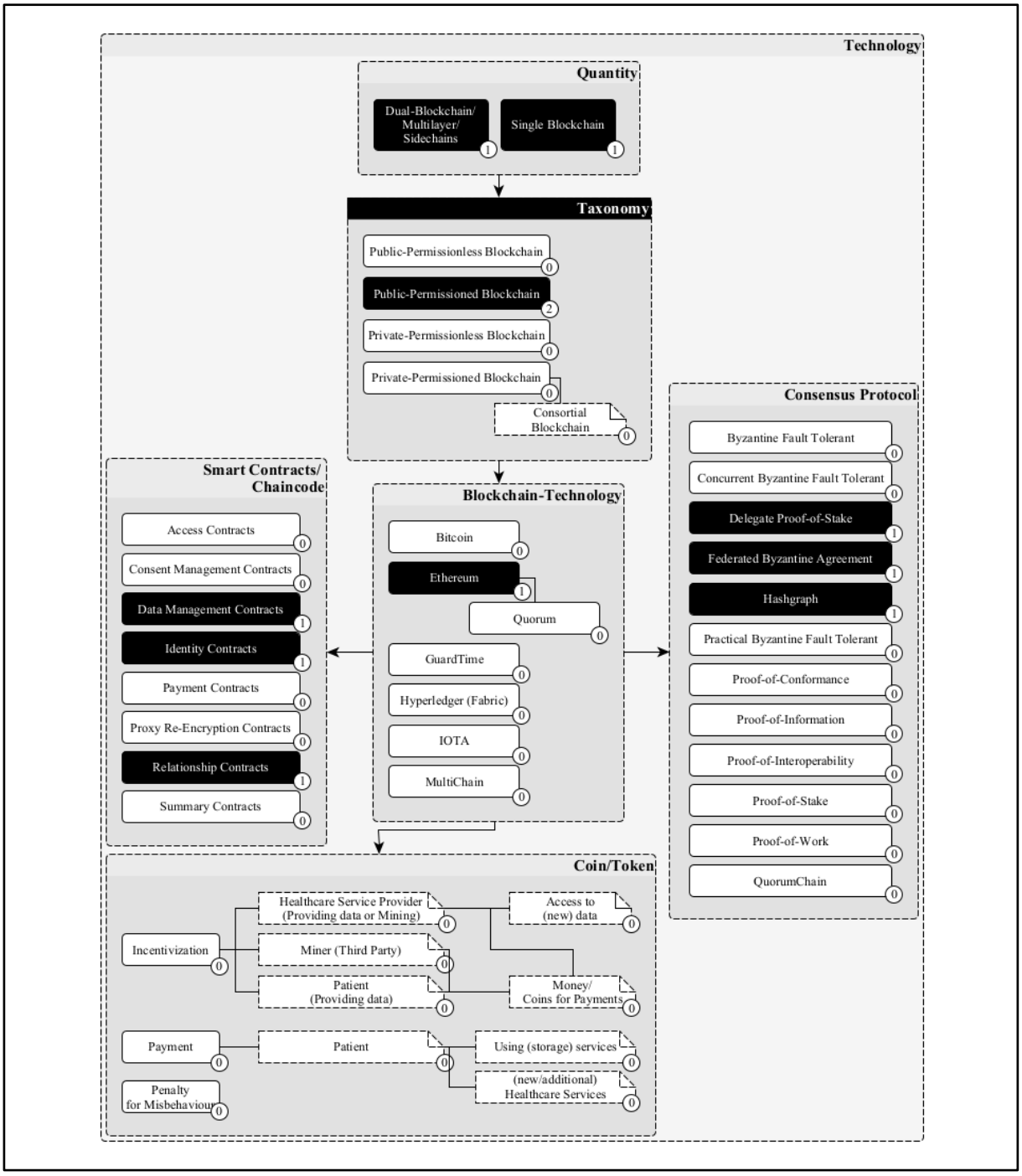


Abbildung 7-49: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Public-Permissioned Blockchain'
(Quelle: Eigene Darstellung)

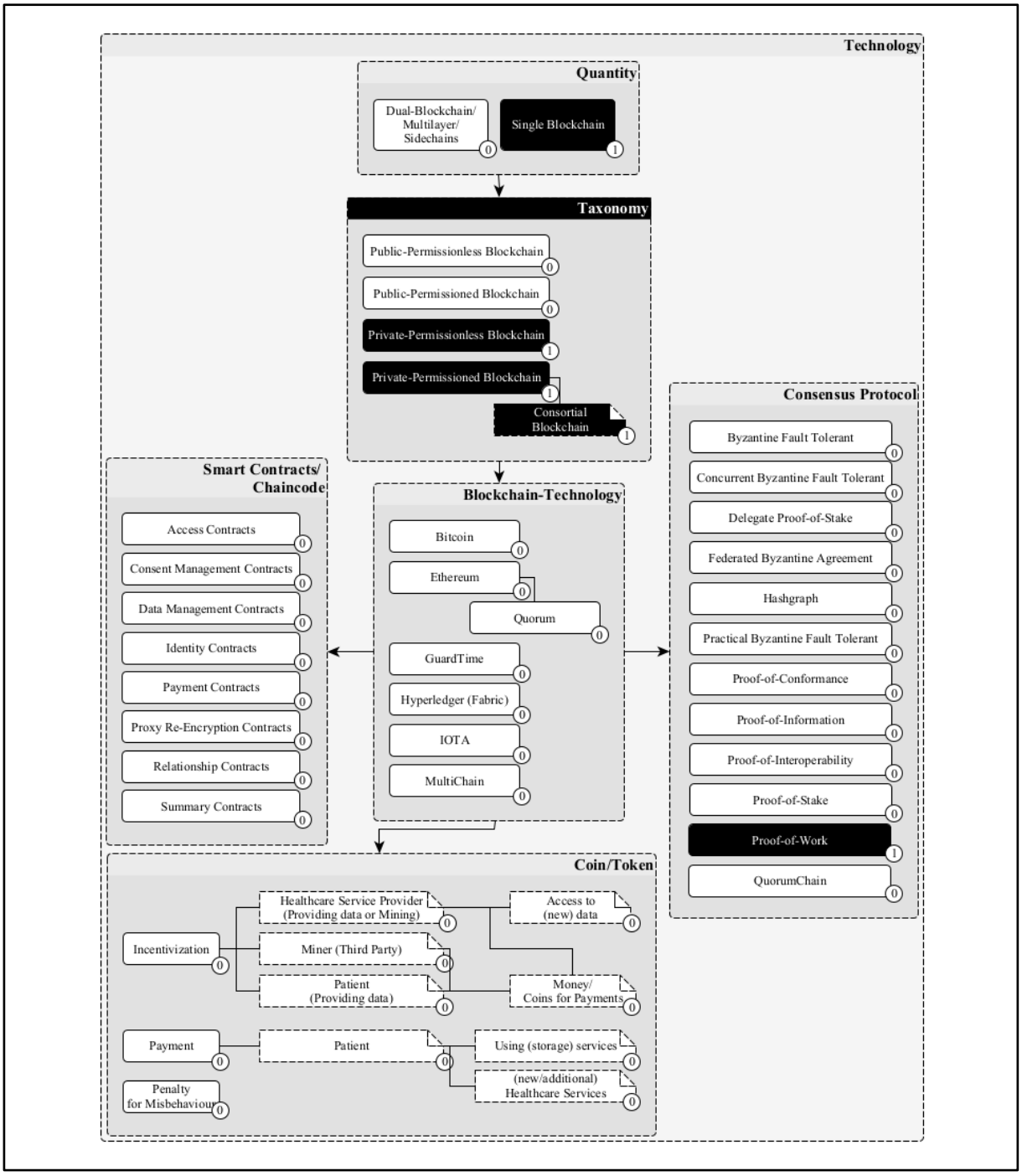


Abbildung 7-50: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Private-Permissionless Blockchain'
(Quelle: Eigene Darstellung)

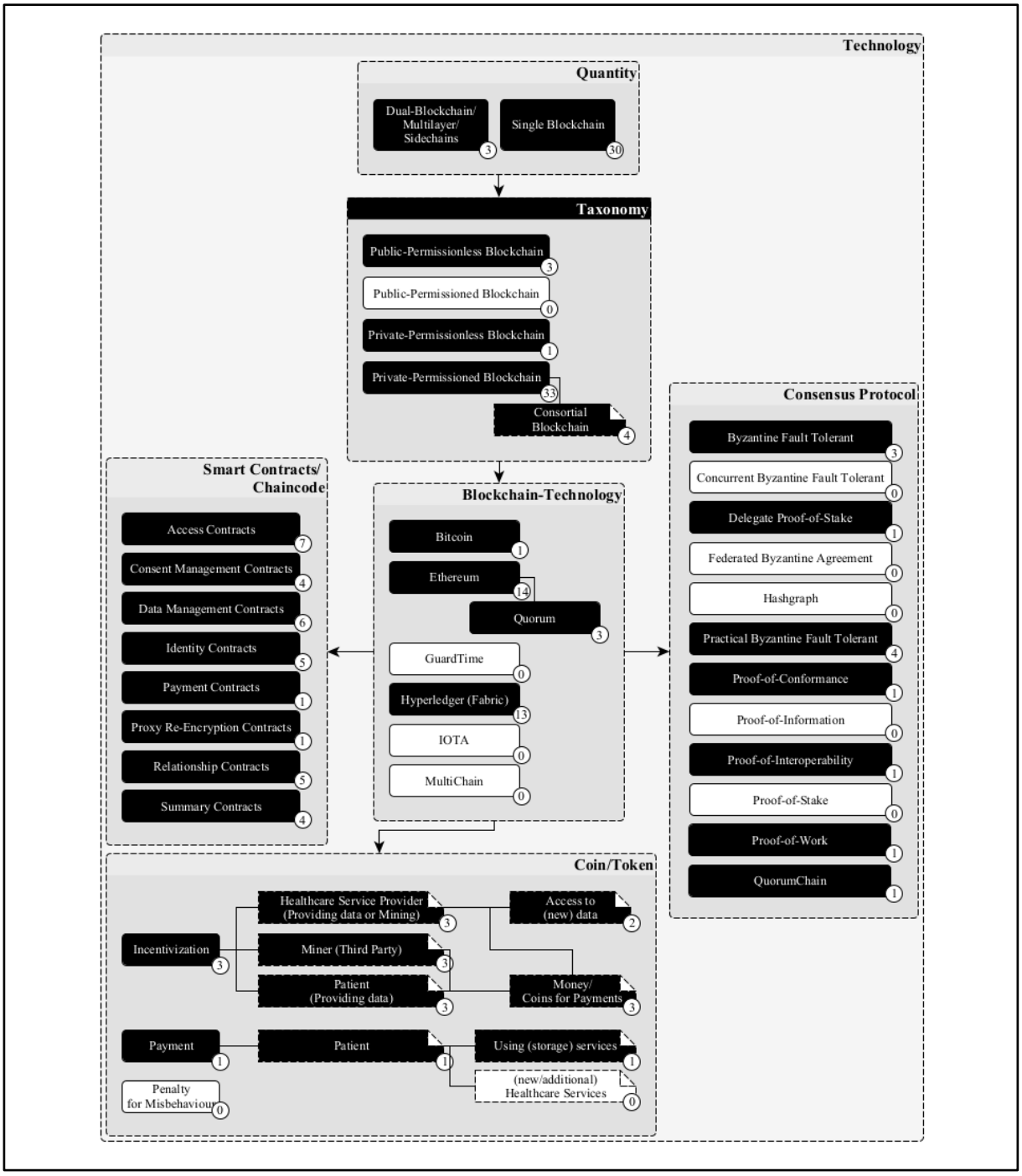


Abbildung 7-51: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Private-Permissioned Blockchain'
(Quelle: Eigene Darstellung)

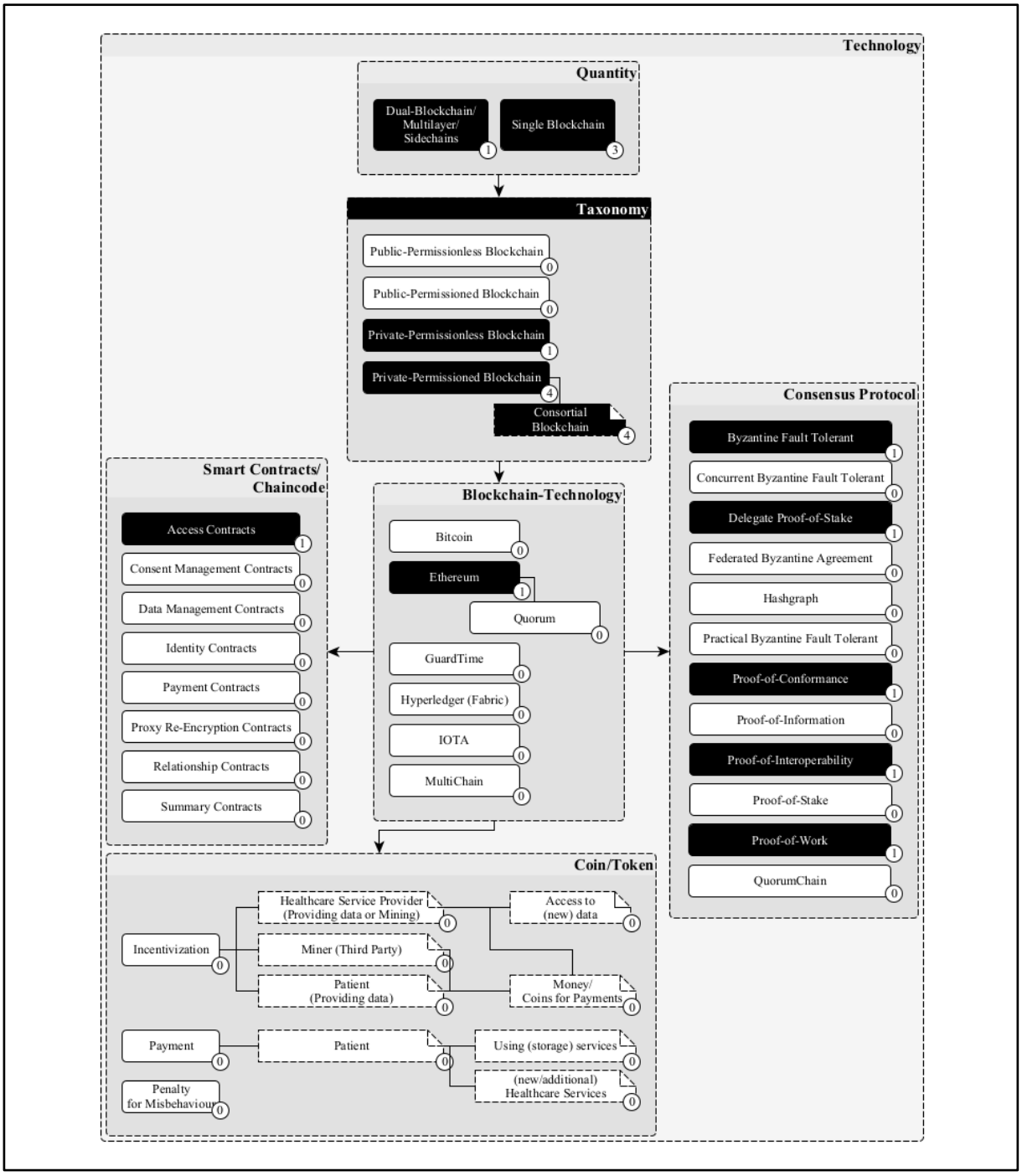


Abbildung 7-52: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Consortial Blockchain' (Quelle: Eigene Darstellung)

Ein weiterer Ansatz ist die Fokussierung auf die Blockchain-Technologie statt auf die Blockchain-Taxonomie. Hier ergeben sich die folgenden möglichen Ausprägungen:

i. Bitcoin (siehe *Abbildung 7-53*)

ii. Ethereum (siehe *Abbildung 7-54*)

iii. Quorum (siehe *Abbildung 7-55*)

iv. Hyperledger (Fabric) (siehe *Abbildung 7-56*)

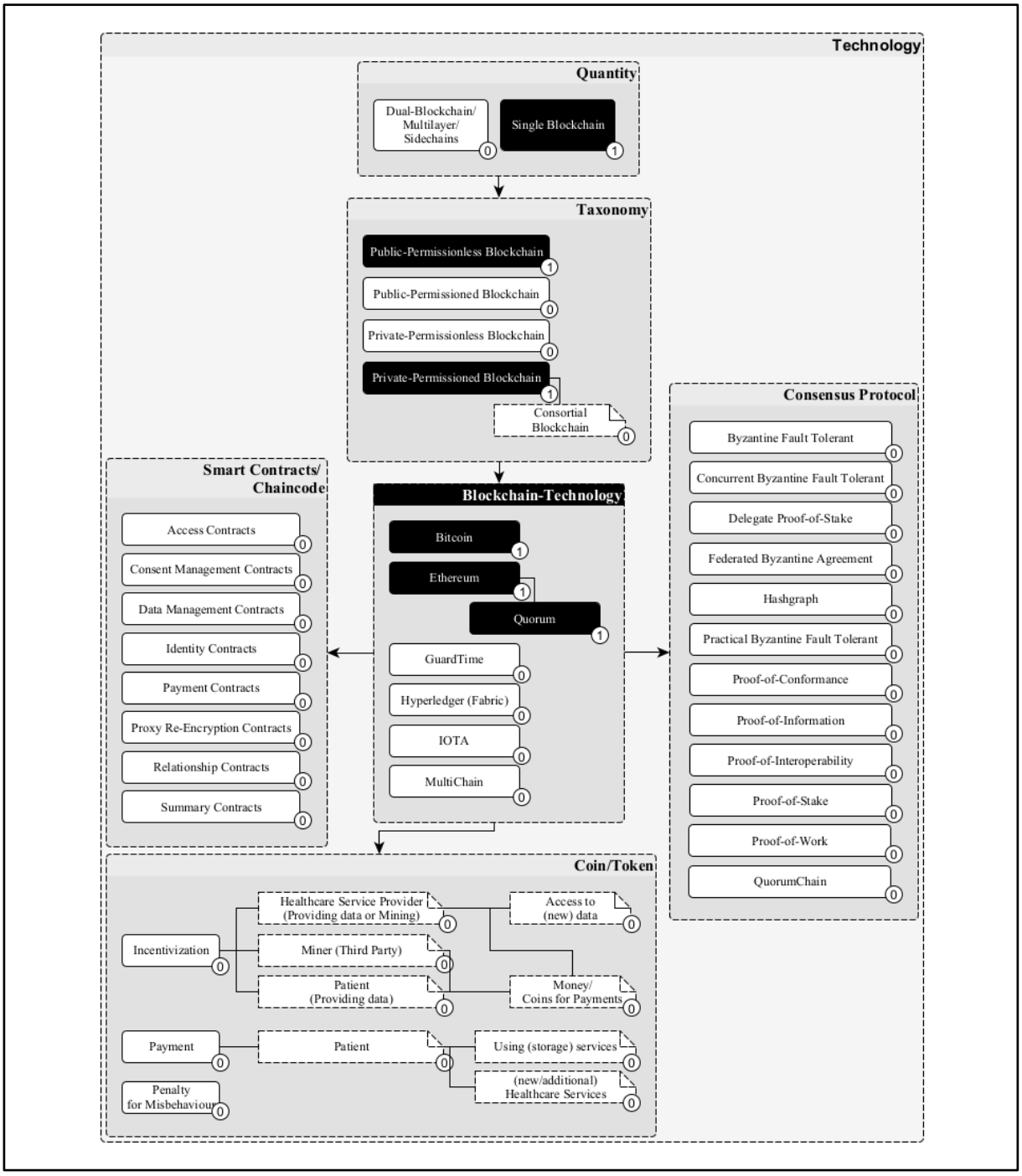


Abbildung 7-53: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Bitcoin' (Quelle: Eigene Darstellung)

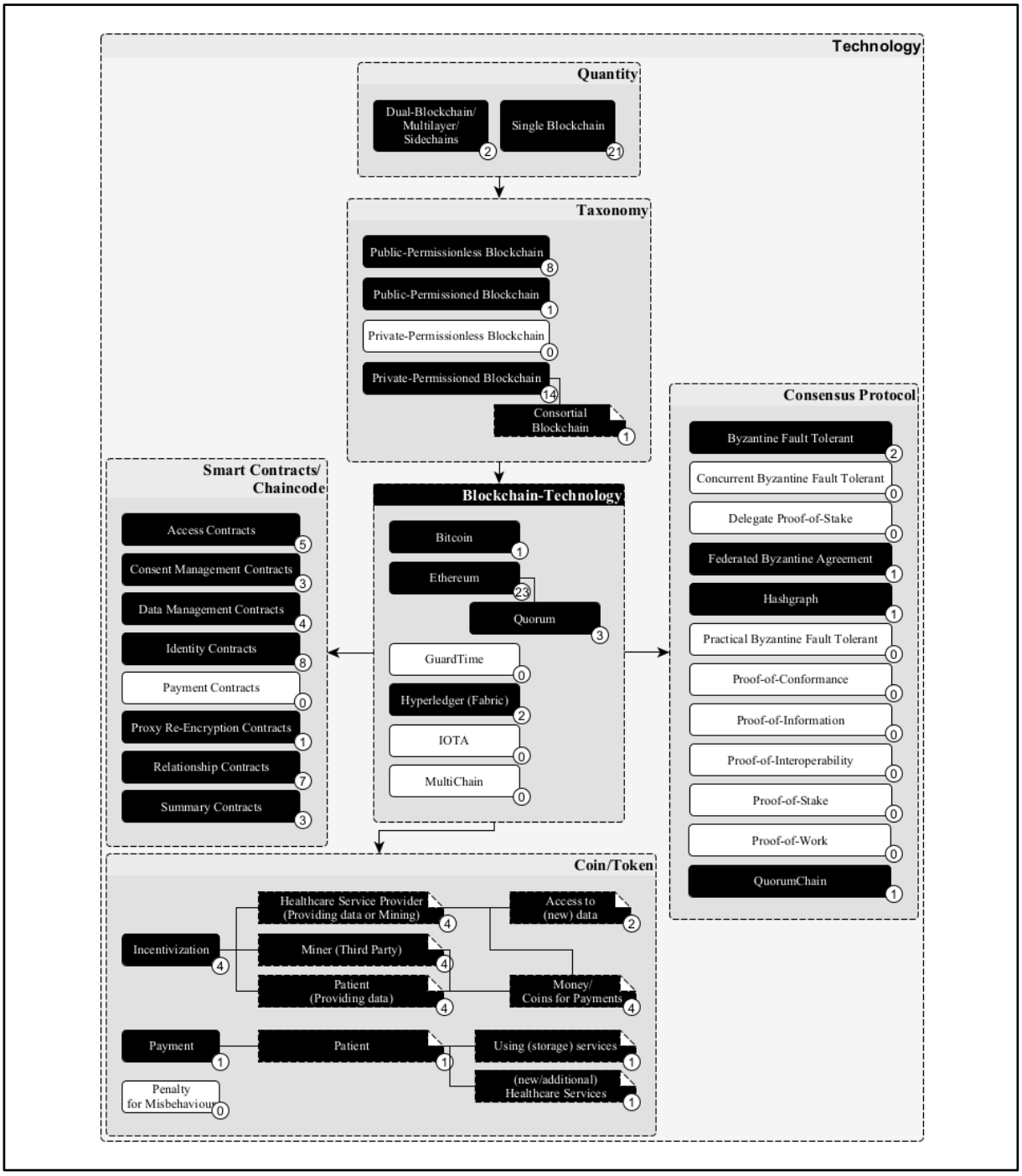


Abbildung 7-54: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Ethereum' (Quelle: Eigene Darstellung)

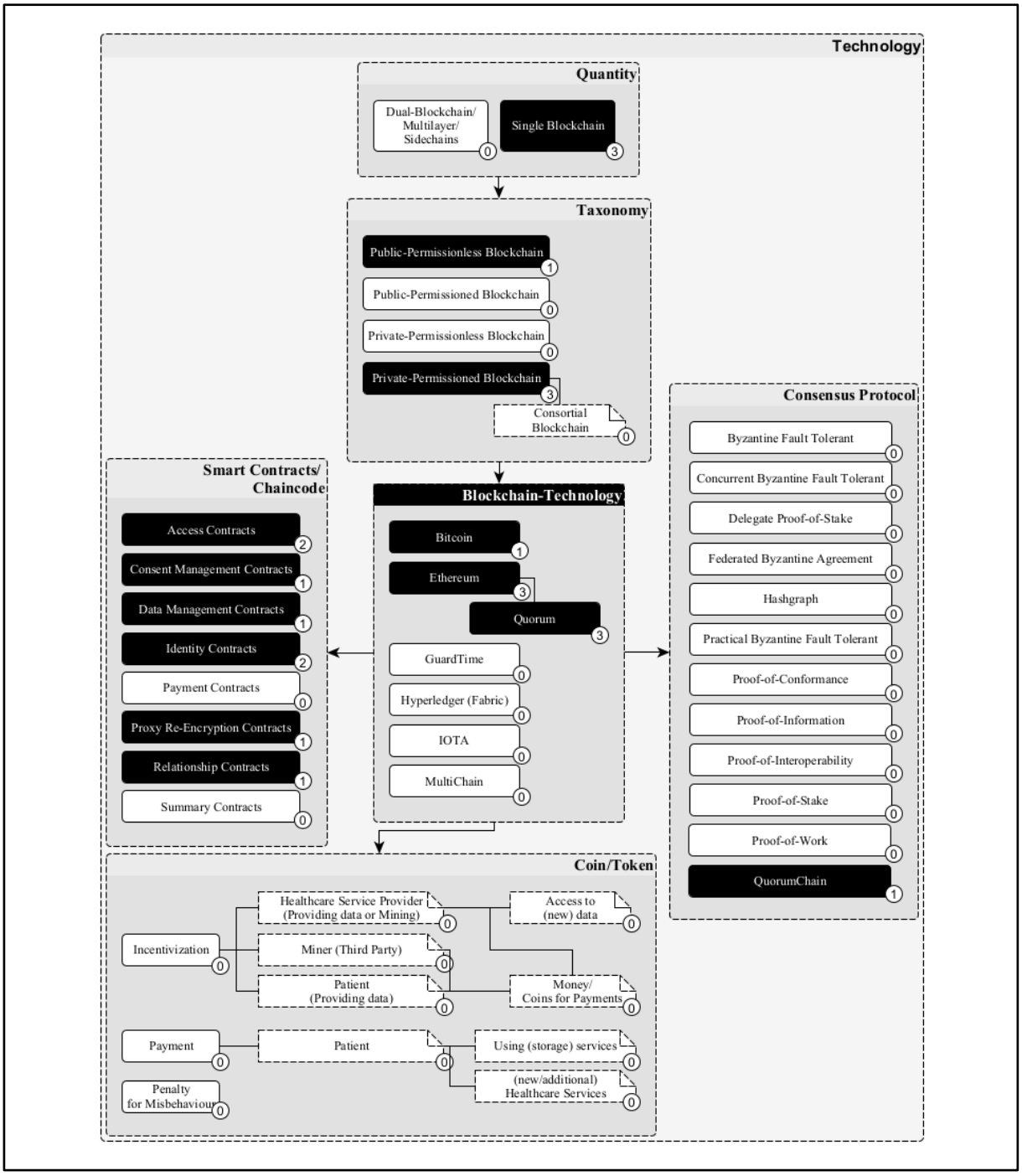


Abbildung 7-55: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Quorum' (Quelle: Eigene Darstellung)

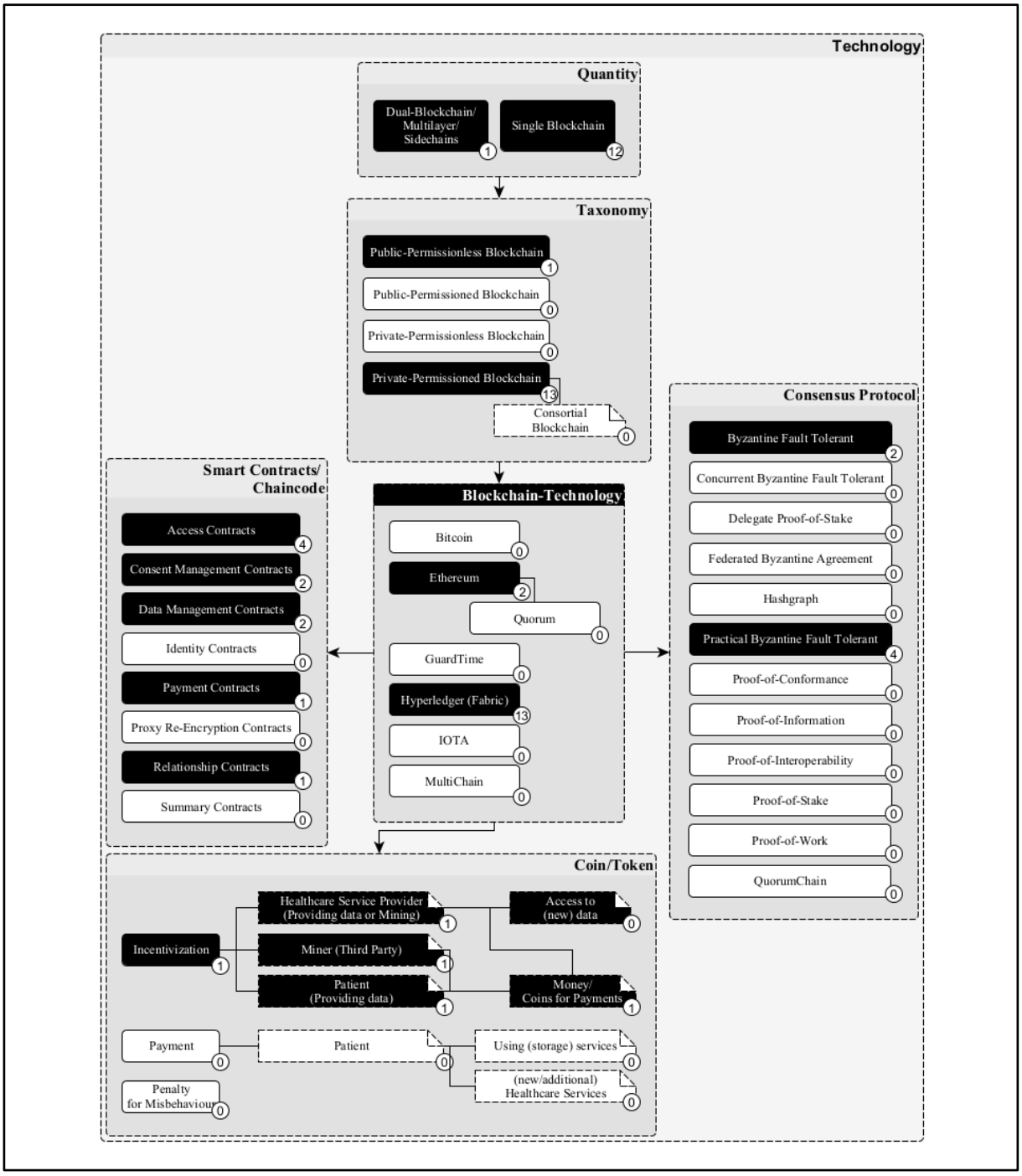


Abbildung 7-56: PHR-Variationen in der Sicht ‚Technology' mit Filterung auf ‚Hyperledger' (Quelle: Eigene Darstellung)

Im Resümee ergeben sich für jeden Aktentyp verschiedene Variationspunkt-Kombinationen in jeder der identifizierten Sichten. Das folgende Kapitel greift die Erkenntnisse aus Referenzarchitektur und Entscheidungsmodell auf und evaluiert deren tatsächliche Relevanz unter Anwendung entsprechender Methoden.

8 Evaluation und Diffusion

8.1 Verfügbare Methoden zur Evaluierung

In der wissenschaftlichen Literatur haben sich diverse Verfahren zur Evaluation von Referenzarchitekturen entwickelt. Grundsätzlich wird zwischen der Evaluation von *Technologie*- und *Software*-Architektur unterschieden. Erstere betrachtet insbesondere die beim Einsatz von Software relevanten Rahmenbedingungen, wie bspw. Hardware, Netzwerke, Betriebssysteme und Infrastruktur, die mittels Benchmarkings geprüft werden.[642] Software-Architektur-Evaluierung beschränkt sich auf eine konkrete Software und bewertet den Grad der Effizienz und Effektivität.[643] Beide Evaluationsmethoden werden ebenfalls für Informationssystem-Architekturen genutzt. Nur die für Softwarearchitekturen etablierten Metriken zur quantitativen Analyse eignen sich nicht.[644] Konkrete, in diesem Zusammenhang relevante Evaluationsmethoden sind:

i. *Frühe* und *späte* Evaluation
ii. Fragebogen und Checklisten
iii. Mathematische Modelle
iv. Architektur-Prototyp
v. Szenario-basierte Evaluation

Frühe bzw. späte Evaluation (i) definiert den Zeitpunkt einer Evaluation. Eine frühe Evaluation wird bspw. durchgeführt, wenn kaum Informationen zur Zielarchitektur vorliegen und Evaluationen auf Basis von Szenario-Beschreibungen, Anforderungsanalysen oder Experteninterviews durchgeführt werden. Späte Evaluationen hingegen sind detaillierter und erlauben eine Ergebnismessung auf Basis von Kennzahlen, setzen dafür allerdings eine konkrete Konstruktion voraus.[645]

Fragebögen und Checklisten (ii) nutzen das Wissen der Softwareanwender und definieren in einer ersten Phase die Rahmenbedingungen. Darauf aufbauend werden Erfüllungsgrad sowie Nutzen einer Softwarearchitektur statistisch ausgewertet.[646]

Mathematisch basierte Evaluation (iii) greift auf mathematisch formulierte Modelle zurück, die eine theoretische Sicht auf Softwarearchitekturen erlauben. Statt einer qualitativen Analyse

642 Vgl. Hoffmann (2007): 37.
643 Vgl. Hoffmann (2007): 31.
644 Vgl. Vasconcelos/Sousa/Tribolet (2005): 8.
645 Vgl. Hoffmann (2007): 31.
646 Vgl. Hoffmann (2007): 31f; Galster/Avgeriou (2011): 156.

(siehe bspw. Szenario-basierte Evaluation) wird eine quantitative Analyse durchgeführt, deren Kern die Berechnung der Zuverlässigkeit[647] oder Performance[648] von Software ist.[649]

Die Konstruktion eines **Prototyps** (iv) überführt die Erkenntnisse der Architekturkonstruktion unter der Annahme spezieller Einsatzszenarien in ein ausführbares Produkt. Die Bewertung der Architektur beruht anschließend auf qualitativen und quantitativen Ergebnissen des Prototyps unter der Prämisse, dass dessen Konstruktion und Verwendung nicht durch Individualinteressen der potenziellen Stakeholder verzerrt werden. Der evaluierte Prototyp muss dabei kein vollständig auf der Architektur beruhendes Objekt sein, sondern kann auch einen Teilaspekt der Architektur abbilden.[650]

Szenario-basierte Evaluation (v) beschreibt eine Methode, die zur Evaluation spezifische für die Stakeholder relevante Szenarien konstruiert und anschließend hinsichtlich definierter qualitativer Kriterien prüft. Mehrere Szenarien können priorisiert evaluiert werden, dürfen aber untereinander keine Abhängigkeiten, sogenannte funktionale Attribute, aufweisen.[651]

Für diese Forschungsarbeit wird eine Kombination aus *szenario-basierter* Evaluation und deskriptiver *Konstruktion eines Prototyps* gewählt. Dabei werden als Szenarien die beschriebene Problematik einer lebenslang geführten, einrichtungsübergreifenden Patientenakte und die aktuelle Diskussion um die Einführung eines digitalen Impfpasses aufgegriffen. Ziel der Evaluation ist die Validierung der Eignung von Referenzarchitektur und Entscheidungsmodell sowie die Ableitung von Handlungsempfehlungen für die dargestellten Szenarien.

8.2 Definition grundlegender quantitativer Ausprägungen der Anwendungsdomäne zur Unterstützung der Evaluation

Aufgrund des insbesondere in der Wirtschaftsinformatik relevanten ökonomischen Kontextes beschreibt dieses Kapitel die für die Evaluation relevanten Umwelteinflüsse *Netzwerkteilnehmer* und *Datenmenge*. Beide beeinflussen die Wahl von Variationspunkten entsprechend ihrer Ausprägung. Konkrete Performance-Metriken der Blockchain-Technologien werden hier nicht tiefergehend analysiert, da diese nur während des Betriebs der jeweiligen Technologie, bspw.

---

647 Beispiel-Methoden: *path-* bzw. *state-based* (vgl. Shanmugapriya/M. Suresh (2012): 22).

648 Beispiel-Methoden: SPE, WS, PASA, CM, BIM, ABI, AABI (vgl. Shanmugapriya/M. Suresh (2012): 22).

649 Vgl. Hoffmann (2007): 35f; Shanmugapriya/M. Suresh (2012): 22.

650 Vgl. Avgeriou (2003): 20; Hoffmann (2007): 35; Cioroaica et al. (2019): 276.

651 Vgl. Avgeriou (2003): 20; Hoffmann (2007): 32f; Shanmugapriya/M. Suresh (2012): 19f; Cioroaica et al. (2019): 276. Beispiel-Methoden: Software Architecture Analysis Method (SAAM), Architectural Trade-off Analysis Method (ATAM), Active Reviews for Intermediate Designs (ARID), Architecture-Level Modifiability Analysis (ALMA), Family Architecture Assessment Method (FAAM), Cost Benefits Analysis Method (CBAM).

nach der Konstruktion eines Prototyps, gemessen werden können.[652] Dieser Betrieb wird aber im Rahmen dieser Forschungsarbeit keinem Test unterzogen.

8.2.1 Anzahl der zu erwartenden Netzwerkteilnehmer

Die Anzahl der Netzwerkteilnehmer definiert den Umfang des zu konzipierenden Netzwerks und hat damit Auswirkungen auf die Performance von Blockchain-Technologien und deren Erfolgswahrscheinlichkeit. Netzwerkteilnehmer bzw. Stakeholder sind alle Akteure des Gesundheitswesens, auf die Digitalisierung einen Einfluss hat.

Stakeholder werden bereits in den Regelungen des GMG unter dem Begriff der Interessensgruppen eines digitalen Gesundheitswesens adressiert und im weiteren Diskurs durch BERNNAT und HAAS weiter differenziert. Zusammengefasst ergibt sich die in *Tabelle 8-1* dargestellte Übersicht.

Tabelle 8-1: Akteure im Gesundheitswesen (Quelle: Eigene Darstellung in Anlehnung an GMG (2003): 2234; Haas (2006): 188f; Bernnat (2016): 30)

§ 291a Abs. 7 SGB V	**BERNNAT**	**HAAS**
Spitzenverbände der Krankenkassen	Kostenträger	Krankenversicherungen
		Unfallversicherungsträger
Kassenärztliche Bundesvereinigung Kassenzahnärztliche Bundesvereinigung Bundesärztekammer Deutsche Krankenhausgesellschaft Spitzenorganisation der Apotheker	Leistungserbringer	Gesundheitsversorgungseinrichtungen
		Kassenärztliche Vereinigungen
		Ärztekammern
		Betriebsärztliche Dienste
	Privatwirtschaft	Medizininformatik-Unternehmen
		Speziell im Gesundheitswesen tätige Rechenzentren
		Pharmahersteller
		Hersteller von Heil- und Hilfsmitteln
	Staat und Verwaltung	Statistische Bundes-/Landesämter
		Diverse Krankheitsregister (z.B. Krebsregister)
	Patienten	Bürger
	Forscher	

[652] Vgl. Kombe/Ally/Sam (2018): 476f. Hierzu zählen bspw. Transactions per second (TPS), Transactions per network data (TPND), Transactions per memory second (TPMS), Transactions per CPU (TPC), Transactions per disk I/O (TPDIO).

Die von BERNNAT aufgeführten Akteure stehen in einem Interaktionsverhältnis (siehe *Abbildung 8-1*). Während Leistungserbringer untereinander kommunizieren **(1),** versorgen sie nicht nur Patienten und erhalten dafür eine Vergütung **(2)** abhängig von der Versicherungsleistung des Patienten **(6)**, sondern stehen auch mit Kostenträgern zur Abwicklung von Selektiv- oder Kollektivverträgen in Verbindung **(7)**. Patienten interagieren ebenfalls **(3)**, tauschen Erfahrungen aus und nutzen hierfür Produkte und Dienstleistungen aus der Privatwirtschaft **(4)**. Genauso nutzen Leistungserbringer **(5)** und Kostenträger **(8)** Produkte und Dienstleistungen der Privatwirtschaft, um ihrem Auftrag einer guten Gesundheitsversorgung gerecht zu werden.[653] Aufgrund dessen, dass der Staat die Gesetzgebung innehat und Forschung mehreren Akteursgruppen zugeordnet werden kann,[654] werden diese nicht als eigenständige Gruppe deklariert, sondern stattdessen als übergreifender Stakeholder betrachtet.[655]

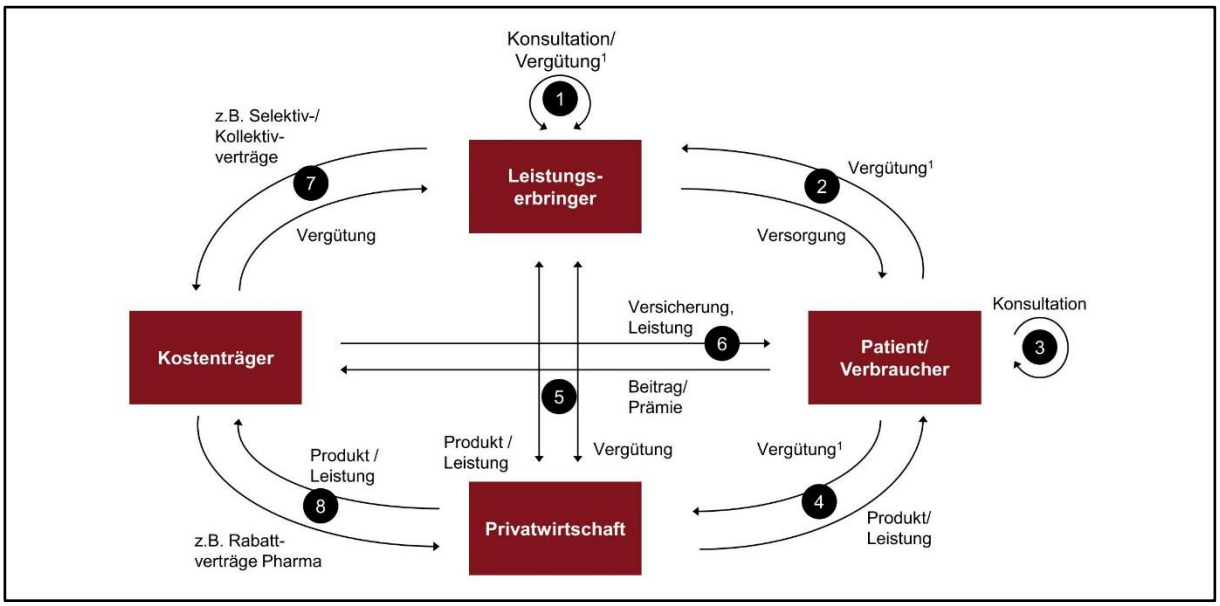


Abbildung 8-1: Akteure im Gesundheitswesen und ihre Beziehungen (Quelle: Bernnat (2016): 31)

Eine alternative Darstellung der Kommunikation zwischen Stakeholdern zeigt *Abbildung 8-2*, wobei Kostenträger von den Autoren nicht berücksichtigt werden.

653 Vgl. Bernnat (2016): 31f.

654 Bspw. können sich Forschungsabteilungen in Krankenhäusern (Leistungserbringer) wie auch bei Versicherern (Kostenträger) oder in der Pharma-Branche (Privatwirtschaft) finden (vgl. Bernnat (2016): 33).

655 Vgl. Bernnat (2016): 32f.

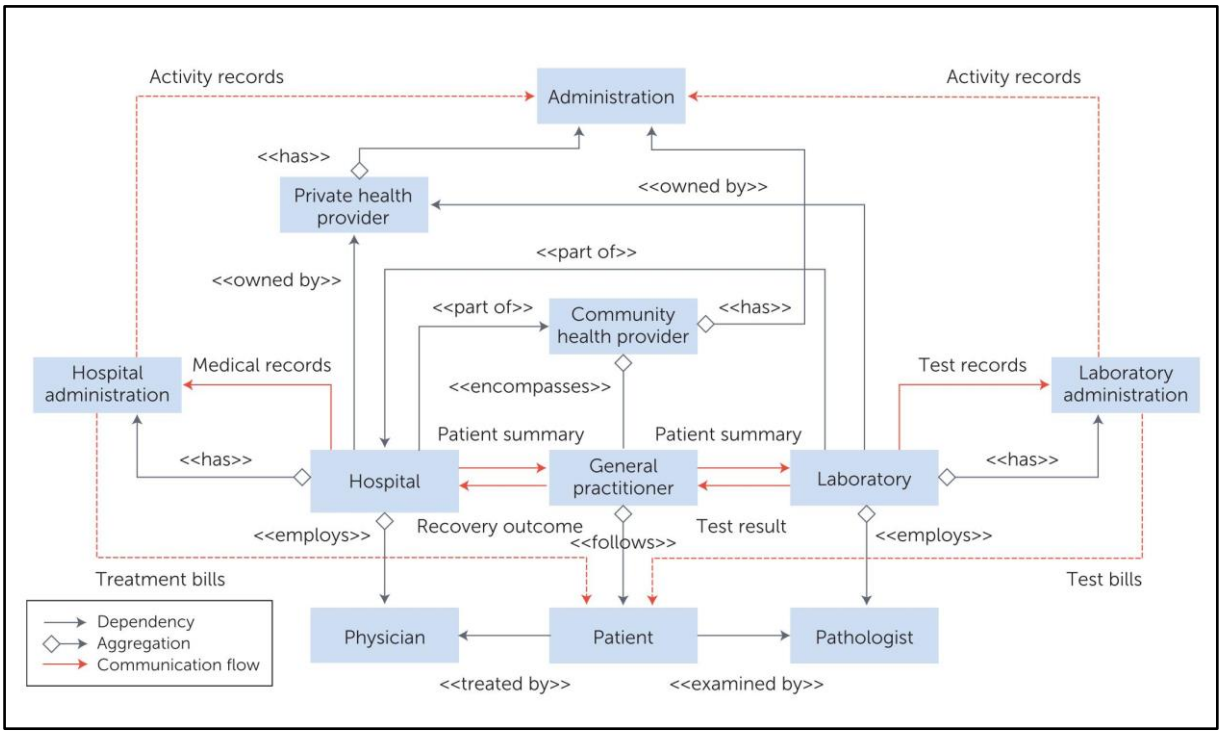


Abbildung 8-2: Alternative Darstellung der Akteure im Gesundheitswesen und ihrer Beziehungen (Quelle: Casola et al. (2016): 11)

In Anbetracht der Zielsetzung der Forschungsarbeit wird die obere Hälfte der *Abbildung 8-1* berücksichtigt, d.h. die Interaktionen von (1), (2), (3), (6) und (7), ergänzt um sämtliche Forschungsakteure. Interaktionen mit der Privatwirtschaft werden nicht betrachtet. Dies reduziert die in *Tabelle 8-1* dargestellte Liste von Stakeholdern und führen zu der in *Tabelle 8-2* aufgeführten Liste. Zur quantitativen Messung des Umfangs des zu erwartenden Blockchain-Netzwerks wird die Tabelle um die Anzahl der aktuell in Deutschland vorhandenen Stakeholder ergänzt. Auf die Zählung von IoT-Geräten, die ebenfalls in die Berechnung der Anzahl der Nodes im Netzwerk einbezogen werden können,[656] wird verzichtet. Jedes dieser Geräte könnte einen eigenen Node darstellen, doch sieht das in dieser Forschungsarbeit angenommene Szenario ein bestehendes Aktensystem vor, das entweder beim Patienten oder beim Leistungserbringer existiert und als Datenlieferant bzw. -empfänger genutzt wird.

[656] Vgl. Badr/Gomaa/Abd-Elrahman (2018): 161.

Tabelle 8-2: Anzahl von Akteuren in Deutschland (Quelle: Statistisches Bundesamt (2018b): 8; Bundesärztekammer (2019): 2; Statistisches Bundesamt (2019a): o. S; Statistisches Bundesamt (2019b): o. S.)

Akteur		Anzahl
Krankenversicherungen (KV)	Gesetzliche KV (2019)	109
	Private KV (n/a)	n/a
Zwischensumme		***109***
Gesundheitsversorgungseinrichtungen	Krankenhäuser (2017)	1.942
	Niedergelassene Ärzte (2019)	116.300
Zwischensumme		***118.351***
Bürger (2019)		83.166.711
Summe		***83.285.062 ~83,3 Mio.***

Anmerkung: Zur privaten KV sind keine verlässlichen Zahlen von 2019 zu ermitteln. Aus diesem Grund wird diese Zahl nicht zusätzlich aufgeführt, stattdessen in die Rundung des Endergebnisses mit einberechnet. Die mögliche Differenz in der Anzahl der Krankenhäuser zwischen dem Erhebungszeitpunkt (2017) und 2019 wird ebenfalls in der Rundung berücksichtigt.

Ein erster Vergleich der zu erwartenden Stakeholder eines Blockchain-Netzwerks mit dem bereits existierenden Bitcoin-Netzwerk zeigt, dass im Falle einer Gesundheitsdaten-Blockchain die Anzahl an potenziellen Nodes (83,3 Mio.) wesentlich höher ist, als es derzeit im Bitcoin- (0,010237 Mio.) oder Ethereum-Netzwerk (0,007294 Mio.) der Fall ist. In *Abbildung 8-3* wird die von BITNODES prognostizierte Anzahl an Full-Nodes dargestellt. Die diesen wiederum untergeordneten Light-Nodes werden dabei nicht erfasst. Im Ethereum-Netzwerk existieren derzeit ca. 7.300 Nodes (siehe *Abbildung 8-4*). Eine entsprechende Dunkelziffer ist möglich.

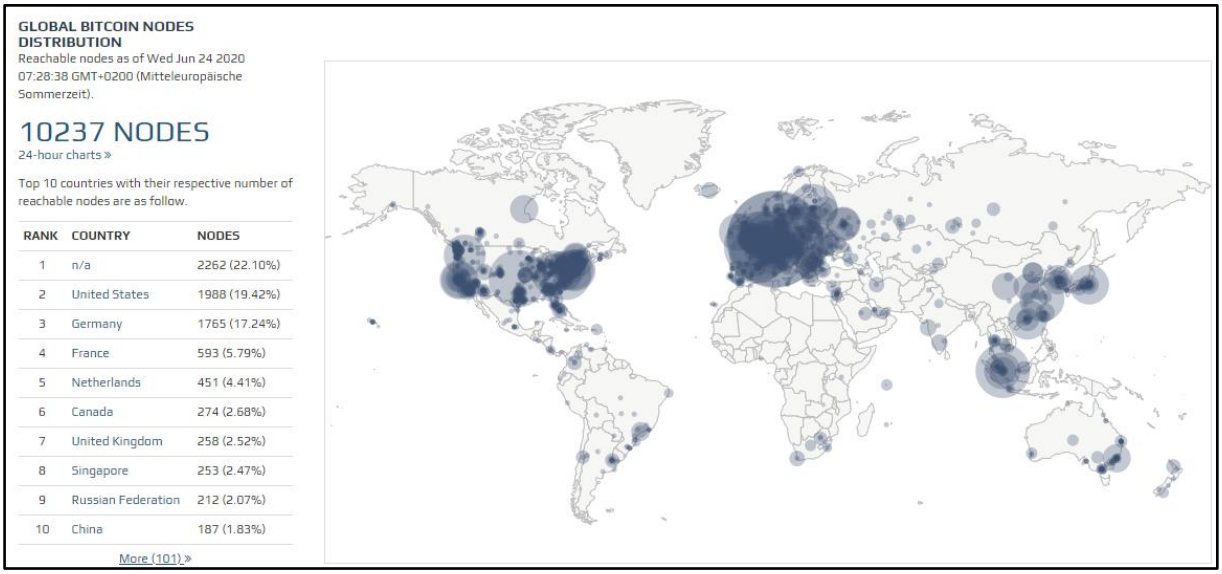


Abbildung 8-3: Anzahl und Verteilung von Full-Nodes im Bitcoin-Netzwerk (Quelle: Bitnodes (2020): o. S.)

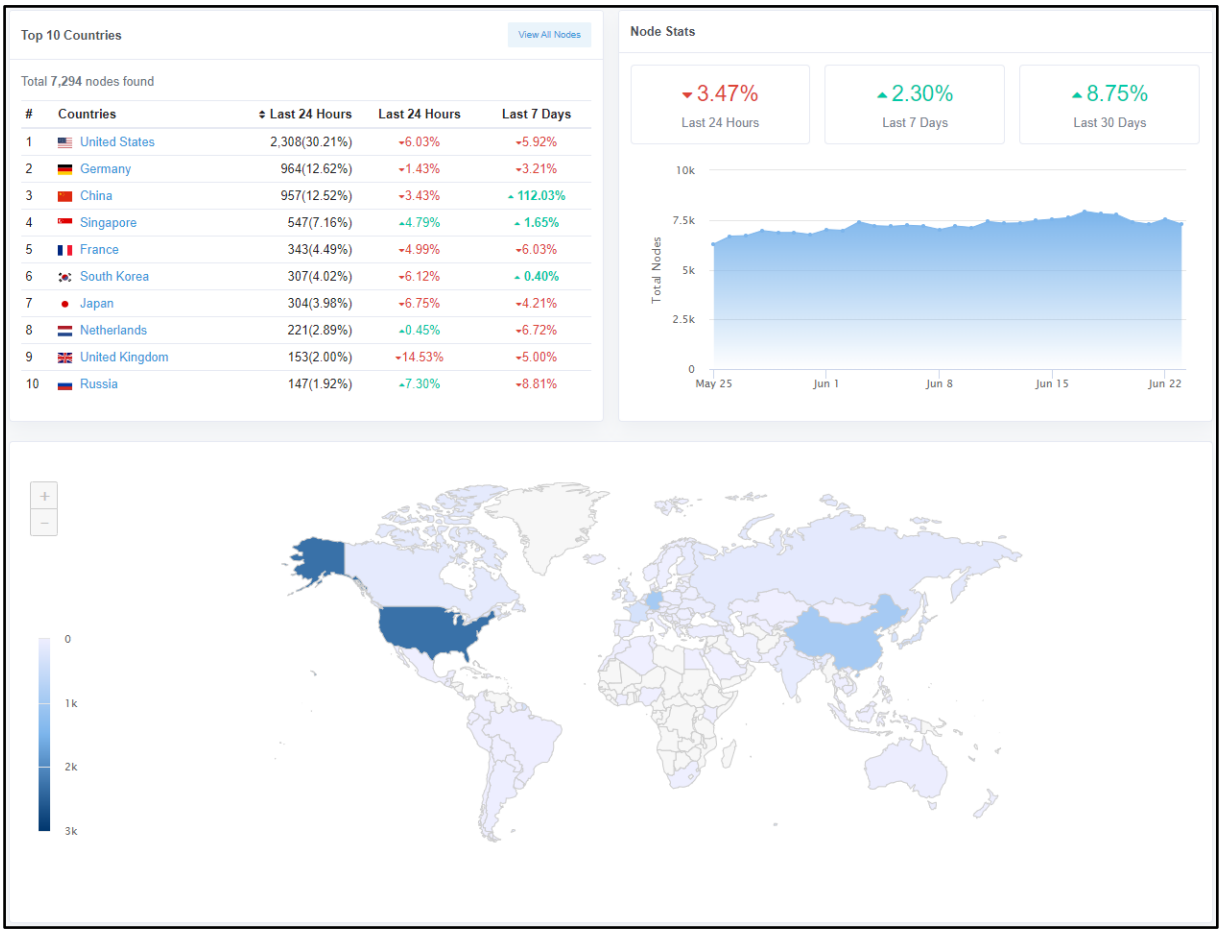


Abbildung 8-4: Anzahl und Verteilung von Full-Nodes im Ethereum-Netzwerk (Quelle: Etherscan (2020): o. S.)

8.2.2 Volumen der im Netzwerk zu erwartenden Gesundheitsdaten

Zur Evaluation der Variationen werden in diesem Kapitel Gesundheitsdaten quantifiziert. Die Menge an Daten innerhalb einzelner Gesundheitseinrichtungen umfasst mehrere Petabytes. So bezifferte beispielsweise 2014 ein amerikanischer Gesundheitsdienstleister die Menge an EHR-Daten in einer Einrichtung auf 26 bis 44 Petabytes.[657] Neben der mit der Komplexität einhergehenden Steigerung der Größe jeder einzelnen Datei steigt die Menge dieser Daten zudem jährlich an. Insbesondere neuronale Bilder sorgen seit 2015 jährlich zu einer Gesamtsteigerung von mehr als 10 Petabytes, Genomsequenzierungen von mehr als 20 Petabytes pro Jahr.[658] Heruntergebrochen auf einzelne Gesundheitsdaten bewegt sich die Größe einzelner Bilder zwischen 131 und 442 Kilobyte für reguläre Aufnahmen und 5 bis 30 Megabyte (MB) für komplexe und hochauflösende Aufnahmen.[659]

657 Vgl. Bell et al. (2018): 4. 1 Petabyte entspricht 1.000 Terrabyte bzw. 1.000.000 Megabyte.

658 Vgl. Dinov (2016): 2.

659 Vgl. Dandu (2008): 287; Garcia Ruiz et al. (2011): 280.

Ein im Jahr 2011 erhobener Durchschnittswert pro Patient lag bei 80 Megabyte, wobei diese sich in 4 Megabyte Text- und 76 Megabyte Bildmaterial aufteilen.[660] Der gleiche Wert findet sich in einer 2018 veröffentlichten Studie.[661] Doch spiegelt dieser konstant gebliebene Durchschnittswert die bereits angesprochene exponentielle Zunahme der Gesundheitsdaten nicht wider.[662] Die jährliche Wachstumsrate liegt entsprechend einem Report von 2014 bei ca. 48%.[663] Diese Wachstumsrate wird für den Zeitraum von 2011 bis 2020 approximiert, begonnen mit einer durchschnittlichen Datenmenge pro Patient, und folglich eine durchschnittliche Datenmenge von gerundet 2.700 Megabyte (2,7 Gigabyte (GB)) ermittelt (siehe *Formel (2)*), die in der weiteren Bearbeitung zugrunde gelegt wird.

$$80\ MB * (1 + 0{,}48)^9 = 2.725{,}5\ MB\ \approx 2.700\ MB \approx 2{,}7\ GB \qquad \textbf{Formel (2)}$$

8.3 Allgemeine Diskussion ausgewählter Variationspunkte

8.3.1 Vergleich von Cloud mit IPFS

Entsprechend der aus den Kapiteln des Entscheidungsmodells bekannten Literaturverteilung wird angenommen, dass insbesondere die Wahl zwischen Cloud und IPFS eine Rolle in der Konstruktion von Blockchain-Lösungen einnimmt. Während Cloud einerseits schnelle Ressourcenallokation und Kostensenkungspotentiale bietet, ermöglicht IPFS eine sichere verteilte Datenhaltung ohne den Einsatz eines Intermediärs.

Trotz der in *Kapitel 6.3.3* genannten Vorteile gibt es auch Kritik an der Nutzung von Cloud-Technologien, die insbesondere die Security von Infrastrukturen betrifft. Einem Cloud Service Provider wird grundsätzlich vorgeworfen, dass dieser ‚*honest-but-curious*' sind,[664] und folglich die Sicherheitsziele *Vertraulichkeit*[665] und *Datenintegrität*[666] nicht gewährleistet werden. Zudem geht die Kontrolle der Verfügungsgewalt über Daten verloren, sobald diese die Cloud-

660 Vgl. Halamka (2011).

661 Vgl. Suter-Crazzolara (2018): 2, zitiert nach Huesch/Mosher (2017). Die Ursprungsquelle ist aus Lizenzgründen nicht abrufbar, sodass deren Literaturnachweis nicht geprüft werden kann.

662 Vgl. Dandu (2008): 287.

663 Vgl. EMC/Research & Analysis by IDC (2014).

664 Vgl. Theodouli et al. (2018): 1375.

665 Kuo (2011): e67.5; McFarlane et al. (2017): 5; Desai et al. (2018): 1555; Hussein et al. (2018): 1.

666 Kuo (2011): e67.5; Liang et al. (2017a): 472.

Infrastruktur verlassen.[667] Mit zunehmender Distanz zwischen CSP und Patient bzw. Leistungserbringer wächst dieses Risiko.[668]

Erste Maßnahmen zur Sicherstellung der Vertraulichkeit sind bspw. die Verschlüsselung von Daten bereits vor dem Upload in die Cloud oder die Absicherung von Cross-Institutionellem Datenaustausch.[669] Eine weitere Maßnahme ist die Teilung von Daten in mehrere Einzelpakete und verteilte Ablage in verschiedenen Cloud-Diensten.[670]

IPFS wird zunehmend als Alternative zur Cloud betrachtet, beide ähneln sich im Aufbau, weil beide eine dezentrale Datenspeicherung versprechen. Da IPFS jedoch nicht abhängig von einem einzigen Dienstleister ist (bspw. einem CSP), verspricht IPFS, die Schwachstellen einer Cloud zu beheben.[671] Zudem erlaubt der P2P-Ansatz eine schnelle Verarbeitung von Datenanfragen und zeitgleiche Integritätsabsicherung durch Hashes.[672] Doch auch in Bezug auf die Nutzung von IPFS gibt es Kritik, denn die besondere Schutzbedürftigkeit von Gesundheitsdaten erlaubt keine verteilte Speicherung von Daten auf Knoten, deren Sicherheit nicht gewährleistet ist.[673] Auch muss zur Auffindung von Daten immer das dazugehörige Register, eine Distributed Hash Table (DHT), abgefragt werden. Dieses bildet somit die Engstelle der gesamten Konstruktion.[674]

8.3.2 Vergleich von PKI und KSI-Infrastrukturen und Identifikation von Synergiepotentialen

Die Ausprägungen von PKI und KSI sind bereits Thema in *Kapitel 6.4.3*. Im direkten Vergleich bietet eine KSI gegenüber einer PKI Vorteile, wie bspw. die fehlende CA oder die bessere Sicherstellung des *Root of Trust* (siehe *Tabelle 8-3*).

---

667 Vgl. Xia et al. (2017b): 44.1.

668 Vgl. Narayan/Gagné/Safavi-Naini (2010): 47; Haas et al. (2011): e27; Fernández-Alemán et al. (2013): 545.

669 Casola et al. (2016): 12f; Yang/Yang (2017): 104; Chowdhury et al. (2018): 1333; Desai et al. (2018): 1555; Zheng et al. (2018): 163.

670 Vgl. Du et al. (2018): 34.

671 Vgl. Nguyen et al. (2019): 66796; Shah et al. (2020): 384; Sun et al. (2020): 59390. Auch wird die Speicherung von Duplikaten vermieden, die insbesondere bei der Nutzung von mehreren CSP entstehen können (vgl.Sun et al. (2020): 59392). Dies kann passieren, wenn Leistungserbringer B von Leistungserbringer A Daten über einen Patienten erhält, jedoch bei einem anderen CSP unter Vertrag steht (*Beispiel konstruiert durch Autor der Dissertation*)

672 Vgl. Mani et al. (2021): 3003.5. Der Ablauf eines IPFS-Datei-Uploads wird von Shah et al. beschrieben (vgl. Shah et al. (2020): 386).

673 Vgl. Hanley/Tewari (2018): 248.

674 Vgl. Confais/Lebre/Parrein (2017): 43.

Tabelle 8-3: Vergleich von PKI und KSI (Quelle: Buldas/Laanoja/Truu (2017): 123)

	PKI	***KSI***
Signature creation	Potentially offline	Server-assisted
Result of key leak	The number of forgeries is unlimited	Limited, server closes access on detection
Revocation check	During verification	During creation
Revocation solution	Complex	Simple
Evidence integrity	Relies on key secrecy and TTP-s	Mathematically provable
Root of trust	Pre-distributed certificate list	Widely witnessed publication
Server compromise	Unlimited damage	Broken signatures or wrong ID-s, back-dating still not possible
Quantum threat	Insecure: needs new PQ schemes	Secure as far as we know

Neben einer getrennten Verwendung beider Infrastrukturen können sich beide auch gegenseitig unterstützen.[675] Es ergeben sich folgende Kombinationsmöglichkeiten:

i. KSI unterstützt PKI
ii. PKI unterstützt KSI
iii. KSI mit externen Identitätsprovidern erweitern

(i) Die Manipulation oder fehlerhafte Funktion eines Zeitstempeldienstes innerhalb der PKI hat zur Folge, dass sämtliche Signaturen kompromittiert wären. In Kombination mit einer KSI werden alle für die Erstellung einer Signatur relevanten Informationen (bspw. Zeitstempel oder Prüfungsergebnisse der Validität von Informationen) in einer KSI gespeichert. Diese dient als geprüfter und valider Container. Im Falle einer Kompromittierung enthält dieser Container alle historischen Signaturen und ermöglicht so weiterhin eine Validierung der aktuell verwendeten Signaturen. Insbesondere im Zusammenhang mit der Entwicklung von Quanten-Computern, die aufgrund ihrer hohen Rechenleistung grundsätzlich ein Risiko für Verschlüsselungen darstellen, ist die Verwendung dieser Container vielversprechend.[676]

(ii) Wird eine KSI betrieben, unterstützt PKI diese durch Validierung der Identität sämtlicher beteiligter Server sowie in der Einhaltung der Integrität neuer KSI-Root-Hashes vor deren Veröffentlichung. Auf diese Weise wird das Vertrauen zwischen Institutionen eines weltweiten Netzes von KSI-Infrastrukturen gestärkt.[677]

675 Vgl. Buldas/Laanoja/Truu (2017): 124, 129.
676 Vgl. Buldas/Laanoja/Truu (2017): 125f.
677 Vgl. Buldas/Laanoja/Truu (2017): 126f.

(iii) Im Vergleich zur PKI schafft KSI nicht die von der Informationssicherheit geforderte *Nachweisbarkeit* (*non-repudiation*). Deshalb bedarf es ergänzender Mechanismen, die diese Nachweisbarkeit ermöglichen. In diesem Fall können bspw. ein *Lightweight Directory Access Protocol* (LDAP), eine Smartcard oder externe Identitätsprovider, wie OAuth oder OpenID, genutzt werden.[678]

Diese Gegenüberstellung und die Beschreibung der Unterstützungspotentiale zeigt, dass beide in der Architektur dargestellten Infrastruktur-Variationen Vorteile für ein Blockchain-Netzwerk bieten; doch insbesondere die kombinierte Verwendung der Konzepte ist zu empfehlen, auch wenn die in dieser Forschungsarbeit identifizierten Konzeptionen bisher keine Kombination verwenden.

8.3.3 Vergleich von Blockchain-Klassifikationen und Konsensprotokollen

In diesem Kapitel werden die Unterschiede der in der Architektur identifizierten Blockchain-Technologien sowie Konsensprotokolle beschrieben.

Wie aus *Kapitel 3.2.4* bekannt, unterscheiden sich Blockchain-Technologien in *Lokalität*, *Scripting-Fähigkeit* sowie *Applikationsspezifizität*.[679] Um Vergleichbarkeit herzustellen und eine Basis für eine Evaluation, werden die in der Literatur gängigen Vergleichsmaßstäbe für Blockchain-Technologien herangezogen (*Tabelle 8-4*).

Tabelle 8-4: Evaluationskriterien gemäß Literatur (Quelle: Eigene Darstellung)

Nr.	Eigenschaft	Literaturquelle
1	**Open Source**	Kuo/Zavaleta Rojas/Ohno-Machado (2019); Yu et al. (2019); Polge/Robert/Le Traon (2021)
2	**Unterstützung von Smart Contract**	Agbo/Mahmoud (2019); Kuo/Zavaleta Rojas/Ohno-Machado (2019); Yu et al. (2019); Polge/Robert/Le Traon (2021)
3	**Entwicklungssprache**	Kuo/Zavaleta Rojas/Ohno-Machado (2019); Yu et al. (2019)
4	**Konsens-Protokoll**	Macdonald/Liu-Thorrold/Julien (2017); Agbo/Mahmoud (2019); Kuo/Zavaleta Rojas/Ohno-Machado (2019); Polge/Robert/Le Traon (2021)
5	**Transaktionen pro Sekunde**	Ploom (2016); Agbo/Mahmoud (2019)
6	**Transaktionskosten**	Macdonald/Liu-Thorrold/Julien (2017); Agbo/Mahmoud (2019)
7	**Skalierbarkeit**	Macdonald/Liu-Thorrold/Julien (2017); Agbo/Mahmoud (2019); Oliveira et al. (2019); Hou/Tang/Liang (2020)
8	**Security**	Macdonald/Liu-Thorrold/Julien (2017)
9	**Einsatz und Limitierung von Token/Coins**	Macdonald/Liu-Thorrold/Julien (2017); Agbo/Mahmoud (2019); Kuo/Zavaleta Rojas/Ohno-Machado (2019); Polge/Robert/Le Traon (2021)

678 Vgl. Buldas/Laanoja/Truu (2017): 127f.

679 Vgl. Ploom (2016): 123.

10	**Sonstiges**[680]	Macdonald/Liu-Thorrold/Julien (2017); Macdonald/Liu-Thorrold/Julien (2017); Polge/Robert/Le Traon (2021)

Anmerkung: Die Literaturhinweise sind keine direkten Zitate, sondern verweisen allgemein auf die Quelle. Teilweise stimmt die hier in der Tabelle genutzte Kategorisierung nicht mit den in der Ursprungsliteratur genannten Termini überein, sondern wurde zur Kategorisierung in einen einheitlich zu verwendenden Begriff überführt.

In der Evaluation werden sämtliche in der Architektur identifizierten Blockchains berücksichtigt, und es wird auf Ergebnisse in der Literatur zurückgegriffen. Hierzu zählen *Bitcoin*, *Ethereum*, *Quorum*, *GuardTime*, *Hyperledger (Fabric)*, *IOTA* und *MultiChain.*

Mit Ausnahme der GuardTime-Blockchain sind alle Blockchain-Technologien als **Open Source (1)** Lösung konzipiert.[681] Open-Source-Implementierungen bringen den Entwicklern diverse Vorteile, wie bspw. die Minimierung von Entwicklungs- und Betriebskosten.[682] Darüber hinaus bieten Open-Source-Lösungen durch ihre interoperablen Schnittstellen eine einfache Implementierung in bestehende Ökosysteme und reduzieren so das Risiko eines Vendor-Lock-In.[683] Außerdem schafft die transparente Bereitstellung des Quellcodes eine Code-Security, die permanent durch eine Community überwacht wird und durch diese optimiert werden kann.[684] Dem gegenüber stehen die mit Open-Source verbundenen Herausforderungen.[685] So bedarf es bspw. einer ausreichenden Dokumentation der Lösung, die über die Kommentierung des Codes hinausgeht, sodass auch für einen Anwendungsfall relevante Anpassungen vorgenommen werden können.[686] Jede Weiterentwicklung führt dazu, dass die neueste Version nicht unbedingt mit der aktuellen Infrastruktur kompatibel ist und somit Auswirkungen auf der horizontalen sowie vertikalen Ebene einer Systemarchitektur hat.[687] Insbesondere beim

680 Unter *Sonstiges* fällt bspw. die Größe der Entwicklungs-Community (vgl. Macdonald/Liu-Thorrold/Julien (2017): 6), der Umfang der Dokumentation (vgl. Macdonald/Liu-Thorrold/Julien (2017): 6; Polge/Robert/Le Traon (2021): 230) sowie die Notwendigkeit von umfangreichem Vorwissen (vgl. Macdonald/Liu-Thorrold/Julien (2017): 6)

681 Bitcoin (vgl. Kuo/Zavaleta Rojas/Ohno-Machado (2019): 472), Ethereum (vgl. Kuo/Zavaleta Rojas/Ohno-Machado (2019): 472; Polge/Robert/Le Traon (2021): 230), Quorum (vgl. Polge/Robert/Le Traon (2021): 230), Hyperledger (vgl. Kuo/Zavaleta Rojas/Ohno-Machado (2019): 472; Polge/Robert/Le Traon (2021): 230), IOTA (vgl. Pinjala/Sivalingam (2019): 13) und MultiChain (vgl. Kuo/Zavaleta Rojas/Ohno-Machado (2019): 472; Polge/Robert/Le Traon (2021): 230).

682 Vgl. Phansalkar (2021): 35.

683 Vgl. Phansalkar (2021): 35.

684 Vgl. Phansalkar (2021): 35.

685 Neben den im weiteren Verlauf dargestellten Herausforderungen existieren weitere, die hier aufgrund ihrer Relevanz nicht weiter behandelt werden. So haben Institutionen bspw. das Problem, dass es viele unterschiedliche Lösungen am Markt gibt und sie nicht die notwendige Zeit haben, alle Lösungen zu begutachten (vgl. Stol/Ali Babar (2010): 18; Phansalkar (2021): 38). Auch die Migration bestehender Systeme in eine Open-Source-Lösung ist eine Herausforderung (vgl. Stol/Ali Babar (2010): 20f; Phansalkar (2021): 38).

686 Vgl. Stol/Ali Babar (2010): 18; Phansalkar (2021): 38.

687 Vgl. Stol/Ali Babar (2010): 20; Phansalkar (2021): 37.

Thema Weiterentwicklung und Support, der zwar auch von professionellen Dienstleistern übernommen werden kann, besteht eine Abhängigkeit von der Community, die ihre Stärke insbesondere im Falle von Sicherheitsrisiken im Code[688] aus dezentralem Wissen zieht.[689] Des Weiteren bedarf es einer permanenten Überwachung der Lizenzen, unter denen eine Open-Source-Lösung entwickelt wird, da sich diese Lizenzen mit der Zeit ändern und eine weitere Nutzung ausschließen können.[690] Die hier dargestellten Blockchain-Technologien Ethereum,[691] Hyperledger[692] und MultiChain[693] werden unter diversen GPL- und Apache-Lizenzen entwickelt.

Nicht jede Blockchain unterstützt den Einsatz von **Smart Contracts bzw. Chaincode (2)**. In der Bitcoin-Blockchain existiert keine Funktion, Prozesse automatisiert auszuführen,[694] und MultiChain erlaubt diese Funktion erst seit Version 2.[695] IOTA unterstützt seit Anfang 2021 Smart Contracts und orientiert sich dabei an Ethereum.[696] Ethereum (respektive Quorum[697]) sowie Hyperledger bieten diese Funktion. Ethereum-Smart-Contracts werden in der Solidity-, Serpent- und anderen Low-Level-Programmiersprachen entwickelt und erlauben so die Entwicklung von dezentralen Apps.[698] Hyperledger unterstützt mehrere Programmiersprachen, wie bspw. Java, Java Script und Go.[699] Doch Smart Contracts sind nicht für komplexe Zusammenhänge ausgelegt. Je komplexer ein Zusammenhang ist, desto größer wird der Smart Contract und desto länger dauert die Ausführung. Eine weitere Limitation betrifft explizit die Ethereum-Blockchain, die einen Aufruf externer Applikationen und REST-Services über Smart Contracts ausschließt. Hyperledger erlaubt hingegen diese Aufrufe.[700]

688 Vgl. Phansalkar (2021): 38.

689 Vgl. Stol/Ali Babar (2010): 19f; Phansalkar (2021): 37.

690 Vgl. Stol/Ali Babar (2010): 21; Phansalkar (2021): 36.

691 Lizenzen, abhängig von der Entwicklung (siehe Quelle): LGPL v3.0, GPL v3.0, MIT License, GPL v3.0, GPL v3.0 (vgl. Yu et al. (2019): 1269).

692 Lizenzen: Apache License v2.069 (vgl. Yu et al. (2019): 1269).

693 Lizenzen: GPL v3.070 (vgl. Yu et al. (2019): 1269).

694 Vgl. Agbo/Mahmoud (2019): e122.5; Kuo/Zavaleta Rojas/Ohno-Machado (2019): 471.

695 Vgl. Kuo/Zavaleta Rojas/Ohno-Machado (2019): 471; Polge/Robert/Le Traon (2021): 230.

696 Vgl. IOTA Foundation (2021b).

697 Vgl. Polge/Robert/Le Traon (2021): 230.

698 Vgl. Agbo/Mahmoud (2019): e122.5; Kuo/Zavaleta Rojas/Ohno-Machado (2019): 471; Yu et al. (2019): 1267, 1269; Polge/Robert/Le Traon (2021): 230.

699 Vgl. Agbo/Mahmoud (2019): e122.5; Kuo/Zavaleta Rojas/Ohno-Machado (2019): 471; Yu et al. (2019): 1268; Polge/Robert/Le Traon (2021): 229f.

700 Vgl. Ploom (2016): 144f.

Neben den bereits genannten Smart-Contract-Entwicklungssprachen unterscheiden sich Blockchain-Technologie entsprechend der zugrundeliegenden **Entwicklungssprache (3)**. Bitcoin, IOTA und MultiChain nutzen C++,[701] während bei Ethereum abhängig von der Entwicklung Go, Python, Java und weitere nicht näher genannte Sprachen zum Einsatz kommen.[702] Gleiches gilt für Hyperledger.[703] Guardtime dokumentiert keine explizite Entwicklungssprache, doch nennt die Möglichkeit, über entsprechende Software Development Kits (SDK) unterschiedliche Sprachen zu unterstützen.[704]

Blockchain-Technologien unterscheiden sich des Weiteren in der Wahl des zugrundeliegenden **Konsens-Protokolls (4).** Bitcoin und Ethereum nutzen den PoW-Konsens,[705] wobei Ethereum sich mittlerweile in Richtung PoS entwickelt. Ergänzend finden sich, mit Blick auf die durchgeführte Literaturanalyse, Tendenzen bei auf *Ethereum* basierenden Blockchain-Entwicklungen in Richtung BFT, FBA, Hashgraph, PBFT und QuorumChain. Bezüglich *Hyperledger* werden hingegen einzig BFT und PBFT identifiziert.[706] Konsens-Protokolle unterscheiden sich insbesondere im Rahmen der Fehlertoleranz, der Skalierbarkeit sowie im Ressourcenverbrauch. Während bspw. PoW, PoS und DPoS eine geringe Fehlertoleranz aufweisen,[707] ist diese bei PBFT höher.[708] Auch im Rahmen der Skalierbarkeit ist PBFT den drei anderen Protokollen unterlegen,[709] weil dieser Konsens auf eine hohe Performance ausgelegt ist.[710] Da im PBFT ein Knoten immer mit allen anderen Knoten kommuniziert, sind Netzwerkstrukturen stärker betroffen als bei den anderen Protokollen.[711] Hingegen verbraucht PoW aufgrund der komplizierten Berechnungsmethoden wesentlich mehr Energie im einzelnen Knoten.[712] Diesem Problem begegnen PoS und DPoS, indem sie durch ihre abweichende Implementierungslogik den Energiebedarf reduzieren.[713] Guardtime liefert keine Information zum zugrundeliegenden Konsensprotokoll. In der IOTA-Blockchain wird das Coordicide-Konsensprotokoll verwendet, das in keiner der bisher analysierten Publikationen Erwähnung findet. In diesem Protokoll wird für

[701] Vgl. IOTA Foundation (2017); Kuo/Zavaleta Rojas/Ohno-Machado (2019): 472; Yu et al. (2019): 1269.
[702] Vgl. Kuo/Zavaleta Rojas/Ohno-Machado (2019): 472; Yu et al. (2019): 1269.
[703] Vgl. Kuo/Zavaleta Rojas/Ohno-Machado (2019): 472; Yu et al. (2019): 1269.
[704] Vgl. Guardtime (2019).
[705] Vgl. Macdonald/Liu-Thorrold/Julien (2017): 7.
[706] Dieser Fokus wird ebenfalls von der Literatur bestätigt (vgl. Macdonald/Liu-Thorrold/Julien (2017): 9).
[707] Vgl. Zhang/Lee (2020): 95.
[708] Vgl. Zhang/Lee (2020): 95f.
[709] Vgl. Zhang/Lee (2020): 96.
[710] Vgl. Zhang/Lee (2020): 96.
[711] Vgl. Zhang/Lee (2020): 96.
[712] Vgl. Zhang/Lee (2020): 96.
[713] Vgl. Zhang/Lee (2020): 96.

jede in Konflikt stehende Transaktion ein Voting-System genutzt, das insbesondere Sicherheit gegenüber der Sybil-Attacke verspricht.[714] MultiChain beschreibt ein Consensus Protokoll, das ähnlich dem PBFT-Consensus ist.[715]

Jede Technologie schafft aufgrund des zugrunde gelegten Konsensprotokolls eine bestimmte **Anzahl an Transaktionen (5)**,[716] die einen limitierenden Faktor für deren Einsatz darstellen. Im direkten Vergleich ist die Bitcoin-Blockchain mit ihren 3,5 bis 7 Transaktionen pro Sekunde die langsamste Variante,[717] gefolgt von der Ethereum-Blockchain mit 10 bis 20 Transaktionen pro Sekunde.[718] IOTA[719] und MultiChain[720] schaffen bereits 1.000 bis zu 2.500 Transaktionen, während Hyperledger[721] und Guardtime[722] 100.000 Transaktionen pro Sekunde verarbeiten können. Für eine Gesundheitsdaten-Blockchain ist der tatsächliche Einsatzzweck entscheidend für die Auswahl der Blockchain-Technologie. Bei geringer Transaktionsmenge kann sich bereits die Bitcoin- und Ethereum-Blockchain eignen, wohingegen sich bspw. im Falle eines Echtzeit-Monitorings hochfrequente Blockchains wie Hyperledger und Guardtime eher eignen.[723]

Mit der Evaluation der Transaktionsmenge sind die Themen der **Transaktionskosten (6)** und **Skalierbarkeit (7)** verknüpft. Transaktionskosten sind insbesondere in der Verwendung des PoW-Konsenses hoch, da die Computing-Leistung zur Herstellung eines Hashs, unter der Voraussetzung, weitere Bedingungen zu erfüllen, mit zunehmender Transaktionshistorie zunimmt.[724] Hyperledger hat hingegen niedrige bis gar keine Transaktionskosten.[725] Genauso IOTA[726] und MultiChain[727]. Dem stehen Bitcoin und Ethereum gegenüber, die aufgrund ihrer Konstruktion Gebühren zur Validierung erheben.[728] Die Höhe der Transaktionskosten sowie

---

714 Vgl. IOTA Foundation (2019): 5f, 9f.

715 Vgl. MultiChain.com (2015): 7f.

716 Vgl. Agbo/Mahmoud (2019): e122.3.

717 Vgl. Ploom (2016): 140; Agbo/Mahmoud (2019): e122.5.

718 Vgl. Ploom (2016): 140; Agbo/Mahmoud (2019): e122.5.

719 Vgl. Cech (2021). In der Literaturquelle wird darauf hingewiesen, dass die Menge der möglichen Transaktionen mit der Menge an aktiven Nutzern positiv korreliert. In welchem Verhältnis dies geschieht, wird nicht weiter ausgeführt.

720 Vgl. MultiChain.com (o. J.).

721 Vgl. Ploom (2016): 140; Agbo/Mahmoud (2019): e122.5.

722 Vgl. Ploom (2016): 139.

723 Vgl. Agbo/Mahmoud (2019): e122.3.

724 Vgl. Agbo/Mahmoud (2019): e122.4-5. An dieser Stelle wird erneut auf die Aktualisierung des Ethereum-Konsenses von PoW auf PoS hingewiesen. Folglich sinken die Transaktionskosten.

725 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 9.

726 Vgl. IOTA Foundation (2017).

727 Vgl. Greenspan (2015): 8.

728 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 8.

die Menge an Transaktionen pro Sekunde erlauben einen Rückschluss auf die Skalierbarkeit der jeweiligen Technologie. Bitcoin- und MultiChain weisen aufgrund der steigenden Komplexität mit Zunahme der Transaktionsmenge eine geringe Skalierbarkeit auf.[729] Ethereum und Quorum basieren im Grunde auf dem gleichen Konsensmechanismus, bieten aber aufgrund des Konzepts und des Wechsels auf den PoS-Konsens eine höhere Skalierbarkeit.[730] Hyperledger bietet zusammen mit IOTA die höchste Skalierbarkeit.[731] Guardtime liefert keine Informationen über das zugrundeliegende Konsensprotokoll und damit verbundenen Transaktionskosten, verspricht aber eine hohe Skalierbarkeit.[732]

Security (8) betrachtet die Vorkehrungen, Identitäten anonym zu halten und Transaktionsdaten nur berechtigten Personen zu offenbaren.[733] Tatsächlich muss berücksichtigt werden, dass insbesondere öffentliche Blockchains, wie Ethereum und Bitcoin, sämtliche Daten öffentlich bereitstellen, sodass grundsätzlich keine sensiblen Informationen direkt auf der Blockchain gespeichert werden sollten.[734] Hyperledger adressiert hingegen konkret die Anonymität der Nutzer und stellt ergänzend Zugriffskontrollen und Mechanismen der Netzwerksicherheit zur Verfügung.[735] Guardtime erlaubt wegen des kommerziellen Fokus keine unabhängige Prüfung der Sicherheit. Mit Blick auf die technische Konstruktion und das Konstrukt der KSI ergibt sich ein gewisses Security-Potential, doch die fehlende Information zum Konsensprotokoll ermöglicht keine einwandfreie Analyse der Sicherheit. Grundsätzlich existieren für alle Technologien allgemeine mit der Blockchain einhergehende Sicherheitsrisiken, die detailliert in *Kapitel 8.3.4* beschrieben werden.

Nicht jede Blockchain-Technologie nutzt **Token bzw. Coins (9).** Die Bitcoin-Blockchain, die ihren Ursprung in der Bereitstellung einer Alternativwährung hat, stellt folglich Coins bereit, die sogenannten Bitcoins, und incentiviert mit diesen den Aufwand der Rechenknoten (Miner).[736] Dabei existiert ein rechnerisches Limit von 21 Millionen Bitcoins.[737] Ähnlich ist es

729 Vgl. Agbo/Mahmoud (2019): e122.5; Oliveira et al. (2019): 187.

730 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 7; Agbo/Mahmoud (2019): e122.5.

731 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 8f; Agbo/Mahmoud (2019): e122.5; Hou/Tang/Liang (2020): 1610.2.

732 Vgl. Shorthouse/Xie (2020): 9.

733 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 6.

734 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 8.

735 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 9.

736 Vgl. Agbo/Mahmoud (2019): e122.5.

737 Vgl. Kuo/Zavaleta Rojas/Ohno-Machado (2019): 471.

bei der Ethereum-Blockchain, deren Währung *Ether*[738] genannt wird und ebenfalls zur Incentivierung der Miner genutzt wird. Als Incentivierungsinstrument wird *Ether* allerdings als *Gas* bezeichnet.[739] Anders als bei der Bitcoin-Blockchain existiert hier kein Limit.[740] Auch können Entwickler ergänzend zu Ether eigene Währungen implementieren, die auf ihren Anwendungsfall angepasst sind.[741] IOTA incentiviert Netzwerkteilnehmer nicht durch einen Coin. Stattdessen stärkt die Mitwirkung am Netzwerk die Rolle des Netzwerkteilnehmers und ermöglicht diesem den Zugang und die Nutzung der Blockchain.[742] Obwohl Quorum auf der Ethereum Blockchain basiert und nur eine private Ausgliederung ist, wird hier auf den Einsatz von Token bzw. Coins verzichtet.[743] Auch MultiChain[744], Guardtime und Hyperledger[745] verzichten auf Coins. Eine Incentivierung findet folglich nicht bzw. nicht über die Blockchain statt.[746]

Unter das Evaluationskriterium **Sonstiges (10)** fällt bspw. die Größe der Entwicklungs-Community,[747] der Umfang der Dokumentation[748] sowie die Notwendigkeit von umfangreichem Vorwissen.[749] Ethereum und Hyperledger bieten Entwicklern eine umfangreiche Dokumentation über Online-FAQs, Git-Repositories, Whitepaper und Community-Diskussionen. Neuentwicklungen folgen einer definierten Roadmap und finden so auch den Weg in die Produktivumgebung, wodurch sie einen Vorteil gegenüber der Bitcoin-Blockchain haben.[750] Bei dieser wird zwar auch auf die vorhandene Dokumentation und Community hingewiesen, doch fehlt es für Neuentwicklungen an einer konsequent verfolgten Roadmap. Stattdessen verlieren sich Entwickler in Diskussionen.[751] Neben den öffentlichen Communities stehen hinter den Technologien bspw. die *Ethereum Foundation* für Ethereum,[752] für Quorum ergänzend *JPMorgan*

738 Vgl. Polge/Robert/Le Traon (2021): 230.

739 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 8; Agbo/Mahmoud (2019): e122.5.

740 Vgl. Kuo/Zavaleta Rojas/Ohno-Machado (2019): 471.

741 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 8.

742 Vgl. IOTA Foundation (2021a). Am Kryptowährungs-Markt existiert ein MIOTA-Coin, der auf der IOTA-Blockchain basiert. Allerdings wird dieser nicht im Zusammenhang mit der Incentivierung von Netzwerkteilnehmern erwähnt und findet sich tatsächlich nur im Kryptowährungs-Kontext.

743 Vgl. Polge/Robert/Le Traon (2021): 230.

744 Vgl. Kuo/Zavaleta Rojas/Ohno-Machado (2019): 471; Polge/Robert/Le Traon (2021): 230.

745 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 9; Kuo/Zavaleta Rojas/Ohno-Machado (2019): 471; Polge/Robert/Le Traon (2021): 230.

746 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 9; Agbo/Mahmoud (2019): e122.5.

747 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 6.

748 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 6; Polge/Robert/Le Traon (2021): 230.

749 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 6.

750 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 7; Macdonald/Liu-Thorrold/Julien (2017): 8.

751 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 7.

752 Vgl. Macdonald/Liu-Thorrold/Julien (2017): 6; Polge/Robert/Le Traon (2021): 230.

Chase,[753] *Linux Foundation* für Hyperledger[754], IOTA Foundation für IOTA[755] und *Coin Sciences* für MultiChain,[756] die in der Entwicklung unterstützen bzw. die o.g. Roadmap umsetzen. Aufgrund der in Punkt (3) bereits dargestellten zugrundeliegenden Entwicklungssprachen der Technologien müssen Entwickler bei einer Nutzung der Technologien zudem keine neuen Programmiersprachen erlernen.[757]

Sämtliche Ergebnisse dieses Vergleichs werden unter Berufung auf die in *Tabelle 8-4* identifizierten Evaluationskriterien in *Tabelle 8-5* zusammengefasst.

Tabelle 8-5: Vergleichsergebnis der Blockchain-Technologien (Quelle: Eigene Darstellung)

Nr.	Bitcoin	Ethereum	Quorum	Guard-Time	Hyper-ledger (Fabric)	IOTA	MultiChain
1	✓	✓	✓	x	✓	✓	✓
2	x	✓	✓	x	✓	✓	✓ (v2)
3	C++	Go, Python, Java, Rust	Go, Python, Java, Rust	*SDKs*	Go, Python	C++	C++
4	PoW	PoW, PoS, BFT, FBA, Hashgraph, PBFT	Quorum-Chain	Keine Informationen	BFT, PBFT	Coordicide	Nicht definiert, ähnlich PBFT
5	3,5 - 7	10 - 20	10 - 20	100.000	100.000	1.000	2.000 - 2.500
6	Hoch	Hoch, aber sinkend	Hoch	Keine Informationen	Niedrig	Niedrig	Niedrig
7	Niedrig	Niedrig, aber steigend	Niedrig, aber steigend	Hoch	Hoch	Hoch	Niedrig
8	Niedrig	Niedrig	Niedrig	Niedrig	Hoch	Niedrig	Hoch
9	Vorhanden. Auf 21 Mio. limitiert	Vorhanden, kein Limit	Keine	Keine	Keine	MIOTA nur als Kryptowährung	Keine
10	Große Community, unklare Entwicklungsprozesse	Große Community, Entwicklungsroadmap, Freie Community & Ethereum Foundation	Entwicklungsroadmap, Ethereum Foundation & JPMorgan Chase	Keine Community, GuardTime verkauft sich als Dienstleistung	Community, Entwicklungsroadmap, Linux Foundation	Entwicklungsroadmap, IOTA Foundation	Entwicklungsroadmap, Coin Sciences

[753] Vgl. Polge/Robert/Le Traon (2021): 230.

[754] Vgl. Polge/Robert/Le Traon (2021): 230.

[755] Vgl. IOTA Foundation (2017).

[756] Vgl. Polge/Robert/Le Traon (2021): 230.

[757] Vgl. Macdonald/Liu-Thorrold/Julien (2017): 6.

8.3.4 Exkurs: Risiko-Szenarien auf Gesundheitsdaten-Blockchains

Die Umsetzung der Gesundheitsdatenvernetzung mit der Blockchain-Technologie ist grundsätzlich sämtlichen mit der Blockchain-Technologie einhergehenden technologischen Risiken ausgesetzt, deren Umfang wiederum von der in der Umsetzung gewählten Technologie abhängig ist. In der analysierten wissenschaftlichen Literatur werden insbesondere folgende Risiken identifiziert, deren Verteilung in *Abbildung 8-5* dargestellt wird:

i. 51%-Attack
ii. Double Spending
iii. Eclipse Attack
iv. Preimage Attack
v. Quanten-Computer
vi. Root-Exploit
vii. Sybil-Attack

Dabei ist zu erkennen, dass die Literatur insbesondere in der *51%-Attack* und der Entwicklung von *Quanten-Computern* ein Risiko sieht, wobei Ersteres sich mit der Macht eines einzelnen Stakeholders in einem Netzwerk beschäftigt und Letzteres die Verschlüsselungsmethoden infrage stellt, da die Computing-Performance von Quanten-Computern Verschlüsselungen dechiffrieren könnte.

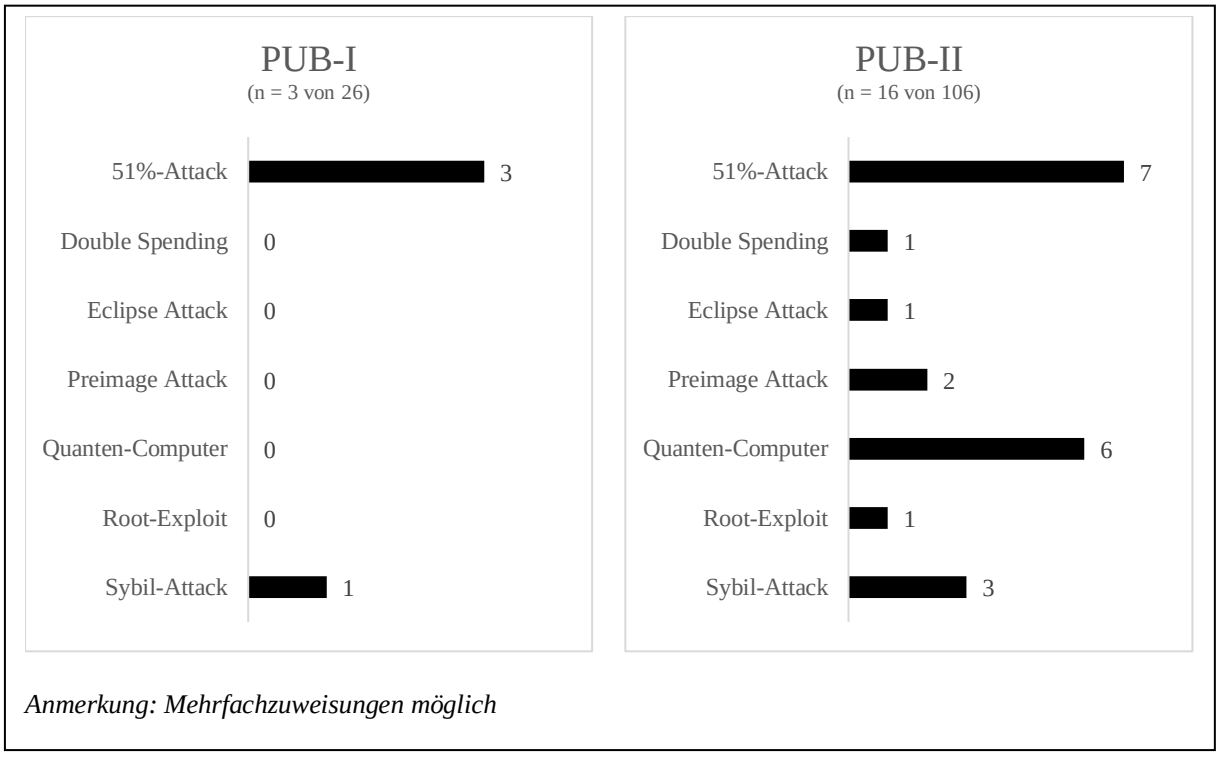


Abbildung 8-5: Verteilung der beschriebenen Angriffsmöglichkeiten (Quelle: Eigene Darstellung)

51%-Attack (i) ist die am häufigsten in PUB-I und PUB-II genannte Möglichkeit, dem Blockchain-Netzwerk Schaden zuzufügen.[758] Hintergrund ist die Annahme, dass in einem Netzwerk 51% der verfügbaren Leistungsfähigkeit durch einen einzigen Knoten aufgebracht wird und dieser folglich den Inhalt der Blockchain-Transaktionen nachträglich verändern und diese Änderung eigenständig validieren kann.[759] Mit sinkender Menge an Knoten, die in einem Blockchain-Netzwerk aktiv sind, steigt die Gefahr.[760] Eine Lösung ist der Einsatz von *Permissioned Blockchains*[761] oder genauer *Private Blockchains*[762], denn dort sind nicht nur die Netzwerkteilnehmer bekannt, sondern auch die Computing-Leistung zielstiftend auf Miner aufgeteilt..[763]

Double Spending (ii) beschreibt das Problem, dass der Besitz an einer Sache mehrfach übertragen wird, obwohl diese Sache nur einmal existiert. Im Zusammenhang mit Bitcoin wäre dies die Durchführung von zwei Zahlungen, obwohl nur eine Zahlung berechtigt ist.[764] In Bezug auf Gesundheitsdaten ist dieses Problem ausschließlich im Falle von Übertragungen monetärer Einheiten von Relevanz.

Eclipse Attack (iii) beschreibt das Problem, dass sämtliche Knoten im direkten Umfeld eines Ausgangsknotens nicht vertrauenswürdig sind. Diese sind entweder grundsätzlich nicht vertrauensvoll oder suggerieren Vertrauen, obwohl sie über eine manipulierte Liste von Ein- und Ausgangs-IP-Adressen angesprochen werden.[765]

Preimage Attack (iv), zu Deutsch *Urbild-Angriff*, verfolgt nicht das Ziel, bestehende Blöcke einer Blockchain zu verändern, sondern schneller als das Netzwerk neue Blöcke zu erstellen, sodass die eigene Blockchain als längste und damit valide Blockchain wahrgenommen wird.[766]

Quanten-Computer (v) sind in PUB-I kein Thema, jedoch in den PUB-II ähnlich relevant wie die 51%-Attacke. Dabei wird darauf hingewiesen, dass Quanten-Computer die Fähigkeit besitzen, Verschlüsselungen, auch asymmetrische Verschlüsselungen, aufgrund ihrer gesteigerten

---

758 Vgl. Swan (2015): 85; Kuo/Kim/Ohno-Machado (2017): 1217; Sixt (2017): 105f; Kamel Boulos/Wilson/Clauson (2018): 25.8; Meinel/Gayvoronskaya/Schnjakin (2018): 49-51.

759 Vgl. Yli-Huumo et al. (2016): e0163477.14–15; Kuo/Kim/Ohno-Machado (2017): 1217; Lazar et al. (2017): 4; Kamel Boulos/Wilson/Clauson (2018): 25; Kuo/Ohno-Machado (2018): 9; Liu et al. (2018): 6190; Radanović/Likić (2018): 584; Zhang/Lin (2018): 140.12.

760 Vgl. Yli-Huumo et al. (2016): e0163477.3–4.

761 Vgl. Kuo/Kim/Ohno-Machado (2017): 1217; Zhang et al. (2018b): 276.

762 Vgl. Kuo/Ohno-Machado (2018): 10; Zhuang et al. (2018): 1170.

763 Vgl. Radanović/Likić (2018): 584.

764 Vgl. Rahmadika/Rhee (2018): 10.

765 Vgl. Rahmadika/Rhee (2018): 8-10.

766 Vgl. Brogan/Baskaran/Ramachandran (2018): 260; Rahmadika/Rhee (2018): 11.

Leistungsfähigkeit zu entschlüsseln,[767] einen Hash-Wert wieder in seinen Original-Inhalt zurückzuführen[768] sowie mittels Hash-Collision-Attacks eine Original-Nachricht durch einen gleich lautenden Hash-Wert einer anderen Nachricht auszutauschen.[769] Zur Abwehr dieses Risikos wird auf den Einsatz des IOTA-Protokolls verwiesen, das nur Einmal-Signaturen verwendet.[770] Alternativ kann auch eine Verschlüsselung entsprechend eines Revocable-Attribute-based-Key-Agreement (RAKA) genutzt[771] oder komplett auf Schlüssel (Keyless Signature Infrastructure (KSI)) verzichtet werden.[772]

Root-Exploit (vi) beschreibt eine der gefährlichsten Malware-Varianten, die sich im Kernel des vom Node genutzten Endgeräts einnistet und bereits vor Nutzung einer Blockchain-Infrastruktur unautorisierte Änderungen vornimmt, sodass bereits fehlerhafte Daten oder Zugriffsbeschränkungen dem Netzwerk kommuniziert werden.[773]

Sybil-Attack (vii) beschreibt den Fall, dass eine einzige Entität in einem Blockchain-Netzwerk mehrere Identitäten besitzt, aber allen anderen Teilnehmern suggeriert, dass sämtliche Identitäten unabhängig voneinander sind.[774] Folglich wird, ähnlich wie bei einer 51%-Attacke, ein negativer Einfluss auf die Vertraulichkeit und Integrität des Netzwerks genommen. Auch dieser möglichen Attacke können *Permissioned Blockchains* bzw. ein zentralisiertes Mitgliedsmanagement entgegenwirken.[775]

8.4 Szenarien-basierte Diskussion und Ableitung von Handlungsempfehlungen

8.4.1 Szenario 1: Eine lebenslang geführte einrichtungsübergreifende Patientenakte

8.4.1.1 Einführung, Anforderungsaufnahme und Methodik

Das in diesem Kapitel behandelte Szenario beschreibt die Konstruktion einer über die von der GEMATIK beschriebenen elektronischen Patientenakte hinausgehenden persönlichen Patientenakte. Der Zeithorizont wird auf das gesamte Leben eines Patienten ausgeweitet und das von

[767] Vgl. Bayle et al. (2018): 790.

[768] Vgl. Alhadhrami et al. (2017): 376.

[769] Vgl. Liang et al. (2018a): e3.4.

[770] Vgl. Brogan/Baskaran/Ramachandran (2018): 259.

[771] Vgl. Wang et al. (2018a): 14.

[772] Vgl. Liang et al. (2017a): 470.

[773] Vgl. Firdaus et al. (2018): 112.3-4.

[774] Vgl. Alhadhrami et al. (2017): 376; Kuo/Ohno-Machado (2018): 2; Meinel/Gayvoronskaya/Schnjakin (2018): 51; Rahmadika/Rhee (2018): 10f.

[775] Vgl. Dubovitskaya et al. (2017): 657.

SHABO beschriebene Konzept der *Independent Health Record Bank* aufgegriffen. Die von SHABO gewählte Ausrichtung richtet den Fokus für die Auswahl und Evaluation der Konstruktionsentscheidungen auf *Personal Health Records (PHR)*, die anders als *Electronic Health Records (EHR)* die Moderation der Zugriffe dem Patienten überlassen.[776] Ergänzend werden Variationspunkte für Versicherungen und klinische Forschung berücksichtigt, da diese auch in der von der GEMATIK beschriebenen Lösung (beschränkten) Zugriff auf Gesundheitsdaten erhalten.[777]

Bekanntermaßen ist das Ziel der IHRB die Entkopplung der Gesundheitsdaten von Partikularinteressen der diese Daten erhebenden Parteien (Leistungserbringer, Kostenträger, Private Unternehmen) und Konzentrierung der Datenhaltungs- und Analysekompetenzen in einem bzw. mehreren spezialisierten und voneinander unabhängigen Instituten.

Die dort vorgehaltenen Daten werden in Konten geführt, ähnlich den Bankkonten im Finanzsektor. Dieser Vergleich mit Bankkonten begründet zugleich die Relevanz der Blockchain-Technologie in der Anwendungsdomäne des digitalen Gesundheitswesens. Eine Gegenüberstellung von HRB[778] und Finanzinstituten findet sich in *Tabelle 8-6*.

Tabelle 8-6: Commercial banking compared with health-record banking (Quelle: Gold/Ball (2007): 46)

	Commercial Banking	**Health-Record Banking**
Account holders		
Small	Personal or joint	Individual, joint, or family personal health records
Medium-sized	Small and medium-sized businesses	Solo physicians, group practices, pharmacies, etc.
Large	Corporations	HMOs, hospitals, etc.
Types of accounts	Savings, checking, safe deposit services, IRA, etc.	Text health record, imaging, audiovisual/monitoring, laboratory/pathology, genomic record
Bank types	Savings, savings and loan, credit union, investment, etc.	Full-service bank, genomic speciality bank, physician services bank, etc.
Chief revenue sources	Investment, lending, etc.	Member services, lease of deidentified data, disaster recovery plans, speciality services, health kiosks, health-record curation, etc.

HMO: Health Maintenance Organization
IRA: Individual Retirement Account

776 Vgl. Shabo (2006b): 500.

777 Siehe Zonen-Separierung in *Kapitel 2.3.1*.

778 HRB sind gleichzusetzen mit IHRB. Der fehlende Buchstabe *I*, der für *Independent* steht, bezeichnet bloß eine Eigenschaft der HRB, sodass dieser Buchstabe für die hier dargestellte Gegenüberstellung keine Relevanz hat.

Daraus ergibt sich, dass die Motivation der ursprünglichen Bitcoin-Blockchain, Banken zu ersetzen, ebenfalls auf ein Szenario angewendet werden kann, das die für eine lebenslang geführte Patientenakte proklamierten IHRB ersetzt.

Unter diesen Gesichtspunkten wird für eine potentielle Blockchain-Lösung zur Ablösung von IHRB folgende Kernanforderungen abgeleitet:[779]

(1) Speicher sämtlicher Gesundheitsdaten (EHR)[780]
(2) Interoperabilität, sodass Daten konsistent übermittelt, verarbeitet und gelesen werden[781]
(3) Zugriffskontrolle, sodass Gesundheitsdaten nicht missbräuchlich verwendet werden[782]
(4) Zugriffsmöglichkeiten für Kostenträger für den Abruf abrechnungsrelevanter Daten
(5) Zugriffsmöglichkeiten für Forschungseinrichtungen für den Abruf (anonymisierter) forschungsrelevanter Daten

Die Evaluation der Handlungsempfehlungen, die sich aus der konzipierten Referenzarchitektur und dem Entscheidungsmodell ergeben, wird durch Analyse aktueller Literatur vorgenommen, die im Zeitraum von Januar 2019 bis Juli 2021 in der Suchmaschine GoogleScholar identifiziert wird. Dieser Zeitraum liegt nach dem für die Literaturanalyse verwendeten Zeitraum. Dabei werden mehrere Suchwort-Kombinationen genutzt und jeweils die ersten 10 Seiten der Suchergebnisse betrachtet:[783]

i. *phr* AND *blockchain*
ii. *clinical trial* AND *blockchain*
iii. *health insurance* AND *blockchain*

Um Verwechslungen zwischen der Basis-Literatur zur Konstruktion der Referenzarchitektur und der neuen Validierungs-Literatur zu vermeiden, wird im Folgenden der Begriff *Scholar-Literatur* für die gesamte seit Januar 2019 identifizierte Literatur genutzt.

8.4.1.2 Sicht: Data Storage & Provisioning

Ausgehend von der Annahme, einen PHR zu ersetzen, erlaubt die konzipierte Referenzarchitektur und das damit verbundene Entscheidungsmodell die Auswahl diverser Variationen. Bei der Entscheidung, ob eine *on-chain*- oder *off-chain-Lösung* gewählt wird, wird entsprechend

[779] Die hier dargestellten Anforderungen entsprechen der Anforderung an eine IHRB und stellen noch keine finale Konzeption mittels Blockchain dar.

[780] Vgl. Shabo (2006b): 500.

[781] Vgl. Shabo (2006b): 503. Der Fokus liegt dabei auf HL7, DICOM und CEN (vgl. Shabo (2006b): 503f.).

[782] Vgl. Shabo (2006b): 502.

[783] Die Auswahl der in diesem Fall relevanten Literatur wird durch Analyse von Titel und Abstract der Suchergebnisse durchgeführt und folgt somit dem ursprünglichen Ansatz der Literaturanalyse.

dem Entscheidungsmodell eine *off-chain*-Lösungen präferiert, auch wenn vereinzelt Beschreibungen in der Literatur existieren, die auf on-chain-Lösungen setzen.[784] Insbesondere die Datenschutz-Relevanz bei Gesundheitsdaten motiviert zur Speicherung von Daten außerhalb der Blockchain und zur Verwaltung von Metadaten eben dieser Gesundheitsdaten auf der Blockchain. Doch auch der Blick auf die zu erwartenden Datenmenge begründet diesen Schritt. So würde unter Annahme der in *Kapitel 8.2.2* ermittelten Durchschnittsdatenmenge von 2,7 GB pro Patient eine Gesamtdatenmenge von 224,55 Petabyte (PB) entsprechend der in *Formel (3)* dargestellten Kalkulation ergeben:

$$2{,}7\ GB * 83.166.711 \approx 224.550.120\ GB \approx 224{,}55\ PB \qquad \textbf{Formel (3)}$$

Diese Datenmenge würde in einem Blockchain-Netzwerk auf jedem Knoten repliziert, sodass Patient, Leistungserbringer, Kostenträger oder Forschungseinrichtung diese Information lokal abfragen kann. Bereits in diesem Stadium ist ersichtlich, dass eine *on-chain*-Datenhaltung für Gesundheitsdaten aufgrund der zu erwartenden Datenmenge nicht in Frage kommt.[785] Zu diesem Ergebnis kommt ebenfalls die *Scholar-Literatur*, die grundsätzlich eine von der Blockchain extern geführte Datenhaltung (off-chain) vorzieht.[786]

Aus der Entscheidung für off-chain-Datenhaltung mit Metadatenspeicher auf der Blockchain ergibt sich als nächste mögliche Variation die physischen Datenhaltung. Diese wird entweder in einer *Cloud*, einer zentral organisierten Datenbank, oder mittels IPFS durchgeführt. Auch das Thema Interoperabilität und die Verwendung von Standards sind hier relevant. Im direkten Vergleich ist IPFS im Entscheidungsmodell von geringerer Bedeutung und wird daher zunächst nicht in die Handlungsempfehlungen aufgenommen.

In der *Scholar-Literatur* setzt sich Cloud nach wie vor als Datenspeicher durch.[787] Obwohl spärlich in der Architektur-Entwicklungs-Literatur erwähnt, wird IPFS aufgrund der steigenden

---

[784] Diese Quellen gehen in der Konzeptionsbeschreibung weniger detailliert auf tatsächliche Umsetzungen ein. So beschreiben zum Thema *Datenhaltung* von vier Publikationen einzig AHRAM ET AL. (2017) den Einsatz einer Cloud und ZHANG/LIN (2018) die mögliche Interoperabilität, während sämtliche anderen Publikationen keine tiefergehende Beschreibung vornehmen.

[785] Die hier dargestellten Zahlen spiegeln zudem nur den Status des approximierten Wertes für das Jahr 2020 wider. Unter Berücksichtigung einer Steigerungsrate von 48% (siehe *Kapitel 8.2.2*) wird diese Menge stetig wachsen.

[786] Vgl. Franceschi et al. (2019): 589; Hylock/Zeng (2019): e13592.5; Chenthara et al. (2020): e0243043.7; Kung et al. (2020): 1782; Madine et al. (2020a): 193105; Ruggeri et al. (2020): 118; Wang et al. (2020): 59; Wu et al. (2020): 344; Yang et al. (2020b): 45471; Meier et al. (2021): 23; Rajput/Li/Ahvanooey (2021): 206.8; Uddin et al. (2021): 2384, 2391.

[787] Vgl. Wang/Zhang/Zhang (2019): 102891; Quasim et al. (2020): 607; Ruggeri et al. (2020): 117; Wang/Luo/Zhou (2020): 3; Yang et al. (2020b): 45471; Yang et al. (2020a): 70607.

Anzahl an Nennungen in der *Scholar-Literatur* nun doch in die Handlungsempfehlungen aufgenommen.[788] Dem gegenüber steht, dass, obwohl im Entscheidungsmodell das Thema *zentrale Datenbank* genannt wird, dies durch keine der neuen Publikationen bestätigt wird. Das Thema Interoperabilität durch die Verwendung von Standards ist weiterhin von Bedeutung, insbesondere die Standards *FHIR*[789], *HL7*[790] und *openEHR*[791].

Bei der Bereitstellung von Daten spielen entsprechend dem Entscheidungsmodell *Pointer bzw. Links* zur Lokalisierung der Gesundheitsdaten sowie Indizes und Gatekeeper eine Rolle, wobei die Bereitstellung von Pointern aufgrund des Fokus auf off-chain-Datenspeicher dominiert.

In der *Scholar-Literatur* spiegelt sich dieser Fokus ebenfalls wider.[792] Die Erstellung eines Index wird erwähnt, jedoch nicht umfänglich behandelt. Die Bereitstellung von Daten über Gatekeeper findet keine Berücksichtigung.

Unter Einbezug von Anforderung (3) und (4), also der Einbindung von Forschung und Kostenträgern, ergibt sich entsprechend dem Entscheidungsmodell die Möglichkeit, on-chain-Datenspeicherung in die Liste der potentiellen Variationen aufzunehmen.[793] Da die Grundlagenliteratur des Entscheidungsmodells zahlungsrelevante Informationen auf der Blockchain verwaltet, wird in diesem Fall davon ausgegangen, dass diese Informationen auf der Blockchain ergänzend zu den Metadaten der konkreten Gesundheitsdaten gespeichert werden, ohne dabei das Rohmaterial in der Blockchain vorzuhalten.

Die Berücksichtigung forschungsrelevanter Daten führt zu keinen neuen Erkenntnissen. Es bleibt bei off-chain-Speicherung in der Cloud oder mittels IPFS, während Pointer auf der Blockchain gespeichert werden.

Das Entscheidungsmodell folgt ebenfalls der *Scholar-Literatur*, sodass zahlungsrelevante Informationen der Kostenträger on-chain[794] gespeichert sowie forschungsrelevante Daten off-

[788] Vgl. Shahnaz/Qamar/Khalid (2019): 147788; Chenthara et al. (2020): e0243043.7; Madine et al. (2020b): 225780; Madine et al. (2020a): 193105f; Wu et al. (2020): 344.

[789] Vgl. Hylock/Zeng (2019): e13592.5; Kung et al. (2020): 1782.

[790] Vgl. Fatokun/Nag/Sharma (2021): 580.6.

[791] Vgl. Roehrs et al. (2019): 103140.3.

[792] Vgl. Guo et al. (2019): 44; Wang et al. (2020): 58; Wang et al. (2020): 59; Yang et al. (2020b): 45471.

[793] Die in dieser Dissertation beschriebene Konzeption, abrechnungsrelevante Daten bereitzustellen, greift dabei auf Informationen auf der Blockchain zurück, um ihre eigenen Zahlungsprozesse zu verwalten.

[794] Vgl. Mackey et al. (2020): 7.

chain[795] vorgehalten und entweder in der Cloud[796] oder mittels IPFS[797] bereitgestellt werden. Ein Verweis in Form von Pointern wird on-chain gespeichert.[798]

Im Rahmen der Interoperabilitäts-Diskussion ergibt sich ebenfalls keine Veränderung der bereits für PHR identifizierten Handlungsempfehlungen. Der Schwerpunkt der Kostenträger-relevanten Datenbereitstellung liegt auf den Standards *HL7* bzw. *FHIR*.[799] Für forschungsrelevante Daten können diverse Interoperabilitäten definiert werden.[800] Dies ist der Grund, weshalb in *Abbildung 8-6* keine konkrete Markierung auf *HL7* bzw. *FHIR* vorgenommen, sondern die Wahl des Interoperabilitätsstandards offengelassen wird. Auch in diesem Fall stimmen Entscheidungsmodell und *Scholar-Literatur* überein.[801]

Sämtliche Handlungsempfehlungen des Entscheidungsmodells, korrigiert um die neuen Erkenntnisse aus der *Scholar-Literatur*, sind in *Abbildung 8-6* dargestellt.

795 Vgl. Omar et al. (2019): 3; Zhuang et al. (2020a): e19029.4.

796 Vgl. Hirano et al. (2020): e18938.2.

797 Vgl. Omar et al. (2019): 3.

798 Vgl. Zhuang et al. (2020a): e19029.4.

799 Vgl. Mackey et al. (2020): 5.

800 Vgl. Zhuang et al. (2020a): e19029.4. Die Autoren beschreiben eine Technik, bei der Netzwerkteilnehmer die Wahl des für ihn relevanten Interoperabilitäts-Standards hat und entsprechend die Pointer definiert.

801 Die relevante *Scholar-Literatur* ist in diesem Absatz den Ausführungen des Entscheidungsmodells als Fußnote angehängt.

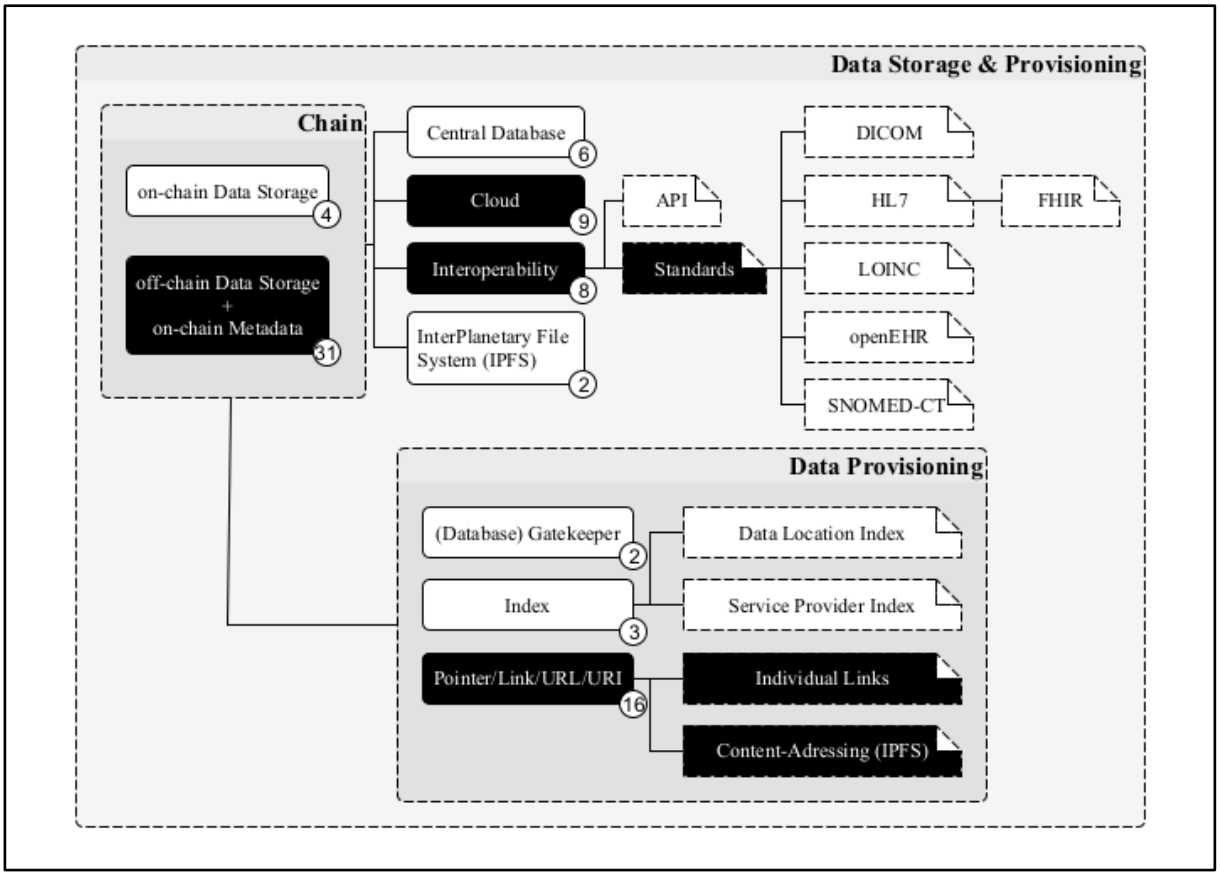


Abbildung 8-6: Patientenakten-Handlungsempfehlungen für ‚Data-Storage-& Provisioning'-Variationen der Referenzarchitektur
(Quelle: Eigene Darstellung)

8.4.1.3 Sicht: Security

In der Sicht *Security* sind unter Anwendung des Entscheidungsmodells sämtliche Aspekte der *Authorization*, *Authentication*, *Infrastructure* und *Logging* maßgeblich.

Beginnend mit *Authorization* sind alle Access-Control-Techniken, bis auf EBAC, von Bedeutung. Schwerpunkt ist dabei die Nutzung von RBAC, deren Fokus sich allein auf die Rolle eines Akteurs beschränkt und entsprechend die Rechtevergabe definiert. Im Hinblic auf die aktuellen Entwicklungen in der *Scholar-Literatur* reduziert sich diese Liste an Access-Control-Techniken jedoch auf *ABAC*[802] und *RBAC*[803].

[802] Vgl. Guo et al. (2019): 46.

[803] Vgl. Chenthara et al. (2020): e0243043.14.

Im Rahmen der *Authentifizierung* finden attribut- sowie identitätsbasierte Verfahren Anwendung. Diese verwenden Benutzername und Passwort[804] oder biometrische Daten zur Authentifizierung.[805] Dabei speichert die eingesetzte Blockchain sämtliche identitäts- und zugriffsrelevanten Informationen.[806] Diese Informationen werden innerhalb von Einrichtungen der Leistungserbringer erzeugt und mit der Realidentität eines Akteurs verknüpft, mindestens aber gegengeprüft.[807] Sie dienen in der Folge der in der zugrundeliegenden *PKI*[808] notwendigen *Certificate Authority*[809] und garantieren so die Validität der entsprechenden Authentifizierung. Neben der Erstellung eines *Master Patient Index* wird zudem über die Möglichkeit diskutiert, dass ein Patient mehrere Identitäten im Netzwerk nutzen kann.[810] Sämtliche Inhalte finden sich in der *Scholar-Literatur* wieder.[811] Der Schwerpunkt liegt im Entscheidungsmodell wie auch in der *Scholar-Literatur* auf dem Einsatz von TTPs, sodass die Identität eines Patienten zweifelsfrei nachgewiesen werden kann. Neben dem Einsatz einer *PKI* hält nun auch *KSI* Einzug in die Liste der Handlungsempfehlungen.[812]

Bei *Logging & Audit* wird die Blockchain vorrangig als Speicher für Hash-Werte einzelner Daten zur Integritätssicherung genutzt und zweitrangig als Log für Zugriffe bzw. Zugriffsberechtigungen. Ein Log über einzelne Transaktionen ist ein nachrangiges Ziel im Rahmen des Entscheidungsmodells. Dieser Erkenntnis folgt auch die *Scholar-Literatur*, die Blockchain weiterhin als Logging-Instrument für sämtliche Transaktionen und Zugriffs-Regeln[813] sowie zur auditsicheren Speicherung von Datei-Hashes nutzt.[814] Aufgrund dessen, dass hier keine Ableitung von Schwerpunkten möglich ist, bleibt es bei der Annahme, dass Blockchain zwar in der

804 Vgl. Chenthara et al. (2020): e0243043.14; Chelladurai/Pandian (2021): 5.

805 Vgl. Zhuang et al. (2020b): 2172.

806 Vgl. Cernian et al. (2020): 6538.10; Yang et al. (2020a): 70605.

807 Vgl. Guo et al. (2019): 46; Cernian et al. (2020): 6538.13; Madine et al. (2020b): 225786; Chelladurai/Pandian (2021): 5.

808 Vgl. Madine et al. (2020b): 225780.

809 Vgl. Madine et al. (2020b): 225781; Madine et al. (2020a): 193105. Weitere Publikationen benennen den Einsatz einer CA, ohne dabei zu spezifizieren, welche Einrichtung oder Institution diese Aufgabe übernimmt (vgl. Nortey et al. (2019): 372; Ismail/Materwala (2020): 165f.).

810 Vgl. Franceschi et al. (2019): 589; Zhuang et al. (2020b): 2172. Auch Shabo führt in seiner Publikation zu IHRB die Möglichkeit an, dass Patienten einen einzigen oder mehrere Accounts bzw. Identitäten in einer oder mehreren IHRB haben können (vgl. Shabo (2006b): 502).

811 Die relevante *Scholar-Literatur* ist in diesem Absatz den Ausführungen des Entscheidungsmodells als Fußnote angehängt.

812 Vgl. Franceschi et al. (2019): 589.

813 Vgl. Franceschi et al. (2019): 589; Hylock/Zeng (2019): e13592.5; Sikander/Sridevi (2020): 593; Yang et al. (2020a): 70609.

814 Vgl. Franceschi et al. (2019): 589; Hylock/Zeng (2019): e13592.5; Wang/Zhang/Zhang (2019): 102891; Cernian et al. (2020): 6538.8; Kung et al. (2020): 1784; Wang et al. (2020): 58; Zhuang et al. (2020b): 2172.

Lage ist, einen Log für sämtliche Transaktionen bereitzustellen, allerdings nachgelagert zu den oben genannten Logs für Zugriffe und der Integritätsabsicherung.

Unter Einbeziehung der Literatur zu forschungs- und kostenträgerbezogener Integration ergeben sich keine neuen Erkenntnisse. Auch in der *Scholar-Literatur* wird auf eine PKI gesetzt,[815] die auf eine CA zurückgreift,[816] Benutzername und Passwort zur Authentifizierung verwendet[817] und die Blockchain vornehmlich als Audit-Instrument zur Sicherstellung der Integrität während einer Studie nutzt.[818]

Diese Erläuterungen und die Verknüpfung von Referenzarchitektur, Entscheidungsmodell und *Scholar-Literatur* ergeben die in *Abbildung 8-7* dargestellten Handlungsempfehlungen zur Konstruktion der Security-Sicht.

[815] Vgl. Hang et al. (2021): 5554487.9.

[816] Vgl. Hang et al. (2021): 5554487.9.

[817] Vgl. Zhuang et al. (2020a): e19029.4.

[818] Vgl. Choudhury et al. (2019): 282; Hirano et al. (2020): e18938.7; Hang et al. (2021): 5554487.7.

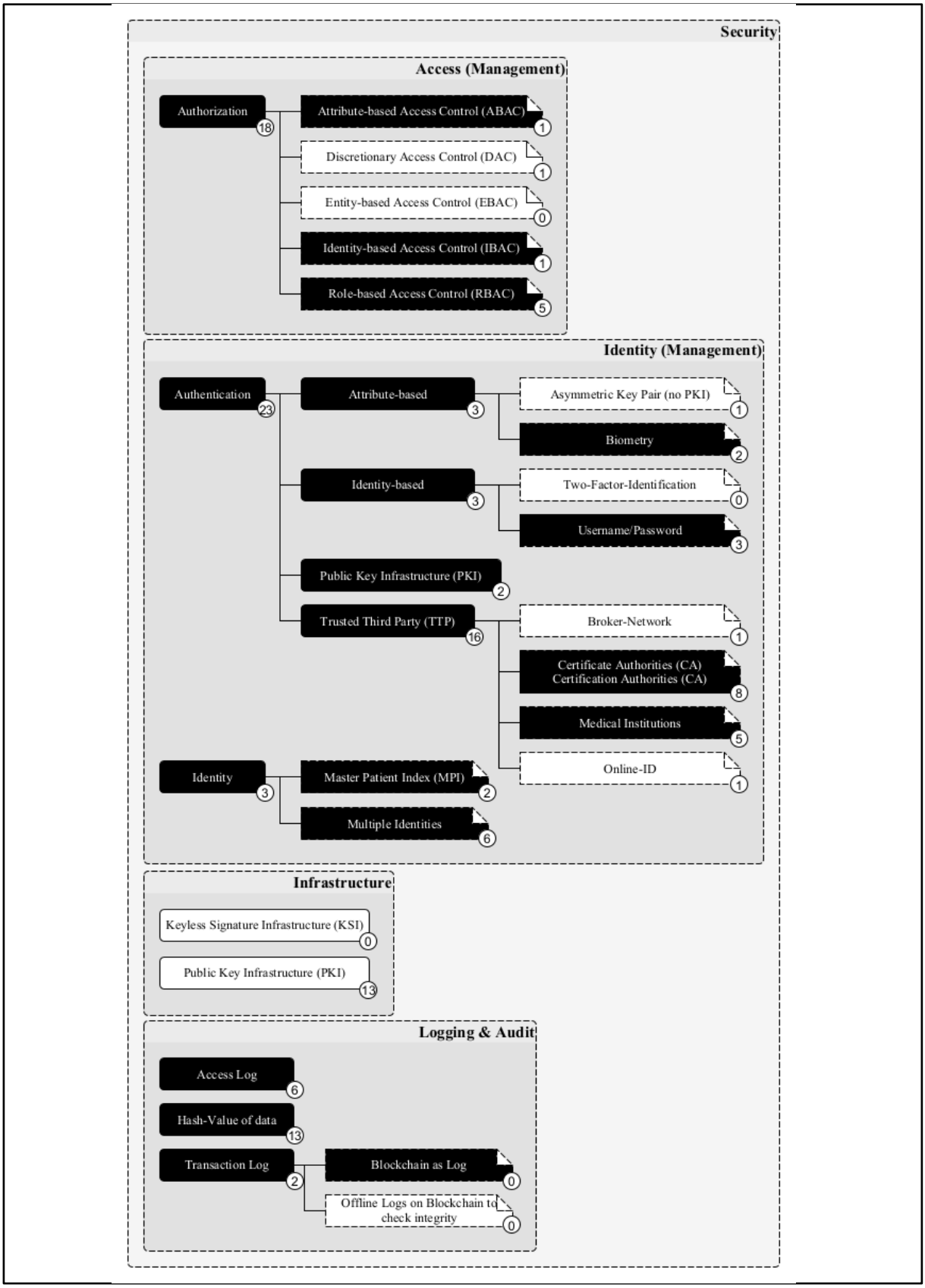


Abbildung 8-7: Patientenakten-Handlungsempfehlungen für ‚Security'-Variationen der Referenzarchitektur (Quelle: Eigene Darstellung)

8.4.1.4 Sicht: Technology

Zu Beginn der Variantenauswahl liegt die Entscheidung, ob eine einzelne oder mehrere Blockchains betrieben werden. In der Architekturkonstruktion wird der Betrieb einer einzelnen Blockchain vorrangig betrachtet. Gleiches gilt in der *Scholar-Literatur*, die nur in einer einzigen Publikation vom Betrieb mehrerer Blockchains spricht.[819]

Im nächsten Schritt findet die Auswahl gemäß der Blockchain-Taxonomie statt. Entsprechend dem definierten Entscheidungsmodell ist vornehmlich eine *Private-Permissioned*-Blockchain zu wählen. Doch auch die hybride Variante (*Consortium-Blockchain*) spielt eine relevante Rolle. Die gleiche Lösung wird in der *Scholar-Literatur* bevorzugt, wobei hier vornehmlich auf den Begriff der *Permissioned-Blockchain* abgestellt wird, ohne dabei zwischen *Private-Permissioned* oder *Public-Permissioned Blockchain* zu differenzieren.[820] Auch die *Consortial Blockchain* findet Anwendung.[821]

Darauf aufbauend ergeben sich die zu nutzenden Blockchain-Technologien, die sich dabei auf die *Ethereum*- und *Hyperledger-Blockchain* beschränken. *Quorum* ist schwach repräsentiert. In der *Scholar-Literatur* sind ebenfalls *Ethereum*-[822] und *Hyperledger*-Blockchains[823] im Einsatz. Hinzu kommt, dass in mehreren Publikationen von einer privaten Ethereum-Blockchain die Rede ist, ohne dabei jedoch konkret auf *Quorum* hinzuweisen.[824]

Nach Auswahl der Technologie wird ein zur Technologie und zum Anwendungsfall passendes Konsensprotokoll festgelegt, das sich entsprechend der Referenzarchitektur auf *BFT*, *DPoS*, *PBFT* und *PoW* beschränkt. Aufgrund der Weiterentwicklung der Ethereum-Blockchain und dem damit verbundenen Wechsel vom bis dato genutzten PoW-Konsens-Protokolls hin zum

---

819 Vgl. Abunadi/Kumar (2021): 2865.4. In dieser betreibt jeder Patient seine eigene Blockchain, doch wird in der Konzeptionsbeschreibung nicht näher beschrieben, wie diese aufgebaut ist oder Ärzte konkret auf deren Inhalte zugreifen können.

820 Vgl. Hylock/Zeng (2019): e13592.4; Nortey et al. (2019): 372; Niu et al. (2020): 7198.

821 Vgl. Wang/Luo/Zhou (2020): 3; Yang et al. (2020b): 45471.

822 Vgl. Shahnaz/Qamar/Khalid (2019): 147788; Wang/Zhang/Zhang (2019): 102891; Cernian et al. (2020): 6538.8; Kung et al. (2020): 1784; Madine et al. (2020a): 193105; Ruggeri et al. (2020): 118; Wang et al. (2020): 51; Wu et al. (2020): 343; Fatokun/Nag/Sharma (2021): 580.1.

823 Vgl. Guo et al. (2019): 46; Cernian et al. (2020): 6538.8; Chenthara et al. (2020): e0243043.7; Ismail/Materwala (2020): 165; Sharma/Balamurugan (2020): 176; Meier et al. (2021): 23; Uddin et al. (2021): 2385. Die hier genannten Publikationen nutzen das Hyperledger Fabric Framework. Darüber hinaus existieren Beschreibungen, alternative Frameworks zu nutzen, wie *Hyperledger Besu* (vgl. Madine et al. (2020b): 225780), *Hyperledger Composer* (vgl. Meier et al. (2021): 23; Rajput/Li/Ahvanooey (2021): 206.2) oder *Hyperledger Sawtooth* (vgl. Cernian et al. (2020): 6538.8).

824 Vgl. Kung et al. (2020): 1781; Madine et al. (2020b): 225780; Zhuang et al. (2020b): 2171.

PoS-Protokoll[825] wird PoS in die Liste der Handlungsempfehlungen aufgenommen. *PoS*[826], *PoW*[827] und *BFT*[828] finden nach Analyse der *Scholar-Literatur* auch weiterhin Anwendung.

Eine weitere, auf die Wahl der Technologie zurückzuführende Entscheidung ist die Verwendung von Smart Contracts. Durch den Fokus auf Ethereum und Hyperledger ist ihre Nutzung möglich. Entsprechend der Referenzarchitektur und dem Entscheidungsmodell übernehmen diese in der Regel die Kontrolle der Identität und die damit verbundene Verwaltung von Zugriffsbeschränkungen, die Darstellung und Validierung von Verbindungen zwischen Patienten und Leistungserbringern sowie Datenmanagement-Aufgaben. Die *Scholar-Literatur* bestätigt dies, da diese weiterhin ihren Fokus auf Identitätsprüfung,[829] Zugriffskontrolle,[830] Relationship-Management[831] und Datenmanagement[832] ausrichtet.

Zusammen mit der Technologiewahl ergibt sich zudem die Möglichkeit, Netzwerkteilnehmer für ihr Engagement zu incentivieren. In der Referenzarchitektur werden Ansätze identifiziert, die entweder eine materielle Incentivierung durch die Gewährung von Zugriffen auf bislang unbekannte Daten erlauben oder monetäre Anreize zur Nutzung von Dienstleistungen setzen. In der *Scholar-Literatur* wird die Incentivierung nicht behandelt, sodass eine Bestätigung dieser Handlungsempfehlung zum jetzigen Zeitpunkt nicht möglich ist.[833]

---

825 Vgl. Bussac (2019): 26.

826 Vgl. Quasim et al. (2020): 607; Yang et al. (2020b): 45471.

827 Vgl. Madine et al. (2020a): 193105; Fatokun/Nag/Sharma (2021): 580.6.

828 Vgl. Uddin et al. (2021): 2385.

829 Vgl. Franceschi et al. (2019): 590f; Wu et al. (2020): 346f. Neben der Identitätsprüfung übernehmen Smart Contracts auch die Erstellung bzw. Registrierung von Identitäten (vgl. Franceschi et al. (2019): 590; Chelladurai/Pandian (2021): 6f; Uddin et al. (2021): 2386).

830 Vgl. Guo et al. (2019): 46; Hylock/Zeng (2019): e13592.8; Roehrs et al. (2019): 103140.6; Shahnaz/Qamar/Khalid (2019): 147788f; Madine et al. (2020a): 193106; Wang/Luo/Zhou (2020): 5; Wu et al. (2020): 346f; Zhuang et al. (2020b): 2171; Chelladurai/Pandian (2021): 8; Rajput/Li/Ahvanooey (2021): 206.11.

831 Vgl. Madine et al. (2020a): 193106; Chelladurai/Pandian (2021): 7f.

832 Vgl. Franceschi et al. (2019): 591f; Wang et al. (2020): 51; Wang/Luo/Zhou (2020): 5; Wu et al. (2020): 347; Chelladurai/Pandian (2021): 7. Dieses Management umfasst ebenfalls reines Meta-Datenmanagement sowie die Gewährleistung der Einhaltung von Integritätsregeln (vgl. Wang/Zhang/Zhang (2019): 102896; Madine et al. (2020a): 193106).

833 In der Ergänzung des Evaluationsumfangs hin zu Kostenträgern kann diese Aussage eingeschränkt bestätigt werden.

Mit der Integration der Forschungsdaten in die Konzeption ergeben sich keine neuen Erkenntnisse hinsichtlich der Handlungsempfehlungen. Der Fokus liegt in der Referenzarchitekturdarstellung wie auch in der *Scholar-Literatur* auf *Private*[834] und *Permissioned*[835] Blockchains sowie auf der Nutzung von *Ethereum*[836] und *Hyperledger*[837]. Für den Einsatz einer rein forschungsorientierten Blockchain sind konsortialgeführte Blockchains zwar nicht relevant, doch bleiben diese aufgrund der Kombination von PHR und Forschung möglich. Die Aufgaben von Smart Contracts ähneln denen für PHR und decken sich mit den Erkenntnissen aus Architektur- und *Scholar-Literatur*. So werden diese zur Verwaltung von Identitäten[838] und Zugriffskontrollen[839] verwendet sowie für Daten-[840] und Consent-Management[841]. Darüber hinaus existieren noch individuelle Smart Contracts, die sich bspw. mit der Identifikation von passenden Teilnehmern,[842] dem Monitoring einer Studie[843] oder der konkreten Datenanalyse[844] beschäftigen.

Die Integration von Kostenträgern bringt ebenfalls keine neuen Erkenntnisse. In der *Scholar-Literatur* wird ebenso auf konsortiale Blockchains,[845] alternativ auf eine private Ethereum Blockchain[846] gesetzt. Smart Contracts werden zur Identifikation relevanter Personen und der dazugehörigen zu vergütenden Behandlungen genutzt und umfassen laut Architektur- wie auch *Scholar-Literatur* die Themen Zugriffskontrolle (Access) und Zahlung (Payment).[847] Neben der bereits für PHR beschriebenen Incentivierung der Netzwerkteilnehmer findet sich eine Literaturquelle, die konkret den Einsatz eines ERC-20-Token anspricht, der einem Patienten, abhängig von seinem Engagement in der Verwaltung der Blockchain, eine entsprechende Aufwandsentschädigung verspricht.[848]

---

834 Vgl. Wong/Bhattacharya/Butte (2019): 917.2; Zhuang et al. (2020a): e19029.4.

835 Vgl. Choudhury et al. (2019): 282; Hang et al. (2021): 5554487.21.

836 Vgl. Omar et al. (2019): 3. Ebenfalls relevant ist die Private Ethereum Blockchain, ohne dabei auf die Quorum explizit hinzuweisen (vgl. Zhuang et al. (2019): 1278; Zhuang et al. (2020a): e19029.4).

837 Vgl. Choudhury et al. (2019): 284; Hirano et al. (2020): e18938.2; Hang et al. (2021): 5554487.21.

838 Vgl. Choudhury et al. (2019): 286; Zhuang et al. (2019): 1278; Ruggeri et al. (2020): 118; Zhuang et al. (2020a): e19029.6.

839 Vgl. Omar et al. (2019): 3f; Hang et al. (2021): 5554487.14.

840 Vgl. Choudhury et al. (2019): 284; Zhuang et al. (2020a): e19029.4.

841 Vgl. Choudhury et al. (2019): 286f.

842 Vgl. Franceschi et al. (2019): 591; Zhuang et al. (2019): 1278.

843 Vgl. Choudhury et al. (2019): 286.

844 Vgl. Choudhury et al. (2019): 287.

845 Vgl. Mackey et al. (2020): 3.

846 Vgl. Mackey et al. (2020): 7. Ergänzend wird ein Proof-of-Authority-Konsensprotokoll verwendet, das sonst keine Relevanz in anderen Konstruktionsbeschreibungen in der Literatur hat (vgl. Mackey et al. (2020): 6).

847 In der Literatur wird ein sogenanntes *Claim Monitoring* beschrieben, das diese Aufgaben gebündelt durchführt (vgl. Mackey et al. (2020): 8).

848 Vgl. Mackey et al. (2020): 8.

Die Ergebnisse aus Referenzarchitektur und Entscheidungsmodell, zusammengeführt mit der Evaluation des Szenarios, ergeben die in *Abbildung 8-8* dargestellten Handlungsempfehlungen.

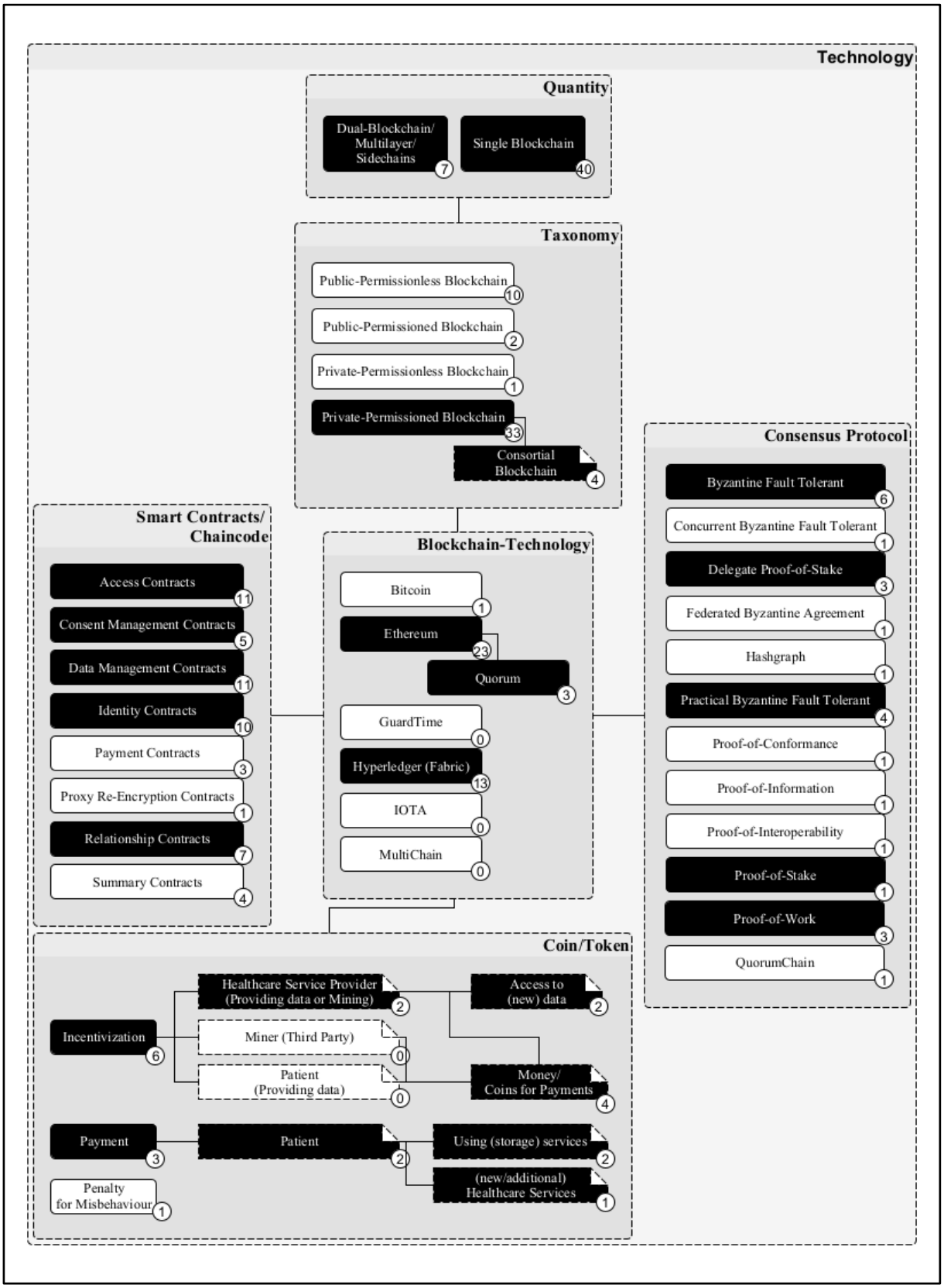


Abbildung 8-8: Patientenakten-Handlungsempfehlungen für ‚Technology'-Variationen der Referenzarchitektur
(Quelle: Eigene Darstellung)

8.4.1.5 Fazit zur Erfüllung der definierten Anforderungen

Die in *Kapiteln 8.4.1.2* bis *8.4.1.4* beschriebenen Handlungsempfehlungen führen zur Erfüllung aller in *Kapitel 8.4.1.1* definierten Anforderungen.

Anforderung (1) und (2) verlangen die Möglichkeit, sämtliche Gesundheitsdaten eines Patienten zu speichern, und zwar in einem Format, das die umfassende Nutzung der Gesundheitsdaten erlaubt. In *Kapitel 8.4.2.2* wird festgestellt, dass eine Speicherung von Gesundheitsdaten nicht direkt auf der Blockchain vorgenommen wird, sondern auf externen Speichersystemen, wie z.B. Cloud oder IPFS. Die entsprechenden Metadaten werden wiederum auf der Blockchain gespeichert, die die Aufgabe eines Index übernimmt und neben der konkreten Speicheradresse im Speichersystem ergänzende Informationen, wie bspw. den Hashwert der gespeicherten Daten, bereitstellt. Insbesondere der auf der Blockchain gespeicherte Hashwert garantiert dabei die Integrität der in externen Systemen abgelegten Gesundheitsdaten. Aufgrund der Speicherung von Daten in externen Speichersystemen fordert die Blockchain die Nutzung von bereits im Gesundheitswesen etablierten Standards, wie bspw. HL7 oder FHIR, sodass nicht nur der Ort von Daten, sondern auch deren Inhalt von Dritten abgerufen werden können und Interoperabilität gewährleistet wird.

Gemäß Anforderungen (3), (4) und (5) hat jeder Akteur in der Gesundheitsversorgung, vom Leistungserbringer über den Patienten bis hin zu Kostenträgern und Forschungseinrichtungen, Zugriff auf Gesundheitsdaten zu erhalten, sofern die Berechtigung besteht. *Kapitel 8.4.1.3* zeigt, wie diese Anforderungen erfüllt werden. Die Blockchain übernimmt einen Großteil der Identitäts- und Zugriffsverwaltung und greift dabei auf das im IAM-Umfeld bereits etablierte RBAC und ABAC zurück. Während für Zugriffskontrollen entsprechende Regeln, bspw. in Smart Contracts, definiert werden und auf der Blockchain Zugriffsprotokolle revisionssicher gespeichert werden, wird Leistungserbringern oder CAs die Aufgabe der Identitätsfeststellung und -registrierung übertragen. Grundsätzlich wird weiterhin auf die Nutzung der bereits bekannten PKI-Infrastruktur gesetzt.

Gestützt durch die Ergebnisse der Evaluation, eignen sich die konzipierte Referenzarchitektur und das Entscheidungsmodell für die Entwicklung einer blockchain-basierten IHRB-Alternative.

8.4.2 Szenario 2: Ein digitaler Impfpass

8.4.2.1 Einführung, Anforderungsaufnahme und Methodik

Zur Nachverfolgung von Schutzimpfungen existieren, neben den bei Leistungserbringern geführten Patientenakten, Impfpässe bzw. Impfausweise, die den aktuellen Impfstatus einer Person dokumentieren, d.h. Datum und Art der Impfung, Chargennummer und Leistungserbringer. Den Umfang der dokumentierten Informationen regelt in Deutschland §22 des Infektionsschutzgesetzes.

Mit zunehmender Digitalisierung der Patientenakten verringert sich die Zahl der analog auf Papier geführten Impfpässe stetig, weil die Informationen in den digitalen Systemen der Leistungserbringer gespeichert werden.[849] Dabei verliert das Dokument den Charakter eines einrichtungs- und sogar länderübergreifenden Informationsmediums, insbesondere unter der Annahme, dass die Informationen nicht zwischen den Leistungserbringern ausgetauscht werden. Doch auch ein analog vorhandenes Dokument ist Risiken, wie Verlust oder Manipulation, ausgesetzt und könnte zudem gefälscht werden.[850]

Um diesen Problemen zu begegnen, werden Impfausweise zunehmend digitalisiert und durch die Blockchain-Technologie dahingehend unterstützt, Impfzertifikate und Testergebnisse[851] revisionssicher zu verwalten sowie die Informationen einrichtungsübergreifend zur Verfügung zu stellen.[852]

In Deutschland wird die Blockchain bereits eingesetzt, indem nach erfolgter Covid19-Impfung ein Hashwert von *Name*, *Datum* und *Impfstoff* erzeugt und auf einer Blockchain gespeichert wird. Die gleichen Daten werden im Klartext in einem QR-Code gespeichert, sodass jeder Prüfende den QR-Code einlesen, einen Hash aus den vorliegenden Daten erzeugen und mit dem auf der Blockchain gespeicherten Hash abgleichen kann.[853] Das gleiche Vorgehen wird für eine Lösung auf Ebene der Europäischen Union beschrieben.[854] Doch spätestens im internationalen Kontext fehlt es derzeit an der Dokumentation eines einheitlichen Blockchain-Frameworks.[855]

---

849 Vgl. Wagner (2019): 2845.

850 Vgl. Wagner (2019): 2844; Marhold/Fell (2021): 738; Mbunge et al. (2021): 100136.1.

851 Testergebnisse insbesondere aufgrund der COVID19-Pandemie (*Corona*).

852 Vgl. Ahmad et al. (2020): 6f; Mbunge et al. (2021): 100136.1; Tsoi et al. (2021): 339.

853 Vgl. Schrahe/Städter (2021): 316.

854 Vgl. Hernández-Ramos et al. (2021): 5.

855 Vgl. Mbunge et al. (2021): 100136.2. Obwohl die Lösung der EU eine internationale Absprache suggeriert, gibt es in der Fachwelt Zweifel an der tatsächlichen Umsetzung (vgl. Schrahe/Städter (2021): 317).

Die in dieser Forschungsarbeit entwickelte Referenzarchitektur setzt hier an und wird dahingehend evaluiert, ob sie auf Basis der abgeleiteten Handlungsempfehlungen eine valide Grundlage für das fehlende internationale Blockchain-Framework bietet.

Ein digitaler Impfpass wird durch einen Leistungserbringer geführt und enthält nur einen Auszug der gesamten Patientendaten. Deshalb ergibt sich als zugrundeliegender *Record Type* das sog. *Patient Summary*.

An die Entwicklung eines elektronischen Impfpasses werden unterschiedliche Anforderungen gestellt, die von technologischer und organisatorischer Natur sind. Hierzu zählen auszugsweise:[856]

(1) Interoperabilität und Nutzung bestehender Standards
(2) Sichere Datenhaltung ohne Preisgabe personenbezogener Daten
(3) Sichere Authentifizierung, einfache Registrierung sämtlicher Stakeholder und Potential zur anonymen Nutzung
(4) Manipulationssicherheit und Transparenz durch Nachvollziehbarkeit sämtlicher Transaktionen
(5) Respektierung geltender Gesetze und ethischer Diskussionen (Datenschutzfreundlichkeit)
(6) Verständlichkeit für Nutzer und Betreiber
(7) Keine Notwendigkeit spezialisierter Hardware
(8) Finanzierbarkeit durch alle Stakeholder

Die Evaluation der Handlungsempfehlungen, die sich aus der konzipierten Referenzarchitektur und dem Entscheidungsmodell ergeben, wird durch Analyse aktueller Literatur vorgenommen, die im Zeitraum von Januar 2019 bis Juli 2021 in der Suchmaschine *GoogleScholar* identifiziert wird. Dieser Zeitraum liegt nach dem für die Literaturanalyse verwendeten Zeitraum. Dabei werden mehrere Suchwort-Kombinationen genutzt und jeweils die ersten 10 Seiten der Suchergebnisse betrachtet:[857]

i. *Vaccination certificate* AND *blockchain*
ii. *Vaccination* AND *blockchain*

[856] Vgl. Polley et al. (2021): 2; Schrahe/Städter (2021): 316; Wilson/Flood (2021): E487.

[857] Die Auswahl der in diesem Fall relevanten Literatur wird auf Basis des Titels und Abstracts der Suchergebnisse durchgeführt und folgt somit dem ursprünglichen Ansatz der Literaturanalyse.

Um Verwechslungen zwischen Basis-Literatur zur Konstruktion der Architektur und der Literatur zur Validierung des Modells zu vermeiden, wird im Folgenden der Begriff *Scholar-Literatur* für sämtliche seit Januar 2019 identifizierte Literatur genutzt.

8.4.2.2 Sicht: Data Storage & Provisioning

Entsprechend der definierten Referenzarchitektur wird in einem ersten Schritt zwischen den Speichervariationen *on-* bzw. *off-chain* entschieden. Im Entscheidungsmodell existieren für *Patient Summaries* keine Erkenntnisse über Best-Practices im Bereich der Datenhaltung. Die Wahl wird aus diesem Grund über den Umfang der zu verwaltenden Daten getroffen.

Für einen Impfausweis werden Textinformationen und keine Bilddateien benötigt. Im vorliegenden Fall orientiert sich der Umfang eines Impfausweises an § 22 Infektionsschutzgesetz[858]:

i. Datum der Impfung
ii. Bezeichnung und Chargennummer des Impfstoffes
iii. Name der Krankheit, gegen die geimpft wurde
iv. Name der geimpften Person, deren Geburtsdatum sowie Name und Anschrift der für die Durchführung der Schutzimpfung verantwortlichen Person

In der weiteren Bearbeitung wird davon ausgegangen, dass ein Datensatz, der dieser Liste folgt, eine durchschnittliche Zeichenlänge von ca. 200 Zeichen und folglich eine Größe von ca. 200 Byte[859] aufweist.

Unter der Annahme, dass die Informationen in einem Leistungserbringer-Netzwerk verteilt werden und für die Erreichung einer Herdenimmunität, z.B. gegen Covid19, 67% der Bevölkerung geimpft sein müssen,[860] sind bereits für diese Inhalte die in Formel (4) ermittelten Datenmengen anzunehmen:

$$200\ Byte * (0{,}67 * 83.166.711) \approx 11.144.339.274\ Byte \approx 11{,}1\ GB \qquad \textbf{Formel (4)}$$

Allein für die einmalige Covid19-Impf-Registrierung von 67% der in Deutschland lebenden Bevölkerung müssen demzufolge 11,1 GB in jedem Knoten des Netzwerks bereitstehen.

Im Hinblick darauf, dass jeder Bundesbürger nicht nur Covid19-Impfungen, sondern auch andere teilweise auch wiederkehrende Impfungen erhält, ist bei der erwartende Datenmenge eine

858 Vgl. SeuchRNeuG (2000): 1055. Zusätzlich sämtliche Neuregelungen bis IfSG (2022).

859 200 Zeichen haben eine Textgröße von 203 Byte. Für eine einfachere Bewertung und unter Berücksichtigung von Durchschnittswerten wird hier von eine Byte-Größe von 200 Byte festgelegt.

860 Vgl. Randolph/Barreiro (2020): 738.

off-chain-Speicherung vorzuziehen und die Speicherung eines Verweises und/oder eines Integritätsnachweises auf der Blockchain vorzunehmen. Dies gilt insbesondere, sobald nicht nur Leistungserbringer sondern auch Patienten Zugriff auf diese Informationen erhalten. Als Datenspeicher stehen Cloud oder IPFS zur Wahl, die für die Datenbereitstellung einen Pointer auf der Blockchain hinterlegen und über einen Gatekeeper den Zugriff auf sämtliche Daten steuern. Des Weiteren wird auf bestehende Standards gesetzt, sodass eine Interoperabilität gewährleistet wird.

Mit Blick auf die *Scholar-Literatur* und die bestehenden Impfpass-Lösungen werden *on-* sowie *off-chain*-Ansätze thematisiert, wobei der *on-chain*-Ansatz von den Autoren nicht tiefergehend beschrieben wird.[861] Dem gegenüber steht der off-chain-Ansatz, der lediglich einen Hashwert auf der Blockchain speichert. Dieser Hashwert reduziert die oben unter der Annahme einer vollständigen on-chain-Datenhaltung dargestellte Datenmenge um 84%.[862] Dabei existieren zwei Ansätze über die Konstruktion des Hash-Werts. Im ersten Fall wird aus den o.g. Impfinformationen ein Hashwert erzeugt, der zur Überprüfung der Gültigkeit genutzt wird.[863] Im zweiten Fall wird der Pfad in einem IPFS-basierten Datenmanagement abgelegt und ein Pointer festgelegt.[864] IPFS wird in diesem Kontext wiederholt erwähnt.[865] Cloud hingegen wird vornehmlich zur Speicherung bzw. Verwaltung von Identitäten, nicht von Gesundheitsdaten, genutzt.[866] Das Thema Interoperabilität wird in nur einer Publikation erwähnt (*HL7* und *FHIR*) jedoch nicht tiefergehend behandelt.[867]

Aus diesen Erkenntnissen resultieren die in *Abbildung 8-9* dargestellten Empfehlungen für die Datenhaltung und -bereitstellung eines blockchain-basierten Impfpasses.

---

861 Vgl. Fiquaro et al. (2021): 153.

862 Diese Aussage trifft auf einen Hash mit einer Länge von 256 Bits zu. 256 Bits entsprechen 32 Byte und entsprechen somit einer Reduzierung um 84% der ursprünglich angenommen 200 Byte pro Impfung.

863 Vgl. Eisenstadt et al. (2020): 149f. Im Fall einer Überprüfung der Gültigkeit einer Impfung wird aus den gleichen Daten, gespeichert auf einem Endgerät des Patienten, ein neuer Hash generiert, der mit dem auf der Blockchain gespeicherten Hash verglichen wird.

864 Vgl. Abid et al. (2021): 7.

865 Vgl. Deka/Goswami/Anand (2020): 136f.

866 Vgl. Eisenstadt et al. (2020): 149; Fiquaro et al. (2021): 153.

867 Vgl. Polley et al. (2021): 4.

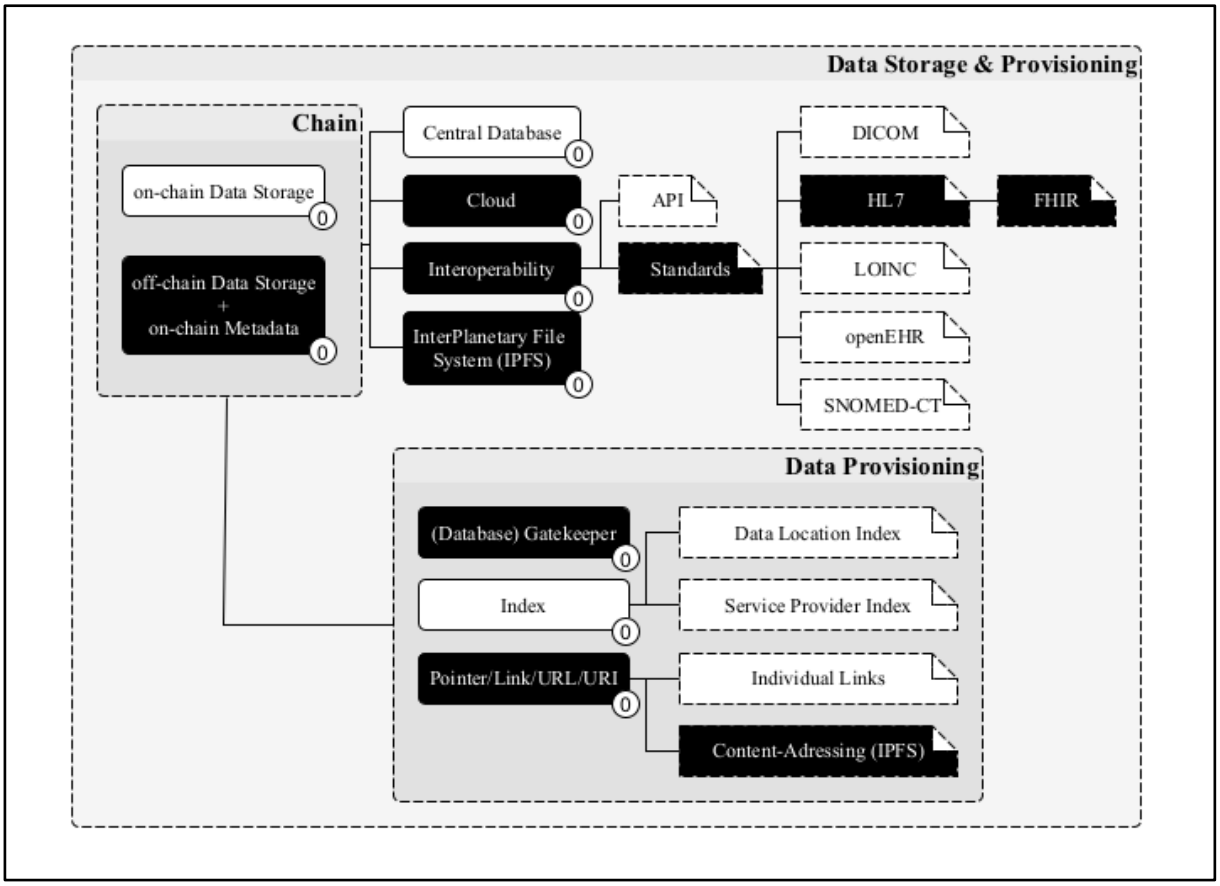


Abbildung 8-9: Impfpass-Handlungsempfehlungen für ‚Data-Storage-& Provisioning'-Variationen der Referenzarchitektur
(Quelle: Eigene Darstellung)

8.4.2.3 Sicht: Security

Zum Thema Security existieren, wie die Analyse zur Entwicklung der Referenzarchitektur offenlegt, nur rudimentäre Beschreibungen für *Patient Summaries*. So beschränkt sich der Einsatzbereich der Blockchain-Technologie bisher auf die revisionssichere Speicherung von Transaktions-Logs. Des Weiteren wird zur Gewährleistung der Sicherheit auf eine PKI-Infrastruktur unter Anwendung der damit verbundenen TTP gesetzt.

Auch in der Anwendungsdomäne der Impfpässe wird die Blockchain-Technologie zur Führung eines auditfähigen Logs genutzt.[868] Darüber hinaus wird Blockchain von den Autoren der *Scholar-Literatur* als potentielle Technologie zur Verschlüsselung von Gesundheitsdaten sowie für die gesicherte Authentifizierung (von Patienten) definiert.[869] In diesem Zusammenhang etabliert sich zudem das Konzept der *Decentralized Identities* (DIDs) bzw. *Self-Sovereign Iden-*

[868] Vgl. Polley et al. (2021): 6.

[869] Vgl. Mbunge (2020): 1632; Mbunge et al. (2021): 100136.1.

tities, die eine feingranulare Verwaltung von Identitäten und Zugriffen durch den Patienten erlauben.[870] Neben der üblichen PKI-Infrastruktur wird hier auch KSI als potentielle Infrastruktur erwähnt.[871] In der *Scholar-Literatur* wird derzeit das Thema *Autorisierung* nicht diskutiert. Im Gesundheitswesen hat sich insbesondere RBAC durchgesetzt, weshalb diese Form der Autorisierung in die Handlungsempfehlungen aufgenommen wird.

Aus diesen Erkenntnissen resultieren die in *Abbildung 8-10* dargestellten Handlungsempfehlungen für Security.

[870] Vgl. Abid et al. (2021): 9.

[871] Vgl. Polley et al. (2021): 3. In diesem Zusammenhang wird auf den in *Kapitel 8.3.2* vorgenommenen Vergleich von PKI und KSI sowie deren gegenseitiges Unterstützungspotential verwiesen.

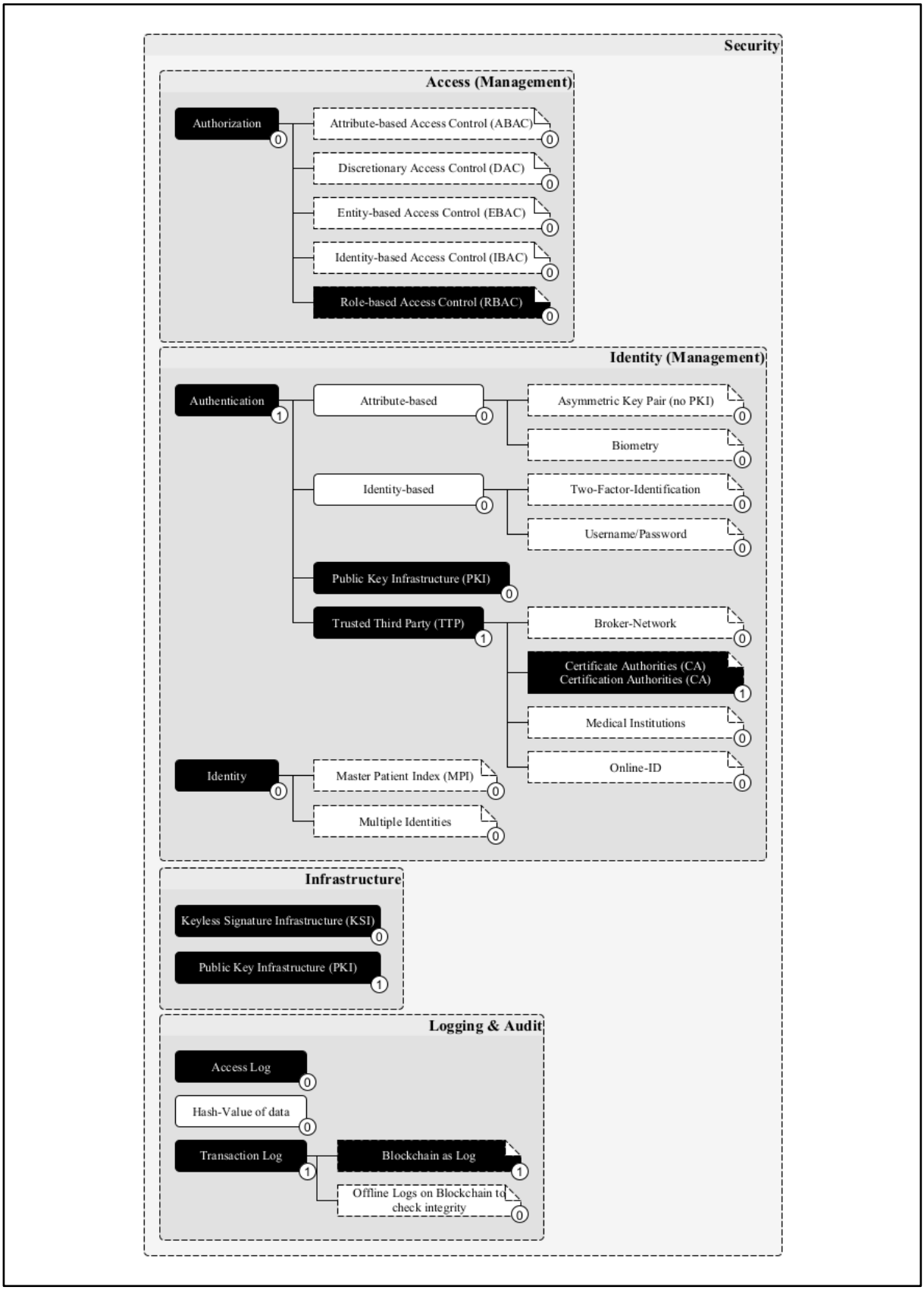


Abbildung 8-10: Impfpass-Handlungsempfehlungen für ‚Security'-Variationen der Referenzarchitektur (Quelle: Eigene Darstellung)

8.4.2.4 Sicht: Technology

Patient Summaries verwenden in der analysierten Literatur der Referenzarchitektur in der Regel eine einzige *Private-Permissioned-Blockchain*. Die einzige dokumentierte Technologie ist zudem Multi-Chain, die jedoch nicht im direkten Zusammenhang zur Blockchain-Klassifikation steht.

Eine *Private-Permissioned-Blockchain* wird in Netzwerken genutzt, in denen die Nutzer bekannt sind und im Vorfeld einen Registrierungsprozess durchlaufen müssen. Da insbesondere im Rahmen der Covid-19-Pandemie eine Impfbescheinigung auch außerhalb des Kreises der Leistungserbringer geprüft wird, kann die *Consortial-Blockchain* genauso wie die *Public-Permissioned Blockchain* in die Handlungsempfehlungen aufgenommen werden.

Tatsächlich ist gerade der Umstand, dass bspw. Restaurants oder Reiseveranstalter die auf der Blockchain gespeicherten Hashwerte zur Validierung der ihnen vorgelegten Informationen nutzen, ein Anlass, auf den Betrieb einer reinen *Private-Permissioned-Blockchain* zu verzichten.

Unter Berücksichtigung dieser Erkenntnis werden in der Auswahl der *Private-Permissioned-Blockchain* folgende Technologien mit konsortialen Potentialen berücksichtigt:

i. Hyperledger (Fabric)
ii. Ethereum bzw. Quorum

Für *Public-Permissioned-Blockchains* konnten keine Beispiele in der Referenzarchitektur identifiziert werden.[872] Mit der Wahl von Hyperledger bzw. Ethereum/Quorum stehen sämtliche Variationspunkte der Smart Contracts-/Chaincode-Gruppe zur Verfügung. Eine Auswahl der mit Hyperledger in Verbindung zu bringenden Chaincodes ist:

i. Access Contracts
ii. Consent Management Contracts
iii. Data Management Contracts
iv. Payment Contracts (Durchführung von Zahlungen)
v. Relationship Contracts
vi. Summary Contracts[873]

Aufgrund der gewählten Technologie-Variation wird eine Beschränkung auf folgende Konsens-Protokolle vorgenommen:

---

[872] *R3 Corda* ist ein prominentes Beispiel und wird in der Literatur rund um Blockchain im Gesundheitswesen ein Mal erwähnt.

[873] Diese werden nicht explizit in der Kombination mit Hyperledger genannt. Wegen der Beschränkung auf Patient Summary in diesem Kapitel wird dieser Chaincode hier ergänzend hinzugefügt.

i. BFT
ii. PBFT
iii. Proof-of-Stake
iv. Proof-of-Work
v. QuorumChain

Im letzten Schritt werden Coins bzw. Token thematisiert, die für Patient Summaries bislang nicht in der Literatur diskutiert werden. Grundsätzlich ist eine Incentivierung für Leistungserbringer oder Netzwerkbetreiber für die Ausstellung bzw. Bereitstellung der Impfzertifikate wünschenswert. Doch verzichtet insbesondere Hyperledger auf die Nutzung von Coins und incentiviert seine Teilnehmer im Rahmen der Konsortial-Partnerschaft und des daraus gewonnenen indirekten Nutzens. Aus diesem Grund werden keine Handlungsempfehlungen für diesen Block definiert.

Im direkten Vergleich mit den in der *Scholar-Literatur* identifizierten blockchain-basierten Impfpass-Konzeptionen ergibt sich, dass die hier getroffenen Entscheidungen deckungsgleich sind. So werden *Consortial-*[874] und *Permissioned-Blockchains*[875] genutzt. Public-Permissioned Blockchains werden insbesondere im Zusammenhang mit der Identitätsverwaltung, genauer der Self-Sovereign-Identity,[876] beschrieben. Dabei wird auf die Technologien *Hyperledger*[877] und *Ethereum*[878] gesetzt. Auch wird die Nutzung von Smart Contracts bzw. Chaincode beschrieben, die insbesondere die Verwaltung von Inhalten (Zusammenfassungen und Datenmanagement) und die Gewährleistung der Interoperabilität sowie die Kontrolle der Zugriffe übernehmen.[879]

Aus den hier festgestellten Erkenntnissen ergibt sich die in *Abbildung 8-11* dargestellte Auswahl von Konstruktionsvariationen für das Thema Technology.

[874] Vgl. Eisenstadt et al. (2020): 150.

[875] Vgl. Fiquaro et al. (2021): 153; Hernández-Ramos et al. (2021): 4.

[876] Vgl. Abid et al. (2021): 9; Schrahe/Städter (2021): 318.

[877] Vgl. Fiquaro et al. (2021): 153. Hier wird jedoch nicht das *Hyperledger-Fabric*-Framework genannt, sondern ein alternatives Framework namens *Hyperledger Besu*.

[878] Vgl. Deka/Goswami/Anand (2020): 137. In der Literatur wird keine Unterscheidung zwischen *Ethereum* und *Quorum* getroffen. Der Hinweis auf Ethereum in Verbindung mit dem Einsatz als *Private-Permissioned Blockchain* findet sich in einer alternativen Konzeption (*NovidChain*) und begründet folglich die unklare Differenzierung der Technologien (vgl. Abid et al. (2021): 7).

[879] Vgl. Deka/Goswami/Anand (2020): 138; Abid et al. (2021): 12f; Hernández-Ramos et al. (2021): 6.

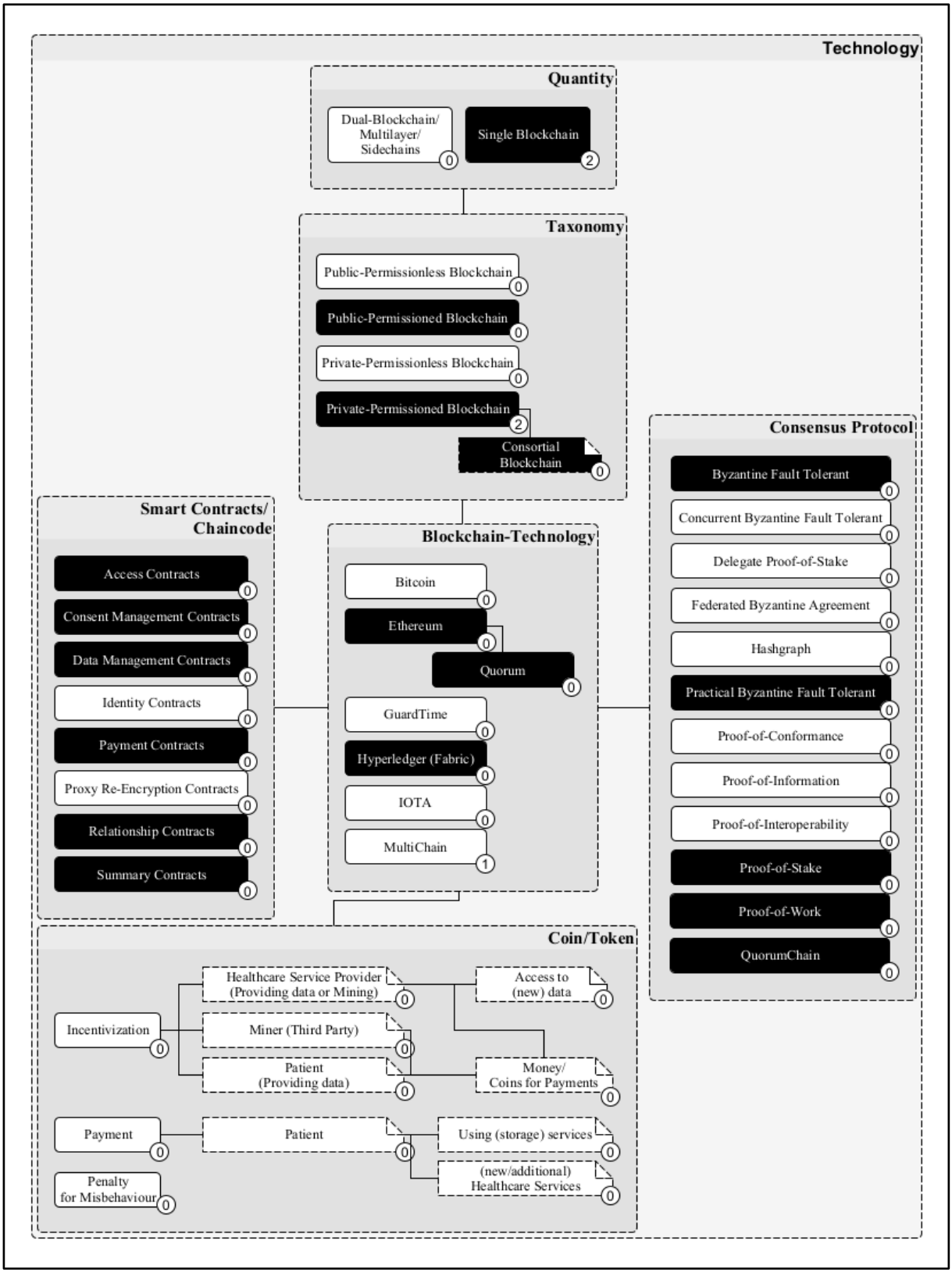


Abbildung 8-11: Impfpass-Handlungsempfehlungen für ‚Technology'-Variationen der Referenzarchitektur (Quelle: Eigene Darstellung)

8.4.2.5 Fazit zur Erfüllung der definierten Anforderungen

Auf der Grundlage der in *Kapitel 8.4.2.2*, *8.4.2.3* und *8.4.2.4* formulierten Handlungsempfehlungen wird im Folgenden validiert, ob die konstruierte Referenzarchitektur und das Entscheidungsmodell unter Berücksichtigung der *Scholar-Literatur* ein geeignetes Werkzeug darstellen, die in *Kapitel 8.4.2.1* definierten Anforderungen zu bedienen.

Anforderung (1), Interoperabilität und Nutzung bestehender Standards, wird in *Kapitel 8.4.2.2* bearbeitet. Die Referenzarchitektur liefert hier keine Erkenntnisse, erlaubt aber die Ableitung von Handlungsempfehlungen durch die Darstellung von Auswahlmöglichkeiten. Mit Blick auf die *Scholar-Literatur* lässt sich als Handlungsempfehlung aber die Verwendung von Standards, insbesondere HL7 und FHIR, ableiten.

Dass keine personenbezogenen Daten preisgegeben werden (Anforderung (2)), wird durch die Bereitstellung von Metadaten statt Rohdaten sichergestellt. Der Zugriff auf Rohdaten wird durch Database Gatekeeper gesteuert. Die mit dieser Anforderung zusammenhängende sichere Authentifizierung (Anforderung (3)) wird durch die in *Kapitel 8.4.2.3* formulierten Handlungsempfehlungen abgedeckt. Authentifikation wird durch eine PKI- und KSI-Infrastruktur unterstützt. Eine TTP, bspw. ein Leistungserbringer, übernimmt dabei die Identitätsprüfung und Registrierung. Eine anonyme Nutzung des Dienstes ist im Grunde nicht vorgesehen, jedoch kann unter Anwendung eines *Master-Patient-Index* eine Vielzahl von Identitäten unter Anwendung von Pseudonymen verwaltet werden, die bspw. im Falle einer Impfnachweis-Pflicht mitgeteilt werden, ohne die Realidentität preiszugeben.

Anforderung (4), Manipulationssicherheit und Transparenz, ist technologisch (*Kapitel 8.4.2.4*) bedingt und wird bereits durch den Aufbau einer Blockchain erfüllt, da diese wegen der Verkettung der Blöcke ein revisionssicheres Log sämtlicher Transaktionen bereitstellt. Die Auswahl der Technologie sowie die Menge der im Netzwerk berechtigten Nodes zu Validierung der Transaktionen bedingen dabei die Sicherheit des Netzwerks.

Grundsätzlich ist die Berücksichtigung von Ethik und geltenden Gesetzen (Anforderung (5)) organisatorisch zu betrachten und im Rahmen dieser Forschungsarbeit nicht validierbar. Jedoch wird darauf hingewiesen, dass die Blockchain aufgrund ihrer Konstruktion grundsätzlich keine Löschung von Daten erlaubt und somit der EU-DSGVO, die eine Möglichkeit zur Löschung konkret vorschreibt, nicht entsprechen kann.

Das Konzept der Blockchain ist für Nutzer und Betreiber nicht in Gänze zu verstehen (Anforderung (6)). Allerdings wird keine spezielle Hardware für den Betrieb benötigt (Anforderung (7)). Die Finanzierbarkeit (Anforderung (8)) bedarf der Klärung durch Politik und Kostenträger,

aber grundsätzlich ist eine Refinanzierung durch den Einsatz von Coins/Token möglich (siehe *Kapitel 8.4.2.4*).

Die Betrachtung dieses Szenarios zeigt, dass die in dieser Forschungsarbeit entwickelte Referenzarchitektur und das Entscheidungsmodell grundsätzlich zur Konstruktion eines digitalen Impfpasses geeignet sind. Auch wenn das Entscheidungsmodell unter der Annahme eines *Patient Summaries* nicht ausreichend Inhalt für eine konkrete Handlungsempfehlung liefert, erlaubt die Gesamtauswahl an Variationspunkten der Referenzarchitektur die Ableitung einer solchen.

9 Fazit

Ziel dieser Forschungsarbeit ist die Entwicklung einer Referenzarchitektur zur Unterstützung von Entwicklern, die blockchain-basierte Lösungen zur Entlastung der Gesundheitsbranche konzipieren, sowie von Wissenschaftlern bei der Identifikation offener Forschungsfelder und ergänzender Validierung von hier definierten Variationspunkte. Der Fokus liegt dabei auf der Unterstützung der Behandlungsdokumentation, sodass eine für den Patienten optimal ausgerichtete Behandlung möglich ist. Zur Erreichung dieses Ziels orientiert sich diese Forschungsarbeit am herkömmlichen Aufbau wirtschaftsinformatischer Literatur und der DSR, der systematischen Analyse von Literatur und deren Strukturierung zur Ableitung von Artefakten, respektive der Referenzarchitektur und dem Entscheidungsmodell.

Kapitel 1 führt hierzu in das Thema der Gesundheitsversorgung ein, greift dabei die Kostendiskussion auf und beschreibt Faktoren wie bspw. die fehlende oder nicht vollständig umgesetzte einrichtungsübergreifende Dokumentation und Kommunikation, die im Resultat zu einer schlechteren Gesundheitsversorgung führen und zu höheren Ausgaben. Erste Lösungsversuche, die einen übergreifenden Zugriff auf Daten und Informationen ermöglichen sollen, hier namentlich durch die Telematik-Infrastruktur der GEMATIK und die Forschungsinitiativen des BMBF, werden erstmalig erwähnt und als Intermediäre identifiziert, die durch eine Blockchain ersetzt werden könnten. Darüber hinaus wird ein Überblick über den wissenschaftlichen Ansatz der Forschungsarbeit gegeben und die Wirtschaftsinformatik statt der Medizininformatik als Forschungsrichtung definiert. Darauf aufbauend wird das Methodenspektrum der Wirtschaftsinformatik auf die gestaltungsorientierten und für diese Forschungsarbeit zur Verfügung stehenden Methoden eingegrenzt. Erstmalig wird hier die Methodik der Referenzmodellierung genannt und im späteren *Kapitel 5* weiter differenziert. Das Kapitel schließt mit der Beschreibung des für die Wirtschaftsinformatik idealtypischen Aufbaus der gesamten Forschungsleistung und ordnet dabei die Kapitel der Forschungsarbeit entsprechend ein.

Kapitel 2 beginnt mit der Grundlagenarbeit und löst dabei die uneinheitliche Nutzung der Begriffe in der Gesundheitsdokumentation, genauer den Patientenakten, auf. So wird eine Unterscheidung und gleichzeitig Schärfung der Begriffe vorgenommen und die grundsätzliche Unterscheidung zwischen institutionell- und patientenkontrollierten Akten identifiziert. In diesem Zusammenhang wird erneut der Begriff der Intermediäre im Gesundheitswesen aufgegriffen und ihre Rolle im Gesundheitswesen beschrieben, um im Folgenden auf Basis der detaillierten Beschreibung der in *Kapitel 1* angeführten Konzepte in Deutschland (Telematik-Infrastruktur der GEMATIK und Forschungsinitiativen des BMBF) sowie der Vorstellung des Alternativkonzepts einer *Independent Health Record Bank* Schwächen eben dieser Intermediäre aufzuzeigen,

die nicht nur in der technischen Ausgestaltung liegen, sondern auch unter dem Begriff des *Misplaced Trust* zusammengefasst werden. Neben dem Fakt, dass jeder Intermediär nicht nur ein *Single-Point-of-Truth*, sondern auch ein *Single-Point-of-Failure* darstellt, verfolgen diese zusätzlich eigene Interessen, die denen der Patienten und Leistungserbringer gegenüberstehen können. Ob sich nun die Blockchain-Technologie als Alternativ-Technologie zu Intermediären eignet, wird auf Basis von zwei Bewertungsframeworks geprüft und resultiert in der Annahme, dass sich die Technologie mindestens für ausgewählte Aufgaben, wie bspw. das Identitäts-Management, eignet.

Kapitel 3 setzt die Grundlagenarbeit fort und erläutert die Blockchain-Technologie. So werden neben dem grundsätzlichen Aufbau einer Blockchain die Begriffe *Nodes*, *Transaktionen* und *Konsens* erläutert. Darüber hinaus wird die Taxonomie der Blockchain-Technologien dargestellt und damit die Unterscheidung in *Private* und *Public Blockchain* sowie *Permissioned* und *Unpermissioned Blockchain* beschrieben. Ergänzend werden die *Consortial Blockchain*, ein hybrides Modell der privaten und öffentlichen Blockchain, sowie eine erste Auswahl von Blockchain-Technologien (Bitcoin, Ethereum, Guardtime und Hyperledger) vorgestellt. Diese Liste wird im Laufe der Forschungsarbeit um weitere Technologien ergänzt und in den entsprechenden Kapiteln weiter erläutert. Wie in *Kapitel 2* thematisiert, ist die Verwendung der Blockchain-Technologien zur Disintermediation eine offene Diskussion, weshalb in *Kapitel 3* Potentiale und Limitationen der Technologie unter konkreter Anwendung im Gesundheitswesen aufgezeigt werden. Während die Blockchain Transparenz für alle im Netzwerk und den Zugriff auf Daten entlang des gesamten Behandlungsprozesses sowie in der medizinischen Forschung verspricht, stellt insbesondere der öffentliche Zugang zu diesen Informationen eine Beschränkung der Anwendbarkeit dar. Auch können ökonomische Interessen der Datenverantwortlichen oder technische Limitationen der Einführung eines Blockchain-Netzwerkes entgegenstehen. Dabei ergibt sich ein Trade-off zwischen Kosten und Nutzen eines solchen Systems, der im Rahmen einer Konstruktion grundsätzlich zu berücksichtigen ist.

Kapitel 4 eröffnet die wissenschaftliche Analyse und identifiziert unter Anwendung von Methoden eines systematischen Literature Reviews die für die Forschungsarbeit relevante Literatur. Hierzu werden mehrere Internetsuchmaschinen ausgewählt, die zusammengenommen eine breite Basis unterschiedlicher Fachrichtungen abdecken, ohne sich dabei konkret auf einen Verlag oder eine Domäne zu beschränken. Begonnen mit Stichwortsuchen über Backward- und schließlich Forward-Analysen werden 132 Publikationen für die weitere Analyse identifiziert, wobei 25 Publikationen konkrete Lösungsbeschreibungen präsentieren und 107 Publikationen allgemein an das Thema herangehen und Teilbereiche beschreiben. Eine erste Grobanalyse

wird durchgeführt, die sich nicht nur auf die strukturelle Analyse, bspw. Verteilung auf Jahre oder Verteilung auf Publikationstyp, fokussiert, sondern auch eine Stichwort-Clusterung der in den Publikationen bereitgestellten Stichworte (engl. Keywords) vornimmt. Diese Analyse führt zu der Erkenntnis, dass sich vier Schwerpunkte in der Literatur gebildet haben, nämlich *Aktentyp* (engl. *Record Type*), *Datenhaltung und -bereitstellung* (engl. *Data Storage & Provisioning*), *Sicherheit* (engl. *Security*) und *Technologie* (engl. *Technology*). In diesem Zusammenhang fällt auf, dass in der vorliegenden Literatur eine Diskrepanz nicht nur in der Verwendung bestimmter Begriffe, sondern auch im Umfang der beschriebenen Lösungen existiert. Daraus ergibt sich die wissenschaftliche Notwendigkeit eine Referenzarchitektur zu entwickeln, die diese fragmentierten Informationen aggregiert, evaluiert und zur Wiederverwendung einem breiten Publikum bereitstellt.

Kapitel 5 greift das Thema der Referenzarchitektur auf, beleuchtet die in *Kapitel 1* beschriebene Forschungsmethodik der Referenzmodellierung und führt eine terminologische Abgrenzung zwischen Referenzmodell und Referenzarchitektur durch. Während ein Referenzmodell in der Konzeption neuer Modelle und insbesondere von Prozessen unterstützt, ergänzt eine Referenzarchitektur diese Modelle um technische Aspekte. Da sich beide Referenzmodelle und Referenzarchitekturen speziell in der Softwarearchitektur-Forschung wiederfinden, wird in diesem Kapitel ein Exkurs vorgenommen, der zwischen Software-Architekturen und Informationssystem-Architekturen differenziert. Letztere sind Thema der Wirtschaftsinformatik und ergänzen Software-Architekturen um strategische Aspekte. Da sich in der Clusterbildung in *Kapitel 4* bereits abzeichnet, dass in einer möglichen Referenzarchitektur eine Abhängigkeit der Konstruktionsentscheidungen zum Aktentyp existiert sowie Smart Contracts einen Einfluss auf die Prozessgestaltung in einer möglichen Blockchain-Architektur haben, verbleibt der wissenschaftliche Fokus der Referenzarchitektur auf der *Wirtschaftsinformatik* sowie *Informationssystem-Architekturen*. Im Rahmen der Referenzarchitektur-Definition wird ein Klassifikationsschema identifiziert, das abschließend ausgefüllt wird und die in der Folge konzipierte Referenzarchitektur charakterisiert. Darüber hinaus werden Methoden zur Architektur-Konstruktion beschrieben und erneut eine Einordnung der folgenden Kapitel vorgenommen. Konkret wird eine Methodik gewählt, die Erkenntnisse aus mehreren bestehenden Konstruktionen erfasst und diese aggregiert darstellt.

Kapitel 6 greift die in *Kapitel 4* definierten Cluster auf und analysiert die Literatur detailliert. Dabei werden Variationspunkte identifiziert, die bspw. *Record Type* in die unterschiedlichen Aktentypen und *Security* weiter in *Access Management* und *Identity Management* unterteilen.

Insbesondere in der Klassifizierung der Aktentypen wird erneut das Problem der uneinheitlichen Aktendefinition ersichtlich. Aus diesem Grund wird zu Beginn eine weitere Analyse vorgenommen, die die Begriffe des *data owner* bzw. *user* betrachtet und aus diesen ableitet, ob der der Publikation zugrunde gelegte Aktentyp eine institutions- oder patientenkontrollierte Dokumentation ist. Sämtliche Analyse-Ergebnisse des Kapitels werden als Tabelle unter Nennung der konkreten Publikationen sowie zur quantitativen Darstellung in Balkendiagrammen präsentiert. Darauf folgt die qualitative Beschreibung der Erkenntnisse unter Verweis auf die Literaturquellen. Im Cluster der *Security* wird erneut ein Exkurs präsentiert, der die grundlegenden Konzepte und Begriffe des *Identity and Access Managements* beschreibt sowie dessen Relevanz im Gesundheitswesen. Die Relevanz begründet sich insbesondere in der sicheren Patientenidentifikation und der besonderen Schutzbedürftigkeit von Gesundheitsdaten.

Kapitel 7 konstruiert die in dieser Forschungsarbeit avisierte Referenzarchitektur auf Basis der Beschreibungen und Variationspunkte aus *Kapitel 6*. Einleitend wird die Notation erläutert, anschließend werden die Ergebnisse aus *Kapitel 6* komprimiert zusammengefasst und in Grafiken abgebildet. Dabei wird jede Sicht der Gesamtarchitektur einzeln präsentiert und schlussendlich in einer Gesamtsicht dargestellt. Die strukturierte Analyse der Literatur erlaubt zudem die Entwicklung eines Entscheidungsmodells. Das Entscheidungsmodell basiert auf der Filterung der Analyseergebnisse ausgehend von der Wahl des Aktentyps. So ergeben sich unterschiedliche Schwerpunkte bei den Variationspunkten, bspw. andere Wahlmöglichkeiten, wenn ein Blockchain-Netzwerk für *Patient Summaries* konzipiert wird im Vergleich zu vom Patienten kontrollierten Aktensystemen (*PHR*). Ergänzend zur Referenzarchitektur wird in der Modelldarstellung zusätzlich die Menge an Publikationen angezeigt, um eine Gewichtung der entsprechenden Variationspunkte zu visualisieren.

Kapitel 8 evaluiert die in dieser Forschungsarbeit konzipierte Referenzarchitektur sowie das Entscheidungsmodell. Hierzu werden zu Beginn die unterschiedlichen Methoden zur Evaluation in der Wirtschaftsinformatik beschrieben und schlussendlich eine Kombination aus szenario-basierter und deskriptiver Evaluation gewählt. Insbesondere aufgrund der deskriptiven Evaluation werden in einem nächsten Schritt allgemeine quantitative Ausprägungen eines potentiellen Blockchain-Netzwerks identifiziert und beschrieben. Hierzu gehört eine Übersicht der zu erwartenden Akteure in einem Netzwerk (zwischen 119.000 und ca. 83 Mio.) wie auch die zu erwartende Menge an Daten (approximiert ca. 2,7gb pro Patient mit einer Wachstumsrate von 48% pro Jahr). Bevor die Referenzarchitektur anhand von zwei Szenarien evaluiert wird, wird eine allgemeine Diskussion und Evaluation mehrerer Variationspunkte vorangestellt, sodass auf eine doppelte Ausführung in den Szenarien verzichtet werden kann. Zu diesen Themen

gehören der Vergleich von Cloud und IPFS, ein Vergleich von PKI und KSI sowie die Gegenüberstellung der Blockchain-Technologien inklusive ihrer Konsensprotokolle. Während die Cloud ihre Vorteile insbesondere in ihrer Ressourcenelastizität und Kostenstruktur hat, ist das Interesse eines CSP an den von ihm gespeicherten Daten sowie der Verlust der Verfügungsgewalt über die Daten als nachteilig anzusehen. IPFS hingegen verfolgt einen ähnlichen Ansatz wie die Cloud, speichert Daten allerdings dezentral und stellt ein Register über die Speicherorte bereit. Eben dieses Register ist ein Nachteil, da für die Identifikation von relevanten Daten immer das gesamte Register geprüft wird. Auch ist die Sicherheit eines jeden Knotens im Netzwerk zu gewährleisten, da jeder unsichere Knoten ein Risiko für das gesamte Netzwerk darstellt. Die Diskussion über PKI und KSI offenbart insbesondere die Synergiepotentiale beider Technologien. Eine Kombination sollte folglich in jeder Konzeption in Erwägung gezogen werden. Abschließend werden noch die einzelnen Blockchain-Technologien anhand von 10 Kriterien miteinander verglichen, sodass die Entscheidung für eine Technologie-Auswahl vereinfacht wird. Ein weiterer Exkurs beschreibt eine Menge allgemeiner Risiken einer Blockchain, die in den oben genannten Publikationen erwähnt werden, wie bspw. 51%-Attack, Double-Spending, Sibyll-Attack und Quanten-Computer, sodass neben der reinen Technologie-Auswahl auch ein Bewusstsein für diese Risiken geschaffen wird. Als Szenarien werden zwei aktuell für die Praxis relevante Themen ausgewählt: Eine einrichtungsübergreifende Patientenakte, die nicht nur Behandlungsdaten entlang des gesamten Behandlungsverlaufs bereitstellt, sondern auch den Zugang für Forschung und Kostenträger bereitstellt, sowie als zweites Szenario die Einrichtung eines digitalen Impfpasses. Die Szenarien-Evaluation beginnt grundsätzlich mit der Beschreibung des Szenarios und der Definition von konkreten Anforderungen. Die Anwendung der Referenzarchitektur und des Entscheidungsmodells unter Filterung nach dem entsprechenden Aktentyp führt zur Ableitung von Variationspunkten, die anschließend unter Zuhilfenahme der als *Scholar Literatur* bezeichneten Literatur aus den Jahren 2019 bis 2021 evaluiert werden. Aus dieser Evaluation ergeben sich konkrete Handlungsempfehlungen. Dabei zeigt sich eine hohe Übereinstimmung zwischen den auf Basis der Literatur bis 2018 konstruierten Artefakten und den Beschreibungen in der *Scholar-Literatur*.

Demnach eignen sich die hier konstruierten Artefakte, die Referenzarchitektur und das Entscheidungsmodell, zur Konstruktion blockchain-basierter Patientenakten-Systeme im Gesundheitswesen. Architekten können abhängig vom gewählten Aktentyp entlang der einzelnen Sichten navigieren und entsprechend dem Entscheidungsmodell Variationen für eigene Konstruktionen wählen.

Die Menge und die unterschiedliche inhaltliche Dichte der Publikationen limitiert das Entscheidungsmodell insofern, als nicht für jede Variation eine entsprechende Kombination von Variationspunkten abzuleiten ist. Dies wird insbesondere aus den weniger umfangreich diskutierten Aktentypen, wie dem *Patient Summary*, ersichtlich. Aber auch die Ausführungen der Publikationen sind nicht von einheitlicher inhaltlicher Dichte, wie bereits an den Beschreibungen der Blockchain-Taxonomie zu sehen ist, da sich diese häufig auf *Permissioned* oder *Unpermissioned* bzw. *Private* und *Public* beschränkt, ohne dabei die Kombinationen konkreter herauszuarbeiten. Hier ergeben sich folglich für die wissenschaftliche Forschung weitere Felder für inhaltliche Diskurse.

Literaturverzeichnis

Abid, Amal/Cheikhrouhou, Saoussen/Kallel, Slim/Jmaiel, Mohamed (2021): NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. In: Software: Practice and Experience.

Abunadi, Ibrahim/Kumar, Ramasamy (2021): BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients. In: Sensors (Basel, Switzerland), 21(8).

ACC/HIMSS/RSNA (2005): IT Infrastructure Technical Framework, Volume 1, (ITI TF-1) Integration Profiles. o. O.

Agbo, Cornelius/Mahmoud, Qusay (2019): Comparison of blockchain frameworks for healthcare applications. In: Internet Technology Letters, 2(5): e122.

Ahmad, Raja/Salah, Khaled/Jayaraman, Raja/Yaqoob, Ibrar/Ellahham, Samer/Omar, Mohammed (2020): Blockchain and COVID-19 Pandemic: Applications and Challenges. o. O.

Ahram, Tareq/Sargolzaei, Arman/Sargolzaei, Saman/Daniels, Jeff/Amaba, Ben (2017): Blockchain technology innovations. In: IEEE (Hrsg.): 2017 IEEE Technology & Engineering Management Conference (TEMSCON). Piscataway (NJ, USA): IEEE: 137–141.

Aier, Stephan/Winter, Robert (2009): Virtuelle Entkopplung von fachlichen und IT-Strukturen für das IT/Business Alignment – Grundlagen, Architekturgestaltung und Umsetzung am Beispiel der Domänenbildung. In: Wirtschaftsinformatik, 51(2): 175–191.

Al Omar, Abdullah/Rahman, Mohammad/Basu, Anirban/Kiyomoto, Shinsaku (2017): MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. In: Wang, Guojin/Atiquazzaman, Mohammed/Yan, Zhen (Hrsg.): Security, privacy, and anonymity in computation, communication, and storage. Cham, Switzerland: Springer: 534–543.

Alessi, M./Camillò, A./Giangreco, E./Matera, M./Pino, S./Storelli, D. (2018): Make users own their data: a decentralized personal data store prototype based on Ethereum and IPFS. In: IEEE (Hrsg.): 2018 3rd International Conference on Smart and Sustainable Technologies (SpliTech 2018). Piscataway (NJ, USA): IEEE: 173–179.

Alexaki, Sofia/Alexandris, George/Katos, Vasilis/Nikolaos Petroulakis, E. (2018): Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions. In: IEEE (Hrsg.): 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2018). Piscataway (NJ, USA): IEEE: 254–259.

Alhadhrami, Zainab/Alghfeli, Salma/Alghfeli, Mariam/Abedlla, Juhar/Shuaib, Khaled (2017): Introducing blockchains for healthcare. In: IEEE (Hrsg.): 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA). Piscataway (NJ, USA): IEEE: 374–377.

Ali, Muneeb (2017): Trust-to-Trust design of a new internet, Dissertation. New Jersey.

Ali, Muneeb/Nelson, Jude/Shea, Ryan/Freedman, Michael (2016): Bootstrapping Trust in Distributed Systems with Blockchains. In: ;login:, 41(3): 52–58.

Alpar, Paul/Alt, Rainer/Bensberg, Frank/Weimann, Peter (2019): Anwendungsorientierte Wirtschaftsinformatik. Wiesbaden: Springer Fachmedien Wiesbaden.

Amofa, Sandro/Sifah, Emmanuel/Obour Agyekum, Kwame/Abla, Smahi/Xia, Qi/Gee, James/Gao, Jianbin (2018): A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data. In: IEEE (Hrsg.): 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). Piscataway (NJ, USA): IEEE: 167–172.

Andoni, Merlinda/Robu, Valentin/Flynn, David/Abram, Simone/Geach, Dale/Jenkins, David/McCallum, Peter/Peacock, Andrew (2019): Blockchain technology in the energy sector: A systematic review of challenges and opportunities. In: Renewable and Sustainable Energy Reviews, 100: 143–174.

Angeletti, Fabio/Chatzigiannakis, Ioannis/Vitaletti, Andrea (2017): Privacy preserving data management in recruiting participants for digital clinical trials. In: Association for Computing Machinery (Hrsg.): HumanSys'17: Proceedings of the First International Workshop on Human-centered Sensing, Networking, and Systems. New York (NY, USA): ACM Press: 7–12.

Angelov, Samuil/Trienekens, Jos/Grefen, Paul (2014): Extending and Adapting the Architecture Tradeoff Analysis Method for the Evaluation of SoftwareReference Architectures (Beta Working Paper). Eindhoven, Netherlands.

Angraal, Suveen/Krumholz, Harlan/Schulz, Wade (2017): Blockchain Technology: Applications in Health Care. In: Circulation. Cardiovascular quality and outcomes, 10(9): 1–3.

Antonopoulos, Andreas (2015): Mastering Bitcoin. Sebastopol, CA: O'Reilly Media.

Appavu, Soloman (1997): Analysis of unique patient identifier options. o. O.

Ardagna, Claudio/Cremonini, Marco/Di Capitani Vimercati, Sabrina de/Samarati, Pierangela (2008): A privacy-aware access control system. In: Journal of Computer Security, 16(4): 369–397.

ÄrzteZeitung.de (2019): BMG jetzt mit Mehrheit bei der gematik. URL: https://www.aerztezeitung.de/Wirtschaft/BMG-jetzt-mit-Mehrheit-bei-der-gematik-254819.html, Abruf am 02.05.2021.

Avgeriou, Paris (2003): Describing, Instantiating and Evaluating a Reference Architecture: A Case Study. In: Journal of Computer Science.

Azaria, Asaph/Ekblaw, Ariel/Vieira, Thiago/Lippman, Andrew (2016): MedRec: Using Blockchain for Medical Data Access and Permission Management. In: IEEE (Hrsg.): 2016 2nd International Conference on Open and Big Data. Piscataway (NJ, USA): IEEE: 25–30.

Back, Adam (1997): Hash Cash. URL: http://www.cypherspace.org/hashcash/, Abruf am 16.12.2019.

Back, Adam (2002): Hashcash - A Denial of Service Counter-Measure. URL: http://www.hashcash.org/hashcash.pdf, Abruf am 16.12.2019.

Badr, Shaimaa/Gomaa, Ibrahim/Abd-Elrahman, Emad (2018): Multi-tier Blockchain Framework for IoT-EHRs Systems. In: Procedia Computer Science, 141: 159–166.

Baksi, Dibyendu (2009): Integrating MPI and deduplication engines: a software architecture roadmap. In: International journal of medical informatics, 78(3): 161–169.

Balani, Navveem/Hathi, Rajeev (2017): Enterprise blockchain, First edition. o. O.

Balkin, Jack (2016): Information Fiduciaries and the First Amendment. In: US Davis Law Review, 49(4): 1183.

Banerjee, Mandrita/Lee, Junghee/Choo, Kim-Kwang (2018): A blockchain future for internet of things security: a position paper. In: Digital Communications and Networks, 4(3): 149–160.

Baran, Paul (1964): On Distributed Communications Networks. In: IEEE Transactions on Communications, 12(1): 1–9.

Bass, Len/Clements, Paul/Kazman, Rick (2010): Software architecture in practice, 2. ed, 14. print. Boston (MA): Addison-Wesley.

Baumann, Christian/Dehning, Oliver/Hühnlein, Detlef/Janhoff, Axel/Kudra, André/Lang, Philipp/Pirozhkov, Sebastian/Raumann, Michael/Schmidt, Jörn-Marc/Stommel, Sebastian (2017): TeleTrust-Positionspapier Blockchain. Berlin.

Bayle, Aurelie/Koscina, Mirko/Manset, David/Perez-Kempner, Octavio (2018): When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry. In: IEEE (Hrsg.): 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI 2018). Piscataway (NJ, USA): IEEE: 788–792.

Becker, Jörg (2010): Prozess der gestaltungsorientierten Wirtschaftsinformatik. In: Österle, Hubert/Winter, Robert/Brenner, Walter (Hrsg.): Gestaltungsorientierte Wirtschaftsinformatik. Nürnberg: Infowerk: 13–17.

Becker, Jörg/Holten, Roland/Knackstedt, Ralf/Niehaves, Björn (2004): Epistemiologische Positionierung in der Wirtschaftsinformatik am Beispiel einer konsensorientierten Informationsmodellierung. In: Frank, Ulrich (Hrsg.): Wissenschaftstheorie in Ökonomie und Wirtschaftsinformatik. Wiesbaden: Deutscher Universitätsverlag: 335–366.

Becker, Jörg/Niehaves, Björn/Olbrich, Sebastian/Pfeiffer, Daniel (2009): Forschungsmethodik einer Integrationsdisziplin – Eine Fortführung und Ergänzung zu Lutz Heinrichs „Beitrag zur Geschichte der Wirtschaftsinformatik“ aus gestaltungsorientierter Perspektive. In: Becker, Jörg/Krcmar, Helmut/Niehaves, Björn (Hrsg.): Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik. Heidelberg, New York: Physica-Verlag: 1–22.

Bell, Liam/Buchanan, William/Cameron, Jonathan/Lo, Owen (2018): Applications of Blockchain Within Healthcare. In: Blockchain in Healthcare Today, 1: 1–7.

Benchoufi, Mehdi/Ravaud, Philippe (2017): Blockchain technology for improving clinical research quality. In: Trials, 18(1): 335.

Benet, Juan (2014): IPFS - Content Addressed, Versioned, P2P File System. o. O.

Benhamouda, Fabrice/Halevi, Shai/Halevi, Tzipora (2018): Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation. In: IEEE (Hrsg.): 2018 IEEE International Conference on Cloud Engineering (IC2E 2018). Piscataway (NJ, USA): IEEE: 357–363.

Berentsen, Aleksander/Schär, Fabian (2017): Bitcoin, Blockchain und Kryptoassets, Erste Auflage. Norderstedt: BoD - Books on Demand.

Bernnat, Rainer (2006): Kosten-Nutzen-Analyse der Einrichtung einer Telematik- Infrastruktur im deutschen Gesundheitswesen. Düsseldorf.

Bernnat, Rainer (2016): Weiterentwicklung der eHealth-Strategie. o. O.

Bhuiyan, Md/Zaman, Aliuz/Wang, Tian/Wang, Guojun/Tao, Hai/Hassan, Mohammad (2018): Blockchain and Big Data to Transform the Healthcare. In: Association for Computing Machinery (Hrsg.): ICDPA 2018: Proceedings of the International Conference on Data Processing and Applications. New York (NY, USA): ACM Press: 62–68.

Bitnodes (2020): Global Bitcoin Nodes Distribution. URL: https://bitnodes.io/, Abruf am 24.06.2020.

Bogaerts, Jasper/Decat, Maarten/Lagaisse, Bert/Joosen, Wouter (2015): Entity-Based Access Control. In: Association for Computing Machinery (Hrsg.): Proceedings of the 31st Annual Computer Security Applications Conference on - ACSAC 2015. New York (NY, USA): ACM Press: 291–300.

Bönisch, Sebastian (2017): Was bringt Vernetzung im Gesundheitswesen. Wiesbaden: Springer Fachmedien.

Brennan-Marquez, Kiel (2015): Fourth Amendment Fiduciaries. In: SSRN Electronic Journal: 611-659.

Brewer, Eric (2002): Towards Robust Distributed Systems. Portland (Oregon, USA).

Brocke, Jan vom (2015): Referenzmodellierung: Gestaltung und Verteilung von Konstruktionsprozessen, Dissertation. Berlin.

Brocke, Jan vom/Buddendick, Christian (2004): Organisationsformen in der Referenzmodellierung — Forschungsbedarf und Gestaltungsempfehlungen auf Basis der Transaktionskostentheorie. In: Wirtschaftsinformatik, 46(5): 341–352.

Brogan, James/Baskaran, Immanuel/Ramachandran, Navin (2018): Authenticating Health Activity Data Using Distributed Ledger Technologies. In: Computational and structural biotechnology journal, 16: 257–266.

Brühl, Volker (2017): Bitcoins, Blockchain und Distributed Ledgers. In: Wirtschaftsdienst, 97(2): 135–142.

Bruns, Ralf/Dunkel, Jürgen (2010): Event-Driven Architecture. Berlin: Springer.

Buldas, Ahto/Kroonmaa, Andres/Laanoja, Risto (2013): Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees. In: Riis Nielsen, Hanne/Gollmann, Dieter (Hrsg.): Secure IT Systems. Berlin, Heidelberg: Springer Berlin Heidelberg: 313–320.

Buldas, Ahto/Laanoja, Risto/Truu, Ahto (2017): Keyless signature infrastructure and PKI: hash-tree signatures in pre- and post-quantum world. In: International Journal of Services Technology and Management, 23(1/2): 117–130.

Bundesärztekammer (2019): Ärztestatistik zum 31. Dezember 2019. o. O.

Bundesministerium für Bildung und Forschung (2015): Förderkonzept Medizininformatik. Berlin.

Bundesministerium für Gesundheit (2018): Schnellere Termine, mehr Sprechstunden, bessere Angebote für gesetzlich Versicherte. URL: https://www.bundesgesundheitsministerium.de/terminservice-und-versorgungsgesetz.html, Abruf am 21.01.2019.

Büning, Hans/Lettmann, Theodor (1994): Aussagenlogik: Deduktion und Algorithmen. Wiesbaden: Vieweg+Teubner Verlag.

Burgwinkel, Daniel (2016): Blockchaintechnologie und deren Funktionsweise verstehen. In: Burgwinkel, Daniel (Hrsg.): Blockchain Technology. Berlin, Boston (MA): De Gruyter Oldenbourg: 3–50.

Bussac, Enée (2019): Bitcoin, Ethereum & Co. Berlin: ERICH SCHMIDT VERLAG.

Camp, L. (2004): Digital identity. In: IEEE Technology and Society Magazine, 23(3): 34–41.

Casola, Valentina/Castiglione, Aniello/Choo, Kim-Kwang/Esposito, Christian (2016): Healthcare-Related Data in the Cloud: Challenges and Opportunities. In: IEEE Cloud Computing, 3(6): 10–14.

Castaldo, Luigi/Cinque, Vincenzo (2018): Blockchain-Based Logging for the Cross-Border Exchange of eHealth Data in Europe. In: Gelenbe, Erol/Campegiani, Paolo/Czachórski, Tadeusz/ Katsikas, Sokratis K./ Komnios, Ioannis/ Romano, Luigi/Tzovaras, Dimitrios (Hrsg.): Security in Computer and Information Sciences. Cham, Switzerland: Springer International Publishing: 46–56.

Caumanns, Jörg/Rode, Olaf/Kraufmann, Ben (2017): Umsetzung standardbasierter Sicherheitsdienste mit eGK, HBA und SMC-B. In: Pfannstiel, Mario/Da-Cruz, Patrick/Mehlich, Harald (Hrsg.): Digitale Transformation von Dienstleistungen im Gesundheitswesen I. Wiesbaden: Springer Gabler: 133–148.

Cech, Jakub (2021): A Deep Dive Into IOTA. URL: https://coinmarketcap.com/alexandria/article/a-deep-dive-into-iota, Abruf am 10.10.2021.

Cernian, Alexandra/Tiganoaia, Bogdan/Sacala, Ioan/Pavel, Adrian/Iftemi, Alin (2020): PatientDataChain: A Blockchain-Based Approach to Integrate Personal Health Records. In: Sensors (Basel, Switzerland), 20(22).

Chadwick, David (2009): Federated Identity Management. In: Aldini, Alessandro/Barthe, Gilles/Gorrieri, Roberto (Hrsg.): Foundations of Security Analysis and Design V. Berlin, Heidelberg: Springer Berlin Heidelberg: 96–120.

Chang, Edward/Liao, Shih-Wei/Liu, Chun-Ting/Lin, Wei-Chen/Liao, Pin-Wei/Fu, Wei-Kang/Mei, Chung-Huan/Chang, Emily (2018): DeepLinQ: Distributed Multi-Layer Ledgers for Privacy-Preserving Data Sharing. In: IEEE (Hrsg.): 2018 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR). Piscataway (NJ, USA): IEEE: 173–178.

Chelladurai, Usharani/Pandian, Seethalakshmi (2021): A novel blockchain based electronic health record automation system for healthcare. In: Journal of Ambient Intelligence and Humanized Computing.

Chen, Jieying/Ma, Xiaofeng/Du, Mingxiao/Wang, Zhuping (2018a): A Blockchain Application for Medical Information Sharing. In: IEEE (Hrsg.): 2018 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE 2018). Piscataway (NJ, USA): IEEE: 204–210.

Chen, Yi/Ding, Shuai/Xu, Zheng/Zheng, Handong/Yang, Shanlin (2018b): Blockchain-Based Medical Records Secure Storage and Medical Service Framework. In: Journal of medical systems, 43(1): 5.

Chenthara, Shekha/Ahmed, Khandakar/Wang, Hua/Whittaker, Frank/Chen, Zhenxiang (2020): Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. In: PloS one, 15(12): e0243043.

Choudhury, Olivia/Sylla, Issa/Fairoza, Noor/Das, Amar (2019): A Blockchain Framework for Ensuring Data Quality in Multi-Organizational Clinical Trials. In: IEEE (Hrsg.): 2019 IEEE International Conference on Healthcare Informatics (ICHI 2019). Piscataway (NJ, USA): IEEE: 282–290.

Chowdhury, Mohammad/Colman, Alan/Kabir, Muhammad/Han, Jun/Sarda, Paul (2018): Blockchain as a Notarization Service for Data Sharing with Personal Data Store. In: IEEE (Hrsg.): 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE 2018). Piscataway (NJ, USA): IEEE: 1330–1335.

Cioroaica, Emilia/Chren, Stanislav/Buhnova, Barbora/Kuhn, Thomas/Dimitrov, Dimitar (2019): Towards creation of a reference architecture for trust-based digital ecosystems. In: Association for Computing Machinery (Hrsg.): ECSA '19: Proceedings of the 13th European Conference on Software Architecture - Volume 2. New York (NY, USA): ACM Press: 273–276.

Cisneros, Jose/Aarestrup, Frank/Lund, Ole (2018): Public Health Surveillance using Decentralized Technologies. In: Blockchain in Healthcare Today, 1.

Cloutier, Robert/Muller, Gerrit/Verma, Dinesh/Nilchiani, Roshanak/Hole, Eirik/Bone, Mary (2009): The Concept of Reference Architectures. In: Systems Engineering: 14-27.

Colón, Kenneth (2018): Creating a Patient-Centered, Global, Decentralized Health System: Combining New Payment and Care Delivery Models with Telemedicine, AI, and Blockchain Technology. In: Blockchain in Healthcare Today, 1: 1–18.

Conceição, Arlindo/Silva, Flavio/Rocha, Vladimir/Locoro, Angela/Barguil, João (2018): Eletronic Health Records using Blockchain Technology. o. O.

Confais, Bastien/Lebre, Adrien/Parrein, Benoit (2017): An Object Store Service for a Fog/Edge Computing Infrastructure Based on IPFS and a Scale-Out NAS. In: IEEE (Hrsg.): 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC 2017). Piscataway (NJ, USA): IEEE: 41–50.

Cunningham, James/Ainsworth, John (2017): Enabling Patient Control of Personal Electronic Health Records Through Distributed Ledger Technology. In: IOS Press (Hrsg.): MEDINFO 2017 Proceedings of the 16th World Congress on Medical and Health Informatics. Amsterdam, Netherlands: IOS Press: 45–48.

Cyran, Marek (2018): Blockchain as a Foundation for Sharing Healthcare Data. In: Blockchain in Healthcare Today, 1.

Dagher, Gaby/Mohler, Jordan/Milojkovic, Matea/Marella, Praneeth (2018): Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. In: Sustainable Cities and Society, 39: 283–297.

Dandu, Ravi (2008): Storage media for computers in radiology. In: The Indian journal of radiology & imaging, 18(4): 287–289.

Deka, Sanjib/Goswami, Subhasish/Anand, Abhinav (2020): A Blockchain Based Technique for Storing Vaccination Records. In: IEEE (Hrsg.): 2020 IEEE Bombay Section Signature Conference (IBSSC 2020). Piscataway (NJ, USA): IEEE: 135–139.

Deng, Mina/Scandariato, Riccardo/Cock, Danny de/Preneel, Bart/Joosen, Wouter (2008): Identity in federated electronic healthcare. In: IEEE (Hrsg.): 2008 1st IFIP Wireless Days (WD). Piscataway (NJ, USA): IEEE: 475–479.

Dern, Gernot (2009): Management von IT-Architekturen. Wiesbaden: Springer Fachmedien.

Desai, Harsh/Liu, Kevin/Kantarcioglu, Murat/Kagal, Lalana (2018): Adjudicating Violations in Data Sharing Agreements Using Smart Contracts. In: IEEE (Hrsg.): 2018 IEEE International Conference on Internet of Things (iThings 2018) and IEEE Green Computing and Communications (GreenCom 2018) and IEEE Cyber, Physical and Social Computing (CPSCom 2018) and IEEE Smart Data (SmartData 2018). Piscataway (NJ, USA): IEEE: 1553–1560.

DeSalvo, Karen (2016): Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap. o. O.

Deutsche Krankenhausgesellschaft (2006): Gesetzliche Regelungen zur Telematik: Amtliche Begründungen. o. O.

Deutscher Bundestag (2018): Unterschiedliche Rahmenbedingungen für von der gesetzlichen Krankenversicherung finanzierte elektronische Patienten- und Gesundheitsakten. Berlin.

Deutscher Bundestag (2019a): Antwort: Konkrete Pläne der Bundesregierung zur elektronischen Patientenakte. Berlin.

Deutscher Bundestag (2019b): Kleine Anfrage: Konkrete Pläne der Bundesregierung zur elektronischen Patientenakte. Berlin.

Dias, João/Luís, Reis/Sereno Ferreira, Hugo/Martins, Ângelo (2018): Blockchain for Access Control in e-Health Scenarios. o. O.

Dinov, Ivo (2016): Volume and Value of Big Healthcare Data. In: Journal of medical statistics and informatics, 4(3): 1–7.

Dólera Tormo, Ginés/Gómez Mármol, Felix/Girao, Joao/Martínez Pérez, Gregorio (2013): Identity Management--In Privacy We Trust: Bridging the Trust Gap in eHealth Environments. In: IEEE Security & Privacy Magazine, 11(6): 34–41.

Drescher, Daniel (2017): Blockchain Grundlagen. Frechen: mitp.

Du, Yiwen/Liu, Jianwei/Guan, Zhenyu/Feng, Hanwen (2018): A Medical Information Service Platform Based on Distributed Cloud and Blockchain. In: IEEE (Hrsg.): 2018 IEEE International Conference on Smart Cloud (SmartCloud 2018). Piscataway (NJ, USA): IEEE: 34–39.

Dubovitskaya, Alevtina/Xu, Zhigang/Ryu, Samuel/Schumacher, Michael/Wang, Fusheng (2017): Secure and Trustable Electronic Medical Records Sharing using Blockchain. In: AMIA Annual Symposium Proceedings, 2017: 650–659.

Duden.de (o. J.): In-ter-me-di-är. URL: https://www.duden.de/rechtschreibung/intermediaer, Abruf am 01.01.2022.

Dünnebeil, Sebastian/Sunyaev, Ali/Leimeister, Jan/Krcmar, Helmut (2013): Modulare Softwarearchitektur für Mehrwertanwendungen der deutschen Gesundheitstelematik. In: Wirtschaftsinformatik, 55(1): 3–18.

Eckert, Claudia (2014): IT-Sicherheit, 9, aktualisierte Aufl. Berlin: De Gruyter Oldenbourg.

Eisenstadt, Marc/Ramachandran, Manoharan/Chowdhury, Niaz/Third, Allan/Domingue, John (2020): COVID-19 Antibody Test/Vaccination Certification: There's an App for That. In: IEEE Open Journal of Engineering in Medicine and Biology, 1: 148–155.

Ekblaw, Ariel/Azaria, Asaph/Halamka, John/Lippman, Andrew (2016): A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data. o. O.

EMC/Research & Analysis by IDC (2014): The Digital Universe Driving Data Growth in Healthcare. URL: https://www.cycloneinteractive.com/cyclone/assets/File/digital-universe-healthcare-vertical-report-ar.pdf, Abruf am 06.06.2021.

Erlei, Mathias (1998): Institutionen, Märkte und Marktphasen. Tübingen: Mohr Siebeck.

Esmaeilzadeh, Pouyan/Mirzaei, Tala (2019): The Potential of Blockchain Technology for Health Information Exchange: Experimental Study From Patients' Perspectives. In: Journal of medical Internet research, 21(6): e14184.

Esposito, Christian/Santis, Alfredo de/Tortora, Genny/Chang, Henry/Choo, Kim-Kwang (2018): Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? In: IEEE Cloud Computing, 5(1): 31–37.

Etherscan (2020): Ethereum Node Tracker. URL: https://etherscan.io/nodetracker, Abruf am 24.06.2020.

Fan, Kai/Wang, Shangyang/Ren, Yanhui/Li, Hui/Yang, Yintang (2018): MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. In: Journal of medical systems, 42(8): 136.

Fatokun, Tomilayo/Nag, Avishek/Sharma, Sachin (2021): Towards a Blockchain Assisted Patient Owned System for Electronic Health Records. In: Electronics, 10(5): 580.

Ferdous, Md./Poet, Ron (2013): Portable Personal Identity Provider in Mobile Phones. In: IEEE (Hrsg.): 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2013). Piscataway (NJ, USA): IEEE: 736–745.

Fernández-Alemán, José/Señor, Inmaculada/Lozoya, Pedro/Toval, Ambrosio (2013): Security and privacy in electronic health records: a systematic literature review. In: Journal of biomedical informatics, 46(3): 541–562.

Fettke, Peter/Loos, Peter (2004): Referenzmodellierungsforschung. In: Wirtschaftsinformatik, 46(5): 331–340.

Fiquaro, Monafin/Zahilah, Raja/Othman, Siti/Arshad, Marina/Sheikh Saad, Sheikh (2021): Vaccination System using Blockchain Technology: A Prototype Development. In: IEEE (Hrsg.): 2021 3rd International Cyber Resilience Conference (CRC 2021). Piscataway (NJ, USA): IEEE: 151–156.

Firdaus, Ahmad/Anuar, Nor/Razak, Mohd/Hashem, Ibrahim/Bachok, Syafiq/Sangaiah, Arun (2018): Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management. In: Journal of medical systems, 42(6): 112.

Fragoso Rodriguez, U./Laurent Maknavicius, M./Incera Dieguez, J. (2006): Federated identity architectures. In: MCIS (Hrsg.): Proceedings of 1st Mexican Conference on Informatics Security 2006. o. O.

Franceschi, Matteo/Morelli, Davide/Plans, David/Brown, Alan/Collomosse, John/Coutts, Louise/Ricci, Laura (2019): ComeHere: Exploiting Ethereum for Secure Sharing of

Health-Care Data. In: Mencagli, Gabriele/Hers, Dora (Hrsg.): Euro-Par 2018: Parallel Processing Workshops. Cham, Switzerland: Springer: 585–596.

Franco, Pedro (2014): Understanding Bitcoin. Chichester, UK: John Wiley & Sons, Ltd.

Fritsch, Michael/Wein, Thomas/Ewers, Hans-Jürgen (1999): Marktversagen und Wirtschaftspolitik, 3, völlig überarb. und erw. Aufl. München: Vahlen.

Gagnon, Michael/Stephen, Grant (2018): A Pragmatic Solution to a Major Interoperability Problem: Using Blockchain for the Nationwide Patient Index. In: Blockchain in Healthcare Today, 1.

Galster, Matthias/Avgeriou, Paris (2011): Empirically-grounded reference architectures. In: Association for Computing Machinery (Hrsg.): QoSA-ISARCS '11: Proceedings of the joint ACM SIGSOFT conference -- QoSA and ACM SIGSOFT symposium -- ISARCS on Quality of software architectures -- QoSA and architecting critical systems -- ISARCS. New York (NY, USA): ACM Press: 153–157.

Garcia Ruiz, Manuel/Garcia Chaves, Alvin/Ruiz Ibañez, Carlos/Gutierrez Mazo, Jorge/Ramirez Giraldo, Juan/Pelaez Echavarria, Alejandro/Valencia Diaz, Edison/Pelaez Restrepo, Gustavo/Montoya Munera, Edwin/Garcia Loaiza, Bernardo/Gomez Gonzalez, Sebastian (2011): mantisGRID: a grid platform for DICOM medical images management in Colombia and Latin America. In: Journal of digital imaging, 24(2): 271–283.

Gehring, Stefanie/Eulenfeld, René (2018): German Medical Informatics Initiative: Unlocking Data for Research and Health Care. In: Methods of information in medicine, 57(S 01): e46-e49.

gematik (o. J.a): Gesellschafter und Gremien. URL: https://www.gematik.de/ueber-uns/unternehmensstruktur/, Abruf am 02.05.2021.

gematik (o. J.b): Über die gematik. URL: https://www.gematik.de/ueber-uns/, Abruf am 04.04.2018.

gematik (2008): Gesamtarchitektur. Berlin.

gematik (2013): Speicherstrukturen der eGK für die Fachanwendung VSDM. Berlin.

gematik (2014): Glossar der Telematikinfrastruktur. Berlin.

gematik (2016): Whitepaper Datenschutz und Informationssicherheit. Berlin.

gematik (2017): Systemspezifisches Konzept Versichertenstammdatenmanagement (VSDM). Berlin.

gematik (2018a): Einheitliche elektronische Patientenakte für das deutsche Gesundheitssystem. URL: https://www.gematik.de/news/news/einheitliche-elektronische-patientenakte-fuer-das-deutsche-gesundheitssystem/, Abruf am 19.07.2019.

gematik (2018b): KOM-LE: Für eine sichere Kommunikation unter Kollegen. URL: https://www.gematik.de/news/news/kom-le-fuer-eine-sichere-kommunikation-unter-kollegen/, Abruf am 19.07.2019.

gematik (2018c): Konzept Architektur der TI-Plattform. Berlin.

gematik (2018d): Spezifikation des elektronischen Heilberufsausweises. Berlin.

gematik (2018e): Systemspezifisches Konzept ePA. Berlin.

gematik (2019a): Schemaversion 5.2 VSD - Überblick und Änderungen. Berlin.

gematik (2019b): Spezifikation der elektronischen Gesundheitskarte. Berlin.

Genestier, Philippe/Zouarhi, Sajida/Limeux, Pascal/Excoffier, David/Prola, Alain/Sandon, Stephane/Temerson, Jean-Marc (2017): Blockchain for Consent Management in the eHealth Environment: A Nugget for Privacy and Security Challenges. In: Journal of the International Society for Telemedicine and EHealth, 5: 1–4.

Gesetz für schnellere Termine und bessere Versorgung (Terminservice- und Versorgungsgesetz – TSVG) (TSVG) (2019): Bundesgesetzblatt Teil 1 06.05.2019(18): 646–691. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5B@attr_id=%27bgbl119s0646.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl119s0646.pdf%27%5D__1641117424123, Abruf am 02.01.2022.

Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) (2015): Bundesgesetzblatt Teil 1 21.12.2015(54): 2408–2423. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5B@attr_id=%27bgbl115s2408.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s2408.pdf%27%5D__1641117685253, Abruf am 02.01.2022.

Gesetz zur Änderung des Infektionsschutzgesetzes und anderer Vorschriften (IfSG) (2022): Bundesgesetzblatt Teil 1 18.03.2022(10): 466–472. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5B@attr_id=%27bgbl115s2408.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl122s0466.pdf%27%5D__1654351155921, Abruf am 04.06.2022.

Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV Modernisierungsgesetz - GMG) (GMG) (2003): Bundesgesetzblatt Teil 1 14.11.2003(55): 2190–2258. URL: https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl103s2190.pdf%27%5D__1641116886063, Abruf am 02.01.2022.

Gesetz zur Neuordnung seuchenrechtlicher Vorschriften (SeuchRNeuG) (2000): Bundesgesetzblatt Teil 1 25.07.2000(33): 1045–1077. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl121s4906.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl100033.pdf%27%5D__1654350792347, Abruf am 04.06.2022.

Giebler, Corinna/Gröger, Christoph/Hoos, Eva/Schwarz, Holger/Mitschang, Bernhard (2019): Leveraging the Data Lake: Current State and Challenges. In: Ordonez, Carlos/Song, Il-Yeol/Anderst-Kotsis, Gabriele/ Tjoa, A. Min/Khalil, Ismail (Hrsg.): Big Data Analytics and Knowledge Discovery. Cham, Switzerland: Springer International Publishing: 179–188.

Gilbert, Seth/Lynch, Nancy (2002): Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. In: ACM SIGACT News, 33(2): 51–59.

Gilbert, Seth/Lynch, Nancy (2012): Perspectives on the CAP Theorem. In: Computer, 45(2): 30–36.

Glaser, Florian (2017): Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. In: HICSS (Hrsg.): Proceedings of the 50th Hawaii International Conference on System Sciences (2017). o. O.: AIS Electronic Library (AISeL): 1543–1552.

Glasser, Uwe/Vajihollahi, Mona (2008): Identity management architecture. In: IEEE (Hrsg.): 2008 IEEE International Conference on Intelligence and Security Informatics. Piscataway (NJ, USA): IEEE: 137–144.

GMDS (o. J.): Medizinische Informatik. URL: https://gmds.de/aktivitaeten/medizinische-informatik/, Abruf am 07.02.2019.

Goddard, Maria (2015): Competition in Healthcare: Good, Bad or Ugly? In: International journal of health policy and management, 4(9): 567–569.

Gökalp, Ebru/Gökalp, Mert/Çoban, Selin/Eren, P. (2018): Analysing Opportunities and Challenges of Integrated Blockchain Technologies in Healthcare. In: Wrycza, Stanisław/Maślankowski, Jacek (Hrsg.): Information Systems: Research, Development, Applications, Education. Cham, Switzerland: Springer International Publishing: 174–183.

Gold, J./Ball, M. (2007): The Health Record Banking imperative: A conceptual model. In: IBM Systems Journal, 46(1): 43–55.

Gomes de Andrade, Norberto Nuno/Monteleone, Shara/Martin, Aaron (2013): Electronic identity in Europe. Luxembourg: Publications Office.

Gordon, William/Catalini, Christian (2018): Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. In: Computational and structural biotechnology journal, 16: 224–230.

Graham, I. (1994): HISA - informatics enhancing health. Melbourne.

Gray, Kathleen/Sockolow, Paulina (2016): Conceptual Models in Health Informatics Research: A Literature Review and Suggestions for Development. In: JMIR medical informatics, 4(1): e7.

Greenes, Robert/Shortliffe, Edward (1990): Medical Informatics. In: JAMA, 263(8): 1114–1120.

Greenspan, Gideon (2015): MultiChain Private Blockchain - White Paper. o. O.

Gregor, Shirley/Hevner, Alan (2013): Positioning and Presenting Design Science Research for Maximum Impact. In: MIS Quarterly, 37(2): 337–355.

Grishin, Dennis/Obbad, Kamal/Estep, Preston/Quinn, Kevin/Zaranek, Sarah/Zaranek, Alexander/Vandewege, Ward/Clegg, Tom/César, Nico/Cifric, Mirza/Church, George (2018): Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation. In: Blockchain in Healthcare Today, 1: 1–23.

Grönlund, Åke (2010): Electronic identity management in Sweden: governance of a market approach. In: Identity in the Information Society, 3(1): 195–211.

Gropper, Adrian (2016): Powering the physician-patient relationship with hie of one blockchain health it. Maryland.

Guardtime (2016): Estonian Government, Guardtime Accelerate Adoption of Blockchain Technology to Secure 1M Patient Health Records. URL: https://www.globenewswire.com/news-release/2016/03/03/1202115/0/en/Estonian-Government-Guardtime-Accelerate-Adoption-of-Blockchain-Technology-to-Secure-1M-Patient-Health-Records.html, Abruf am 08.01.2020.

Guardtime (2019): KSI Service Disclosure Statement. URL: https://m.guardtime.com/files/GT-KSI-TSA-DS-v2.2.pdf, Abruf am 03.10.2021.

Guo, Hao/Li, Wanxin/Nejad, Mark/Shen, Chien-Chung (2019): Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture. In: IEEE (Hrsg.): 2019 IEEE International Conference on Blockchain (Blockchain). Piscataway (NJ, USA): IEEE: 44–51.

Guo, Rui/Shi, Huixian/Zhao, Qinglan/Zheng, Dong (2018): Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. In: IEEE Access, 6: 11676–11686.

Gutierrez, Omar/Saavedra, Jeffreys/Zurbaran, Mayra/Salazar, Augusto/Wightman, Pedro (2018): User-Centered Differential Privacy Mechanisms for Electronic Medical Records. In: IEEE (Hrsg.): 2018 International Carnahan Conference on Security Technology (ICCST 2018). Piscataway (NJ, USA): IEEE: 211–217.

Haarbrandt, Birger/Schreiweis, Björn/Rey, Sabine/Sax, Ulrich/Scheithauer, Simone/Rienhoff, Otto/Knaup-Gregori, Petra/Bavendiek, Udo/Dieterich, Christoph/Brors, Benedikt/Kraus, Inga/Thoms, Caroline/Jäger, Dirk/Ellenrieder, Volker/Bergh, Björn/Yahyapour, Ramin/Eils, Roland/HiGHmed Consortium/Marschollek, Michael (2018): HiGHmed - An Open Platform Approach to Enhance Care and Research across Institutional Boundaries. In: Methods of information in medicine, 57(S 01): e66-e81.

Haas, Peter (2006): Gesundheitstelematik. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg.

Haas, Peter (2017): Elektronische Patientenakten. Dortmund: BStift - Bertelsmann Stiftung.

Haas, Sebastian/Wohlgemuth, Sven/Echizen, Isao/Sonehara, Noboru/Müller, Günter (2011): Aspects of privacy for electronic health records. In: International journal of medical informatics, 80(2): e26-e31.

Haber, Stuart/Stornetta, W.Scott (1991): How to time-stamp a digital document. In: Journal of Cryptology, 3(2): 99-11.

Halamka, John (2011): The Cost of Storing Patient Records. URL: http://geekdoctor.blogspot.com/2011/04/cost-of-storing-patient-records.html, Abruf am 06.06.2021.

Han, Huirui/Huang, Mengxing/Zhang, Yu/Bhatti, Uzair (2018): An Architecture of Secure Health Information Storage System Based on Blockchain Technology. In: Sun, Xingming/Pan, Zhaoqing/Bertino, Elisa (Hrsg.): Cloud Computing and Security. Cham, Switzerland: Springer International Publishing: 578–588.

Hang, Lei/Kim, BumHwi/Kim, KyuHyung/Kim, DoHyeun (2021): A Permissioned Blockchain-Based Clinical Trial Service Platform to Improve Trial Data Transparency. In: BioMed research international, 2021: 5554487.

Hanley, Mark/Tewari, Hitesh (2018): Managing Lifetime Healthcare Data on the Blockchain. In: IEEE (Hrsg.): 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/UIC/ATC/SCALCOM/CBDCom/IOP/SC. Piscataway (NJ, USA): IEEE: 246–251.

Hansen, Hans/Mendling, Jan/Neumann, Gustaf (2015): Wirtschaftsinformatik, 11, völlig neu bearb. Aufl. Berlin [u.a.]: De Gruyter.

Hansen, Marit/Meints, Martin (2006): Digitale Identitäten — Überblick und aktuelle Trends. In: Datenschutz und Datensicherheit - DuD, 30(9): 543–547.

Heinrich, Lutz (2005): Forschungsmethodik einer Integrationsdisziplin: Ein Beitrag zur Geschichte der Wirtschaftsinformatik. In: NTM International Journal of History and Ethics of Natural Sciences, Technology and Medicine, 13(2): 104–117.

Heinrich, Lutz/Heinzl, Armin/Riedl, René (2011): Wirtschaftsinformatik, 4, überarb. und erw. Aufl. Berlin [u.a.]: Springer.

Hernández-Ramos, José/Karopoulos, Georgios/Geneiatakis, Dimitris/Martin, Tania/Kambourakis, Georgios/Fovino, Igor (2021): Sharing pandemic vaccination certificates through blockchain: Case study and performance evaluation. o. O.

Hevner, Alan (2007): A Three Cycle View of Design Science Research. In: Scandinavian Journal of Information Systems, 19(2): 87–92.

Hevner, Alan/Chatterjee, Samir (2010): Design Research in Information Systems. Boston (MA): Springer Science+Business Media LLC.

Hevner, Alan/March, Salvatore/Park, Jinsoo (2004): Design Science in Information Systems Research. In: MIS Quarterly, 28(1): 75–105.

Hirano, Tomonobu/Motohashi, Tomomitsu/Okumura, Kosuke/Takajo, Kentaro/Kuroki, Taiyo/Ichikawa, Daisuke/Matsuoka, Yutaka/Ochi, Eisuke/Ueno, Taro (2020): Data Validation and Verification Using Blockchain in a Clinical Trial for Breast Cancer: Regulatory Sandbox. In: Journal of medical Internet research, 22(6): e18938.

Hoffmann, Martin (2007): Architecture Evaluation Methods. o. O.

Hölbl, Marko/Kompara, Marko/Kamišalić, Aida/Nemec Zlatolas, Lili (2018): A Systematic Review of the Use of Blockchain in Healthcare. In: Symmetry, 10(10): 470.

Hou, Li-Yuan/Tang, Tsung-Yi/Liang, Tyng-Yeu (2020): IOTA-BT: A P2P File-Sharing System Based on IOTA. In: Electronics, 9(10): 1610.

Hovenga, Evelyn/Kidd, Michael/Garde, Sebastian/Lucay Cossio, Carola (2010): Health informatics. In: Hovenga, Evelyn/Kidd, Michael/Garde, Sebastian/Lucay Cossio, Carola Hullin (Hrsg.): Health informatics. Washington (D.C, USA): IOS Press: 9–15.

Hu, Hongxin/Ahn, Gail-Joon/Jorgensen, Jan (2013): Multiparty Access Control for Online Social Networks: Model and Mechanisms. In: IEEE Transactions on Knowledge and Data Engineering, 25(7): 1614–1627.

Hu, Jun/Peyton, Liam (2009): Integrating Identity Management With Federated Healthcare Data Models. In: Aalst, Will/Babin, Gilbert/Kropf, Peter/ Mylopoulos, John/ Sadeh, Norman M./ Shaw, Michael J./ Szyperski, Clemens/Weiss, Michael (Hrsg.): E-Technologies: Innovation in an Open World. Berlin, Heidelberg: Springer: 100–112.

Hu, Vincent/Ferraiolo, David/Kuhn, Rick/Schnitzer, Adam/Sandlin, Kenneth/Miller, Robert/Scarfone, Karen (2014): Guide to Attribute Based Access Control (ABAC) Definition and Considerations. o. O.: National Institute of Standards and Technology.

Huber, Michael/Sunyaev, Ali/Krcmar, Helmut (2008): Technische Sicherheitsanalyse der elektronischen Gesundheitskarte. München.

Huesch, D./Mosher, T. (2017): Using It or Losing It? The Case for Data Scientists Inside Health Care. URL: https://catalyst.nejm.org/doi/full/10.1056/CAT.17.0493, Abruf am 06.06.2021.

Hussein, Ahmed/ArunKumar, N./Ramirez-Gonzalez, Gustavo/Abdulhay, Enas/Tavares, João/Albuquerque, Victor de (2018): A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform. In: Cognitive Systems Research, 52: 1–11.

Hussien, H./Yasin, S./Udzir, S./Zaidan, A./Zaidan, B. (2019): A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. In: Journal of medical systems, 43(10): 320.

Hylock, Ray/Zeng, Xiaoming (2019): A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. In: Journal of medical Internet research, 21(8): e13592.

Hyperledger (2021): hyperledger-fabricdocs Documentation. o. O.

International Organization of Standardization (2005): ISO/TR 20514:2005 - Health informatics - Electronic health record - Definition, scope and context. Geneva, Switzerland.

IOTA Foundation (2017): IOTA Development Roadmap. URL: https://blog.iota.org/iota-development-roadmap-74741f37ed01/, Abruf am 03.10.2021.

IOTA Foundation (2019): TheCoordicide. o. O.

IOTA Foundation (2021a): Incentives to Run an IOTA Node. URL: https://blog.iota.org/incentives-to-run-an-iota-node/, Abruf am 12.06.2022.

IOTA Foundation (2021b): IOTA Smart Contracts Protocol Alpha Release. URL: https://blog.iota.org/iota-smart-contracts-protocol-alpha-release/, Abruf am 03.10.2021.

Ismail, Leila/Materwala, Huned (2020): BlockHR - A Blockchain-based Framework for Health Records Management. In: Association for Computing Machinery (Hrsg.): ICCMS '20: Proceedings of the 12th International Conference on Computer Modeling and Simulation. New York (NY, USA): ACM Press: 164–168.

ISO/IEC (Hrsg.): ISO/IEC 29146:2016 - Information technology - Security techniques - A framework for access management, 2016.

ISO/IEC (Hrsg.): Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts, 2019.

Issel, L. (2014): It's health care, not healthcare. In: Health care management review, 39(4): 269.

Ito, Kenichi/Tago, Kiichi/Jin, Qun (2018): i-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data. In: IEEE (Hrsg.): 2018 9th International Conference on Information Technology in Medicine and Education (ITME). Piscataway (NJ, USA): IEEE: 829–833.

Jentzsch, Nicola (2018): Dateneigentum. Berlin.

Jiang, Hao/Peng, Hao/Dian, Songyi (2018): A Design of Medical Information Sharing Model Based on Blockchain Technology. In: IOP Conference Series: Materials Science and Engineering, 428: 12006.

Jiang, Shan/Cao, Jiannong/Wu, Hanqing/Yang, Yanni/Ma, Mingyu/He, Jianfei (2018): BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange. In: IEEE (Hrsg.): 2018 IEEE International Conference on Smart Computing (SMARTCOMP 2018). Piscataway (NJ, USA): IEEE: 49–56.

Johnston, David/Yilmaz, Sam/Kandah, Jeremy/Bentenitis, Nikos/Hashemi, Farzad/Gross, Ron/Wilkinson, Shawn/Mason, Steven (2014): The General Theory of Decentralized Applications, DApps. o. O.

Jøsang, Audun/Fabre, John/Hay, Brian/Dalziel, James/Pope, Simon (2005): Trust requirements in identity management. In: Australian Computer Society (Hrsg.): ACSW Frontiers '05: Proceedings of the 2005 Australasian workshop on Grid computing and e-research. Darlinghurst: Australian Computer Society: 99–108.

Just, Beth/Marc, David/Munns, Megan/Sandefer, Ryan (2016): Why Patient Matching Is a Challenge: Research on Master Patient Index (MPI) Data Discrepancies in Key Identifying Fields. In: Perspectives in health information management, 13: 1e.

Kamau, Gabriel/Boore, Caroline/Maina, Elizaphan/Njenga, Stephen (2018): Blockchain Technology: Is this the Solution to EMR Interoperability and Security Issues in Developing Countries? In: IEEE (Hrsg.): 2018 IST-Africa Week Conference (IST-Africa 2018). Piscataway (NJ, USA): IEEE: 618–625.

Kamel Boulos, Maged/Wilson, James/Clauson, Kevin (2018): Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. In: International journal of health geographics, 17: 25.

Kassenärztliche Bundesvereinigung (2017): KBV-Positionen zur elektronischen Patientenakte. Berlin.

Kaur, Harleen/Alam, M./Jameel, Roshan/Mourya, Ashish/Chang, Victor (2018): A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. In: Journal of medical systems, 42(8): 156.

Kienzler, Romeo (2016): Hyperledger – eine offene Blockchain Technologie. In: Burgwinkel, Daniel (Hrsg.): Blockchain Technology. Berlin, Boston (MA): De Gruyter Oldenbourg: 111–122.

Kim, Kyoung-jin/Hong, Seng-phil (2017): A Trusted Sharing Model for Patient Records based on Permissioned Blockchain. In: Journal of Internet Computing and Services, 18(6): 75–84.

Kim, Seung-Hyun/Ko, Han-Gyu/Choi, Daeseon/Kim, Soo/Jin, Seunghun (2008): Personalized Identity Agent for User-Centric IdM. In: IEEE (Hrsg.): 2008 The 10th International Conference on Advanced Communication Technology. Piscataway (NJ, USA): IEEE: 1308–1313.

Kirkham, Tom/Winfield, Sandra/Ravet, Serge/Kellomaki, Sampo (2013): The Personal Data Store Approach to Personal Data Security. In: IEEE Security & Privacy Magazine, 11(5): 12–19.

Kish, Leonard/Topol, Eric (2015): Unpatients-why patients should own their medical data. In: Nature biotechnology, 33(9): 921–924.

Kiyomoto, Shinsaku/Rahman, Mohammad/Basu, Anirban (2017): On blockchain-based anonymized dataset distribution platform. In: IEEE (Hrsg.): 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA 2017). Piscataway (NJ, USA): IEEE: 85–92.

Klebsch, Wolfgang/Hallensleben, Sebastian/Kosslers, Sebastian (2019): Roter Faden durch das Thema Blockchain. Frankfurt am Main.

Knaup, Petra/Deserno, Thomas/Prokosch, Hans-Ulrich/Sax, Ulrich (2018): Implementation of a National Framework to Promote Health Data Sharing. In: Yearbook of medical informatics, 27(01): 302–304.

Kombe, Cleverence/Ally, Mussa/Sam, Anael (2018): A review on healthcare information systems and consensus protocols in blockchain technology. In: International Journal of Advanced Technology and Engineering Exploration, 5(49): 473–483.

Kotsiuba, Igor/Velvkzhanin, Artem/Yanovich, Yury/Bandurova, Iuna/Dyachenko, Yuriy/Zhygulin, Viacheslav (2018): Decentralized e-Health Architecture for Boosting Healthcare Analytics. In: IEEE (Hrsg.): 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4 2018). Piscataway (NJ, USA): IEEE: 113–118.

Krcmar, Helmut (1990): Bedeutung und Ziele von Informationssystem-Architekturen. In: Wirtschaftsinformatik, 32(5): 395–402.

Krcmar, Helmut (2015): Informationsmanagement, 6, überarb. Aufl. Wiesbaden: Springer Gabler.

Kruchten, P. (1995): The 4+1 View Model of architecture. In: IEEE Software, 12(6): 42–50.

Kumar, Tanesh/Ramani, Vidhya/Ahmad, Ijaz/Braeken, An/Harjula, Erkki/Ylianttila, Mika (2018): Blockchain Utilization in Healthcare: Key Requirements and Challenges. In: IEEE (Hrsg.): 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). Piscataway (NJ, USA): IEEE: 154–160.

Kung, Hsin/Cheng, Ya-Fang/Lee, Hsiu-An/Hsu, Chien-Yeh (2020): Personal Health Record in FHIR Format Based on Blockchain Architecture. In: Hung, Jason/Yen, Neil/Chang, Jia-Wei (Hrsg.): Frontier Computing. Singapore: Springer Singapore: 1776–1788.

Kuo, Alex (2011): Opportunities and challenges of cloud computing to improve health care services. In: Journal of medical Internet research, 13(3): e67.

Kuo, Tsung-Ting/Kim, Hyeon-Eui/Ohno-Machado, Lucila (2017): Blockchain distributed ledger technologies for biomedical and health care applications. In: Journal of the American Medical Informatics Association : JAMIA, 24(6): 1211–1220.

Kuo, Tsung-Ting/Ohno-Machado, Lucila (2018): ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. o. O.

Kuo, Tsung-Ting/Zavaleta Rojas, Hugo/Ohno-Machado, Lucila (2019): Comparison of blockchain platforms: a systematic review and healthcare examples. In: Journal of the American Medical Informatics Association, 26(5): 462–478.

Lamport, Leslie/Shostak, Robert/Pease, Marshall (1982): The Byzantine Generals Problem. In: ACM Transactions on Programming Languages and Systems, 4(3): 382–401.

Lazar, Max/Pan, Zihang/Ragguett, Renee-Marie/Lee, Yena/Subramaniapillai, Mehala/Mansur, Rodrigo/Rodrigues, Nelson/McIntyre, Roger (2017): Digital revolution in depression: A technologies update for clinicians. In: Personalized Medicine in Psychiatry, 4-6: 1–6.

Leimeister, Jan (2015): Einführung in die Wirtschaftsinformatik, 12. vollst. neu überarb. und aktualisierte Aufl. Berlin [u.a.]: Springer Gabler.

Levy, Yair/J. Ellis, Timothy (2006): A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. In: Informing Science: The International Journal of an Emerging Transdiscipline, 9: 181–212.

Li, Hongyu/Zhu, Liehuang/Shen, Meng/Gao, Feng/Tao, Xiaoling/Liu, Sheng (2018): Blockchain-Based Data Preservation System for Medical Data. In: Journal of medical systems, 42(8): 141.

Li, Ming/Yu, Shucheng/Ren, Kui/Lou, Wenjing (2010): Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings. In: Jajodia, Sushil/Zhou, Jianying (Hrsg.): Security and Privacy in Communication Networks. Berlin, Heidelberg: Springer Berlin Heidelberg: 89–106.

Liang, Xueping/Shetty, Sachin/Tosh, Deepak/Bowden, Daniel/Njilla, Laurent/Kamhoua, Charles (2018a): Towards Blockchain Empowered Trusted and Accountable Data Sharing and Collaboration in Mobile Healthcare Applications. In: EAI Endorsed Transactions on Pervasive Health and Technology, 4(15): e3.

Liang, Xueping/Shetty, Sachin/Tosh, Deepak/Kamhoua, Charles/Kwiat, Kevin/Njilla, Laurent (2017a): ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In: IEEE (Hrsg.): 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID 2017). Piscataway (NJ, USA): IEEE: 468–477.

Liang, Xueping/Shetty, Sachin/Zhao, Juan/Bowden, Daniel/Li, Danyi/Liu, Jihong (2018b): Towards Decentralized Accountability and Self-sovereignty in Healthcare Systems. In: Qing, Sihan/Mitchell, Chris/Chen, Liqun/Liu, Dongmei (Hrsg.): Information and Communications Security. Cham, Switzerland: Springer International Publishing: 387–398.

Liang, Xueping/Zhao, Juan/Shetty, Sachin/Liu, Jihong/Li, Danyi (2017b): Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: IEEE (Hrsg.): 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC 2017). Piscataway (NJ, USA): IEEE: 1167–1171.

Liao, Katherine/Cai, Tianxi/Gainer, Vivian/Goryachev, Sergey/Zeng-treitler, Qing/Raychaudhuri, Soumya/Szolovits, Peter/Churchill, Susanne/Murphy, Shawn/Kohane, Isaac/Karlson, Elizabeth/Plenge, Robert (2010): Electronic medical records for discovery research in rheumatoid arthritis. In: Arthritis care & research, 62(8): 1120–1127.

Linn, Laure/Koo, Martha (2016): Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research. In: Use of Blockchain for Healthcare and Research Workshop.

Liu, Jingwei/Li, Xiaolu/Ye, Lin/Zhang, Hongli/Du, Xiaojiang/Guizani, Mohsen (2018): BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records.

In: IEEE (Hrsg.): 2018 IEEE Global Communications Conference (GLOBECOM). Piscataway (NJ, USA): IEEE: 6186–6191.

Liu, Paul (2016): Medical Record System Using Blockchain, Big Data and Tokenization. In: Lam, Kwok-Yan/Chi, Chi-Hung/Qing, Sihan (Hrsg.): Information and communications security. Cham, Switzerland: Springer: 254–261.

Liu, W./Zhu, S./Mundie, T./Krieger, U. (2017): Advanced Block-Chain Architecture for e-Health Systems. In: IEEE (Hrsg.): 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom). Piscataway (NJ, USA): IEEE: 37–42.

Livari, Juhani (2007): A paradigmatic analysis of information systems as a design science. In: Scandinavian Journal of Information Systems, 19: 39.

Lo, Sin/Xu, Xiwei/Chiam, Yin/Lu, Qinghua (2017): Evaluating Suitability of Applying Blockchain. In: IEEE (Hrsg.): 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS). Piscataway (NJ, USA): IEEE: 158–161.

Looser, Hansjörg (2010): Patientenidentifikation – ein Beitrag zur integrierten und prozessorientierten Versorgung. In: Rohner, Peter/Winter, Robert (Hrsg.): Patientenidentifikation und Prozessorientierung. Berlin: Springer: 1–13.

Lux, Thomas (2017): E-Health - Begriff und Abgrenzung. In: Müller-Mielitz, Stefan/Lux, Thomas (Hrsg.): E-Health-Ökonomie. Wiesbaden: Springer Gabler: 3–22.

Macdonald, M./Liu-Thorrold, L./Julien, R. (2017): The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin. o. O.

Mackey, Tim/Miyachi, Ken/Fung, Danny/Qian, Samson/Short, James (2020): Combating Health Care Fraud and Abuse: Conceptualization and Prototyping Study of a Blockchain Antifraud Framework. In: Journal of medical Internet research, 22(9): e18623.

Madine, Mohammad/Battah, Ammar/Yaqoob, Ibrar/Salah, Khaled/Jayaraman, Raja/Al-Hammadi, Yousof/Pesic, Sasa/Ellahham, Samer (2020a): Blockchain for Giving Patients Control Over Their Medical Records. In: IEEE Access, 8: 193102–193115.

Madine, Mohammad/Salah, Khaled/Jayaraman, Raja/Yaqoob, Ibrar/Al-Hammadi, Yousof/Ellahham, Samer/Calyam, Prasad (2020b): Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records. In: IEEE Access, 8: 225777–225791.

Magyar, Gabor (2017): Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. In: IEEE (Hrsg.): 2017 IEEE 30th Neumann Colloquium (NC 2017). Piscataway (NJ, USA): IEEE: 135–140.

Mahlmann, Peter/Schindelhauer, Christian (2007): Peer-to-Peer-Netzwerke. Berlin: Springer.

Maini, Ekta/Venkateswarlu, Bondu/Gupta, Arbind (2020): Bringing Digital Transformation from a Traditional RDBMS Centric Solution to a Big Data Platform with Azure Data Lake Store. In: Smys, S./Iliyasu, Abdullah/Bestak, Robert/Shi, Fuqian (Hrsg.): New Trends in Computational Vision and Bio-inspired Computing. Cham, Switzerland: Springer International Publishing: 595–601.

Mani, Vinodhini/Manickam, Prakash/Alotaibi, Youseef/Alghamdi, Saleh/Khalaf, Osamah (2021): Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. In: Electronics, 10(23): 3003.

Marhold, Klaus/Fell, Jan (2021): Electronic vaccination certificates: avoiding a repeat of the contact-tracing 'format wars'. In: Nature medicine, 27(5): 738739.

Massias, H./Serret Avila, X./Quisquater, J.-J. (1999): Design of a secure timestamping service with minimal trust requirement. In: Barbé, A. (Hrsg.): Proceedings of the 20th Symposium on Information Theory in the Benelux. Enschede: Werkgemeenschaft voor Informatie en Communicatietheorie: 79–86.

Mathis, Christian (2017): Data Lakes. In: Datenbank-Spektrum, 17(3): 289–293.

Mbunge, Elliot (2020): Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls. In: Diabetes & metabolic syndrome, 14(6): 1631–1636.

Mbunge, Elliot/Dzinamarira, Tafadzwa/Fashoto, Stephen/Batani, John (2021): Emerging technologies and COVID-19 digital vaccination certificates and passports. In: Public health in practice (Oxford, England), 2: 100136.

McFarlane, Chrissa/Beer, Michael/Brown, Jesse/Prendergast, Nelson (2017): Patientory : A Healthcare Peer-to-Peer EMR Storage Network v1.1. o. O.

Medicalchain (2018): Whitepaper: Medicalchain. o. O.

Medizininformatik-Initiative (o. J.): DIFUTURE. URL: https://www.medizininformatik-initiative.de/de/konsortien/difuture, Abruf am 22.07.2019.

Meier, Pascal/Beinke, Jan/Fitte, Christian/Schulte to Brinke, Jan/Teuteberg, Frank (2021): Generating design knowledge for blockchain-based access control to personal health records. In: Information Systems and e-Business Management, 19(1): 13–41.

Meinel, Christoph/Gayvoronskaya, Tatiana/Schnjakin, Maxim (2018): Blockchain. Potsdam: Universitätsverlag Potsdam.

Mendes, David/Rodrigues, Irene/Fonseca, César/Lopes, Manuel/García-Alonso, José/Berrocal, Javier (2018): Anonymized Distributed PHR Using Blockchain for Openness and Non-repudiation Guarantee. In: Méndez, Eva/Crestani, Fabio/Ribeiro, Cristina/ David,

Gabriel/Lopes, João Correia (Hrsg.): 22nd International Conference on Theory and Practice of Digital Libraries, TPDL 2018. Cham, Switzerland: Springer International Publishing: 381–385.

Mense, Alexander/Athanasiadis, Leandros (2018): Concept for Sharing Distributed Personal Health Records with Blockchains. In: Studies in health technology and informatics, 251: 7–10.

Merz, Michael (2016): Einsatzpotenziale der Blockchain im Energiehandel. In: Burgwinkel, Daniel (Hrsg.): Blockchain Technology. Berlin, Boston (MA): De Gruyter Oldenbourg: 51–98.

Mikula, Tomas/Jacobsen, Rune (2018): Identity and Access Management with Blockchain in Electronic Healthcare Records. In: IEEE (Hrsg.): 2018 21st Euromicro Conference on Digital System Design (DSD 2018). Piscataway (NJ, USA): IEEE: 699–706.

Moher, David/Liberati, Alessandro/Tetzlaff, Jennifer/Altman, Douglas (2009): Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. In: PLoS medicine, 6(7): e1000097.

Muller, Gerrit/van de Laar, Piërre (2011): Researching Reference Architectures. In: van de Laar, Pierre/Punter, Teade (Hrsg.): Views on Evolvability of Embedded Systems. Dordrecht: Springer Netherlands: 107–119.

MultiChain.com (o. J.): Tips for performance optimization. URL: https://www.multichain.com/developers/performance-optimization/, Abruf am 10.10.2021.

MultiChain.com (2015): MultiChain Private Blockchain - White Paper. o. O.

Mutschler, Ernst/Geisslinger, Gerd/Kroemer, Heyo/Menzel, Sabine/Ruth, Peter (2013): Mutschler Arzneimittelwirkungen, 10, vollständig überarbeitete und erweiterte Auflage. Stuttgart: WVG Wissenschaftliche Verlagsgesellschaft.

Mwachofi, Ari/Al-Assaf, Assaf (2011): Health care market deviations from the ideal market. In: Sultan Qaboos University medical journal, 11(3): 328–337.

Nagasubramanian, Gayathri/Sakthivel, Rakesh/Patan, Rizwan/Gandomi, Amir/Sankayya, Muthuramalingam/Balusamy, Balamurugan (2018): Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. In: Neural Computing and Applications: 639–647.

Nakagawa, Elisa/Guessi, Milena/Maldonado, Jose/Feitosa, Daniel/Oquendo, Flavio (2014): Consolidating a Process for the Design, Representation, and Evaluation of Reference Architectures. In: IEEE (Hrsg.): 2014 IEEE/IFIP Conference on Software Architecture (WICSA 2014). Piscataway (NJ, USA): IEEE: 143–152.

Nakagawa, Elisa/Oquendo, Flavio/Becker, Martin (2012): RAModel: A Reference Model for Reference Architectures. In: IEEE (Hrsg.): 2012 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture (WICSA-ECSA 2012). Piscataway (NJ, USA): IEEE: 297–301.

Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. o. O.

Narayan, Shivaramakrishnan/Gagné, Martin/Safavi-Naini, Reihaneh (2010): Privacy preserving EHR system using attribute-based infrastructure. In: Association for Computing Machinery (Hrsg.): CCSW '10: Proceedings of the 2010 ACM workshop on Cloud computing security workshop. New York (NY, USA): ACM Press: 47–52.

National HIE Governance Forum (2013): Identity and Access Management for Health Information Exchange. o. O.

Nguyen, Dinh/Pathirana, Pubudu/Ding, Ming/Seneviratne, Aruna (2019): Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. In: IEEE Access, 7: 66792–66806.

Ni, Qun/Bertino, Elisa/Lobo, Jorge/Brodie, Carolyn/Karat, Clare-Marie/Karat, John/Trombeta, Alberto (2010): Privacy-aware role-based access control. In: ACM Transactions on Information and System Security, 13(3): 24.

Nichol, Peter/Brandt, Jeff (2016): Co-Creation of Trust for Healthcare: The Cryptocitizen Framework for Interoperability with Blockchain. o. O.: Unpublished.

Niu, Shufen/Chen, Lixia/Wang, Jinfeng/Yu, Fei (2020): Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain. In: IEEE Access, 8: 7195–7204.

Noh, Si-Wan/Park, Youngho/Sur, Chur/Shin, Sang-Uk/Rhee, Kyung-Hyune (2017): Blockchain-Based User-Centric Records Management System. In: International Journal of Control and Automation, 10(11): 133–144.

Nortey, Richard/Yue, Li/Agdedanu, Promise/Adjeisah, Michael (2019): Privacy Module for Distributed Electronic Health Records(EHRs) Using the Blockchain. In: IEEE (Hrsg.): 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA 2019). Piscataway (NJ, USA): IEEE: 369–374.

Novikov, Sergey/Kazakov, Oleg/Kulagina, Natalya/Azarenko, Natalya (2018): Blockchain and Smart Contracts in a Decentralized Health Infrastructure. In: IEEE (Hrsg.): 2018 IEEE International Conference 'Quality Management, Transport and Information Security, Information Technologies' (IT&QM&IS 2018). Piscataway (NJ, USA): IEEE: 697–703.

Nuss, Martin/Puchta, Alexander/Kunz, Michael (2018): Towards Blockchain-Based Identity and Access Management for Internet of Things in Enterprises. In: Furnell, Steven/Mouratidis, Haralambos/Pernul, Günther (Hrsg.): Trust, Privacy and Security in Digital Business. Cham, Switzerland: Springer International Publishing: 167–181.

OECD (2013): OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. URL: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2, Abruf am 15.06.2020.

OECD (2017): Health at a Glance 2017: OECD Indicators. Paris: OECD Publishing.

Oliveira, Marcela/Carrara, Gabriel/Fernandes, Natalia/Albuquerque, Celio/Carrano, Ricardo/Medeiros, Dianne/Mattos, Diogo (2019): Towards a Performance Evaluation of Private Blockchain Frameworks using a Realistic Workload. In: IEEE (Hrsg.): 2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN 2019). Piscataway (NJ, USA): IEEE: 180–187.

Omar, I./Jayaraman, R./Salah, K./Simsekler, M. (2019): Exploiting Ethereum Smart Contracts for Clinical Trial Management. In: IEEE (Hrsg.): 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA 2019). Piscataway (NJ, USA): IEEE: 1–6.

Otto, Boris/Jürjens, Jan/Schon, Jochen/Auer, Sören/Menz, Nadja/Wenzel, Sven/Cirullies, Jan (2016): Industrial Data Space. München.

Patel, Vishal (2018): A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. In: Health informatics journal: 1-14.

Peffers, Ken/Tuunanen, Tuure/Rothenberger, Marcus/Chatterjee, Samir (2007): A Design Science Research Methodology for Information Systems Research. In: Journal of Management Information Systems, 24(3): 45–77.

Perry, Dewayne/Wolf, Alexander (1992): Foundations for the study of software architecture. In: ACM SIGSOFT Software Engineering Notes, 17(4): 40–52.

Peterson, Kevin/Deeduvanu, Rammohan/Kanjamala, Pradip/Boles, Kelly (2016): A Blockchain-Based Approach to Health Information Exchange Networks. o. O.

Pfitzmann, Andreas/Hansen, Marit (2008): Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology. o. O.

Pfitzmann, Andreas/Hansen, Marit (2010): A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. o. O.

Phansalkar, Ajeet (2021): Open-Source Software Challenges and Opportunities. In: Sharma, Neha/Chakrabarti, Amlan/Balas, Valentina/Martinovic, Jan (Hrsg.): Data Management, Analytics and Innovation. Singapore: Springer Singapore: 33–42.

Phan-Vogtmann, Lo/Helhorn, Alexander/Kruse, Henner/Thomas, Eric/Heidel, Andrew/Saleh, Kutaiba/Rissner, Florian/Specht, Martin/Henkel, Andreas/Scherag, André/Ammon, Danny (2019): Approaching Clinical Data Transformation from Disparate Healthcare IT Systems Through a Modular Framework. In: Shabo, Amnon/Madsen, Inge/Prokosch, Hans-Ulrich/ Häyrinen, Kristiina/ Wolf, Klaus-Hendrik/ Martin-Sanchez, Fernando/ Löbe, Matthias/Deserno, Thomas M. (Hrsg.): ICT for Health Science Research. Amsterdam, Netherlands: IOS Press, Incorporated: 85–89.

Phys.org (2006): Building interoperability into medical information. URL: https://phys.org/news/2006-01-interoperability-medical.html, Abruf am 28.12.2020.

Pinjala, Sandeep/Sivalingam, Krishna (2019): DCACI: A Decentralized Lightweight Capability Based Access Control Framework using IOTA for Internet of Things. In: IEEE (Hrsg.): 2019 IEEE 5th World Forum on Internet of Things (WF-IoT 2019). Piscataway (NJ, USA): IEEE: 13–18.

Pirtle, Claude/Ehrenfeld, Jesse (2018): Blockchain for Healthcare: The Next Generation of Medical Records? In: Journal of medical systems, 42(9): 172.

Ploom, Tarmo (2016): Blockchains - wichtige Fragen aus IT-Sicht. In: Burgwinkel, Daniel (Hrsg.): Blockchain Technology. Berlin, Boston (MA): De Gruyter Oldenbourg: 123–148.

Pohlmann, Norbert (2018): Eine vertrauenswürdige Zusammenarbeit mit Hilfe der Blockchain-Technologie. In: Bartsch, Michael/Frey, Stefanie (Hrsg.): Cybersecurity Best Practices. Wiesbaden: Springer Fachmedien Wiesbaden: 553–569.

Pohlmann, Norbert (2019): Cyber-Sicherheit. Wiesbaden: Springer Fachmedien Wiesbaden.

Polemi, Despina (1998): Trusted third party services for health care in Europe. In: Future Generation Computer Systems, 14(1-2): 51–59.

Polge, Julien/Robert, Jérémy/Le Traon, Yves (2021): Permissioned blockchain frameworks in the industry: A comparison. In: ICT Express, 7(2): 229–233.

Polley, John/Politis, Ilias/Xenakis, Christos/Master, Adarbad/Kępkowski, Michał (2021): On an innovative architecture for digital immunity passports and vaccination certificates. o. O.

Porter, Michael/Teisberg, Elizabeth (2006): Redefining health care. Boston (MA): Harvard Business School Press.

Portmann, Edy/Risch, Daniel (2017): Was ist „Wirtschaftsinformatik in Action“? Eine Wegleitung zu den folgenden Kapiteln. In: Portmann, Edy (Hrsg.): Wirtschaftsinformatik in Theorie und Praxis. Wiesbaden: Springer Vieweg: 1–8.

Prasser, Fabian/Kohlbacher, Oliver/Mansmann, Ulrich/Bauer, Bernhard/Kuhn, Klaus (2018): Data Integration for Future Medicine (DIFUTURE). In: Methods of information in medicine, 57(S 01): e57-e65.

Procter, Paul (2002): Cambridge international dictionary of English, Repr. Cambridge: Cambridge Univ. Press.

Prokosch, Hans-Ulrich/Acker, Till/Bernarding, Johannes/Binder, Harald/Boeker, Martin/Boerries, Melanie/Daumke, Philipp/Ganslandt, Thomas/Hesser, Jürgen/Höning, Gunther/Neumaier, Michael/Marquardt, Kurt/Renz, Harald/Rothkötter, Hermann-Josef/Schade-Brittinger, Carmen/Schmücker, Paul/Schüttler, Jürgen/Sedlmayr, Martin/Serve, Hubert/Sohrabi, Keywan/Storf, Holger (2018): MIRACUM: Medical Informatics in Research and Care in University Medicine. In: Methods of information in medicine, 57(S 01): e82-e91.

Pukas, A./Smal, V./Zabchuk, V. (2018): Software based on blockchain technology for consolidation the medical data about the patients examination. In: ACIT (Hrsg.): 8th International Conference Advanced Computer Information Technologies, ACIT 2018. o. O.: 170–174.

Pussewalage, Harsha/Oleshchuk, Vladimir (2018): Blockchain Based Delegatable Access Control Scheme for a Collaborative E-Health Environment. In: IEEE (Hrsg.): 2018 IEEE International Conference on Internet of Things (iThings 2018) and IEEE Green Computing and Communications (GreenCom 2018) and IEEE Cyber, Physical and Social Computing (CPSCom 2018) and IEEE Smart Data (SmartData 2018). Piscataway (NJ, USA): IEEE: 1204–1211.

Qiu, Jinglin/Liang, Xueping/Shetty, Sachin/Bowden, Daniel (2018): Towards Secure and Smart Healthcare in Smart Cities Using Blockchain. In: IEEE (Hrsg.): 2018 IEEE International Smart Cities Conference (ISC2). Piscataway (NJ, USA): IEEE: 681–684.

Quaini, T./Roehrs, Alex/da Costa, Cristiano/da Rosa Righi, Rodrigo (2018): UNiReC: An architecture proposal for integrating distributed electronic health records using blockchain. In: IEEE (Hrsg.): WWW/Internet 2018 and Applied Computing 2018. Piscataway (NJ, USA): IEEE: 167–174.

Quasim, Mohammad/Radwan, Alaa/Alshmrani, Goram/Meraj, Mohammad (2020): A Blockchain Framework for Secure Electronic Health Records in Healthcare Industry. In: IEEE

(Hrsg.): 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE 2020). Piscataway (NJ, USA): IEEE: 605–609.

Quorum (2018): Quorum Whitepaper. URL: https://github.com/ConsenSys/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.2.pdf, Abruf am 21.10.2020.

Radanović, Igor/Likić, Robert (2018): Opportunities for Use of Blockchain Technology in Medicine. In: Applied health economics and health policy, 16(5): 583–590.

Rahmadika, Sandi/Rhee, Kyung-Hyune (2018): Blockchain technology for providing an architecture model of decentralized personal health information. In: International Journal of Engineering Business Management, 10(3): 1.

Rajput, Ahmed/Li, Qianmu/Ahvanooey, Milad (2021): A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition. In: Healthcare (Basel, Switzerland), 9(2): 206.

Ramani, Vidhya/Kumar, Tanesh/Bracken, An/Liyanage, Madhusanka/Ylianttila, Mika (2018): Secure and Efficient Data Accessibility in Blockchain Based Healthcare Systems. In: IEEE (Hrsg.): 2018 IEEE Global Communications Conference (GLOBECOM). Piscataway (NJ, USA): IEEE: 3718–3723.

Ramsaroop, P./Ball, M. (2000): The 'bank of health': A model for more useful patient health records. In: M.D. Computing, 17(4): 45–48.

Randall, David/Goel, Pradeep/Abujamra, Ramzi (2017): Blockchain Applications and Use Cases in Health Information Technology. In: Journal of Health & Medical Informatics, 08(03): 1000276.

Randolph, Haley/Barreiro, Luis (2020): Herd Immunity: Understanding COVID-19. In: Immunity, 52(5): 737–741.

Rao, Umesh/Nayak, Umesha (2014): The InfoSec handbook. New York (NY, USA): Apress.

Rasmussen, Luke (2014): The electronic health record for translational research. In: Journal of cardiovascular translational research, 7(6): 607–614.

Read the Docs (2019): Solidity. URL: https://solidity.readthedocs.io/en/latest/, Abruf am 05.01.2020.

Reichertz, Peter (1975): Hospital and Health Care Systems. In: IFAC Proceedings Volumes, 8(1): 705–727.

Reidt, Andreas (2019): Referenzarchitektur eines integrierten Informationssystems zur Unterstützung der Instandhaltung, Dissertation. München.

Reidt, Andreas/Pfaff, Matthias/Krcmar, Helmut (2018): Der Referenzarchitekturbegriff im Wandel der Zeit. In: HMD Praxis der Wirtschaftsinformatik, 55(5): 893–906.

Reuse, Svend/Frère, Eric/Schaab, Ilja (2019): Auswirkungen der Blockchain-Technologie auf das Geschäftsmodell und die Strategie einer Bank. In: Seidel, Marcel (Hrsg.): Banking & Innovation 2018/2019. Wiesbaden: Springer Fachmedien Wiesbaden: 43–68.

Ribitzky, Ron/St. Clair, James/Houlding, David/McFarlane, Chrissa/Ahier, Brian/Gould, Michael/Flannery, Heather/Pupo, Erik/Clauson, Kevin (2018): Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare. In: Blockchain in Healthcare Today.

Richter, Peggy/Schlieter, Hannes (2019): Understanding Patient Pathways in the Context of Integrated Health Care Services. In: Association for Information Systems (AIS) eLibrary (Hrsg.): WI 2019, Proceedings of the 14th International Conference on business informatics. o. O.: Association for Information Systems: 987–1001.

Riege, Christian/Saat, Jan/Bucher, Tobias (2009): Systematisierung von Evaluationsmethoden in der gestaltungsorientierten Wirtschaftsinformatik. In: Becker, Jörg/Krcmar, Helmut/Niehaves, Björn (Hrsg.): Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik. Heidelberg, New York: Physica-Verlag: 69–86.

Rifi, Nabil/Rachkidi, Elie/Agoulmine, Nazim/Taher, Nada (2017): Towards using blockchain technology for eHealth data access management. In: IEEE (Hrsg.): 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME). Piscataway (NJ, USA): IEEE: 198–201.

Rodrigues, Bruno/Bocek, Thomas/Stiller, Burkhard (2018): The Use of Blockchains: Application-Driven Analysis of Applicability. In: Raj, Pethuru/Deka, Ganesh (Hrsg.): Blockchain technology, First edition. Cambridge, MA, San Diego, CA, Oxford, London: Academic Press an imprint of Elsevier: 163–198.

Roehrs, Alex/da Costa, Cristiano/da Rosa Righi, Rodrigo (2017): OmniPHR: A distributed architecture model to integrate personal health records. In: Journal of biomedical informatics, 71: 70–81.

Roehrs, Alex/da Costa, Cristiano/da Rosa Righi, Rodrigo/da Silva, Valter/Goldim, José/Schmidt, Douglas (2019): Analyzing the performance of a blockchain-based personal health record implementation. In: Journal of biomedical informatics, 92: 103140.

Rose, Frank (1999): The Economics, Concept, and Design of Information Intermediaries. Heidelberg: Physica-Verlag HD.

Rouhani, Sara/Butterworth, Luke/Simmons, Adam/Humphery, Darryl/Deters, Ralph (2018): MediChain: A Secure Decentralized Medical Data Asset Management System. In: IEEE (Hrsg.): 2018 IEEE International Conference on Internet of Things (iThings 2018) and

IEEE Green Computing and Communications (GreenCom 2018) and IEEE Cyber, Physical and Social Computing (CPSCom 2018) and IEEE Smart Data (SmartData 2018). Piscataway (NJ, USA): IEEE: 1533–1538.

Ruggeri, Armando/Fazio, Maria/Celesti, Antonio/Villari, Massimo (2020): Blockchain-Based Healthcare Workflows in Federated Hospital Clouds. In: Brogi, Antonio/Zimmermann, Wolf/Kritikos, Kyriakos (Hrsg.): Service-Oriented and Cloud Computing. Cham, Switzerland: Springer International Publishing: 113–121.

Salomaa, Arto (1996): Public-key cryptography, 2, enl. ed. Berlin: Springer.

Sargsyan, Tatevik (2016): The privacy role of information intermediaries through self-regulation. In: Internet Policy Review, 5(4): 1–17.

Schaar, Peter (2005): 20. Tätigkeitsbericht zum Datenschutz 2003 - 2004. Bonn.

Scheer, August-Wilhelm (1997): Wirtschaftsinformatik, 7. durchges. Aufl. Berlin: Springer.

Schneider, Uwe (2016): Einrichtungsübergreifende elektronische Patientenakten. Wiesbaden: Springer Vieweg.

Schollmeier, Rüdiger (2001): A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In: IEEE (Hrsg.): Proceedings First International Conference on Peer-to-Peer Computing. Piscataway (NJ, USA): IEEE Comput. Soc: 101–102.

Schrahe, Dominik/Städter, Thomas (2021): COVID-19-Impf- und -Testnachweise. In: Datenschutz und Datensicherheit - DuD, 45(5): 315–319.

Schuemie, M./Talmon, J./Moorman, P./Kors, J. (2009): Mapping the Domain of Medical Informatics. In: Methods of Information in Medicine, 48(01): 76–83.

Schütte, Reinhard (1998): Grundsätze ordnungsmäßiger Referenzmodellierung. Wiesbaden: Gabler Verlag.

Schwab, Wolfgang (2014): eGK: Einsatz einer Trust-service Status List in der Telematikinfrastruktur. In: Datenschutz und Datensicherheit - DuD, 38(4): 262–266.

Schwarzer, Bettina/Krcmar, Helmut (2014): Wirtschaftsinformatik, 5, überarb. Aufl. Stuttgart: Schäffer-Poeschel.

Sein/Henfridsson/Purao/Rossi/Lindgren (2011): Action Design Research. In: MIS Quarterly, 35(1): 37–56.

Shabo, Amnon (2006a): A global socio-economic-medico-legal model for the sustainability of longitudinal electronic health records - Part 1. In: Methods of information in medicine, 45(3): 240–245.

Shabo, Amnon (2006b): A global socio-economic-medico-legal model for the sustainability of longitudinal electronic health records - Part 2. In: Methods of information in medicine, 45(5): 498–505.

Shabo, Amnon (2010): Independent health record banks for older people--the ultimate integration of dispersed and disparate medical records. In: Informatics for health & social care, 35(3-4): 188–199.

Shabo, Amnon (2014): It's time for health record banking! In: Methods of information in medicine, 53(2): 63–65.

Shae, Zonyin/Tsai, Jeffrey (2017): On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine. In: IEEE (Hrsg.): 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS 2017). Piscataway (NJ, USA): IEEE: 1972–1980.

Shah, Meet/Shaikh, Mohammedhasan/Mishra, Vishwajeet/Tuscano, Grinal (2020): Decentralized Cloud Storage Using Blockchain. In: IEEE (Hrsg.): 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI 2020). Piscataway (NJ, USA): IEEE: 384–389.

Shahnaz, Ayesha/Qamar, Usman/Khalid, Ayesha (2019): Using Blockchain for Electronic Health Records. In: IEEE Access, 7: 147782–147795.

Shanmugapriya, P./M. Suresh, R. (2012): Software Architecture Evaluation Methods A Survey. In: International Journal of Control and Automation, 49(16): 19–26.

Sharma, Brihat/Sekharan, Chandra/Zuo, Fanyu (2018): Merkle-Tree Based Approach for Ensuring Integrity of Electronic Medical Records. In: IEEE (Hrsg.): 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). Piscataway (NJ, USA): IEEE: 983–987.

Sharma, Yogesh/Balamurugan, B. (2020): Preserving the Privacy of Electronic Health Records using Blockchain. In: Procedia Computer Science, 173: 171–180.

Shorthouse, David/Xie, Michael (2020): Blockchain Designed for Supply Chains: Guardtime Supply Chain Framework. o. O.

Sikander, Shaik/Sridevi, R. (2020): A Framework for Dynamic Access Control System for Cloud Federations Using Blockchain. In: Raju, K./Govardhan, A./Rani, B./ Sridevi, R./Murty, M. Ramakrishna (Hrsg.): Proceedings of the Third International Conference on Computational Intelligence and Informatics (ICCII 2018). Singapore: Springer Singapore: 591–600.

Simić, Miloš/Sladić, Goran/Milosavljević, Branko (2017): A Case Study IoT and Blockchain powered Healthcare. In: V, Katić (Hrsg.): The 8th PSU-UNS International Conference on Engineering and Technology (ICET-2017). o. O.: 1–4.

Simoneit, Monika (1998): Informationsmanagement in Universitätsklinika. Wiesbaden: Dt. Univ.-Verl. [u.a.].

Sinz, Elmar (2010): Konstruktionsforschung in der Wirtschaftsinformatik: Was sind die Erkenntnisziele gestaltungsorientierter Wirtschaftsinformatik-Forschung? In: Österle, Hubert/Winter, Robert/Brenner, Walter (Hrsg.): Gestaltungsorientierte Wirtschaftsinformatik. Nürnberg: Infowerk: 27–33.

Sixt, Elfriede (2017): Bitcoins und andere dezentrale Transaktionssysteme. Wiesbaden: Springer Fachmedien Wiesbaden.

Soenens, Els (2009): Identity Management Systems in Healthcare: The Issue of Patient Identifiers. In: Matyáš, Vashek/Fischer-Hübner, Simone/Cvrček, Daniel/Švenda, Petr (Hrsg.): The Future of Identity in the Information Society. Berlin, Heidelberg: Springer Berlin Heidelberg: 56–66.

Sørensen, Carsten (2002): This Is Not an Article - Just Some Thoughts on How to Write One. Großbritannien.

Spitz, Stephan/Pramateftakis, Michael/Swoboda, Joachim (2011): Kryptographie und IT-Sicherheit. Wiesbaden: Vieweg+Teubner.

Staffa, Mariacarla/Coppolino, Luigi/Sgaglione, Luigi/Gelenbe, Erol/Komnios, Ioannis/Grivas, Evangelos/Stan, Oana/Castaldo, Luigi (2018): KONFIDO: An OpenNCP-Based Secure eHealth Data Exchange System. In: Gelenbe, Erol/Campegiani, Paolo/Czachórski, Tadeusz/ Katsikas, Sokratis K./ Komnios, Ioannis/ Romano, Luigi/Tzovaras, Dimitrios (Hrsg.): Security in Computer and Information Sciences. Cham, Switzerland: Springer International Publishing: 11–27.

Stanzel, Matthias (2007): Qualität des Aktienresearchs von Finanzanalysten. Wiesbaden: DUV.

Statistisches Bundesamt (2018a): Entwicklung der Gesundheitsausgaben in Deutschland je Einwohner im Zeitraum von 1996 bis 2016 (in Euro). URL: https://de.statista.com/statistik/daten/studie/6588/umfrage/gesundheitsausgaben-in-deutschland-je-einwohner-seit-1996/, Abruf am 03.07.2018.

Statistisches Bundesamt (2018b): Gesundheit - Grunddaten der Krankenhäuser. Berlin.

Statistisches Bundesamt (2018c): Jährliche Gesundheitsausgaben in Deutschland in den Jahren von 1992 bis 2016 (in Millionen Euro). URL: https://de.statista.com/statistik/daten/

studie/5463/umfrage/gesundheitssystem-in-deutschland---ausgaben-seit-1992/, Abruf am 03.07.2018.

Statistisches Bundesamt (2019a): Bevölkerung: Deutschland, Stichtag 31.12.2019. Berlin.

Statistisches Bundesamt (2019b): Statistik der gesetzlichen Krankenversicherung. Berlin.

Stol, Klaas-Jan/Ali Babar, Muhammad (2010): Challenges in using open source software in product development. In: Erenkrantz, Justin/Wright, Hyrum (Hrsg.): Proceedings of the 3rd International Workshop on Emerging Trends in Free/Libre/Open Source Software Research and Development (FLOSS '10). New York (NY, USA): ACM Press: 17–22.

Sun, Jin/Yao, Xiaomin/Wang, Shangping/Wu, Ying (2020): Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS. In: IEEE Access, 8: 59389–59401.

Sun, You/Zhang, Rui/Wang, Xin/Gao, Kaiqiang/Liu, Ling (2018): A Decentralizing Attribute-Based Signature for Healthcare Blockchain. In: IEEE (Hrsg.): 2018 27th International Conference on Computer Communication and Networks (ICCCN). Piscataway (NJ, USA): IEEE: 278–287.

Sunyaev, Ali/Kaletsch, Alexander/Dünnebeil, Sebastian/Krcmar, Helmut (2010): Attack Scenarios for possible misuse of peripheral parts in the German Health Information Infrastructure. In: Filipe, Joaquim (Hrsg.): Proceedings of the 12th International Conference on Enterprise Information Systems. Setúbal: SciTePress: 229–235.

Sunyaev, Ali/Kaletsch, Alexander/Mauro, Christian/Krcmar, Helmut (2009): Security Analysis of the German electronic Health Card's peripheral parts. In: Cordeiro, José (Hrsg.): Proceedings of the 11th International Conference on Enterprise Information Systems. Setúbal: INSTICC: 19–26.

Sunyaev, Ali/Leimeister, Jan/Krcmar, Helmut (2010): Open Security Issues in German Healthcare Telematics. In: INSTICC Press (Hrsg.): HEALTHINF 2010 - Proceedings of the Third International Conference on Health Informatics. Setúbal: INSTICC Press: 187–194.

Suter-Crazzolara, Clemens (2018): Better Patient Outcomes Through Mining of Biomedical Big Data. Walldorf (Germany).

Sutherland, Scott/Kaelber, David/Downing, N./Goel, Veena/Longhurst, Christopher (2016): Electronic Health Record-Enabled Research in Children Using the Electronic Health Record for Clinical Discovery. In: Pediatric clinics of North America, 63(2): 251–268.

Swan, Melanie (2015): Blockchain. Beijing: O'Reilly.

Swan, Melanie (2018): Blockchain for Business: Next-Generation Enterprise Artificial Intelligence Systems. In: Raj, Pethuru/Deka, Ganesh (Hrsg.): Blockchain technology, First

edition. Cambridge, MA, San Diego, CA, Oxford, London: Academic Press an imprint of Elsevier: 121–162.

Szabo, Nick (1994): Smart Contracts. URL: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, Abruf am 27.12.2019.

Talia, Domenico (2013): Clouds for Scalable Big Data Analytics. In: Computer, 46(5): 98–101.

Tarouco, Liane/Bertholdo, Leandro/Granville, Lisandro/Arbiza, Lucas/Carbone, Felipe/Marotta, Marcelo/Santanna, Jose de (2012): Internet of Things in healthcare: Interoperatibility and security issues. In: IEEE (Hrsg.): 2012 IEEE International Conference on Communications (ICC 2012). Piscataway (NJ, USA): IEEE: 6121–6125.

Teeter, Cale (o. J.): Quorum Consortium Network in Azure Marketplace. o. O.

Theodouli, Anastasia/Arakliotis, Stelios/Moschou, Konstantinos/Votis, Konstantinos/Tzovaras, Dimitrios (2018): On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing. In: IEEE (Hrsg.): 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE 2018). Piscataway (NJ, USA): IEEE: 1374–1379.

Thiemer, Andreas (2005): Markt. In: Schubert, Klaus (Hrsg.): Handwörterbuch des ökonomischen Systems der Bundesrepublik Deutschland. Wiesbaden: VS Verlag für Sozialwissenschaften: 285–293.

Thwin, Thein/Vasupongayya, Sangsuree (2018): Blockchain Based Secret-Data Sharing Model for Personal Health Record System. In: IEEE (Hrsg.): 2018 5th International Conference on Advanced Informatics: Concept Theory and Applications (ICAICTA 2018). Piscataway (NJ, USA): IEEE: 196–201.

Tsoi, Kelvin/Sung, Joseph/Lee, Helen/Yiu, Karen/Fung, Hong/Wong, Samuel (2021): The way forward after COVID-19 vaccination: vaccine passports with blockchain to protect personal privacy. In: BMJ Innovations, 7(2): 337–341.

Tsolkas, Alexander/Schmidt, Klaus (2017): Rollen und Berechtigungskonzepte. Wiesbaden: Springer Fachmedien Wiesbaden.

U.S. Department of Health and Human Services Office for Civil Rights (2013): HIPAA Administrative Simplification Regulation Text. URL: https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf, Abruf am 05.02.2020.

Uddin, Mueen/S. Memon, M./Memon, Irfana/Ali, Imtiaz/Memon, Jamshed/Abdelhaq, Maha/Alsaqour, Raed (2021): Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. In: Computers, Materials & Continua, 68(2): 2377–2397.

Vaishnavi, Vijay/Kuechler, William (2008): Design science research methods and patterns. Boca Raton: Auerbach Publications.

van der Linden, Helma/Kalra, Dipak/Hasman, Arie/Talmon, Jan (2009): Inter-organizational future proof EHR systems. A review of the security and privacy related issues. In: International journal of medical informatics, 78(3): 141–160.

Vasconcelos, André/Sousa, P./Tribolet, J. (2005): Information System Architecture Evaluation: From Software to Enterprise Level Approaches. Lisbon/Portugal.

Verband der Hochschullehrer für Betriebswirtschaft e.V. (2015a): VHB-JOURQUAL3 Teilrating Managements im Gesundheitswesen. URL: https://vhbonline.org/vhb4you/jourqual/vhb-jourqual-3/teilrating-gesundheitswesen/, Abruf am 11.09.2018.

Verband der Hochschullehrer für Betriebswirtschaft e.V. (2015b): VHB-JOURQUAL3 Teilrating Wirtschaftsinformatik. URL: https://vhbonline.org/vhb4you/jourqual/vhb-jourqual-3/teilrating-wi/, Abruf am 11.09.2018.

Viswanathan, Ram/Dasgupta, Diptiman/Govindaswamy, Srinivasa (2019): Blockchain Solution Reference Architecture (BSRA). In: IBM Journal of Research and Development, 63(2/3): 1.1–1.12.

Vogel, Oliver/Arnold, Ingo/Chughtai, Arif/Ihler, Edmund/Kehrer, Timo/Mehlig, Uwe/Zdun, Uwe (2009): Software-Architektur, 2. Auflage. Heidelberg: Spektrum Akademischer Verlag.

Vora, Jayneel/Nayyar, Anand/Tanwar, Sudeep/Tyagi, Sudhanshu/Kumar, Neeraj/Obaidat, M./Rodrigues, Joel (2018): BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. In: IEEE (Hrsg.): 2018 IEEE Globecom Workshops (GC Wkshps 2018). Piscataway (NJ, USA): IEEE: 976–981.

Wagner, Abram (2019): The use and significance of vaccination cards. In: Human vaccines & immunotherapeutics, 15(12): 2844–2846.

Walter, Benedikt von (2007): Intermediation und Digitalisierung. Wiesbaden: DUV.

Wang, Hao/Song, Yujiao (2018): Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. In: Journal of medical systems, 42(8): 152.

Wang, Jitao/Sun, Guozi/Gu, Yu/Liu, Kun (2020): Distributed Electronic Data Storage and Proof System Based on Blockchain. In: Si, Xueming/Jin, Hai/Sun, Yi/ Zhu, Jianming/ Zhu, Liehuang/ Song, Xianhua/Lu, Zeguang (Hrsg.): Second CCF China Blockchain

Conference Blockchain Technology and Application (CBCC 201). Singapore: Springer Singapore: 48–67.

Wang, Rong/Tsai, Wei-Tek/He, Juan/Liu, Can/Li, Qi/Deng, Enyan (2018a): A Medical Data Sharing Platform Based On Permissioned Blockchains. In: Association for Computing Machinery (Hrsg.): ICBTA 2018: Proceedings of the 2018 International Conference on Blockchain Technology and Application. New York (NY, USA): ACM Press: 12–16.

Wang, Shangping/Zhang, Dan/Zhang, Yaling (2019): Blockchain-Based Personal Health Records Sharing Scheme With Data Integrity Verifiable. In: IEEE Access, 7: 102887–102901.

Wang, Shuai/Wang, Jing/Wang, Xiao/Qiu, Tianyu/Yuan, Yong/Ouyang, Liwei/Guo, Yuanyuan/Wang, Fei-Yue (2018b): Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. In: IEEE Transactions on Computational Social Systems, 5(4): 942–950.

Wang, Ziyu/Luo, Nanqing/Zhou, Pan (2020): GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare. In: Journal of Parallel and Distributed Computing, 142: 1–12.

Wanitcharakkhakul, Lakkana/Rotchanakitumnuai, Siriluck (2017): Blockchain Technology Acceptance in Electronic Medical Record System. In: Association for Information Systems (AIS) eLibrary (Hrsg.): ICEB 2017 Proceedings. o. O.: Association for Information Systems (AIS) eLibrary: 53–58.

Webster, Jane/Watson, Richard (2002): Analyzing the past to prepare for the future: Writing a literature review. In: MIS Quarterly, 26(2): 13–23.

Wilde, Thomas/Hess, Thomas (2006): Methodenspektrum der Wirtschaftsinformatik: Überblick und Portfoliobildung. o. O.

Wilde, Thomas/Hess, Thomas (2007): Forschungsmethoden der Wirtschaftsinformatik. In: Wirtschaftsinformatik, 49(4): 280–287.

Williamson, Oliver (2010): The economic institutions of capitalism, [Nachdr.]. New York (NY, USA): Free Press.

Wilson, Kumanan/Flood, Colleen (2021): Implementing digital passports for SARS-CoV-2 immunization in Canada. In: CMAJ : Canadian Medical Association journal = journal de l'Association medicale canadienne, 193(14): E486-E488.

Winter, Alfred/Stäubert, Sebastian/Ammon, Danny/Aiche, Stephan/Beyan, Oya/Bischoff, Verena/Daumke, Philipp/Decker, Stefan/Funkat, Gert/Gewehr, Jan/Greiff, Armin de/Haferkamp, Silke/Hahn, Udo/Henkel, Andreas/Kirsten, Toralf/Klöss, Thomas/Lippert, Jörg/Löbe, Matthias/Lowitsch, Volker/Maassen, Oliver/Maschmann, Jens/Meister,

Sven/Mikolajczyk, Rafael/Nüchter, Matthias/Pletz, Mathias/Rahm, Erhard/Riedel, Morris/Saleh, Kutaiba/Schuppert, Andreas/Smers, Stefan/Stollenwerk, André/Uhlig, Stefan/Wendt, Thomas/Zenker, Sven/Fleig, Wolfgang/Marx, Gernot/Scherag, André/Löffler, Markus (2018): Smart Medical Information Technology for Healthcare (SMITH). In: Methods of information in medicine, 57(S 01): e92-e105.

Winter, Robert/Fischer, Ronny (2006): Essential Layers, Artifacts, and Dependencies of Enterprise Architecture. In: IEEE (Hrsg.): 10th IEEE International Enterprise Distributed Object Computing Conference (EDOCW 2006). Piscataway (NJ, USA): IEEE: 30.

WKWI/GI FB WI (2011): Profil der Wirtschaftsinformatik. o. O.

Wobst, Reinhard (1998): Abenteuer Kryptologie, 2, überarb. Aufl. Bonn: Addison-Wesley Longman.

Wong, Daniel/Bhattacharya, Sanchita/Butte, Atul (2019): Prototype of running clinical trials in an untrustworthy environment using blockchain. In: Nature communications, 10(1): 917.

Wu, Hanqing/Cao, Jiannong/Jiang, Shan/Yang, Ruosong/Yang, Yanni/Hey, Jianfei (2018): TSAR: A Fully-Distributed Trustless Data ShARing Platform. In: IEEE (Hrsg.): 2018 IEEE International Conference on Smart Computing (SMARTCOMP 2018). Piscataway (NJ, USA): IEEE: 350–355.

Wu, Hsin-Te/Tsai, Chun-Wei (2018): Toward Blockchains for Health-Care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy in Data Sharing. In: IEEE Consumer Electronics Magazine, 7(4): 65–71.

Wu, Xuguang/Han, Yiliang/Zhang, Minqing/Zhu, Shuaishuai (2020): Secure Personal Health Records Sharing Based on Blockchain and IPFS. In: Han, Weili/Zhu, Liehuang/Yan, Fei (Hrsg.): Trusted Computing and Information Security. Singapore: Springer Singapore: 340–354.

Wüst, Karl/Gervais, Arthur (2018): Do you Need a Blockchain? In: IEEE (Hrsg.): 2018 Crypto Valley Conference on Blockchain Technology (CVCBT 2018). Piscataway (NJ, USA): IEEE: 45–54.

Wyatt, J./Liu, J. (2002): Basic concepts in medical informatics. In: Journal of Epidemiology & Community Health, 56(11): 808–812.

Xia, Qi/Sifah, Emmanuel/Asamoah, Kwame/Gao, Jianbin/Du, Xiaojiang/Guizani, Mohsen (2017a): MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. In: IEEE Access, 5: 14757–14767.

Xia, Qi/Sifah, Emmanuel/Smahi, Abla/Amofa, Sandro/Zhang, Xiaosong (2017b): BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. In: Information, 8(2): 44.

Xiao, Qinghan (2005): Security issues in biometric authentication. In: IEEE (Hrsg.): 6th Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop. Piscataway (NJ, USA): IEEE: 8–13.

Xiao, Zhe/Li, Zengxiang/Liu, Yong/Feng, Ling/Zhang, Weiwen/Lertwuthikarn, Thanarit/Mong Goh, Rick (2018): EMRShare: A Cross-Organizational Medical Data Sharing and Management Framework Using Permissioned Blockchain. In: IEEE (Hrsg.): 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS 2018). Piscataway (NJ, USA): IEEE: 998–1003.

Yang, Caixia/Tan, Liang/Shi, Na/Xu, Bolei/Cao, Yang/Yu, Keping (2020a): AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud. In: IEEE Access, 8: 70604–70615.

Yang, Guang/Li, Chunlei (2018): A Design of Blockchain-Based Architecture for the Security of Electronic Health Record (EHR) Systems. In: IEEE (Hrsg.): 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). Piscataway (NJ, USA): IEEE: 261–265.

Yang, Huihui/Yang, Bian (2017): A Blockchain-based Approach to the Secure Sharing of Healthcare Data. In: Erdödi, Lazlo/Jøsang, Audun (Hrsg.): Norwegian Information Security Conference 2017 (NISK 2017). o. O.: 100–111.

Yang, Xiaodong/Li, Ting/Pei, Xizhen/Wen, Long/Wang, Caifen (2020b): Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology. In: IEEE Access, 8: 45468–45476.

Yli-Huumo, Jesse/Ko, Deokyoon/Choi, Sujin/Park, Sooyong/Smolander, Kari (2016): Where Is Current Research on Blockchain Technology?-A Systematic Review. In: PloS one, 11(10): e0163477.

Yu, Hongru/Sun, Haiyang/Wu, Danyi/Kuo, Tsung-Ting (2019): Comparison of Smart Contract Blockchains for Healthcare Applications. In: AMIA … Annual Symposium proceedings. AMIA Symposium, 2019: 1266–1275.

Yue, Xiao/Wang, Huiju/Jin, Dawei/Li, Mingqiang/Jiang, Wei (2016): Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. In: Journal of medical systems, 40(10): 218.

Zhang, Aiqing/Lin, Xiaodong (2018): Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. In: Journal of medical systems, 42(8): 140.

Zhang, Guozhen/Li, Tong/Li, Yong/Hui, Pan/Jin, Depeng (2018a): Blockchain-Based Data Sharing System for AI-Powered Network Operations. In: Journal of Communications and Information Networks, 3(3): 1–8.

Zhang, Ke-Jun/Jin, Wei (2004): Putting role-based discretionary access control into practice. In: IEEE (Hrsg.): Proceedings of 2004 International Conference on Machine Learning and Cybernetics Vol. 5. Piscataway (NJ, USA): IEEE: 2691–2696.

Zhang, Peng/Walker, Michael/White, Jules/Schmidt, Douglas/Lenz, Gunther (2017): Metrics for assessing blockchain-based healthcare decentralized apps. In: IEEE (Hrsg.): 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom). Piscataway (NJ, USA): IEEE: 121–124.

Zhang, Peng/White, Jules/Schmidt, Douglas/Lenz, Gunther/Rosenbloom, S. (2018b): FHIR-Chain: Applying Blockchain to Securely and Scalably Share Clinical Data. In: Computational and structural biotechnology journal, 16: 267–278.

Zhang, Rui/Liu, Ling (2010): Security Models and Requirements for Healthcare Application Clouds. In: IEEE (Hrsg.): 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD 2010). Piscataway (NJ, USA): IEEE: 268–275.

Zhang, Shijie/Lee, Jong-Hyouk (2020): Analysis of the main consensus protocols of blockchain. In: ICT Express, 6(2): 93–97.

Zhang, Xiaoshuai/Poslad, Stefan/Ma, Zixiang (2018): Block-Based Access Control for Blockchain-Based Electronic Medical Records (EMRs) Query in eHealth. In: IEEE (Hrsg.): 2018 IEEE Global Communications Conference (GLOBECOM). Piscataway (NJ, USA): IEEE: 3724–3729.

Zheng, Xiaochen/Mukkamala, Raghava/Vatrapu, Ravi/Ordieres-Mere, Joaqun (2018): Blockchain-based Personal Health Data Sharing System Using Cloud Storage. In: IEEE (Hrsg.): 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). Piscataway (NJ, USA): IEEE: 161–166.

Zhou, Jiayu/Tang, Fengyi/Zhu, He/Nan, Ning/Zhou, Ziheng (2018): Distributed Data Vending on Blockchain. In: IEEE (Hrsg.): 2018 IEEE International Conference on Internet of Things (iThings 2018) and IEEE Green Computing and Communications (GreenCom 2018) and IEEE Cyber, Physical and Social Computing (CPSCom 2018) and IEEE Smart Data (SmartData 2018). Piscataway (NJ, USA): IEEE: 1100–1107.

Zhou, Lijing/Wang, Licheng/Sun, Yiru (2018): MIStore: a Blockchain-Based Medical Insurance Storage System. In: Journal of medical systems, 42(8): 149.

Zhuang, Yan/Chen, Yin-Wu/Shae, Zon-Yin/Shyu, Chi-Ren (2020a): Generalizable Layered Blockchain Architecture for Health Care Applications: Development, Case Studies, and Evaluation. In: Journal of medical Internet research, 22(7): e19029.

Zhuang, Yan/Sheets, Lincoln/Chen, Yin-Wu/Shae, Zon-Yin/Tsai, Jeffrey/Shyu, Chi-Ren (2020b): A Patient-Centric Health Information Exchange Framework Using Blockchain Technology. In: IEEE journal of biomedical and health informatics, 24(8): 2169–2176.

Zhuang, Yan/Sheets, Lincoln/Shae, Zonyin/Chen, Yin-Wu/Tsai, Jeffrey/Shyu, Chi-Ren (2019): Applying Blockchain Technology to Enhance Clinical Trial Recruitment. In: AMIA … Annual Symposium proceedings. AMIA Symposium, 2019: 1276–1285.

Zhuang, Yu/Sheets, Lincoln/Shae, Zonyin/Tsai, Jeffrey/Shyu, Chi-Ren (2018): Applying Blockchain Technology for Health Information Exchange and Persistent Monitoring for Clinical Trials. In: AMIA Annual Symposium Proceedings, 2018: 1167–1175.

Zobel, Justin (2005): Writing for computer science, 2. ed. London: Springer.

ZTG (2011): Elektronische Akten im Gesundheitswesen. Bochum.

Zyskind, Guy/Nathan, Oz/Pentland, Alex (2015): Decentralizing Privacy: Using Blockchain to Protect Personal Data. In: IEEE (Hrsg.): 2015 IEEE Security and Privacy Workshops (SPW 2015). Piscataway (NJ, USA): IEEE: 180–184.

Anhang A: Gesundheitsausgaben in Deutschland

Tabelle A-1: Jährliche Gesamtausgaben in Deutschland von 1992 bis 2016 (Quelle: Statistisches Bundesamt (2018c))

Jahr	Ausgaben in Millionen Euro
1992	159.381
1993	163.751
1994	175.455
1995	187.525
1996	195.764
1997	196.627
1998	201.655
1999	207.689
2000	214.098
2001	221.559
2002	229.966
2003	235.603
2004	234.813
2005	241.326
2006	247.783
2007	256.173
2008	266.206
2009	280.753
2010	290.424
2011	295.857
2012	303.309
2013	314.639
2014	327.577
2015	343.513
2016	356.537

Tabelle A-2: Gesundheitsausgaben pro Einwohner in Deutschland von 1996 bis 2016 (Quelle: Statistisches Bundesamt (2018a))

Jahr	Ausgaben pro Einwohner in Euro
1996	2.390
1997	2.390
1998	2.460
1999	2.530
2000	2.628
2001	2.680
2002	2.770
2003	2.840
2004	2.840
2005	2.967
2006	2.990
2007	3.090
2008	3.220
2009	3.410
2010	3.617
2011	3.686
2012	3.771
2013	3.902
2014	4.045
2015	4.205
2016	4.330

Anhang B: Ranking-Listen der untersuchten Journale

Tabelle B-1: Ranking-Liste der untersuchten Journale für Betriebswirtschaftslehre, Teilgebiet Management im Gesundheitswesen (Quelle: Verband der Hochschullehrer für Betriebswirtschaft e.V. (2015a))

Zeitschrift	ISSN (Druckversion, sofern verfügbar)
A = Führende wissenschaftliche Zeitschrift auf dem Gebiet der BWL oder ihrer Teildisziplinen	
Health Economics	1057-9230
Journal of Health Economics	0167-6296
Medical Decision Making	0272-989X
PharmacoEconomics	1170-7690
Health Services Research (HSR)	0017-9124
Health Care Management Science	1386-9620
B = Wichtige und angesehene wissenschaftliche Zeitschrift auf dem Gebiet der BWL oder ihrer Teildisziplinen	
European Journal of Health Economics	1618-7598
Health Care Management Review	0361-6274
Value in Health	1098-3015
Health Policy	0168-8510
Applied Health Economics and Health Policy	1175-5652
International Journal of Technology Assessment in Health Care	0266-4623
C = Anerkannte wissenschaftliche Zeitschrift auf dem Gebiet der BWL oder ihrer Teildisziplinen	
Journal of Health Services Research & Policy	1355-8196
BMC Health Services Research	1472-6963
British Journal of Healthcare Management	1358-0574
Das Gesundheitswesen	0941-3790
Health Services Management Research	0951-4848
Journal of Healthcare Management	1096-9012

Tabelle B-2: Ranking-Liste der untersuchten Journale für Betriebswirtschaftslehre, Teilgebiet Wirtschaftsinformatik (Quelle: Verband der Hochschullehrer für Betriebswirtschaft e.V. (2015b))

Zeitschrift	ISSN (Druckversion, sofern verfügbar)
A+ = Herausragende, weltweit führende wissenschaftliche Zeitschrift auf dem Gebiet der BWL oder ihrer Teildisziplinen	
Information Systems Research (ISR)	1047-7047
Management Information Systems Quarterly (MISQ)	0276-7783
A = Führende wissenschaftliche Zeitschrift auf dem Gebiet der BWL oder ihrer Teildisziplinen	
Journal of Management Information Systems	0742-1222
Mathematical Programming	0025-5610
Journal of the Association for Information Systems (JAIS)	1536-9323
Journal of Information Technology	0268-3962
Proceedings of the International Conference on Information Systems (ICIS)	keine
Information Systems Journal (ISJ)	1350-1917
The Journal of Strategic Information Systems	0963-8687
European Journal of Information Systems (EJIS)	0960-085X
INFORMS Journal on Computing (JOC)	1091-9856
SIAM Journal on Computing	0097-5397
B = Wichtige und angesehene wissenschaftliche Zeitschrift auf dem Gebiet der BWL oder ihrer Teildisziplinen	
Journal of the ACM (JACM)	0004-5411
Decision Support Systems (DSS)	0167-9236
Decision Sciences	0011-7315
Computers and Operations Research	0305-0548
IEEE Transactions on Engineering Management	0018-9391
Business & Information Systems Engineering (BISE) (früher: Wirtschaftsinformatik WI)	0937-6429
ACM Transactions on Information Systems	1046-8188
International Journal of Electronic Commerce (IJEC)	1086-4415
ACM Transactions on Management Information Systems	2158-656X
ACM Computing Surveys	0360-0300
Journal of Computational Finance	1460-1559
Artificial Intelligence	0004-3702
Group Decision and Negotiation	0926-2644
ACM SIGMIS Database	0095-0033
Proceedings of the European Conference on Information Systems (ECIS)	keine
IEEE Transactions on Software Engineering	0098-5589
Data & Knowledge Engineering	0169-023X
Proceedings of the International Conference on Conceptual Modeling (ER)	keine
Communications of the ACM (CACM)	0001-0782
Information & Management	0378-7206

Information Systems (IS)	0306-4379
MIS Quarterly Executive	1540-1960
Journal of Decision Systems	1246-0125
Information and Organization	1471-7727
Information Systems Frontiers	1387-3326
Electronic Markets (em)	1019-6781
ACM Transactions on Computer-Human Interaction	1073-0516

Anhang C: Schlagwort Analyse der Literatur

Tabelle C-1: Alphabetisch sortierte Schlagwortliste (Quelle: Eigene Darstellung)

Schlagwort	Anzahl
Accountability	2
Activity data	1
Adoption	2
analytics	1
Android	1
Anonymized Dataset	1
application	1
Application programming interface	1
Architecture	5
Architecture_Model	1
Artificial intelligence (AI)	5
Arvados	1
Asset Tracking	1
attention	1
Attribute	4
Attribute-based cryptosystem	1
Attribute-based signature	1
Audit and Tracking	3
Authentication	2
Authorization	4
Behavioral Health	1
Big Data	5
Big Data_Analytics	2
biosensor nodes	1
Blockchain_Cloud	1
Blockchain_Consensus	2
Blockchain_Consortium	1
Blockchain_Healthcare Systems	1
Blockchain_Permissioned	8
Blockchain_Private	1
Blockchain_Public	1
Blockchain_Security	1
Blockchain_Technology_Bitcoin	2
Blockchain_Technology_Ethereum	8
Blockchain_Technology_General	3
Blockchain_Technology_Hyperledger fabric	7
Blockchain_Technology_IOTA	1
body sensor networks	1
Business	2
Cancer care	1
Capital	1
chord-based distribution	1
Circular Economy	1
Clinical data	2
Clinical data sharing	1
Clinical Research	4

Schlagwort	Anzahl
Cloud Computing	12
Cloud Computing_Distributed	1
Co-Creation of Trust	1
Collaboration	1
Collaborative Care	1
Collaborative security	1
Computer networks	1
Computer science	1
Conformance	1
context-aware	1
Control Systems	1
Corruption	1
Cosmos Framework	1
Cost containment	1
Cryptocurrencies	1
Cryptography	9
Cryptography_ Secured Data Storage	1
Cryptography_Protocols	1
Crypto-spatial coordinate system	1
Data Accessibility	1
Data Asset	1
Data Consolidation	1
Data Control	1
data integration	1
Data integrity	3
Data preservation	1
Data processing	1
Data protection	2
Data provenance	1
Data Quality	1
Data retrieval	1
Data Sharing	13
Data Trading	1
database	3
Decentralised processing	1
Decentralization	5
Decentralized app	1
Decentralized network	1
Decentralized Technology	1
DevOps	1
Digital currencies	1
Digital Ecosystems	1
Digital health identity	1
digital healthcare	1
Digital Ledger	1
digital register	1

Schlagwort	Anzahl	Schlagwort	Anzahl
digital trust	1	Identity_Authentication	1
Digitalization	1	Identity_IAM_General	10
Direct Primary Care	1	Identity_Management	1
Discrete Wavelet Transform	1	Implementation	1
Distributed and parallel computing	1	Incentive Mechanism	1
Distributed Databases	3	Indexing	1
Distributed Ledger Technologies (DLT)	7	Indicator-centric schema	1
Distributed Systems	6	Industry 4.0	1
DNA Sequencing	1	Information security	1
document integrity	1	Information sharing	1
DoubleChainMethod	1	innovation	1
Drug tracking	1	Integration	1
Ecosystems	2	Integrity	2
Efficiency	1	Intel SGX	2
eHealth	9	Intellectual property	1
eHealth system	1	Internet access	1
electronic medical card (EMC)	1	Internet-of-military things	1
Evaluation	1	Interoperability	12
Finance	1	InterPlanetary File System	1
Framework	2	Intrusion-prevention system	1
fuzzy vault	1	Investments	1
GDPR	1	IoT	9
GDPR_Right to be forgotten	1	IoT_Security	1
Genetic Algorithm	1	IPFS	1
Genomics	2	Keyless signature infrastructure (KSI)	1
Global	1	Law	1
goal-oriented requirements engineering	1	Logging	3
Government	2	machine learning	4
Guidelines	1	maintenance	1
Health Care data	2	Master Patient Index (MPI)	1
Health Care data sharing	1	Measurement	1
Health Care industry	2	Medical Computing	1
Health Care policy	2	Medical Data	5
Health Care utilization	1	Medical data sharing	3
Health data storage	1	Medical data storage	1
Health information	4	Medical database management	1
Health Information Exchange (HIE)	5	Medical diagnostic imaging	2
Health information system	3	Medical education	1
Health insurance	2	Medical Information Sharing	1
HIBBE system	1	medical information systems	3
Holistic Approach	1	Medical personnel	1
Homomorphic Encryption	1	Medical research	1
Hospitals	3	Medical sensors	1
Identity	23	Medical services	7
Identity_Access Control	6	Medicine	4
Identity_Access Control_Fine-Grained	1	Merkle-tree	2
Identity_Access Control_Role-based	1	mHealth	3
Identity_Access Control_User-centered	1	MIMIC-III	1

Schlagwort	Anzahl
mobile computing	1
Mobile Platform	2
Multi-parties computing	1
multiple access system	1
multiple authorities	1
multisignature data access	1
MyHealthMyData	1
Nebula	1
Non-Reputation Systems	1
Open access	1
Openness	1
Opportunities	1
Organizations	2
Overlaying network	1
Ownership	1
Parallel Healthcare Systems	1
Parallel Intelligence	1
Patent Data	1
Patient Centric Medicine	1
patient examination	1
Patient Identity	1
patient-centered care	1
Payment Models	1
Peer-to-peer computing	4
Performance evaluation	1
Persistent Monitoring	1
personal data	1
Personal health data	1
Personal Health Information (PHI)	2
Pharmaceuticals	2
Platforms	1
PPG signals	1
Precision medicine	2
Privacy	38
Privacy_Preservation	4
Privacy_Protection	3
Privacy_Risk	1
proxy re-encryption	2
Pseudonyme	2
Public finance	1
Public Health Surveillance	2
Public Key Infrastructure_digital signatures	1
Public Key Infrastructure_PKI	1
Public participation	1
Records (EHR)	16
Records (EMR)	10
Records (EMR)_Record Management	3
Records (lifetime)	1
Records (PHR)	3
Reliability	2
Remote monitoring	1
Reproducibility	1
Requirements and Challenges	1
Research & Development	1
Root exploit	1
Scalability	2
Scientometrics	1
Secret sharing	1
Secure Multiparty Computation	1
Secure storage	1
Security	49
Security_Predictive	1
Security_Protocol	1
Security_Storage	1
Self-Sovereignty	3
Sensitive data	1
smart and connected	1
Smart City	3
Smart Contracts	17
Smart Healthcare	1
Smart Medicine	1
software	1
Stakeholders	1
Static analysis	1
Stichwortsuche	1
Students	1
Subsidies	1
suitability	1
Supply chain	1
System design	1
Systematic review	1
Telemedicine	1
Throughput	1
Timestamped algorithm	1
Tokenization	2
Transparency	1
Trust	3
Virtual Assistants	1
Wearables	4

Anhang D: Verteilung der Literatur unterteilt nach Sicht

Tabelle D-1: Literatur-Kategorien ‚Record Type' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Variation	PUB-I	PUB-II
Clinical Trial/Clinical Research	Kuo/Ohno-Machado (2018)	Angeletti/Chatzigiannakis/Vitaletti (2017); Benchoufi/Ravaud (2017); Dubovitskaya et al. (2017); Shae/Tsai (2017); Bell et al. (2018); Cisneros/Aarestrup/Lund (2018); Radanović/Likić (2018)
Electronic Health Record (EHR)	Gropper (2016); Xia et al. (2017a); Hanley/Tewari (2018); Yang/Li (2018); Zhang et al. (2018b)	Liu (2016); Angraal/Krumholz/Schulz (2017); Magyar (2017); Hussein et al. (2018); Jiang/Peng/Dian (2018); Nagasubramanian et al. (2018); Pirtle/Ehrenfeld (2018); Pussewalage/Oleshchuk (2018); Sun et al. (2018); Zhang/Poslad/Ma (2018)
Insurance and other payers	Zhou/Wang/Sun (2018)	Liang et al. (2017b); Liang et al. (2018a); Radanović/Likić (2018)
Patient Summary	Staffa et al. (2018)	Castaldo/Cinque (2018)
Patient Health Record (PHR)	Azaria et al. (2016); Ekblaw et al. (2016); Gropper (2016); Yue et al. (2016); Ahram et al. (2017); Al Omar et al. (2017); McFarlane et al. (2017); Chang et al. (2018); Du et al. (2018); Fan et al. (2018); Ito/Tago/Jin (2018); Jiang et al. (2018); Medicalchain (2018); Quaini et al. (2018); Rouhani et al. (2018); Vora et al. (2018); Xiao et al. (2018); Zhang/Lin (2018)	Linn/Koo (2016); Nichol/Brandt (2016); Cunningham/Ainsworth (2017); Dubovitskaya et al. (2017); Genestier et al. (2017); Kim/Hong (2017); Liang et al. (2017b); Noh et al. (2017); Rifi et al. (2017); Roehrs/da Costa/da Rosa Righi (2017); Yang/Yang (2017); Zhang et al. (2017); Alexaki et al. (2018); Amofa et al. (2018); Badr/Gomaa/Abd-Elrahman (2018); Bell et al. (2018); Bhuiyan et al. (2018); Chen et al. (2018b); Chen et al. (2018a); Chowdhury et al. (2018); Conceição et al. (2018); Cyran (2018); Dagher et al. (2018); Esposito et al. (2018); Gagnon/Stephen (2018); Gökalp et al. (2018); Gordon/Catalini (2018); Grishin et al. (2018); Guo et al. (2018); Han et al. (2018); Jiang/Peng/Dian (2018); Kamau et al. (2018); Kotsiuba et al. (2018); Liang et al. (2018a); Liang et al. (2018b); Liu et al. (2018); Mendes et al. (2018); Mense/Athanasiadis (2018); Novikov et al. (2018); Patel (2018); Radanović/Likić (2018); Ramani et al. (2018); Theodouli et al. (2018); Thwin/Vasupongayya (2018); Wang et al. (2018b); Wang et al. (2018a); Wang/Song (2018); Zheng et al. (2018); Zhuang et al. (2018)

Tabelle D-2: Literatur-Kategorien ‚Data Storage & Provisioning' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
Central Database	Hanley/Tewari (2018); Jiang et al. (2018); Medicalchain (2018)	Linn/Koo (2016); Bhuiyan et al. (2018); Chowdhury et al. (2018); Gökalp et al. (2018)
Chain_Off-Chain	Azaria et al. (2016); Ekblaw et al. (2016); Gropper (2016); McFarlane et al. (2017); Chang et al. (2018); Fan et al. (2018); Hanley/Tewari (2018); Ito/Tago/Jin (2018); Jiang et al. (2018); Medicalchain (2018);	Linn/Koo (2016); Dubovitskaya et al. (2017); Lo et al. (2017); Magyar (2017); Rifi et al. (2017); Simić/Sladić/Milosavljević (2017); Banerjee/Lee/Choo (2018); Bayle et al. (2018); Bhuiyan et al. (2018); Chen et al.

	Quaini et al. (2018); Rouhani et al. (2018); Vora et al. (2018); Xiao et al. (2018); Yang/Li (2018); Zhang et al. (2018b)	(2018a); Chen et al. (2018b); Chowdhury et al. (2018); Cisneros/Aarestrup/Lund (2018); Conceição et al. (2018); Desai et al. (2018); Esposito et al. (2018); Gagnon/Stephen (2018); Gökalp et al. (2018); Jiang/Peng/Dian (2018); Kaur et al. (2018); Liu et al. (2018); Mense/Athanasiadis (2018); Nagasubramanian et al. (2018); Patel (2018); Pirtle/Ehrenfeld (2018); Pukas/Smal/Zabchuk (2018); Ribitzky et al. (2018); Sun et al. (2018); Theodouli et al. (2018); Wang et al. (2018b); Zheng et al. (2018)
Chain_On-Chain	Ahram et al. (2017); Al Omar et al. (2017); Zhang/Lin (2018); Zhou/Wang/Sun (2018)	Benhamouda/Halevi/Halevi (2018); Han et al. (2018)
Cloud	Yue et al. (2016); Ahram et al. (2017); McFarlane et al. (2017); Xia et al. (2017a); Du et al. (2018)	Dubovitskaya et al. (2017); Liang et al. (2017a); Liang et al. (2017b); Noh et al. (2017); Xia et al. (2017b); Yang/Yang (2017); Badr/Gomaa/Abd-Elrahman (2018); Chen et al. (2018b); Chowdhury et al. (2018); Conceição et al. (2018); Desai et al. (2018); Esposito et al. (2018); Grishin et al. (2018); Guo et al. (2018); Hussein et al. (2018); Kaur et al. (2018); Liang et al. (2018b); Liang et al. (2018a); Liu et al. (2018); Nagasubramanian et al. (2018); Theodouli et al. (2018); Thwin/Vasupongayya (2018); Wang/Song (2018); Zhang et al. (2018a); Zheng et al. (2018)
Interoperability	Azaria et al. (2016); Ekblaw et al. (2016); Gropper (2016); McFarlane et al. (2017); Ito/Tago/Jin (2018); Kuo/Ohno-Machado (2018); Quaini et al. (2018); Zhang et al. (2018b); Zhang/Lin (2018)	Linn/Koo (2016); Nichol/Brandt (2016); Randall/Goel/Abujamra (2017); Roehrs/da Costa/da Rosa Righi (2017); Yang/Yang (2017); Gordon/Catalini (2018); Kamau et al. (2018); Kaur et al. (2018); Mense/Athanasiadis (2018); Ribitzky et al. (2018)
InterPlanetary File System	Hanley/Tewari (2018); Quaini et al. (2018)	Rifi et al. (2017); Cisneros/Aarestrup/Lund (2018); Cyran (2018); Grishin et al. (2018); Ribitzky et al. (2018); Wu et al. (2018)
Data Provisioning_ (Database) Gatekeeper	Azaria et al. (2016); Ekblaw et al. (2016)	Dagher et al. (2018); Pukas/Smal/Zabchuk (2018); Zhang et al. (2018a)
Data Provisioning_ Index	Yang/Li (2018)	Simić/Sladić/Milosavljević (2017); Banerjee/Lee/Choo (2018); Chen et al. (2018b); Chen et al. (2018a); Dagher et al. (2018); Li et al. (2018); Liu et al. (2018)
Data Provisioning_ Pointer/Link/URL/URI	Azaria et al. (2016); Ekblaw et al. (2016); McFarlane et al. (2017); Chang et al. (2018); Du et al. (2018); Fan et al. (2018); Hanley/Tewari (2018); Medicalchain (2018); Quaini et al. (2018); Rouhani et al. (2018); Vora	Linn/Koo (2016); Peterson et al. (2016); Rifi et al. (2017); Bayle et al. (2018); Bhuiyan et al. (2018); Conceição et al. (2018); Kaur et al. (2018); Patel (2018); Ribitzky et al. (2018); Sun et al. (2018); Theodouli et al. (2018)

	et al. (2018); Xiao et al. (2018); Zhang et al. (2018b)	

Tabelle D-3: Literatur-Kategorien ‚Security' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
Access Management	Azaria et al. (2016); Ekblaw et al. (2016); Al Omar et al. (2017); McFarlane et al. (2017); Chang et al. (2018); Medicalchain (2018); Quaini et al. (2018); Rouhani et al. (2018); Xiao et al. (2018); Yang/Li (2018); Zhang et al. (2018b)	Zyskind/Nathan/Pentland (2015); Linn/Koo (2016); Alhadhrami et al. (2017); Dubovitskaya et al. (2017); Genestier et al. (2017); Kim/Hong (2017); Liu et al. (2017); Rifi et al. (2017); Xia et al. (2017b); Cyran (2018); Dias et al. (2018); Hussein et al. (2018); Mikula/Jacobsen (2018); Patel (2018); Pussewalage/Oleshchuk (2018); Ramani et al. (2018); Ribitzky et al. (2018); Theodouli et al. (2018); Zhang et al. (2018a); Zhang/Poslad/Ma (2018)
Identity Management	Azaria et al. (2016); Ekblaw et al. (2016); Gropper (2016); Al Omar et al. (2017); Fan et al. (2018); Hanley/Tewari (2018); Jiang et al. (2018); Medicalchain (2018); Quaini et al. (2018); Rouhani et al. (2018); Vora et al. (2018); Zhang et al. (2018b); Zhang/Lin (2018)	Zyskind/Nathan/Pentland (2015); Linn/Koo (2016); Peterson et al. (2016); Yli-Huumo et al. (2016); Cunningham/Ainsworth (2017); Dubovitskaya et al. (2017); Genestier et al. (2017); Liang et al. (2017b); Liu et al. (2017); Noh et al. (2017); Yang/Yang (2017); Badr/Gomaa/Abd-Elrahman (2018); Bhuiyan et al. (2018); Castaldo/Cinque (2018); Chen et al. (2018a); Chen et al. (2018b); Chowdhury et al. (2018); Conceição et al. (2018); Gagnon/Stephen (2018); Gordon/Catalini (2018); Gutierrez et al. (2018); Liang et al. (2018a); Liang et al. (2018b); Mense/Athanasiadis (2018); Mikula/Jacobsen (2018); Pukas/Smal/Zabchuk (2018); Pussewalage/Oleshchuk (2018); Qiu et al. (2018); Ramani et al. (2018); Sharma/Sekharan/Zuo (2018); Thwin/Vasupongayya (2018); Wu/Tsai (2018); Zhang et al. (2018a)
Infrastructure	Fan et al. (2018); Rouhani et al. (2018); Xiao et al. (2018); Zhang et al. (2018b); Zhou/Wang/Sun (2018)	Nichol/Brandt (2016); Benchoufi/Ravaud (2017); Dubovitskaya et al. (2017); Genestier et al. (2017); Liang et al. (2017a); Liang et al. (2017b); Liu et al. (2017); Noh et al. (2017); Bhuiyan et al. (2018); Castaldo/Cinque (2018); Gordon/Catalini (2018); Liang et al. (2018a); Nagasubramanian et al. (2018); Thwin/Vasupongayya (2018); Zhang et al. (2018a); Zheng et al. (2018)
Logging & Audit	Azaria et al. (2016); Ekblaw et al. (2016); Xia et al. (2017a); Chang et al. (2018); Fan et al. (2018); Hanley/Tewari (2018); Jiang et al. (2018); Staffa et al. (2018); Vora et al. (2018); Xiao et al. (2018); Yang/Li (2018); Zhang et al. (2018b)	Liu (2016); Angeletti/Chatzigiannakis/Vitaletti (2017); Kiyomoto/Rahman/Basu (2017); Noh et al. (2017); Yang/Yang (2017); Amofa et al. (2018); Banerjee/Lee/Choo (2018); Bayle et al. (2018); Castaldo/Cinque (2018); Chen et al. (2018b); Chen et al. (2018a); Chowdhury et al. (2018); Dagher et al.

		(2018); Liang et al. (2018b); Mense/Athanasiadis (2018); Pukas/Smal/Zabchuk (2018); Theodouli et al. (2018); Thwin/Vasupongayya (2018); Wang et al. (2018b); Wu et al. (2018)

Tabelle D-4: Literatur-Kategorien ‚Technology' in PUB-I und PUB-II (Quelle: Eigene Darstellung)

Kategorie	PUB-I	PUB-II
Blockchain-Technology	Azaria et al. (2016); Ekblaw et al. (2016); Ahram et al. (2017); McFarlane et al. (2017); Chang et al. (2018); Hanley/Tewari (2018); Ito/Tago/Jin (2018); Medicalchain (2018); Quaini et al. (2018); Rouhani et al. (2018); Vora et al. (2018); Xiao et al. (2018); Zhang et al. (2018b); Zhou/Wang/Sun (2018)	Zyskind/Nathan/Pentland (2015); Angeletti/Chatzigiannakis/Vitaletti (2017); Angraal/Krumholz/Schulz (2017); Cunningham/Ainsworth (2017); Dubovitskaya et al. (2017); Genestier et al. (2017); Kim/Hong (2017); Kiyomoto/Rahman/Basu (2017); Liang et al. (2017b); Rifi et al. (2017); Yang/Yang (2017); Zhang et al. (2017); Alexaki et al. (2018); Amofa et al. (2018); Bell et al. (2018); Benhamouda/Halevi/Halevi (2018); Bhuiyan et al. (2018); Brogan/Baskaran/Ramachandran (2018); Castaldo/Cinque (2018); Chen et al. (2018a); Chowdhury et al. (2018); Colón (2018); Conceição et al. (2018); Cyran (2018); Dagher et al. (2018); Desai et al. (2018); Li et al. (2018); Liang et al. (2018a); Mendes et al. (2018); Mikula/Jacobsen (2018); Novikov et al. (2018); Pukas/Smal/Zabchuk (2018); Ramani et al. (2018); Thwin/Vasupongayya (2018); Zhang et al. (2018a); Zheng et al. (2018)
Coin/Token	Azaria et al. (2016); Ekblaw et al. (2016); McFarlane et al. (2017); Du et al. (2018); Kuo/Ohno-Machado (2018); Medicalchain (2018); Zhou/Wang/Sun (2018)	Magyar (2017); Wanitcharakkhakul/Rotchanakitumnuai (2017); Colón (2018); Grishin et al. (2018); Zheng et al. (2018)
Consensus Protocol	Ahram et al. (2017); Chang et al. (2018); Du et al. (2018); Jiang et al. (2018); Kuo/Ohno-Machado (2018); Yang/Li (2018); Zhang/Lin (2018); Zhou/Wang/Sun (2018)	Cunningham/Ainsworth (2017); Dubovitskaya et al. (2017); Kiyomoto/Rahman/Basu (2017); Chen et al. (2018b); Chen et al. (2018a); Chowdhury et al. (2018); Dagher et al. (2018); Han et al. (2018); Hölbl et al. (2018); Jiang/Peng/Dian (2018); Kombe/Ally/Sam (2018); Kotsiuba et al. (2018); Liang et al. (2018a); Liu et al. (2018); Mendes et al. (2018); Patel (2018); Sun et al. (2018); Thwin/Vasupongayya (2018); Wang et al. (2018a); Wang et al. (2018b); Zhang et al. (2018a)
Quantity	Azaria et al. (2016); Ekblaw et al. (2016); Ahram et al. (2017); Al Omar et al. (2017); McFarlane et al. (2017); Chang et al. (2018); Hanley/Tewari (2018); Ito/Tago/Jin (2018); Jiang et al. (2018); Kuo/Ohno-Machado (2018); Medicalchain (2018); Quaini et al. (2018); Rouhani et al. (2018); Staffa et al. (2018); Vora et al. (2018); Xiao et al. (2018); Yang/Li (2018);	Zyskind/Nathan/Pentland (2015); Linn/Koo (2016); Angeletti/Chatzigiannakis/Vitaletti (2017); Angraal/Krumholz/Schulz (2017); Cunningham/Ainsworth (2017); Dubovitskaya et al. (2017); Genestier et al. (2017); Kim/Hong (2017); Kiyomoto/Rahman/Basu (2017); Liang et al. (2017b); Liang et al. (2017a); Magyar (2017); Noh et al. (2017); Rifi et al. (2017); Wanitcharakkhakul/Rotchanakitumnuai (2017); Yang/Yang (2017); Zhang et al. (2017); Alexaki et al. (2018); Amofa et al. (2018); Badr/Gomaa/Abd-Elrahman (2018); Banerjee/Lee/Choo (2018); Bayle et al. (2018); Bell et al. (2018); Benhamouda/Halevi/Halevi (2018); Bhuiyan et al. (2018); Brogan/Baskaran/Ramachandran (2018); Castaldo/Cinque (2018); Chen et al. (2018a); Chowdhury et al. (2018); Cisneros/Aarestrup/Lund (2018); Colón (2018); Conceição et al. (2018); Cyran (2018);

	Zhang et al. (2018b); Zhang/Lin (2018); Zhou/Wang/Sun (2018)	Dagher et al. (2018); Desai et al. (2018); Dias et al. (2018); Gökalp et al. (2018); Han et al. (2018); Jiang/Peng/Dian (2018); Li et al. (2018); Liang et al. (2018a); Liu et al. (2018); Mendes et al. (2018); Mikula/Jacobsen (2018); Novikov et al. (2018); Pukas/Smal/Zabchuk (2018); Ramani et al. (2018); Sun et al. (2018); Thwin/Vasupongayya (2018); Wang et al. (2018a); Wang et al. (2018b); Wu et al. (2018); Zhang et al. (2018a); Zheng et al. (2018); Zhuang et al. (2018)
Smart Contract/Chain-code	Azaria et al. (2016); Ekblaw et al. (2016); Ahram et al. (2017); Al Omar et al. (2017); Xia et al. (2017a); Chang et al. (2018); Ito/Tago/Jin (2018); Quaini et al. (2018); Rouhani et al. (2018); Vora et al. (2018); Yang/Li (2018); Zhang et al. (2018b)	Peterson et al. (2016); Benchoufi/Ravaud (2017); Dubovitskaya et al. (2017); Genestier et al. (2017); Kim/Hong (2017); Liang et al. (2017b); Simić/Sladić/Milosavljević (2017); Yang/Yang (2017); Alexaki et al. (2018); Amofa et al. (2018); Benhamouda/Halevi/Halevi (2018); Bhuiyan et al. (2018); Chen et al. (2018a); Colón (2018); Conceição et al. (2018); Cyran (2018); Dagher et al. (2018); Desai et al. (2018); Gökalp et al. (2018); Grishin et al. (2018); Kumar et al. (2018); Liang et al. (2018a); Liu et al. (2018); Mense/Athanasiadis (2018); Novikov et al. (2018); Pukas/Smal/Zabchuk (2018); Qiu et al. (2018); Radanović/Likić (2018); Theodouli et al. (2018); Zhang et al. (2018a); Zhou et al. (2018); Zhuang et al. (2018)
Taxonomy	Azaria et al. (2016); Ekblaw et al. (2016); Ahram et al. (2017); Al Omar et al. (2017); McFarlane et al. (2017); Chang et al. (2018); Hanley/Tewari (2018); Ito/Tago/Jin (2018); Kuo/Ohno-Machado (2018); Medicalchain (2018); Quaini et al. (2018); Rouhani et al. (2018); Staffa et al. (2018); Vora et al. (2018); Xiao et al. (2018); Yang/Li (2018); Zhang et al. (2018b); Zhang/Lin (2018); Zhou/Wang/Sun (2018)	Zyskind/Nathan/Pentland (2015); Linn/Koo (2016); Angeletti/Chatzigiannakis/Vitaletti (2017); Cunningham/Ainsworth (2017); Dubovitskaya et al. (2017); Genestier et al. (2017); Kim/Hong (2017); Kiyomoto/Rahman/Basu (2017); Liang et al. (2017b); Liang et al. (2017a); Magyar (2017); Noh et al. (2017); Rifi et al. (2017); Wanitcharakkhakul/Rotchanakitumnuai (2017); Yang/Yang (2017); Alexaki et al. (2018); Amofa et al. (2018); Badr/Gomaa/Abd-Elrahman (2018); Bayle et al. (2018); Bell et al. (2018); Benhamouda/Halevi/Halevi (2018); Bhuiyan et al. (2018); Brogan/Baskaran/Ramachandran (2018); Castaldo/Cinque (2018); Chen et al. (2018a); Chowdhury et al. (2018); Cisneros/Aarestrup/Lund (2018); Colón (2018); Conceição et al. (2018); Cyran (2018); Dagher et al. (2018); Desai et al. (2018); Dias et al. (2018); Gökalp et al. (2018); Han et al. (2018); Li et al. (2018); Liang et al. (2018a); Liu et al. (2018); Mendes et al. (2018); Mikula/Jacobsen (2018); Pukas/Smal/Zabchuk (2018); Ramani et al. (2018); Sun et al. (2018); Thwin/Vasupongayya (2018); Wang et al. (2018b); Zhang et al. (2018a); Zheng et al. (2018); Zhuang et al. (2018)

DOI: 10.17185/duepublico/78275
URN: urn:nbn:de:hbz:465-20230420-120649-6